

ZOOM
TECHNOLOGIES



Lab Manual

A Practical Guide to Configuring

AWS

(Amazon Web Services)

Cloud Platform

Lab Manual

© 2017 Zoom Technologies India Pvt. Ltd.

All rights reserved. No part of this book or related material may be reproduced in any form or by any means without prior permission from Zoom Technologies India Pvt. Ltd. All precautions have been taken to make this book and related material error-free. However, Zoom Technologies India Pvt. Ltd. is not liable for any errors or omissions. The contents of this book are subject to change without notice.

DISCLAIMER: AWS, AMAZON, and all associated terms are registered trademarks of Amazon Inc. We are in no way affiliated with Amazon Inc.

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 taught at Zoom Technologies.

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

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

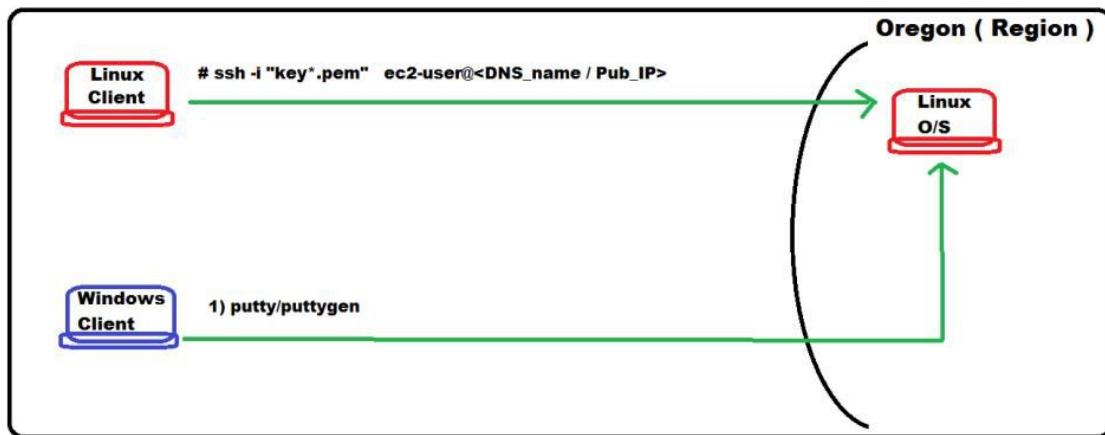
Lab 15: To Configure an Amazon Relational Database Service	337
Lab 16: To Configure Amazon DynamoDB.....	360
Lab 17: To Configure Amazon CloudFormation.....	377
Lab 18: To Configure Amazon Simple E-Mail Service (SES).....	393
Lab 19: To Configure Amazon Simple QUEUE Service SQS	408
Lab 20: To Configure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

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 Windows client PC using putty/puttygen

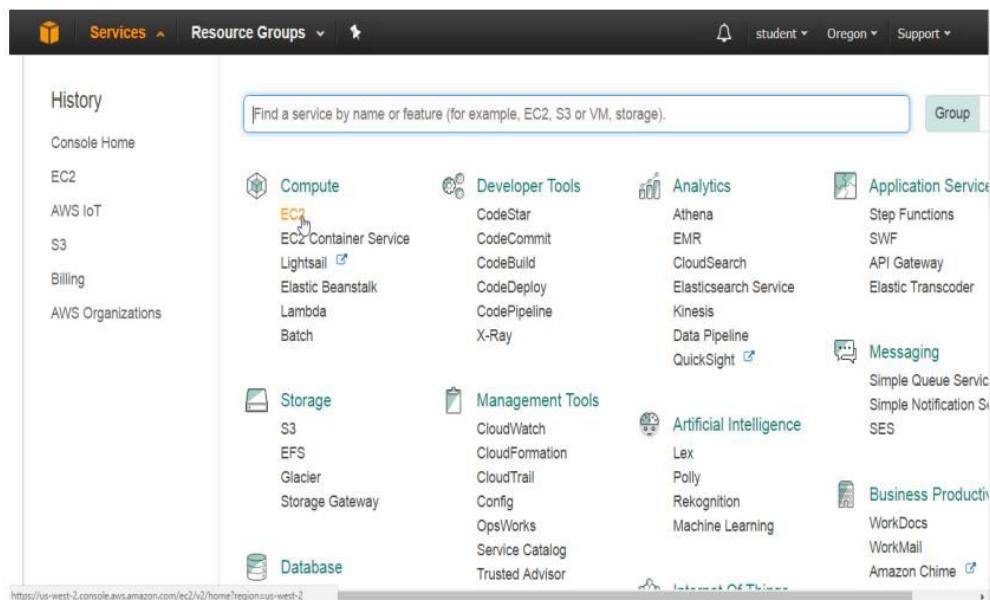
Start/stop/terminate instance

1. To Launch Amazon Linux instance in default VPC

Open the Amazon EC2 console

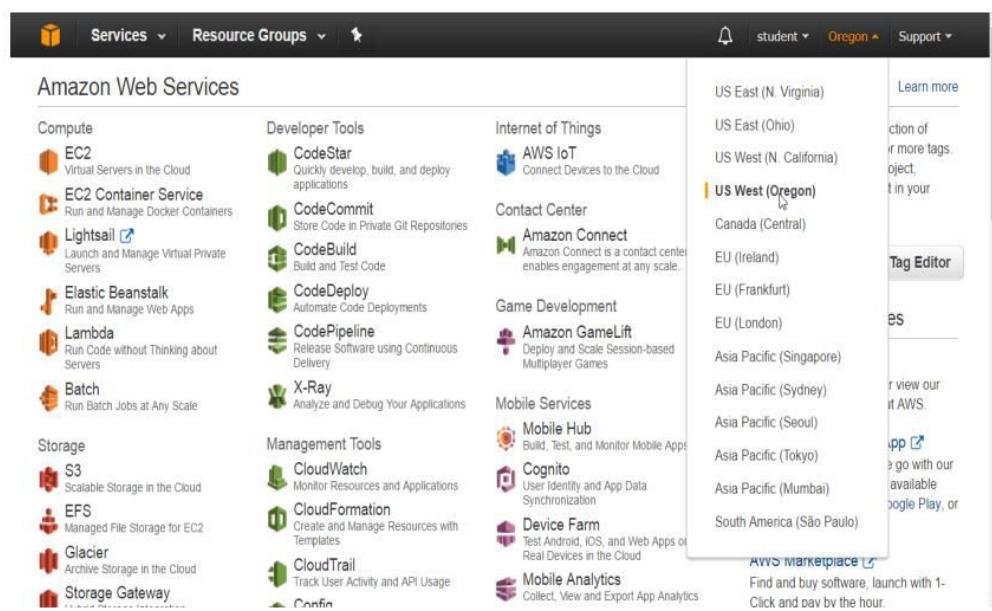
Select **Compute**

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 options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Images, and Elastic Block Store. The main panel is titled "Service Health". It shows "Service Status" with a green checkmark for "US West (Oregon)" and a note that it's operating normally. Below that is "Availability Zone Status" with three green checkmarks for "us-west-2a", "us-west-2b", and "us-west-2c", each noting that the availability zone is operating normally. There's also a link to the "Service Health Dashboard".

From the “EC2 Dashboard” panel

Select Instance

Click on “Launch Instance” button

The screenshot shows the AWS EC2 Instances page. The sidebar on the left is identical to the previous dashboard. The main area has a "Launch Instance" button at the top. Below it is a search bar and a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Two instances are listed: "linuxvma" (Instance ID i-04ca59221f3ac80ba, t2.micro, us-west-2b, shutting-down, None) and "linuxvmb" (Instance ID i-05b8f51f94d4924dd, t2.micro, us-west-2c, shutting-down, None). At the bottom, there are tabs for Description, Status Checks, Monitoring, and Tags, with the Status Checks tab selected. The status checks for both instances show "i-04ca59221f3ac80ba:" and "i-05b8f51f94d4924dd:".

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.**”]

The screenshot shows the AWS Step 1: Choose an Amazon Machine Image (AMI) page. The 'Quick Start' section is selected. The 'Amazon Linux' AMI is highlighted, showing it is 'Free tier eligible'. A 'Select' button is visible next to it.

Step 1: Choose an Amazon Machine Image (AMI)

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

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Free tier only ⓘ

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

Amazon Linux Free tier eligible

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

Root device type: ebs Virtualization type: hvm

Select

64-bit

Red Hat Enterprise Linux 7.3 (HVM), SSD Volume Type - ami-6f68cf0f

Red Hat Free tier eligible

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 EC2 instance creation wizard at Step 2: Choose an Instance Type. The t2.micro instance is selected and highlighted with a blue border. The 'Free tier eligible' badge is visible next to the t2.micro entry. The 'Review and Launch' button is highlighted with a blue box and a cursor arrow pointing to it.

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	No

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

Purchasing option: Request Spot instances

Network: vpc-89c341ee | default-vpc-oregon (default)

Subnet: No preference (default subnet in any Availability Zone)

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

IAM role: None

Shutdown behavior: Stop

Enable termination protection: Protect against accidental termination

Buttons: Cancel, Previous, **Review and Launch**, Next: Add Storage

On “Add Storage”, page

Leave all values as default

Click on “Next: Tag Instance” button

The screenshot shows the AWS EC2 instance creation wizard at Step 4: Add Storage. The top navigation bar includes 'Services', 'Resource Groups', and tabs for 'student', 'Oregon', and 'Support'. Below the tabs are steps 1 through 7: Choose AMI, Choose Instance Type, Configure Instance, **Add Storage**, Add Tags, Configure Security Group, and Review.

Step 4: Add Storage

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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-0ce5f75735518cbdd	8	General Purpose	100 / 3000	N/A	<input checked="" type="checkbox"/>	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 and conditions.](#)

Buttons at the bottom include: Cancel, Previous, **Review and Launch** (highlighted in blue), and Next: Add Tags.

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

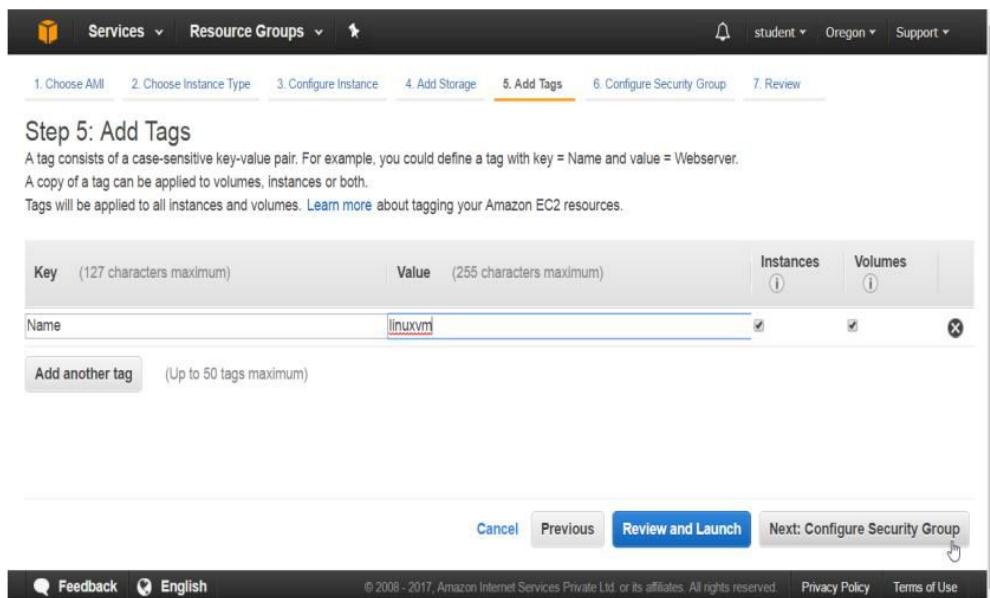
On “Add Tags”, page

Provide following values

Key → Name

Value → linuxvm

Click on “Next: Configure Security Group” button



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

The screenshot shows the AWS EC2 wizard at Step 6: Configure Security Group. The 'Create a new security group' radio button is selected. A new security group named 'launch-wizard-1' is being created with a single rule allowing SSH traffic on port 22 from anywhere. The 'Review and Launch' button is highlighted with a mouse cursor.

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
SSH	TCP	22	Custom 0.0.0.0

Add Rule

Cancel Previous Review and Launch

On “Review Instance Launch”, page

Leave all values as default.

Verify the summary, then drag down

The screenshot shows the AWS EC2 Step 7: Review Instance Launch page. At the top, there are tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. The 7. Review tab is selected. Below the tabs, it says "Step 7: Review Instance Launch". A yellow warning box contains the text: "⚠ 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". The main content area shows "AMI Details" and "Instance Type". Under AMI Details, it lists "Amazon Linux AMI 2017.03.0 (HVM, SSD Volume Type - ami-4836a428)" and indicates "Free tier eligible". Under Instance Type, it lists "t2 micro", "Variable", "1", "1", "EBS only", and "Low to Moderate". At the bottom right, there are "Cancel", "Previous", and a large blue "Launch" button.

Verify the summary

Click on **Launch** button

The screenshot shows the AWS EC2 Step 7: Review Instance Launch page. The "Launch" button is highlighted with a cursor. The summary table includes: Instance Type (t2 micro), ECU (Variable), vCPUs (1), Memory (GiB) (1), Instance Storage (GB) (EBS only), and Network Performance (Low to Moderate). Below the summary, there are sections for "Security Groups" (listing "launch-wizard-1" with a description), "Instance Details", "Storage", and "Tags". At the bottom right, there are "Cancel", "Previous", and a large blue "Launch" button.

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

Select “Create a new key pair”

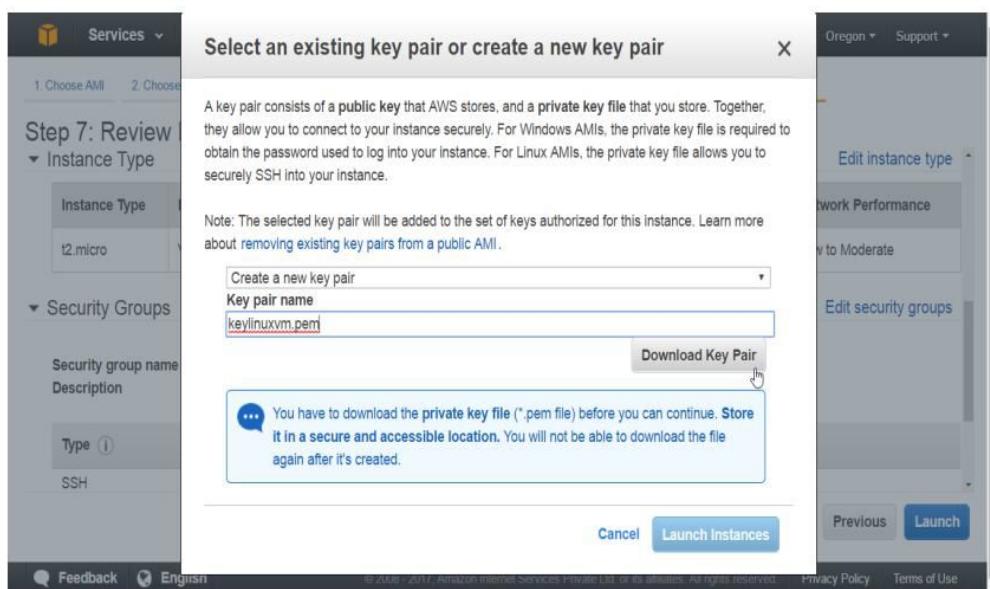
Enter **Key pair name** → keylinuxvm.pem

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 is a navigation bar with icons for Services, Resource Groups, and a bell notification. To the right of the notification icon are dropdown menus for 'student' (set to 'Oregon'), 'Support', and other account details. Below the navigation bar, the main content area is titled 'Launch Status'. It contains a message stating that instances will start immediately and continue to accrue until you stop or terminate them. It also provides a link to 'View Instances' to monitor the status of your instances. A section titled 'Here are some helpful resources to get you started' lists links to 'How to connect to your Linux instance', 'Amazon EC2: User Guide', 'Learn about AWS Free Usage Tier', and 'Amazon EC2: Discussion Forum'. Further down, it suggests creating status check alarms, attaching additional EBS volumes, and managing security groups. At the bottom right of the page, there is a prominent blue 'View Instances' button. The footer of the page includes links for 'Feedback', 'English', and legal notices: '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

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 (which is selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images (AMIs, Bundle Tasks), and Elastic Block Store (Volumes, Snapshots). The main pane shows a table of instances. One instance, named 'linuxvm', is listed with the following details: Instance ID: i-0dad392c31958bef6, Instance Type: t2.micro, Availability Zone: us-west-2b, and Instance State: running (indicated by a green dot). A red circle highlights the 'running' status. At the bottom of the main pane, there are tabs for Description, Status Checks, Monitoring, and Tags, with 'Description' being the active tab.

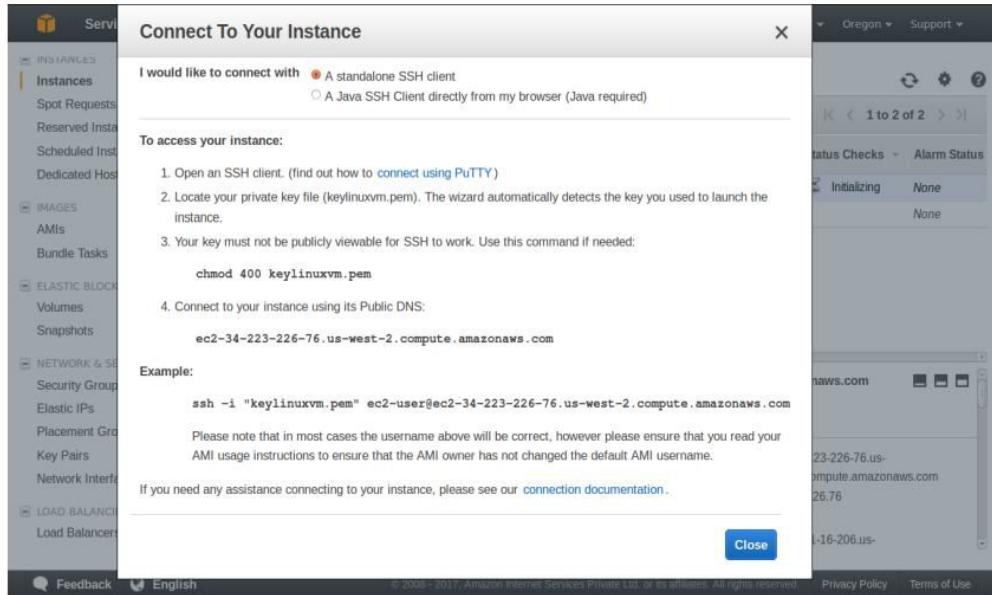
To check instance details like

Description, Status check, Monitoring, Tags

This screenshot is similar to the previous one but focuses on a specific instance named 'linuxvm'. The instance details shown are: Instance ID: i-0dad392c31958bef6, Public DNS: ec2-54-149-138-51.us-west-2.compute.amazonaws.com, Instance State: running, Instance Type: t2.micro, and Availability Zone: us-west-2b. The 'Description' tab is highlighted with a red circle. Below the instance ID, there are sections for Public DNS (IPv4) and IPv6 IPs, Instance state, Instance type, and Elastic IPs. The bottom of the main pane shows the same tabs as the previous screenshot: Description, Status Checks, Monitoring, and Tags, with 'Description' being the active tab.

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.

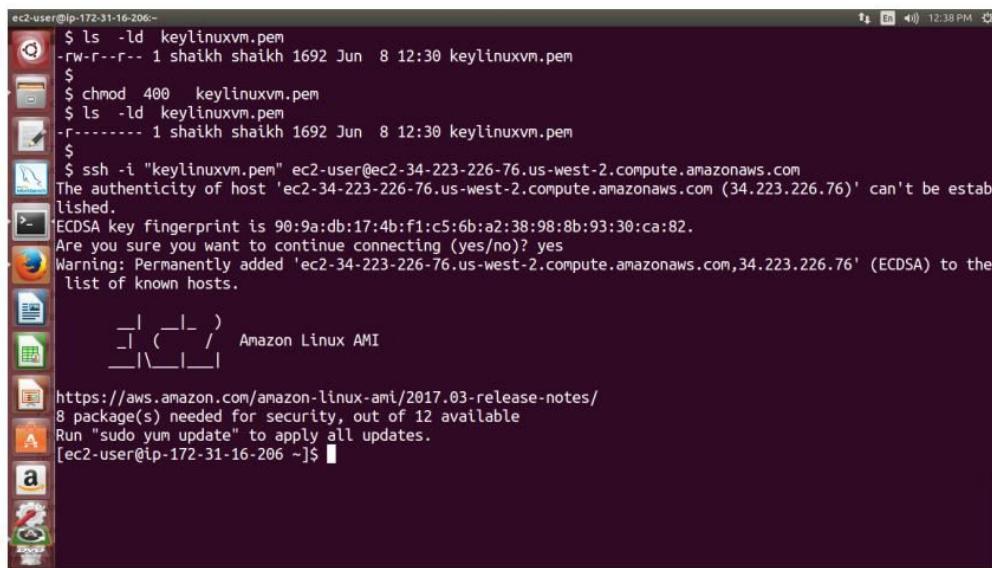


Login to linux client PC, Open the terminal and run following commands.

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

eg : keylinuxvm.pem

```
# ls  
# ll  
# chmod 400 keylinuxvm.pem  
# ssh -i "keylinuxvm.pem" ec2-user@ec2-54-191-200-74.us-west-2.compute.amazonaws.com
```



The screenshot shows a terminal window on an Amazon Linux AMI desktop environment. The user has run the following commands:

```
ec2-user@ip-172-31-16-206:~  
$ ls -ld keylinuxvm.pem  
-rw-r--r-- 1 shaikh shaikh 1692 Jun  8 12:30 keylinuxvm.pem  
$ chmod 400 keylinuxvm.pem  
$ ls -ld keylinuxvm.pem  
-r----- 1 shaikh shaikh 1692 Jun  8 12:30 keylinuxvm.pem  
$  
$ ssh -i "keylinuxvm.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.  
_ | _ / Amazon Linux AMI  
_ | \_ |  
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 ~]$
```

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
```

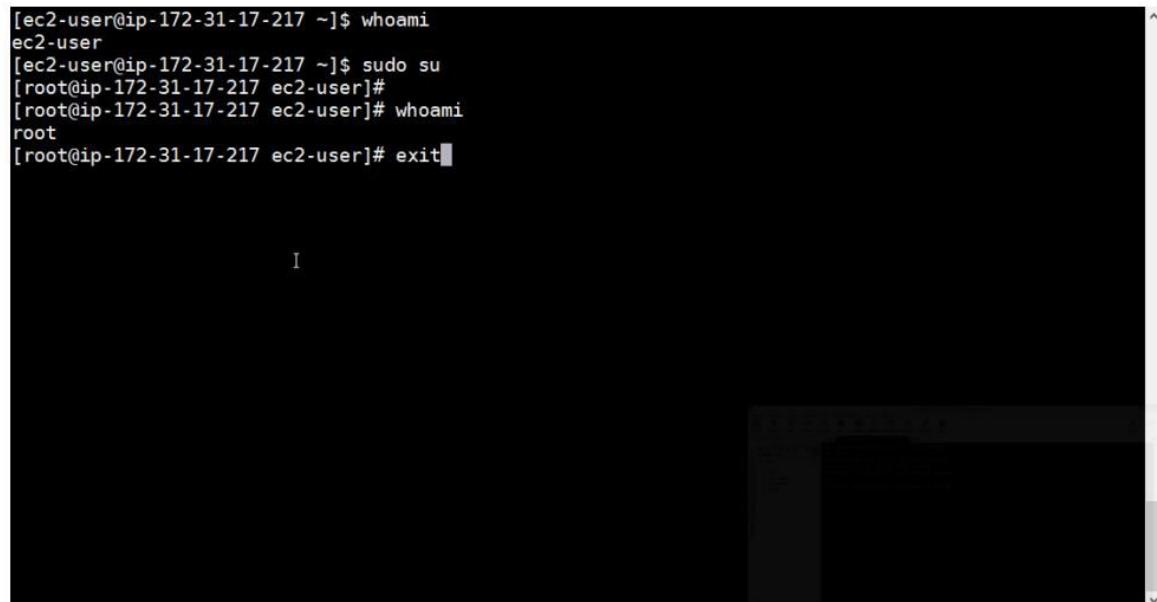
Verify (root user)

```
# whoami
```

To logout

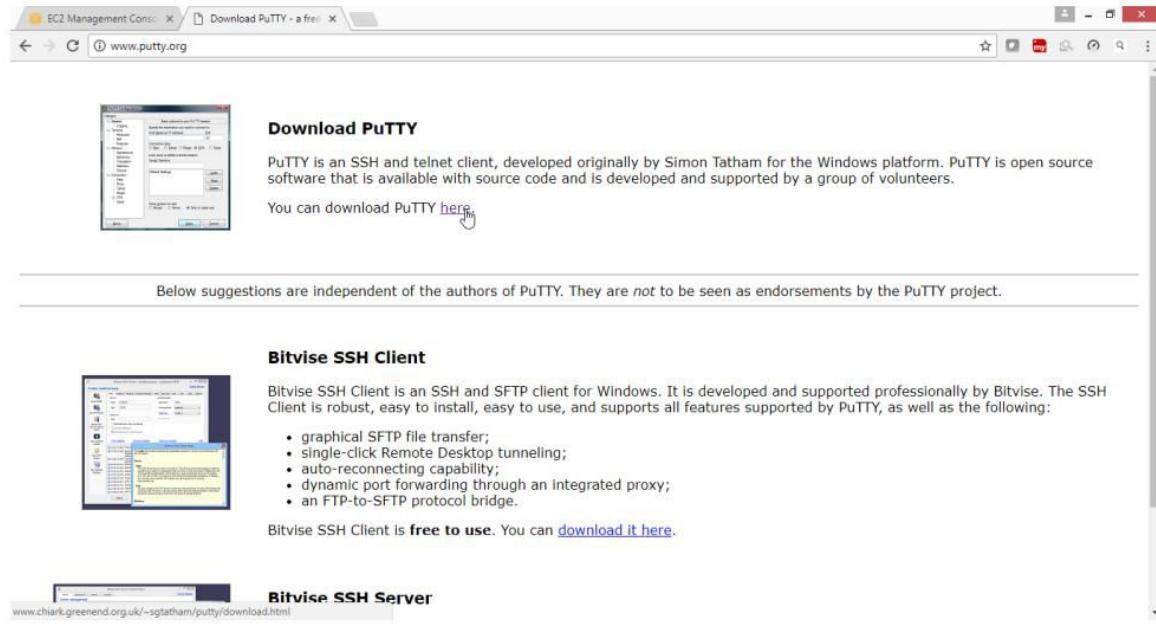
```
# exit
```

```
[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
```



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

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

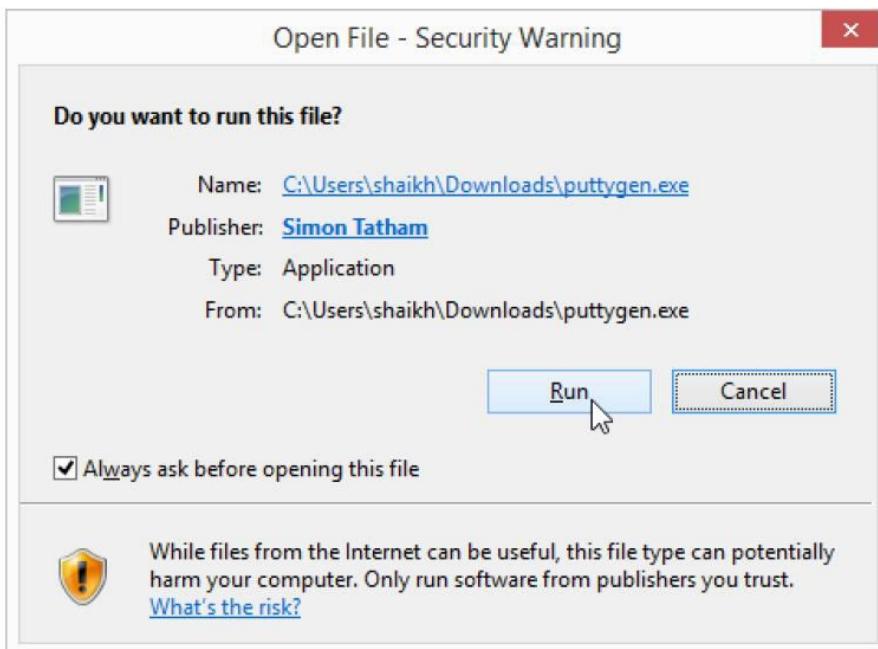


The screenshot shows a web browser window with two tabs open. The active tab is titled "Download PuTTY - a free..." and the URL is "www.putty.org". The content of the page is titled "Download PuTTY" and describes it as an SSH and telnet client developed by Simon Tatham for the Windows platform. It is open source software available with source code and supported by a group of 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." Another section titled "Bitvise SSH Client" is visible, showing its interface and describing it as an SSH and SFTP client developed by Bitvise. It lists several features including graphical SFTP file transfer, single-click Remote Desktop tunneling, auto-reconnecting capability, dynamic port forwarding through an integrated proxy, and an FTP-to-SFTP protocol bridge. A link to download Bitvise SSH Client is also present.

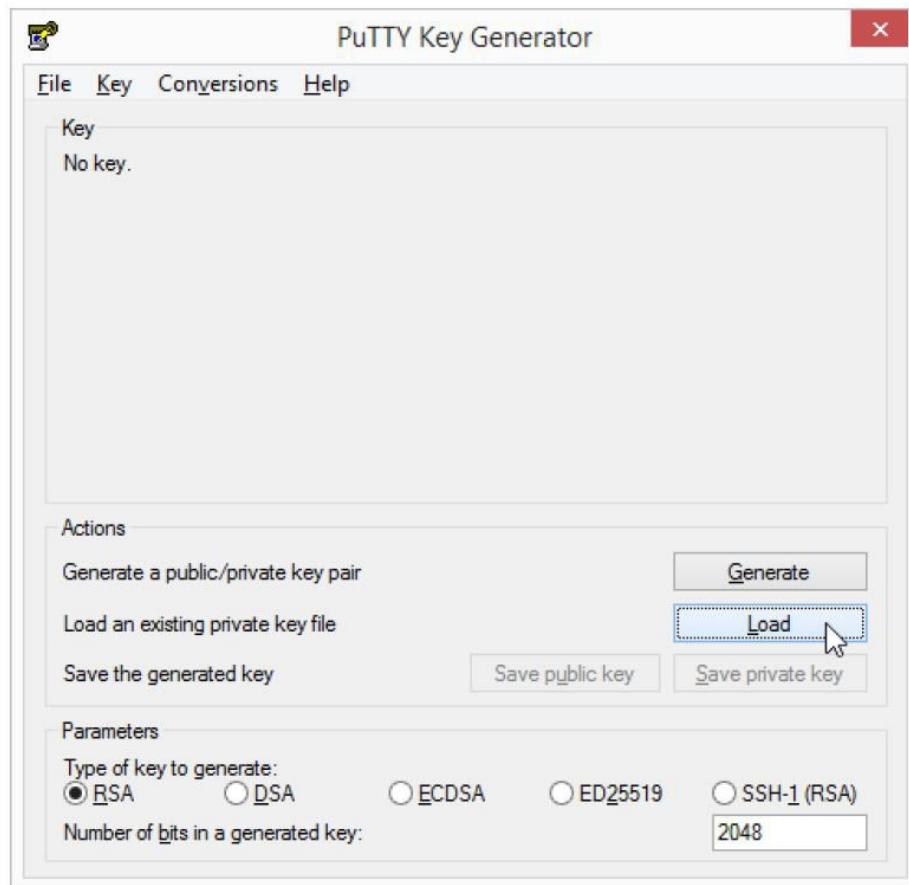
Note: Because putty cannot understand .pem file format, so use puttygen.exe to converting *.pem file into *.ppk format

Click on puttygen.exe file in windows operating system

Click on Run



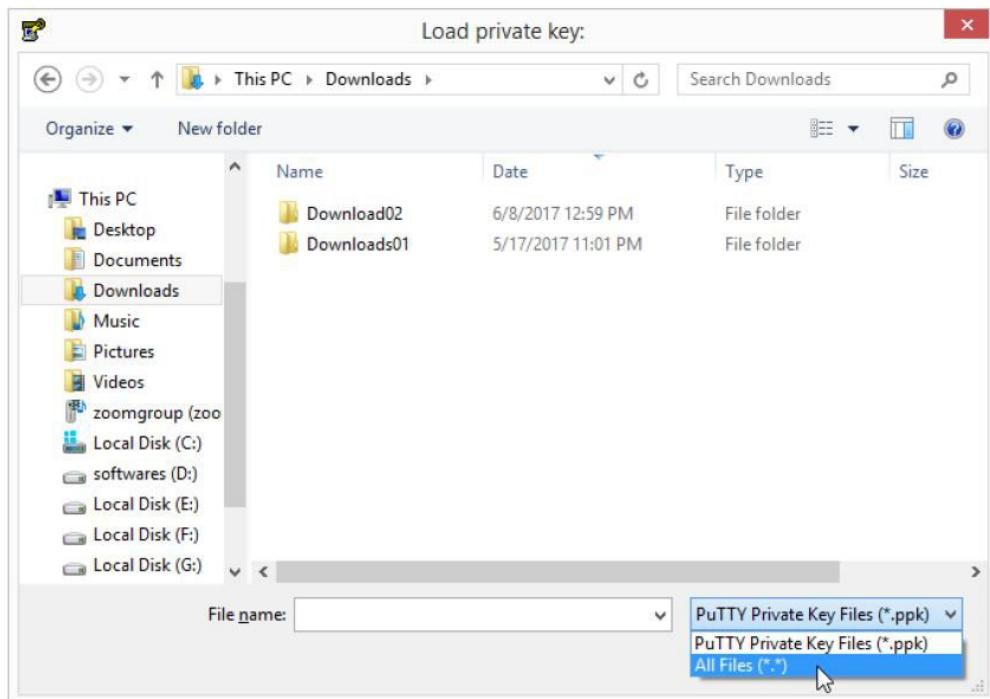
Click on **Load** button



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

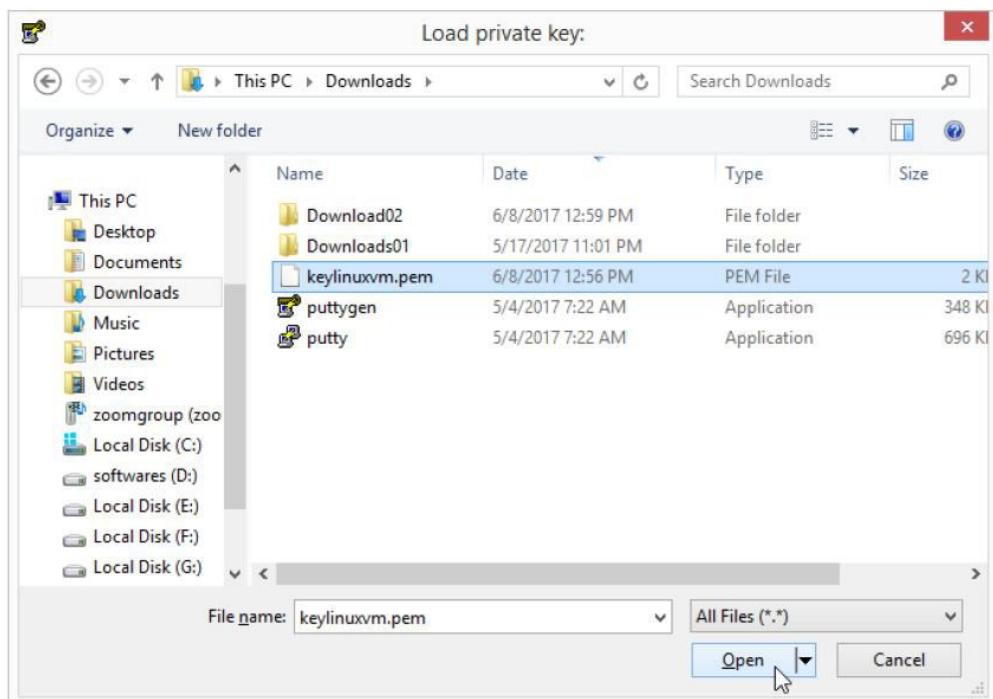
So to locate your .pem file

On file names Select →All files (*.*)

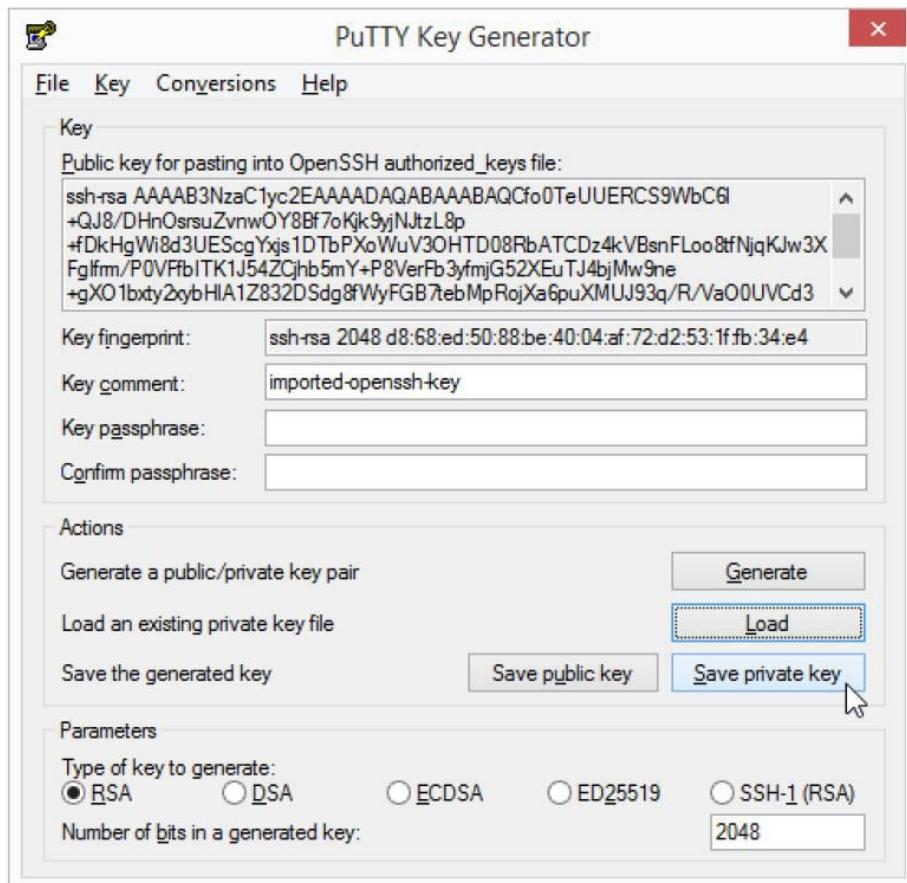


Locate keylinuxvm.pem in your folder

Click on open

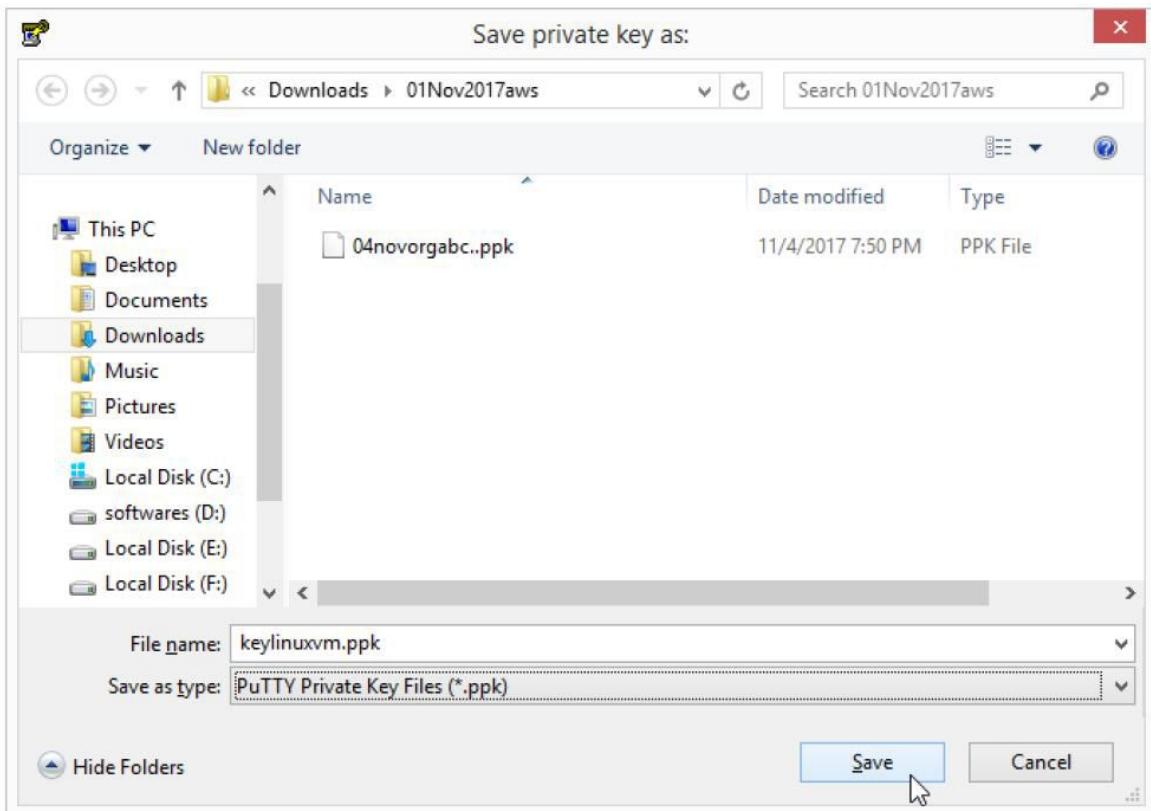


Click on “Save private key” button



Save the file → keylinuxvm.ppk

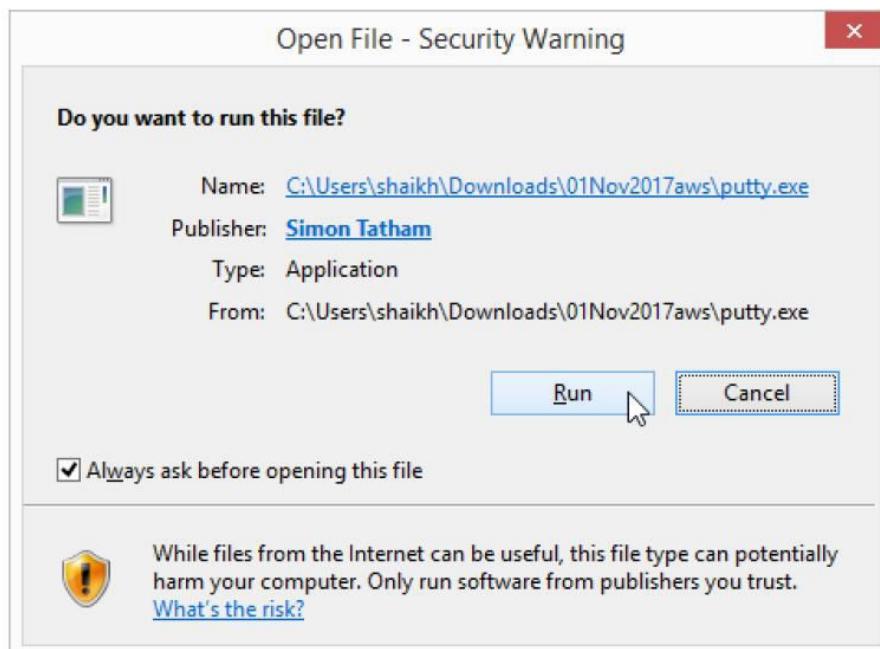
Click on Save button



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

Run putty.exe

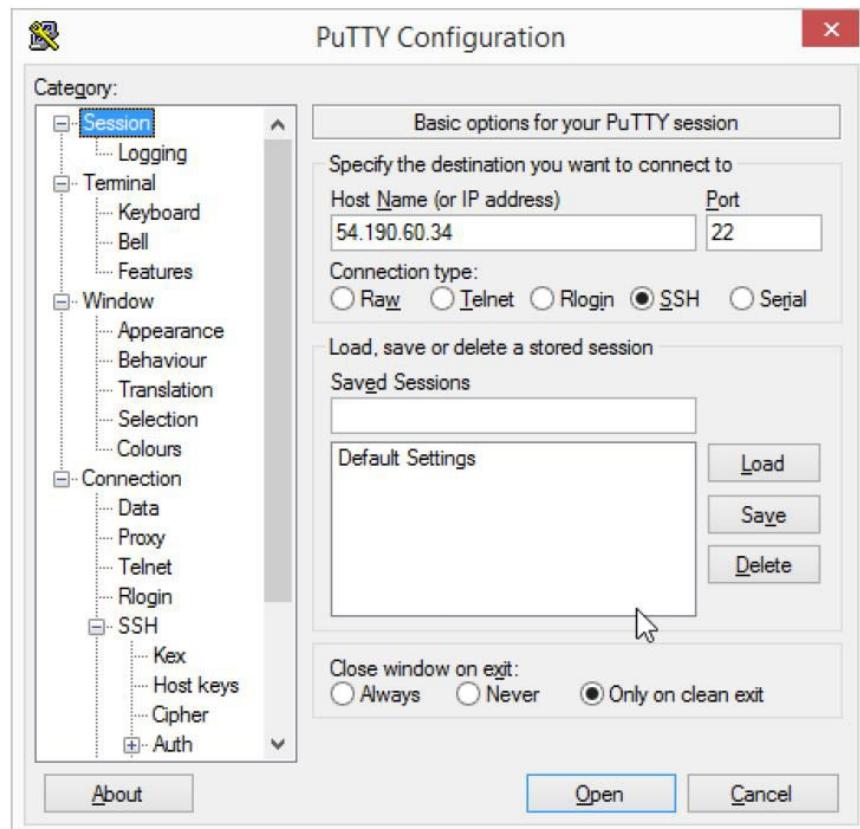
Click on Run



On **Category** page provide following values

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

Port → 22

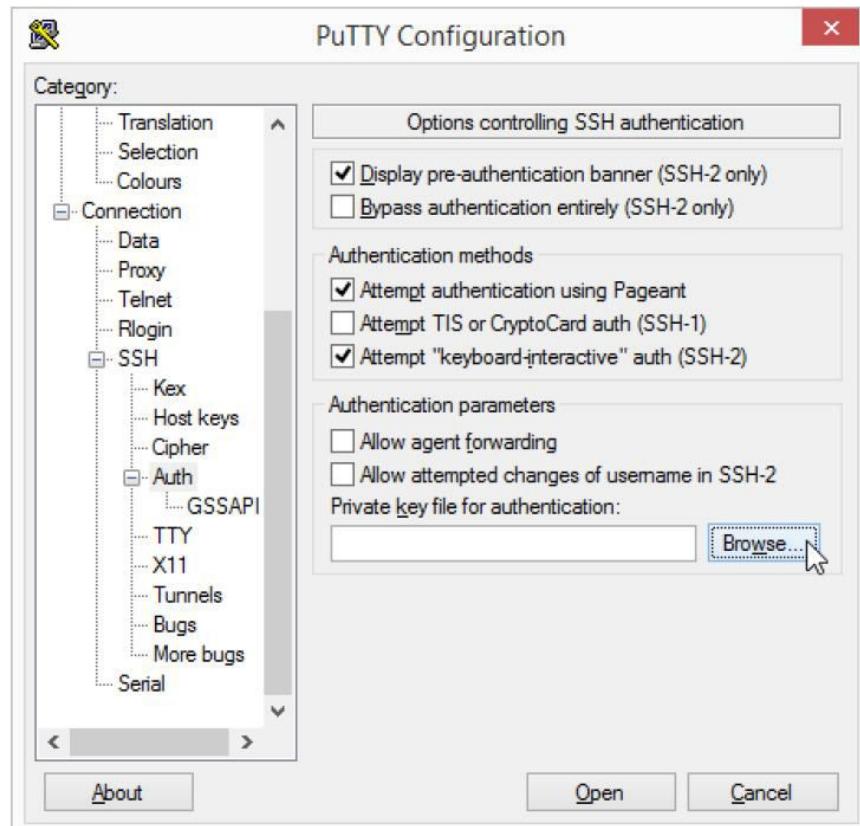


Under Connection expand

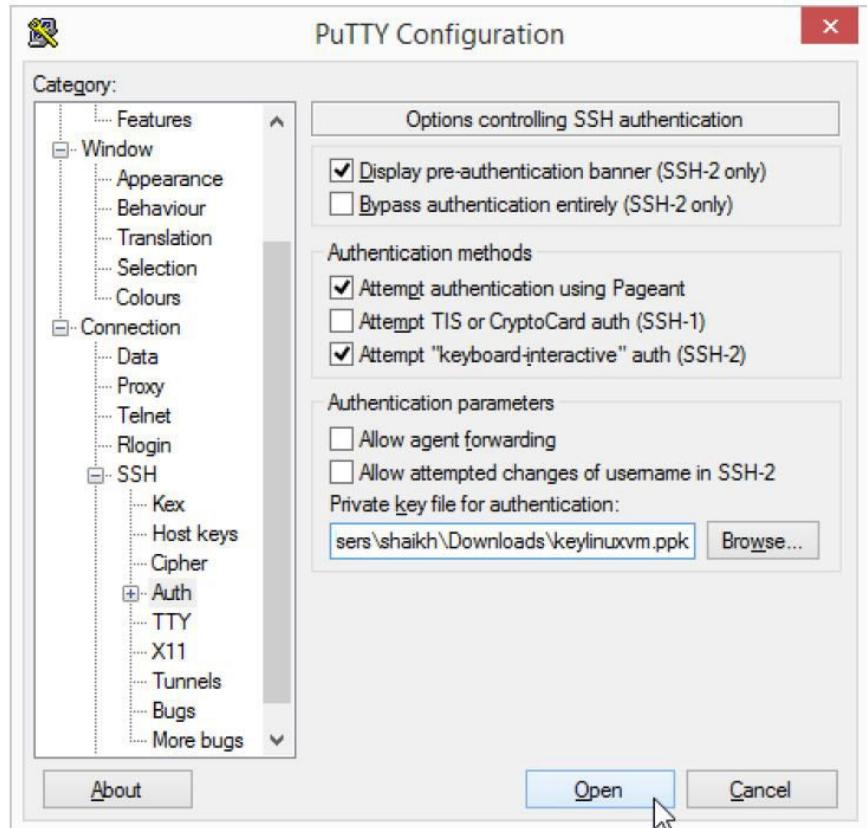
Click on SSH → Auth

Select Browse button

Provide the path of *.ppk file



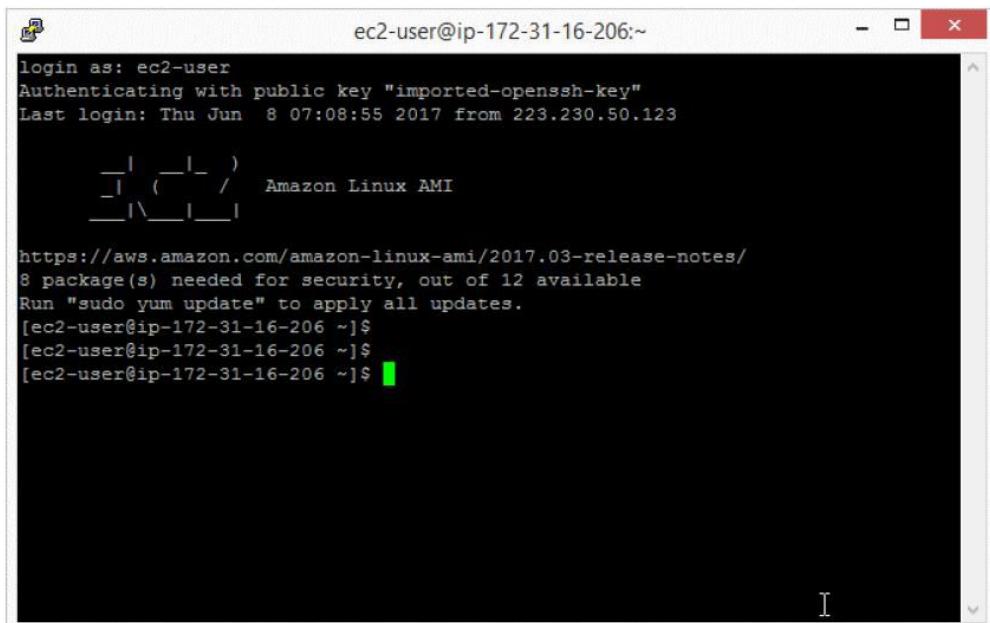
Click on Open button



Verify

Putty login screen is for linux

Provide user name **ec2-user**



A screenshot of a Putty terminal window titled "ec2-user@ip-172-31-16-206:~". The window shows a Linux login session. The text output is as follows:

```
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
[ec2-user@ip-172-31-16-206 ~]$
```

The terminal window has a standard Windows-style title bar and scroll bars.

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

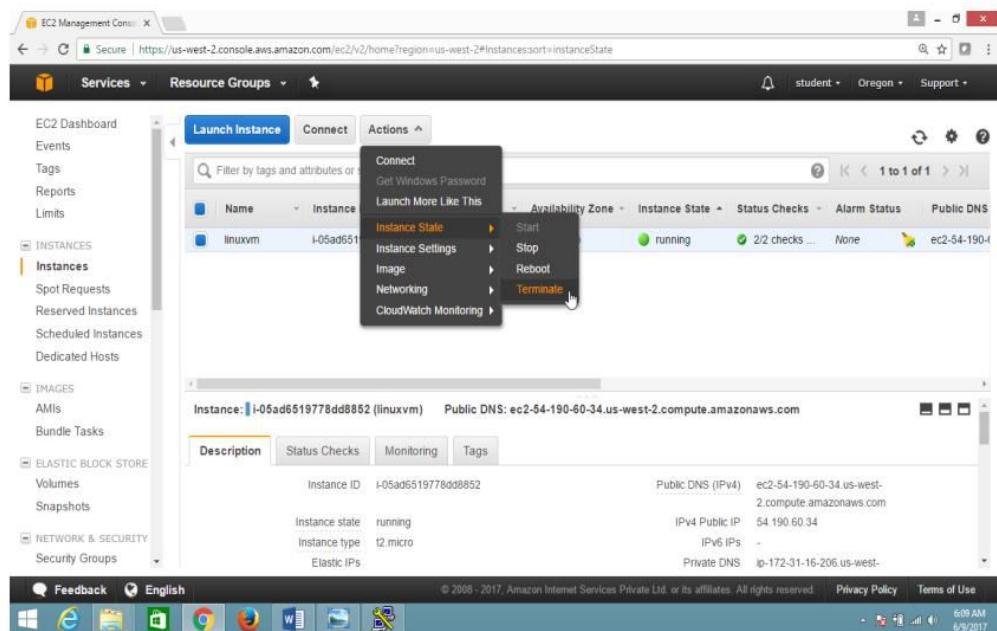
To start/stop/terminate instance

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,

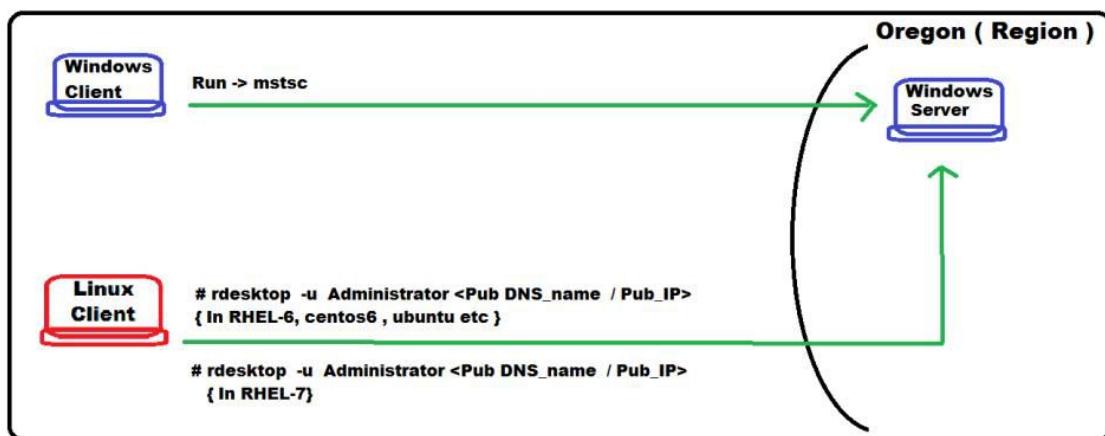
Otherwise it will be charged if the limit is over after free tier usage.

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 :

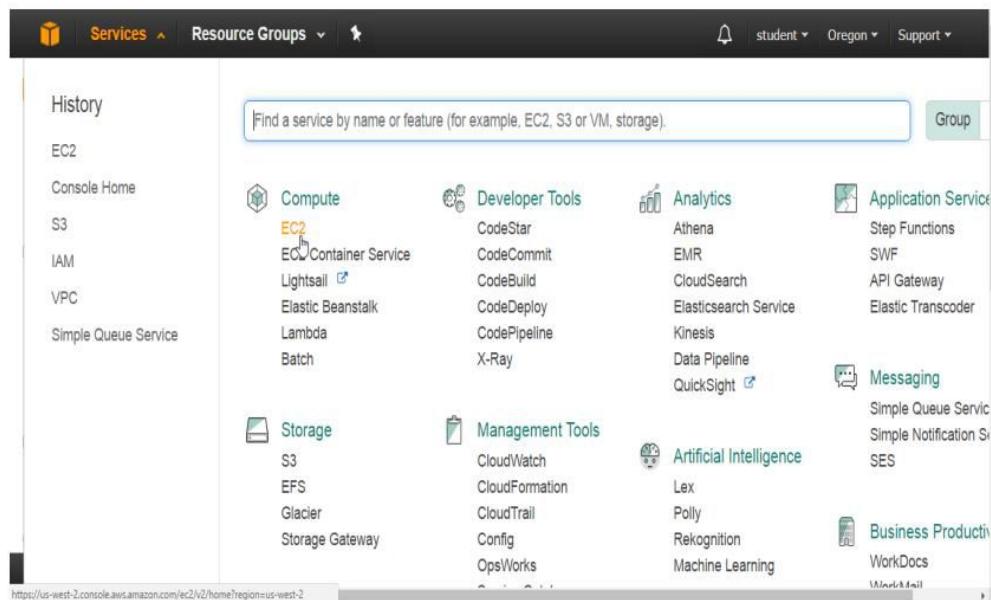
- To Launch Windows instance
- Select Region
- Select Amazon Machine Image (AMI)
- Create key pair
- Connect from Windows operating system
- Connect from Linux Operating system
- Start/stop/terminate instance

1. To Launch Windows instance in default VPC

Open the Amazon EC2 console

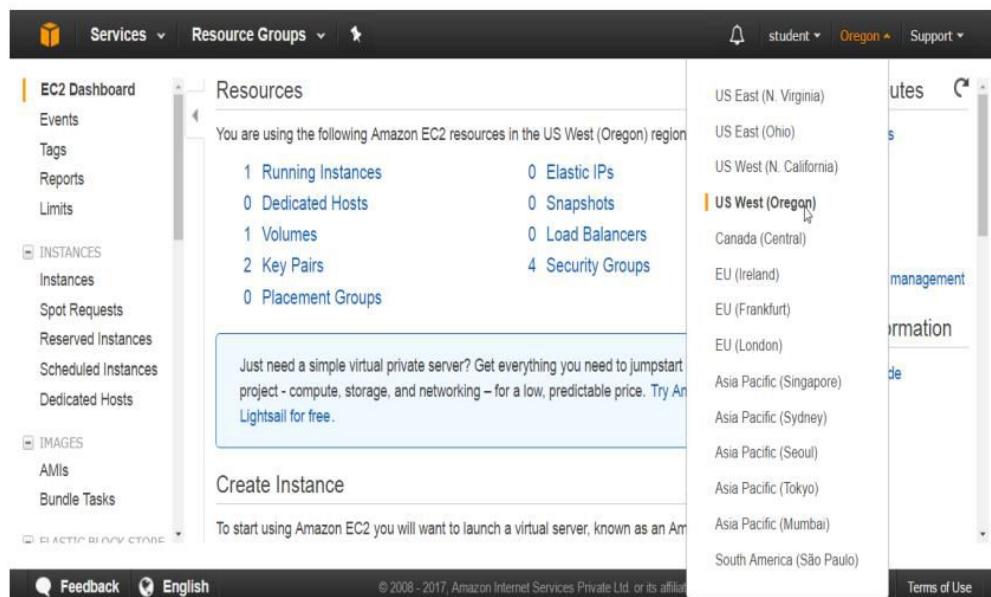
Select **Compute**

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 AWS EC2 Dashboard. On the left, there's a sidebar with links like EC2 Dashboard, Instances, and AMIs. The main area is titled "Service Health". It shows "Service Status: US West (Oregon)" with a green checkmark and the message "This service is operating normally". Below that is "Availability Zone Status" with three entries: "us-west-2a" (green checkmark, "Availability zone is operating normally"), "us-west-2b" (green checkmark, "Availability zone is operating normally"), and "us-west-2c" (green checkmark, "Availability zone is operating normally"). To the right, there's a section titled "Scheduled Events" with a message "No events". A sidebar on the right lists "EC2 Launch Wizard... Or try these popular AMIs:" with options like "Barracuda NextGen Firewall F-Series - PAYG" and "VM-Series Next-Generation Firewall Bundle 2". At the bottom, there are "Feedback" and "English" buttons, and a footer with copyright information and links to Privacy Policy and Terms of Use.

From the “EC2 Dashboard” panel

Select Instance

Click on “Launch Instance” button

This screenshot is similar to the previous one but focuses on the "Instances" section. The "Launch Instance" button is highlighted with a blue box. Below it, a table shows a single instance: "linuxvm" (Instance ID: i-05ad6519778dd8852, Instance Type: t2.micro, Availability Zone: us-west-2b, Status: running). The "Status Checks" tab is selected, showing 2/2 checks passed. At the bottom, detailed instance information is provided: Instance ID: i-05ad6519778dd8852, Public DNS: ec2-54-190-60-34.us-west-2.compute.amazonaws.com, Instance state: running, Instance type: t2.micro, Public DNS (IPv4): ec2-54-190-60-34.us-west-2.compute.amazonaws.com, IPv4 Public IP: 54.190.60.34, and IPv6 IPs: -. The footer includes "Feedback", "English", and links to "Privacy Policy" and "Terms of Use".

On “Choose an Amazon Machine Image (AMI)” page

Select “Quick start”

The screenshot shows the AWS Step 1: Choose an Amazon Machine Image (AMI) page. At the top, there is a navigation bar with 'Services', 'Resource Groups', and other account details. Below the navigation bar, a breadcrumb trail shows '1. Choose AMI' (highlighted in orange), '2. Choose Instance Type', '3. Configure Instance', '4. Add Storage', '5. Add Tags', '6. Configure Security Group', and '7. Review'. To the right of the breadcrumb trail is a 'Cancel and Exit' button. The main content area is titled 'Step 1: Choose an Amazon Machine Image (AMI)'. It contains a sub-instruction: 'An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.' Below this instruction is a search bar with the placeholder 'Quick Start'. At the bottom of the page, there is a pagination control showing '1 to 31 of 31 AMIs'.

Select “Microsoft Windows Server AMI” and click **select** button

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

Click on **Select** button

The screenshot shows the same AWS Step 1: Choose an Amazon Machine Image (AMI) page as the previous one, but now displaying a list of AMIs. The list includes:

- Microsoft Windows Server 2012 with SQL Server Standard - ami-dd91f4bd (Windows, 64-bit, Select button)
- Microsoft Windows Server 2008 R2 Base - ami-0381e463 (Windows, Free tier eligible, 64-bit, Select button)
- Microsoft Windows Server 2008 R2 with SQL Server Express and IIS - ami-3483e654 (Windows, 64-bit, Select button)

A cursor is shown hovering over the 'Select' button for the second item. At the bottom of the page, there are links for 'Feedback', 'English', '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', and '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. The top navigation bar includes 'Services', 'Resource Groups', and account information ('student', 'Oregon', 'Support'). Below the navigation is a progress bar with steps 1 through 7. Step 2, 'Choose an Instance Type', is currently selected. A table lists various instance types based on 'Family' (General purpose), 'Type', 'vCPUs', 'Memory (GiB)', 'Instance Storage (GB)', 'EBS-Optimized Available', 'Network Performance', and 'IPv6 Support'. The 't2.micro' row is highlighted with a green background and has a green label 'Free tier eligible' next to it. At the bottom of the table are buttons for 'Cancel', 'Previous', 'Review and Launch', and 'Next: Configure Instance Details' (which is being pointed to by a cursor).

On “Configure Instance Details”, page

Leave all values as default

Click on “Next : Add storage” button

The screenshot shows the AWS CloudFormation console. The top navigation bar includes 'Services', 'Resource Groups', and account information ('student', 'Oregon', 'Support'). Below the navigation is a progress bar with steps 1 through 7. Step 3, 'Configure Instance Details', is currently selected. The page contains fields for 'Number of Instances' (set to 1), 'Purchasing option' (checkbox for 'Request Spot instances'), network settings (Network: vpc-89c341ee | default-vpc-oregon (default), Subnet: No preference (default subnet in any Availability Zone), Auto-assign Public IP: Use subnet setting (Enable)), and domain join settings (Domain join directory: None). At the bottom of the page are buttons for 'Cancel', 'Previous', 'Review and Launch', and 'Next: Add Storage' (which is being pointed to by a cursor).

On “Add Storage”, page

Leave all values as default

Click on “Next: Tag Instance” button

The screenshot shows the 'Step 4: Add Storage' page of an AWS EC2 instance creation wizard. The top navigation bar includes 'Services', 'Resource Groups', and tabs for 'student', 'Oregon', and 'Support'. The current step is '4. Add Storage', which is highlighted in orange. Below the tabs, a progress bar shows steps 1 through 7. The main content area is titled 'Step 4: Add Storage' and contains instructions about launching with storage device settings. A table lists a single volume configuration:

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-05c5aa21237b4e6c8	30	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Below the table is a button labeled 'Add New Volume'. A note at the bottom 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.' At the bottom right are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is blue), and 'Next: Add Tags' (which has a mouse cursor hovering over it).

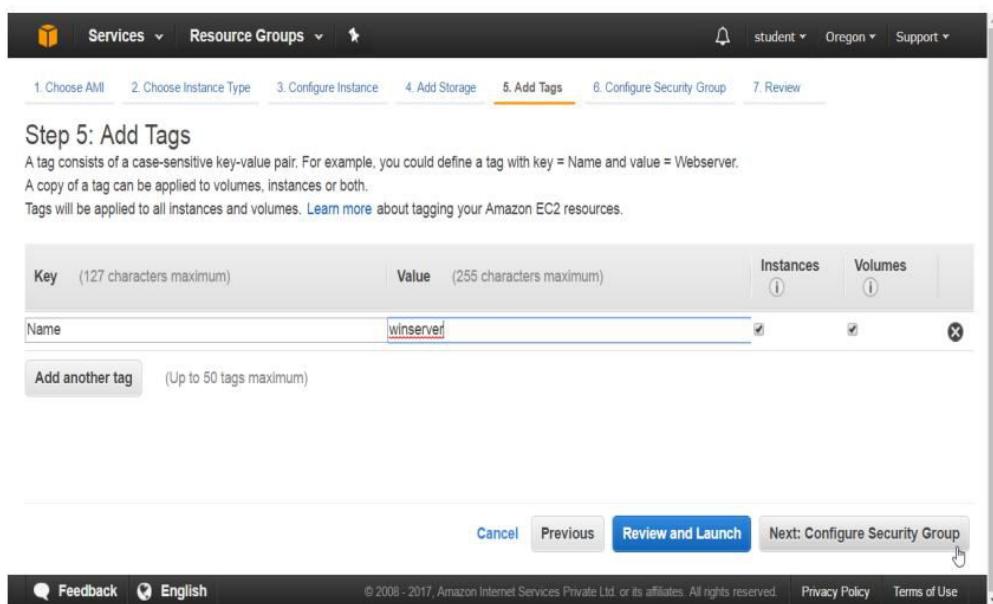
On “Add Tags”, page

Provide following values

Key → Name

Value → winserver

Click on “Next: Configure Security Group” button



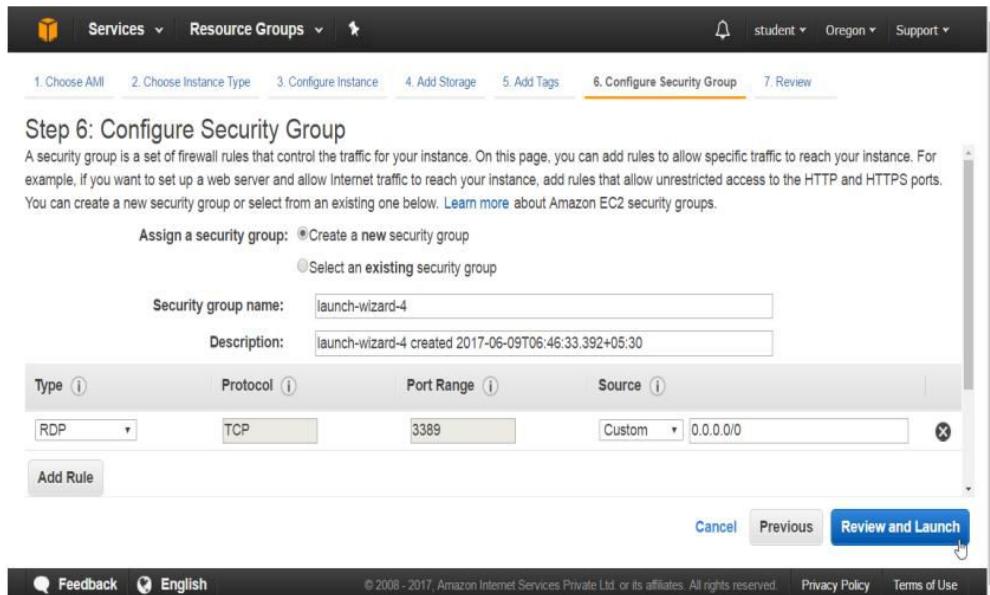
On “Configure Security Group” page

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



On “Review Instance Launch”, page

Leave all values as default.

Verify the summary, then drag down

The screenshot shows the "Step 7: Review Instance Launch" page. At the top, a yellow warning box states: "Improve your instances' security. Your security group, launch-wizard-4, 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](#)". Below this, the "AMI Details" section shows a Microsoft Windows Server 2008 R2 Base AMI. The "Launch" button is highlighted in blue. At the bottom, there are links for Feedback, English, Privacy Policy, and Terms of Use.

Verify the summary

Click on **Launch** button

The screenshot shows the "Step 7: Review Instance Launch" page. The "Launch" button is being clicked by a mouse cursor. The "Security Groups" section shows a single rule: Type RDP, Protocol TCP, Port Range 3389, Source 0.0.0.0/0. Below the security group section, there are sections for "Instance Details", "Storage", and "Tags", each with an "Edit" link. At the bottom, there are links for Feedback, English, Privacy Policy, and Terms of Use.

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

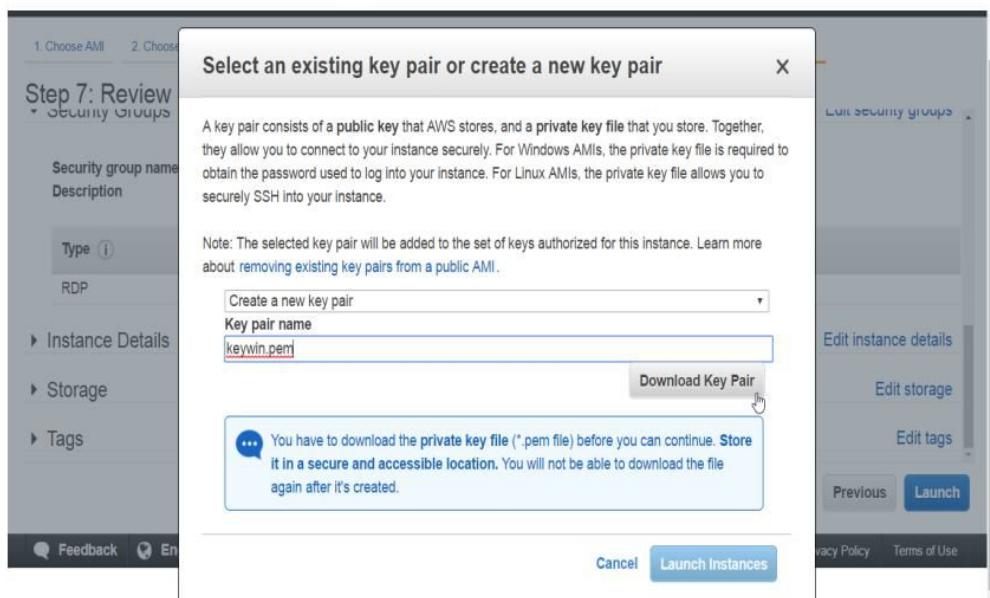
Select “Create a new key pair”

Enter **Key pair name** → keywin.pem

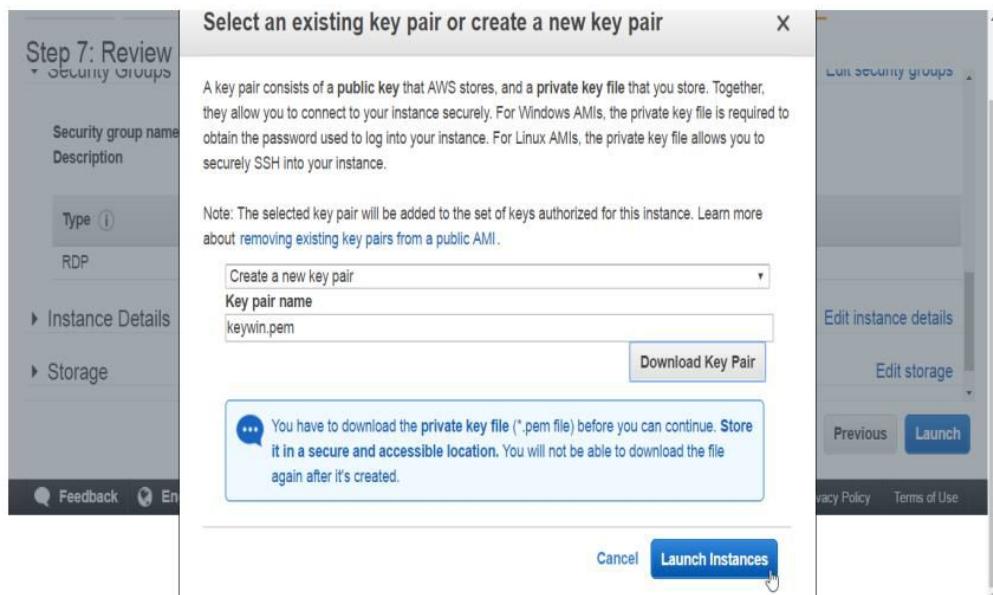
Click on “Download Key Pair”

Note: Store it in a secure and accessible location.

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

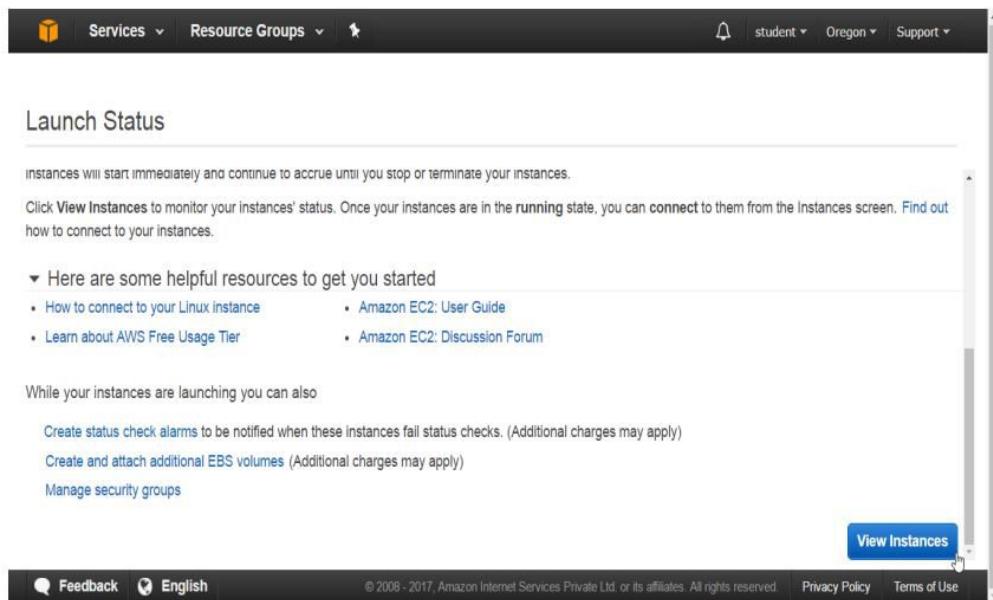


Click on “Launch an instance”



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 Dashboard. On the left, there's a sidebar with links for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (which is selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, IMAGES, AMIs, and Bundle Tasks. At the top, there are buttons for Launch Instance, Connect, and Actions. Below that is a search bar and a table header with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Two instances are listed: 'winserver' (Instance ID: i-0a6e73ff953579363) is in the 'pending' state, indicated by a yellow circle icon with a question mark; 'linuxvm' (Instance ID: i-05ad6519778dd8852) is in the 'running' state, indicated by a green circle icon with a checkmark. The bottom of the screen shows standard AWS footer links for Feedback, English, Privacy Policy, and Terms of Use.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
winserver	i-0a6e73ff953579363	t2.micro	us-west-2b	pending	Initializing	None
linuxvm	i-05ad6519778dd8852	t2.micro	us-west-2b	running	2/2 checks ...	None

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 area displays a table of instances. Two instances are listed: 'linuxvm' and 'winserver'. Both instances are in the 'running' state, indicated by green dots. A red circle highlights the 'running' status for the 'winserver' instance. Below the table, there is a summary for the selected instance ('winserver') with fields for Instance ID, Public DNS, Instance state, and IP address.

To check instance details like

Description, Status check, Monitoring, Tags

This screenshot is similar to the previous one, showing the AWS EC2 Instances page. The 'Status Checks' tab is highlighted with a red circle. This tab provides detailed monitoring information for the selected instance ('winserver'). It includes sections for 'Description', 'Status Checks', 'Monitoring', and 'Tags'. The 'Status Checks' section shows two green dots, indicating successful checks. The 'Monitoring' section shows a single green dot. The 'Tags' section is currently empty.

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

Open Ec2 Dashboard Console

Go to instance

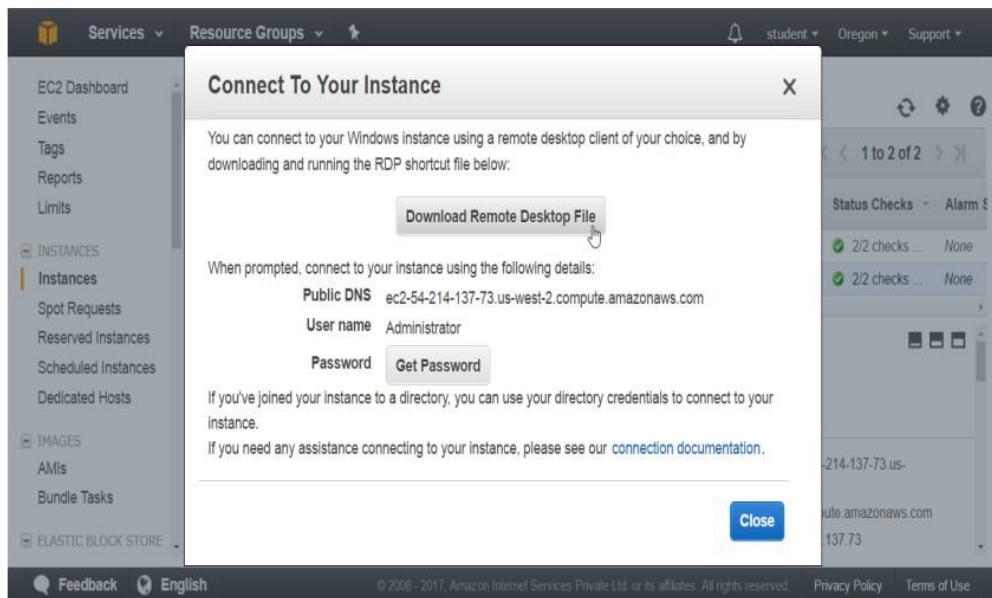
Select the instance you want to connect

Click **Connect** button

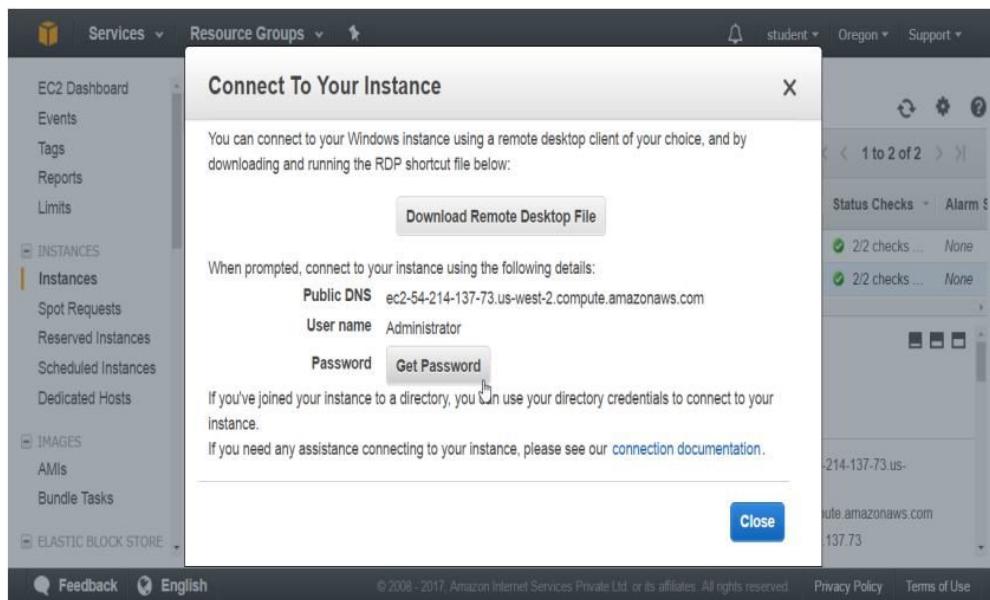
The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images (AMIs, Bundle Tasks), and Elastic Block Store. The main area has tabs for Launch Instance, Connect (which is highlighted with a mouse cursor), 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: "linuxvm" (t2.micro, us-west-2b, running, 2/2 checks, None) and "winserver" (t2.micro, us-west-2b, running, 2/2 checks, None). Below the table, it says "Instance: i-0a6e73ff953579363 (winserver)" and "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 the Description tab, it shows Instance ID: i-0a6e73ff953579363, Public DNS (IPv4): ec2-54-214-137-73.us-west-2.compute.amazonaws.com, Instance state: running, and IPv4 Public IP: 54.214.137.73.

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

Click on “Download Remote Desktop file” button



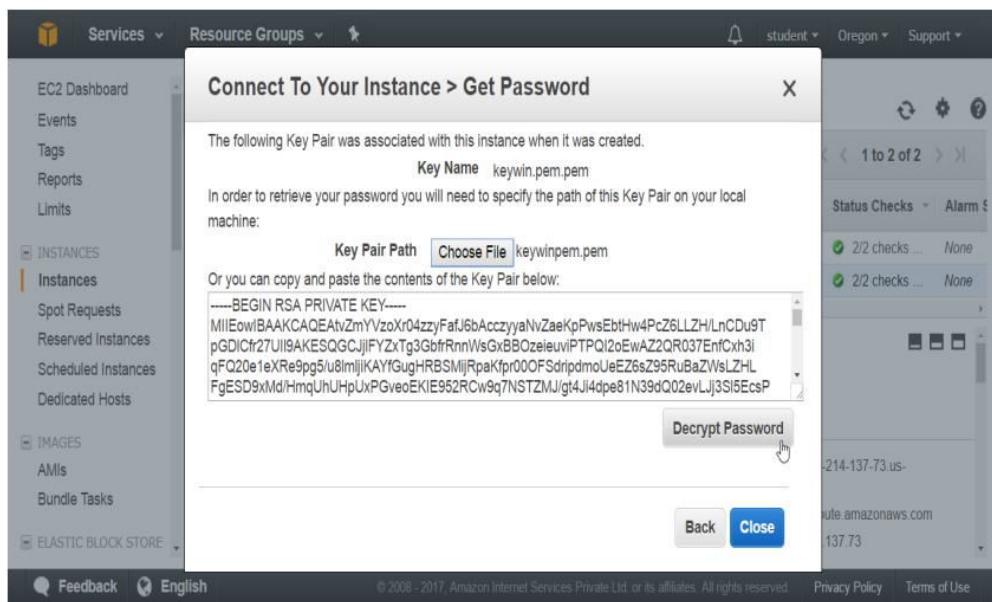
Click on “Get Password” button



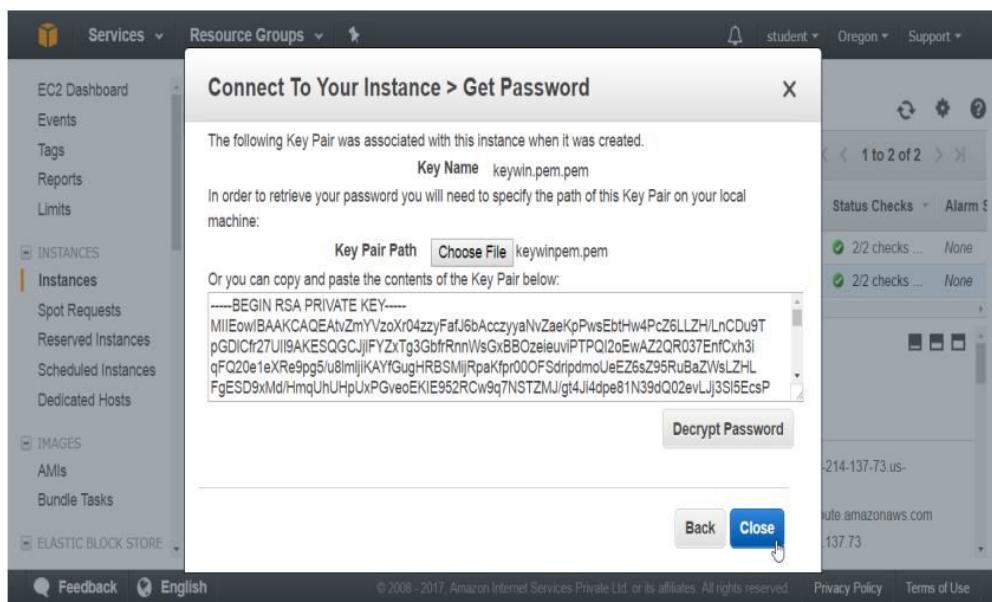
Click on “Choose file” button

Provide the path of key file

Click on “Decrypt Password” button



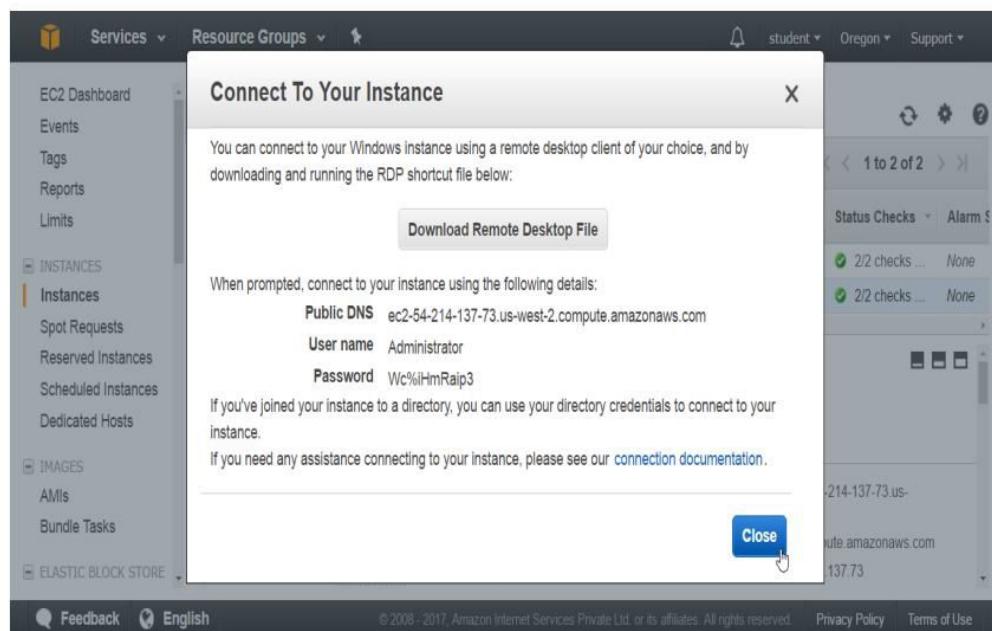
Click on Close button



Copy your instance Detail in Notepad

Public DNS ec2-54-213-234-57.us-west-2.compute.amazonaws.com
User name Administrator
Password *****

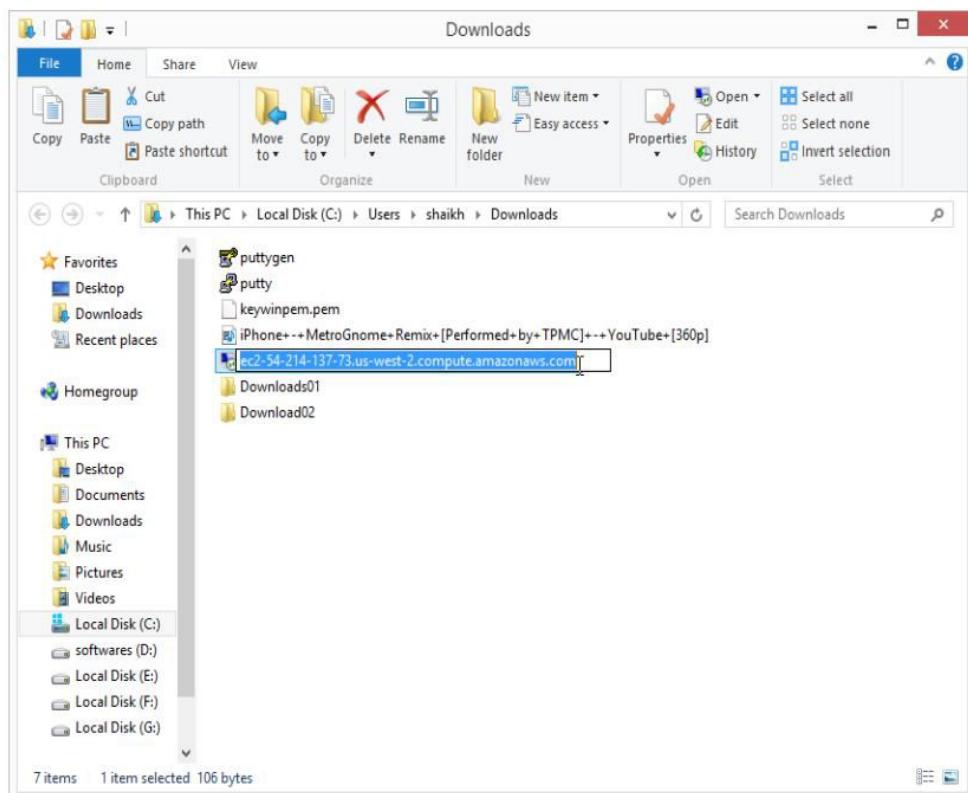
Click on **Close** button.



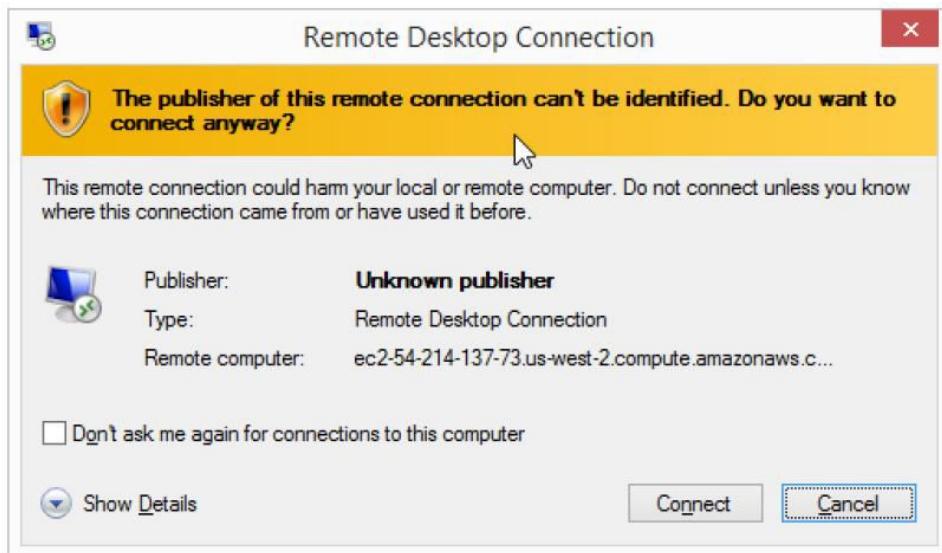
3) Now you can login to Amazon Windows instance

Double click on downloaded RDP file

Provide username as Administrator and give Password.



Click on connect

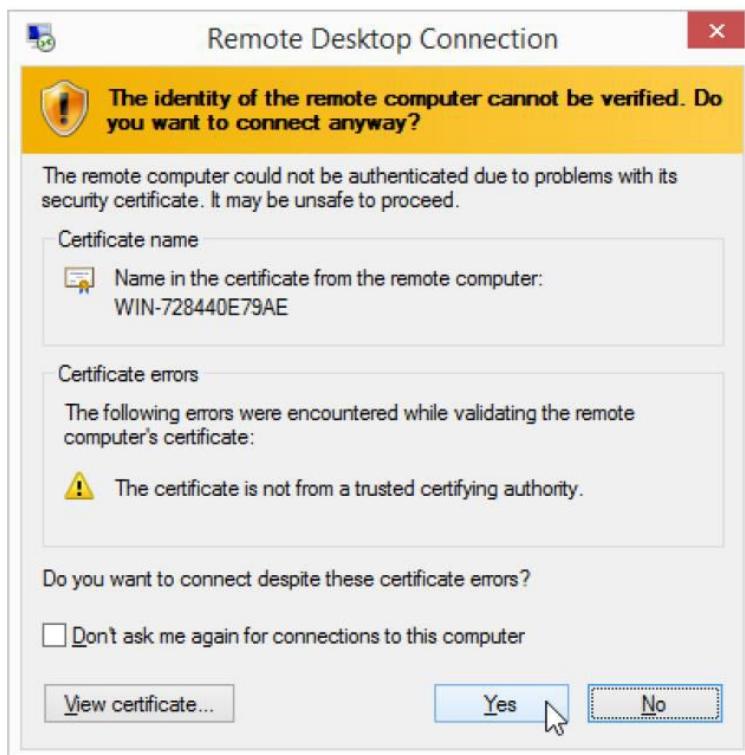


Provide username Administrator and Password

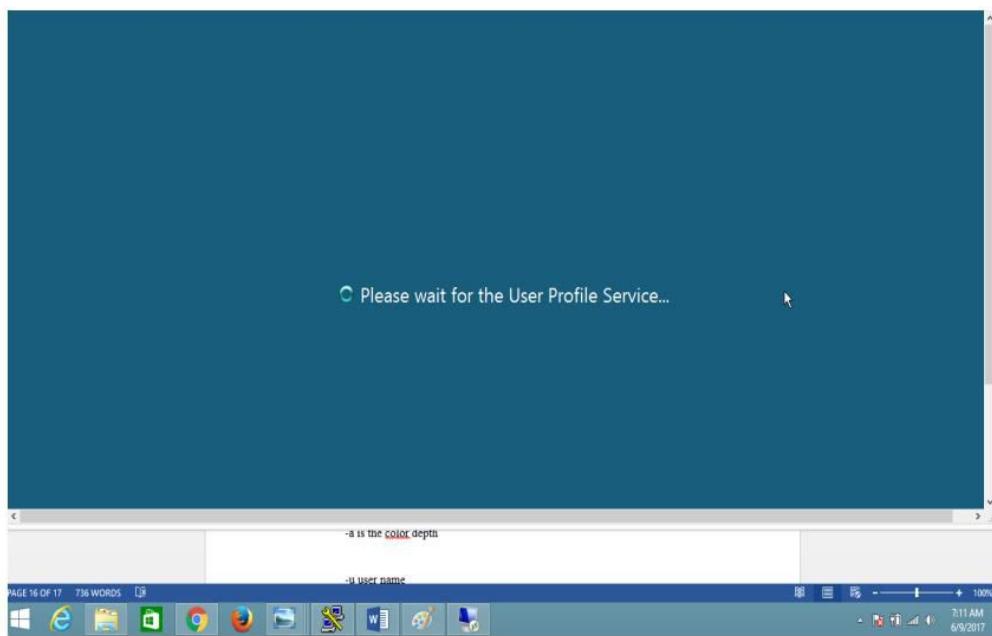
Click on OK



Click on Yes button



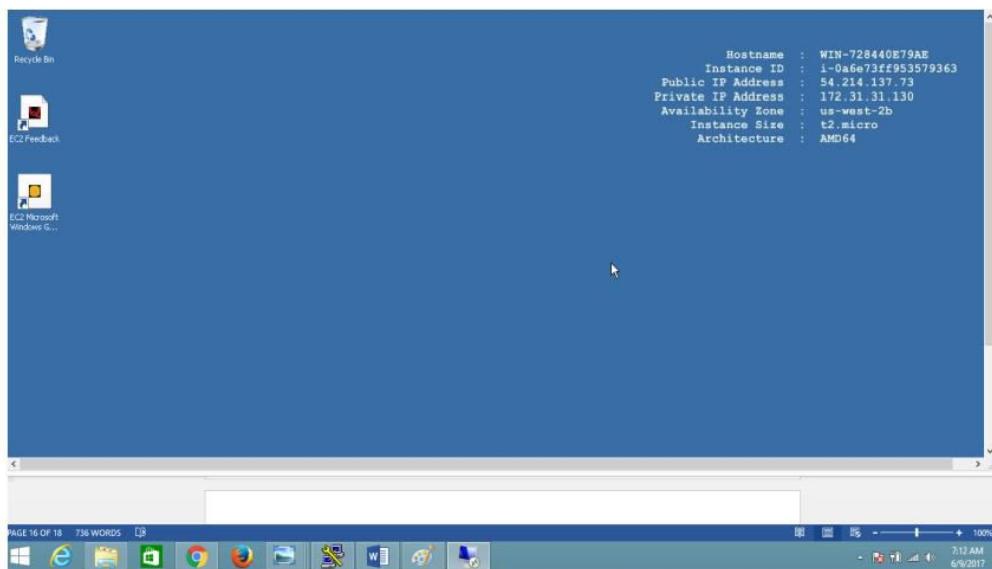
Wait for a movement



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

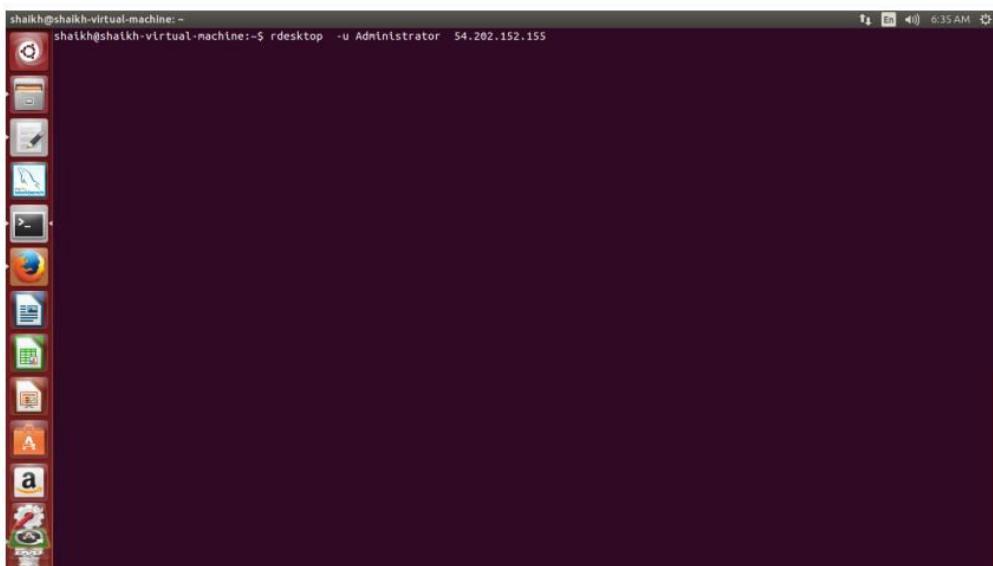
Note: rdesktop or xfreerdp { RHEL-6,7 } package should be installed

\$ rdesktop -u Administrator <Pub_DNS_name / Public_IP>

or

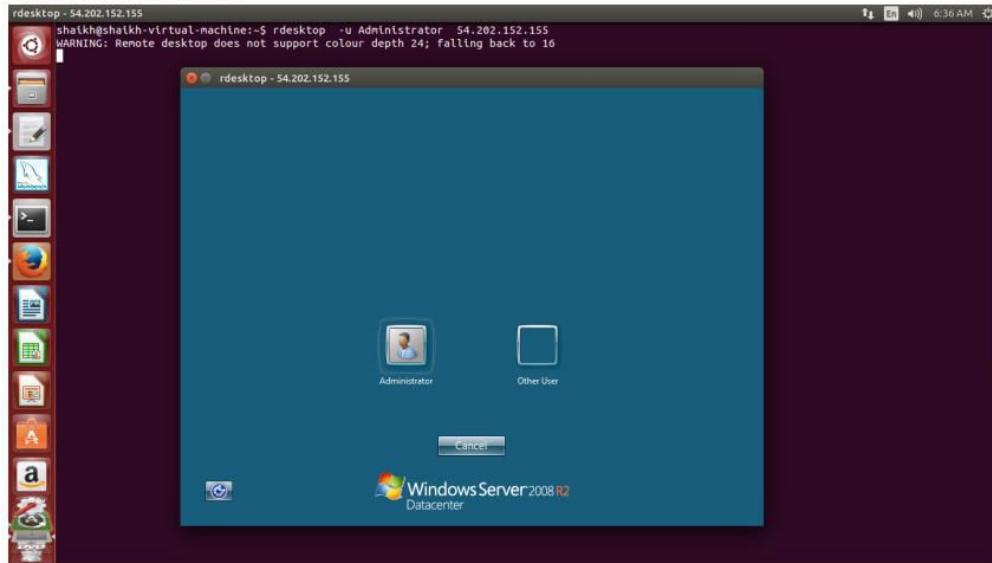
\$ xfreerdp -u Administrator <Pub_DNS_name / Public_IP> { in RHEL 6,7 }

-u → user name



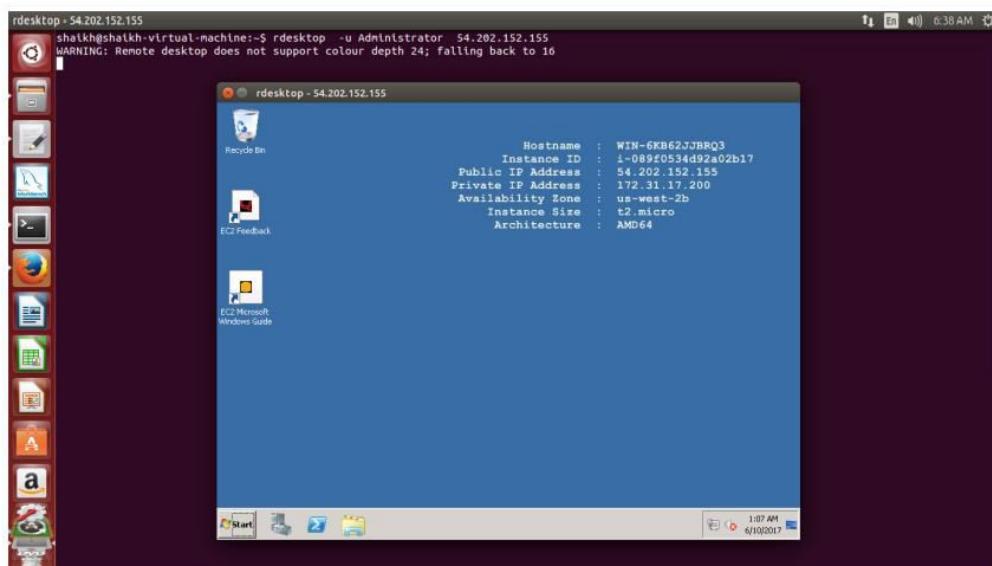
Click on Administrator

Provide the password



Verify:

Once Logged in Windows Desktop is available



Note:

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

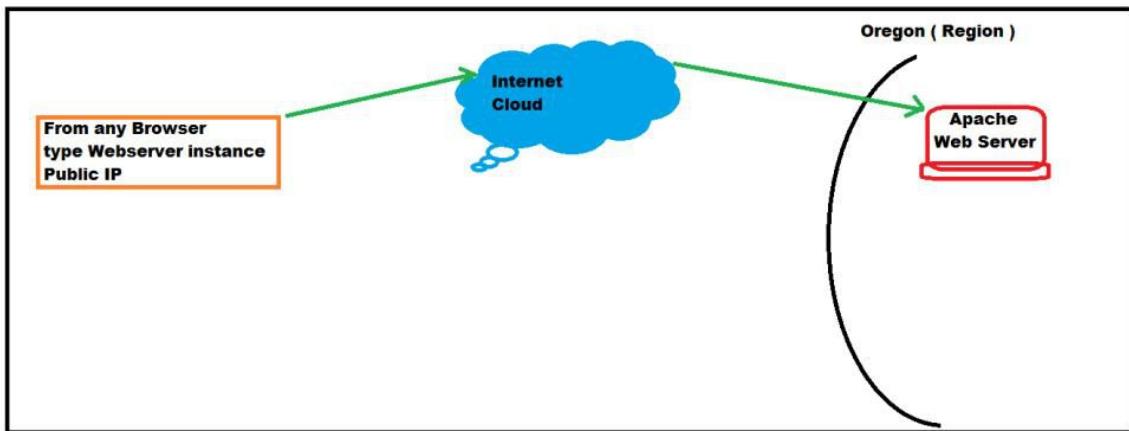
Otherwise it will be charged if the limit is over after free tier usage.

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

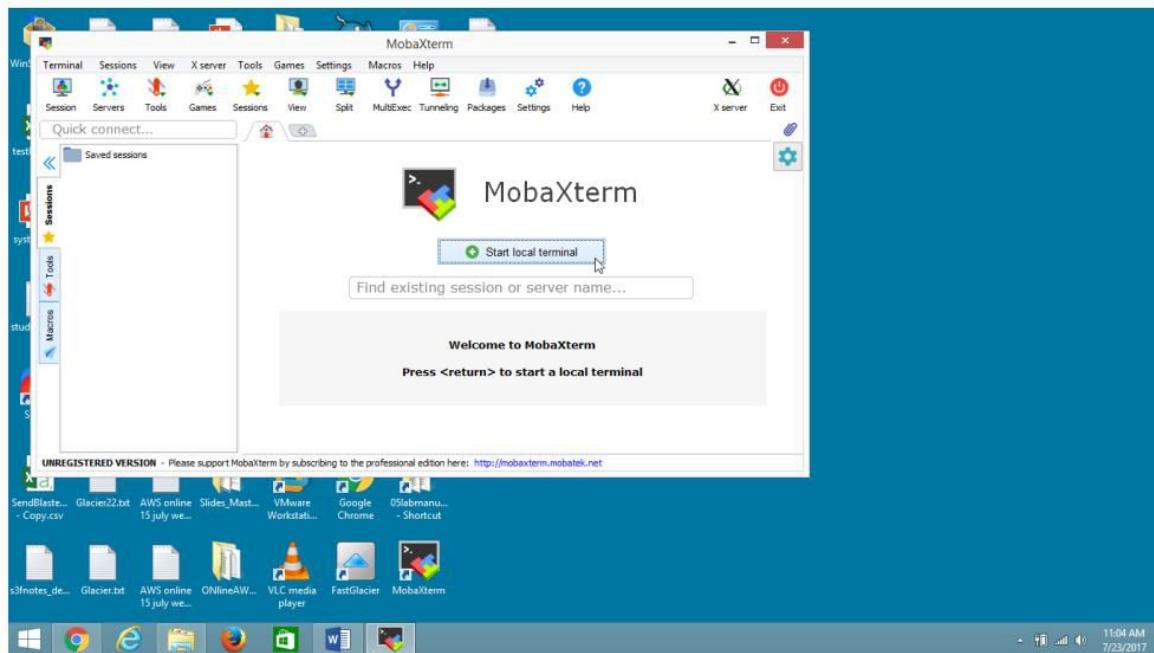
1) Launch Amazon linux instance and login to your instance

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

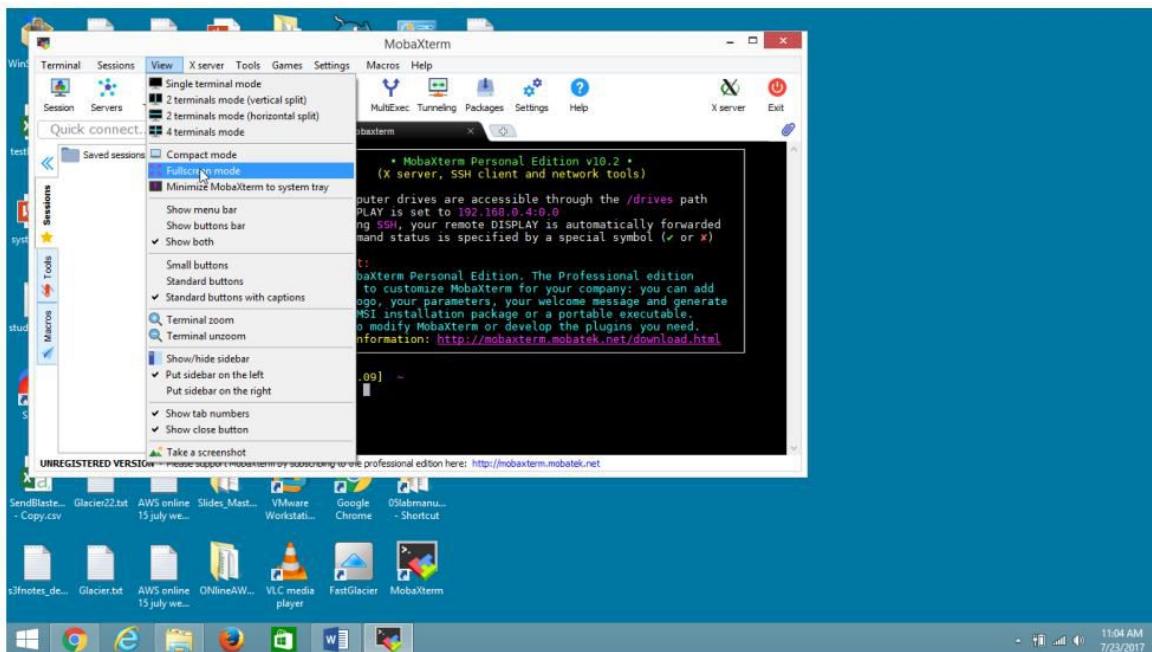
2) Connect to linux instance from windows using MobaXterm

Open **MobaXterm**

Click on **Start local terminal**

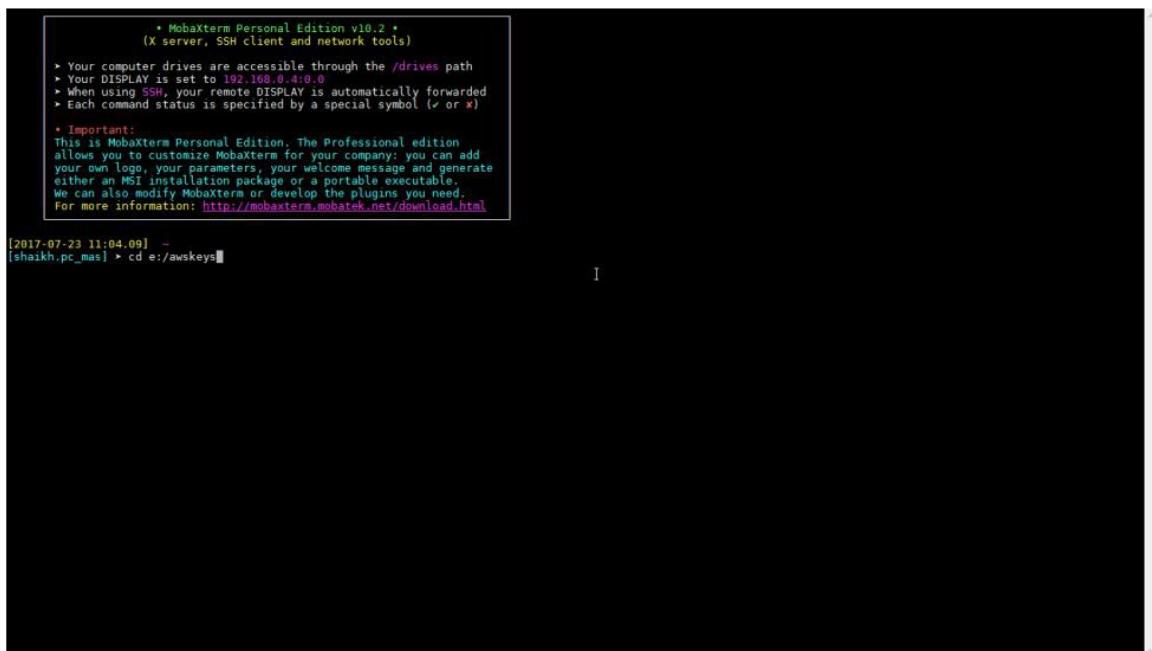


Go to Full Screen mode



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

Eg : cd e:/awskeys



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 list 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 interface. On the left, there's a navigation sidebar with options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block Store. The main area shows a table of instances. One instance is selected, showing its details in a modal window. The instance is named "Linuxwebserver...", has an Instance ID of i-09e8a71e3ce9a9561, is a t2.micro type, and is running in the us-west-2c availability zone. Its Public DNS is ec2-54-186-140.us-west-2.compute.amazonaws.com. The modal also displays the instance's state (running), type (t2.micro), and various IP addresses (IPv4 Public IP: 54.186.150.140, IPv6 IPs: -, Private DNS: in-172-31-10-246.us-west-2.compute.amazonaws.com).

Go to the right end

Select Security Groups

Click on launch-wizard-1

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, and Elastic Block Store. The main area displays an instance named 'i-09e8a71e3ce9a9561 (Linuxwebserver)'. The instance is running and has a Public DNS of 'ec2-54-186-150-140.us-west-2.compute.amazonaws.com'. Below the instance details, there are tabs for Description, Status Checks, Monitoring, and Tags. A specific link 'launch-wizard-1' is highlighted in the Security Groups section of the instance details. 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#instances:sort=tag:Name'.

Click on Inbound button

The screenshot shows the AWS EC2 Management Console interface. The left sidebar includes EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, and Elastic Block Store. The main area is titled 'Create Security Group' and shows a table with columns for Name, Group ID, Group Name, VPC ID, and Description. One row is selected with the values: Name 'sg-6abb0510', Group ID 'sg-6abb0510', Group Name 'launch-wizard-1', VPC ID 'vpc-89c341ee', and Description 'launch-wizard-1 created 2017-07-23T09:27:59.347+05:30'. Below the table, there are tabs for Description, Inbound (which is highlighted), Outbound, and Tags. 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#SecurityGroups:search=sg-6abb0510:sort=groupId'.

Click on **Edit** button

The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, and Elastic Block Store. The main area shows a table for a security group named 'sg-6abb0510'. The 'Inbound' tab is selected. An 'Edit' button is highlighted with a mouse cursor. Below it, the rule details are shown: Type: SSH, Protocol: TCP, Port Range: 22, Source: 0.0.0.0/0. At the bottom right of the dialog, there are 'Cancel' and 'Save' buttons.

Click on **Add Rule** button

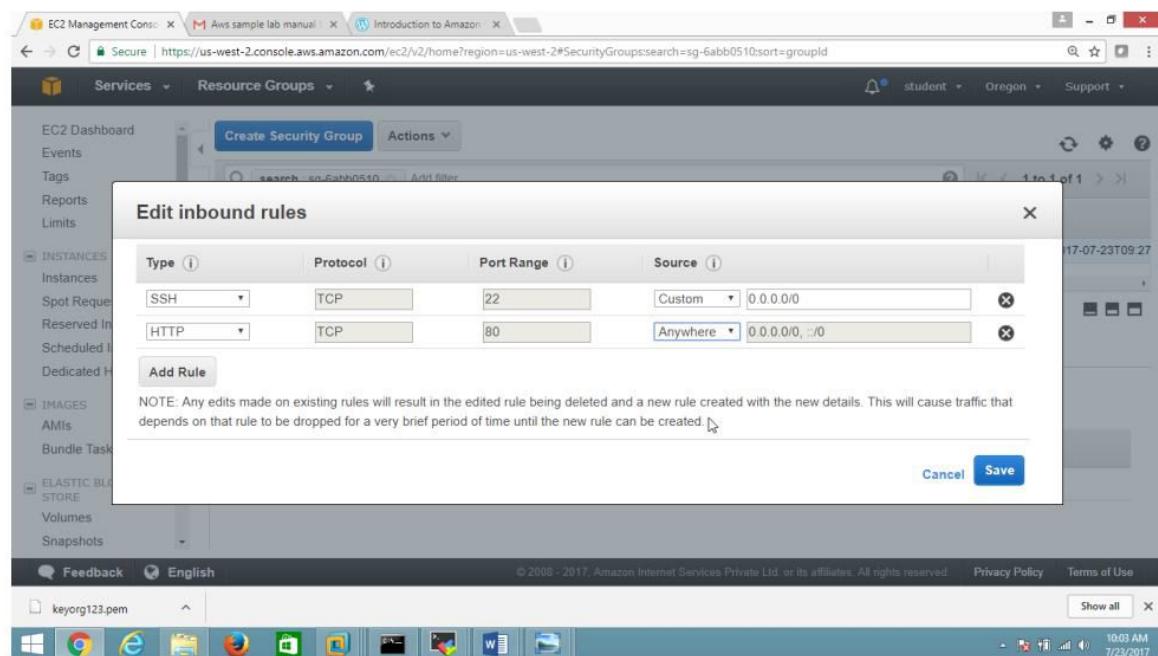
This screenshot shows the 'Edit inbound rules' dialog box overlaid on the EC2 Management Console. The dialog has fields for Type (SSH), Protocol (TCP), Port Range (22), and Source (Custom 0.0.0.0). A prominent 'Add Rule' button is highlighted with a mouse cursor. A note at the bottom of the dialog states: '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 same EC2 interface as the previous screenshot.

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 interface. On the left, there's a navigation sidebar with options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (which is selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, and Bundle Tasks. Below that is another sidebar for Elastic Block Store with Volumes and Snapshots. The main content area shows a table of instances. One instance is selected, showing its details: Name (Linuxwebser...), Instance ID (i-09e8a71e3ce9a9561), Instance Type (t2.micro), Availability Zone (us-west-2c), Instance State (running), Status Checks (2/2 checks ...), Alarm Status (None), and Public DNS (ec2-54-186-150-140.us-west-2.compute.amazonaws.com). At the bottom of the instance details, the IPv4 Public IP is highlighted as 54.186.150.140.

Verify

Website is running

The screenshot shows a web browser window with the address bar containing "54.186.150.140". The main content area displays the Apache welcome message: "Welcome to Apache Webserver in AWS instance". The browser's taskbar at the bottom shows various pinned icons, and the system tray indicates the date and time as 7/23/2017 10:19 AM.

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. The left sidebar has a tree view with "Schemas", "NETWORK & SECURITY" expanded, and "Elastic IPs" selected. The main content area shows a table with one row of data:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
Linuxwebser...	i-09e8a71e3ce9a9561	t2.micro	us-west-2c	running	2/2 checks

Below the table, it says "Instance: i-09e8a71e3ce9a9561 (Linuxwebserver) Public DNS: ec2-54-186-150-140.us-west-2.compute.amazonaws.com". At the bottom, there are tabs for "Description", "Status Checks", "Monitoring", and "Tags".

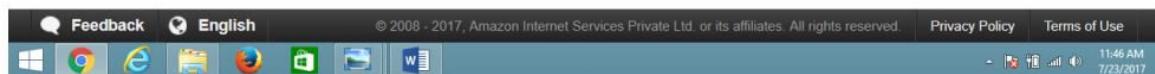
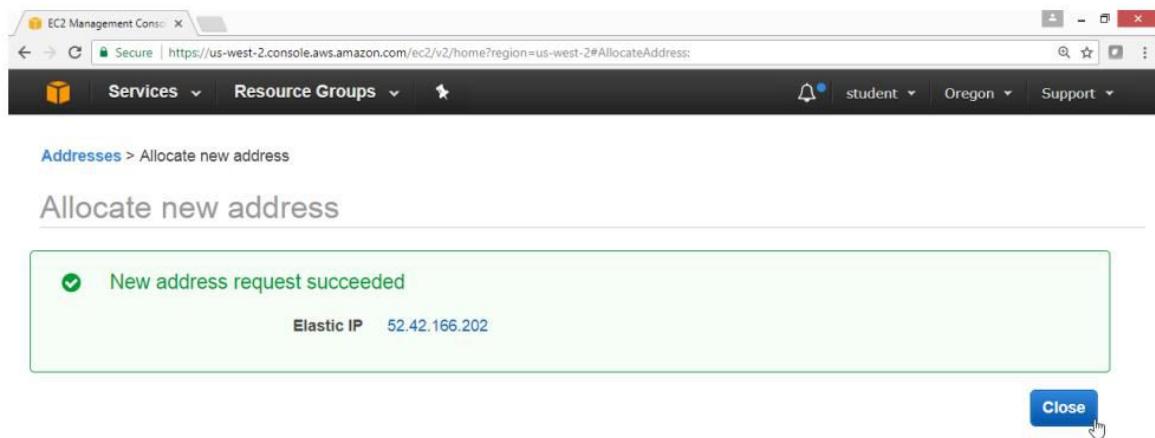
Click on **Allocate new address** button

The screenshot shows the AWS EC2 Management Console. The left sidebar has 'Elastic IPs' selected. The main area displays a message: 'You do not have any Addresses in this region' and 'Click the Create Address button to create your first Address'. A large blue button labeled 'Allocate new address' is centered, with a mouse cursor pointing at it. The top navigation bar includes 'student', 'Oregon', and 'Support'.

Click **Allocate** button

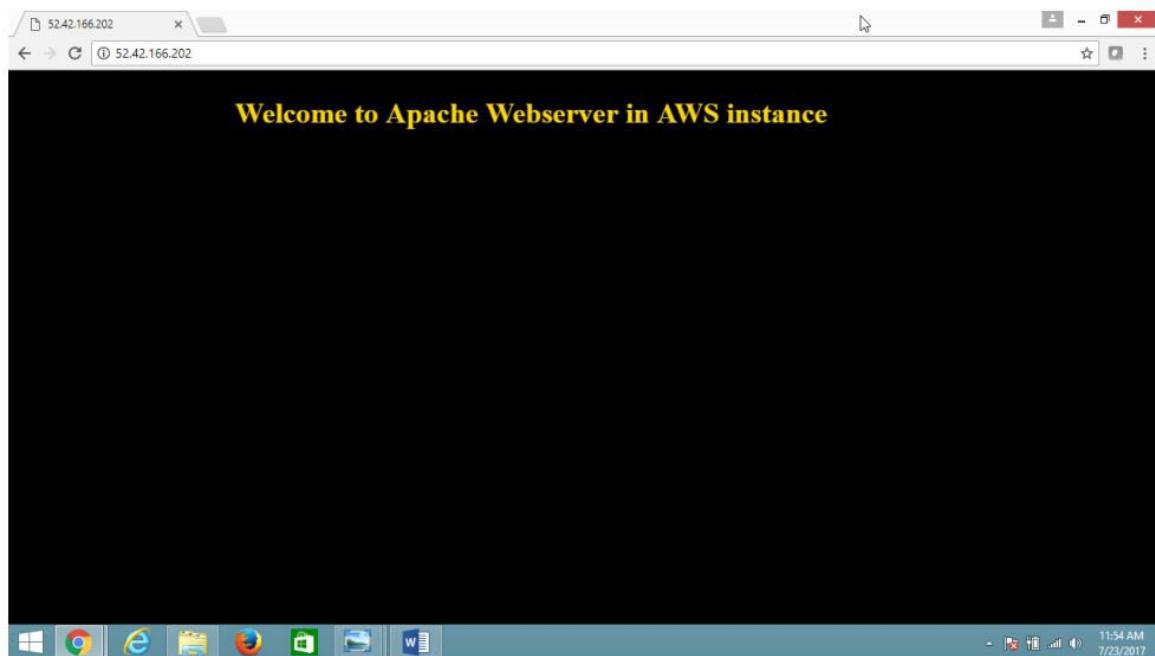
The screenshot shows the 'Allocate new address' dialog box. It has a heading 'Allocate new address' and a sub-instruction 'Allocate a new Elastic IP address by selecting the scope in which it will be used'. At the bottom right are 'Cancel' and 'Allocate' buttons, with the 'Allocate' button highlighted by a mouse cursor. The top navigation bar includes 'student', 'Oregon', and 'Support'.

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

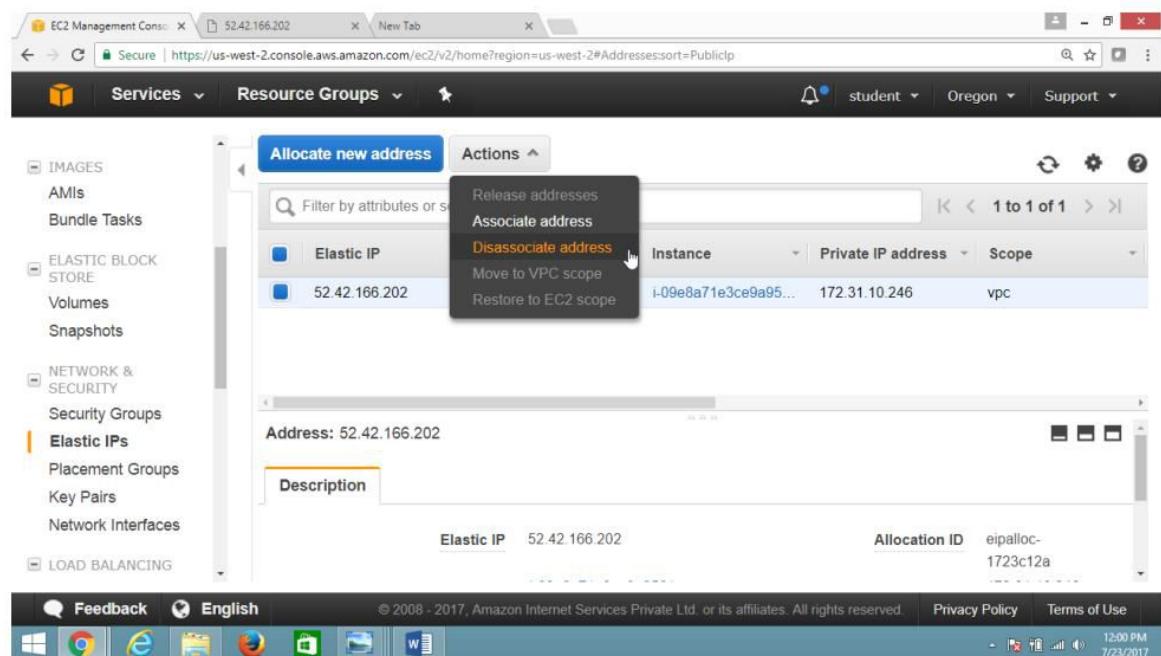
Open the console **EC2 Dashboard**

Expand “Network Security”

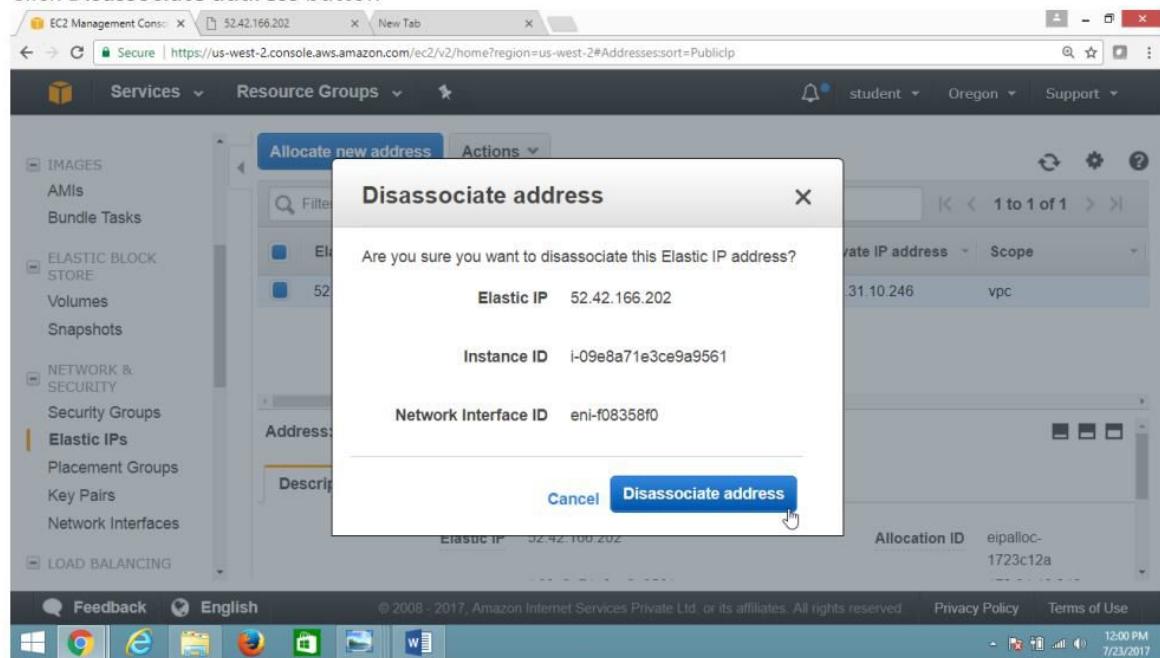
Select **Elastic IP**

Click **Action** button

Select **Disassociate Address**

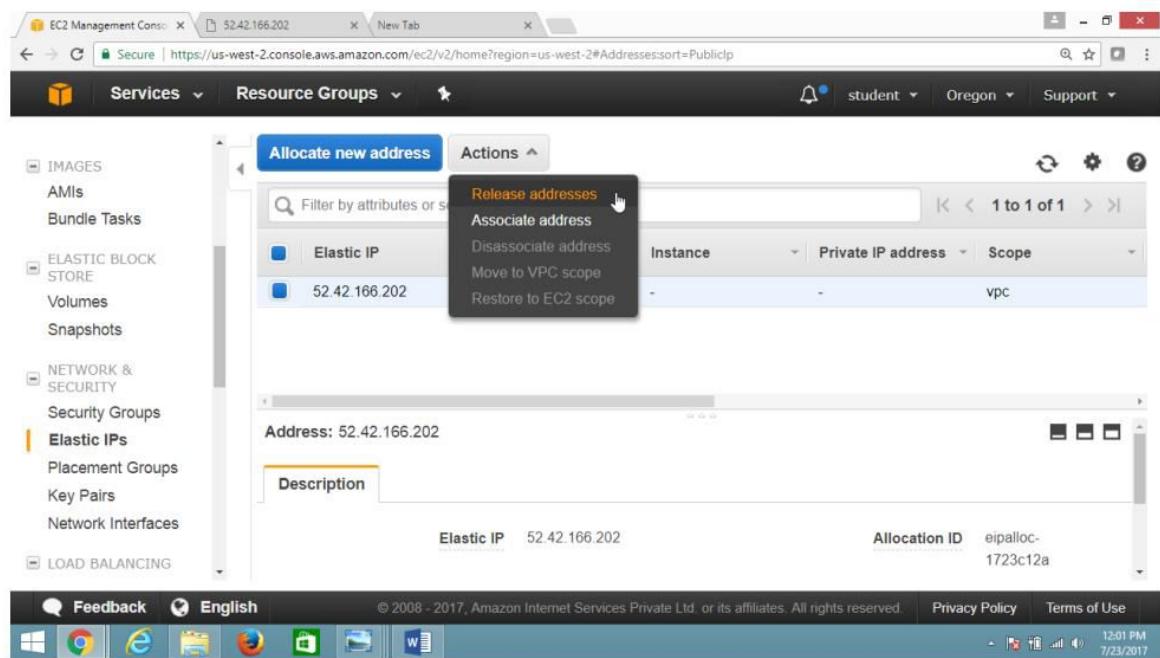


Click Disassociate address button

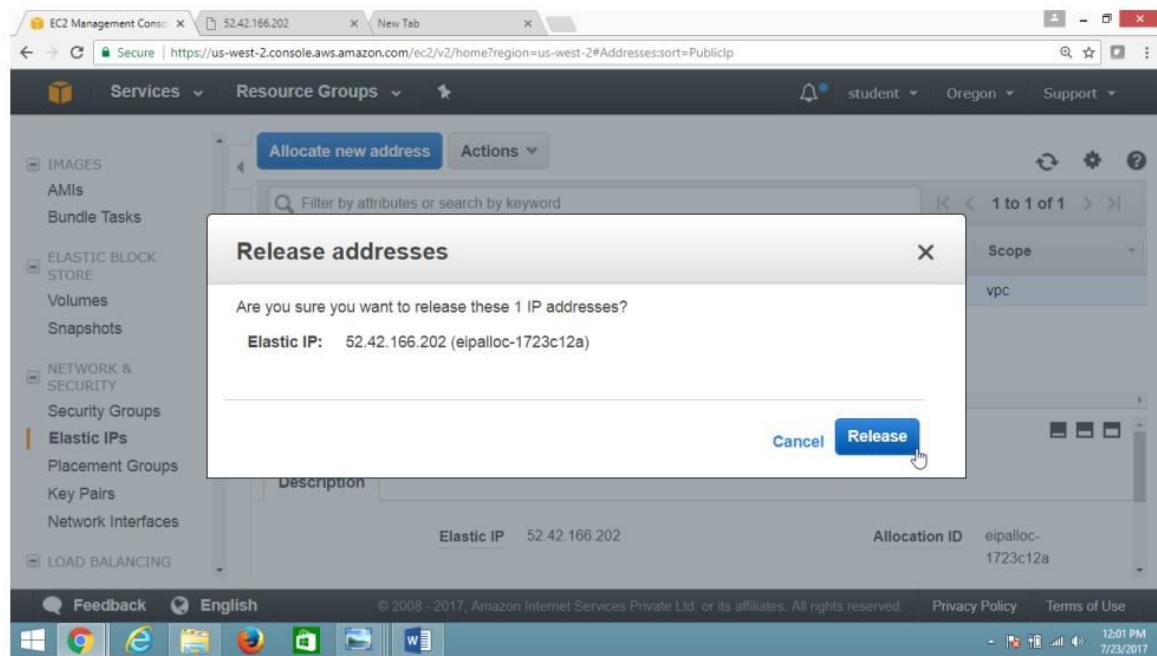


Click Action button

Select Release Addresses



Click Release button

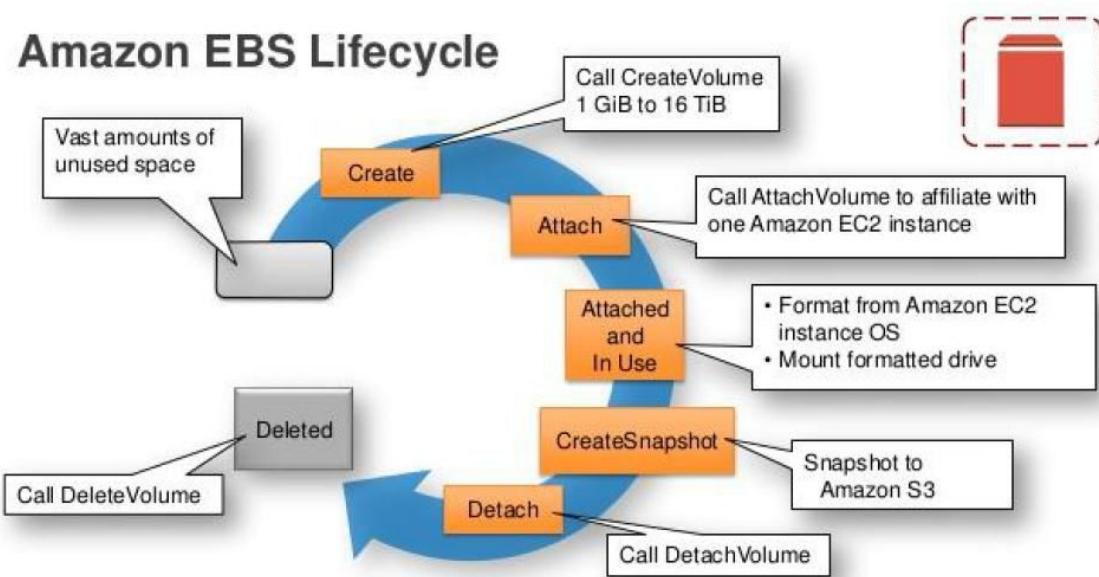


Lab 5: To Manage Elastic Block Store (EBS)

OBJECTIVE

To configure and use AWS EBS service

TOPOLOGY



© 2016, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



68

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 **ELASTIC BLOCK STORE** section, the **Volumes** link is highlighted with a red circle. The main content area displays the following information:

Resources
You are using the following Amazon EC2 resources in the US West (Oregon) region:

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	

Create Instance
To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Launch Instance

Note: Your instances will launch in the US West (Oregon) region

Scheduled Events

Account Attributes

- Supported Platforms: VPC
- Default VPC: vpc-89c341ee
- Resource ID length management

Additional Information

- Getting Started Guide
- Documentation
- All EC2 Resources
- Forums
- Pricing
- Contact Us

AWS Marketplace

Find free software trial products in the AWS Marketplace from the [EC2 Launch Wizard](#). Or try these non-AMIs:

Click on **Create Volumes** button

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation menu includes options like Reserved Instances, Scheduled Instances, Dedicated Hosts, IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots), and NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs). The main content area is titled 'Create Volume' and displays a message: 'You do not have any EBS volumes in this region. Click the Create Volume button to create your first volume.' A prominent blue 'Create Volume' button is centered at the bottom of this section. A search bar at the top right says 'None found'. The bottom of the screen features standard AWS footer links for Feedback, English (US), Privacy Policy, and Terms of Use.

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

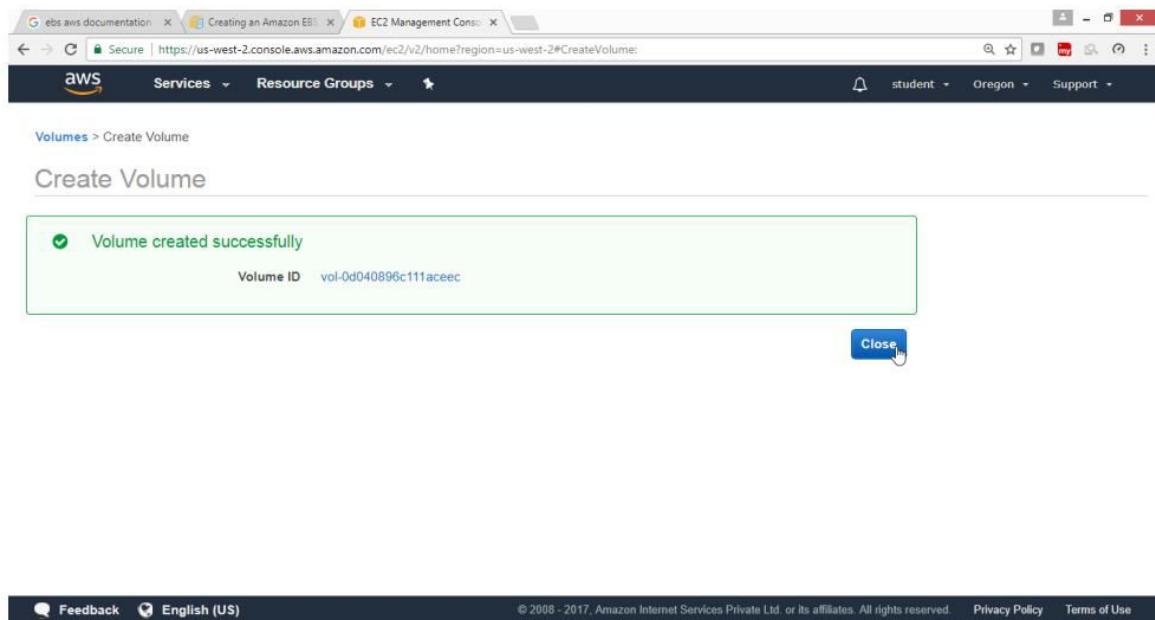
The screenshot shows the 'Create Volume' dialog box on the AWS Management Console. The form fields are as follows:

- Volume Type:** General Purpose SSD (GP2)
- Size (GiB):** 2 (Min: 1 GiB, Max: 16384 GiB)
- IOPS:** 300 / 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
- Snapshot ID:** Select a snapshot
- Encryption:** Encrypt this volume (checkbox checked)
- Tags:** Add tags to your volume (checkbox)

At the bottom right, there are 'Cancel' and 'Create Volume' buttons. The 'Create Volume' button is highlighted with a blue border, indicating it is the active or intended action.

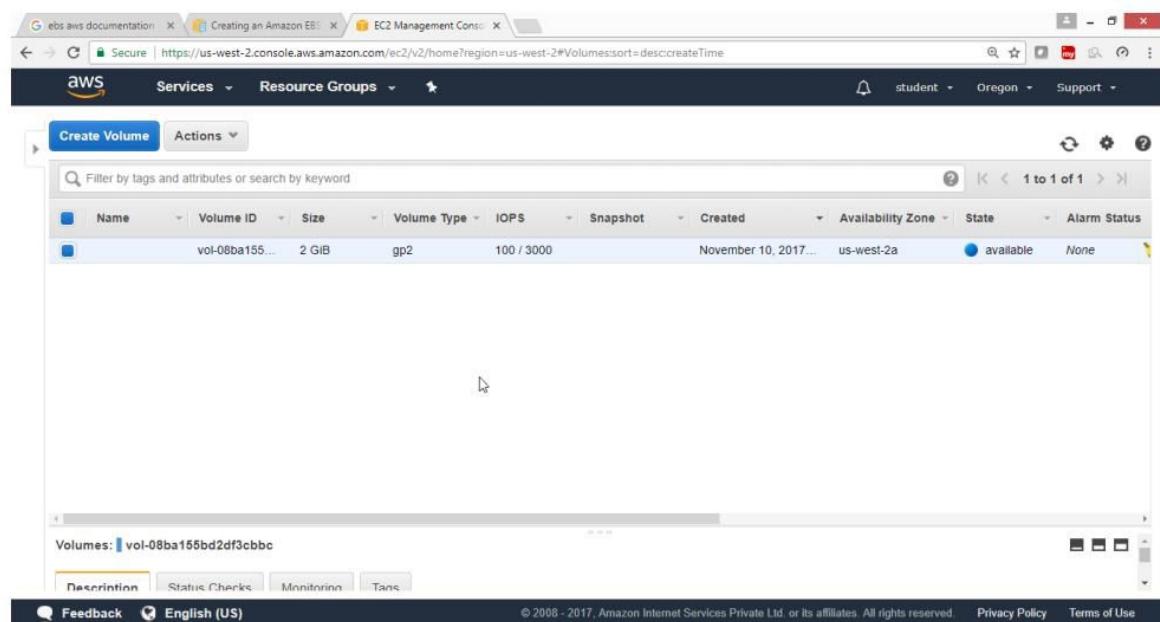
Verify Volume successfully created

Click **Close** button



To Monitoring the State of Your Volumes

Select Volume check state → available



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

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, and Elastic Block Store (selected). Under EBS, 'Volumes' is selected. The main area has a 'Create Volume' button at the top. Below it is a table with columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, and Status. A search bar is above the table. In the table, there are two rows: one for 'Winvm1' and one for '2gb2a'. The '2gb2a' row has its 'Name' field set to '2gb2a'. At the bottom of the table, there's a progress bar showing '5/255' and a checkmark icon. The status bar at the bottom right indicates 'Volumes: vol-08ba155bd2df3cbcc'.

2) To Attaching and Detaching EBS volume in Windows instance

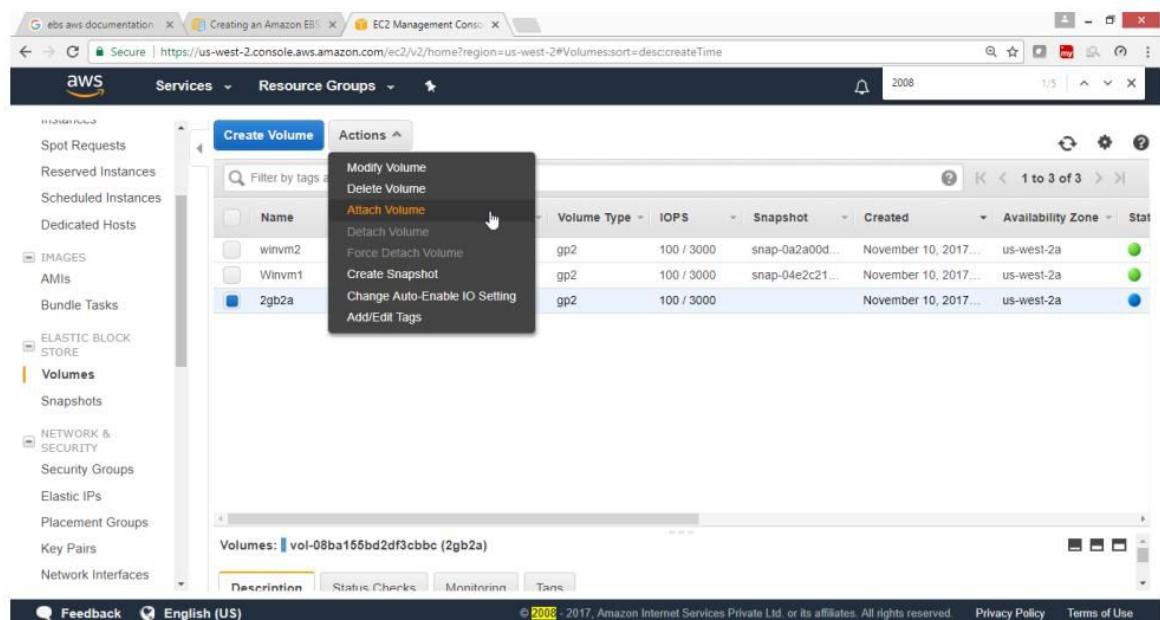
On the **EC2 Dashboard** panel

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

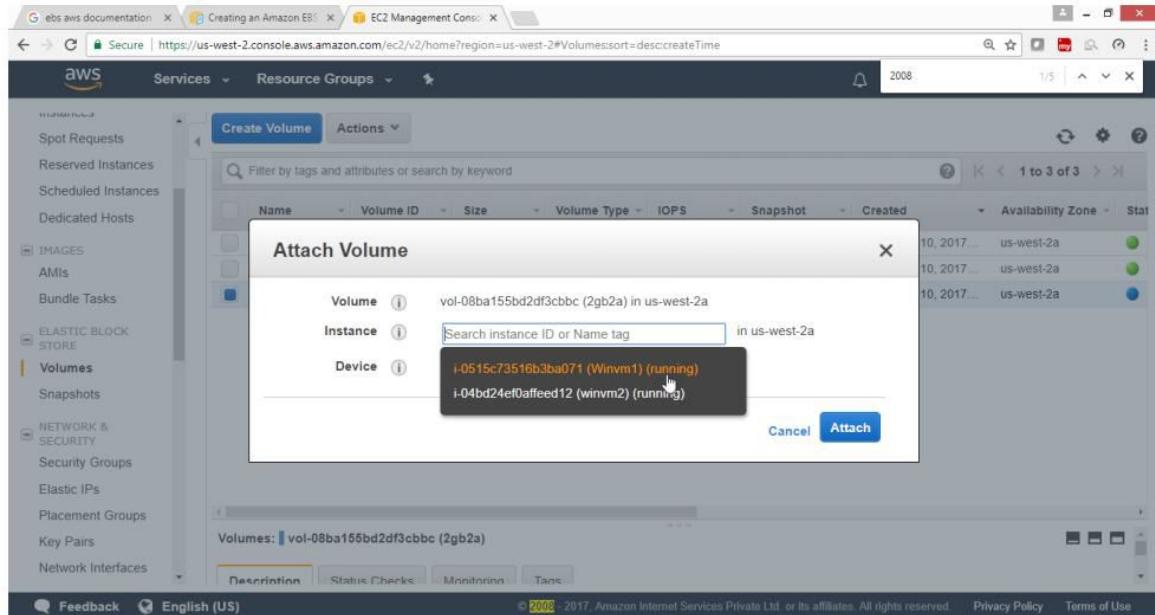
Note : The volume which you want to attach to an instance should be in same Availability zone.

Drop Down **Action** button,

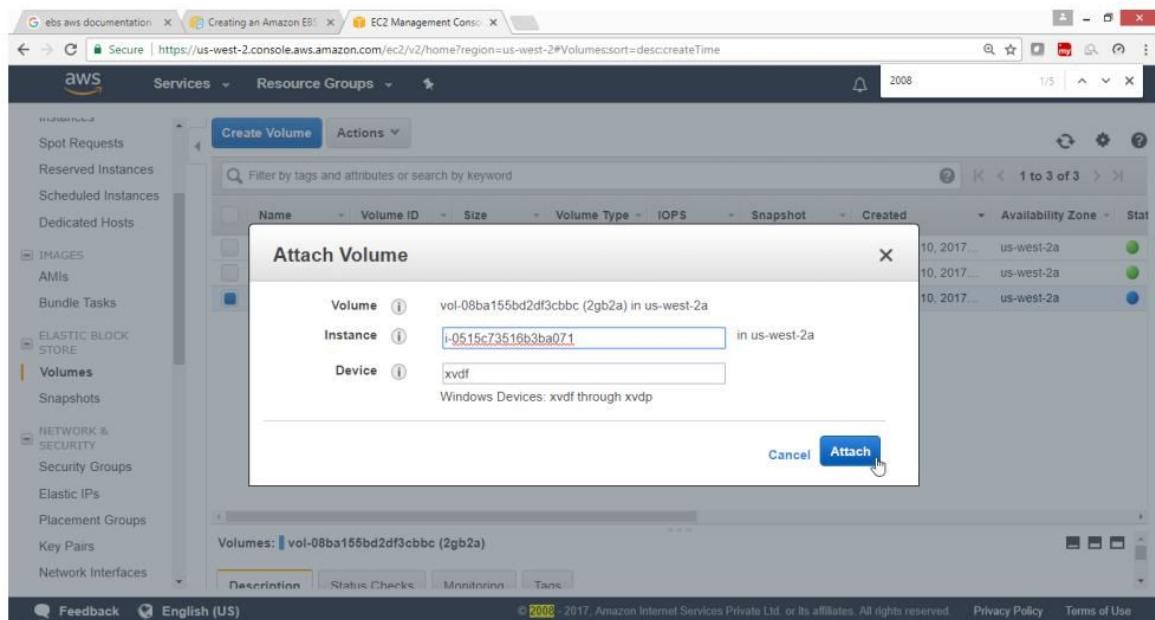
Select **Attach Volume**.



Select instance → Winvm1



Click on Attach

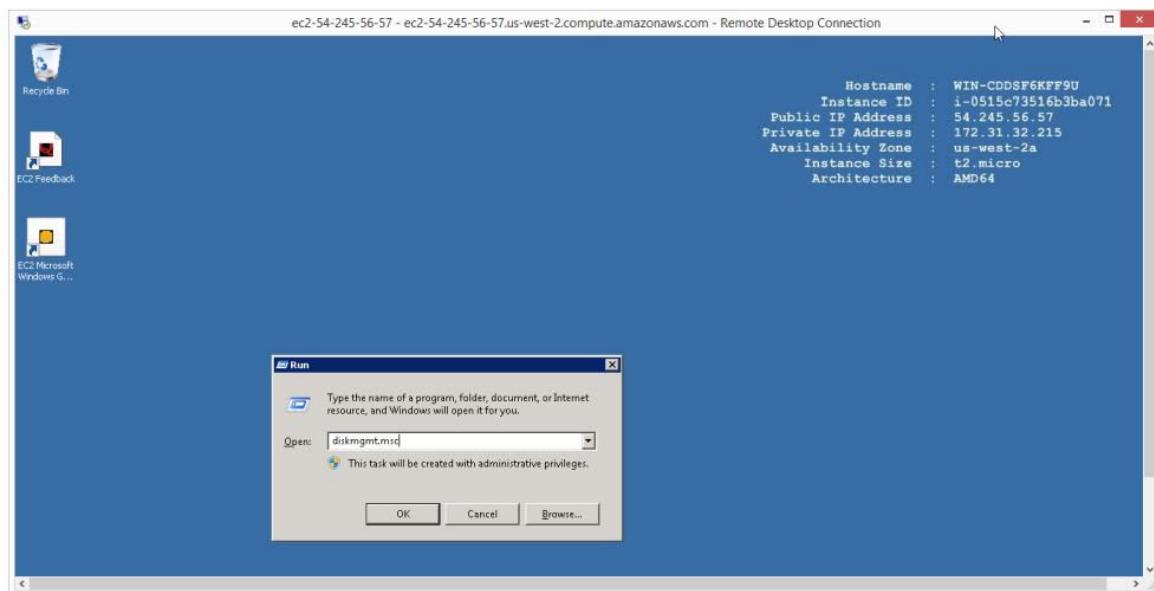


Verify the Availability of new volume

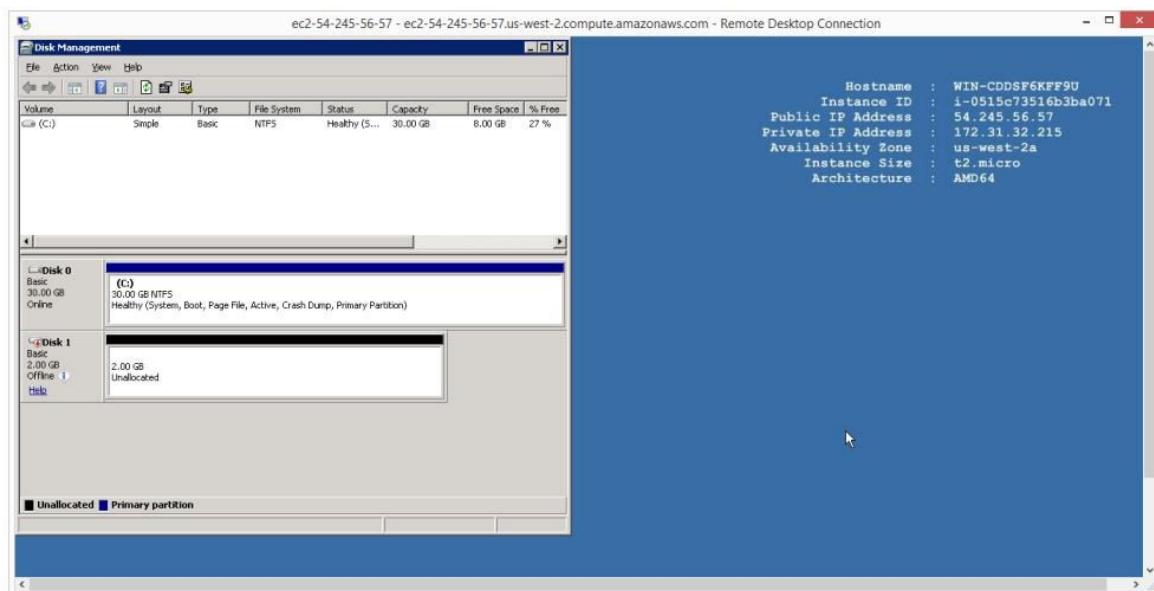
3. To check availability of new drive login to your Windows instance.

Login to windows instance

Run → diskmgmt.msc

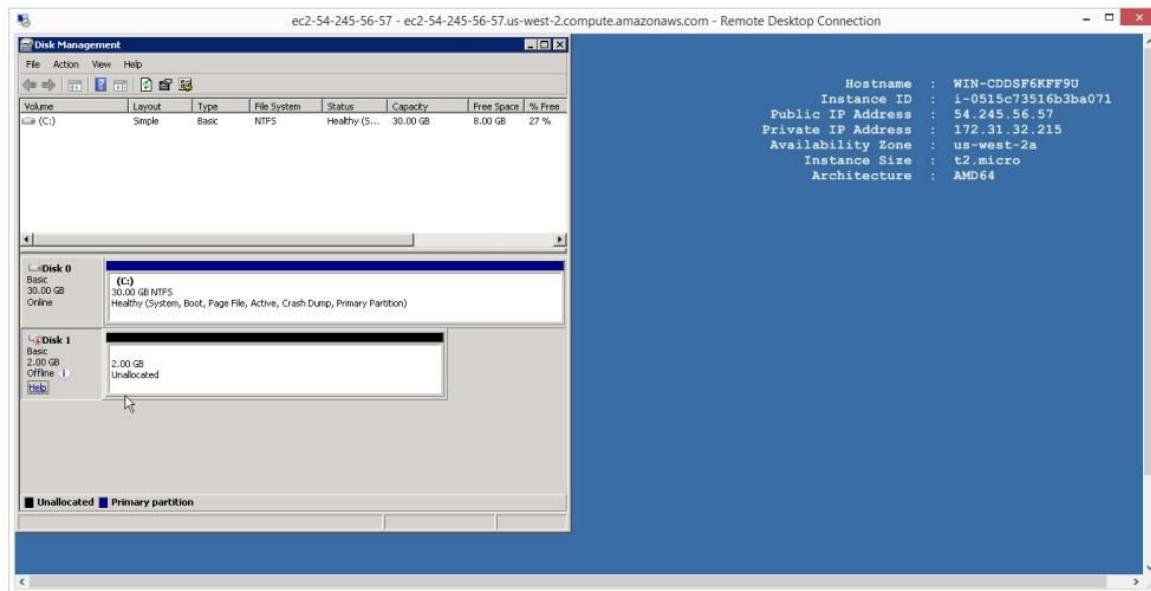


Verifies that 2 GB volume available as unallocated space

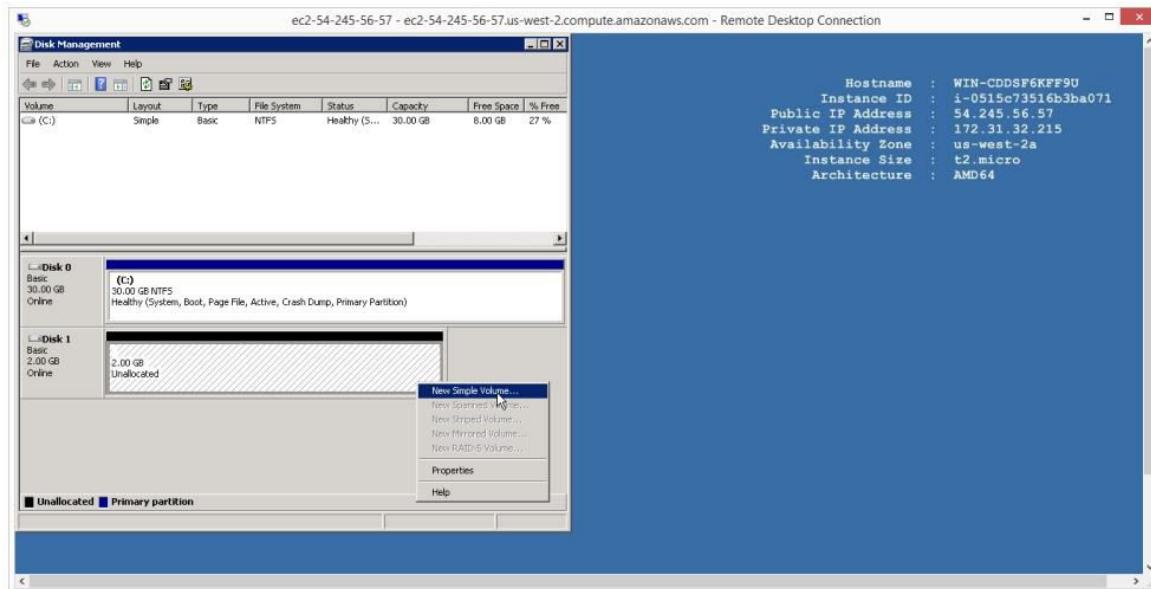


New disk is offline,

So turn it to online by right clicking and select online

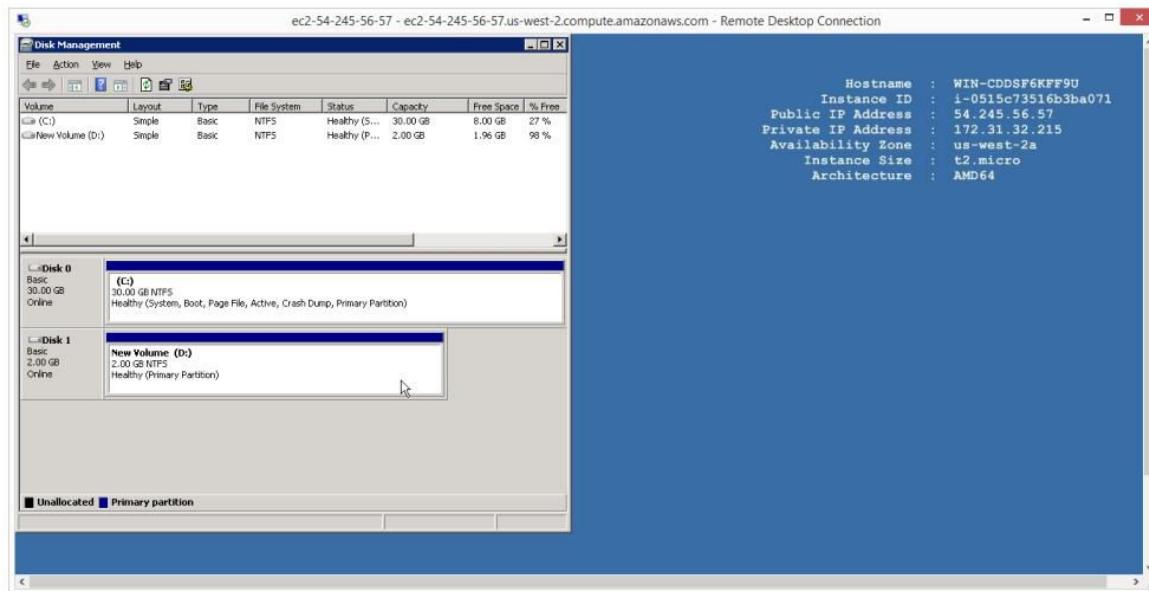


Format the unallocated disk



Verify

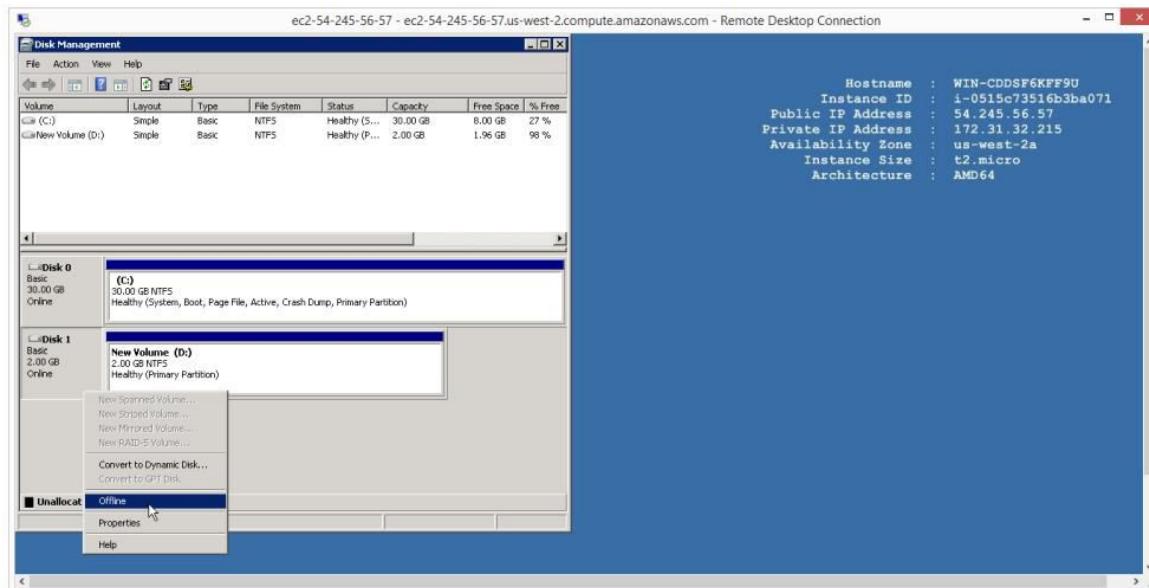
New Volume to 2GB is available to use



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.

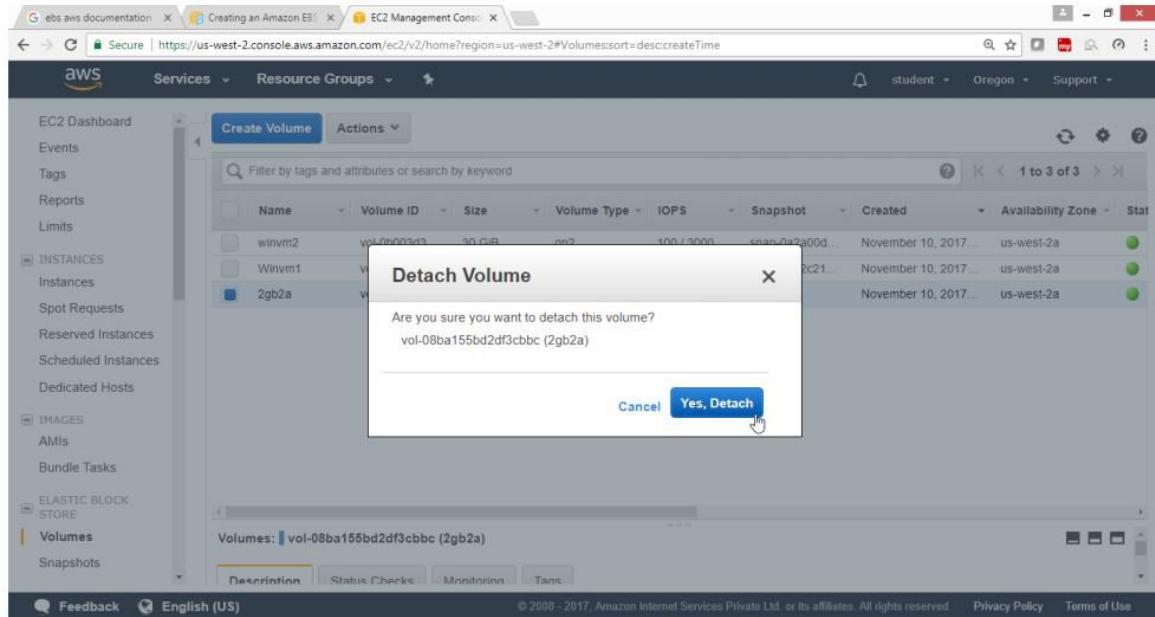
Drop Down **Action** button

Select "Detach Volume"

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, AMIs, and Elastic Block Store. Under EBS, 'Volumes' is selected. In the main area, a table lists three volumes: gp2, 100 / 3000, snap-0a2a00d...; gp2, 100 / 3000, snap-04e2c21...; and gp2, 100 / 3000, snap-0a2a00d.... A context menu is open over the first volume, with 'Actions' expanded. The 'Detach Volume' option is highlighted with a mouse cursor. The table has columns for Volume Type, IOPS, Snapshot, Created, Availability Zone, and Status.

Volume Type	IOPS	Snapshot	Created	Availability Zone	Status
gp2	100 / 3000	snap-0a2a00d...	November 10, 2017...	us-west-2a	green
gp2	100 / 3000	snap-04e2c21...	November 10, 2017...	us-west-2a	green
gp2	100 / 3000	snap-0a2a00d...	November 10, 2017...	us-west-2a	green

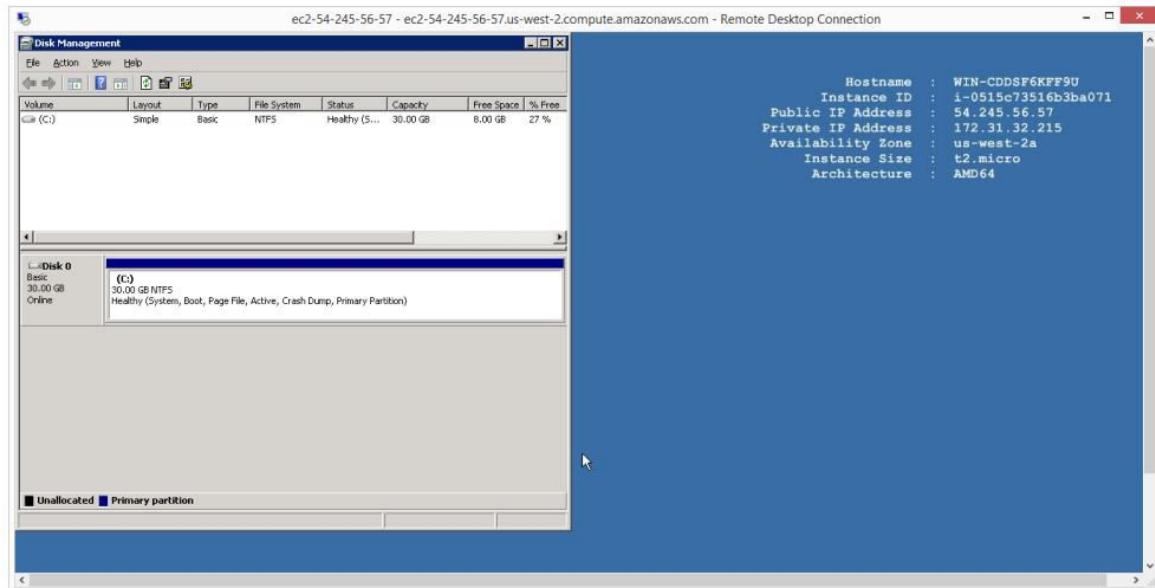
Click on “Yes, Detach” button



Verification

Login to windows instance

Check that D: drive is removed

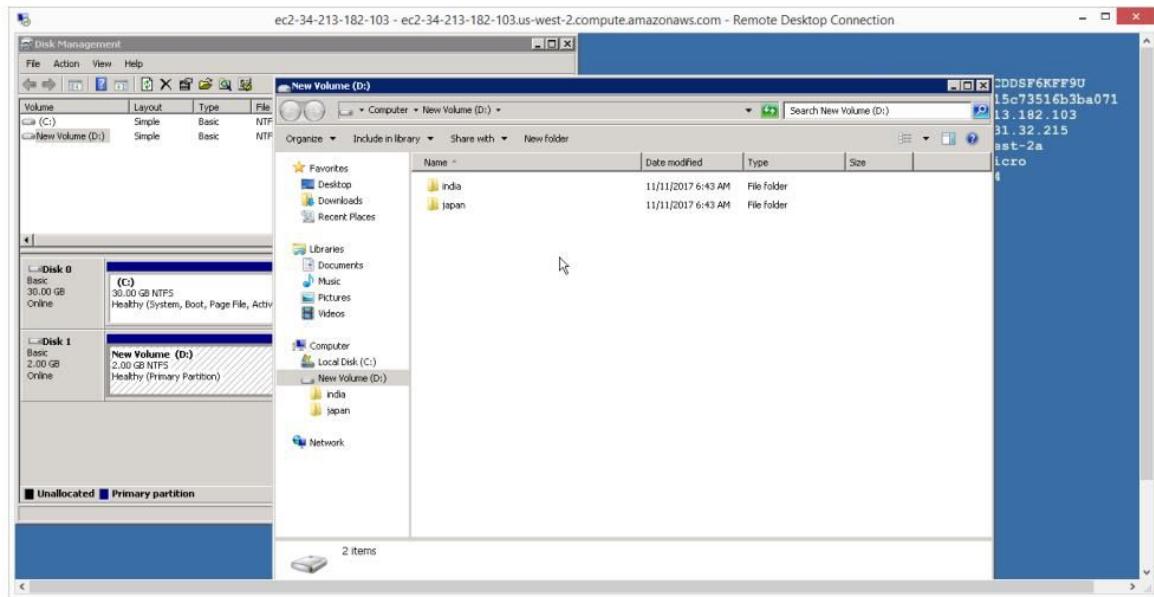


5. To Create Snapshot and Restore EBS volume.

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 open with the 'VOLUMES' section selected under 'ELASTIC BLOCK STORE'. In the main content area, a table lists three volumes: 'gp2', 'gp2', and 'gp2'. A context menu is open over the first 'gp2' volume, with the 'Actions' dropdown expanded. The 'Create Snapshot' option is highlighted with a mouse cursor. The table has columns for 'Volume Type', 'IOPS', 'Snapshot', and 'Created'. The first row's 'Snapshot' column contains 'snap-0a2a00d...', and the 'Created' column shows 'November 10, 2017...'. The second and third rows have similar data.

Provide snapshot details

Click **Create** button

The screenshot shows the 'Create Snapshot' dialog box. It contains four input fields: 'Volume' (set to 'vol-08ba155bd2df3cbcc (2gb2a)'), 'Name' (set to 'snapvol1'), 'Description' (set to 'snapvol1_des'), and 'Encrypted' (set to 'No'). At the bottom right are 'Cancel' and 'Create' buttons, with 'Create' being highlighted.

Verify that snapshot is created.

The screenshot shows the AWS EC2 Management Console interface. The left sidebar has a tree view with 'Scheduled Instances', 'Dedicated Hosts', 'IMAGES', 'AMIs', 'Bundle Tasks', 'ELASTIC BLOCK STORE', 'Volumes', and 'Snapshots'. The 'Snapshots' item is highlighted with an orange circle and a cursor icon. The main content area shows a table titled 'Create Snapshot' with one entry:

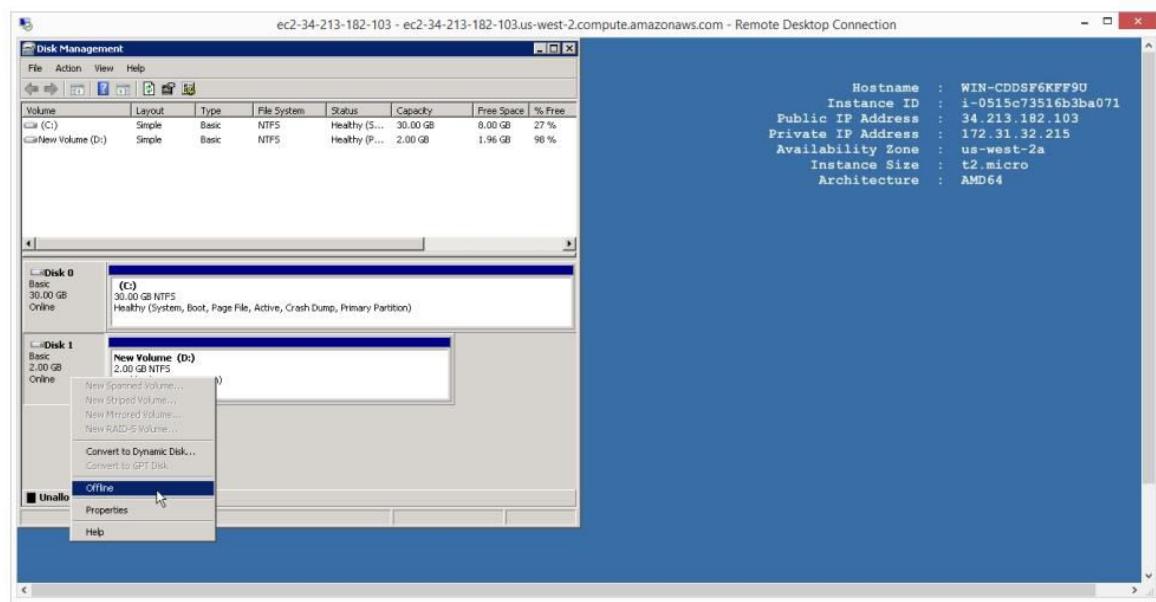
Name	Snapshot ID	Size	Description	Status
snapvol1	snap-08ff48c354563cba0	2 GiB	snapvol1_des	co

Below the table, a message says 'Snapshot: snap-08ff48c354563cba0 (snapvol1)'. There are tabs for 'Description', 'Permissions', and 'Tags'. At the bottom, there's a progress bar at 100% and links for 'Feedback', 'English (US)', '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

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.

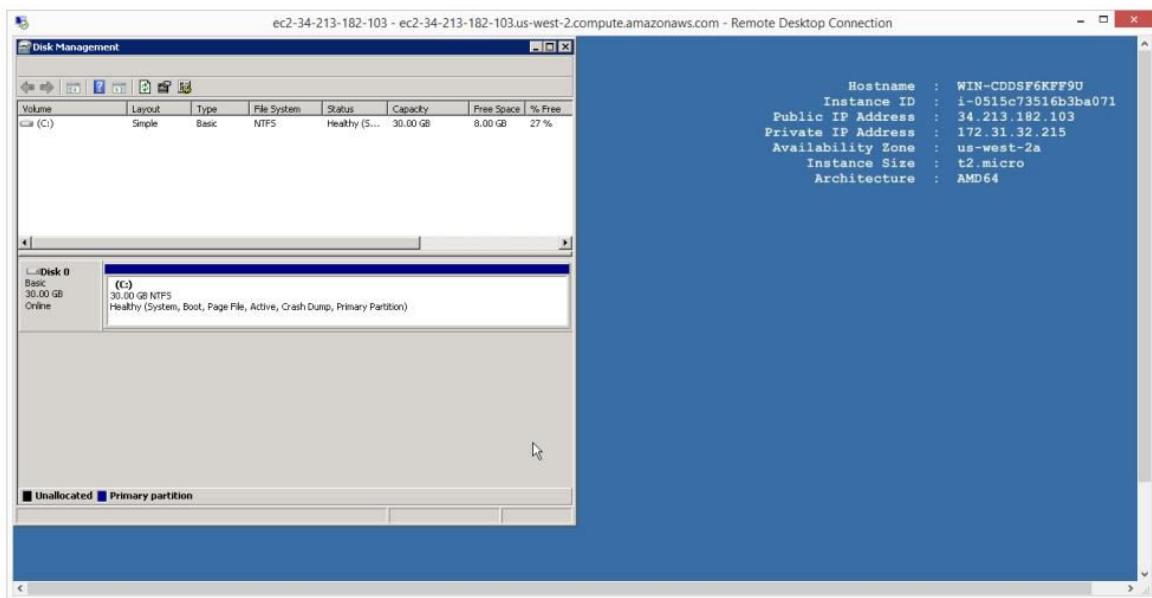
Drop Down Action button, Select “**Delete Volume**”

The screenshot shows the AWS EC2 Management Console interface. On the left, the navigation pane is visible with sections like Scheduled Instances, Dedicated Hosts, IMAGES, AMIs, Bundle Tasks, ELASTIC BLOCK STORE (with Volumes selected), Snapshots, NETWORK & SECURITY, Security Groups, Elastic IPs, Placement Groups, Key Pairs, and Network Interfaces. The main content area displays a table of volumes. A specific volume, "2gb2a", is selected and highlighted with a blue border. A context menu is open over this volume, with the "Actions" option expanded. The "Detach Volume" option is highlighted with a mouse cursor. The table below shows three gp2 volumes with the following details:

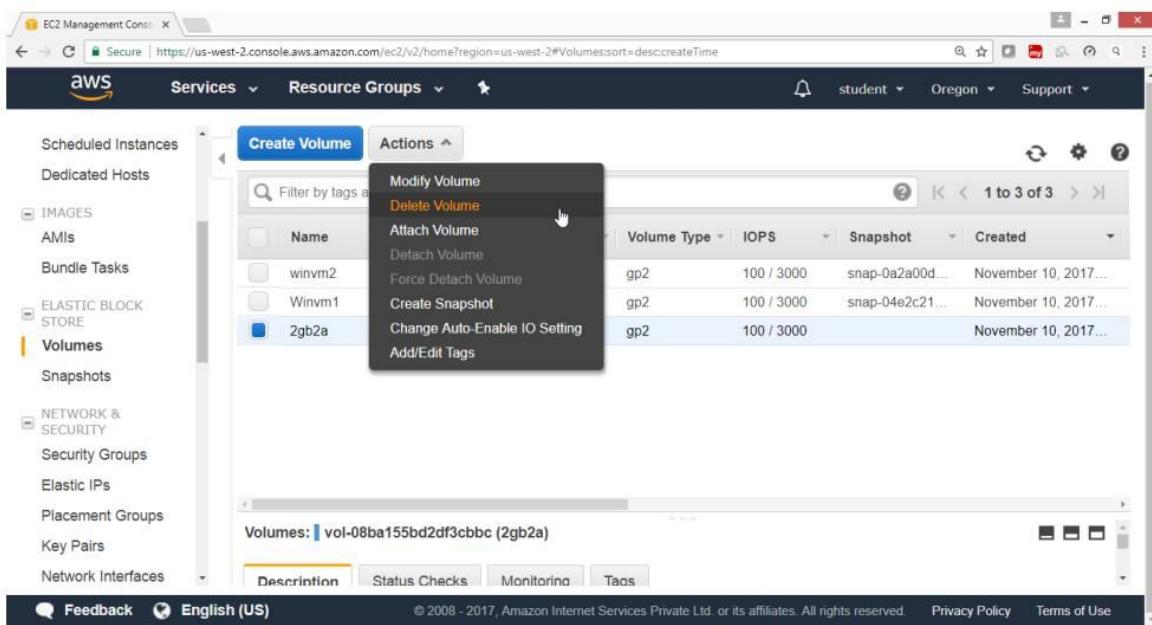
Volume Type	IOPS	Snapshot	Created
gp2	100 / 3000	snap-0a2a00d...	November 10, 2017...
gp2	100 / 3000	snap-04e2c21...	November 10, 2017...
gp2	100 / 3000		November 10, 2017...

Verify from windows instance open disk Management tool

Now D drive is detached



Now delete the volume



Verify volume is deleted.

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation includes: Scheduled Instances, Dedicated Hosts, IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots), NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces). The main content area is titled "Create Volume" and shows a table of existing volumes. The table has columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, and Created. Two volumes are listed: "winvm2" and "Winvm1". Both volumes have a size of 30 GiB, a Volume Type of gp2, and IOPS of 100 / 3000. Their snapshots are "snap-0a2a00d..." and "snap-04e2c21...". They were created on November 10, 2017. Below the table, a message says "Select a volume above". At the bottom of the page, there are links for Feedback, English (US), Privacy Policy, and Terms of Use.

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
winvm2	vol-0b003d3...	30 GiB	gp2	100 / 3000	snap-0a2a00d...	November 10, 2017...
Winvm1	vol-0b2680a...	30 GiB	gp2	100 / 3000	snap-04e2c21...	November 10, 2017...

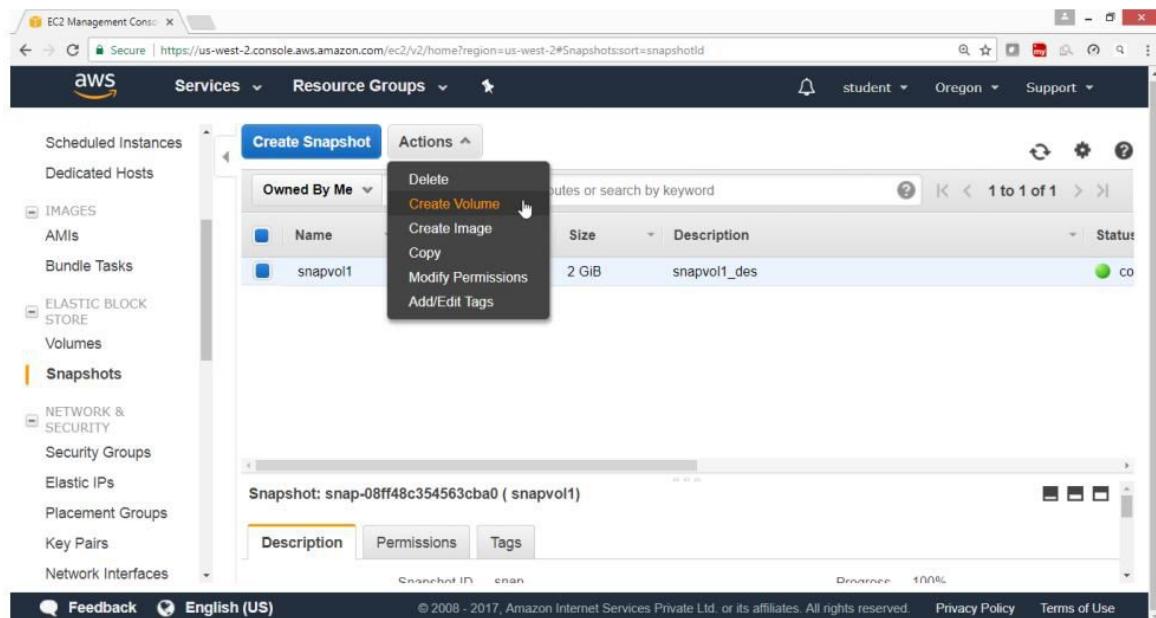
7. To Restore the volume.

From the console **EC2 Dashboard**

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

Select the snapshot

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



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 fields are as follows:

- Snapshot ID:** snap-08ff48c354563cba0 (snapvol01)
- 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

At the bottom, there is a note: *** Required**. The 'Create Volume' button is highlighted with a mouse cursor.

Verify Volume is created

The screenshot shows the 'Volumes' section in the AWS EC2 Management Console. The table displays the following volume information:

Name	Volume ID	Size	Type	IOPS	Snapshot	Created
winvm2	vol-0cd6da3c...	2 GiB	gp2	100 / 3000	snap-08ff48c3...	November 11, 2017...
winvm2	vol-0b003d3...	30 GiB	gp2	100 / 3000	snap-0a2a00d...	November 10, 2017...
Winvm1	vol-0b2680a...	30 GiB	gp2	100 / 3000	snap-04e2c21...	November 10, 2017...

7) To expanding the size of EBS volume.

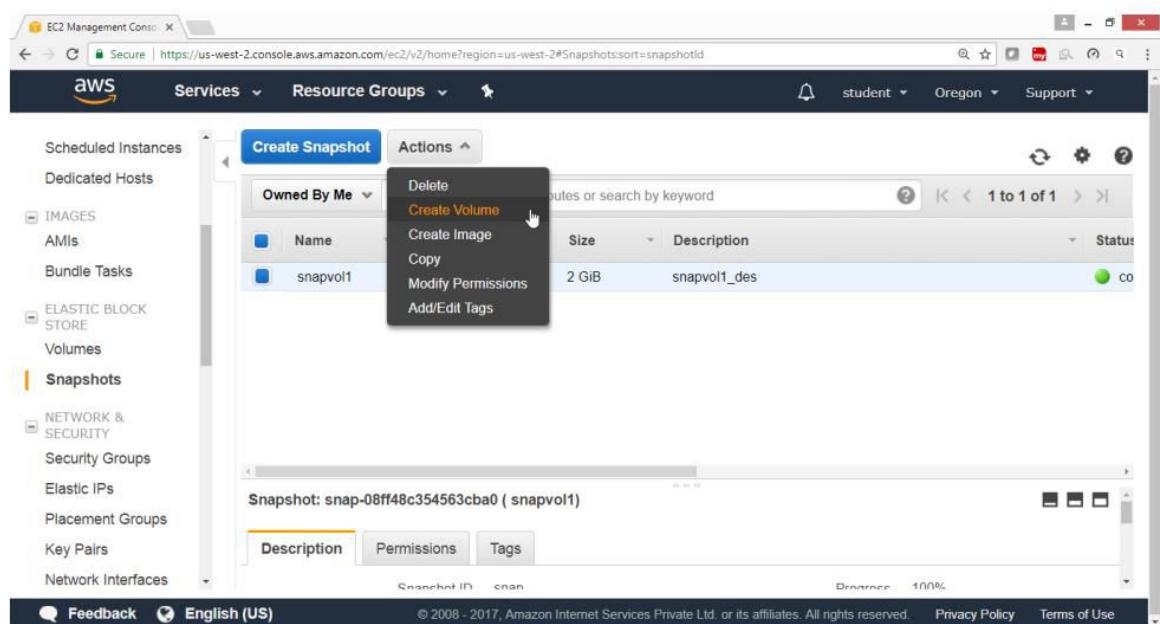
To expand EBS volume first take **snapshot**, now select the snapshot

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' wizard in the AWS Management Console. The configuration is as follows:

- Snapshot ID:** snap-08ff48c354563cba0 (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
- Tags:** Add tags to your volume

* Required

Cancel **Create Volume**

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

Verify that 4 GB is created

The screenshot shows the 'Volumes' page in the AWS Management Console. A new volume has been created and is listed in the table:

Name	Volume ID	Size	Type	IOPS	Snapshot	Created
vol-034d7007ffcef5949	vol-034d7007ffcef5949	4 GiB	gp2	100 / 3000	snap-08ff48c354563cba0	November 11, 2017
vol-0cd6da3c...	vol-0cd6da3c...	2 GiB	gp2	100 / 3000	snap-08ff48c354563cba0	November 11, 2017
winvm2	vol-0b003d3...	30 GiB	gp2	100 / 3000	snap-0a2a00d...	November 10, 2017
Winvm1	vol-0b2680a...	30 GiB	gp2	100 / 3000	snap-04e2c21...	November 10, 2017

Volumes: vol-034d7007ffcef5949

Description Status Checks Monitoring Tags

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

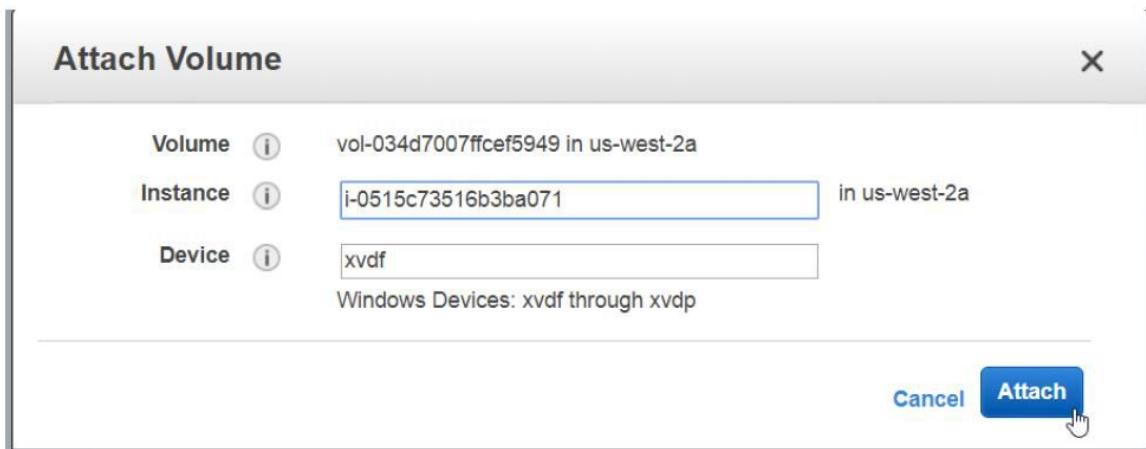
Now attach this expanded volume to your instance.

The screenshot shows the AWS EC2 Management Console. On the left, there's a navigation sidebar with options like Scheduled Instances, Dedicated Hosts, AMIs, Bundle Tasks, Elastic Block Store, Volumes (which is selected), and Snapshots. The main area has a title 'Create Volume' and an 'Actions' dropdown menu. The 'Actions' menu is open, showing options: Modify Volume, Delete Volume, Attach Volume (which is highlighted in orange), Detach Volume, Force Detach Volume, Create Snapshot, Change Auto-Enable IO Setting, and Add/Edit Tags. Below the menu, there's a table listing volumes. The table has columns: Volume Type, IOPS, Snapshot, and Created. There are four entries, all of which are gp2 type with 100 IOPS. The first entry is associated with a snapshot from November 11, 2017, and the others from November 10, 2017. At the bottom of the table, it says 'Volumes: vol-034d7007ffcef5949'. Below the table are tabs for Description, Status Checks, Monitoring, and Tags. At the very bottom of the page, there are links for Feedback, English (US), Privacy Policy, and Terms of Use.

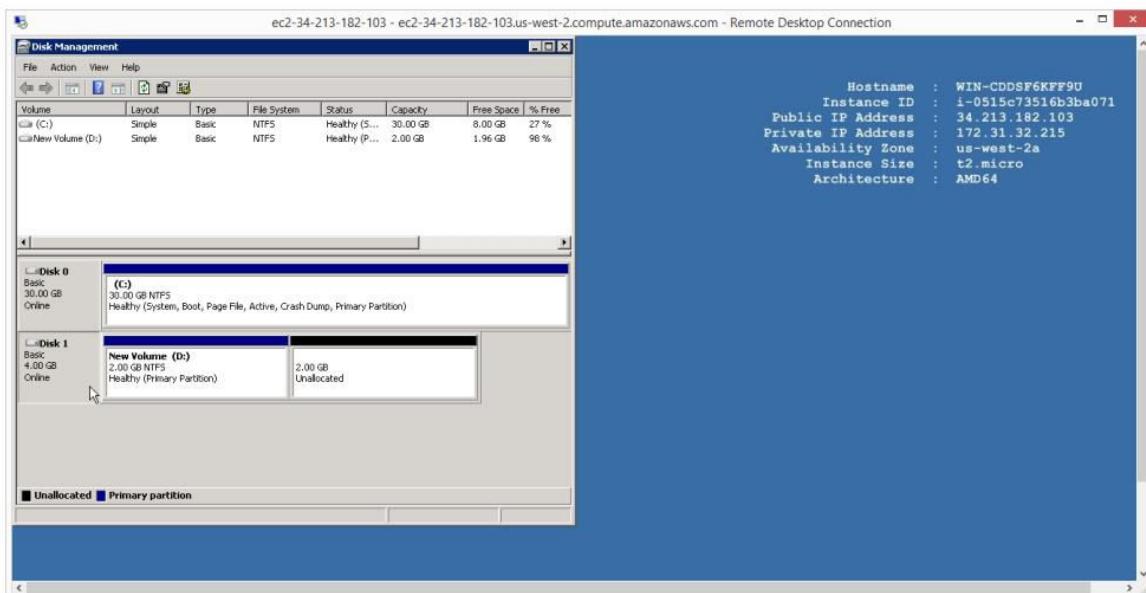
Select instance

This screenshot shows the 'Attach Volume' dialog box. It has fields for 'Volume' (set to 'vol-034d7007ffcef5949 in us-west-2a'), 'Instance' (a search bar containing 'Search instance ID or Name tag in us-west-2a'), and 'Device' (a dropdown menu showing two options: 'i-0515c73516b3ba071 (Winvm1) (running)' and 'i-04bd24ef0affeed12 (winvm2) (running)'). A cursor is hovering over the second device option. At the bottom right of the dialog are 'Cancel' and 'Attach' buttons.

Click **Attach** button

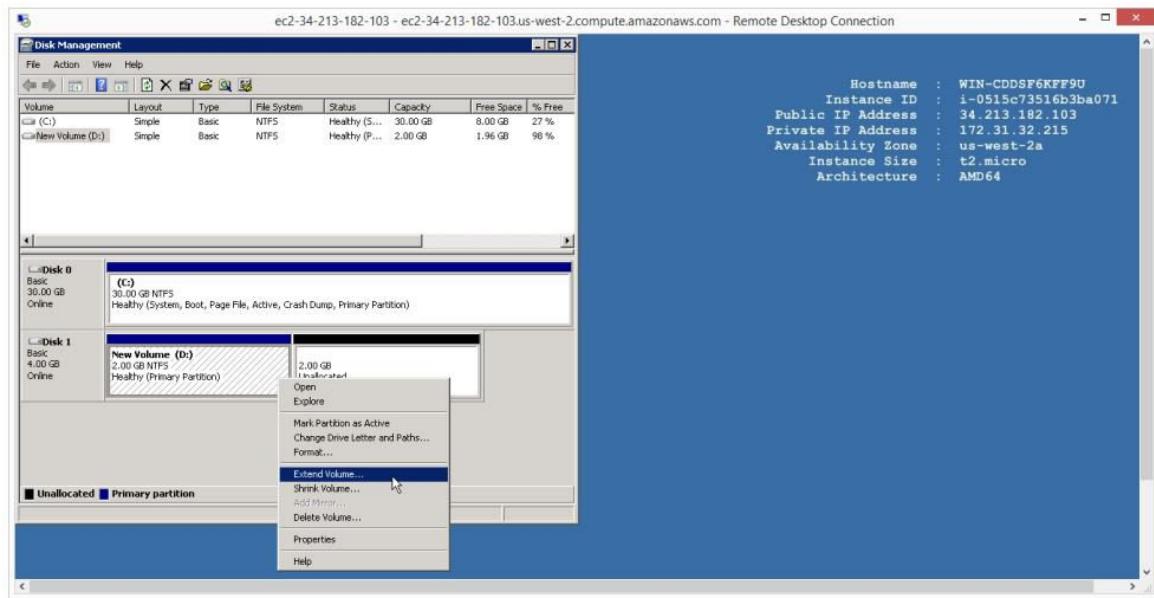


Verify 4 GB drive is available

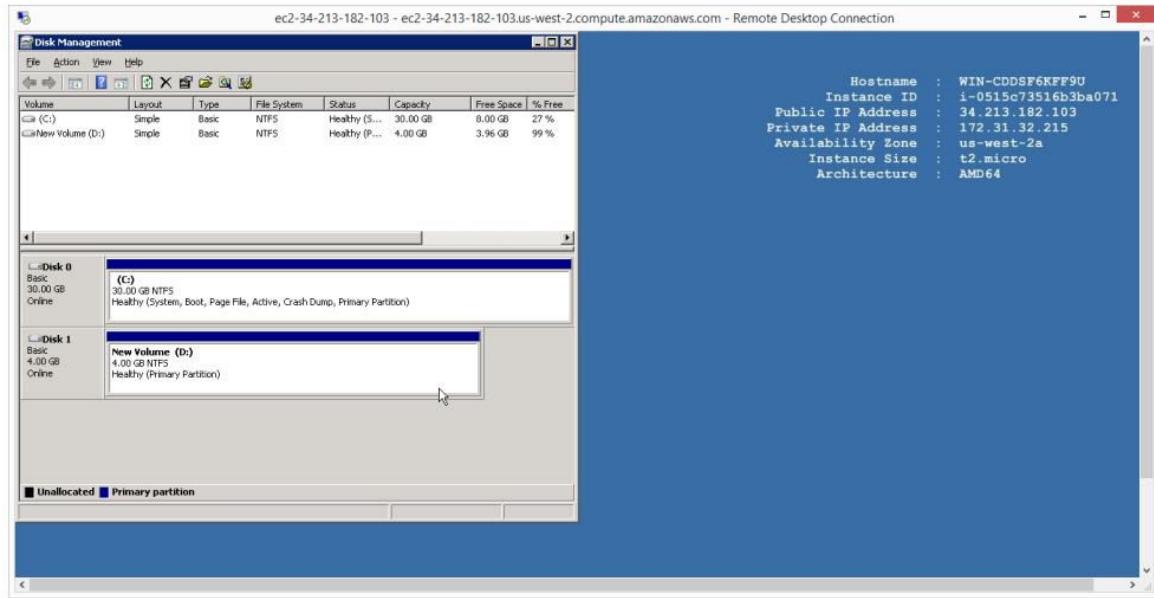


Now with respect to Windows operating system

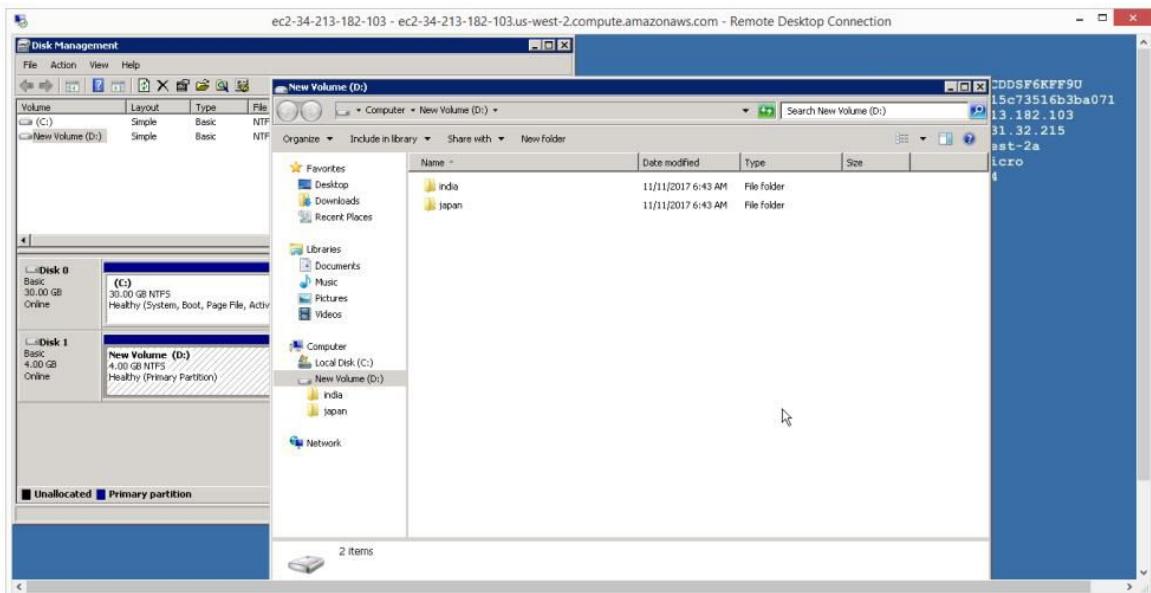
Right click on D drive extend your volume to your desired size



Verified that 4 GB volume available

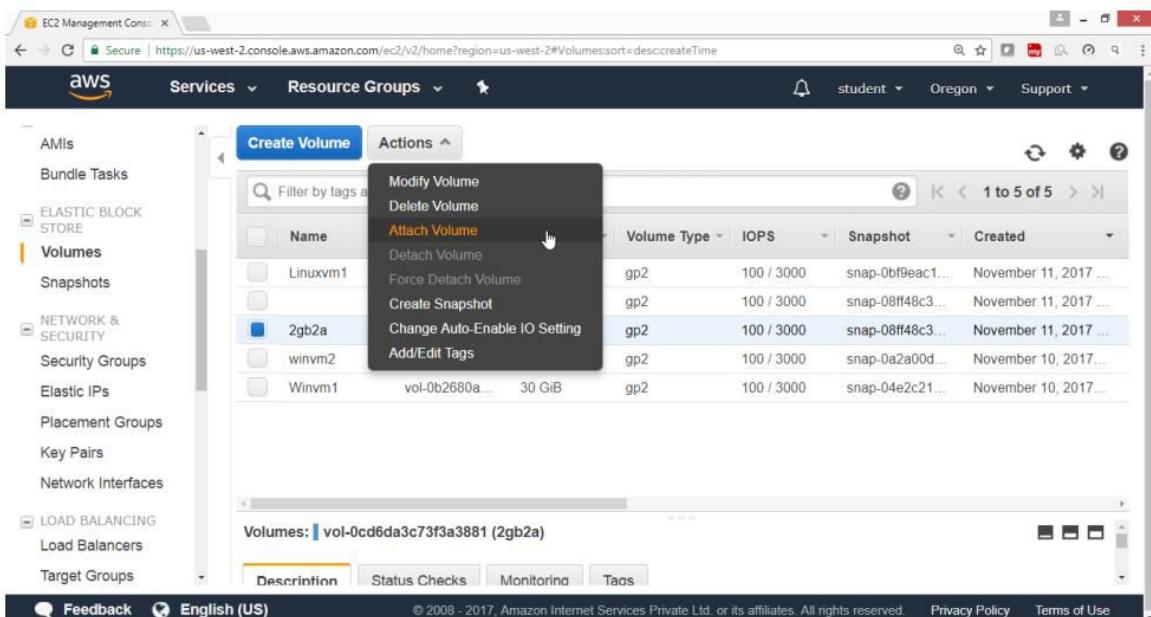


Verified that D drive contains two folders that was there in 2B drive earlier.

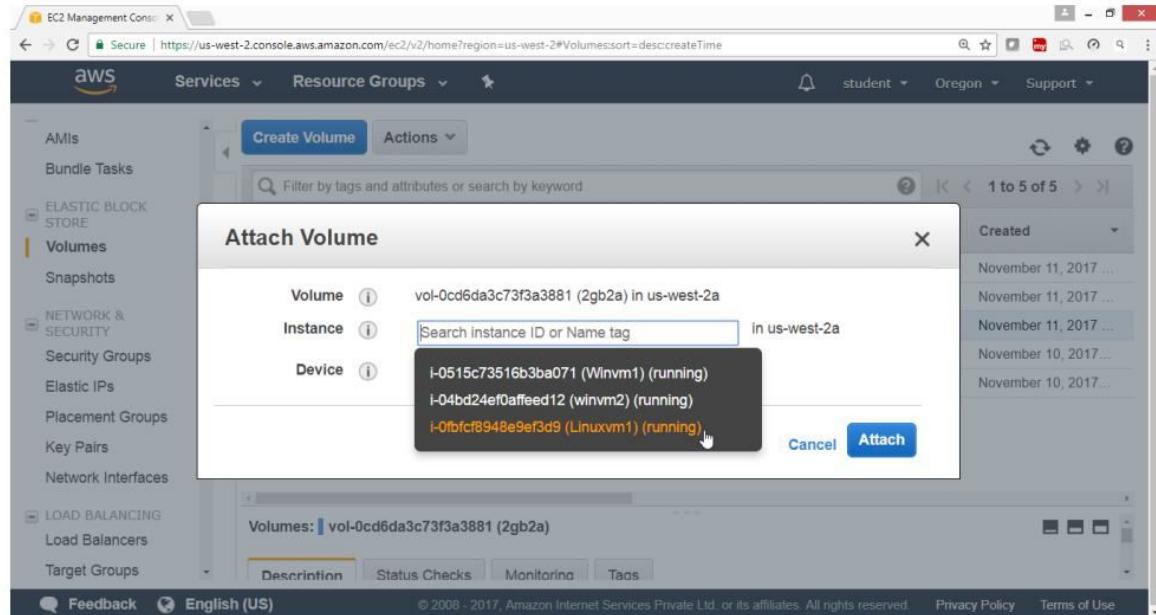


Similarly check volume in linux instance

From Action select **Attach volume**



Select Linux instance



Now connect to Linux instance

```
[2017-11-11 12:58.46] /drives/e/awskeys
[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]#
[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 partition  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
```

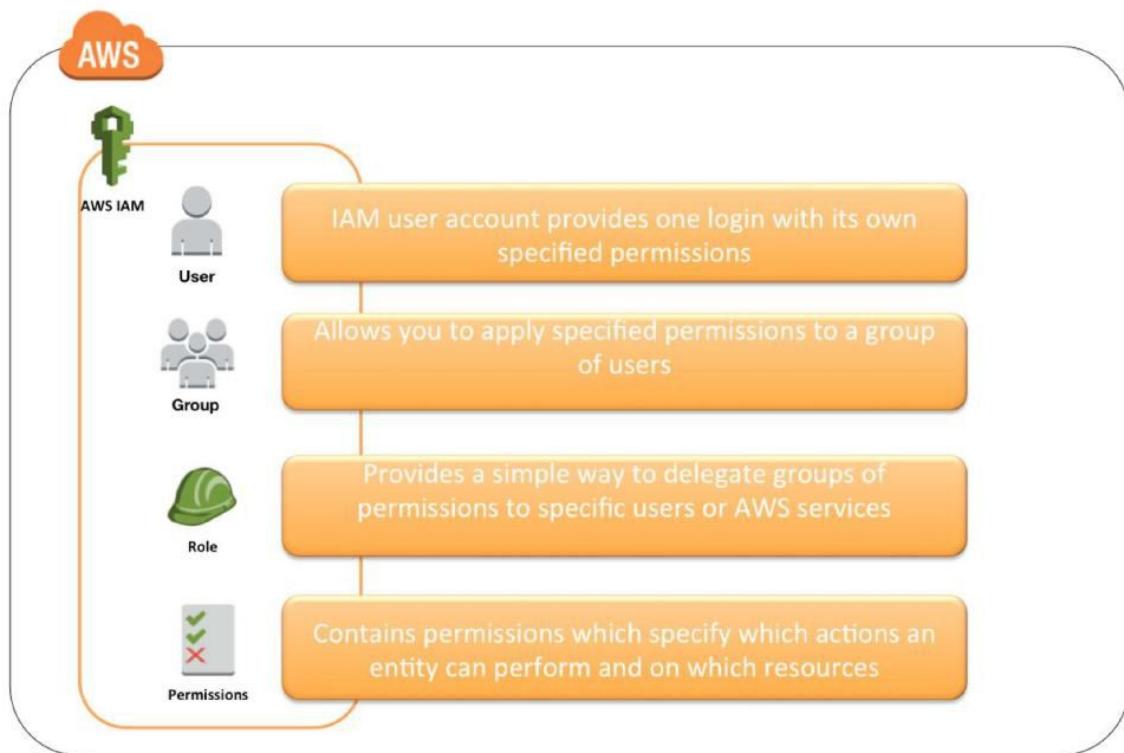
Lab 6: To Manage IAM Users, Groups and Policies

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.

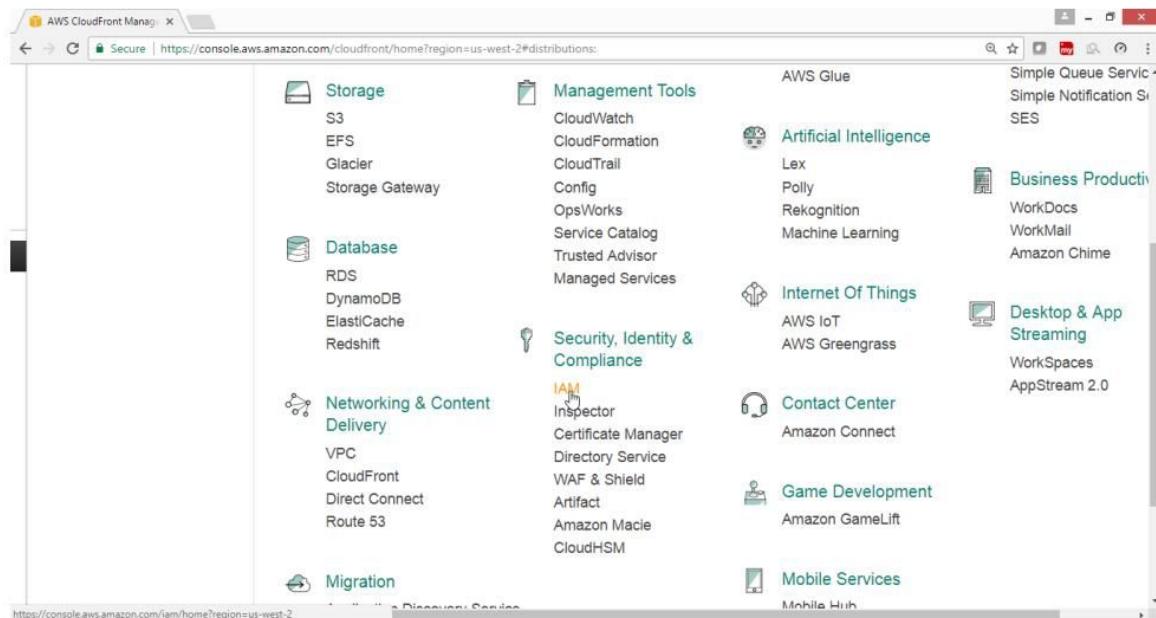
Users Login to sign-in page.

Deleting users and groups.

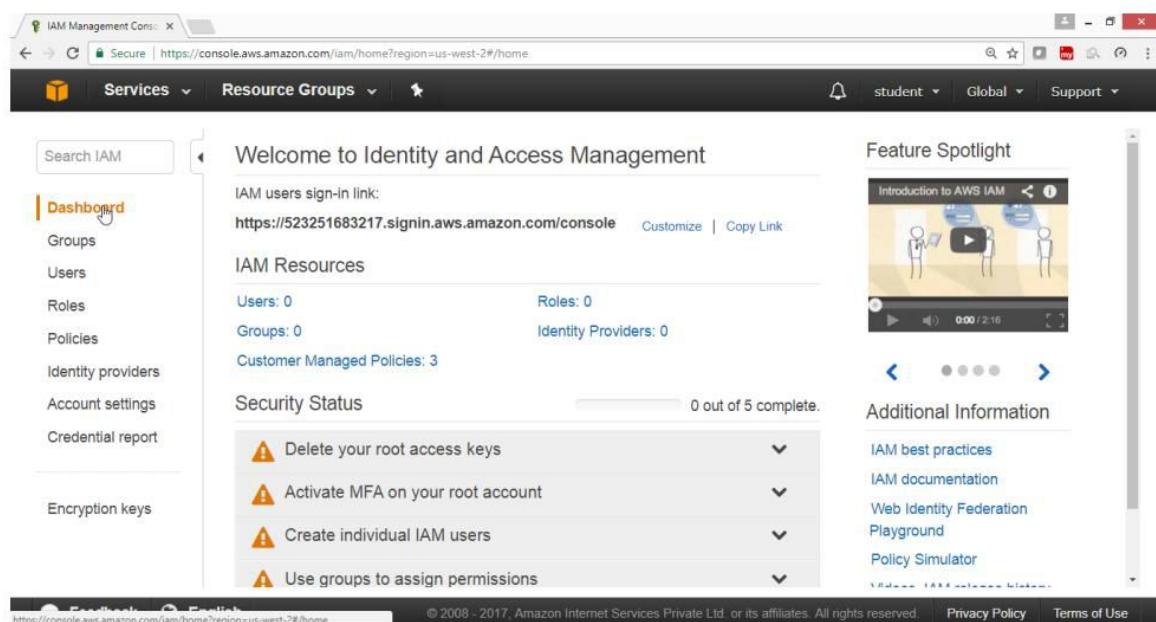
1) To create user, assign password, change password policy.

Open AWS console select **Security, Identity & Compliance**

Click on **IAM service**



IAM Dashboard panel available



2) To Mange Groups and applying policies

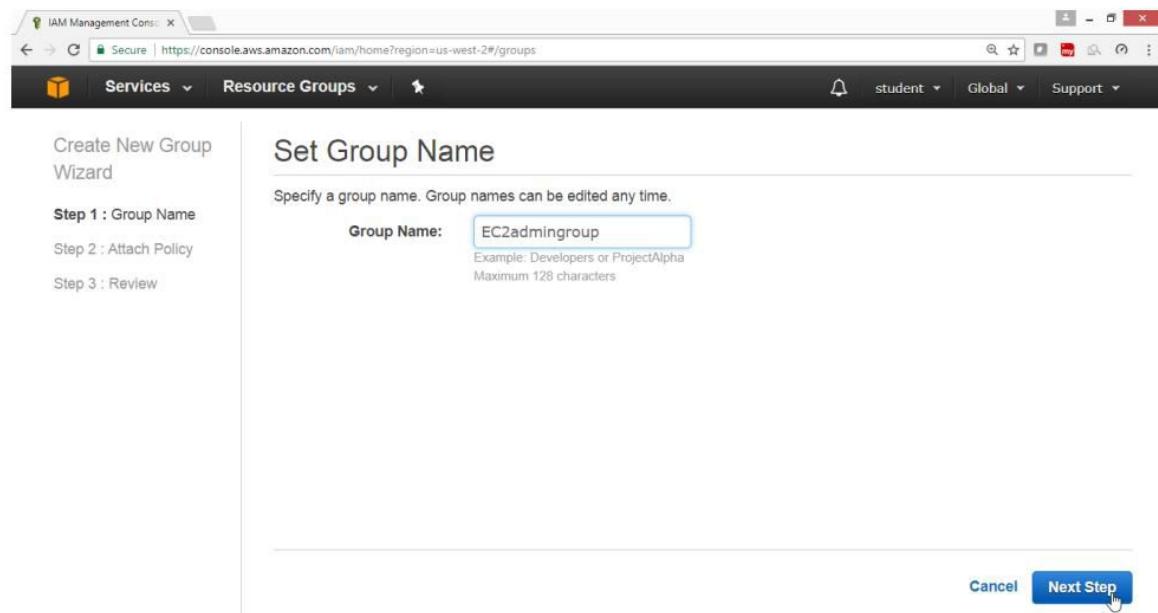
From IAM dashboard, select **Groups**

Click on **Create New Group** button

The screenshot shows the AWS IAM Management Console Groups page. The URL is https://console.aws.amazon.com/iam/home?region=us-west-2#/groups. The left sidebar has 'Groups' selected. The main area has a 'Create New Group' button highlighted with a mouse cursor. The table below shows 0 results with columns for Group Name, Users, Inline Policy, and Creation Time.

Give Group Name → EC2admingroup

Click on **Next Step** button



In Filter type → EC2f

Select check box for **AmazonEC2FullAccess**

Click on **Next Step** button

Attach Policy

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

	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 ...

Cancel Previous Next Step

Click on **Create Group**

Review

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

Group Name	EC2admingroup	Edit Group Name
Policies	arn:aws:iam::aws:policy/AmazonEC2FullAccess	Edit Policies

Cancel Previous Create Group

Verify

Group EC2admingrp got created with AmazonEC2FullAccess policy

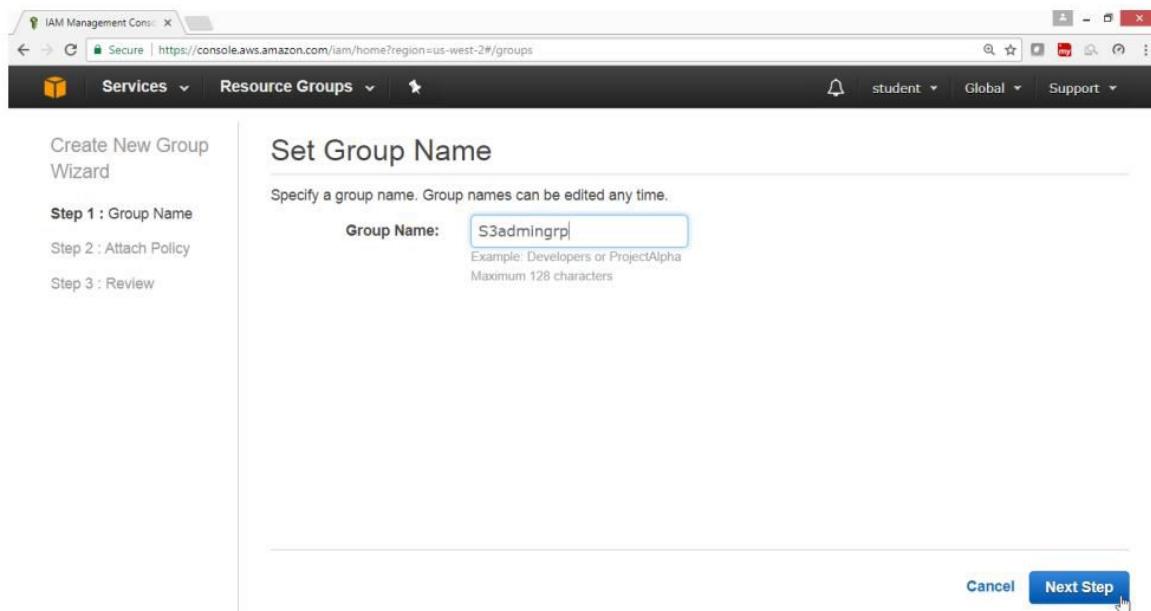
The screenshot shows the IAM Management Console interface. On the left, there's a sidebar with 'Groups' selected. The main area has tabs for 'Users', 'Permissions' (which is active), and 'Access Advisor'. Under 'Permissions', there's a section for 'Managed Policies' with a table showing one policy: 'AmazonEC2FullAccess' with actions 'Show Policy', 'Detach Policy', and 'Simulate Policy'. The 'Creation Time' is listed as 2017-08-15 15:35 UTC+0530.

Now again create Another Group

Click on **Create Group** button

The screenshot shows the 'Create New Group' page. The 'Group Actions' dropdown is open. Below it, a table lists one result: 'EC2admingroup' with 0 users, an inline policy, and a creation time of 2017-08-15 15:35 UTC+0530. The table has columns for 'Group Name', 'Users', 'Inline Policy', and 'Creation Time'.

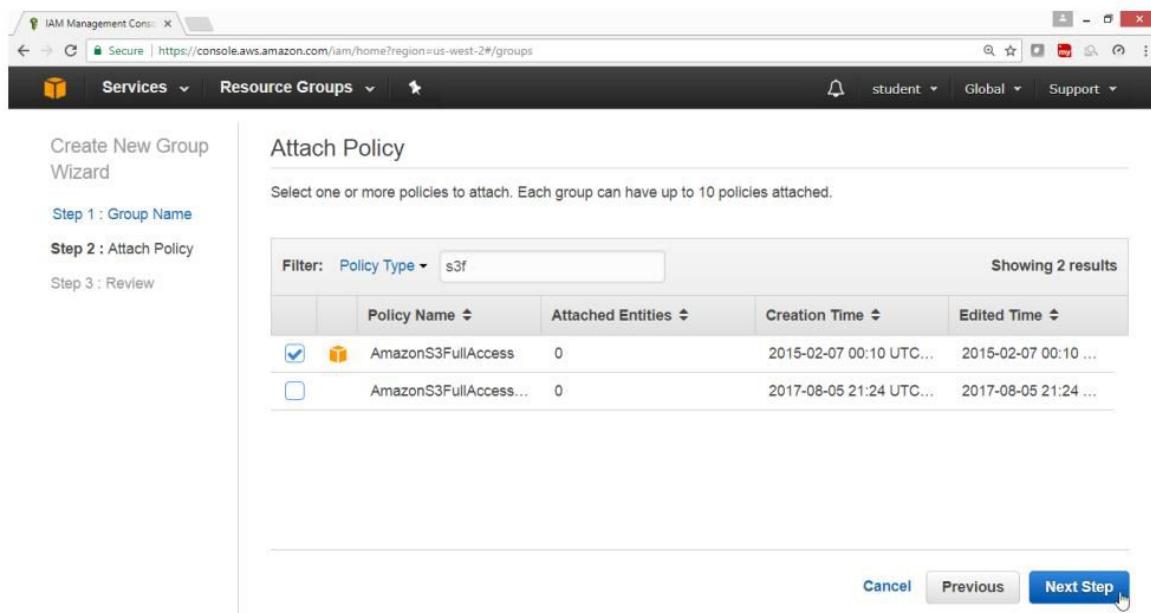
To create a group With S3FullAccess



In Filter type → S3f

Select check box for **AmazonS3FullAccess**

Click on **Next Step** button



Click on **Create Group** button

The screenshot shows the 'Review' step of the 'Create New Group Wizard'. The group name is set to 'S3admingrp'. The attached policy is 'arn:aws:iam::aws:policy/AmazonS3FullAccess'. The 'Create Group' button is highlighted.

Verify EC2admingroup & S3admingr groups got created

The screenshot shows the list of groups in the AWS IAM Management Console. There are two groups listed: 'EC2admingroup' and 'S3admingrp', both created on 2017-08-15 15:35 UTC+0530.

Group Name	Users	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 Permissions page. The navigation bar at the top includes 'Services' (dropdown), 'Resource Groups' (dropdown), a bell icon, 'student' (dropdown), 'Global' (dropdown), and 'Support' (dropdown). On the left, a sidebar menu lists 'Dashboard', 'Groups' (selected), 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Credential report', 'Encryption keys', 'Feedback' (dropdown), and 'English' (dropdown). The main content area has a 'Creation Time' of '2017-08-15 15:42 UTC+0530'. It displays three tabs: 'Users' (selected), 'Permissions' (highlighted in orange), and 'Access Advisor'. Under 'Permissions', there's a section for 'Managed Policies' with a message: 'The following managed policies are attached to this group. You can attach up to 10 managed policies.' A blue 'Attach Policy' button is present. A table lists one policy: 'AmazonS3FullAccess' with actions 'Show Policy', 'Detach Policy', and 'Simulate Policy'. There is also a section for 'Inline Policies' which is currently collapsed.

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

The screenshot shows the AWS IAM Management Console. The URL is https://console.aws.amazon.com/iam/home?region=us-west-2#users. The sidebar on the left has tabs for Dashboard, Groups, Users (which is selected), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area has a search bar labeled 'Find users by username or access key'. Below it is a table with the following columns: 'User name' (with a dropdown arrow), 'Groups', 'Access key age', 'Password age', and 'Last activity'. A message at the bottom of the table says 'There are no IAM users. [Learn more](#)'. At the top right, there are icons for refresh, settings, and help. The top navigation bar includes 'Services', 'Resource Groups', a user icon, 'student', 'Global', and 'Support'.

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', a notification bell, and account information ('student', 'Global', 'Support'). The main title is 'Add user'. A progress bar at the top right shows four steps: 1 (Details, highlighted in blue), 2 (Permissions), 3 (Review), and 4 (Complete). The current step is 'Set user details'. It asks for a 'User name*' and provides a 'tom' placeholder. Below it is a link to 'Add another user'. The next section, 'Select AWS access type', allows choosing between 'Programmatic access' (unchecked) and 'AWS Management Console access' (checked). A note states: 'Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step.' At the bottom, there are links for 'Feedback', 'English', and legal notices: '© 2008–2017, Amazon Internet Services Private Ltd., or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

For Console password → *****

Click on Next Permissions button

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**

Under Group column

Select EC2admingroup

Click on Next Review

Group	Attached policies
<input checked="" type="checkbox"/> EC2admingroup	AmazonEC2FullAccess
<input type="checkbox"/> S3admingrp	AmazonS3FullAccess

Cancel Previous **Next: Review**

Verify users detail

Click on **Create user** button

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

User details

User name	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	EC2admingroup

Cancel Previous Create user

Download 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: <https://523251683217.signin.aws.amazon.com/console>

Download .csv

User	Email login inst...
tom	Send email

Details Permissions Review Complete

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

Click on **close** button

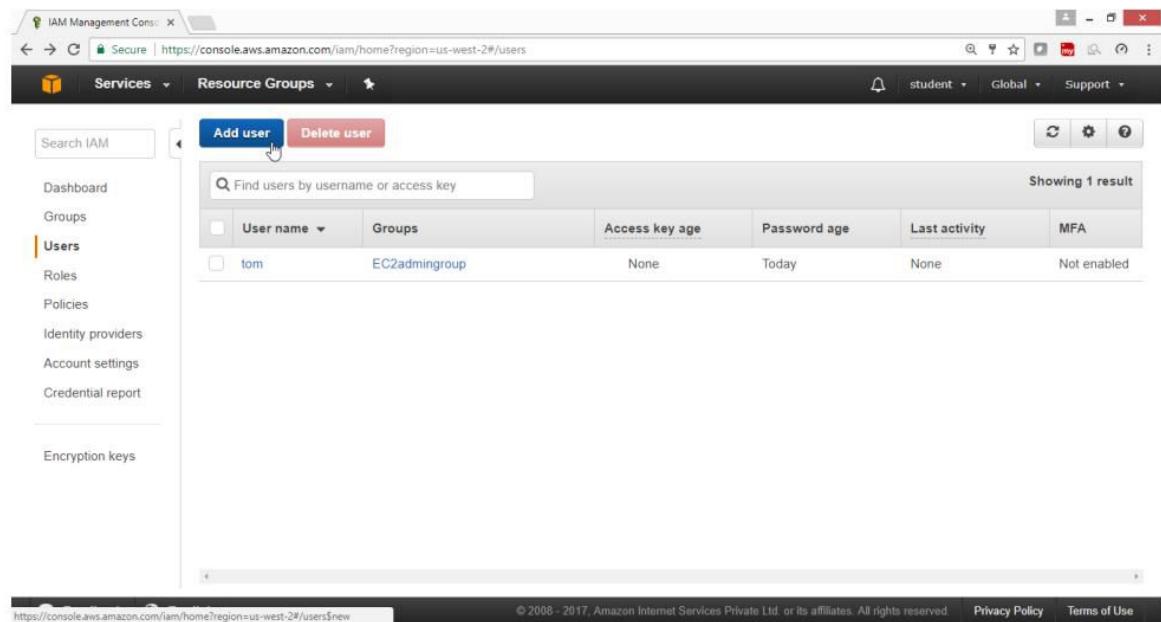
The screenshot shows the AWS IAM Management Console interface. At the top, there's a navigation bar with tabs like 'Services', 'Resource Groups', and 'Details', 'Permissions', 'Review', and 'Complete' buttons. A 'Success' message box is displayed, stating: 'You successfully created the users shown below. 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.' Below this, a table lists a single user named 'tom'. A 'Download .csv' button is available above the table. At the bottom right of the main content area, there's a 'Close' button with a hand cursor icon over it. The footer contains links for 'Feedback', 'English', 'Privacy Policy', and 'Terms of Use', along with copyright information: '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.'

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 is titled 'Services' and has 'Resource Groups' selected. Under 'Users', there is a list of users: 'tom' (EC2admingroup). At the top right, there are buttons for 'Add user' (highlighted with a mouse cursor) and 'Delete user'. Below the buttons is a search bar with placeholder text 'Find users by username or access key'. A table below the search bar shows the user 'tom' with details: Groups (EC2admingroup), Access key age (None), Password age (Today), Last activity (None), and MFA (Not enabled). The URL in the address bar is <https://console.aws.amazon.com/iam/home?region=us-west-2#users>.

- For user name → john
- For Access type → AWS Management Console access
- For console password → *****

Drag down

The screenshot shows the AWS IAM Management Console interface. A user named 'john' has been created. Under the 'Select AWS access type' section, the 'AWS Management Console access' checkbox is checked, while 'Programmatic access' is unchecked. The 'Console password' section shows a 'Custom password' has been set, indicated by a red asterisk. The 'Next Step' button is visible at the bottom.

Click on Next Permission button

The screenshot shows the 'Next: Permissions' step of the user creation process. The 'AWS Management Console access' checkbox is checked. At the bottom, the 'Next: Permissions' button is highlighted with a cursor, indicating it is the next step to click.

Select S3admingrp

Click on **Next Review** button

The screenshot shows the IAM Management Console with the URL [https://console.aws.amazon.com/iam/home?region=us-west-2#users\\$new?step=permissions&login&userNames=john&passwordType=manual](https://console.aws.amazon.com/iam/home?region=us-west-2#users$new?step=permissions&login&userNames=john&passwordType=manual). The 'Attached policies' section shows two entries: 'EC2admingroup' with 'AmazonEC2FullAccess' and 'S3admingrp' with 'AmazonS3FullAccess'. The 'S3admingrp' entry is selected. At the bottom, there are 'Cancel', 'Previous', and 'Next: Review' buttons, with 'Next: Review' being the active one.

Verify user details

Click on **Create user** button

The screenshot shows the IAM Management Console with the URL [https://console.aws.amazon.com/iam/home?region=us-west-2#users\\$new?step=review&login&userNames=john&passwordType=manual&groups=S...](https://console.aws.amazon.com/iam/home?region=us-west-2#users$new?step=review&login&userNames=john&passwordType=manual&groups=S...). It shows a 'User details' section with fields: User name (john), AWS access type (AWS Management Console access - with a password), Console password type (Custom), and Require password reset (No). Below is a 'Permissions summary' section showing the user will be added to the S3admingrp group. At the bottom, there are 'Cancel', 'Previous', and 'Create user' buttons, with 'Create user' being the active one.

Download .csv file

Click on **Close** button

The screenshot shows the AWS IAM Management Console with the URL [https://console.aws.amazon.com/iam/home?region=us-west-2#/users\\$new?step=final&login&userNames=john&passwordType=manual&groups=S3...](https://console.aws.amazon.com/iam/home?region=us-west-2#/users$new?step=final&login&userNames=john&passwordType=manual&groups=S3...). The page title is "Add user". A progress bar at the top indicates four steps: Details (1), Permissions (2), Review (3), and Complete (4). Step 4 is highlighted with a blue circle. A "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." Below the message, there is a "Download .csv" button with a CSV icon. A table lists a single user named "User" with the name "john" and a green checkmark icon. To the right of the table are two buttons: "Email login inst..." and "Send email". At the bottom right of the main content area is a "Close" button. The footer of the browser window includes links for "Feedback", "English", "Privacy Policy", and "Terms of Use".

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 Management Console interface. The left sidebar is titled 'Services' and has a 'Resource Groups' dropdown. The 'Users' option is selected and highlighted with an orange bar. Below the sidebar, there are links for 'Dashboard', 'Groups', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Credential report'. Under 'Encryption keys', it says '0 items'. The main content area has a header with 'Add user' and 'Delete user' buttons. A search bar says 'Find users by username or access key' and displays 'Showing 2 results'. A table lists two users: 'john' and 'tom'. The table columns are 'User name', 'Groups', 'Access key age', 'Password age', 'Last activity', and 'MFA'. Both users have 'None' listed under all columns except 'Groups'. The URL in the browser is https://console.aws.amazon.com/iam/home?region=us-west-2#users\$new.

User name	Groups	Access key age	Password age	Last activity	MFA
john	S3admingrp	None	Today	None	Not enabled
tom	EC2admingroup	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* **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

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

Click on Next permission button

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

 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](#) © 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Click on **Attach existing policies directly** box

The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-west-2#/users/new?step=permissions&login&userNames=sai&passwordType=manual>. The page title is "Add user". A progress bar at the top indicates step 2: Permissions. Below the progress bar, there are three options: "Add user to group", "Copy permissions from existing user", and "Attach existing policies directly". A callout box points to the third option, "Attach existing policies directly". A note below the options states: "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 of the screen, there are links for Feedback, English, Privacy Policy, and Terms of Use.

In Filter type search for ec2f

Select AmazonEC2FullAccess check box

The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-west-2#/users/sai/edit?step=permissions&login&userNames=sai&passwordType=manual&perm...>. The page title is "Edit user: sai". A callout box points to the "AmazonEC2FullAccess" policy in the list of results. The list shows two policies: "AmazonEC2FullAccess" (selected) and "AmazonEC2FullAcc..." (Customer managed). Both policies have a description: "Provides full access to Amazon EC2 via the AWS Man...". At the bottom of the screen, there are links for Feedback, English, Privacy Policy, and Terms of Use.

In Filter type search for s3f

Select AmazonS3FullAccess check box

Click on **Next Review** button

Screenshot of the AWS IAM Management Console showing the 'Permissions' step of user creation. The table lists policies:

Policy name	Type	Attachments	Description
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	1	Provides full access to all buckets via the AWS Management Console.
<input type="checkbox"/> AmazonS3FullAccess-20170...	Customer managed	0	Provides full access to all buckets via the AWS Management Console.

Buttons at the bottom: Cancel, Previous, **Next: Review**.

Verify users detail

Click on Create user button

Screenshot of the AWS IAM Management Console showing the 'Create user' step. It shows 'User details' and 'Permissions summary'.

User details

User name	sai
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No

Permissions summary

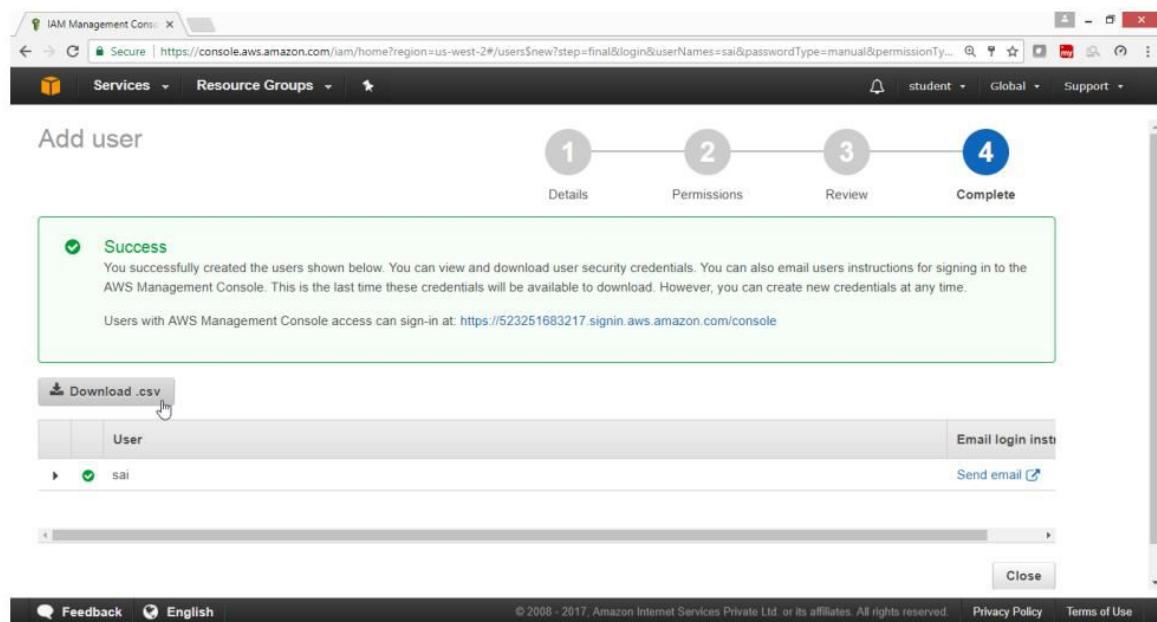
The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonEC2FullAccess
Managed policy	AmazonS3FullAccess

Buttons at the bottom: Cancel, Previous, **Create user**.

Download .csv file

Click on **Close** button



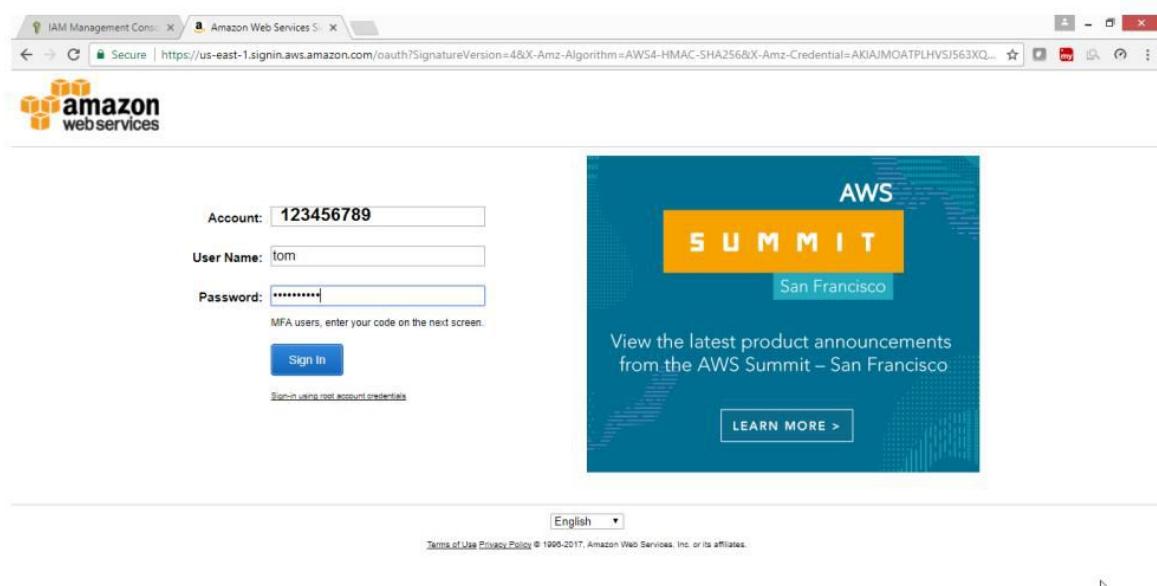
To verify whether users can access particular Service

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

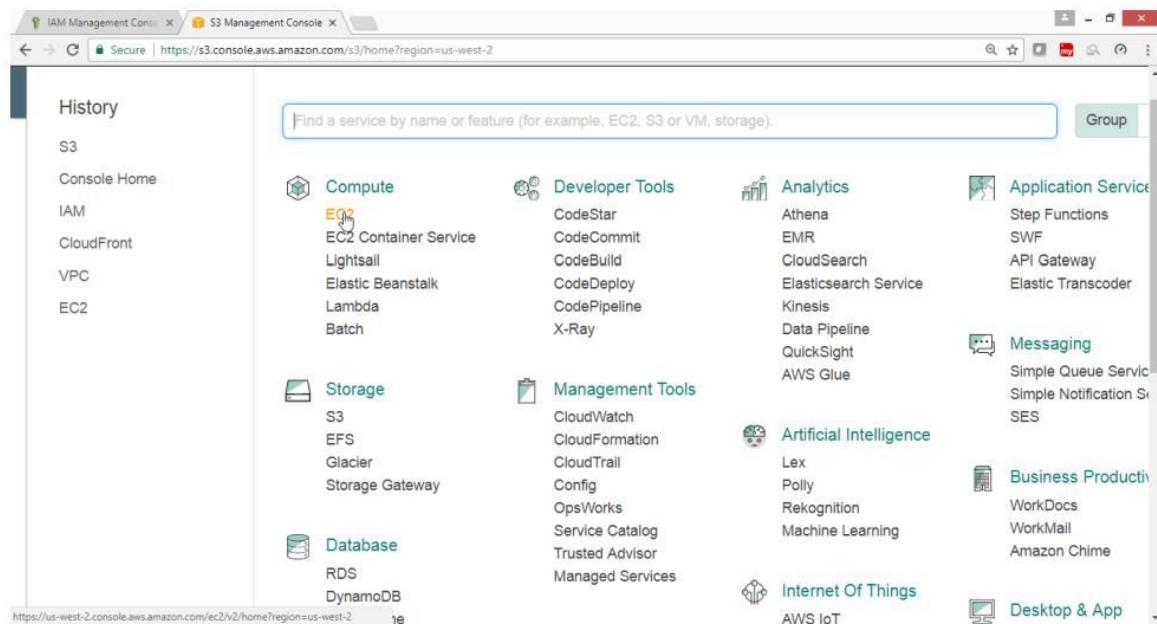
The screenshot shows the AWS Management Console homepage. The top navigation bar includes links for IAM Management Console, AWS Management Console, and AWS Support. The main menu bar has 'Services' and 'Resource Groups' dropdowns, along with account information for 'tom @ 123456789' and the 'Oregon' region. The 'Services' menu is expanded, displaying categories like History, Compute, Developer Tools, Analytics, Storage, Management Tools, and Artificial Intelligence. Under the Storage category, 'S3' is listed with a yellow cursor icon pointing to it. Other storage services like EFS and Glacier are also visible.

Verification

Error Access Denied

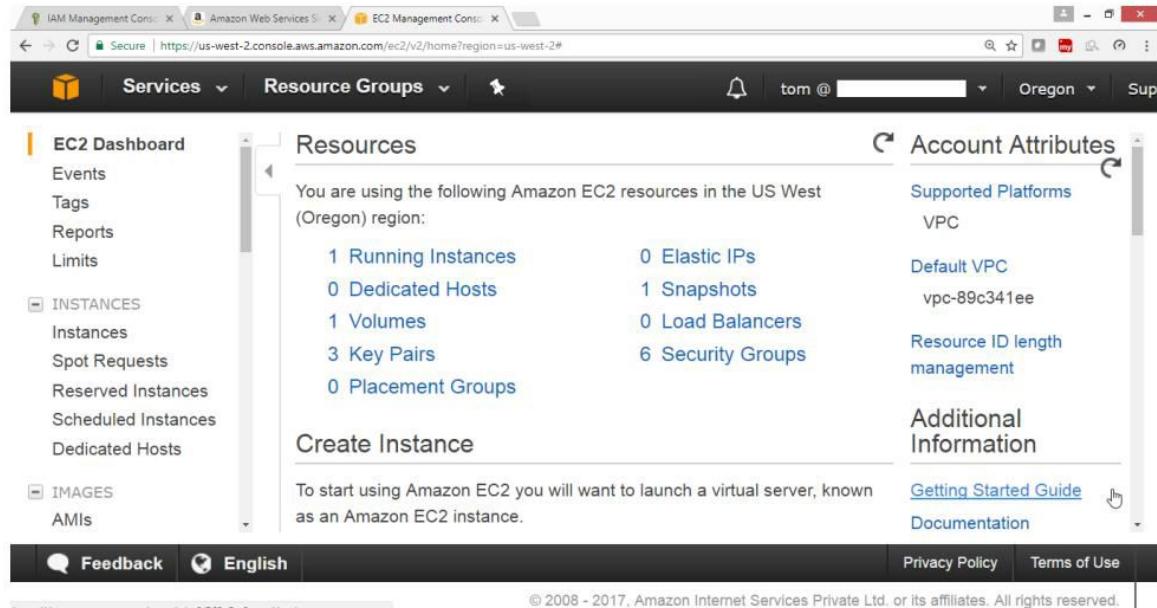
The screenshot shows the S3 Management Console homepage. The top navigation bar includes links for IAM Management Console, S3 Management Console, and AWS Support. The main content area features a banner about identifying optimal storage classes with S3 Analytics and a link to 'Storage Class Analysis'. Below the banner, there's a section for 'Amazon S3' with buttons for '+ Create bucket', 'Delete bucket', and 'Empty bucket'. A red error message box is prominently displayed, stating 'Error' and 'Access Denied'. Navigation links for 'Switch to the old console', 'Discover the new console', 'Quick tips', '- Buckets', and '- Regions' are also present.

Now select EC2 service



Verification

User tom can access EC2 service.



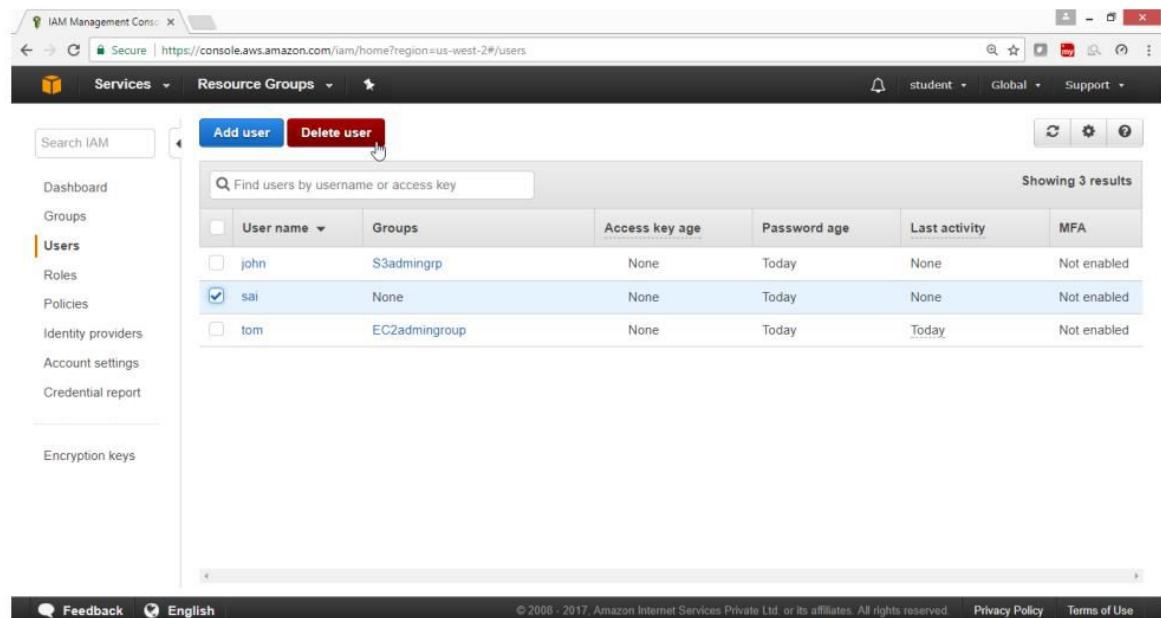
Similarly check for user john

To Delete users and groups

From IAM dashboard, select **Users**

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

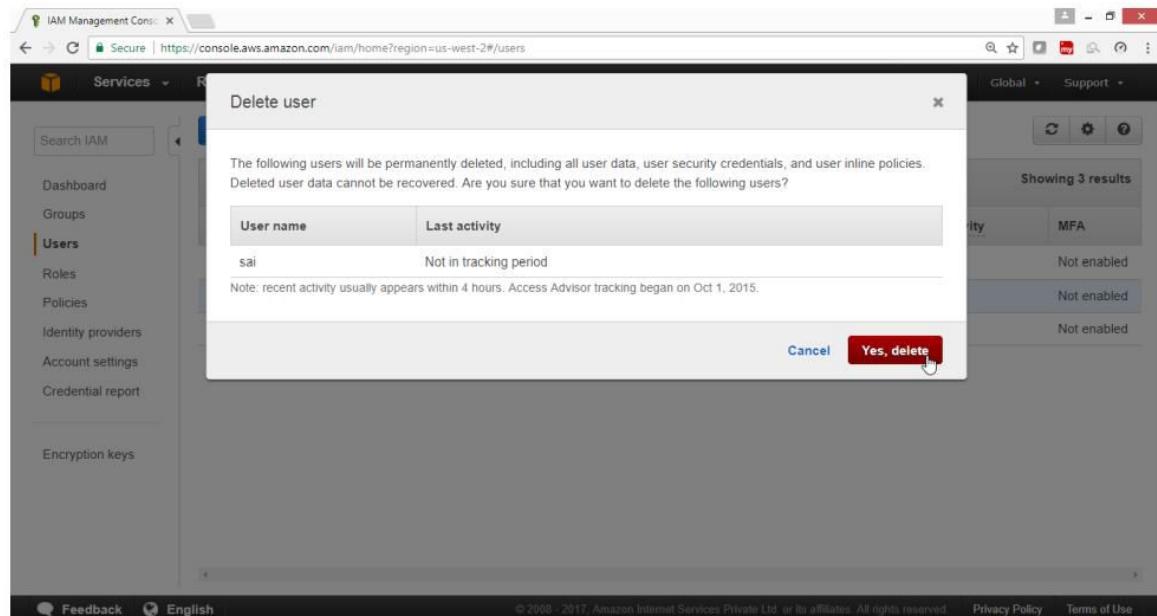
Click on **Delete Users** button



The screenshot shows the AWS IAM Management Console. The left sidebar is collapsed. The main area displays a table of users. The 'Delete user' button is highlighted with a red box and a cursor. The table has columns: User name, Groups, Access key age, Password age, Last activity, and MFA.

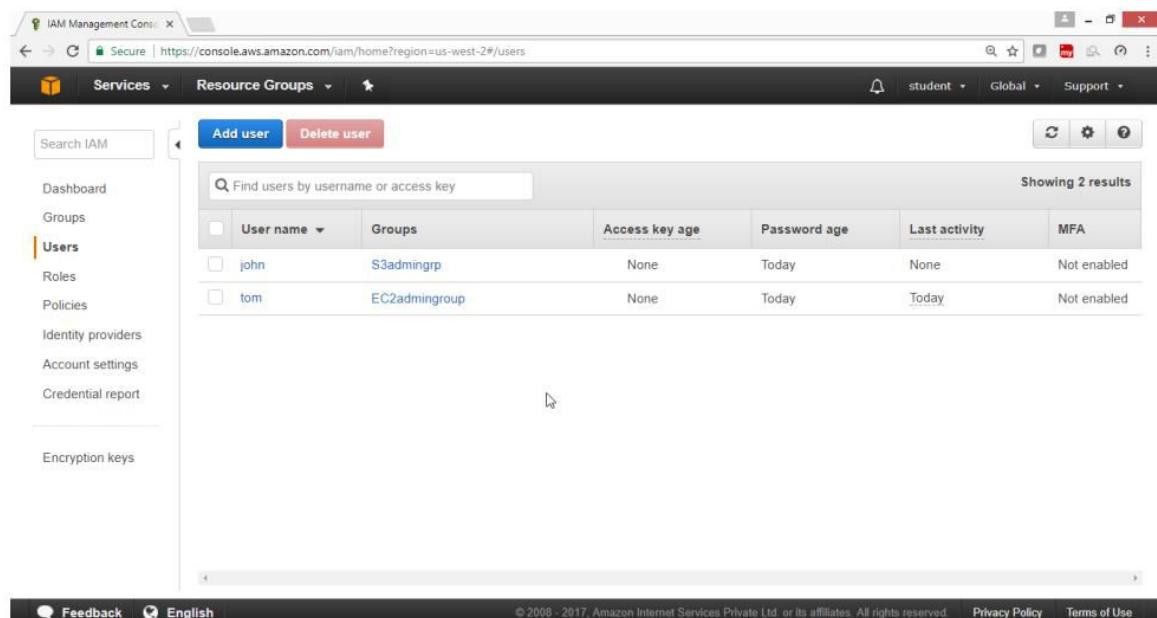
User name	Groups	Access key age	Password age	Last activity	MFA
john	S3admingrp	None	Today	None	Not enabled
sai	None	None	Today	None	Not enabled
tom	EC2admingroup	None	Today	Today	Not enabled

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 Management Console interface. On the left, there's a navigation sidebar with options like 'Dashboard', 'Groups' (which is selected and highlighted in orange), 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Credential report'. Below that is an 'Encryption keys' section. The main content area is titled 'Resource Groups' and shows a table with two results. The first row has a checkbox next to 'EC2admingroup'. The second row has a checked checkbox next to 'S3admingrp'. To the right of the table are columns for 'Inline Policy' and 'Creation Time'. At the top of the main area, there are buttons for 'Create New Group' and 'Group Actions'. A dropdown menu from 'Group Actions' is open, showing options: 'Add Users to Group', 'Delete Group' (which is highlighted with a cursor icon), 'Edit Group Name', and 'Remove Users from Group'. The status bar at the bottom includes links for 'Feedback', 'English', 'Privacy Policy', and 'Terms of Use'.

Click Yes, Delete button

The screenshot shows the AWS IAM Management Console with the 'Groups' section selected in the sidebar. A modal dialog box is centered over the main content area. The dialog has a title 'Delete Group' and a message asking if the user wants to delete the group 'S3admingrp'. At the bottom of the dialog are two buttons: 'Cancel' and 'Yes, Delete'. A mouse cursor is hovering over the 'Yes, Delete' button. The background shows a table listing groups, with one row for 'S3admingrp'.

Verification

Group is deleted

The screenshot shows the AWS IAM Management Console with the 'Groups' section selected in the sidebar. The main content area displays a table with one row, showing the group 'EC2admingroup'. The table includes columns for Group Name, Users, Inline Policy, and Creation Time. The 'Creation Time' column shows '2017-08-15 15:35 UTC+0530'. The 'Users' column shows the number '1'.

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 Management Console interface. The left sidebar is titled 'Services' and has several options: Dashboard, Groups, **Users**, Roles, Policies, Identity providers, Account settings, and Credential report. The 'Users' option is currently selected. The main content area is titled 'User list' and contains a table with two rows. The columns are 'User name', 'Groups', 'Access key age', and 'Password age'. The first row shows a user named 'john' associated with the group 'S3admingrp', with both access and password keys set to 'None' and created 'Today'. The second row shows a user named 'tom' associated with the group 'EC2admingroup', also with both keys set to 'None' and created 'Today'. A search bar at the top of the table says 'Find users by username or access key'. At the bottom of the page, there are links for 'Feedback', 'English', '© 2008 - 2017, Amazon Internet Services Private Ltd. 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

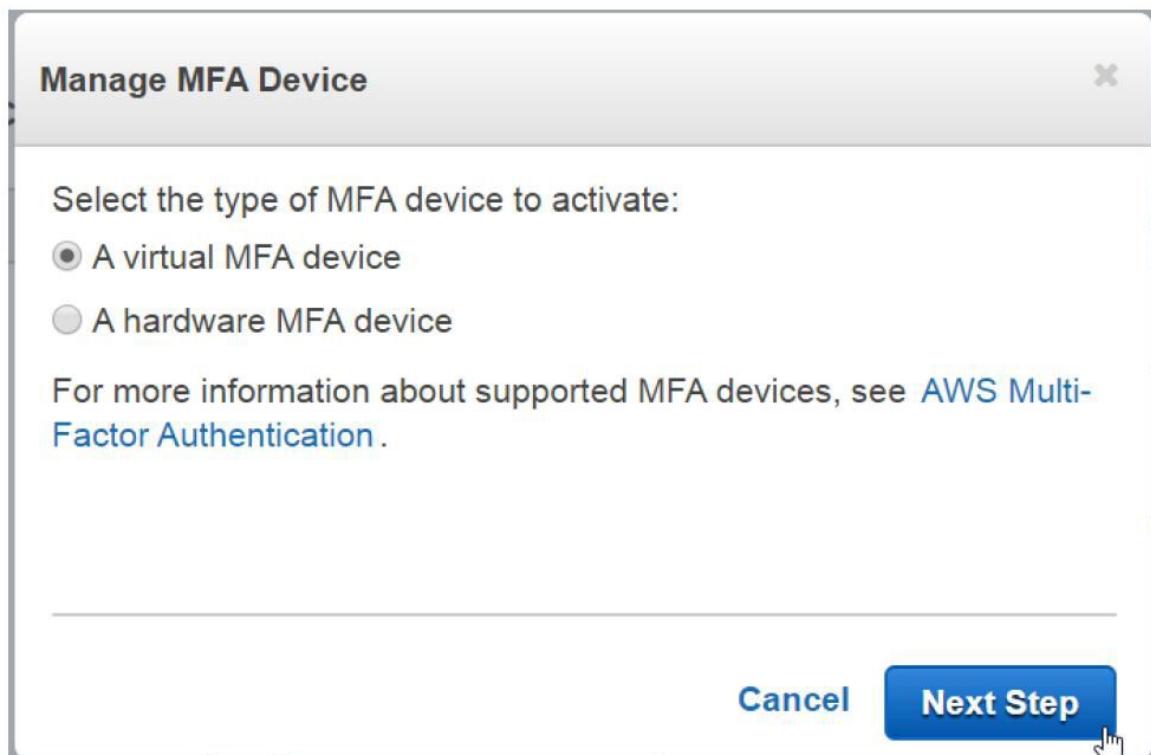
The screenshot shows the AWS IAM Management Console. The URL is <https://console.aws.amazon.com/iam/home?region=us-west-2#users/tom>. The left sidebar shows 'Users' is selected. The main area is titled 'Summary' for the user 'tom'. It displays the User ARN (arn:aws:iam:::user/tom), Path (/), and Creation time (2017-08-15 22:09 UTC+0530). Below this, there are tabs for 'Permissions', 'Groups (1)', 'Security credentials' (which is highlighted with a blue border), and 'Access Advisor'. Under 'Security credentials', there is a button 'Add permissions' and a message 'Attached policies: 1'. A table below shows policy details with columns 'Policy name' and 'Policy type'. At the bottom, there are links for 'Feedback', 'English', 'Privacy Policy', and copyright information.

Click on pen sign for “Assigned MFA device”

The screenshot shows the AWS IAM Management Console. The URL is https://console.aws.amazon.com/iam/home?region=us-west-2#users/tom?section=security_credentials. The left sidebar shows 'Users' is selected. The main area is titled 'Sign-in credentials' for the user 'tom'. It displays the 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 with a blue border), and 'Access Advisor'. Under 'Sign-in credentials', there are five items: 'Console password' (Enabled, Manage password), 'Console login link' (https://signin.aws.amazon.com/console), 'Last login' (2017-08-15 22:50 UTC+0530), 'Assigned MFA device' (No, edit icon), and 'Signing certificates' (None, edit icon). At the bottom, there are links for 'Feedback', 'English', 'Privacy Policy', and copyright information.

Select → “A virtual MFA device”

Click on **Next Step** button



Click on **Next Step** button



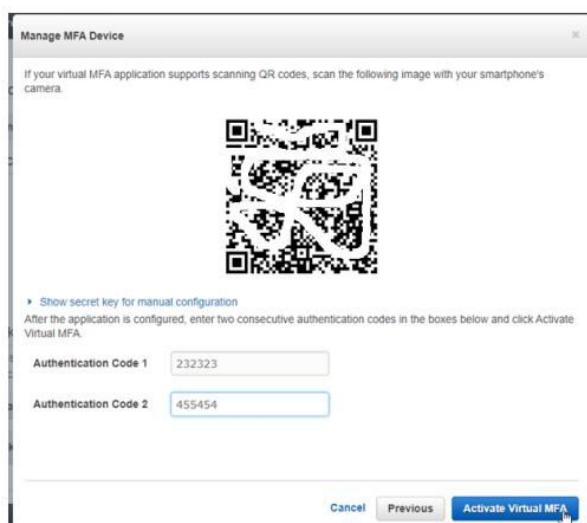
Bar code will be created

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

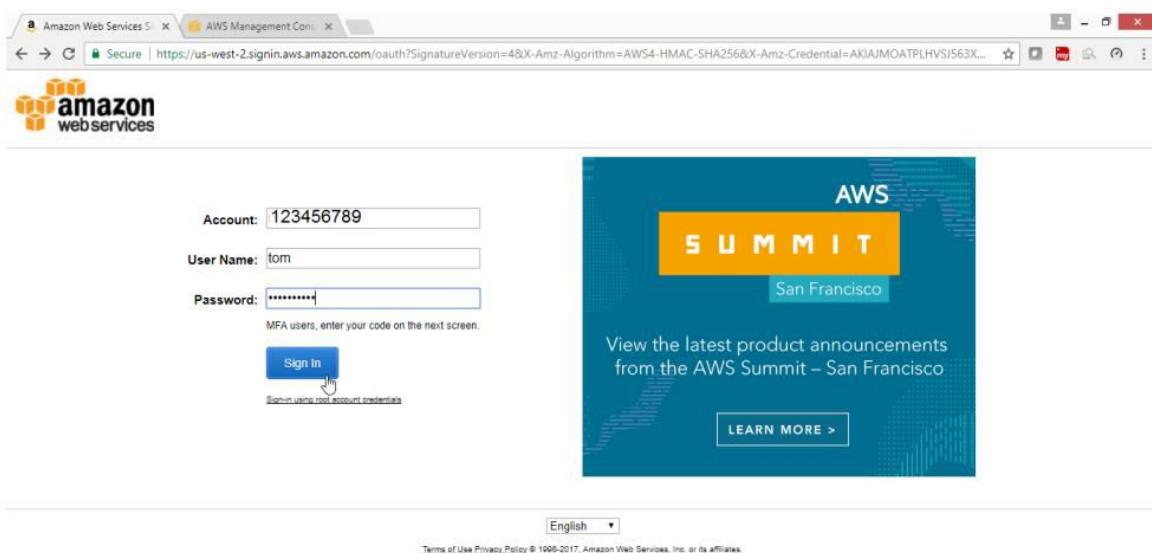
Retype 6 digit bar code in Authentication code 2



Click on Finish



Now login as tom user



<https://us-west-2.sigin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJMOATPLHVSJ563XQ&X-Amz-Date=2017-08-15T17%3A46%3A06.024Z&X-Amz-Signature=7c6497161e96feed27...>

Once the user types the MFA 6 digit code

Click on submit



MFA Code: 132432

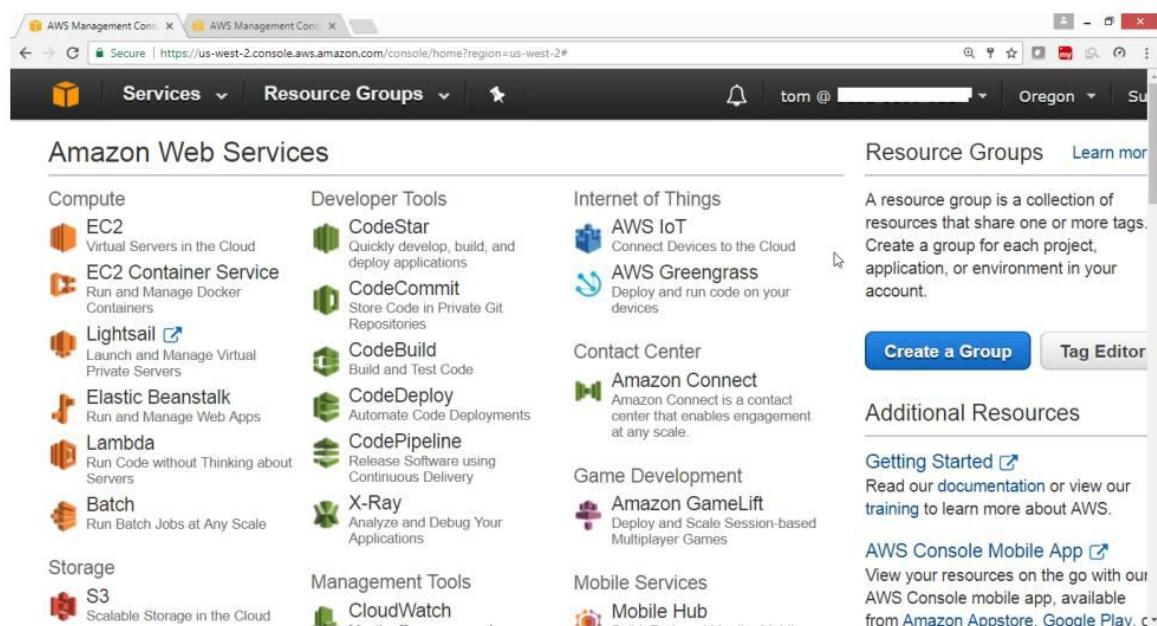
Submit Cancel

English ▾

Terms of Use Privacy Policy © 1996-2017, Amazon Web Services, Inc. or its affiliates.

<https://us-west-2.signin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJMOATPLHVSJ563XQ&X-Amz-Date=2017-08-15T17%3A46%3A06.024Z&X-Amz-Signature=7c6497161e96feed27...>

Verify user had successfully logged in.

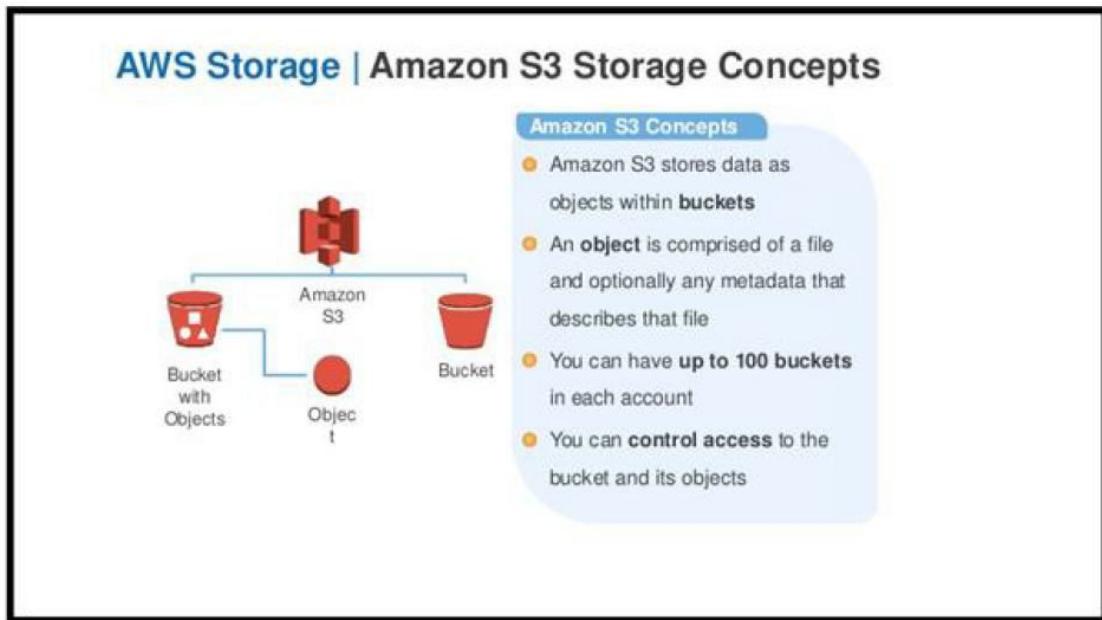


Lab 7: To Configure Amazon Simple Storage Service (Amazon S3)

OBJECTIVE

To configure and use AWS S3 service

TOPOLOGY



PRE-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

The screenshot shows the AWS Management Console Services page. The 'Storage' category is highlighted in blue. Under 'Compute', 'Developer Tools', 'Analytics', 'Application Services', 'Messaging', 'Artificial Intelligence', and 'Business Productivity' are listed. Under 'Storage', 'Database', and 'Management Tools' are listed. Under 'Database', 'S3' is also listed. The URL in the address bar is <https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2>.

On Amazon S3 page

Click on Create Bucket

The screenshot shows the Amazon S3 Management Console. The 'Create bucket' button is highlighted with a mouse cursor. The page displays four buckets in the list: 'alit3june', 'elasticbeanstalk-us-west-2-523251683217', 'srikanthyd', and 'www.cfameerpet.com'. The 'Region' column shows they are located in US West (Oregon) except for 'www.cfameerpet.com' which is in Asia Pacific (Singapore). The 'Date created' column shows the creation dates for each bucket. The URL in the address bar is <https://console.aws.amazon.com/s3/home?region=us-west-2#switchingBackToOldConsole=true>.

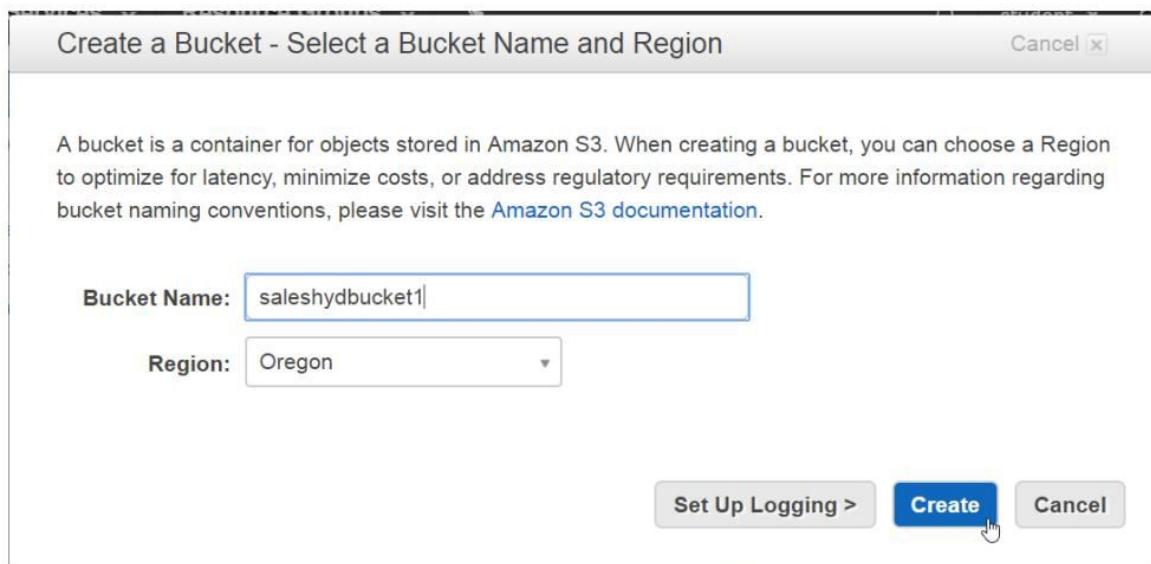
On “Create Bucket - Select a Bucket Name and Region” box

Provide following values

Bucket Name → saleshydbucket

Region → Oregon

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



Verify that bucket is created.

The screenshot shows the AWS S3 Management Console. The left sidebar lists buckets: 'cloudtrialhari', 'ctrialabc', 'saleshydbucket1' (which is selected and highlighted in blue), and 'srikanthhyd'. The right panel displays details for the selected bucket: 'Bucket: saleshydbucket1', 'Region: Oregon', 'Creation Date: Tue Aug 15 08:00:06 GMT+530 2017', and 'Owner: skmvali999'. Below these details are links for 'Permissions', 'Static Website Hosting', 'Logging', 'Events', and 'Versioning'.

To upload files of any type

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

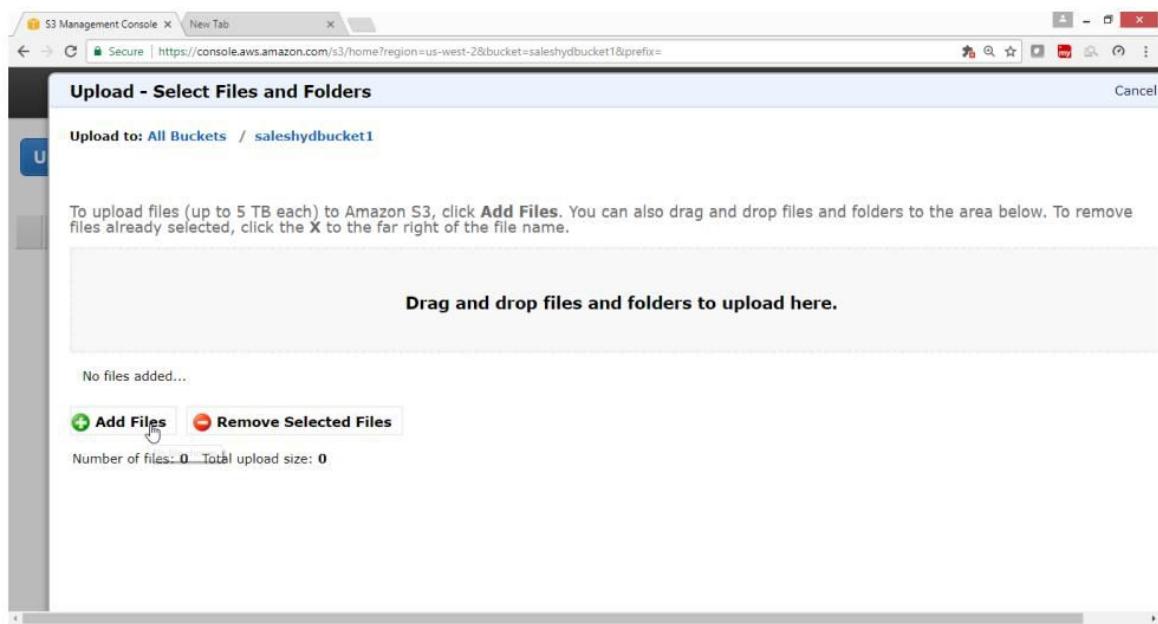
Note: 5 GB can be uploaded

It will be charged if crossed free tier usage.

Click on Created bucket

The screenshot shows the AWS S3 Management Console interface. On the left, a sidebar lists four buckets: 'cloudtrialhari', 'ctrialabc', 'saleshydbucket1' (which is highlighted with a yellow selection bar), and 'srikanthhyd'. On the right, the details for the selected bucket, 'saleshydbucket1', are displayed. The bucket's name is shown at the top, followed by its metadata: Bucket: saleshydbucket1, Region: Oregon, Creation Date: Tue Aug 15 08:00:06 GMT+530 2017, and Owner: skmvali999. Below this, there is a vertical navigation menu with links for Permissions, Static Website Hosting, Logging, Events, and Versioning.

Click on **Add files**

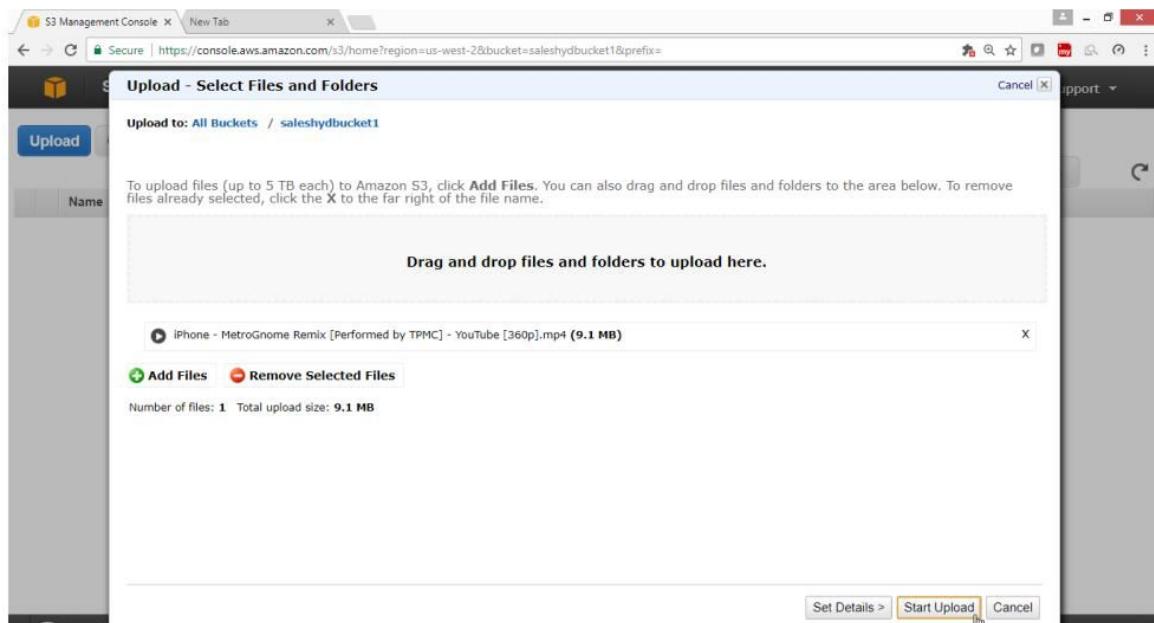


In the upload Wizard

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. At the top, there's a navigation bar with tabs for 'Services' (selected), 'Resource Groups', and 'Actions'. Below the navigation bar is a search bar labeled 'Search by prefix' and a link 'Switch to new console'. To the right of the search bar are buttons for 'None', 'Properties', and 'Transfers'. A checkbox 'Automatically clear finished transfers' is checked. The main area displays a table with one row of data:

Name	Storage Class	Size	Last Modified
iPhone - MetroGnome Remix [Performed by TPMC] - YouTube [360p].mp4	Standard	9.1 MB	Tue Aug

Select the file, Click on Properties on Right Panel,

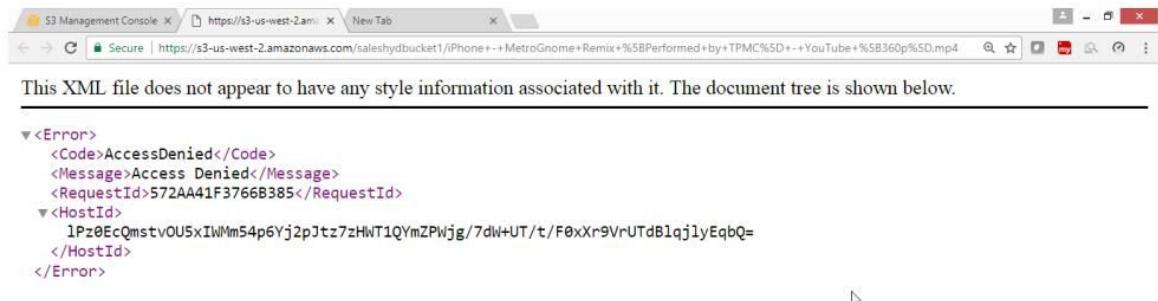
Click on the link

The screenshot shows the AWS S3 Management Console interface, similar to the previous one, but with a different focus. On the right side, there's a detailed view of the selected file: 'iPhone - MetroGnome Remix [Performed by TPMC] - YouTube [360p].mp4'. This view includes the following details:

Bucket: saleshydbucket1
Name: iPhone - MetroGnome Remix [Performed by TPMC] - YouTube [360p].mp4
Link: <https://s3-us-west-2.amazonaws.com/saleshydbucket1/iPhone+-+MetroGnome+Remix+%5BPerformed+by+TPMC%5D+-+YouTube+%5B360p%5D.mp4>
Size: 9630788
Last Modified: Tue Aug 15 08:04:56 GMT+530 2017
Owner: skmvalif99
ETag: 6d036eb69784224115be1291c92017a9
Expiry Date: None
Expiration Rule: N/A

Below these details, there are links to 'Details', 'Permissions', 'Metadata', and 'Tags'.

Verification : Cannot access due to lack of permission

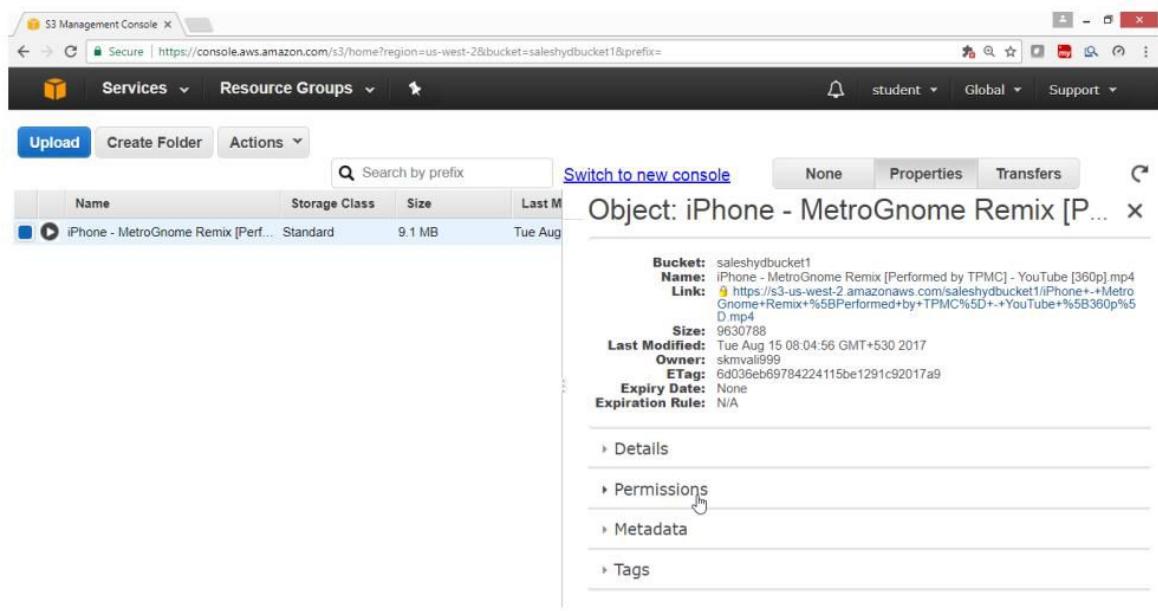


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Error>
    <Code>AccessDenied</Code>
    <Message>Access Denied</Message>
    <RequestId>572AA41F3766B385</RequestId>
    <HostId>
        1Pz0EcQmstvOU5xIWMM54p6Yj2pJtz7zHWT1QYmZPWjg/7dW+UT/t/F0xxXr9VrUTdB1qjlyEqbQ=
    </HostId>
</Error>
```

To allow users to Download, or view give permission

Select, **Permission** tag



Object: iPhone - MetroGnome Remix [P...

Name	Storage Class	Size	Last Modified
iPhone - MetroGnome Remix [Perf...	Standard	9.1 MB	Tue Aug

Bucket: saleshydbucket1
Name: iPhone - MetroGnome Remix [Performed by TPMC] - YouTube [360p].mp4
Link: <https://s3-us-west-2.amazonaws.com/saleshydbucket1/iPhone+-+MetroGnome+Remix+%5BPerformed+by+TPMC%5D+-+YouTube+%5B360p%5D.mp4>
Size: 9630788
Last Modified: Tue Aug 15 08:04:56 GMT+530 2017
Owner: skrnval999
ETag: 6d036eb69784224115be1291c92017a9
Expiry Date: None
Expiration Rule: N/A

▶ 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

The screenshot shows the AWS S3 Management Console interface. In the top navigation bar, 'Services' is selected. The main area displays a table with one item: 'iPhone - MetroGnome Remix [Perf... Standard'. Below the table, the 'Permissions' section is expanded, showing two grantee entries. The first entry has 'Grantee: skmvali999' and checked boxes for 'Open/Download', 'View Permissions', and 'Edit Permissions'. The second entry has 'Grantee: Everyone' and checked boxes for 'Open/Download', 'View Permissions', and 'Edit Permissions'. A link 'Edit Permissions' is visible next to the second entry. At the bottom of the 'Permissions' section is a button labeled 'Add more permissions'. At the very bottom of the page are 'Save' and 'Cancel' buttons.

Verify file is accessible.

The screenshot shows the AWS S3 Management Console. A video thumbnail is displayed, showing a person's hand interacting with a black electronic music controller (likely a Novation Launchpad). Below the thumbnail, the file URL is visible: <https://s3-us-west-2.amazonaws.com/saleshydbucket1/iPhone---MetroGnome+Remix+%5BPerformed+by+TPMC%5D+-+YouTube+-+58360p%5D.mp4>. To the right of the thumbnail, there is a preview pane showing the video frame and some text: "TPMC - YouTube [360p] mp4 saleshydbucket1/iPhone---MetroGnome+Remix+%5BPerformed+by+TPMC%5D+-+YouTube+-+58360p%5D.mp4". Below the thumbnail, there are tabs for "Metadata" and "Tags".

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

Select the file from Bucket or Folder, right click,

now select copy/cut

The screenshot shows the AWS S3 Management Console with a file listed in the table: "iPhone - MetroGnome Remix [Performed by TPMC]". A context menu is open over this file, with the "Copy" option highlighted. The menu options include: Open, Download, Make Public, Rename, Delete, Initiate Restore, Cut, and Copy. The "Copy" option is highlighted with a yellow background and a cursor icon.

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 interface. At the top, there's a navigation bar with 'Services' and 'Resource Groups'. On the right, there's a user profile 'student'. Below the navigation bar, there are tabs for 'Create Bucket', 'Actions', 'Switch to new console', 'None', and 'Properties'. A link 'All Buckets (5)' is visible. A table lists five buckets: 'cloudtrialhari', 'ctrialabc', 'finshydbucket1' (which is highlighted in blue), 'saleshydbucket1', and 'srikanthhyd'. Each bucket entry includes a small icon and a delete button.

Click on Paste

The screenshot shows the AWS S3 Management Console interface, similar to the previous one, but with a different URL in the address bar: `https://console.aws.amazon.com/s3/home?region=us-west-2&bucket=finshydbucket1&prefix=`. The bucket 'finshydbucket1' is selected. The interface shows a message 'The bucket 'finshydbucket1' is empty'. A context menu is open over the empty bucket area, with the 'Paste' option highlighted in orange. Other options in the menu include 'Create Folder...', 'Upload', and 'Paste'.

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

The screenshot shows the AWS S3 Management Console interface. The URL is https://console.aws.amazon.com/s3/home?region=us-west-2&bucket=finshydbucket1&prefix=. The page displays a table of objects in the 'finshydbucket1' bucket. One object is visible:

Name	Storage Class	Size	Last Modified
iPhone - MetroGnome Remix [Performed by TP...	Standard	9.1 MB	Tue Aug 15 08:23:54 GMT+530 2017

Below the table, there is a 'Transfers' section with a checkbox for 'Automatically clear finished transfers'. At the bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use.

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

Right click on it, select Delete

The screenshot shows the AWS S3 Management Console interface. The URL is https://console.aws.amazon.com/s3/home?region=us-west-2&bucket=finshydbucket1&prefix=. A context menu is open over a file named 'iPhone - MetroGnome Remix [Performed by TP...'. The menu options are: Open, Download, Make Public, Rename, Delete, Initiate Restore, Cut, Copy, and Properties. The 'Delete' option is highlighted with a mouse cursor.

To Delete a bucket

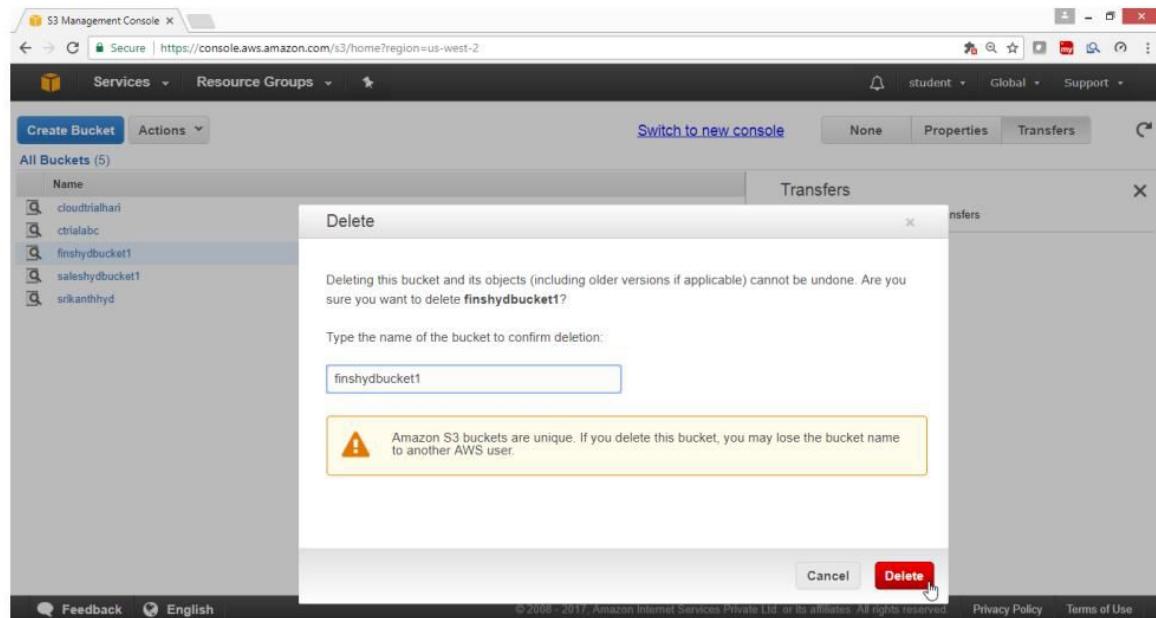
Select the bucket, right click select **Delete Bucket**

The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with 'Services' and 'Resource Groups'. Below it, a toolbar has 'Create Bucket' (highlighted in blue), 'Actions' (with a dropdown arrow), 'Switch to new console', 'None', and 'Properties' buttons. The main area is titled 'All Buckets (5)' and lists five buckets: 'cloudtrialhari', 'ctrialabc', 'finshydbucket1' (which is selected and highlighted in blue), 'saleshydbucket1', and 'srikanthhyd'. A context menu is open over the 'finshydbucket1' row, showing options: 'Create Bucket...', 'Delete Bucket' (which is highlighted in orange), 'Empty Bucket', 'Paste Into', and 'Properties'. To the right of the bucket list, there's a sidebar titled 'Transfers' with a checkbox for 'Automatically clear fin'.

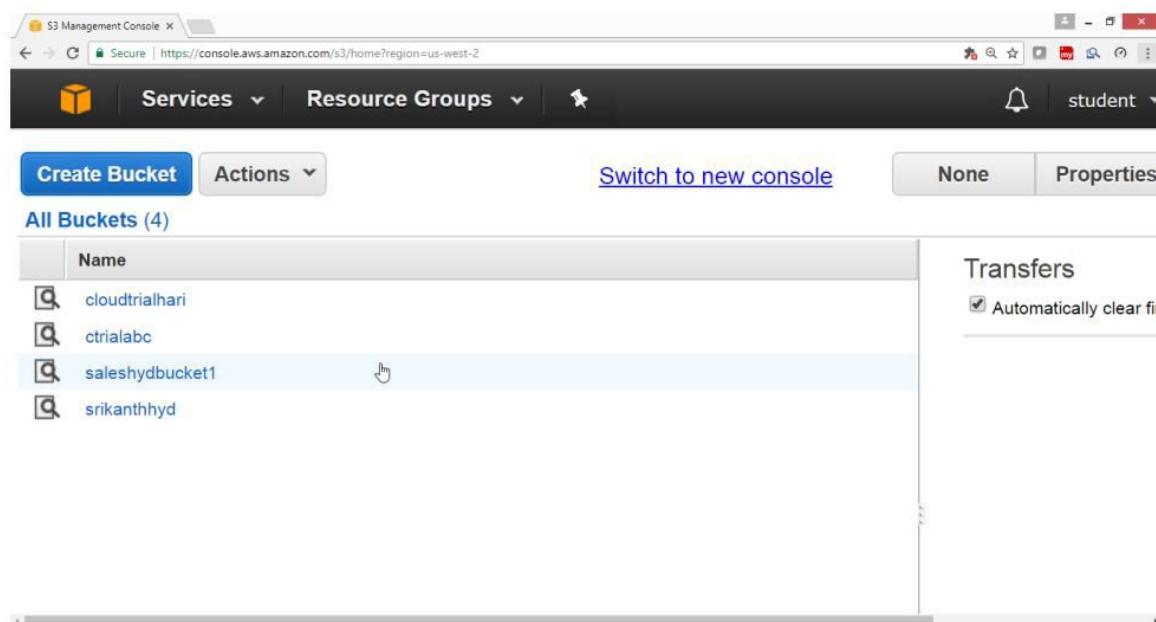
To Delete Bucket

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 S3 Management Console interface. At the top, there's a navigation bar with links for 'Services' and 'Resource Groups'. On the right side of the top bar, there are icons for notifications and user profile, and the text 'student'. Below the navigation bar, there are three buttons: 'Create Bucket' (highlighted with a mouse cursor), 'Actions', and 'Switch to new console'. To the right of these buttons are 'None' and 'Properties' buttons. The main area displays a table titled 'All Buckets (4)'. The table has two columns: 'Name' and 'Transfers'. The 'Name' column lists four buckets: 'cloudtrialhari', 'ctrialabc', 'saleshydbucket1', and 'srikanthhyd'. The 'Transfers' column contains a checkbox labeled 'Automatically clear fin' which is checked. A vertical scroll bar is visible on the right side of the table.

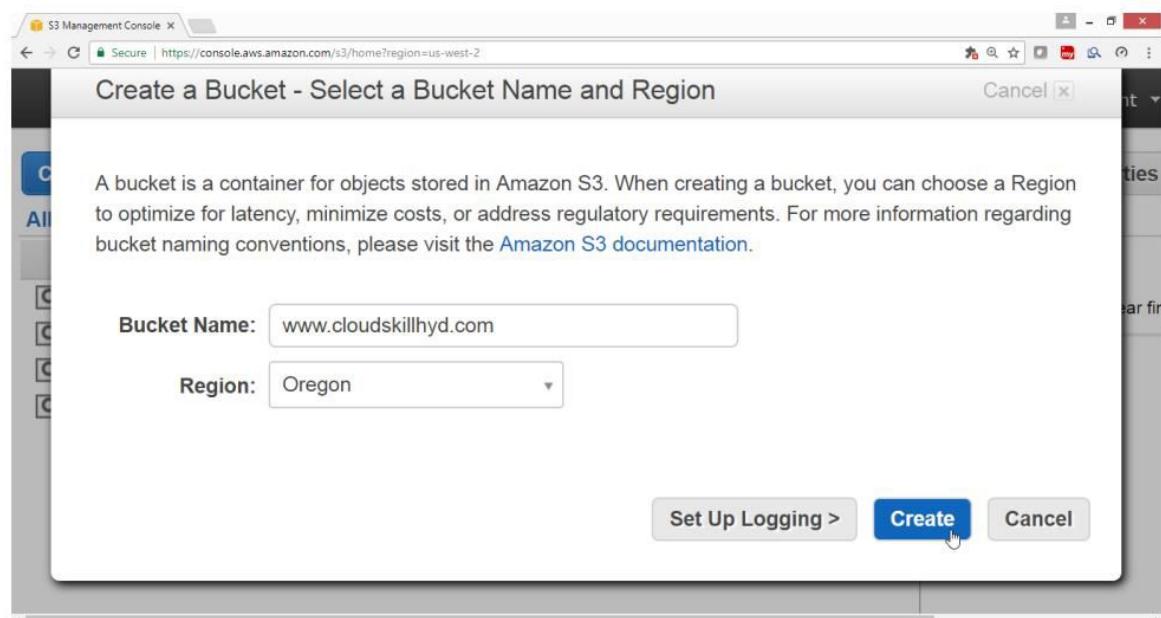
Name	Transfers
cloudtrialhari	<input checked="" type="checkbox"/> Automatically clear fin
ctrialabc	
saleshydbucket1	
srikanthhyd	

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 interface. At the top, there's a navigation bar with 'Services' and 'Resource Groups'. Below it, a toolbar has 'Create Bucket' (highlighted in blue), 'Actions', and 'Switch to new console'. On the right, there are buttons for 'None' and 'Properties'. A dropdown menu shows 'student' and other options. The main area is titled 'All Buckets (4)' and lists five buckets: 'cloudtrialhari', 'ctrialabc', 'saleshydbucket1', 'srikanthhyd', and 'www.cloudskillhyd.com'. The last bucket is currently selected, indicated by a blue background. To the right of the bucket list is a 'Transfers' sidebar with a checkbox for 'Automatically clear finished transfers'.

Upload all website contents in this bucket.

The screenshot shows the AWS S3 Management Console interface for the 'www.cloudskillhyd.com' bucket. At the top, there's a navigation bar with 'Services' and 'Resource Groups'. Below it, a toolbar has 'Upload' (highlighted in blue), 'Create Folder', 'Actions', and 'Switch to new console'. On the right, there are buttons for 'None', 'Properties', and 'Transfers'. A dropdown menu shows 'student' and other options. The main area lists the contents of the bucket, including files like '404.html', 'about-us.html', 'article.html', 'articles.html', 'contact-us.html', 'css', 'images', 'index.html', 'js', and 'sitemap.html'. Each item shows its name, storage class (Standard), size, and last modified date. To the right of the file list is a 'Transfers' sidebar with a checkbox for 'Automatically clear finished transfers'.

Select the bucket and click on properties button

The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with 'Services' and 'Resource Groups'. Below it, a toolbar has buttons for 'Create Bucket', 'Actions', 'Switch to new console', and tabs for 'None', 'Properties' (which is highlighted in blue), and 'Transfers'. A sidebar on the left lists 'All Buckets (4)' with names: 'cloudtrialhari', 'ctrialabc', 'saleshydbucket1', and 'www.cloudskillhyd.com'. The main content area on the right is titled 'Transfers' with a checkbox for 'Automatically clear finished transfers'.

On the **Properties** panel

Click **Static Website Hosting**

Drag Down

This screenshot shows the same S3 Management Console interface, but the 'Static Website Hosting' section under the selected bucket 'www.cloudskillhyd.com' is now expanded. It displays details like the bucket name, region (Oregon), creation date (Tue Aug 15 08:44:43 GMT+530 2017), and owner (skmval999). The 'Static Website Hosting' section is expanded, showing a description of how to host a static website and providing the endpoint 'www.cloudskillhyd.com.s3-website-us-west-2.amazonaws.com'. There's also a note about redirecting requests to another host name.

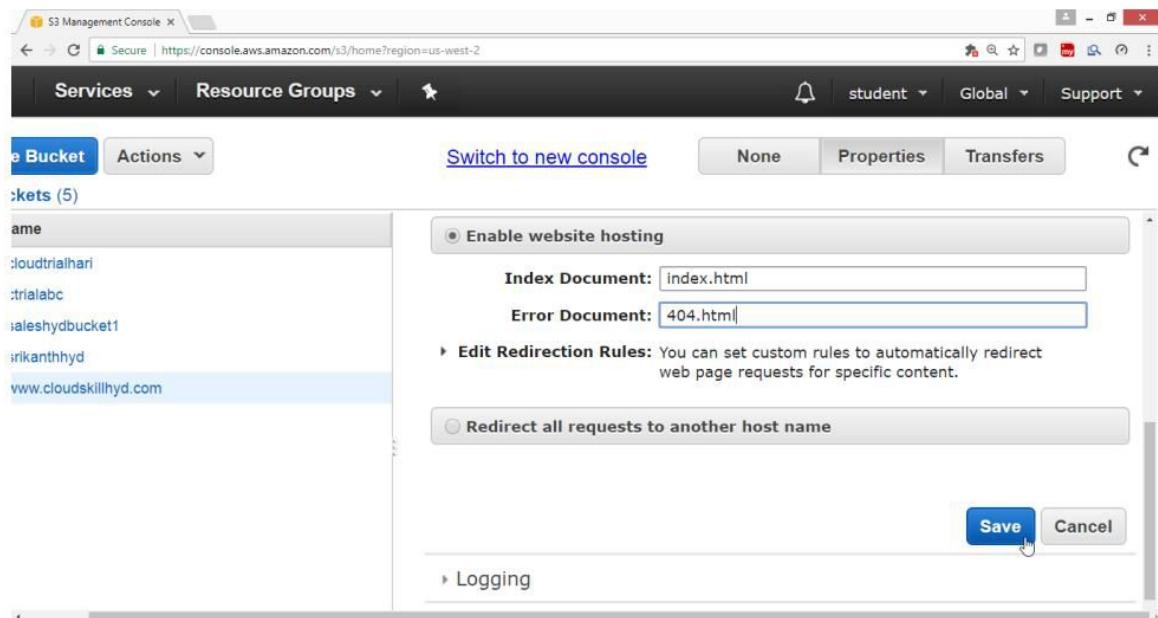
Select the **Enable website hosting**

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 'Create Bucket' button and 'Actions' dropdown menu. In the main area, there's a list of buckets: 'cloudtrialhari', 'ctrilabc', 'saleshydbucket1', 'srikanthhyd', and 'www.cloudskillhyd.com'. The 'www.cloudskillhyd.com' bucket is selected. On the right, the 'Properties' tab is active, showing the 'Endpoint' as www.cloudskillhyd.com.s3-website-us-west-2.amazonaws.com. A note explains that each bucket serves a website namespace and can be used for static website hosting. Below this, there are three options: 'Do not enable website hosting' (radio button is unselected), 'Enable website hosting' (radio button is selected), and 'Redirect all requests to another host name'. Under 'Enable website hosting', fields for 'Index Document' (set to 'index.html') and 'Error Document' (set to '404.html') are shown. A link to 'Edit Redirection Rules' is also present. At the bottom right are 'Save' and 'Cancel' buttons, and a 'Logging' section is visible at the very bottom.

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 interface. On the left, a sidebar lists buckets: cloudtrialhari, ctrialabc, saleshydbucket1, srikanthyd, and www.cloudskillhyd.com. The www.cloudskillhyd.com bucket is selected. The main panel displays the bucket properties for 'Bucket: www.cloudskillhyd.com'. It shows the bucket name, region (Oregon), creation date (Tue Aug 15 08:44:43 GMT+530 2017), and owner (skmvali999). Below this, the 'Permissions' section is expanded, showing a grantee 'Grantee: skmvali999' with checked permissions for 'List', 'Upload/Delete', and 'Edit Permissions'. There are also links to 'View Permissions' and 'Edit Permissions'. At the bottom of the permissions section are three buttons: 'Add more permissions', 'Add bucket policy' (which is highlighted in blue), and 'Add CORS Configuration'. At the very bottom of the page are 'Save' and 'Cancel' buttons.

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.cloudskillhyd.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.cloudskillhyd.com' bucket is selected. On the right, under 'Static Website Hosting', the endpoint is listed as www.cloudskillhyd.com.s3-website-us-west-2.amazonaws.com. The 'Enable website hosting' option is selected, with 'index.html' set as the index document and '404.html' as the error document.

Verify the website which is coming from S3 Bucket

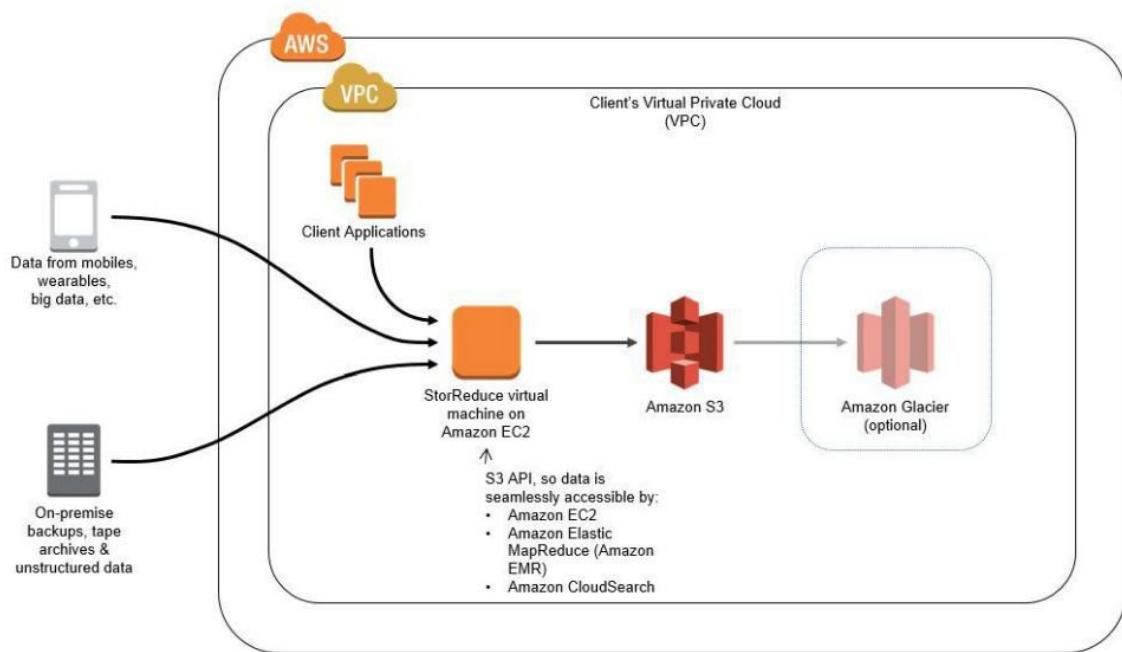
The screenshot shows the 'Car Club' website. The header features a purple navigation bar with links for HOME, ABOUT, ARTICLES, CONTACTS, and SITE MAP. Below the header is a large image of a purple sports car. The main content area includes a 'Latest News' section with two items: one from 10.08.2010 and another from 03.08.2010. To the right is a 'Welcome to Our Club' section with a brief description and a sidebar containing three bulleted items. At the bottom, there is a note about the website template being delivered in two packages.

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 allow 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. The left sidebar lists five buckets: 'cloudtrialhari', 'ctrialabc', 'saleshydbucket1', 'srikanthhyd', and 'www.cloudskillhyd.com'. The right panel displays details for the 'www.cloudskillhyd.com' bucket, which was created on Tue Aug 15 08:44:43 GMT+530 2017 by skmvali999. A sidebar on the right lists navigation options: 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 interface. On the left, there's a sidebar with 'Services' and 'Resource Groups'. The main area shows a list of buckets: 'cloudtrialhari', 'ctrialabc', 'saleshydbucket1', 'srikanthhyd', and 'www.cloudskillhyd.com'. A modal window titled 'Add rule' is open over the list. The modal contains a sub-section titled 'Versioning is not currently enabled on this bucket.' with a note about lifecycle rules managing versions. At the bottom of the modal, there are 'Save' and 'Cancel' buttons. To the right of the modal, there's a vertical sidebar with links: 'Cross-Region Replication', 'Tags', 'Requester Pays', 'Transfer Acceleration', and 'Storage Management'.

Under Lifecycle Rules

select Choose Rule Target

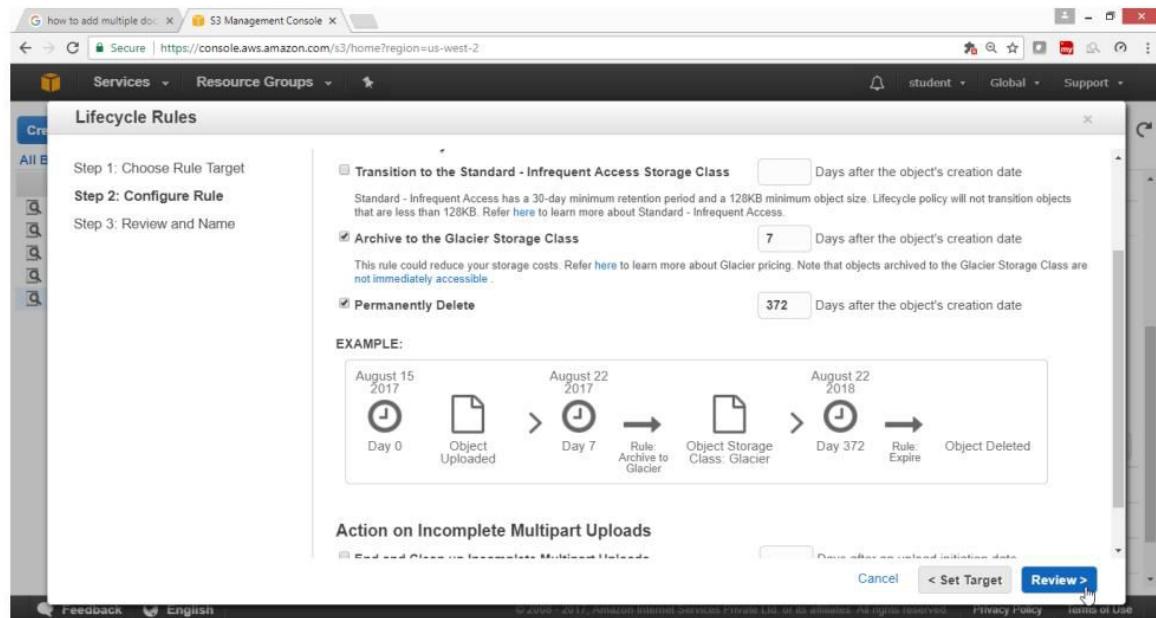
Apply the Rule to → Whole Bucket

The screenshot shows the 'Lifecycle Rules' configuration screen. On the left, there's a sidebar with 'Step 1: Choose Rule Target', 'Step 2: Configure Rule', and 'Step 3: Review and Name'. The main area has a title 'Apply the Rule to:' followed by two radio buttons: one selected for 'Whole Bucket: www.cloudskillhyd.com' and another for 'A Prefix e.g. MyFolder/ or MyFolder/MyObject'. At the bottom right of the modal, there are 'Cancel' and 'Configure Rule >' buttons, with the latter being highlighted.

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

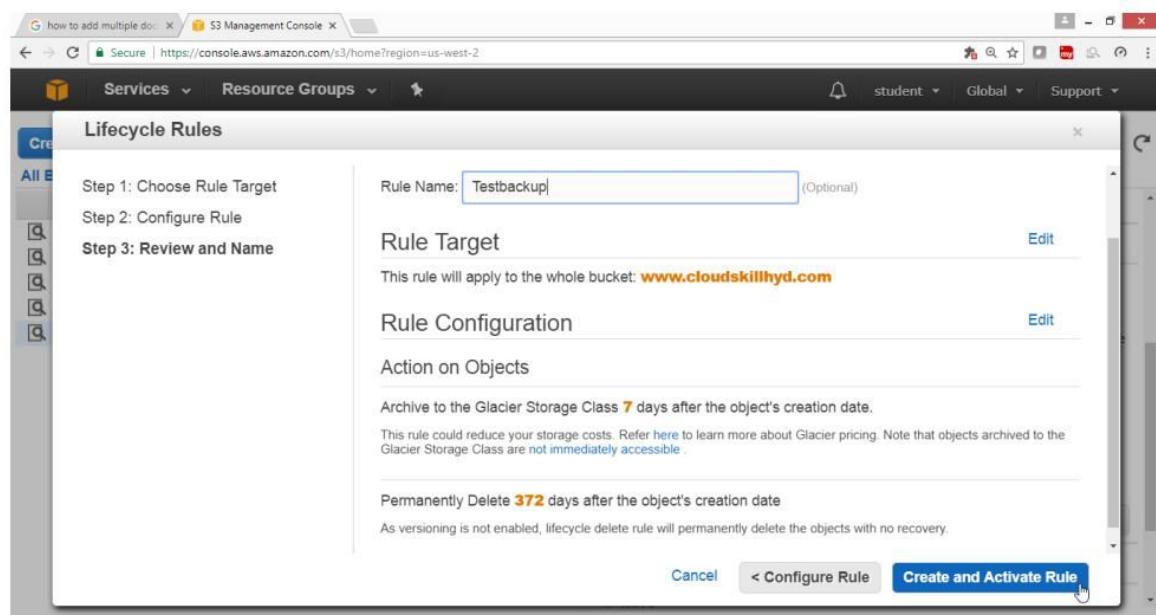
Select the check box **Permanently Delete** → 372

click on **Review**



Provide Rule Name → Testbackup

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



Click on Save button

The screenshot shows the AWS S3 Management Console. In the left sidebar, under 'All Buckets (5)', the bucket 'www.cloudskillhyd.com' is selected. On the right, the 'Lifecycle' section is open, displaying a table with one rule:

Enabled	Name	Rule Target
<input checked="" type="checkbox"/>	Testbackup	Whole Bucket

At the bottom right of the lifecycle configuration panel, there are 'Save' and 'Cancel' buttons, with the 'Save' button being the one currently highlighted by a mouse cursor.

Verify Storage Class is Standard

The screenshot shows the AWS S3 Management Console. The left sidebar lists files and folders in the 'www.cloudskillhyd.com' bucket. The 'contact-us.html' file is selected. The details pane on the right shows the file's properties, including its storage class, which is listed as 'Standard'.

Name	Storage Class	Size	Last Modified
404.html	Standard	6 KB	Tue Aug 15 08:46:32 GMT+05:30 2018
about-us.html	Standard	5.8 KB	Tue Aug 15 08:46:33 GMT+05:30 2018
article.html	Standard	5.3 KB	Tue Aug 15 08:46:34 GMT+05:30 2018
articles.html	Standard	4.8 KB	Tue Aug 15 08:46:34 GMT+05:30 2018
contact-us.html	Standard	4.7 KB	Tue Aug 15 08:46:35 GMT+05:30 2018
css	--	--	--
images	--	--	--
index.html	Standard	6 KB	Tue Aug 15 08:46:36 GMT+05:30 2018
jss	--	--	--
sitemap.html	Standard	4.8 KB	Tue Aug 15 08:46:37 GMT+05:30 2018

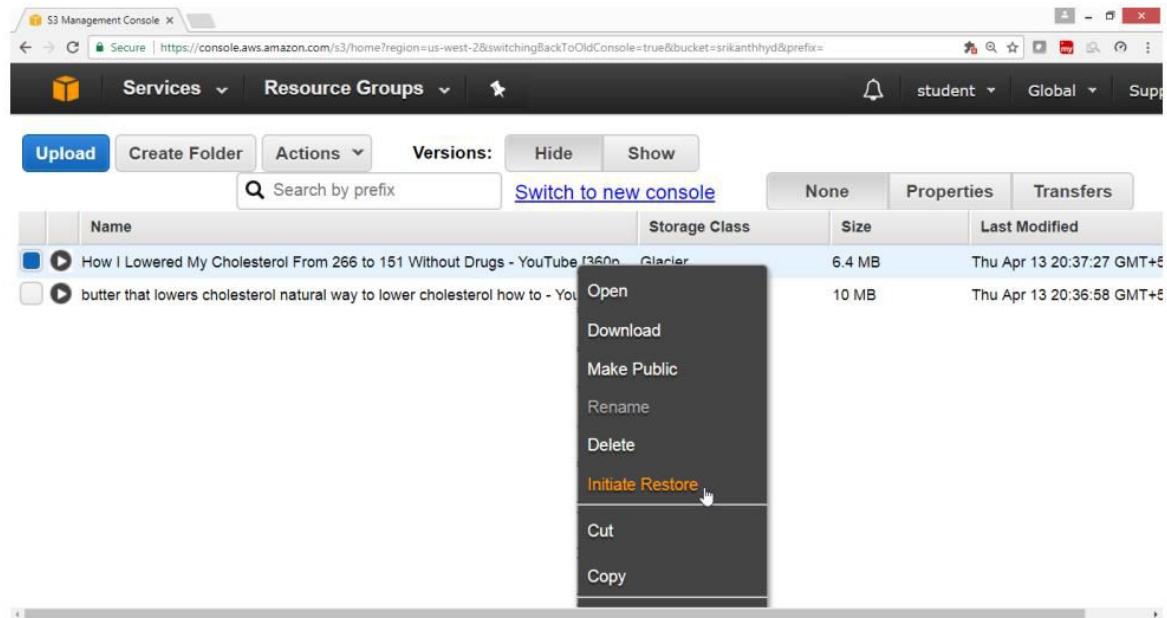
Verify Once the file goes to Glacier then Storage Class is **Glacier**

The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with 'Services' dropdown, 'Resource Groups' dropdown, and other account-related links. Below the navigation is a toolbar with 'Upload' (highlighted in blue), 'Create Folder', 'Actions' (with dropdown options), 'Versions' (with 'Hide' and 'Show' buttons), and a search bar labeled 'Search by prefix'. 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 files in a bucket named 'srikanthhyd'. The columns in the table are 'Name', 'Storage Class', 'Size', and 'Last Modified'. There are two entries:

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+5
butter that lowers cholesterol natural way to lower cholesterol how to - YouTube ...	Glacier	10 MB	Thu Apr 13 20:36:58 GMT+5

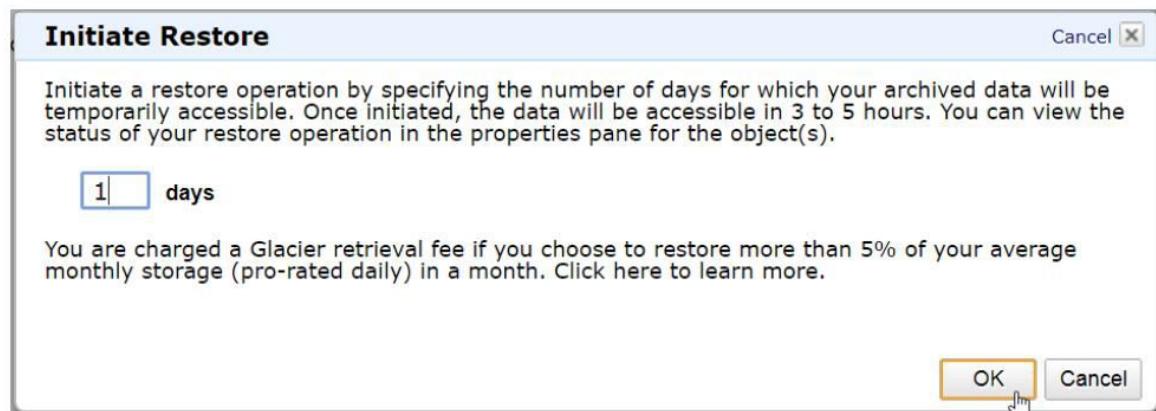
To Restore go to the bucket select the file

Right click and select **Initiate Restore**



Provide number of days → 1

Click on **OK**



Verify

File will get restored after 1 Day

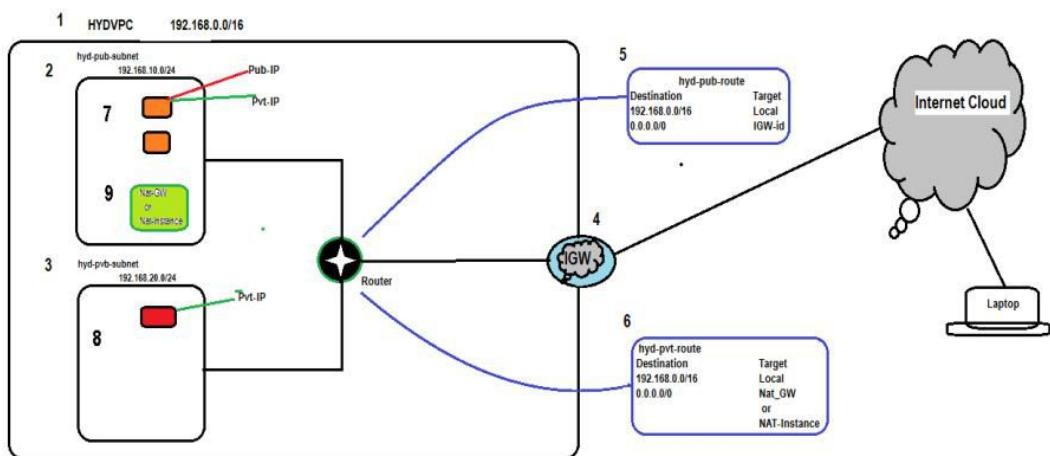
Storage class will become Standard.

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

OBJECTIVE

To configure Amazon Virtual Private Cloud with public and private subnet

TOPOLOGY



PRE-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.

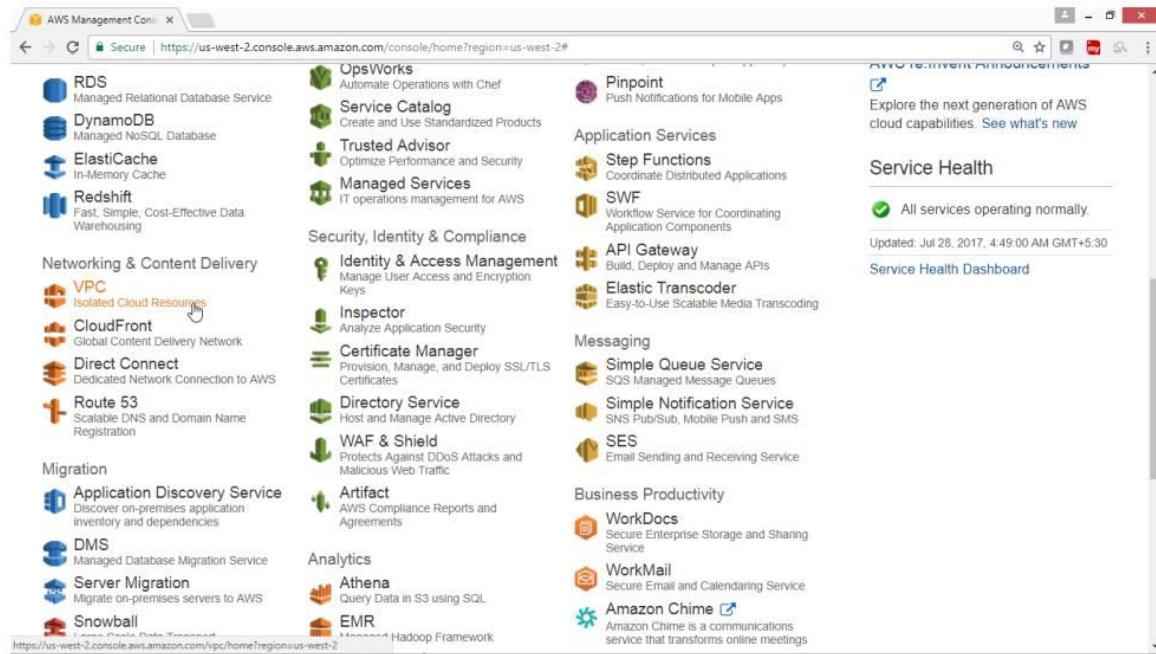
1) To create your own VPC

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

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

Create VPC Actions

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
default-vpc-oregon	vpc-89c341ee	available	172.31.0.0/16		dopt-e494f180

Select a VPC above

https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#vpces: https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#vpces: © 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

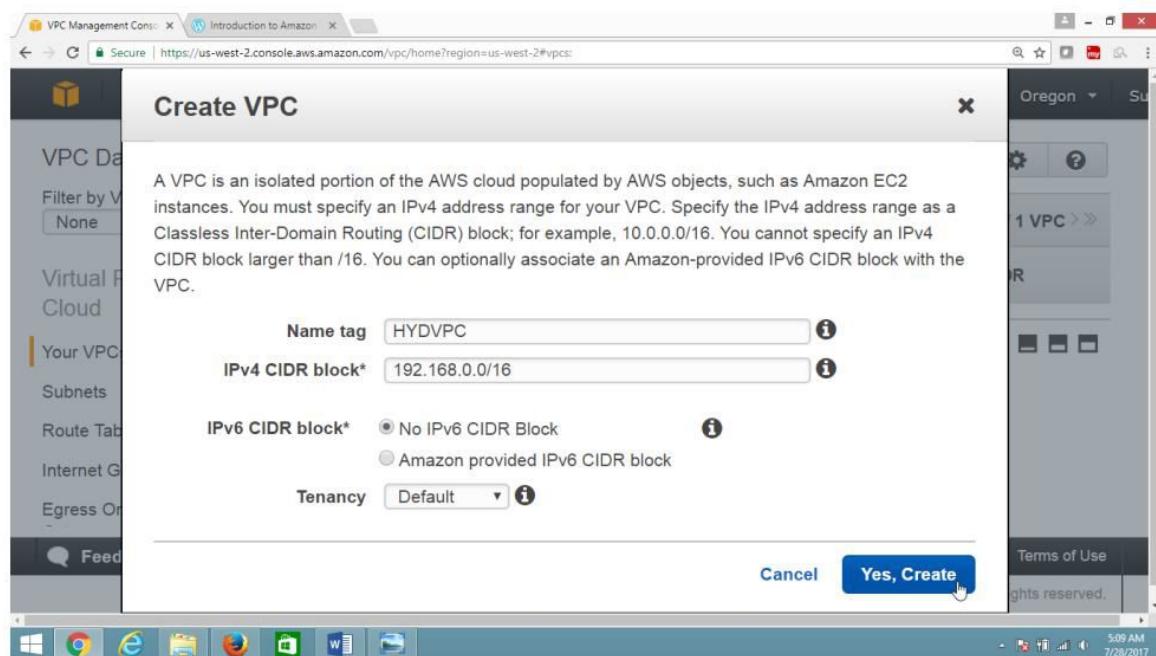
On “Create VPC”, page

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

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
HYDVPC	vpc-7d934d1b	available	192.168.0.0/16	
default-vpc-oregon	vpc-89c341ee	available	172.31.0.0/16	

2) To create public subnet

Click on **Subnet**

Click on **Create Subnet** button

Name	Subnet ID	State	VPC
	subnet-19d0f141	available	vpc-89c341ee default-vpc-oregon
	subnet-13f60e5a	available	vpc-89c341ee default-vpc-oregon

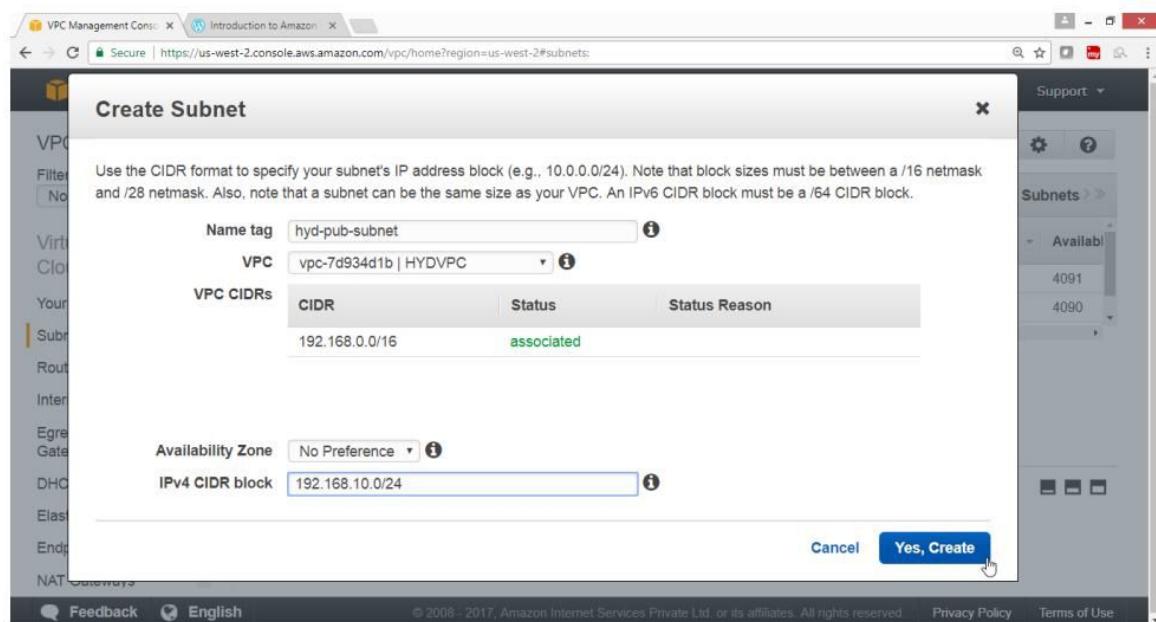
On **Create Subnet**, page

For Name tag → **hyd-pub-subnet**

For VPC → **HYDVPC**

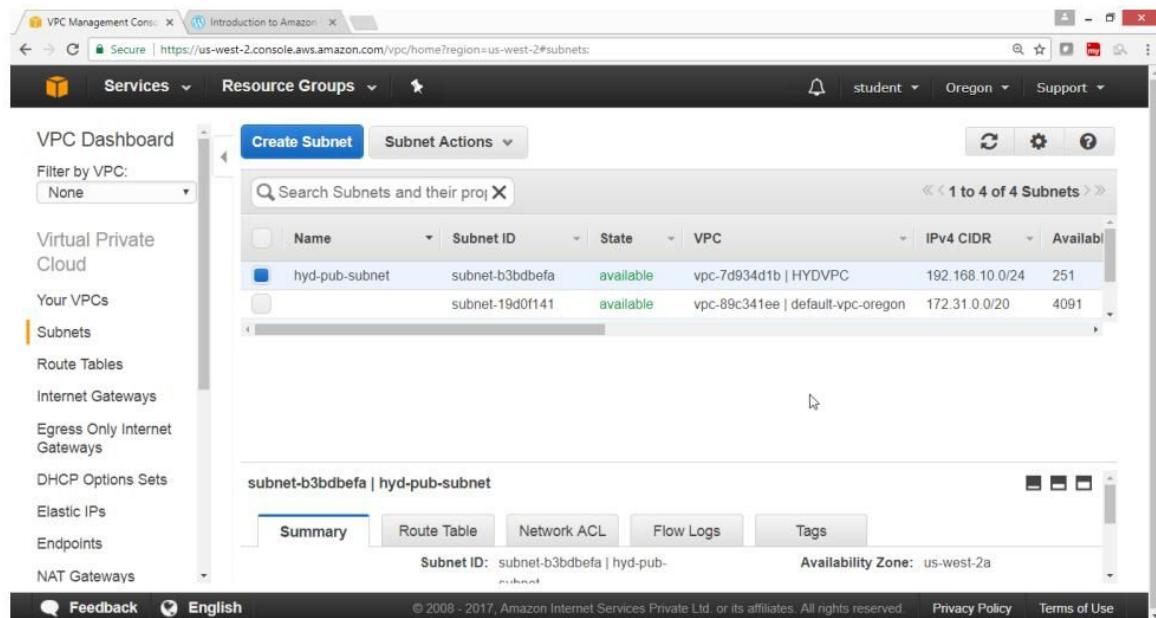
For IPv4 CIDR block → **192.168.10.0/24**

Click on **Yes Create** button



Verify

hyd-pub-subnet got created

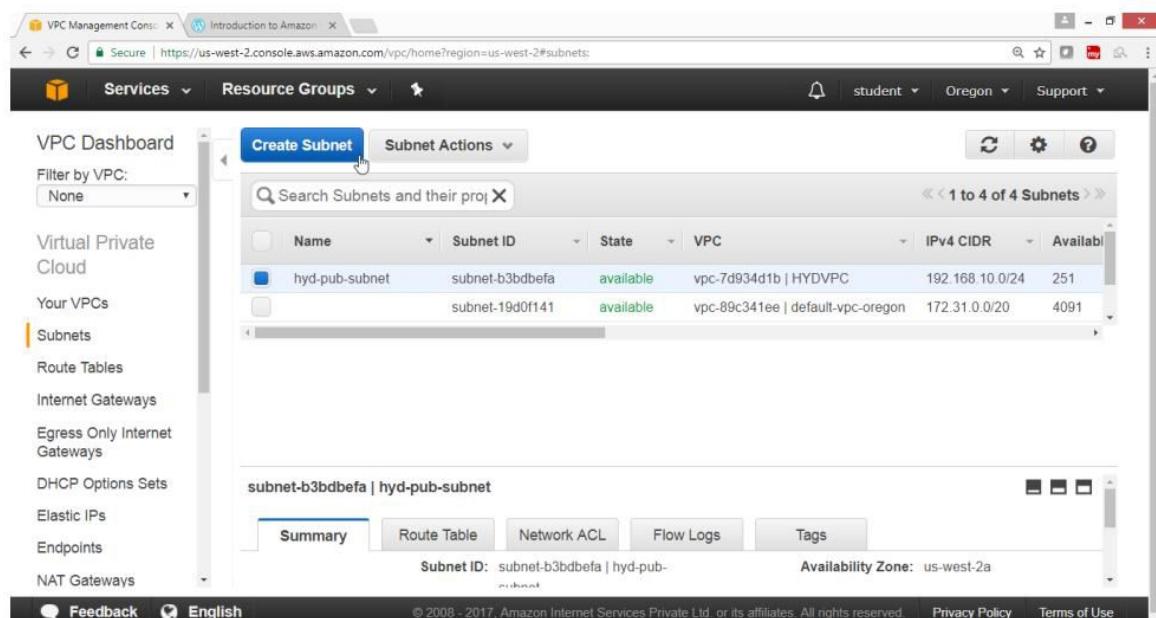


The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with options like 'Virtual Private Cloud', 'Your VPCs', 'Subnets' (which is selected), 'Route Tables', 'Internet Gateways', 'Egress Only Internet Gateways', 'DHCP Options Sets', 'Elastic IPs', 'Endpoints', and 'NAT Gateways'. The main area has tabs for 'Create Subnet' and 'Subnet Actions'. Below that is a search bar and a table with columns: Name, Subnet ID, State, VPC, IPv4 CIDR, and Available. The table shows two rows: one for 'hyd-pub-subnet' (subnet-b3bdbefa) and another for a default subnet (subnet-19d0f141). At the bottom, there are tabs for 'Summary', 'Route Table', 'Network ACL', 'Flow Logs', and 'Tags'. The 'Summary' tab is selected. The subnet ID is 'subnet-b3bdbefa | hyd-pub-subnet' and the availability zone is 'us-west-2a'.

3) To create private subnet

Click on Subnet

Click on Create Subnet button



This screenshot is identical to the one above, showing the AWS VPC Management Console. The 'Create Subnet' button is highlighted with a mouse cursor. The rest of the interface, including the sidebar, table, and bottom tabs, remains the same.

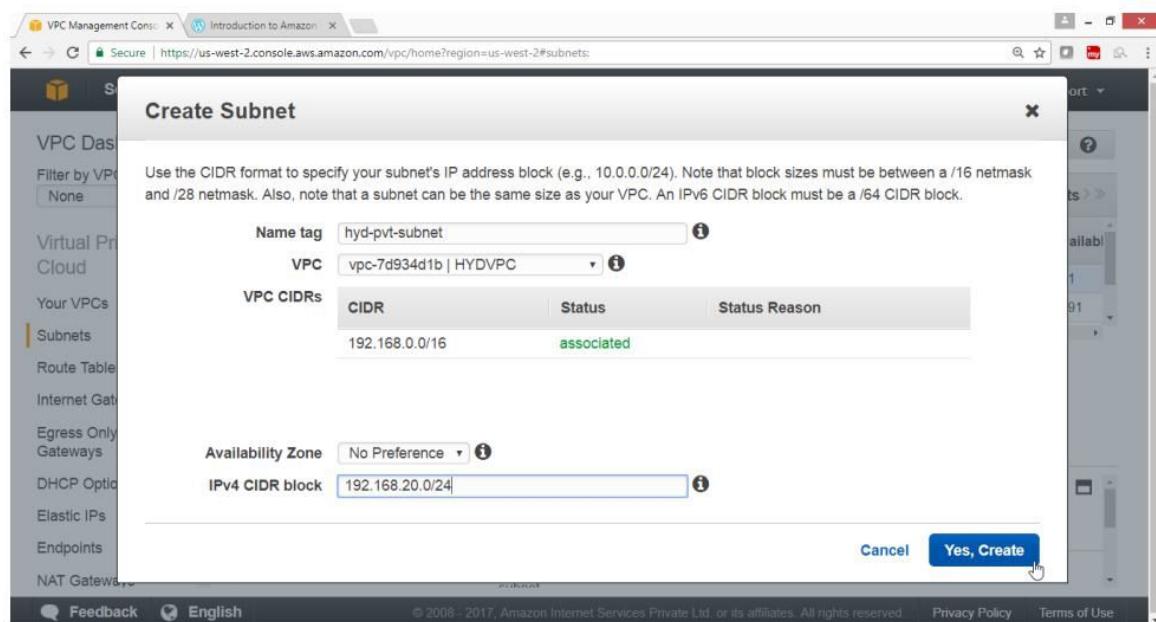
On **Create Subnet**, page

For Name tag → hyd-pvt-subnet

For VPC → HYDVPC

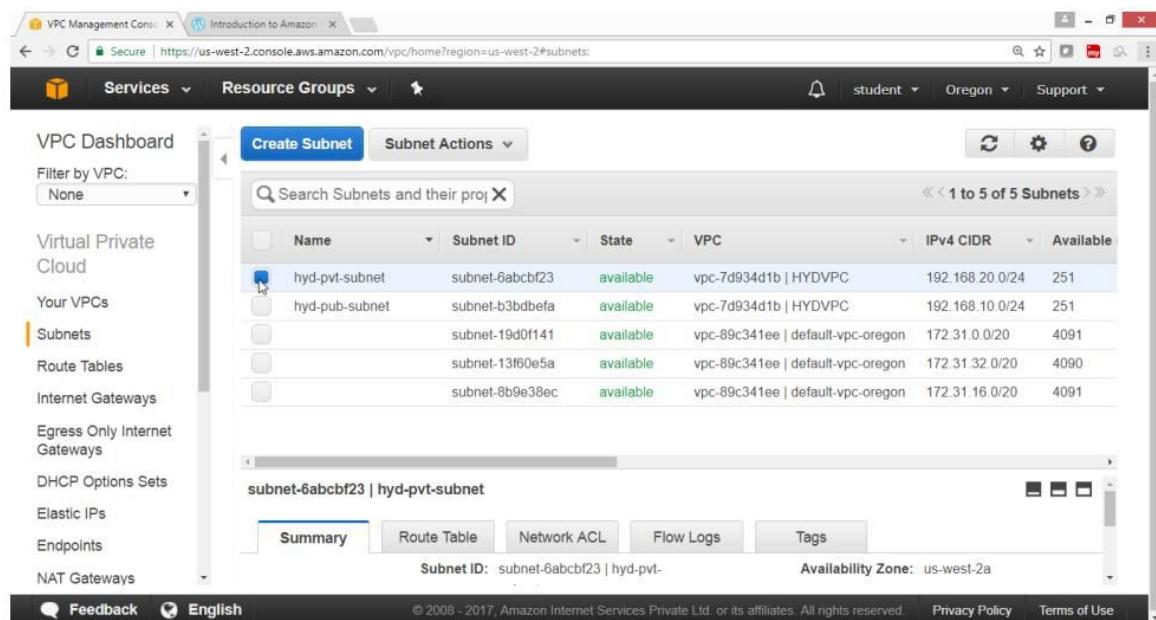
For IPv4 CIDR block → 192.168.20.0/24

Click on **Yes Create** button



Verify

hyd-pvt-subnet got created



The screenshot shows the AWS VPC Management Console with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#subnets>. The left sidebar shows 'Subnets' selected. The main area displays a table of subnets:

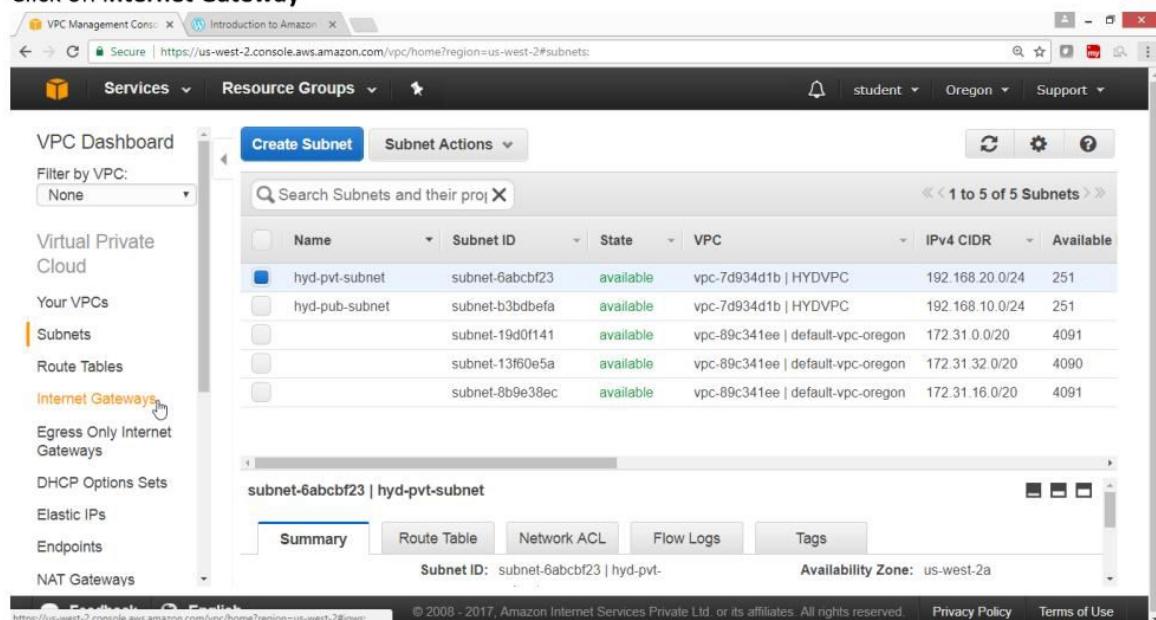
Name	Subnet ID	State	VPC	IPv4 CIDR	Available
hyd-pvt-subnet	subnet-6abcbf23	available	vpc-7d934d1b HYDVPC	192.168.20.0/24	251
hyd-pub-subnet	subnet-b3bdbefa	available	vpc-7d934d1b HYDVPC	192.168.10.0/24	251
	subnet-19d0f141	available	vpc-89c341ee default-vpc-oregon	172.31.0.0/20	4091
	subnet-13f60e5a	available	vpc-89c341ee default-vpc-oregon	172.31.32.0/20	4090
	subnet-8b9e38ec	available	vpc-89c341ee default-vpc-oregon	172.31.16.0/20	4091

The 'Summary' tab is selected. The subnet ID is listed as **subnet-6abcbf23 | hyd-pvt-subnet**, and the availability zone is **us-west-2a**.

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

In VPC Dashboard panel

Click on Internet Gateway



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#gwts>. The left sidebar shows 'Internet Gateways' selected. The main area displays a table of internet gateways:

Name	State	VPC	IPv4 CIDR	Available
hyd-pvt-subnet	available	vpc-7d934d1b HYDVPC	192.168.20.0/24	251
hyd-pub-subnet	available	vpc-7d934d1b HYDVPC	192.168.10.0/24	251
	available	vpc-89c341ee default-vpc-oregon	172.31.0.0/20	4091
	available	vpc-89c341ee default-vpc-oregon	172.31.32.0/20	4090
	available	vpc-89c341ee default-vpc-oregon	172.31.16.0/20	4091

The 'Summary' tab is selected. The subnet ID is listed as **subnet-6abcbf23 | hyd-pvt-subnet**, and the availability zone is **us-west-2a**.

Click on **Create Internet Gateway** button

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with various VPC-related options like Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways (which is selected and highlighted in orange), Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The main area has a header with 'Create Internet Gateway', 'Delete', 'Attach to VPC', and 'Detach from VPC'. Below that is a search bar and a table with columns for Name, ID, State, and VPC. One row is visible: igw-6ea7f10a, attached, vpc-89c341ee | default-vpc-oregon. At the bottom of the main area, it says 'Select an Internet gateway above' and shows three small icons. The footer includes links for Feedback, English, Privacy Policy, 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 that is a 'Name tag' input field containing 'HYDIGW'. At the bottom right of the dialog are two buttons: 'Cancel' and 'Yes, Create', with 'Yes, Create' being highlighted with a mouse cursor. The background shows the same VPC Management Console interface as the previous screenshot, with the 'Internet Gateways' section selected.

Verify

Internet gateway is created

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

Create Internet Gateway Delete Attach to VPC Detach from VPC

Search Internet Gateways and X

1 to 2 of 2 Internet Gateways >>

Name	ID	State	VPC
HYDIGW	igw-be27a9d9	detached	
	igw-6ea7f10a	attached	vpc-89c341ee default-vpc-oregon

igw-be27a9d9 | HYDIGW

Summary Tags

ID: igw-be27a9d9 | HYDIGW Attached VPC ID:

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

Select HYDIGW

Click "Attach to VPC"

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

Create Internet Gateway Delete Attach to VPC Detach from VPC

Search Internet Gateways and X

1 to 2 of 2 Internet Gateways >>

Name	ID	State	VPC
HYDIGW	igw-be27a9d9	detached	
	igw-6ea7f10a	attached	vpc-89c341ee default-vpc-oregon

igw-be27a9d9 | HYDIGW

Summary Tags

ID: igw-be27a9d9 | HYDIGW Attached VPC ID:

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

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 Management Console with the 'Internet Gateways' section selected. The table lists two internet gateways:

Name	ID	State	VPC
HYDIGW	igw-be27a9d9	attached	vpc-7d934d1b HYDVPC
	igw-6ea7f10a	attached	vpc-89c341ee default-vpc-oregon

Below the table, a detailed view for the first internet gateway (igw-be27a9d9 | HYDIGW) is shown, confirming it is attached to the VPC vpc-7d934d1b | HYDVPC.

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 with the URL <https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#igws>. The left sidebar is titled 'VPC Dashboard' and includes links for Virtual Private Cloud, Your VPCs, Subnets, Route Tables (which is highlighted), Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The main content area is titled 'Create Internet Gateway' and shows a table of two Internet Gateways:

Name	ID	State	VPC
HYDIGW	igw-be27a9d9	attached	vpc-7d934d1b HYDVPC
	igw-6ea7f10a	attached	vpc-89c341ee default-vpc-oregon

A modal window for the selected Internet Gateway 'igw-be27a9d9 | HYDIGW' is open, showing its summary: ID: igw-be27a9d9 | HYDIGW and Attached VPC ID: vpc-7d934d1b | HYDVPC.

Click on "Create Route table" button

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 identical to the previous screenshot. The main content area is titled 'Create Route Table' and shows a table of two Route Tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
	rtb-1998c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYDVPC

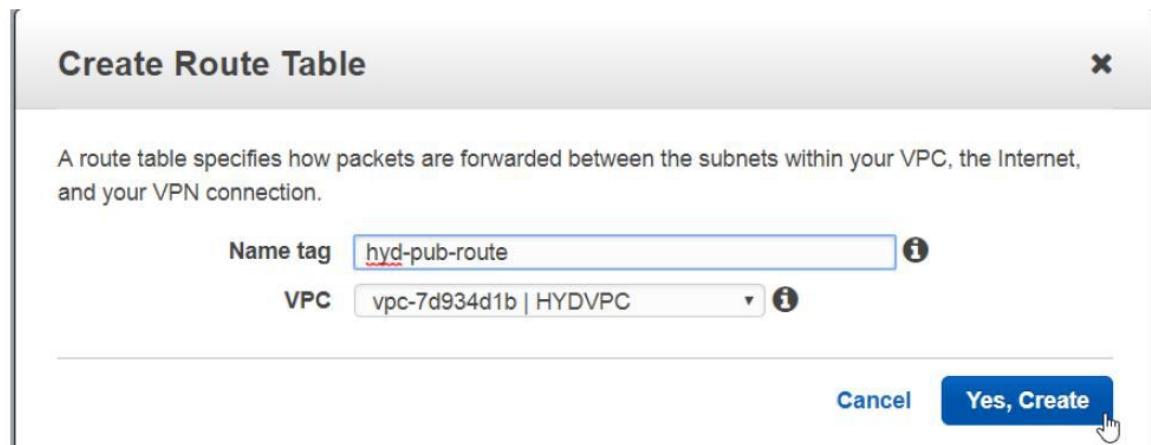
A modal window for creating a new Route Table is partially visible at the bottom.

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. On the left, there's a sidebar with options like '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 table of route tables. The table has columns: Name, Route Table ID, Explicitly Associated, Main, and VPC. One row is selected, showing 'hyd-pub-route' as the name, 'rtb-234b6445' as the ID, '0 Subnets' as the count, 'No' as the main status, and 'vpc-7d934d1b | HYDVPC' as the VPC. Below the table, there's a summary section with tabs for 'Summary', 'Routes', 'Subnet Associations', 'Route Propagation', and 'Tags'. The 'Summary' tab is selected, showing 'Route Table ID: rtb-234b6445 | hyd-pub-route' and 'Main: no'.

Click on “Subnet Association” button

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with options like VPC Dashboard, Filter by VPC (None), Virtual Private Cloud, Your VPCs, Subnets, Route Tables (which is selected and highlighted in orange), Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The main area shows a table of route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	0 Subnets	No	vpc-7d934d1b HYD VPC
	rtb-1998c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYD VPC

Below the table, for the selected route table 'rtb-234b6445 | hyd-pub-route', there are tabs for Summary, Routes, Subnet Associations (which is active and highlighted in blue), Route Propagation, and Tags. The Subnet Associations tab shows the message: "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:". There is an 'Edit' button at the bottom of this section.

Click on Edit button

This screenshot shows the same AWS VPC Management Console interface, but now focusing on the Subnet Associations page for the route table 'rtb-234b6445 | hyd-pub-route'. The 'Edit' button is highlighted with a blue box and a cursor is hovering over it. The rest of the interface is identical to the previous screenshot, showing the table of route tables and the summary for the selected route table.

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

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 shows a list of Route Tables. One route table, 'hyd-pub-route' (ID: rtb-234b6445), is selected. The 'Subnet Associations' tab is active. It lists two subnets: 'subnet-b3bdbefa | hyd-pub-subnet' (IPv4 CIDR: 192.168.10.0/24) and 'subnet-6abcbf23 | hyd-pvt-subnet' (IPv4 CIDR: 192.168.20.0/24). The first subnet has a checked checkbox in the 'Associate' column. At the bottom, there's a 'Save' button.

Verify

hyd-pub-subnet is associated with routing table

This screenshot is similar to the previous one but shows the 'Edit' button being clicked. A message at the bottom states: 'The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:'. The rest of the interface is identical to the previous screenshot.

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, Filter by VPC (set to None), Virtual Private Cloud, Your VPCs, Subnets, Route Tables (which is selected and highlighted in orange), Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The main area has tabs for Create Route Table, Delete Route Table, Set As Main Table, and three route tables listed: rtb-1998c27e and rtb-847d52e2 (both associated with vpc-89c341ee | default-vpc-oregon) and rtb-234b6445 | hyd-pub-route (associated with vpc-7d934d1b | HYDVPC). Below these is a table for subnet associations. The 'Subnet Associations' tab is active, and the 'Edit' button is highlighted with a mouse cursor. The table shows one subnet association for rtb-234b6445 with a CIDR range of 192.168.10.0/24. A note below the table states: "The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:" followed by a list of subnets.

Click on “Add another route” button

This screenshot is similar to the previous one but focuses on the 'Routes' tab for route table rtb-234b6445. The 'Save' button is highlighted. Below it, there's a table with columns for Destination (192.168.0.0/16), Target (local), Status (Active), Propagated (No), and Remove. At the bottom of this table is a button labeled 'Add another route' with a mouse cursor hovering over it.

For Destination → 0.0.0.0/0

For Target → select HYDIGW

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 has tabs for Create Route Table, Delete Route Table, and Set As Main Table. Below that is a search bar and a table showing three route tables. The table has columns for Name, Route Table ID, Explicitly Associated, Main, and VPC. The rows show 'rtb-1998c27e' and 'rtb-847d52e2', both associated with 'vpc-89c341ee | default-vpc-oregon'. The 'Main' column for both is 'Yes'. The 'VPC' column for the first row is 'vpc-89c341ee | default-vpc-oregon'. Below the table are tabs for Summary, Routes (which is selected), Subnet Associations, Route Propagation, and Tags. A 'Save' button is visible. Under the 'Routes' tab, there's a table with columns for Destination, Target, Status, Propagated, and Remove. It shows a row for '192.168.0.0/16' with 'local' as the target, 'Active' status, and 'No' propagating. Below this is an input field for '0.0.0.0/0' and a dropdown menu showing 'igw-be27a9d9 | HYDIGW'. An 'Add another route' button is at the bottom. At the very bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use.

Verification

Public route is added through internet gateway

This screenshot is identical to the one above it, showing the AWS VPC Management Console. The sidebar, main interface, and route table configuration are all the same. The difference is that the 'Save' button is now highlighted with a mouse cursor, indicating the action being performed.

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. The main area displays the 'Route Tables' section. A route table named 'rtb-234b6445 | hyd-pub-route' is selected. The 'Routes' tab is active. The table shows two entries:

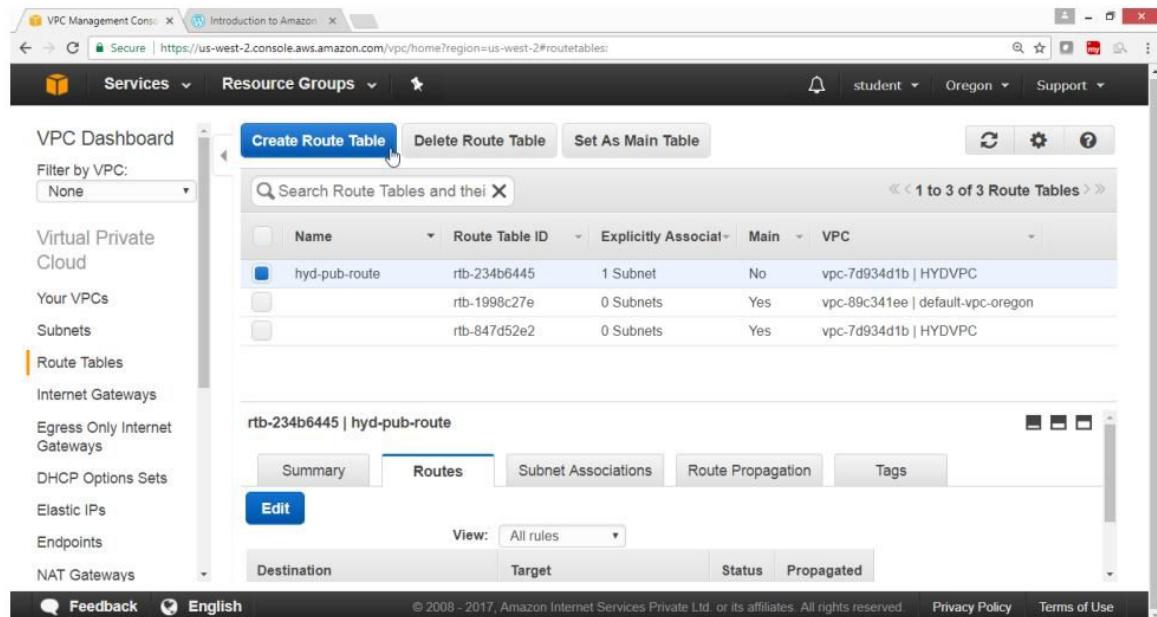
Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	igw-be27a9d9	Active	No

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 VPC Dashboard, Filter by VPC (None), Virtual Private Cloud, Your VPCs, Subnets, and Route Tables (which is selected). The main area shows a table of existing route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	rtb-234b6445	1 Subnet	No	vpc-7d934d1b HYDVPC
	rtb-1998c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYDVPC

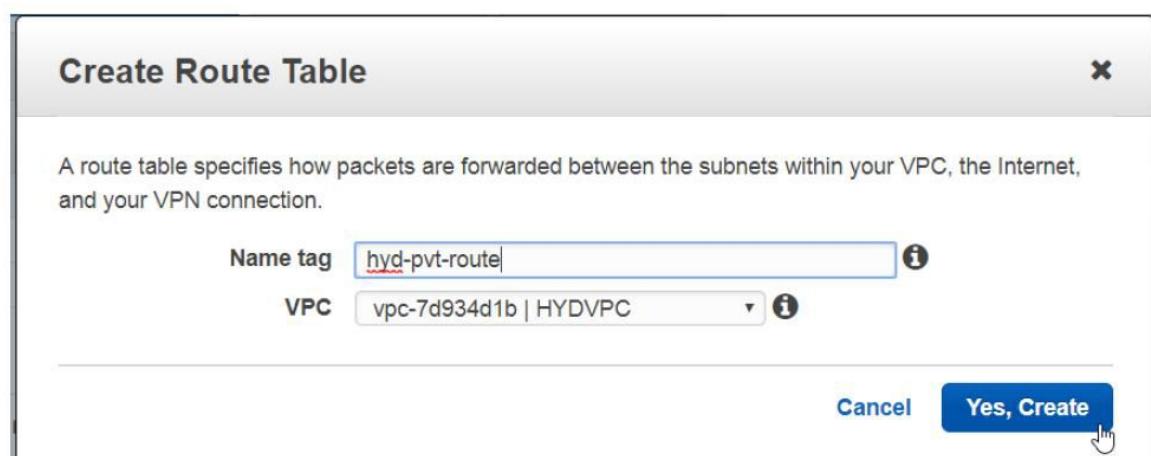
Below the table, a specific route table is selected: "rtb-234b6445 | hyd-pvt-route". The "Routes" tab is active. At the bottom of this panel, there are tabs for Summary, Routes, Subnet Associations, Route Propagation, and Tags, with "Edit" being the current tab.

On “Create Route Table” box

For Name tag → hyd-pvt-route

For VPC → HYDVPC

Click on “Yes, Create” button



The dialog box has a title "Create Route Table". Inside, there's 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" containing "hyd-pvt-route" and "VPC" containing "vpc-7d934d1b | HYDVPC". At the bottom right, there are "Cancel" and "Yes, Create" buttons, with the "Yes, Create" button having a hand cursor icon over it.

Verify

hyd-pvt-route table is created

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

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X 1 to 4 of 4 Route Tables

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	rtb-ac446bca	0 Subnets	No	vpc-7d934d1b HYDVPC
hyd-pub-route	rtb-234b6445	1 Subnet	No	vpc-7d934d1b HYDVPC
	rtb-1998c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYDVPC

rtb-ac446bca | hyd-pvt-route

Summary Routes Subnet Associations Route Propagation Tags

Edit View: All rules

Destination	Target	Status	Propagated
-------------	--------	--------	------------

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

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

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X 1 to 4 of 4 Route Tables

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	rtb-ac446bca	0 Subnets	No	vpc-7d934d1b HYDVPC
hyd-pub-route	rtb-234b6445	1 Subnet	No	vpc-7d934d1b HYDVPC
	rtb-1998c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYDVPC

rtb-ac446bca | hyd-pvt-route

Summary Routes Subnet Associations Route Propagation Tags

Edit View: All rules

Destination	Target	Status	Propagated
-------------	--------	--------	------------

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

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, 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 Subnets	Main	VPC
hyd-pvt-route	rtb-ac446bca	0 Subnets	No	vpc-7d934d1b HYD VPC
hyd-pub-route	rtb-234b6445	1 Subnet	No	vpc-7d934d1b HYD VPC
	rtb-1998c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYD VPC

Below the table, there are tabs for Summary, Routes, Subnet Associations (which is selected), Route Propagation, and Tags. The Subnet Associations tab has buttons for Edit, Associate, and Dissociate. The 'Associate' button is highlighted with a blue box and a mouse cursor. The 'Edit' button above it is also highlighted.

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

The screenshot shows the AWS VPC Management Console. The sidebar and route table list are identical to the previous screenshot. The main area shows the Subnet Associations tab for the 'hyd-pvt-route' route table. There are two subnets listed:

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/>	subnet-b3bdbefa hyd-pub-subnet	192.168.10.0/24	-	rtb-234b6445 hyd-pub-route
<input checked="" type="checkbox"/>	subnet-6abcbf23 hyd-pvt-subnet	192.168.20.0/24	-	Main

Below the table, there are buttons for Cancel and Save. The 'Save' button is highlighted with a blue box and a mouse cursor.

Click on Save 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

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-1998c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon	
hyd-pvt-route	rtb-ac446bca	1 Subnet	No	vpc-7d934d1b HYDVPC

rtb-ac446bca | hyd-pvt-route

Summary Routes Subnet Associations Route Propagation Tags

Edit Save Successful

Subnet IPv4 CIDR IPv6 CIDR

subnet-6abcbf23 | hyd-pvt-subnet 192.168.20.0/24

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

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

Verify

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

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

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-1998c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon	
hyd-pvt-route	rtb-ac446bca	1 Subnet	No	vpc-7d934d1b HYDVPC

rtb-ac446bca | hyd-pvt-route

Summary Routes Subnet Associations Route Propagation Tags

Edit

Subnet IPv4 CIDR IPv6 CIDR

subnet-6abcbf23 | hyd-pvt-subnet 192.168.20.0/24

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

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

Click on Route 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 has tabs for Create Route Table, Delete Route Table, Set As Main Table, and a search bar. Below that is a table with columns for Name, Route Table ID, Explicitly Associated, Main, and VPC. It lists two route tables: 'rtb-1998c27e' and 'hyd-pvt-route'. The 'hyd-pvt-route' table is selected. Under it, there are tabs for Summary, Routes, Subnet Associations (which is selected), Route Propagation, and Tags. The 'Routes' tab shows a single entry: 'subnet-6abcbf23 | hyd-pvt-subnet 192.168.20.0/24'. A tooltip message says: 'The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:'. At the bottom, there are links for Feedback, English, Privacy Policy, and Terms of Use.

Note: No need to add IGW in pvt route

This screenshot is similar to the previous one but focuses on the 'Routes' tab for the 'hyd-pvt-route' route table. The table has columns for Destination, Target, Status, and Propagated. It contains one rule: '192.168.0.0/16' with 'local' as the target, 'Active' status, and 'No' propagation. The rest of the interface is identical to the first screenshot, including the sidebar and footer.

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 homepage. The top navigation bar includes 'Services' (selected), 'Resource Groups', and other account-related options. Below the navigation is a search bar and a 'Group' button. The main content area is organized into several sections:

- Compute:** EC2 Container Service, Lightsail, Elastic Beanstalk, Lambda, Batch.
- Developer Tools:** CodeStar, CodeCommit, CodeBuild, CodeDeploy, CodePipeline, X-Ray.
- Analytics:** Athena, EMR, CloudSearch, Elasticsearch Service, Kinesis, Data Pipeline, QuickSight.
- Application Services:** Step Functions, SWF, API Gateway, Elastic Transcoder.
- Storage:** S3, EFS, Glacier, Storage Gateway.
- Management Tools:** CloudWatch, CloudFormation, CloudTrail, Config, OpsWorks, Service Catalog, Trusted Advisor.
- Artificial Intelligence:** Lex, Polly, Rekognition, Machine Learning.
- Messaging:** Simple Queue Service, Simple Notification Service, SES.
- Business Productivity:** WorkDocs, WorkMail, Amazon Chime.
- Internet Of Things:** (partially visible)

The URL in the address bar is <https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2>.

The screenshot shows the EC2 Management Console dashboard. The left sidebar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (with sub-links for Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), Images (with sub-links for AMIs, Bundle Tasks), and Elastic Block Store (with sub-links for Volumes). The main content area has three main sections:

- Resources:** You are using the following Amazon EC2 resources in the US West (Oregon) region:
 - 0 Running Instances
 - 0 Dedicated Hosts
 - 0 Volumes
 - 0 Key Pairs
 - 0 Placement Groups
 - 0 Elastic IPs
 - 0 Snapshots
 - 0 Load Balancers
 - 2 Security Groups
- Account Attributes:** Supported Platforms (VPC), Default VPC (vpc-89c341ee), Resource ID length management.
- Additional Information:** Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, Contact Us.

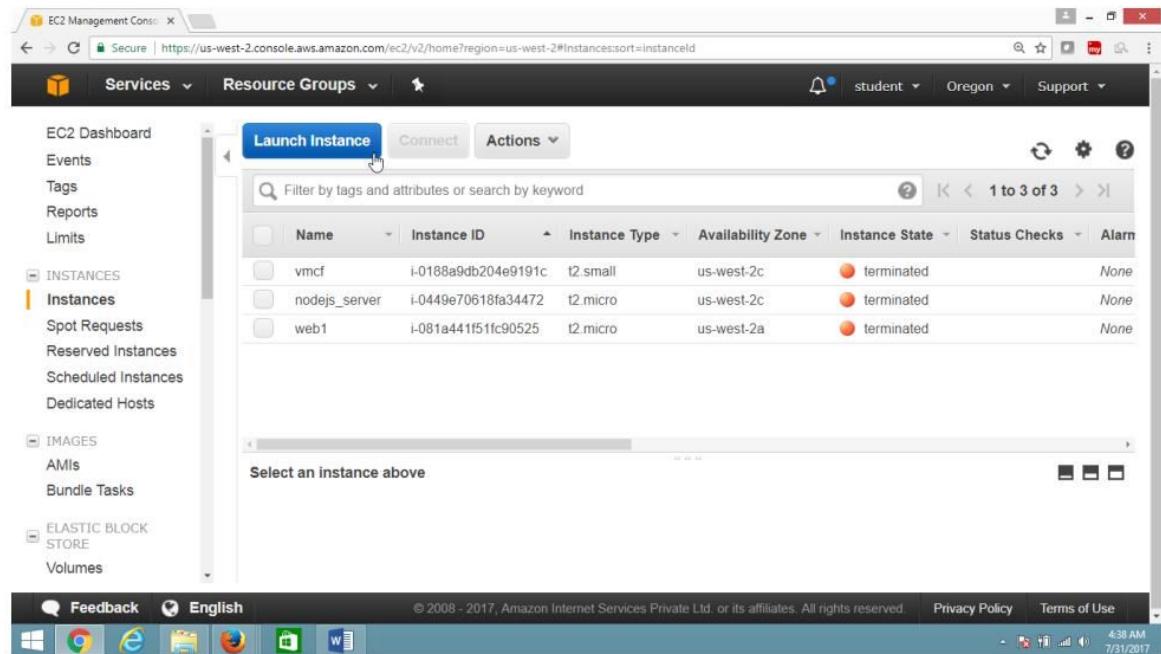
A callout box in the center says: "Just need a simple virtual private server? Get everything you need to jumpstart your project - compute, storage, and networking – for a low, predictable price. Try Amazon Lightsail for free."

The bottom of the page includes a 'Feedback' link, language selection (English), copyright information (© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.), and links for Privacy Policy and Terms of Use.

On the EC2 dashboard panel

Click on **instance**

Click on **Launch instance** button



The screenshot shows the AWS EC2 Management Console interface. The left sidebar menu is visible with options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block Store. The 'Instances' section is selected. The main content area displays a table of existing instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
vmcf	i-0188a9db204e9191c	t2.small	us-west-2c	terminated	None	
nodejs_server	i-0449e70618fa34472	t2.micro	us-west-2c	terminated	None	
web1	i-081a441f51fc90525	t2.micro	us-west-2a	terminated	None	

A large blue button labeled 'Launch Instance' is positioned above the table. Below the table, a message says 'Select an instance above'. The bottom of the screen shows standard browser navigation icons and a status bar indicating the date and time.

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

Free tier eligible

The screenshot shows the "Step 1: Choose an Amazon Machine Image (AMI)" page. At the top, it says "Free tier eligible". Below that, there's a list of AMIs:

Image Name	Description	Action
Microsoft Windows Server 2012 Base - ami-a1c1ddd8	Microsoft Windows 2012 Standard edition with 64-bit architecture. [English]	Select (button)
Microsoft Windows Server 2012 with SQL Server Express - ami-7ac6da03	Microsoft Windows Server 2012 Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Express. [English]	Select (button)
Microsoft Windows Server 2012 with SQL Server Web - ami-f2c6da8b	Microsoft Windows Server 2012 Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Web. [English]	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 "Step 2: Choose an Instance Type" page. It lists instance types under the "General purpose" family:

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	t2.micro	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, there are buttons: "Cancel", "Previous", "Review and Launch" (highlighted), and "Next: Configure Instance Details".

On the “Configuration Instance Details” page

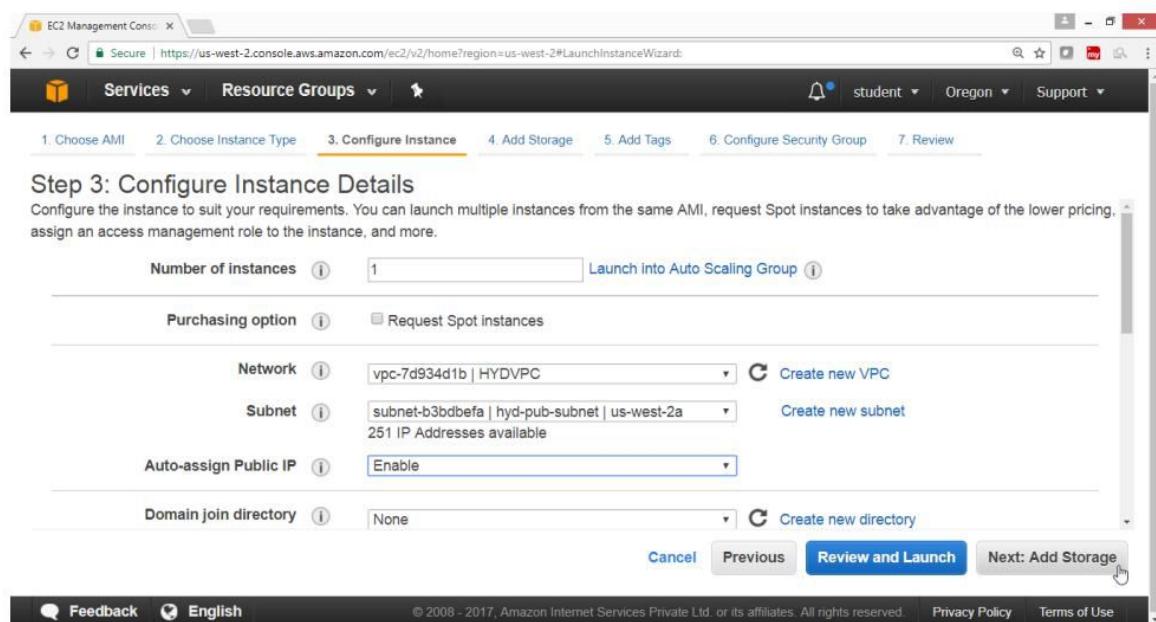
For “Number of instances” → 1

For “Network” → HYDVPN

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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-01e5be77f781e7266	30	General Purpose	100 / 3000	N/A	<input checked="" type="checkbox"/>	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.

Cancel Previous Review and Launch Next: Add Tags

Click on “Add tag” button

Key	(127 characters maximum)	Value	(255 characters maximum)	Instances	Volumes
Name	(127 characters maximum)	Webserver	(255 characters maximum)	<input type="checkbox"/>	<input type="checkbox"/>

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 AWS EC2 Management Console interface. The browser address bar indicates the URL is <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard>. The top navigation bar includes 'Services' (selected), 'Resource Groups', and user information ('student', 'Oregon', 'Support'). Below the navigation is a progress bar with steps 1-7: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (highlighted in yellow), 6. Configure Security Group, 7. Review.

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.

The main form displays a table for adding tags:

Key	(127 characters maximum)	Value	(255 characters maximum)	Instances	Volumes
Name		Winpubvm		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

At the bottom of the page are buttons: Cancel, Previous, Review and Launch (highlighted in blue), and Next: Configure Security Group. There are also 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 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+05:30

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 - ami-a1c1ddd8

Free tier eligible

Microsoft Windows 2012 Standard edition with 64-bit architecture. [English]

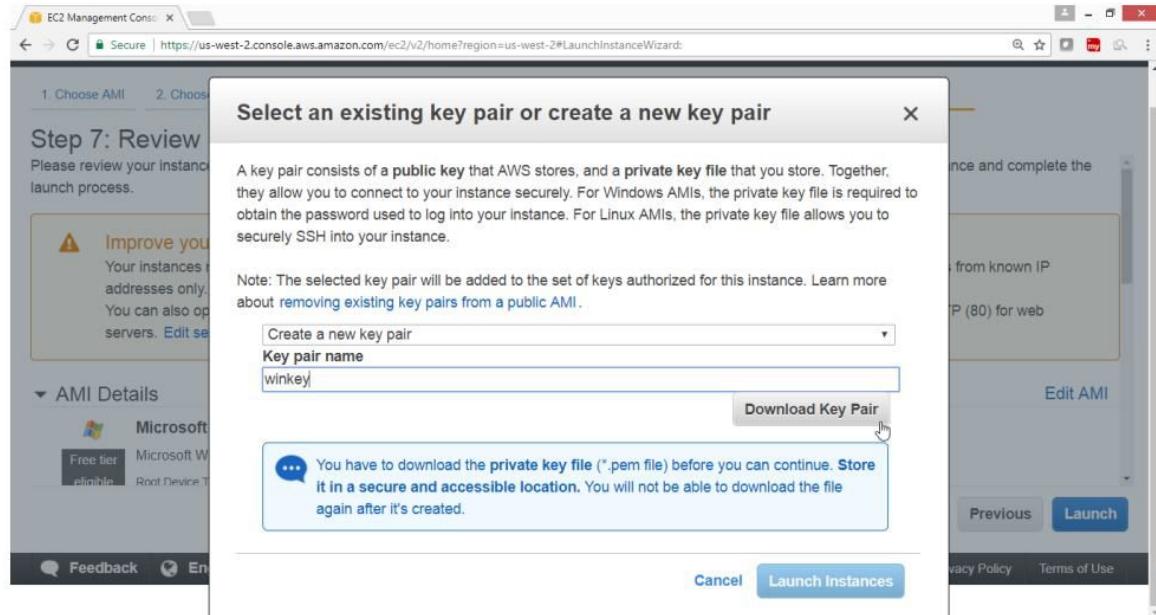
Root Device Type: ebs Virtualization Type: hvm

Cancel Previous Launch

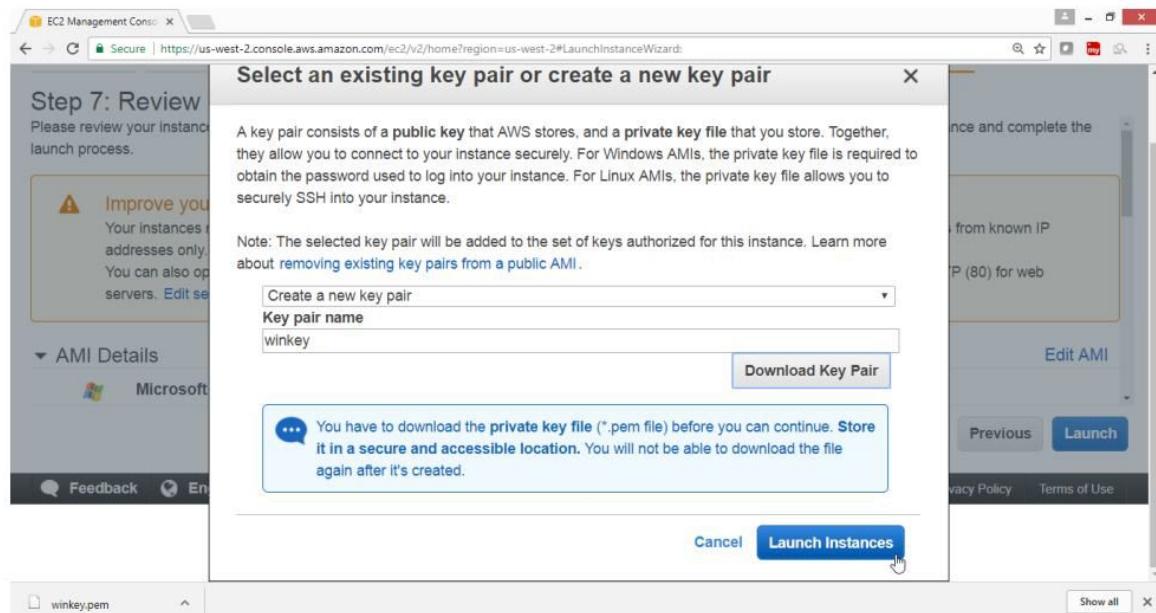
Select “Create a new key pair”

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 EC2 Management Console at the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard>. The page title is "Launch Status". It includes a note to "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, How to connect to your Windows instance, Learn about AWS Free Usage Tier, Amazon EC2: Microsoft Windows Guide, and Amazon EC2: Discussion Forum. Further down, it says "While your instances are launching you can also" and lists "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

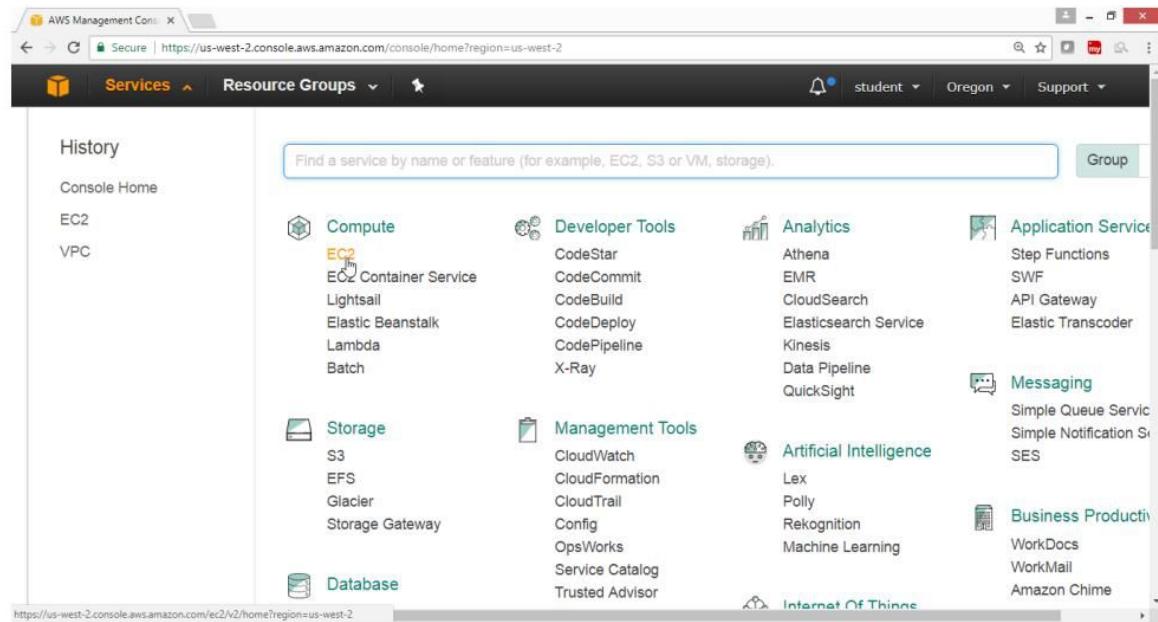
The screenshot shows the EC2 Management Console at the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#InstancesSort=instanceId>. The left sidebar shows navigation options like EC2 Dashboard, Events, Tags, Reports, Limits, and sections for Instances, Images, and Elastic Block Store. The main area has tabs for "Launch Instance", "Connect", and "Actions". A search bar at the top right 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. One row is selected, showing "Winpubvm" as the Name, "i-0cb26994e13174e85" as the Instance ID, "t2.micro" as the Instance Type, "us-west-2a" as the Availability Zone, "running" as the Instance State, and "None" as the Status Checks. At the bottom of the table, it says "1 to 1 of 1". Below the table, there's a detailed view for the selected instance: "Instance: i-0cb26994e13174e85 (Winpubvm) Public IP: 54.202.132.130". It includes tabs for Description, Status Checks, Monitoring, and Tags. Under "Description", it shows "Instance ID: i-0cb26994e13174e85" and "Public DNS (IPv4): 54.202.132.130". The bottom of the page includes standard footer links for Feedback, English, Privacy Policy, and Terms of Use.

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

Open the AWS console

Click on Services

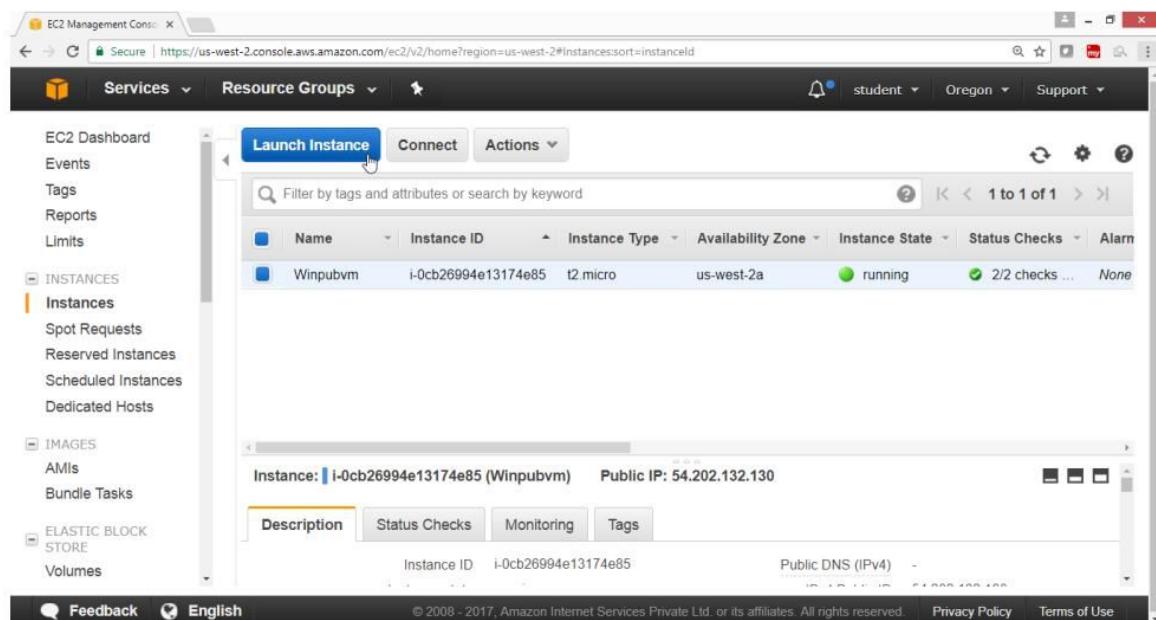
Click on **Ec2** services



On the **EC2 Dashboard** panel

Click on **Instance**

Click on “**Launch instance**” button



The screenshot shows the AWS EC2 Management Console interface. The left sidebar has 'Instances' selected under 'Instances'. The main area displays a table of instances. A single instance, 'Winpubvm' (ID: i-0cb26994e13174e85), is selected. At the top of the main area, there are three buttons: 'Launch Instance' (highlighted with a red box), 'Connect', and 'Actions'. Below the table is a detailed view of the selected instance, showing its ID, type, availability zone, state, and status checks.

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

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 EC2 Management Console Launch Instance Wizard, specifically Step 1: Choose an Amazon Machine Image (AMI). The page title is "Step 1: Choose an Amazon Machine Image (AMI)". The navigation bar includes tabs for 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. A "Cancel and Exit" button is also present. The main content area displays a list of available AMIs:

Image Name	Description	Root device type	Virtualization type	Action
Microsoft Windows Server 2016 with SQL Server Standard - ami-39fae640	Microsoft Windows 2016 Datacenter edition, Microsoft SQL Server 2016 Standard. [English]	ebs	hvm	Select (button)
Microsoft Windows Server 2012 R2 Base - ami-3dcbd744	Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]	ebs	hvm	Select (button)
Microsoft Windows Server 2012 R2 with SQL Server Express - ami-3bc8d442	Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]	ebs	hvm	Select (button)

A "Free tier eligible" badge is visible next to the third item in the list. The "Select" button for the second item is highlighted with a mouse cursor. The bottom of the page includes standard AWS footer links: Feedback, English, Copyright notice (© 2008 - 2017), Privacy Policy, and 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 EC2 Management Console interface. The title bar says "EC2 Management Console". The navigation bar includes "Services", "Resource Groups", and "student Oregon Support". Below the navigation is a breadcrumb trail: "1. Choose AMI" (disabled), "2. Choose Instance Type" (highlighted in orange), "3. Configure Instance" (disabled), "4. Add Storage" (disabled), "5. Add Tags" (disabled), "6. Configure Security Group" (disabled), and "7. Review" (disabled). The main content area is titled "Step 2: Choose an Instance Type". It has a filter bar with "All instance types" and "Current generation". A note says "Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)". A table lists instance types:

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

At the bottom are buttons: "Cancel", "Previous", "Review and Launch" (highlighted in blue), and "Next: Configure Instance Details".

On the “Configuration Instance Details” page

For “Number of instances” → 1

For “Network” → HYDVPN

For “Subnet” → hyd-pvt-subnet

For “Auto-assign Public IP” → Disabled

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 Launch into Auto Scaling Group

Purchasing option Request Spot instances

Network

Subnet
251 IP Addresses available

Auto-assign Public IP

Domain join directory

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 (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-08c5b8b7b19187ab8	30	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

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

Click on “Add tag” button

The screenshot shows the EC2 Management Console interface. The top navigation bar includes 'Services' and 'Resource Groups'. Below it, a progress bar shows steps 1 through 7: 'Choose AMI', 'Choose Instance Type', 'Configure Instance', 'Add Storage', 'Add Tags' (which is highlighted in yellow), 'Configure Security Group', and 'Review'. The main content area is titled 'Step 5: Add Tags'. It contains instructions: 'A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.' Below this, there are fields for 'Key' (with placeholder '(127 characters maximum)') and 'Value' (with placeholder '(255 characters maximum)'). To the right, there are tabs for 'Instances' and 'Volumes'. A note below the fields says 'This resource currently has no tags'. Further down, a button labeled 'Add Tag' is shown with the note '(Up to 50 tags maximum)'. At the bottom, there are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is blue), and 'Next: Configure Security Group'.

For “Key” → Name

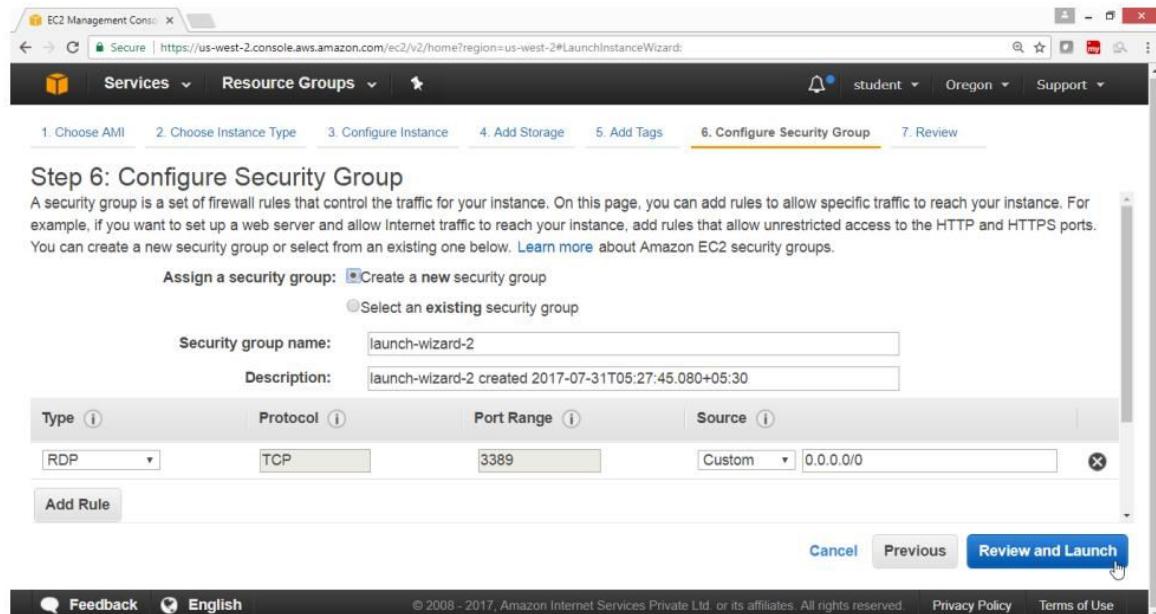
For Value → Winpvtvm

Click on “Next: Configure Security Group” button

This screenshot is identical to the one above, but it shows a tag has been added. In the 'Value' field, 'Winpvtvm' is entered. The 'Instances' and 'Volumes' checkboxes are checked. The 'Add another tag' button is visible below the input fields. The 'Review and Launch' button is still blue, indicating the next step can be selected.

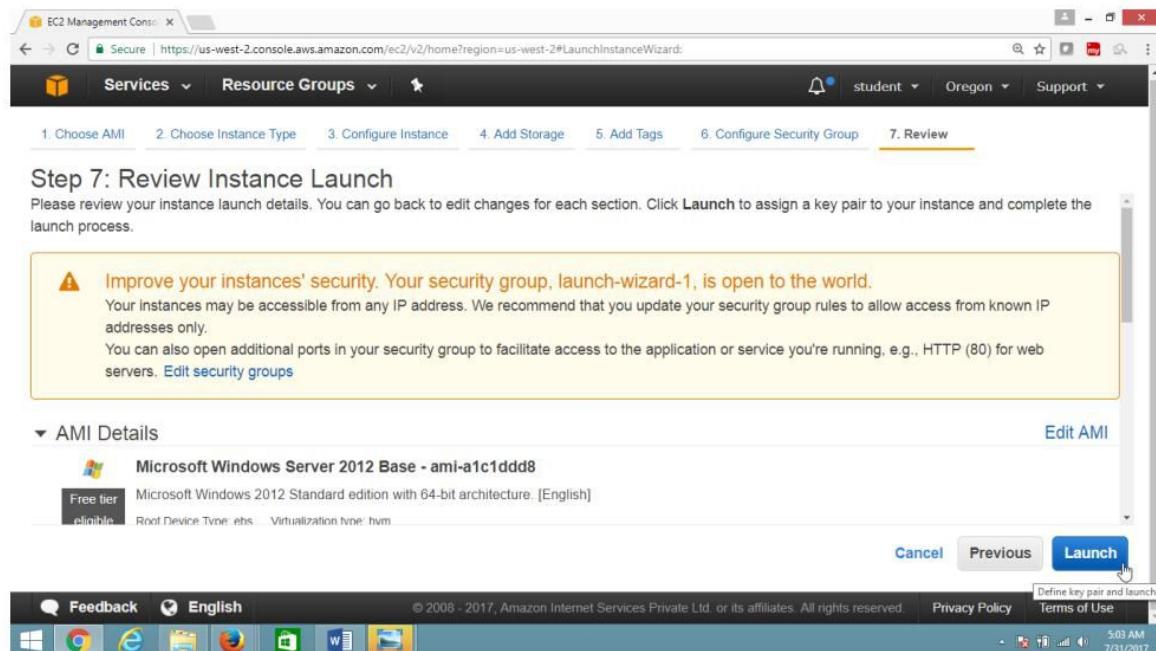
Take Default Values

Click on “Review and Launch” button



Drag down

Click on “Launch” button

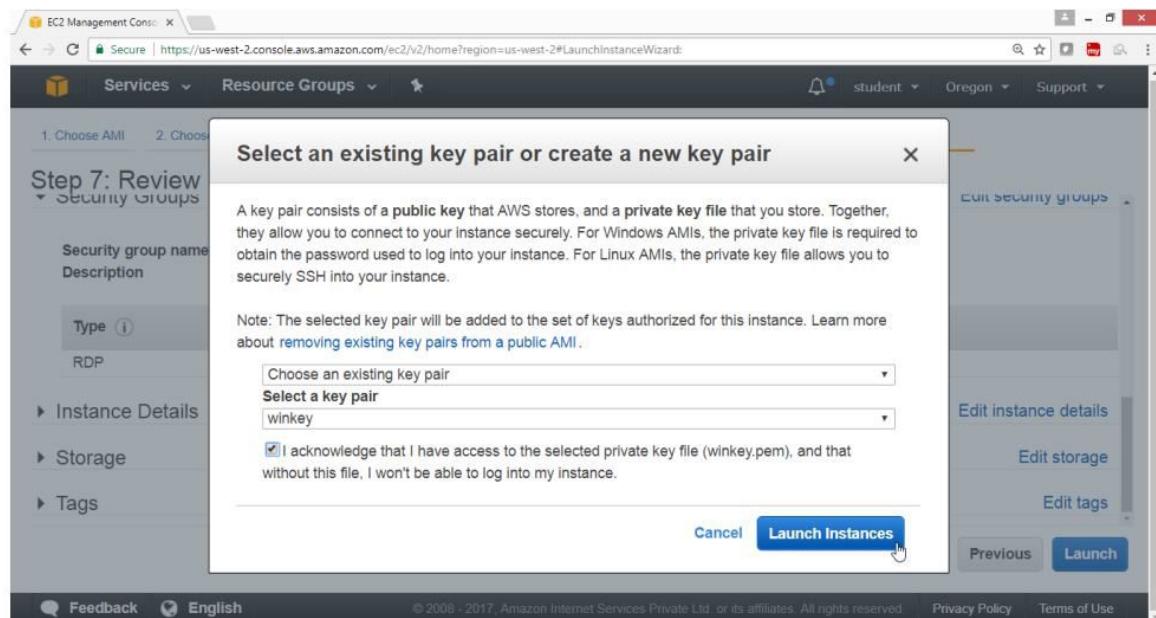


Select “Choose an existing key pair”

For “Key pair name” → winkey

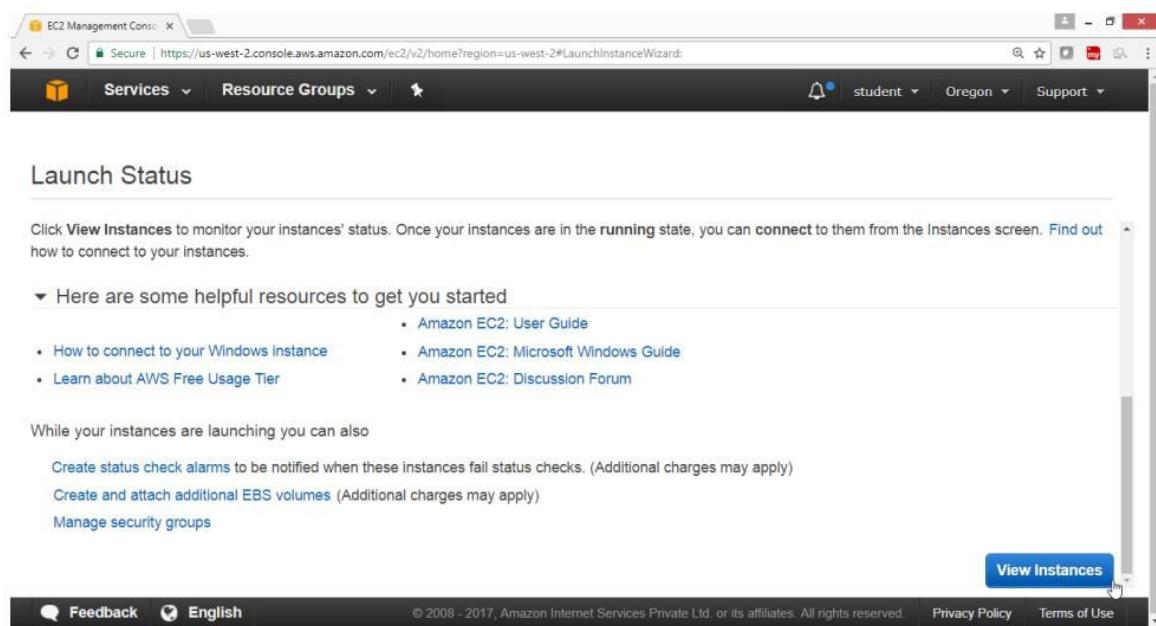
Select I acknowledge check box

Click on “Launch Instance” button

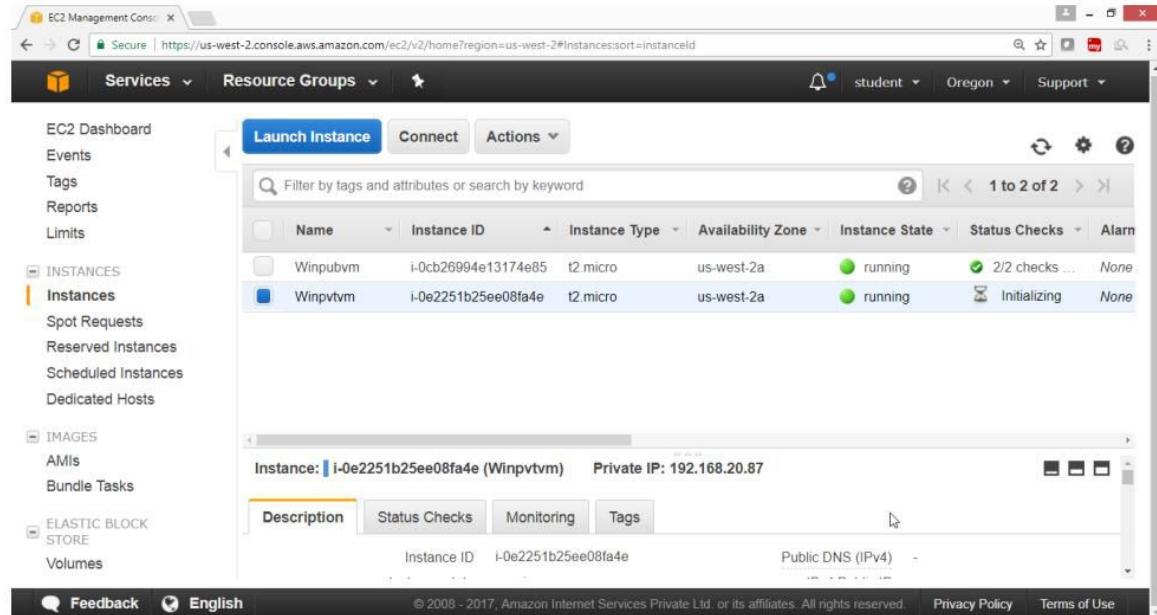


Check summary, Drag down

Click on “View Instance” button



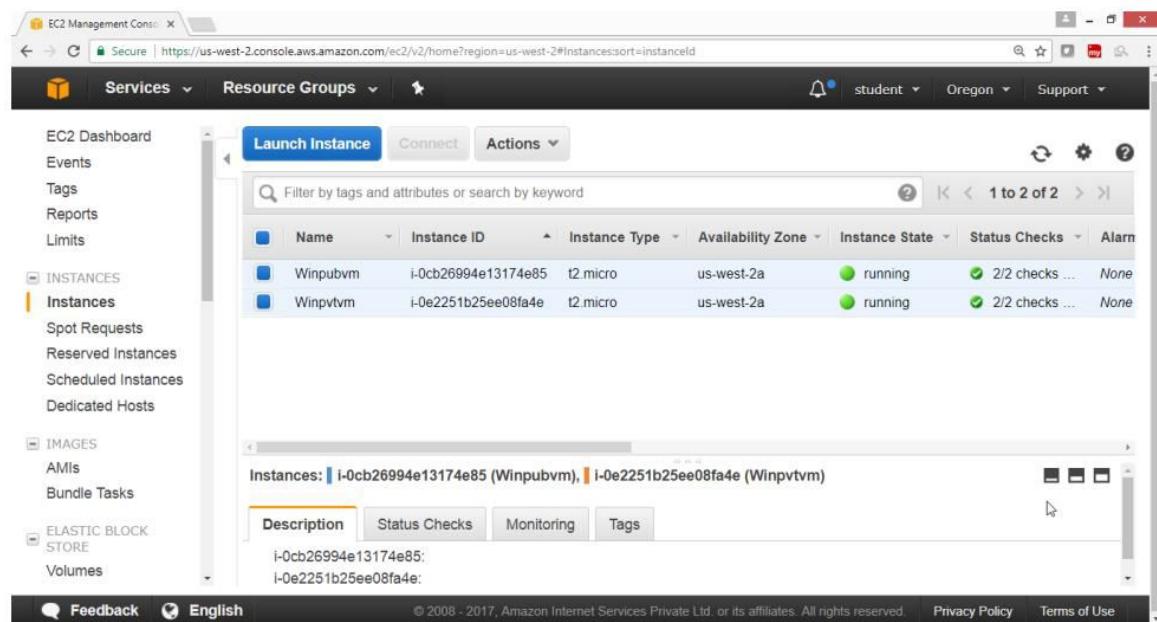
Verify that instance is Running



The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block Store. The 'Instances' section is currently selected. In the main content area, there's a table showing two instances. The first instance, 'Winpubvm', has an Instance ID of i-0cb26994e13174e85, is a t2.micro type, located in us-west-2a, and is running. The second instance, 'Winpvtvm', has an Instance ID of i-0e2251b25ee08fa4e, is also a t2.micro type, located in us-west-2a, and is in the process of initializing. Below the table, a detailed view for the second instance is shown, including its description (Instance: i-0e2251b25ee08fa4e (Winpvtvm), Private IP: 192.168.20.87), status checks (2/2 checks ...), monitoring, and tags.

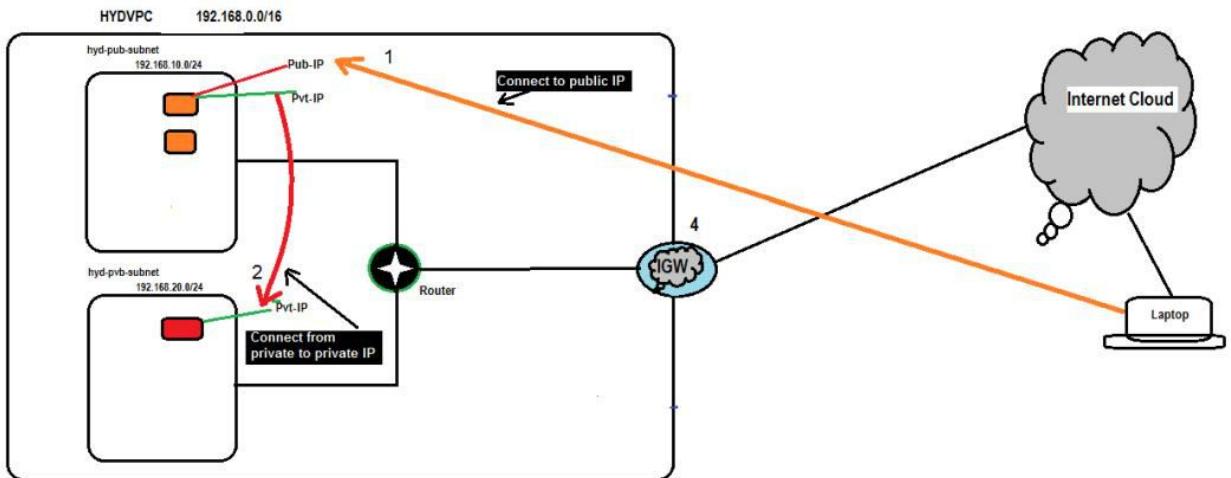
Verification

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 with the 'Instances' section selected. It displays the same two instances: 'Winpubvm' and 'Winpvtvm'. Both instances are listed as running in their respective availability zones. A detailed view for 'Winpubvm' is shown at the bottom, listing its instance ID (i-0cb26994e13174e85) and a note indicating it is in a public subnet (i-0cb26994e13174e85).

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

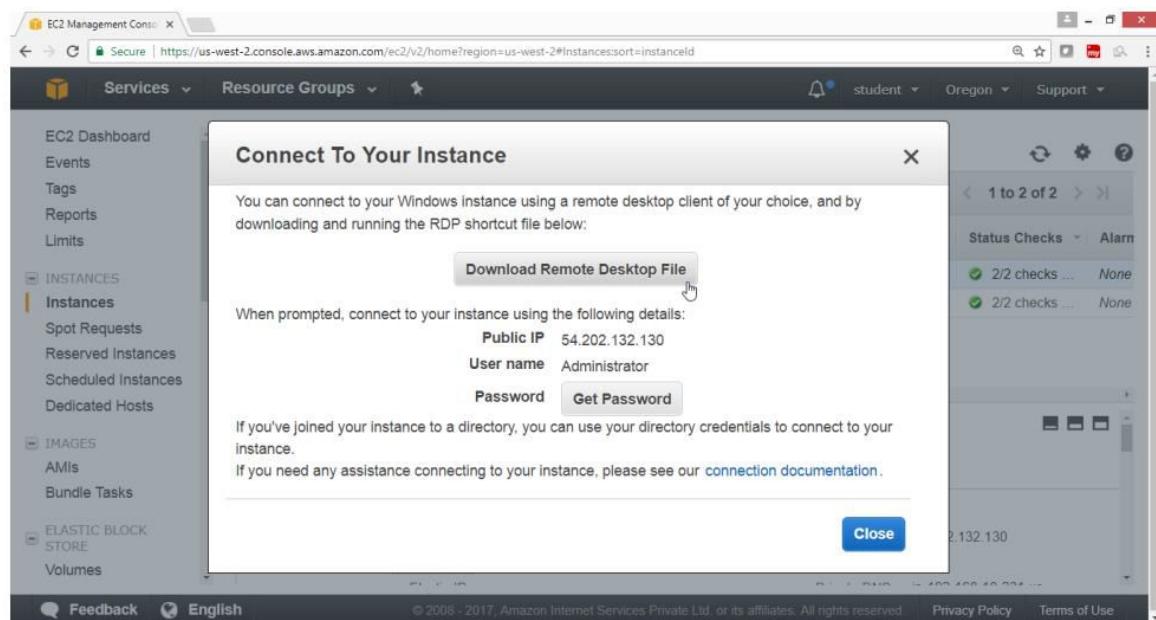
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Winpubvm	i-0cb26994e13174e85	t2.micro	us-west-2a	running	2/2 checks ...	None
Winpvvm	i-0e2251b25ee08fa4e	t2.micro	us-west-2a	running	2/2 checks ...	None

Click on "Connect" button

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
Winpvvm	i-0e2251b25ee08fa4e	t2.micro	us-west-2a	running	2/2 checks ...	None

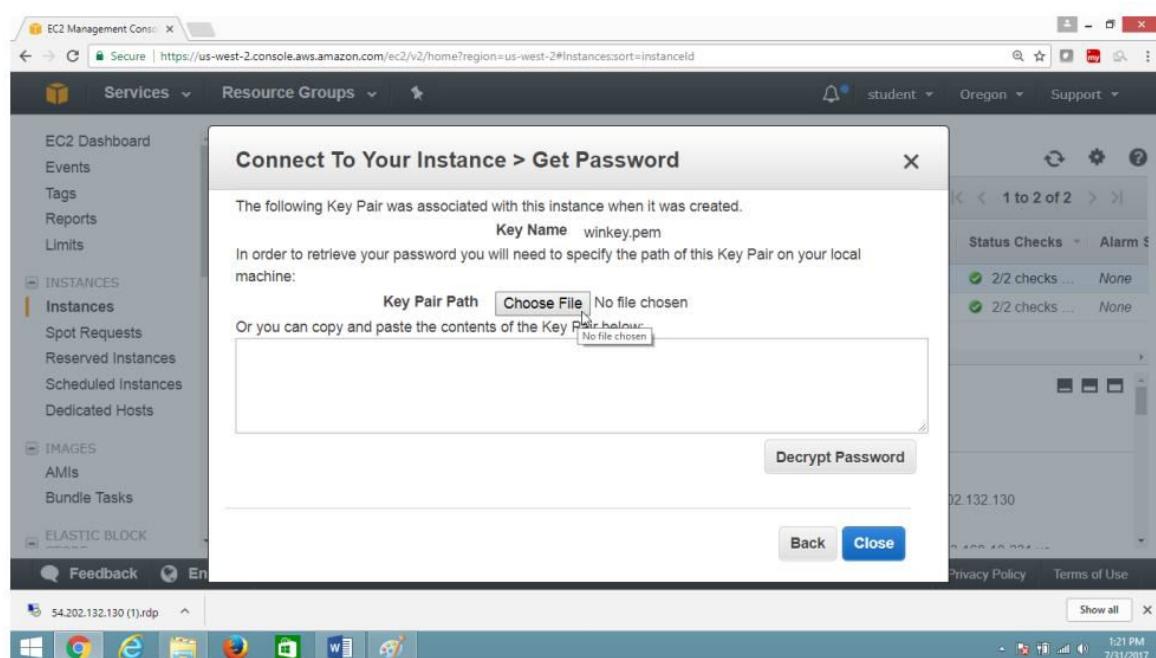
Click on “Download Remote Desktop file”

Click on “Get Password”



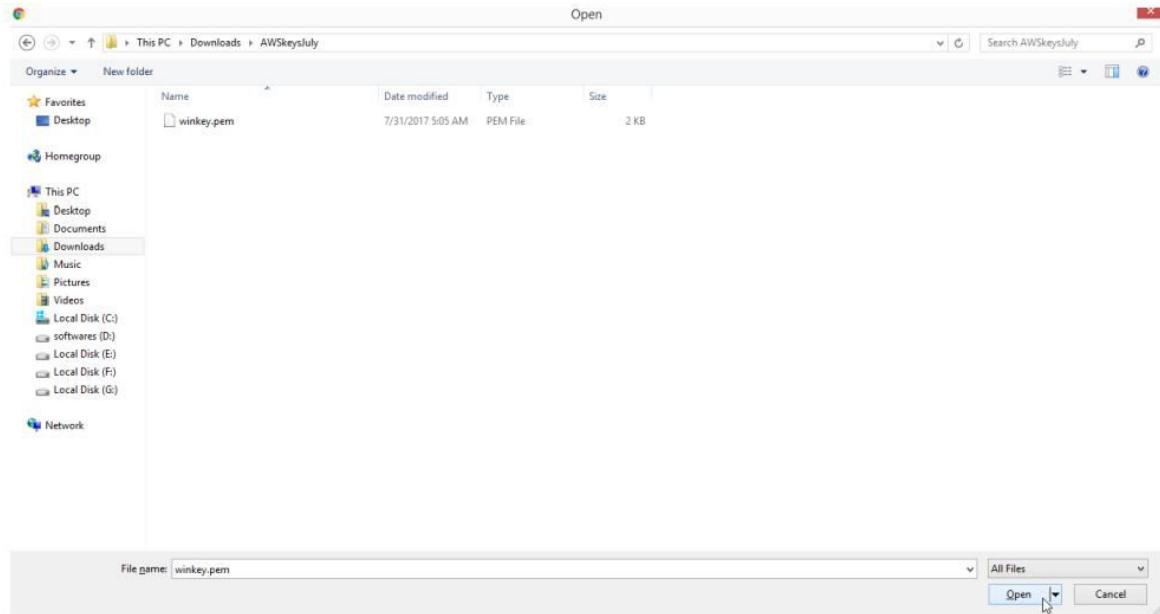
Provide the path of key file

Click on Choose file button

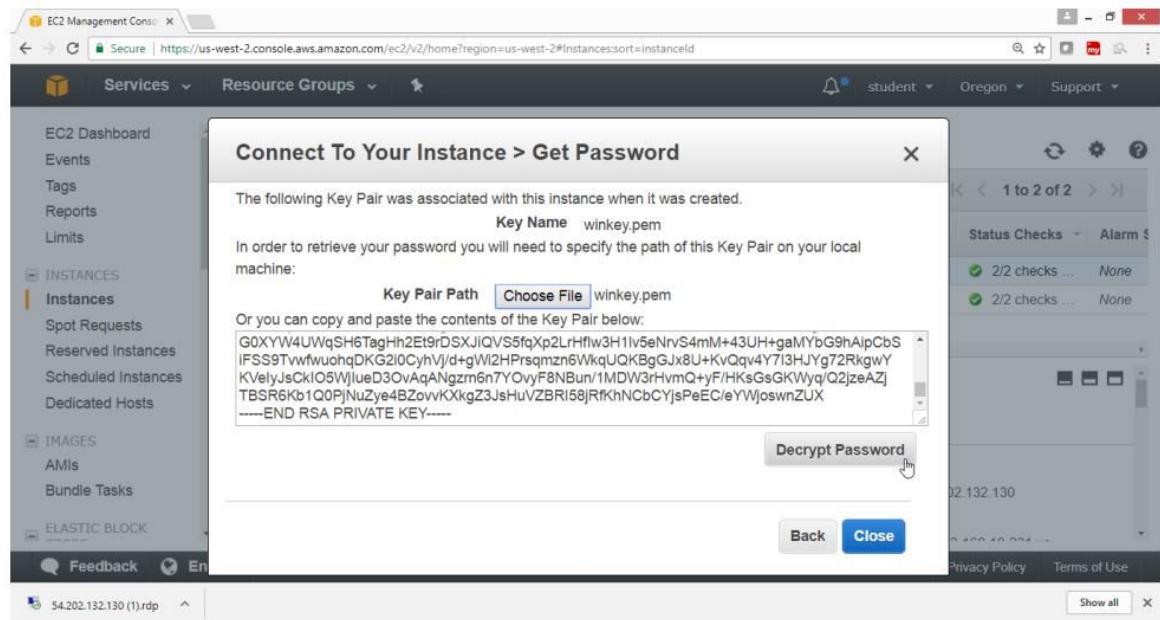


Select the key file

Click on **Open** button



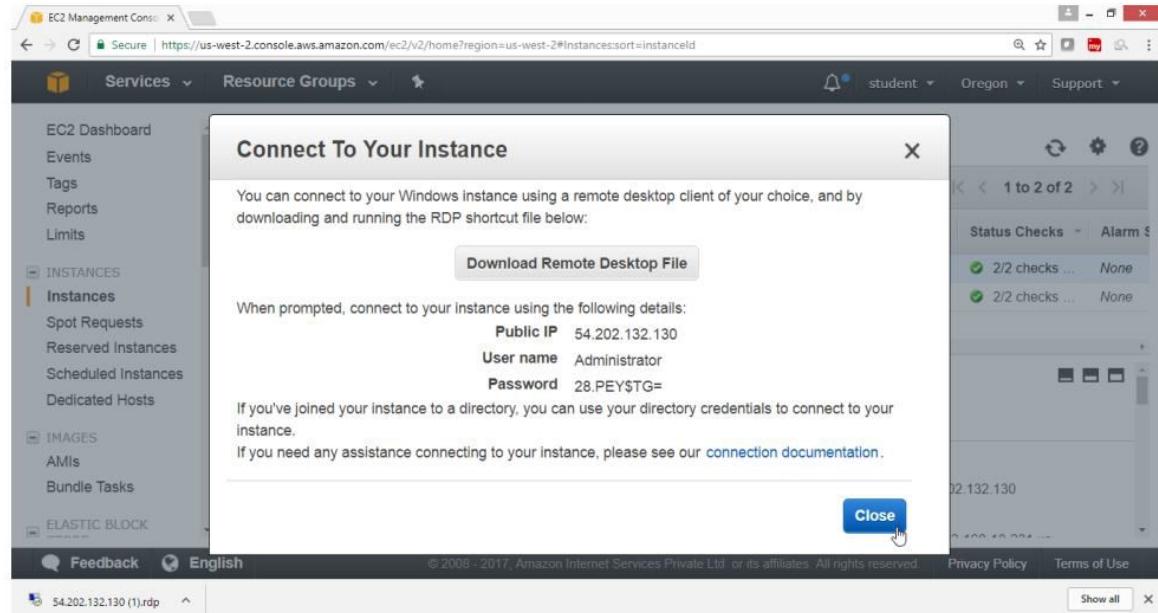
Now click on "Decrypt Password" button



Verification

Password is generated copy in notepad

Click on **Close** button



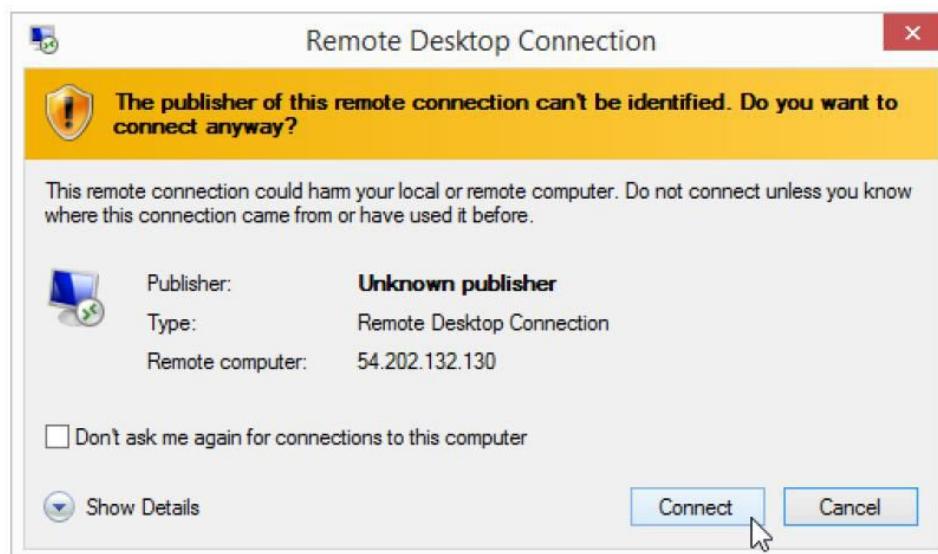
Double Click on RDP file

Provide Windows Username → Administrator

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

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with options like Services, Resource Groups, EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block Store. The Instances section is expanded, showing two instances: Winpubvm and Winpvtvm. Both instances are listed with their instance ID, type (t2.micro), availability zone (us-west-2a), state (running), and status checks (2/2 checks). The instance Winpubvm is currently selected. Below the instances, there are tabs for Description, Status Checks, Monitoring, and Tags. Under the Description tab, details are provided: Instance ID (i-0cb26994e13174e85), Instance state (running), Instance type (t2.micro), Public DNS (IPv4) (-), IPv4 Public IP (54.202.132.130), and IPv6 IPs (-). At the bottom of the main pane, there are buttons for Launch Instance, Connect, and Actions. The status bar at the bottom indicates the file '54.202.132.130 (1).rdp' is open. The taskbar at the very bottom shows the file '54.202.132.130 (1).rdp' and other icons.

Click on “Connect” button

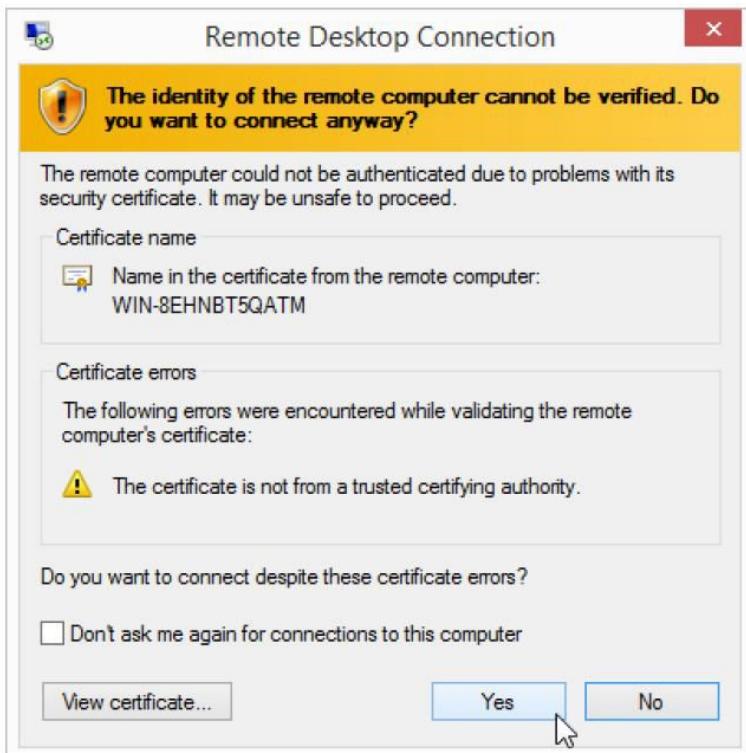


Paste the password

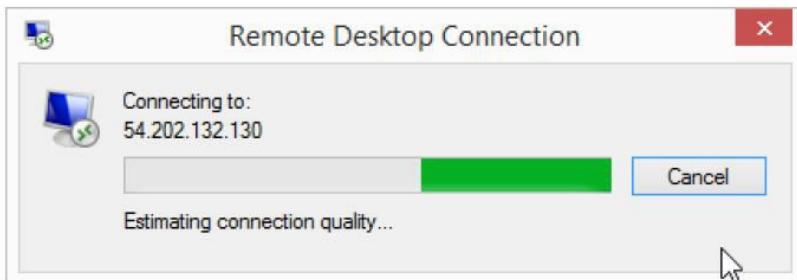
Click on **OK** button



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

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
Winpvtvm	i-0e2251b25ee08fa4e	t2.micro	us-west-2a	running	2/2 checks ...	None

Elastic IPs
Availability zone: us-west-2a
Security groups: launch-wizard-2, view inbound rules
Scheduled events: No scheduled events
AMI ID: Windows Server-

Private DNS: ip-192-168-20-87.us-west-2.compute.internal
Private IPs: 192.168.20.87
Secondary private IPs:
VPC ID: vpc-7d934d1b
Subnet ID: subnet-6abcbf23

Click on Connect button

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
Winpvtvm	i-0e2251b25ee08fa4e	t2.micro	us-west-2a	running	2/2 checks ...	None

Elastic IPs
Availability zone: us-west-2a
Security groups: launch-wizard-2, view inbound rules
Scheduled events: No scheduled events
AMI ID: Windows Server-

Private DNS: ip-192-168-20-87.us-west-2.compute.internal
Private IPs: 192.168.20.87
Secondary private IPs:
VPC ID: vpc-7d934d1b
Subnet ID: subnet-6abcbf23

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-----  
MIIEowlBAAKCAQEAsrhLs36UXn01lHgG/mv0QHxJMq6p3NPPFedup5gUUYge2z8j8QQf1sn2AKs  
Ye9PBAwBxMwlhdUPy0GbIRuBSI7CYOcTkdXjpuhTgG2Ylnkpxuql0BYkw3n9B3AMDmVbSyvrenC  
Lcg05A1sSSmOtTrBqUqkoANQZa+uZO7xDEkQS3G6rTft6XTtcjcio5Wp4erJfMPneJYCdg7ui/Rm  
TCdbD9m8h/ND5+nqajv80X3QSrOGyTddRf29/M1VRh1/FXdi7NV+qK6n3te/lmP2ZP4OIH6uiFuY
```

Verify

IP and password of private subnet instance 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

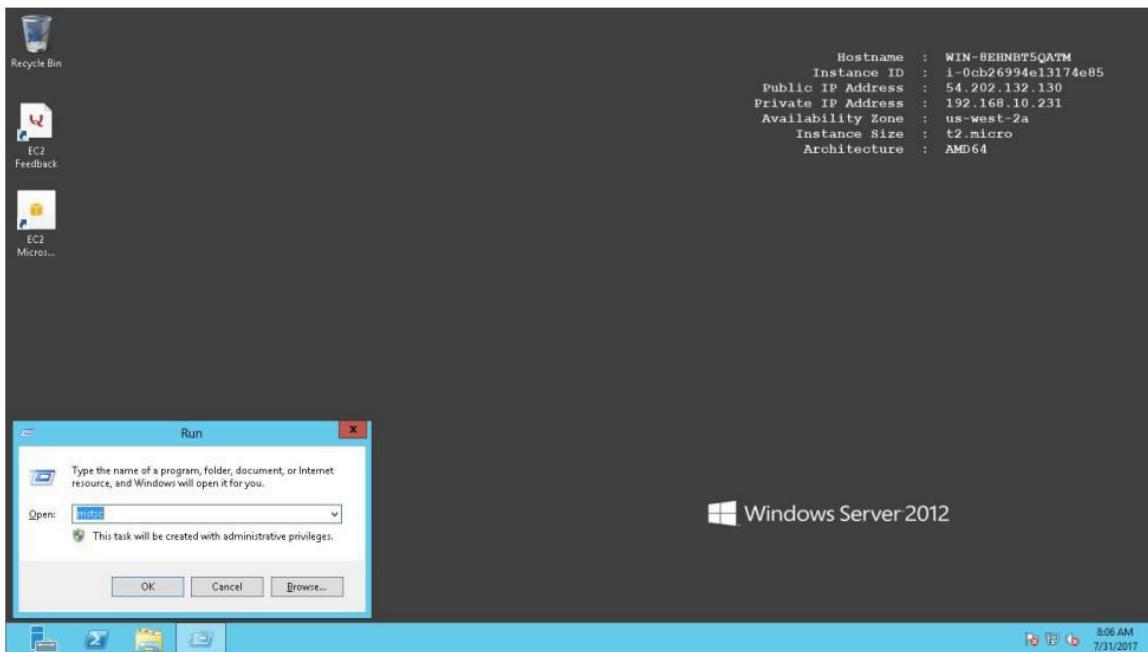
Password G-oV;n\$.@i

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

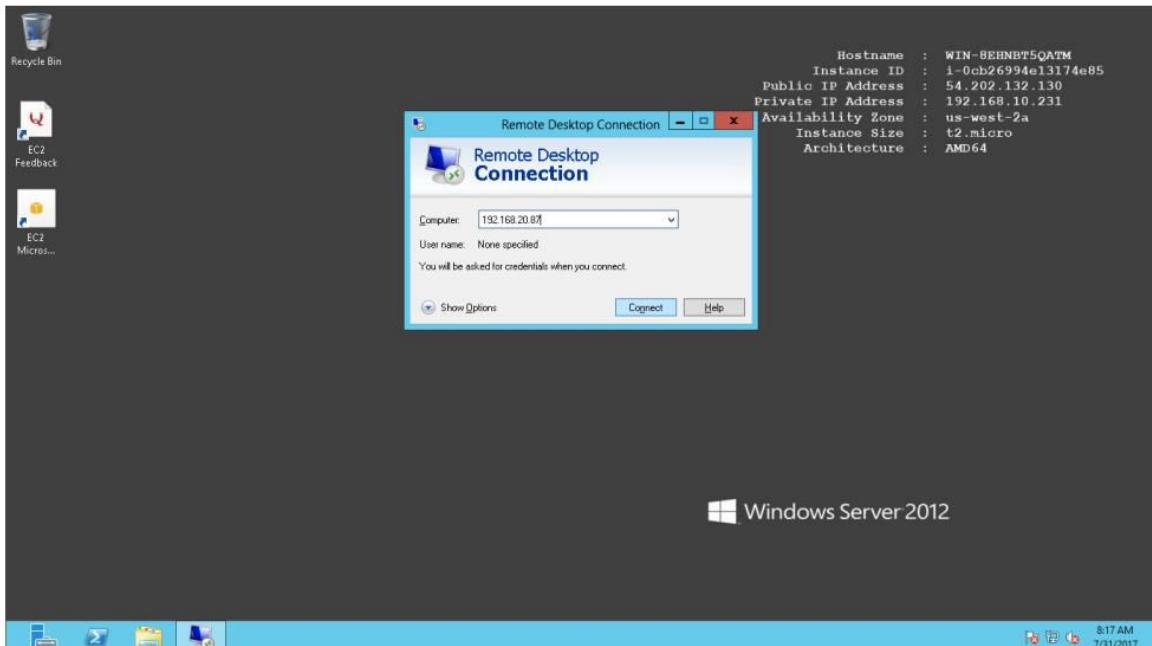


Provide private instance

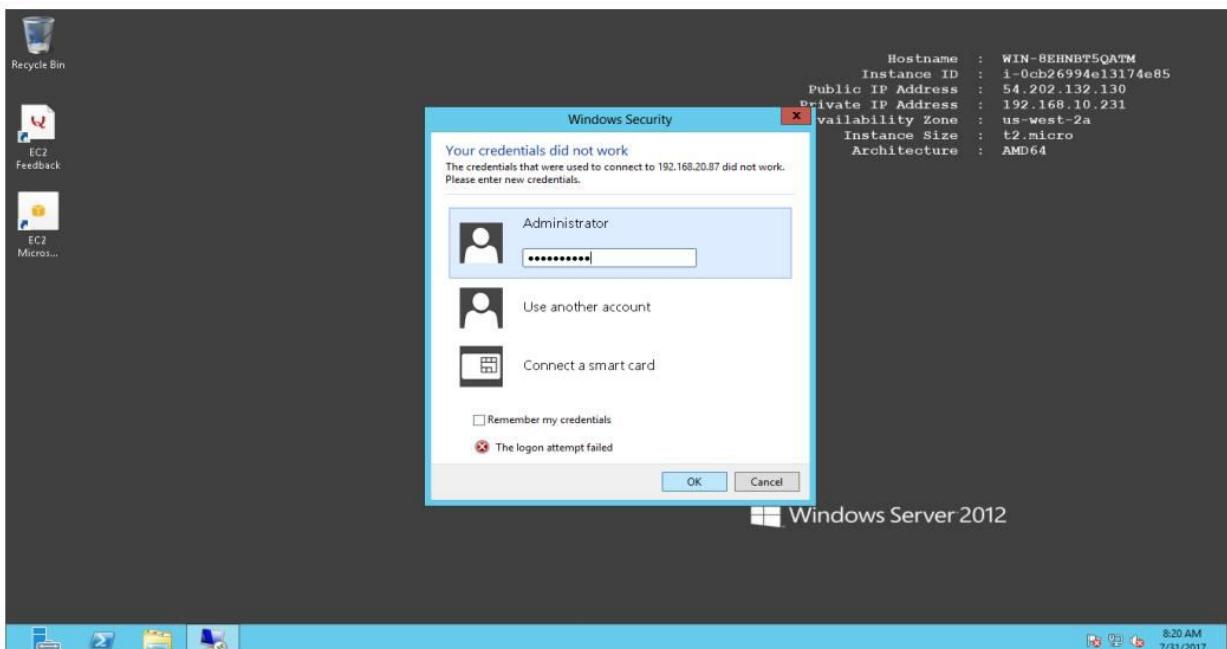
Private IP → 192.168.20.87

Username → Adminsitrator

Password → G-oV;n\$.@i



Now Provide Username & password



Verification

Check private IP at Right top corner

Now you are connected to windows private instance.



11) To connect to linux instance in private subnet

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

Open the AWS console

Click on Services

Click on Instance

Click on “Launch Instance” button

The screenshot shows the AWS EC2 Management Console interface. The left sidebar has categories like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Images, AMIs, and Elastic Block Store. The main 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 Status. The table contains four rows:

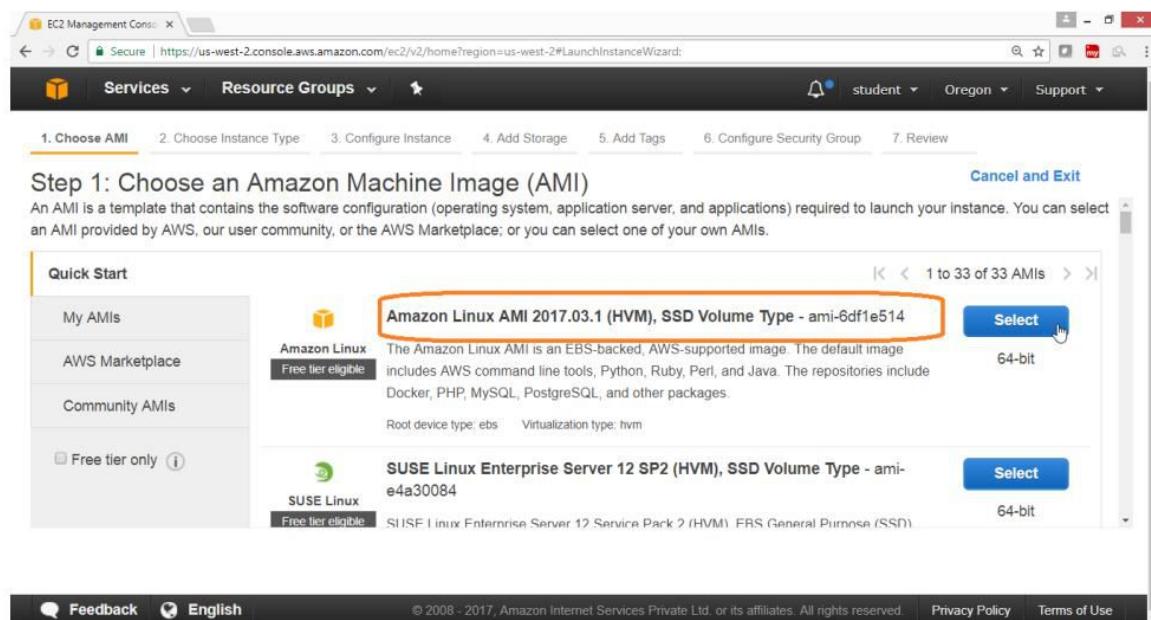
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
linuxvm1	i-08115df0bd38c247a	t2.micro	us-west-2c	terminated		None
win2008vm1	i-0a145faa160320894	t2.micro	us-west-2c	terminated		None
Winpubvbm	i-0cb26994e13174e85	t2.micro	us-west-2a	running	2/2 checks ...	None

At the bottom, there's a note "Select an instance above" and links for Feedback, English, Privacy Policy, and Terms of Use.

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 EC2 Management Console interface. The user is at Step 1: Choose an Amazon Machine Image (AMI). A list of AMIs is displayed, with the "Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-6df1e514" entry highlighted by a red box. To the right of this entry is a blue "Select" button, which has a cursor pointing to it, indicating it is being clicked. Other entries in the list include "SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami-e4a30084". The interface includes a sidebar for "Quick Start" with options like "My AMIs", "AWS Marketplace", and "Community AMIs". The top navigation bar shows "Services", "Resource Groups", and other AWS services like "student", "Oregon", and "Support". The bottom of the screen includes standard AWS footer links for "Feedback", "English", "Privacy Policy", and "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 EC2 Management Console interface. The title bar says "EC2 Management Console". The URL is "https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard". The top navigation bar includes "Services", "Resource Groups", "student", "Oregon", and "Support". Below the navigation is a progress bar with steps: 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. The main content area is titled "Step 2: Choose an Instance Type". It displays a table of instance types:

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	Moderate	No

At the bottom of the table are buttons: "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 EC2 Management Console interface. The URL in the browser is https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard. The top navigation bar includes 'Services' (selected), 'Resource Groups', and user information. Below the navigation is a progress bar with steps 1 through 7. Step 3, 'Configure Instance', is highlighted.

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.

Form fields shown:

- Number of instances: 1
- Purchasing option: Request Spot instances (unchecked)
- Network: vpc-7d934d1b | HYDVPC
- Subnet: subnet-b3bdbea | hyd-pub-subnet | us-west-2a
- Auto-assign Public IP: Enable
- IAM role: None

Buttons at the bottom:

- Cancel
- Previous
- Review and Launch** (highlighted)
- Next: Add Storage

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

On the “Add Storage” page

Leave the values as default

Click on “Next: Add Tags” button

The screenshot shows the AWS EC2 Management Console interface. The title bar says "EC2 Management Console". The URL is "https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard". The top navigation bar includes "Services", "Resource Groups", "student", "Oregon", and "Support". Below the navigation, a progress bar shows steps 1 through 7: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (highlighted in yellow), 5. Add Tags, 6. Configure Security Group, 7. Review.

Step 4: Add Storage

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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-0e8e196a52ed7efc3	8	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	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 and conditions.](#)

Buttons at the bottom: Cancel, Previous, **Review and Launch** (highlighted in blue), and [Next: Add Tags](#).

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

On the “Add Tags” page

Key → Name

Value → Linuxpubvm

Click on “Next: Configure Security Group” button

The screenshot shows the AWS EC2 Management Console interface. At the top, there's a navigation bar with tabs like Services, Resource Groups, and a user profile. Below the navigation, a progress bar indicates the steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (which is currently selected), 6. Configure Security Group, and 7. Review. The main content area is titled "Step 5: Add Tags". It contains a table with two columns: "Key" and "Value". The "Key" column has a placeholder "(127 characters maximum)". The "Value" column has a placeholder "(255 characters maximum)". Below these columns are two checkboxes: "Instances" and "Volumes", each with an information icon. Underneath the table, there's a text input field labeled "Name" containing "Linuxpubvm", with a small "x" icon to its right. Below the input field is a button labeled "Add another tag" followed by the text "(Up to 50 tags maximum)". At the bottom of the page, there are several buttons: "Cancel", "Previous", "Review and Launch" (which is highlighted in blue), and "Next: Configure Security Group" (which has a hand cursor icon over it). At the very bottom, there are links for "Feedback", "English", and some legal notices.

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

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 top navigation bar includes 'Services', 'Resource Groups', and 'Oregon'. Below the navigation is a progress bar with steps 1 through 7: Choose AMI, Choose Instance Type, Configure Instance, Add Storage, Add Tags, Configure Security Group (which is highlighted), and Review. The main content area is titled 'Step 6: Configure Security Group'. It explains what a security group is and how to add rules. A note says 'You can create a new security group or select from an existing one below.' Below this, there are two radio buttons: 'Create a new security group' (selected) and 'Select an existing security group'. The 'Security group name' field contains 'launch-wizard-5'. The 'Description' field contains 'launch-wizard-5 created 2017-08-01T13:31:54.220+05:30'. A table shows a single rule: Type: SSH, Protocol: TCP, Port Range: 22, Source: Anywhere. At the bottom are 'Cancel', 'Previous', and 'Review and Launch' buttons. The 'Review and Launch' button is highlighted with a mouse cursor.

On the “Review Instance Launch” page

Click on **Launch** button

The screenshot shows the AWS EC2 Management Console with the same URL as the previous screenshot. The progress bar shows steps 1 through 7. The main content area is titled 'Step 7: Review Instance Launch'. It says '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.' Below this is a yellow warning box with an exclamation mark icon. It says: '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](#)'.

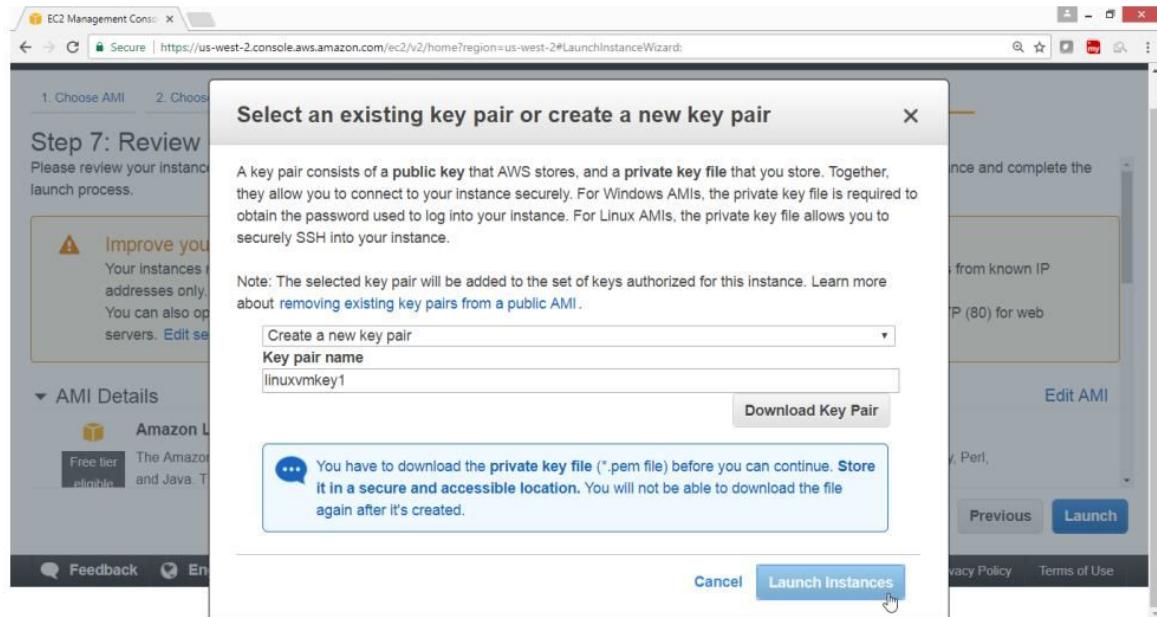
At the bottom, there is an expanded section titled 'AMI Details' with a 'Edit AMI' button. It shows 'Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-6df1e514'. A note says 'The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.' Below this are 'Cancel', 'Previous', and 'Launch' buttons. The 'Launch' button is highlighted with a mouse cursor.

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



Launch Status

how to connect to your instances.

▼ Here are some helpful resources to get you started

- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)

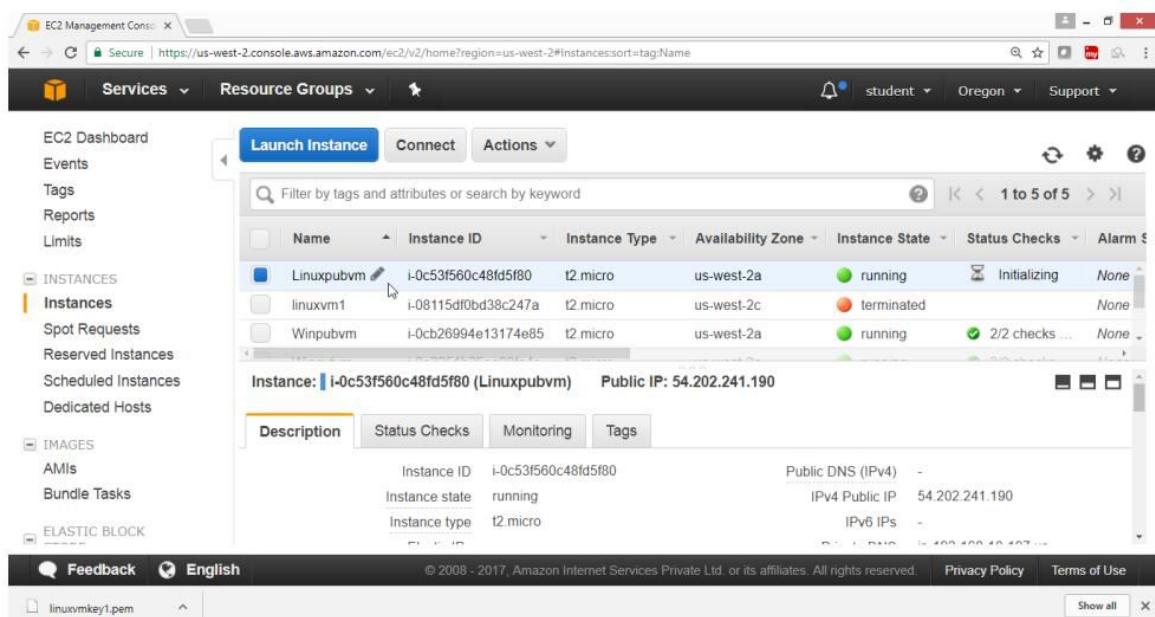
Create and attach additional EBS volumes (Additional charges may apply)

Manage security groups



Verification

Linux instance in public subnet is launched



12) To connect to linux instance in private subnet

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

Open the AWS console

Click on Services

Click on Instance

Click on “Launch Instance” button

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (which is selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images (AMIs, Bundle Tasks), and Elastic Block. The main 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 S. There are three rows: 1. Linuxpubvm (selected), Instance ID i-0c53f560c48fd5f80, t2.micro, us-west-2a, running, Initializing, None. 2. linuxvm1, Instance ID i-08115df0bd38c247a, t2.micro, us-west-2c, terminated. 3. Winpubvm, Instance ID i-0cb26994e13174e85, t2.micro, us-west-2a, running, 2/2 checks, None. Below the table, it says "Instance: i-0c53f560c48fd5f80 (Linuxpubvm) Public IP: 54.202.241.190". At the bottom, there are tabs for Description, Status Checks, Monitoring, and Tags, with the Status Checks tab selected. It also shows detailed information: Instance ID i-0c53f560c48fd5f80, Instance state running, Instance type t2.micro, Public DNS (IPv4) 54.202.241.190, IPv4 Public IP 54.202.241.190, and IPv6 IPs. At the very bottom, there are links for Feedback, English, Privacy Policy, Terms of Use, and a "Show all" link.

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 EC2 Management Console interface. The URL in the address bar is <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard>. The top navigation bar includes 'Services' and 'Resource Groups'. On the left, a sidebar titled 'Quick Start' lists 'My AMIs', 'AWS Marketplace', 'Community AMIs', and a checkbox for 'Free tier only'. The main content area is titled 'Step 1: Choose an Amazon Machine Image (AMI)'. It displays a list of 33 AMIs, with the first one selected: 'Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-6df1e514'. This item is highlighted with a dashed border and includes a 'Free tier eligible' badge. A detailed description of the AMI is provided, mentioning it's EBS-backed, AWS-supported, and includes Docker, PHP, MySQL, PostgreSQL, and other packages. The 'Select' button is visible next to the description. Below this, another AMI entry for 'SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami...' is partially visible. The bottom of the page includes standard AWS footer links for Feedback, English, Privacy Policy, Terms of Use, and a 'Show all' link.

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 EC2 Management Console interface. The title bar says "EC2 Management Console". The URL is "https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard". The top navigation bar includes "Services", "Resource Groups", "student", "Oregon", "Support", and a search bar. Below the navigation is a progress bar with steps: 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. The main content area is titled "Step 2: Choose an Instance Type". It displays a table of instance types:

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

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

Below the table, the footer includes "Feedback", "English", "© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.", "Privacy Policy", "Terms of Use", and "Show all".

On the “Configure Instance Details” page

- Number of instance → 1
- Network → HYDVPC
- Subnet → hyd-pvt-subnet
- Auto-assign Public IP → Disable

The screenshot shows the AWS EC2 Management Console interface. The URL in the browser is <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard>. The top navigation bar includes 'Services', 'Resource Groups', and user information. Below the navigation, a progress bar shows steps 1 through 7: Choose AMI, Choose Instance Type, Configure Instance (which is highlighted), Add Storage, Add Tags, Configure Security Group, and 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

Purchasing option: Request Spot instances

Network: vpc-7d934d1b | HYDVPC

Subnet: subnet-6abcbf23 | hyd-pvt-subnet | us-west-2a
250 IP Addresses available

Auto-assign Public IP: Disable

Buttons at the bottom: Cancel, Previous, **Review and Launch**, Next: Add Storage

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

On the “Add Storage” page

Leave the values as default

Click on “Next: Add Tags” 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 top navigation bar includes 'Services', 'Resource Groups', 'student', 'Oregon', and 'Support'. Below the navigation is a progress bar with steps 1 through 7: Choose AMI, Choose Instance Type, Configure Instance, Add Storage (highlighted in yellow), Add Tags, Configure Security Group, and Review. The main content area is titled 'Step 4: Add Storage' with the sub-instruction: '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 current storage configuration:

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-0e8e196a52ed7efc3	8	General Purpose	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Buttons at the bottom include 'Add New Volume', 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Add Tags'.

Click on Add Tag

The screenshot shows the AWS EC2 Management Console with the same URL and navigation as the previous screenshot. The progress bar highlights step 5: Add Tags. The main content area is titled 'Step 5: Add Tags' with the sub-instruction: '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.' A table allows adding tags:

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

Instructions below the table say: 'Choose the Add tag button or click to add a Name tag. Make sure your IAM policy includes permissions to create tags.' A button labeled 'Add Tag' is highlighted with a mouse cursor. Other buttons include 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Configure Security Group'. The footer includes 'Feedback', 'English', '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', 'Terms of Use', and 'Show all'.

On the “Add Tags” page

Key → Name

Value → Linuxpvtvm

Click on “Next: Configure Security Group” button

The screenshot shows the AWS EC2 Management Console interface. At the top, there's a navigation bar with tabs like 'Services', 'Resource Groups', and 'Support'. Below the navigation bar, a progress bar indicates the steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (which is highlighted), 6. Configure Security Group, and 7. Review. The main content area is titled 'Step 5: Add Tags'. It contains instructions: 'A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.' Below this, it says '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.' There's a table where a tag is being added: 'Key' (Name) and 'Value' (Linuxpvtvm). The table has columns for 'Instances' and 'Volumes'. At the bottom of the form, there's a link 'Add another tag' and a note '(Up to 50 tags maximum)'. At the very bottom of the page, there are links for 'Feedback', 'English', and 'Privacy Policy', along with copyright information: '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' and 'Terms of Use'.

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, ::/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

Instance Details Edit instance details

Storage Edit storage

Tags Edit tags

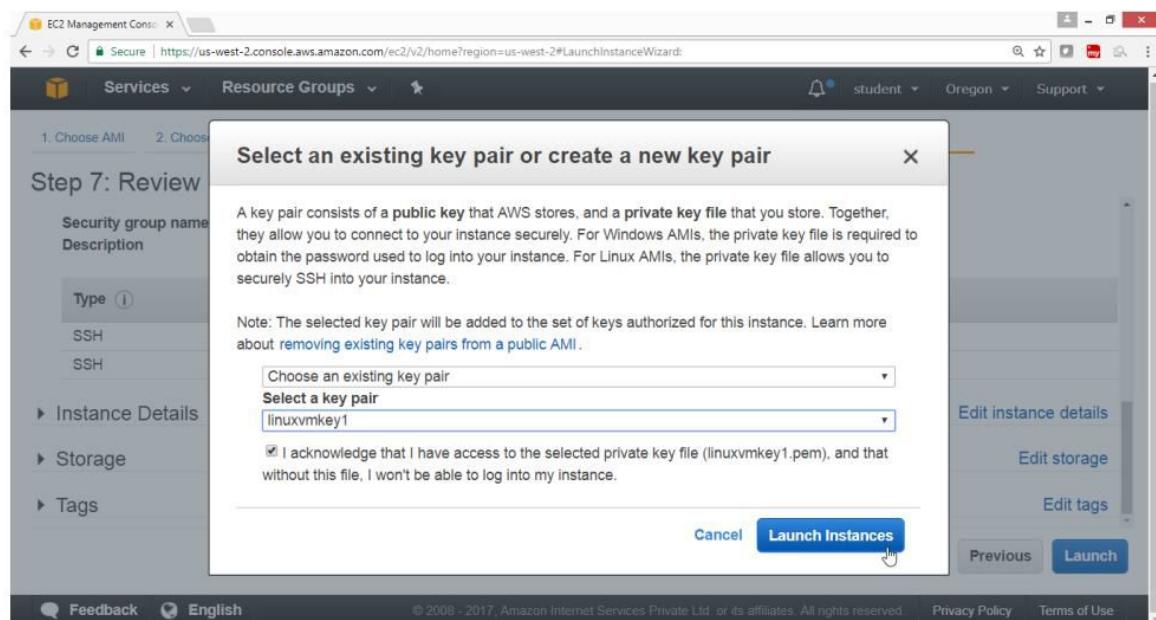
Cancel Previous Launch

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 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 message at the top states: "Your instances are launching, and it may take a few minutes until they are in the running state, which they will be ready for you to use. Usage counts on your free resources will start immediately and continue to accrue until you stop or terminate your instances." Below this, a section titled "Here are some helpful resources to get you started" lists links to "How to connect to your Linux instance", "Amazon EC2 User Guide", "Learn about AWS Free Usage Tier", and "Amazon EC2 Discussion Forum". A note below says "While your instances are launching you can also" followed by links to "Create status check alarms", "Create and attach additional EBS volumes", and "Manage security groups". At the bottom right is a blue "View Instances" button.

Verification

Linux instance in public subnet is launched

The screenshot shows the EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#instances:sort=desc:tag:Name>. The left sidebar shows navigation options like EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES, IMAGES, and ELASTIC BLOCK. The main area has tabs for "Launch Instance", "Connect", and "Actions". A search bar at the top of the main area says "Filter by tags and attributes or search by keyword". Below it is a table titled "Instances" with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, and Status Checks. The table lists four instances: Winpvtvm, Winpubvbm, Linuxpvtvm (which is highlighted with a blue cursor), and Linupubvbm. The Linuxpvtvm instance is shown as "running" with "2/2 checks ...". Below the table, a message says "Instance: i-0da6594c71079c242 (Linuxpvtvm) Private IP: 192.168.20.101". At the bottom are tabs for "Description", "Status Checks", "Monitoring", and "Tags". The "Status Checks" tab is selected, showing details for the instance: Instance ID i-0da6594c71079c242, Instance state running, Public DNS (IPv4) -, and IPv4 Public IP -. The footer includes links for Feedback, English, Privacy Policy, and Terms of Use.

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

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block Store. The 'Instances' section is currently selected. The main area displays a table of running instances:

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
Linuxpvtvmm	i-0da6594e71079c242	t2.micro	us-west-2a	running	2/2 checks ...	None
Winpubvm	i-0cb26994e13174e85	t2.micro	us-west-2a	running	2/2 checks ...	None
Winpvtvmm	i-0e2251b25ee08fa4e	t2.micro	us-west-2a	running	2/2 checks ...	None

Below the table, the instance details for 'Linuxpubvm' are shown:

Instance ID	i-0c53f560c48fd5f80	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	54.202.241.190
Instance type	t2.micro	IPv6 IPs	-

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#Instances:sort=tag:Name>. The left sidebar shows 'Instances' selected under 'Services'. The main panel displays the 'Connect To Your Instance' wizard. It asks if you want to connect with a standalone SSH client (radio button selected) or a Java SSH Client directly from your browser (Java required). Below this, instructions for connecting via SSH are provided:

- Open an SSH client. (find out how to [connect using PuTTY](#))
- Locate your private key file (linuxvmkey1.pem). The wizard automatically detects the key you used to launch the instance.
- Your key must not be publicly viewable for SSH to work. Use this command if needed:
chmod 400 linuxvmkey1.pem
- Connect to your instance using its Public IP:
54.202.241.190

Below these instructions is an example command:

```
ssh -i "linuxvmkey1.pem" ec2-user@54.202.241.190
```

A note states: 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.

The right sidebar shows the Oregon region with status checks and alarms. The status checks table shows four items, all of which are green (2/2 checks ...). The alarm table shows four items, all of which are green (None).

Use the above public ip of linux instance in mobaxterm

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

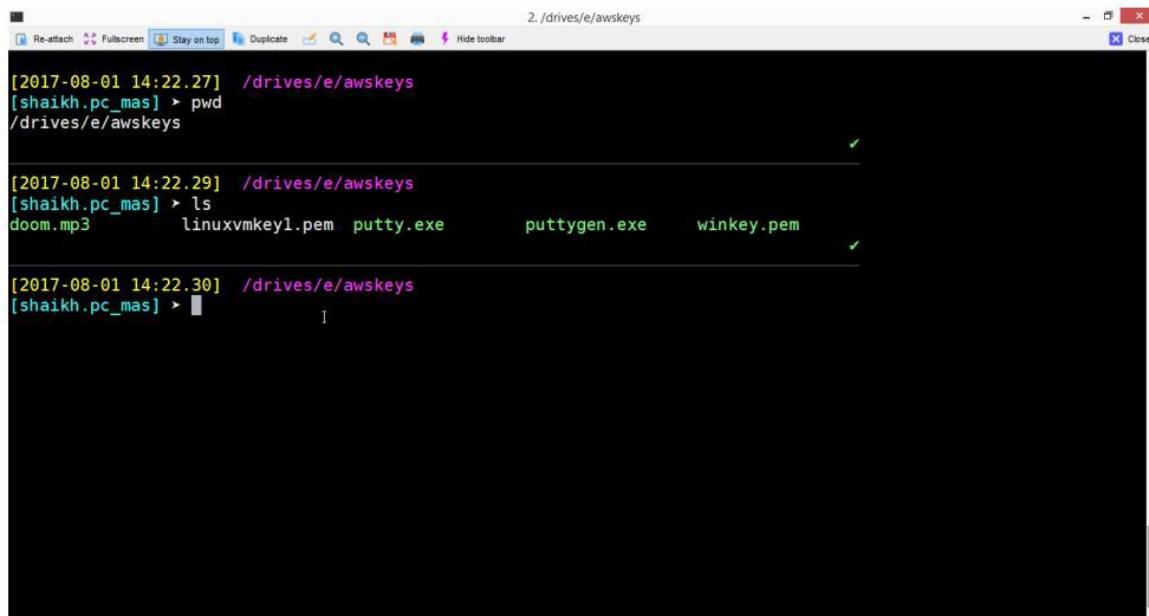
```
[2017-08-01 14:21:18] /drives/e/awskeys
[shaikh_pc_mas] > ls
doom.mp3      linuxvmkey1.pem  putty.exe      puttygen.exe    winkey.pem

[2017-08-01 14:21:20] /drives/e/awskeys
[shaikh_pc_mas] > scp -i "linuxvmkey1.pem" linuxvmkey1.pem ec2-user@54.202.241.190:/home/ec2-user
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

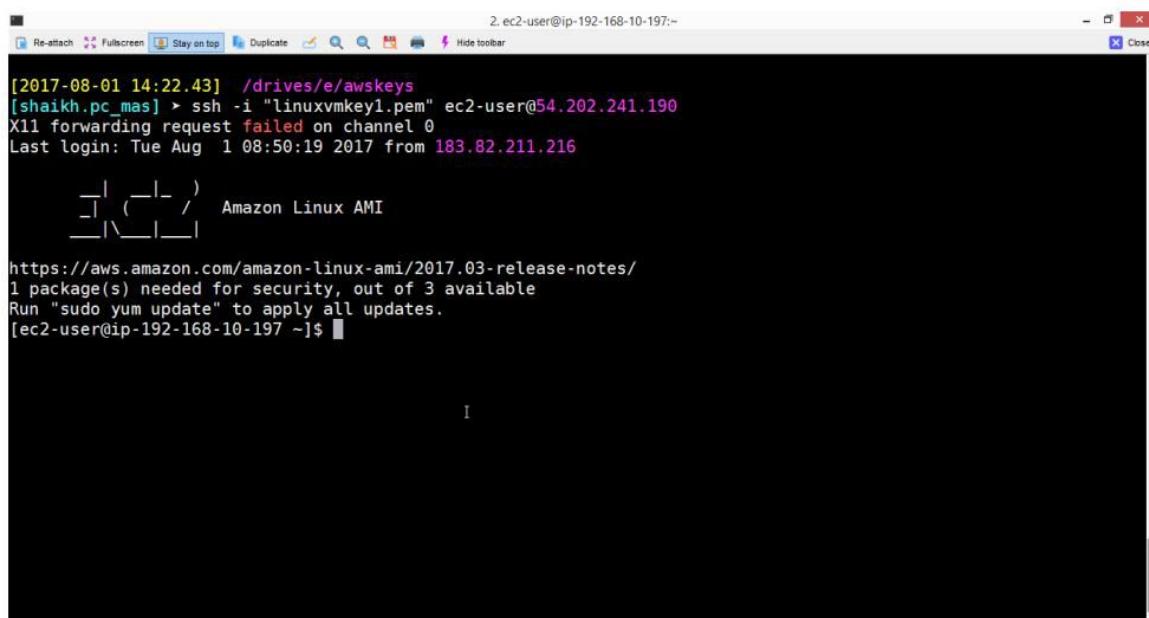


```
[2017-08-01 14:22.27] ./drives/e/awskeys
[shaikh.pc_mas] > pwd
./drives/e/awskeys

[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



```
[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]
[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 interface. On the left, there's a navigation sidebar with options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block Store. The 'Instances' section is currently selected. The main area displays a table of running instances. One instance, 'Linuxpvtvm' (Instance ID: i-0da6594c71079c242), is highlighted with a blue selection bar. Below the table, the instance details are expanded:

Description		Status Checks	Monitoring	Tags
Instance ID	i-0da6594c71079c242	Public DNS (IPv4)	-	
Instance state	running	IPv4 Public IP	-	
Instance type	t2.micro	IPv6 IPs	-	

At the bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use.

View the details of private instance

The screenshot shows a modal dialog box titled 'To access your instance:' which appears when an instance is selected. The dialog 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.

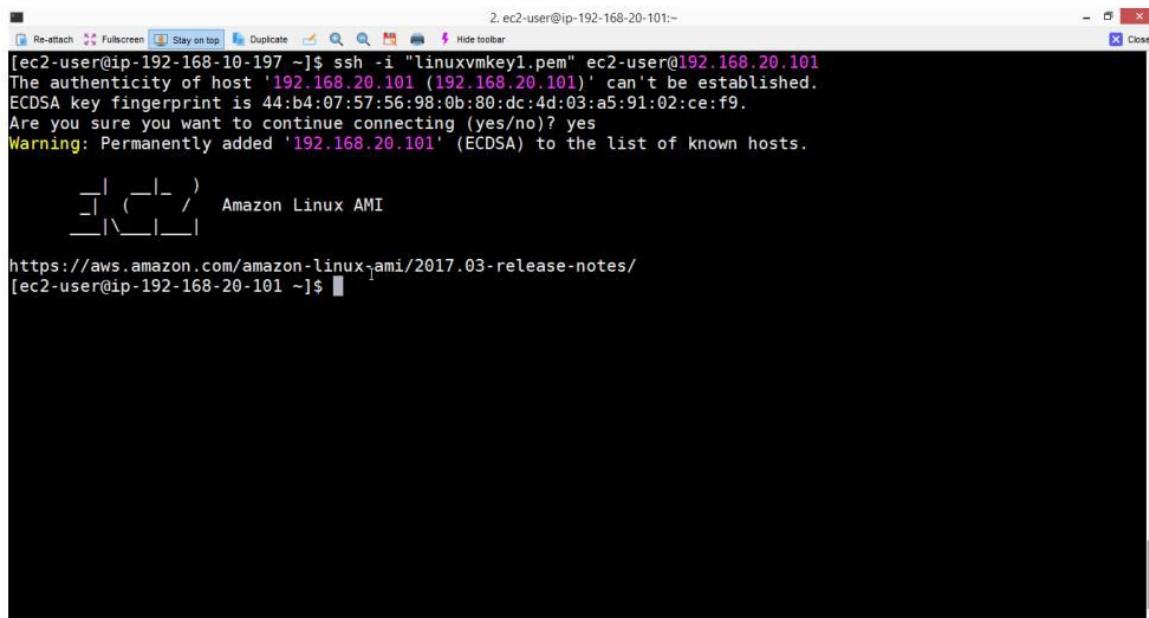
If you need any assistance connecting to your instance, please see our [connection documentation](#).

At the bottom right of the dialog is a 'Close' button.

Verification

Run ssh command to login to private instance

Now you are connected to private instance in private subnet



The screenshot shows an SSH 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:b4:07:57:56:98:0b: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' (ECDSA) to the list of known hosts.

[ec2-user@ip-192-168-20-101 ~]$
```

The terminal window has a toolbar at the top with icons for Re-attach, Fullscreen, Stay on top, Duplicate, Hide toolbar, and Close. The title bar also includes the session identifier "2. 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

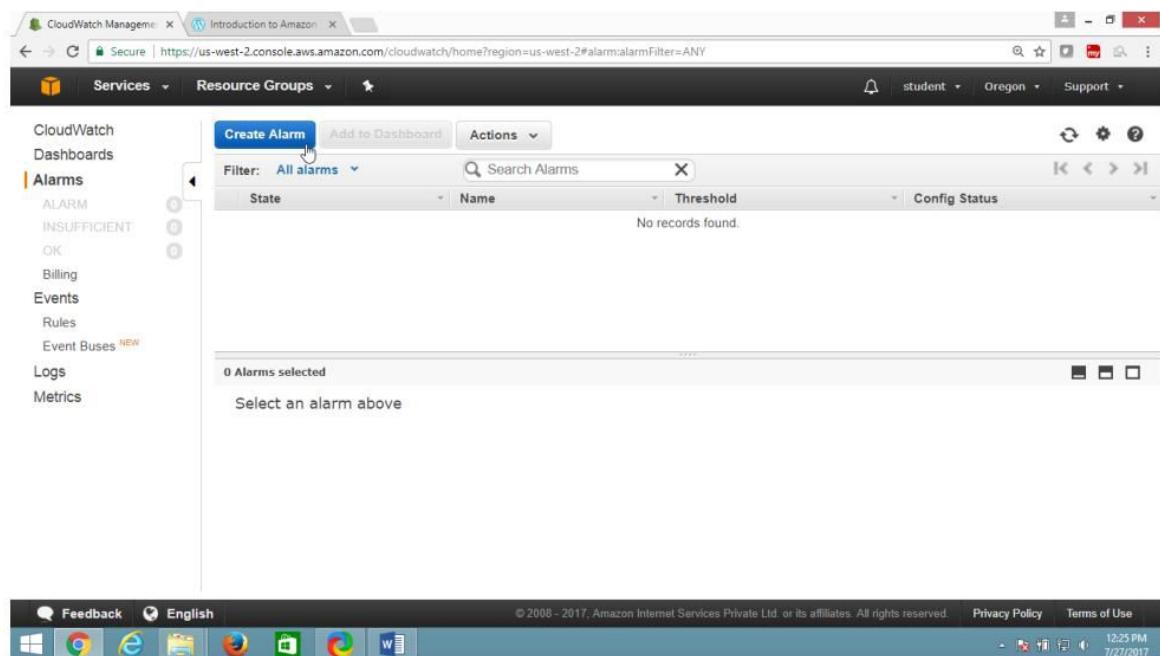
Click on CloudWatch

The screenshot shows the AWS Management Console interface. At the top, there are tabs for 'AWS Management Console' and 'Introduction to Amazon'. Below the tabs, the URL is https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2. The navigation bar includes 'Services' and 'Resource Groups'. On the left, a sidebar lists various AWS services under categories like Compute, Storage, and Database. The 'CloudWatch' icon, which is orange and green, is highlighted with a mouse cursor. In the main content area, 'CloudWatch' is listed under 'Management Tools' with the sub-option 'Monitor Resources and Applications' also highlighted. To the right, there's a 'Resource Groups' section with a 'Create a Group' button, and a 'Additional Resources' section with links to 'Getting Started', 'AWS Console Mobile App', 'AWS Marketplace', and 'AWS re:Invent Announcements'. The bottom of the screen shows the Windows taskbar with icons for File Explorer, Task View, Start, Task Manager, and others.

On “CloudWatch”, panel

Select Alarms

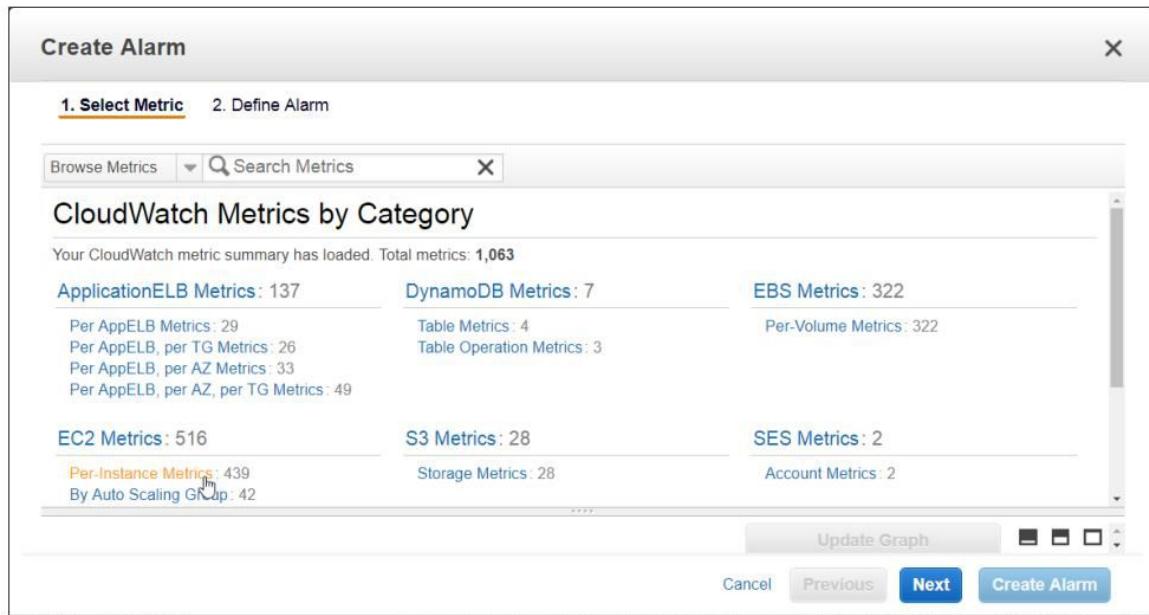
Click on “Create Alaram” button



In “Create Alarm” page

Select “EC2 Metrics”

Click on “Per-instance Metrics”



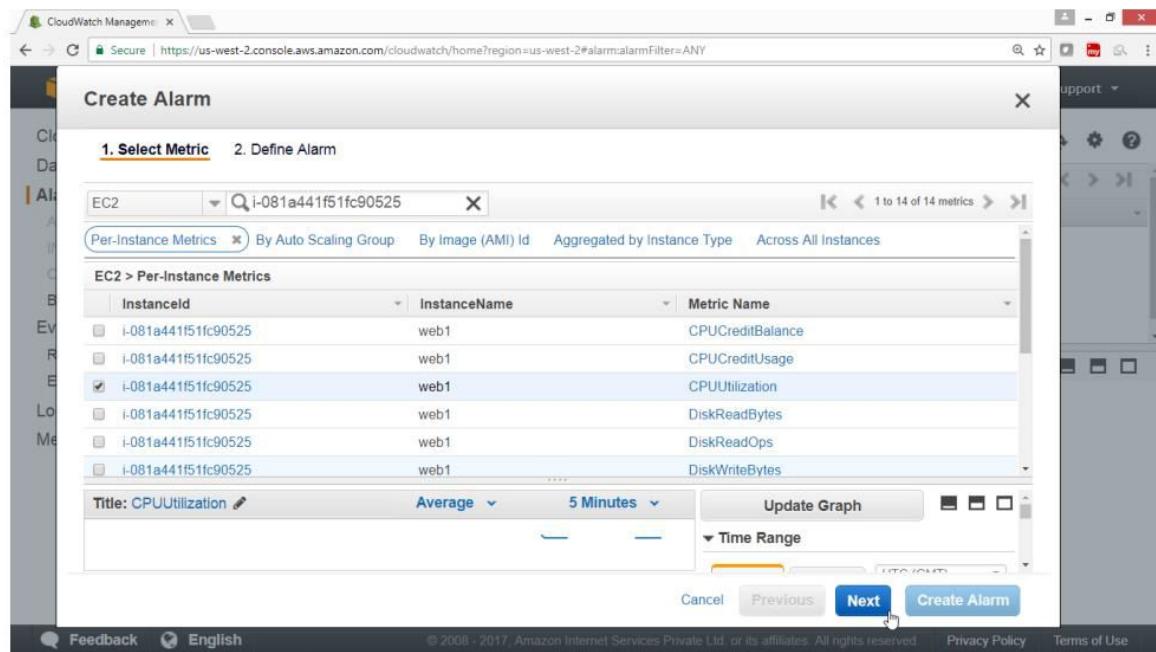
From “Create Alarm” page

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 AWS CloudWatch Metrics console. The current step is '2. Define Alarm'. The 'Alarm Threshold' section is configured with:

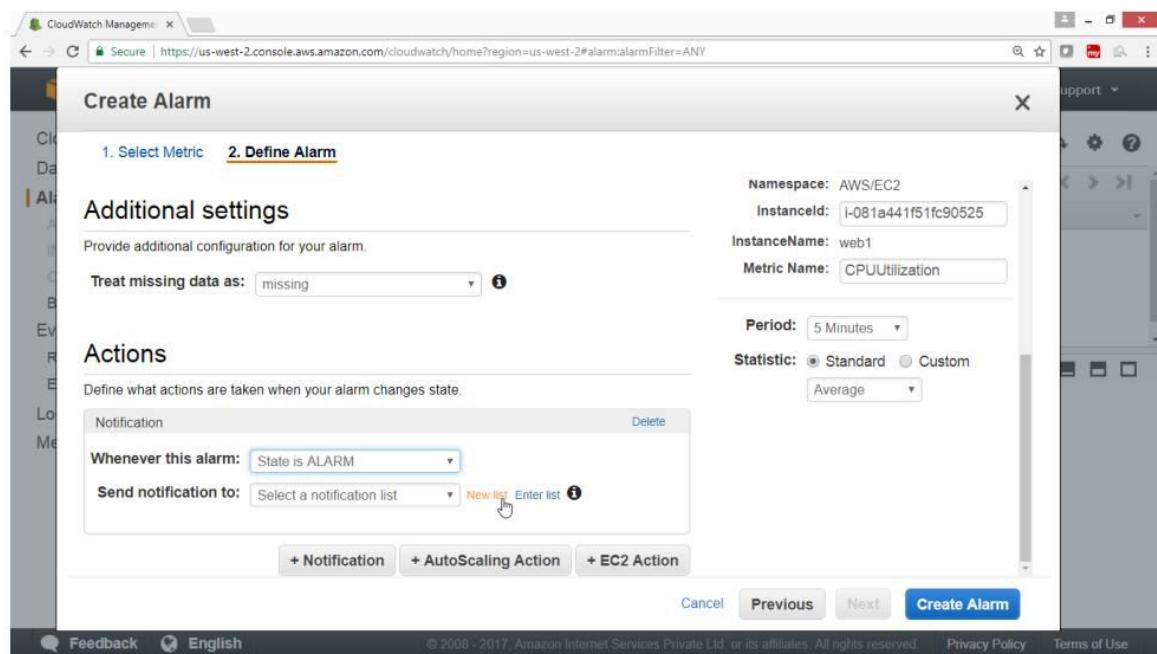
- Name:** testcpuutilization
- Description:** cputest1
- Whenever:** CPUUtilization
- is:** \geq 30
- for:** 1 consecutive period(s)

The 'Additional settings' section is collapsed. On the right, the 'Alarm Preview' section displays a line graph titled 'CPUUtilization \geq 0'. The graph shows a single sharp blue line spike reaching above the red threshold line at approximately 05:00 on July 27, 2017. The x-axis shows time from 05:00 to 07:00 on July 27, 2017. The y-axis ranges from 0 to 1.5. A legend indicates the blue line represents the metric value and the red line represents the threshold.

Under Actions

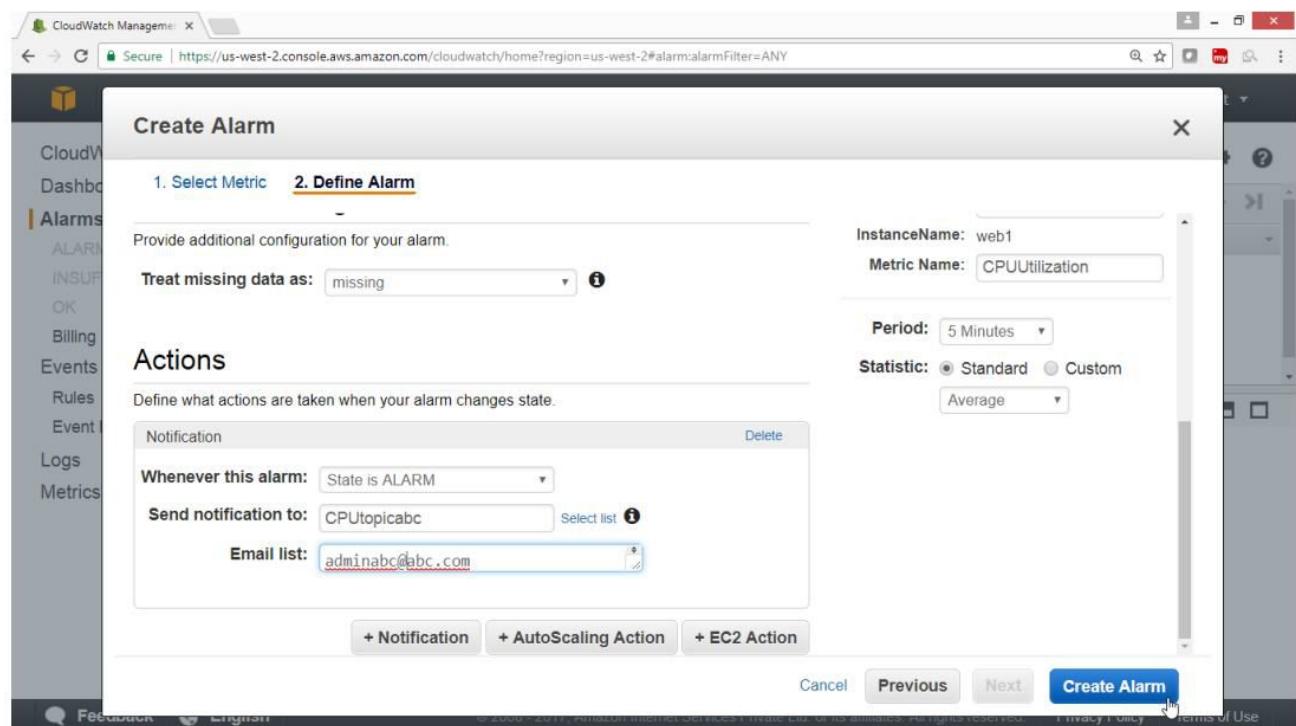
Whenever this alarm → State is Alaram

Send notification to → Click on New list

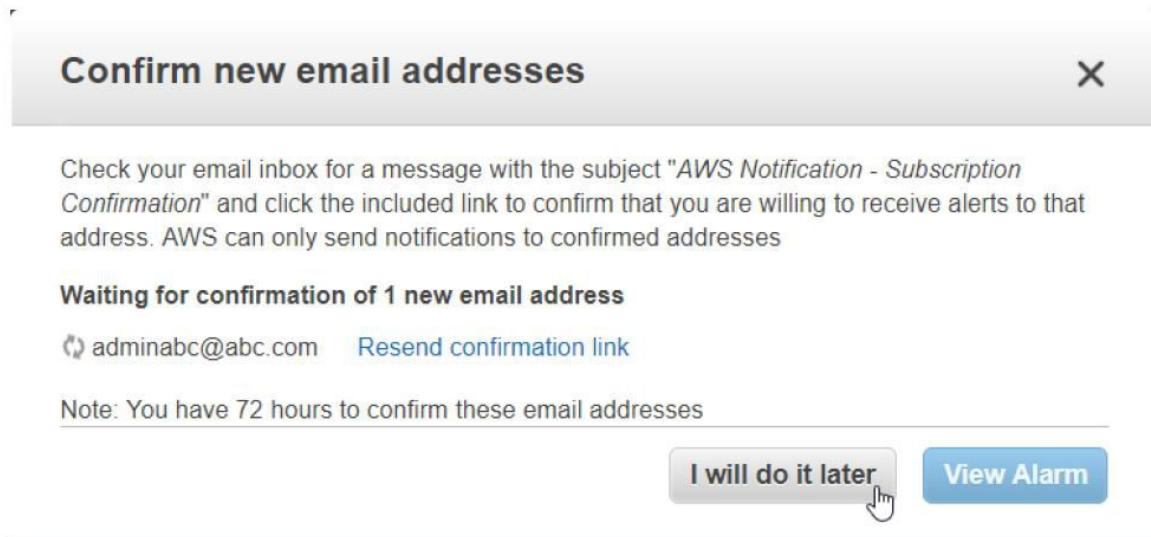


Send notification to → CPUtopicabc
Email → adminabc@abc.com

Click on “Create Alarm” 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 Alarms console. On the left sidebar, under the 'Alarms' section, there is a notification bubble indicating '1' new item. The main area displays a table of alarms:

State	Name	Threshold	Config Status
OK	testcpuitilization	CPUUtilization >= 30 for 5 minutes	Pending confirmation

A green success message at the top states: "Your alarm testcpuitilization has been saved." Below the table, it says "0 Alarms selected" and "Select an alarm above".

Open your email

The screenshot shows the Gmail inbox interface. At the top, there is a banner with the text "Click here to enable desktop notifications for Gmail. Learn more Hide". The inbox header includes "Gmail", "COMPOSE", and "Inbox (113)". Below the header, the inbox lists several categories: Primary (7 new), Social (7 new), Promotions (20 new), and AWS Notification - Subscri... (1:26 pm). A red box highlights the "AWS Notifications" category.

Click on “Confirm subscription”

=====

AWS Notification - Subscription Confirmation Inbox x  

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

to me ▼

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

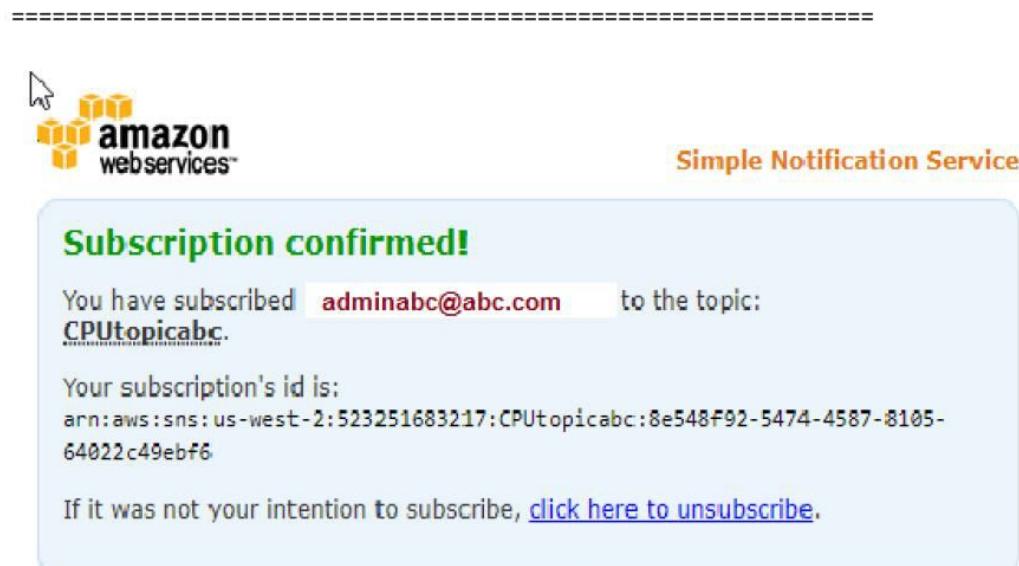
To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
[Confirm subscription](#) 

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 1:26 pm

=====

Verified by this output



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

CloudWatch Management X
Secure | https://us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2#alarm:alarmFilter=ANY

Services Resource Groups

CloudWatch Dashboards Alarms ALARM INSUFFICIENT OK Billing Events Rules Event Buses NEW Logs Metrics

Create Alarm Add to Dashboard Actions

Filter: All alarms Search Alarms

State	Name	Threshold	Config Status
OK	testcpuutilization	CPUUtilization >= 30 for 5 minutes	OK

0 Alarms selected Select an alarm above

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

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): 0.0%us, 0.0%sy, 0.0%ni, 100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 1017372k total, 166080k used, 851292k free, 9224k buffers
Swap: 0k total, 0k used, 0k free, 90380k cached

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

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

```
# stress --cpu 40 --timeout 1000
```

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

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

```
# top
```

Verify the output

Cpu load is 100%

top - 09:07:11 up 2:04, 3 users, load average: 16.16, 6.55, 2.88											
Tasks: 144 total, 41 running, 103 sleeping, 0 stopped, 0 zombie											
(Cpu(s):100.0%us, 0.0%sy, 0.0%ni, 0.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st)											
Mem: 101/372k total, 179324k used, 838048k free, 9460k buffers											
Swap: 0k total, 0k used, 0k free, 90760k cached											
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3143	root	20	0	7260	96	0 R	2.7	0.0	0:00.73	stress	
3147	root	20	0	7260	96	0 R	2.7	0.0	0:00.73	stress	
3179	root	20	0	7260	96	0 R	2.7	0.0	0:00.73	stress	
3141	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3142	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3144	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3145	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3146	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3148	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3149	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3150	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3151	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3152	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3153	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3154	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3155	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3156	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3157	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3158	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3159	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3160	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3161	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3162	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	
3163	root	20	0	7260	96	0 R	2.3	0.0	0:00.72	stress	

Go to CloudWatch service

Check the status

The screenshot shows the AWS CloudWatch Management Console. The left sidebar is titled 'CloudWatch' and includes links for Dashboards, Alarms, OK, Billing, Events, Rules, Event Buses, Logs, and Metrics. The 'Alarms' link is highlighted. The main content area is titled 'Alarm Summary' and displays a message: 'All your alarms are in OK state in US West (Oregon) region.' A 'Create Alarm' button is visible. Below this, there is a chart for an alarm named 'testcpuutilization' with the condition 'CPUUtilization >= 30'. The chart shows a constant value of 30 from 07:00 to 08:00 on July 27, followed by a sharp spike to approximately 35 at 09:00. The right sidebar shows 'Service Health' information for the Amazon CloudWatch Service, which is operating normally.

After 5 minutes Alarm is generated

This screenshot is identical to the one above, showing the 'Alarm Summary' page. However, the 'Alarms' link in the sidebar now has a red badge with the number '1', indicating a new alarm. The main content area now displays the message: 'You have 1 alarm in ALARM state in US West (Oregon) region.' The chart for 'testcpuutilization' now shows a constant value of 30 from 07:00 to 08:00 on July 27, followed by a sharp spike to approximately 60 at 09:00, indicating the alarm has triggered.

Go to email and check mail

The screenshot shows a Gmail inbox with the following details:

- Compose** button.
- Inbox (113)** link.
- Starred** and **Sent Mail** links.
- Primary**, **Social** (7 new), and **Promotions** (20 new) tabs.
- AWS Notifications** (2 new) folder.
- Two emails from "AWS Notifications" are listed:
 - ALARM: "testcpuuitlization" in US West - Oregon** (2:39 pm)
 - AWS Notification - Subscription Confirmation** (2:02 pm)

Click on mail

Verify output

=====

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

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

View this alarm in the AWS Management Console:

<https://console.aws.amazon.com/cloudwatch/home?region=us-west-2#s=Alarms&alarm=testcpuuitlization>

Alarm Details:

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

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

Threshold:

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

Monitored Metric:

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

State Change Actions:

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

↳ State Change Actions:

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

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:

[https://sns.us-west-2.amazonaws.com/unsubscribe.html?](https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:523251683217:CPUtopicabe:e8d238f8-8e77-46ec-8b2f-609f9ba26876&Endpoint=adminabc@abc.com)

[SubscriptionArn=arn:aws:sns:us-west-2:523251683217:
CPUtopicabe:e8d238f8-8e77-46ec-8b2f-609f9ba26876&
Endpoint=adminabc@abc.com](https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:523251683217:CPUtopicabe:e8d238f8-8e77-46ec-8b2f-609f9ba26876&Endpoint=adminabc@abc.com)

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at

<https://aws.amazon.com/support>

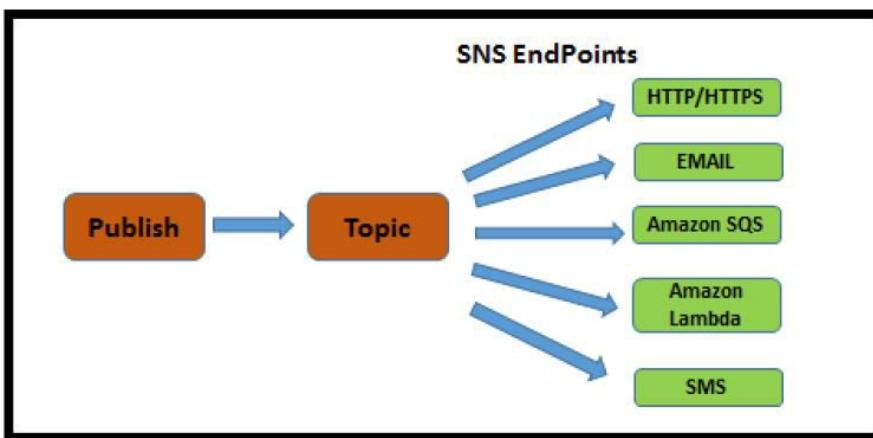
===== END OF OUTPUT =====

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

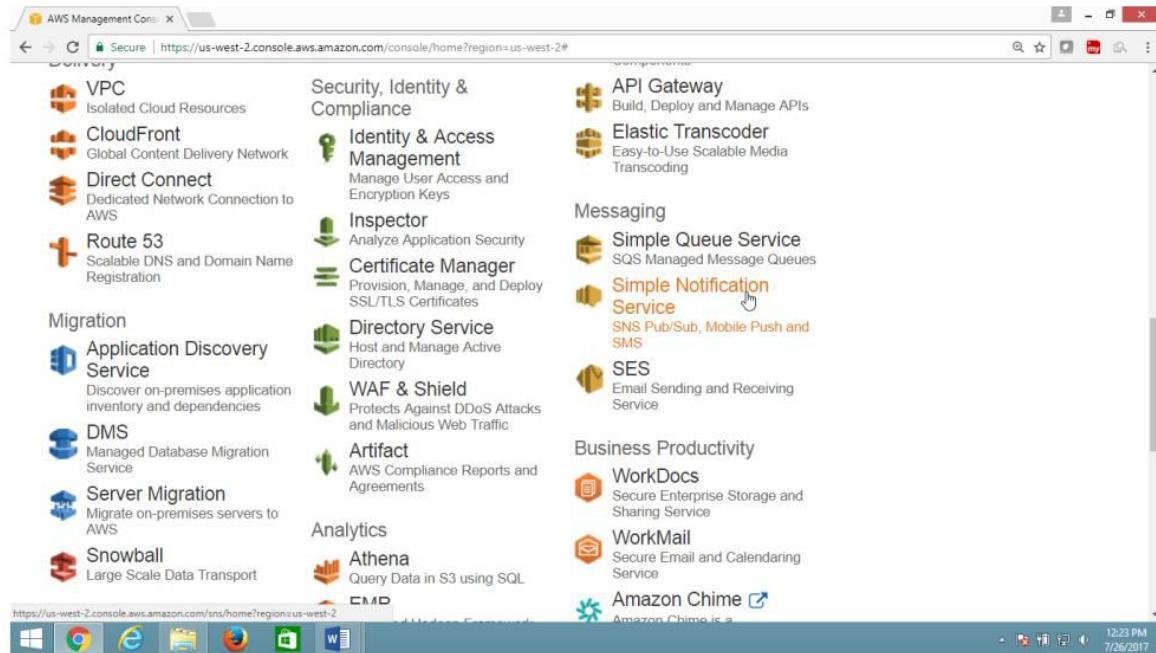
Veriy in your mail account

1) To configure Amazon Simple Notification Service (SNS)

Open AWS console

Select “**Messaging**” service

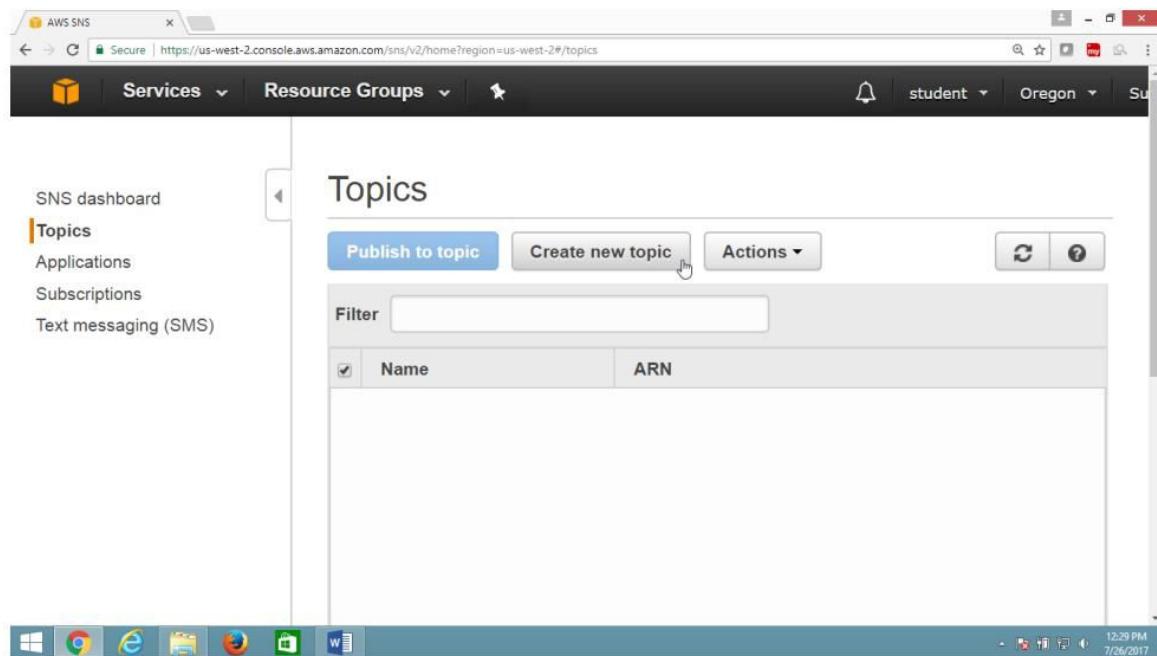
Click on “**Simple Notification service**”



From “SNS Dashboard” panel

Select Topic

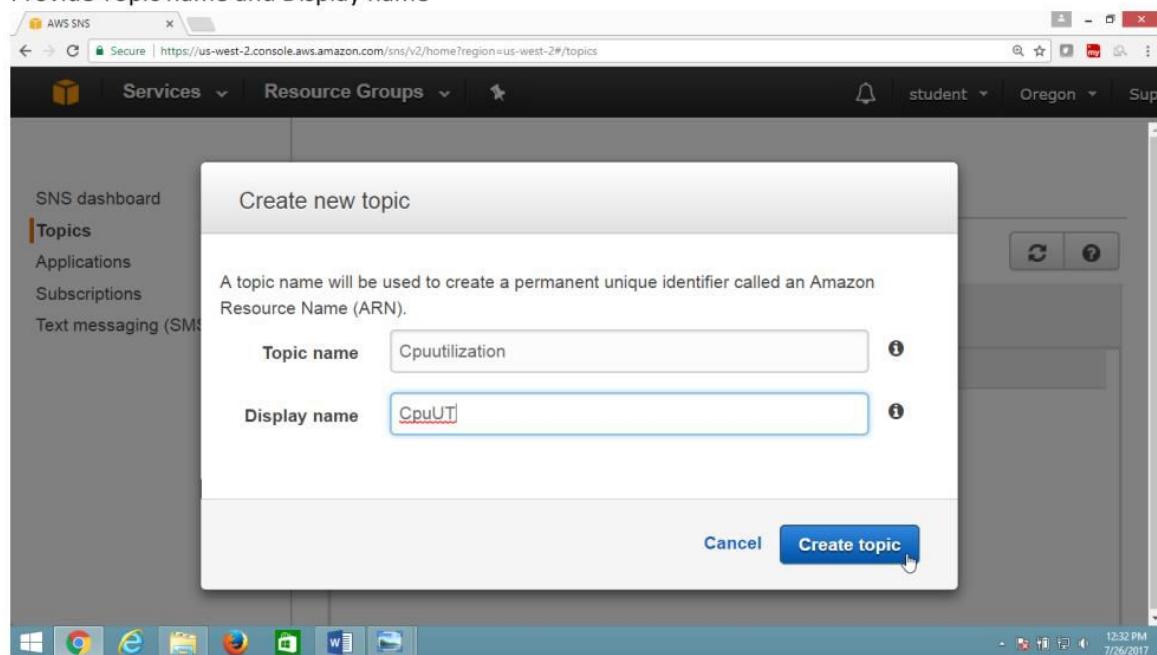
Click on “Create new topic” button



The screenshot shows the AWS SNS Topics page. At the top, there are navigation links for 'Services', 'Resource Groups', and a search bar. On the left, a sidebar menu includes 'Topics' (which is selected and highlighted in orange), 'Applications', 'Subscriptions', and 'Text messaging (SMS)'. In the main content area, there's a toolbar with 'Publish to topic', 'Create new topic' (which is highlighted with a mouse cursor), and 'Actions'. Below the toolbar is a 'Filter' input field. A table header with columns 'Name' and 'ARN' is visible, but no data rows are present. The status bar at the bottom right shows the time as 12:29 PM and the date as 7/26/2017.

In “Create new topic” box

Provide Topic name and Display name



The screenshot shows the 'Create new topic' dialog box. It contains instructions: 'A topic name will be used to create a permanent unique identifier called an Amazon Resource Name (ARN)'. There are two input fields: 'Topic name' with the value 'Cpuutilization' and 'Display name' with the value 'CpuUT'. At the bottom of the dialog are 'Cancel' and 'Create topic' buttons, with 'Create topic' being the active button indicated by a mouse cursor. The background shows the same AWS SNS interface as the previous screenshot.

Click of ARN link

The screenshot shows the AWS SNS Topics page. On the left, there's a sidebar with links: SNS dashboard, Topics (which is selected), Applications, Subscriptions, and Text messaging (SMS). The main area has a title 'Topics' and a message box asking for feedback. Below it is a table with columns 'Name' and 'ARN'. There are two rows: one for 'Cpuutilization' with ARN 'arn:aws:sns:us-west-2:523251683217:Cpuutilization' and another for a feedback topic. At the bottom of the table, there are buttons for 'Publish to topic', 'Create new topic', and 'Actions'. The status bar at the bottom shows the URL 'https://us-west-2.console.aws.amazon.com/sns/v2/home?region=us-west-2#topics/arn:aws:sns:us-west-2:523251683217:Cpuutilization' and the time '1:15 PM 7/26/2017'.

2) To create Subscription

Click on “Createsubscription” button

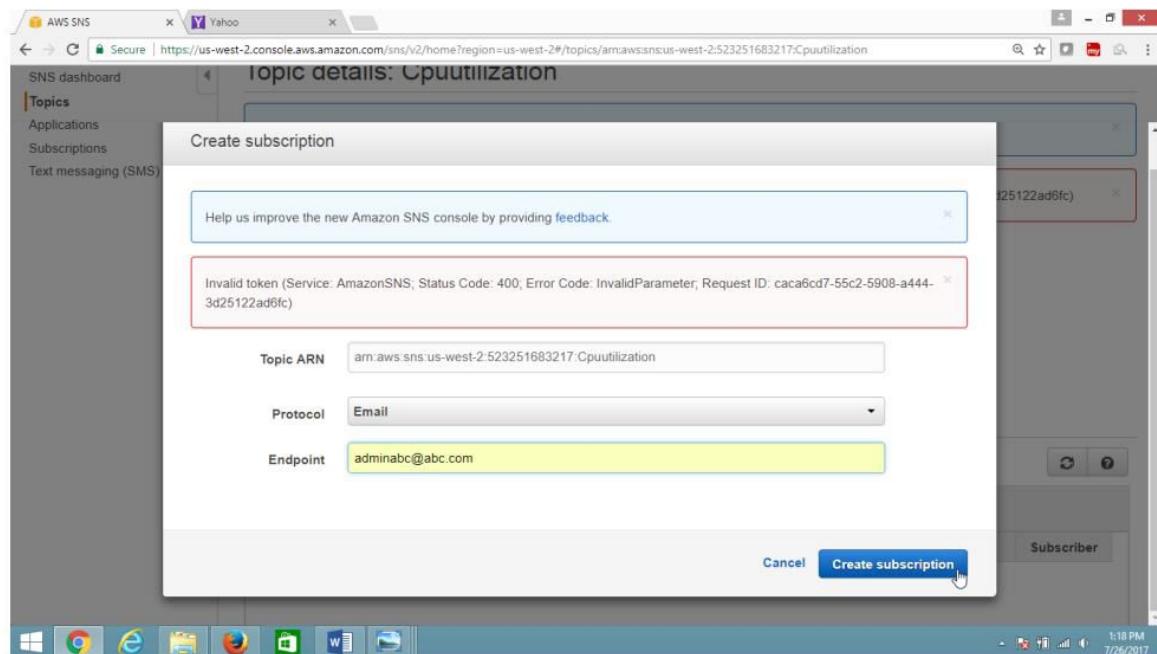
The screenshot shows the 'topic details: Cpuutilization' page. The left sidebar is identical to the previous screenshot. The main area shows the topic configuration with fields: Topic ARN (arn:aws:sns:us-west-2:523251683217:Cpuutilization), Topic owner (523251683217), Region (us-west-2), and Display name (CpuUT). Below this is a 'Subscriptions' section with a table header: 'Subscription ID', 'Protocol', 'Endpoint', and 'Subscriber'. At the top of this section are buttons for 'Create subscription' (which has a cursor over it), 'Request confirmations', 'Confirm subscription', and 'Other subscription actions'. The status bar at the bottom shows the URL 'https://us-west-2.console.aws.amazon.com/sns/v2/home?region=us-west-2#topics/arn:aws:sns:us-west-2:523251683217:Cpuutilization' and the time '1:16 PM 7/26/2017'.

Provide values as

Protocol → EMAIL

Endpoint → adminaws@abc.com

Click “Create subscription” button



3) Verification

Now subscription is in pending state

The screenshot shows the AWS SNS console with the URL <https://us-west-2.console.aws.amazon.com/sns/v2/home?region=us-west-2#/topics/armaws:sns:us-west-2:523251683217:Cpuutilization>. The region is set to us-west-2 and the display name is CpuUT. The 'Subscriptions' section shows a single entry: 'PendingConfirmation' with 'Protocol' set to 'email' and 'Endpoint' set to 'adminabc...'. There are buttons for 'Create subscription', 'Request confirmations', 'Confirm subscription', and 'Other subscription actions'.

Go to your mail account

Click on the mail

The screenshot shows a Gmail inbox with 196 messages. The message from 'CpuUT no-reply@sns.amazonaws.com' is highlighted. The subject is 'AWS Notification - Subscription Confirmation'. The message body contains the text: 'You have chosen to subscribe to the topic: arn:aws:sns:us-west-2:523251683217:Cpuutilization'. Below this, it says 'To confirm this subscription, click or visit the link below (if this was in error no action is necessary):' followed by a link labeled 'Confirm subscription'. At the bottom, there is a note: '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](#)'.

Click on "Confirm message"

The screenshot shows the same Gmail inbox as before, but now the 'Confirm subscription' link has been clicked. The message body now includes the text: 'You have confirmed to subscribe to the topic: arn:aws:sns:us-west-2:523251683217:Cpuutilization'.

Now subscription is verified

The screenshot shows the AWS SNS Topic Subscriptions page. At the top, there are buttons for "Publish to topic" and "Other topic actions". Below that, topic details are shown: Topic ARN (arn:aws:sns:us-west-2:523251683217:Cpuutilization), Topic owner (523251683217), Region (us-west-2), and Display name (CpuUT). The main section is titled "Subscriptions" and contains a table with one row. The table has columns for Subscription ID, Protocol, Endpoint, and Sub. The single entry is: Subscription ID (arn:aws:sns:us-west-2:523251683217:Cpuutilization:b5f880a3-4631-405e-b5e1-a37209c3...), Protocol (email), Endpoint (ski 52:), and Sub (empty).

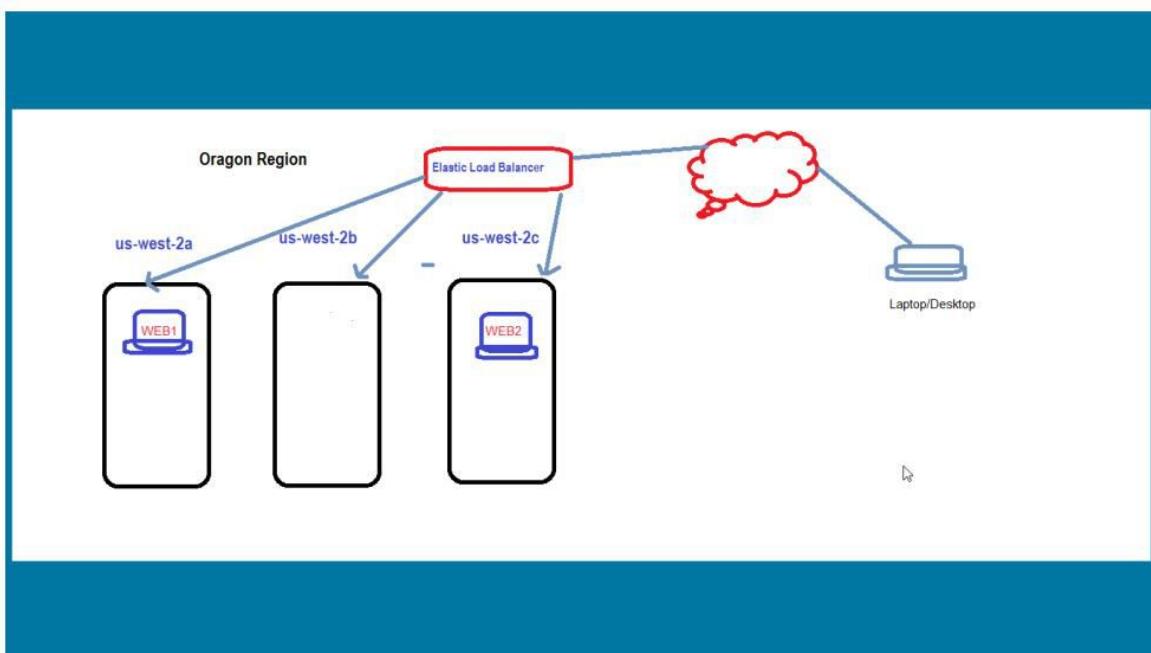
Subscription ID	Protocol	Endpoint	Sub
arn:aws:sns:us-west-2:523251683217:Cpuutilization:b5f880a3-4631-405e-b5e1-a37209c3...	email	ski 52:	

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. The left sidebar navigation bar includes 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES' (selected), 'Instances', 'Spot Requests', 'Reserved Instances', 'Scheduled Instances', and 'Dedicated Hosts'. The main content area displays a table of instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
web1	i-081a441f51fc90525	t2.micro	us-west-2a	running	Initializing	None
web2	i-090dfbcc632605047	t2.micro	us-west-2c	running	Initializing	None

Below the table, a message states 'Instances: i-081a441f51fc90525 (web1), i-090dfbcc632605047 (web2)'. A 'Description' tab is selected, showing the instance IDs and their corresponding public DNS names: ec2-54-218-192-19.us-west-2.compute.amazonaws.com and ec2-54-203-189-115.us-west-2.compute.amazonaws.com. The bottom of the screen shows the Windows taskbar with various icons and the system tray indicating the date and time as 7/25/2017 at 12:45 PM.

Verify Public IP of both instance

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation includes 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES' (selected), 'Instances', 'Spot Requests', 'Reserved Instances', 'Scheduled Instances', 'Dedicated Hosts', 'IMAGES', and 'ELASTIC BLOCK STORE'. The main content area displays a table of instances. The table has columns for 'Instance State', 'Status Checks', 'Alarm Status', 'Public DNS (IPv4)', 'IPv4 Public IP', and 'IPv6 IPs'. There are two entries in the table:

Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
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, a message says 'Instances: i-081a441f51fc90525 (web1), i-090dfbcc632605047 (web2)'. A detailed view for the first instance shows its description: 'i-081a441f51fc90525: ec2-54-218-192-19.us-west-2.compute.amazonaws.com'. The bottom of the page includes links for 'Feedback', 'English', 'Privacy Policy', 'Terms of Use', and standard browser icons.

Verify

Output of Webserver one



Verify

Output of Webserver two



3) To Configure Elastic Load Balancer.

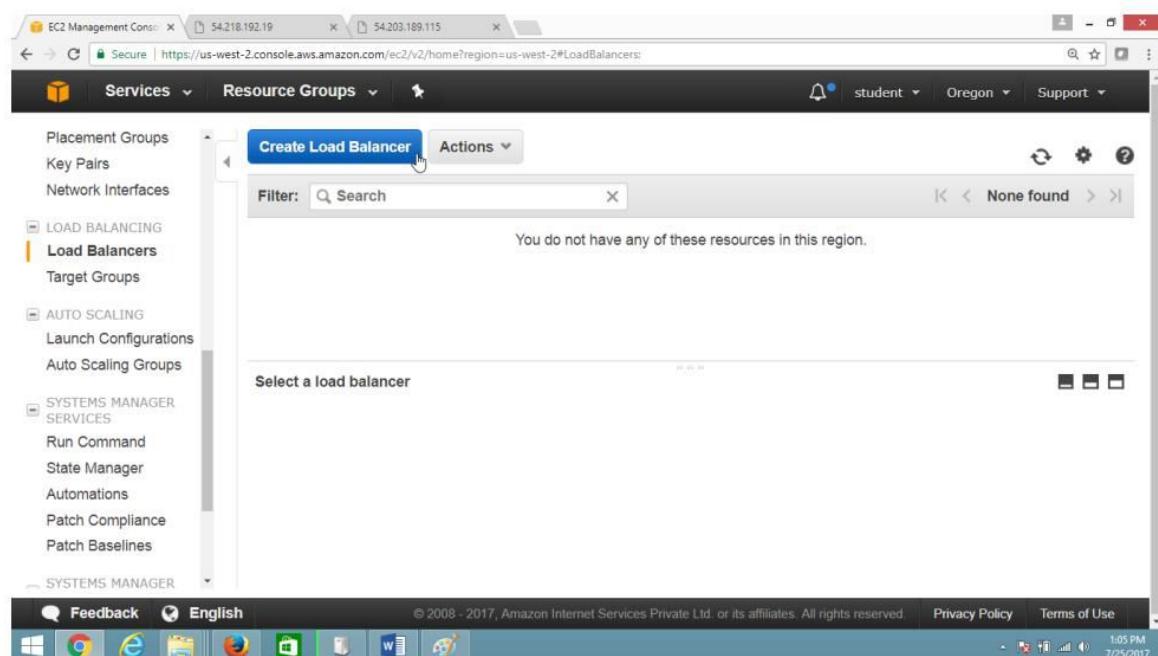
Open the AWS console

On **EC2 Dashboard** panel

Expanding “**LOAD BALANCING**”

Select **Load Balancer**,

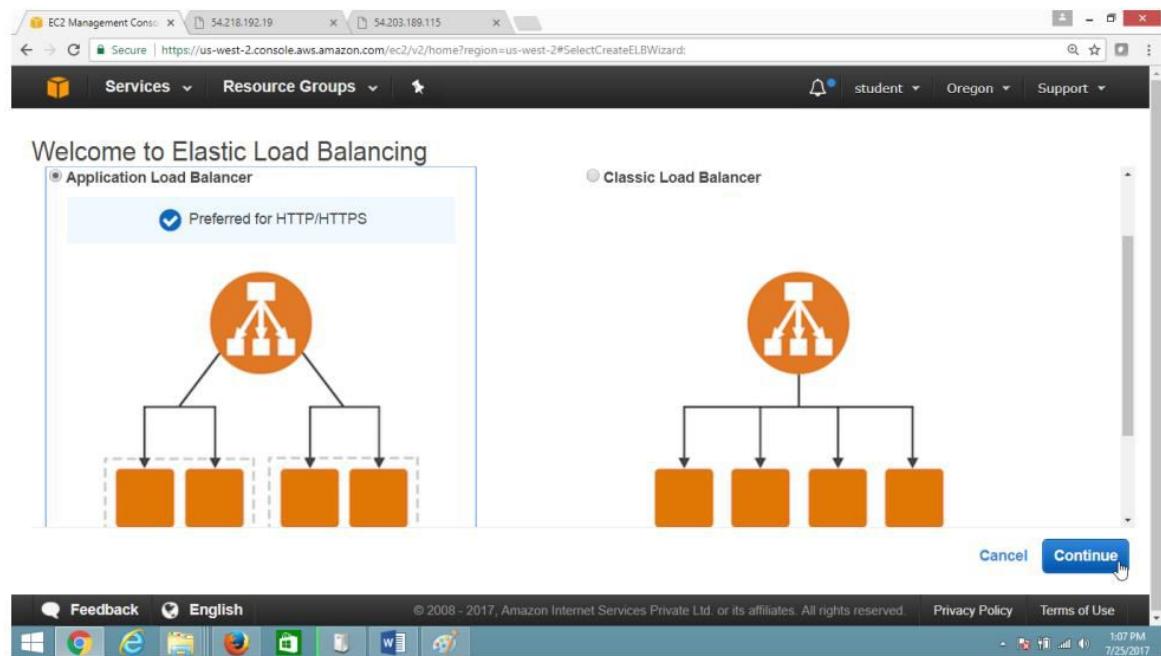
Click on “**Create Load Balancer**” button



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 EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#V2CreateELBWizard>. The browser tabs include EC2 Management Console, 54.218.192.19, and 54.203.189.115. The main window displays the 'Step 1: Configure Load Balancer' section of the 'Configure Load Balancer' wizard. The 'Basic Configuration' step is selected. The configuration fields are as follows:

- Name:** ELBsales
- Scheme:** internet-facing (radio button selected)
- IP address type:** ipv4

Below these fields, the 'Listeners' section is visible, with a note explaining what a listener is. At the bottom right of the wizard, there are 'Cancel' and 'Next: Configure Security Settings' buttons. The status bar at the bottom of the browser shows the date and time as 7/25/2017 1:21 PM.

Under **Listeners**, Provide

Load Balancer Protocol → **HTTP**

Load Balancer Port as → **80**

Drag down

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#V2CreateELBWizard>. The page is titled "Step 1: Configure Load Balancer".

Listeners

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

Load Balancer Protocol	Load Balancer Port
HTTP	80

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

Feedback English © 2008 - 2017, Amazon Internet Services Private Ltd or its affiliates. All rights reserved Privacy Policy Terms of Use 1:22 PM 7/25/2017

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.

Availability Zone	Subnet ID	Subnet IPv4 CIDR	Name
us-west-2a	subnet-13f60e5a	172.31.32.0/20	
us-west-2b	subnet-8b9e38ec	172.31.16.0/20	
us-west-2c	subnet-19d0f141	172.31.0.0/20	

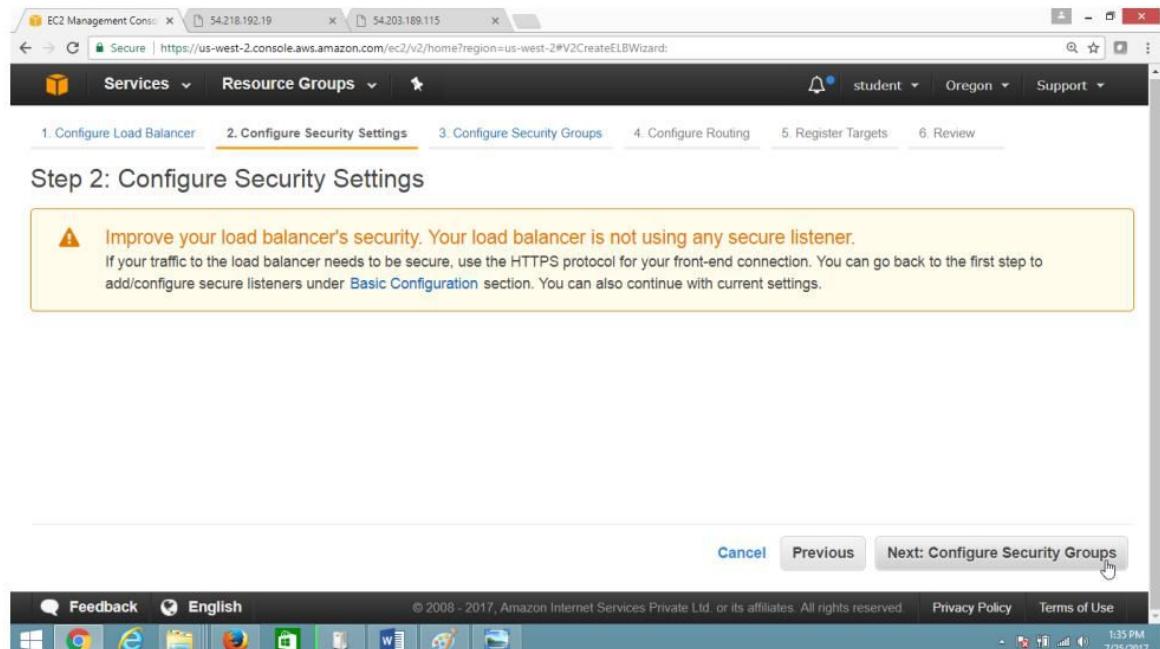
Tags

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

The screenshot shows the AWS EC2 Management Console interface. The URL is <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#V2CreateELBWizard:3>. The top navigation bar includes 'Services', 'Resource Groups', and tabs for 'student', 'Oregon', and 'Support'. The main content area is titled 'Step 3: Configure Security Groups'. It provides instructions: 'A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.' Below this, there are two radio buttons: 'Create a new security group' (selected) and 'Select an existing security group'. The 'Security group name' field contains 'load-balancer-wizard-2'. The 'Description' field shows 'load-balancer-wizard-2 created on 2017-07-25T13:35:42.009+05:30'. A table row for a 'Custom TCP Rule' is shown, with 'Protocol' set to 'TCP', 'Port Range' set to '80', and 'Source' set to 'Custom 0.0.0.0/0, ::/0'. At the bottom, there are 'Cancel', 'Previous', and 'Next: Configure Routing' buttons. The status bar at the bottom right shows '1:35 PM' and '7/25/2017'.

ON “Configure Routing” page give following values

Name → Websales

Leave remaining values as default

click “Next: Register Targets” button

The screenshot shows the AWS EC2 Management Console interface for creating a load balancer. The current step is "Step 4: Configure Routing".

Target group:

- Target group: New target group
- Name: WebSales
- Protocol: HTTP
- Port: 80

Health checks:

- Protocol: HTTP
- Path: /

At the bottom right, there are buttons for "Cancel", "Previous", and "Next: Register Targets". The "Next: Register Targets" button is highlighted with a mouse cursor.

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

Step 5: Register Targets

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Instance	Name	State	Security	Zone	Subnet ID	Subnet CIDR
i-081a441f51fc...	web1	running	launch-wizard-5	us-west-2a	subnet-13f60e5a	172.31.32.0/20
i-090dfbcc632605047	web2	running	launch-wizard-6	us-west-2c	subnet-19d0ff141	172.31.0.0/20

Add to registered on port 80

Cancel Previous Next: Review

Verify that running instances are registered

Click on “Next: Review” button

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Instance	Name	Port	State	Security groups	Zone
i-081a441f51fc90525	web1	80	running	launch-wizard-5	us-west-2a
i-090dfbcc632605047	web2	80	running	launch-wizard-6	us-west-2c

Instances

Cancel Previous Next: Review

Verify

Check the summary

Drag Down

The screenshot shows the EC2 Management Console interface. The URL is https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#V2CreateELBWizard:Step 6: Review. The top navigation bar includes Services, Resource Groups, student, Oregon, and Support. Below the navigation, a progress bar shows steps 1 through 6, with step 6 being the current active step. The main content area displays the configuration for a new load balancer named 'ELBsales'. It includes details such as Scheme (internet-facing), Listeners (Port:80 - Protocol:HTTP), IP address type (ipv4), VPC (vpc-89c341ee), Subnets (subnet-13f60e5a, subnet-8b9e38ec, subnet-19d0f141), and Tags. Under Security settings, it lists Certificate name and Security policy name. At the bottom right, there are 'Cancel', 'Previous', and 'Create' buttons. The status bar at the bottom indicates the browser version (IE 11) and the date (7/25/2017).

Click on "Create" button

This screenshot is identical to the previous one, showing the Step 6: Review page of the ELB creation wizard. The configuration details for the load balancer 'ELBsales' are the same. The 'Create' button is highlighted with a blue border, indicating it is the next action to be taken. The status bar at the bottom right shows the time as 1:43 PM.

Verify

Load balancer successfully created.

The screenshot shows a browser window with three tabs open: 'EC2 Management Consl' (closed), '54.218.192.19' (closed), and '54.203.189.115'. The main content area displays the 'Load Balancer Creation Status' page. A message box is visible, containing a green checkmark icon and the text: 'Successfully created load balancer'. Below this, it says 'Load balancer ELBSales was successfully created.' and includes a note: '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 the initial health checks.' At the bottom right of the message box is a blue 'Close' button, which has a mouse cursor hovering over it. The browser's status bar at the bottom shows the URL 'https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#V2CreateELBWizard:' and the date '7/25/2017'.

4) Verification

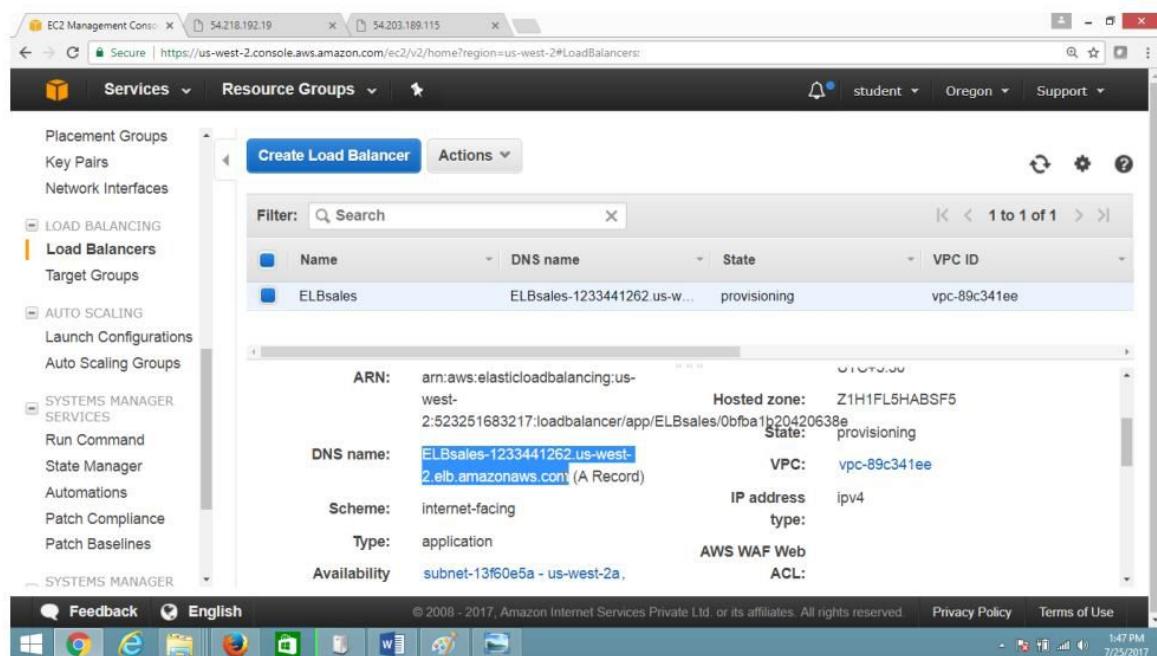
To verify Websites are coming through Load Balancer

Go to **EC2 Dashboard** panel

Expanding **LOAD BALANCING**

Select **Load Balancer**.

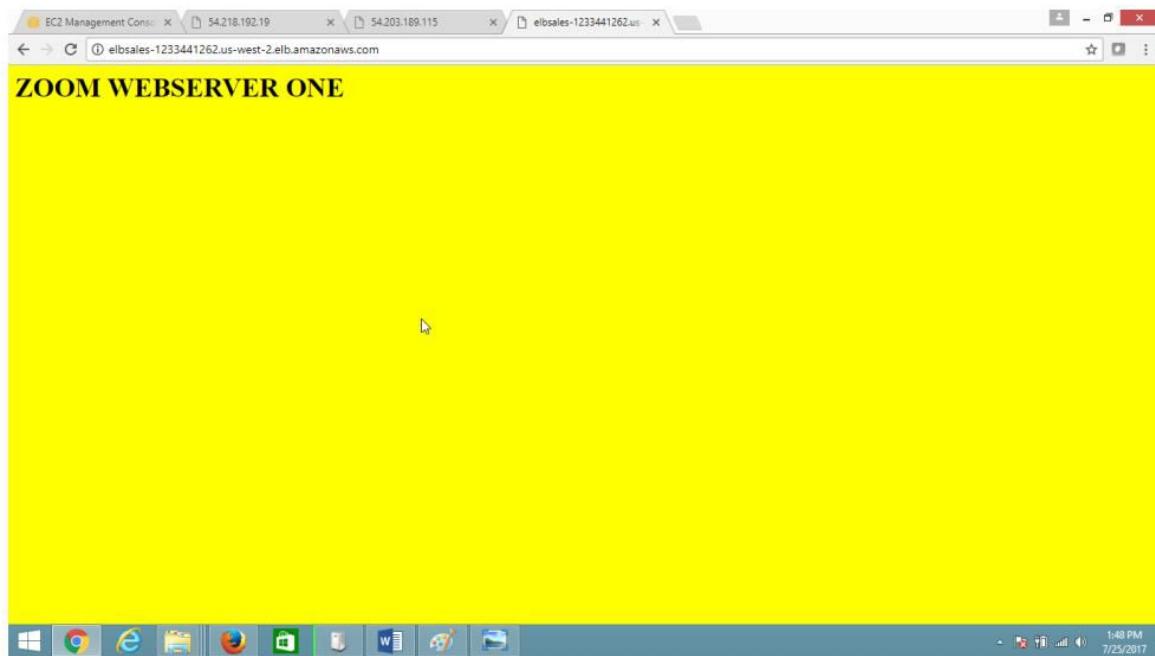
Copy Load Balancer DNS Name



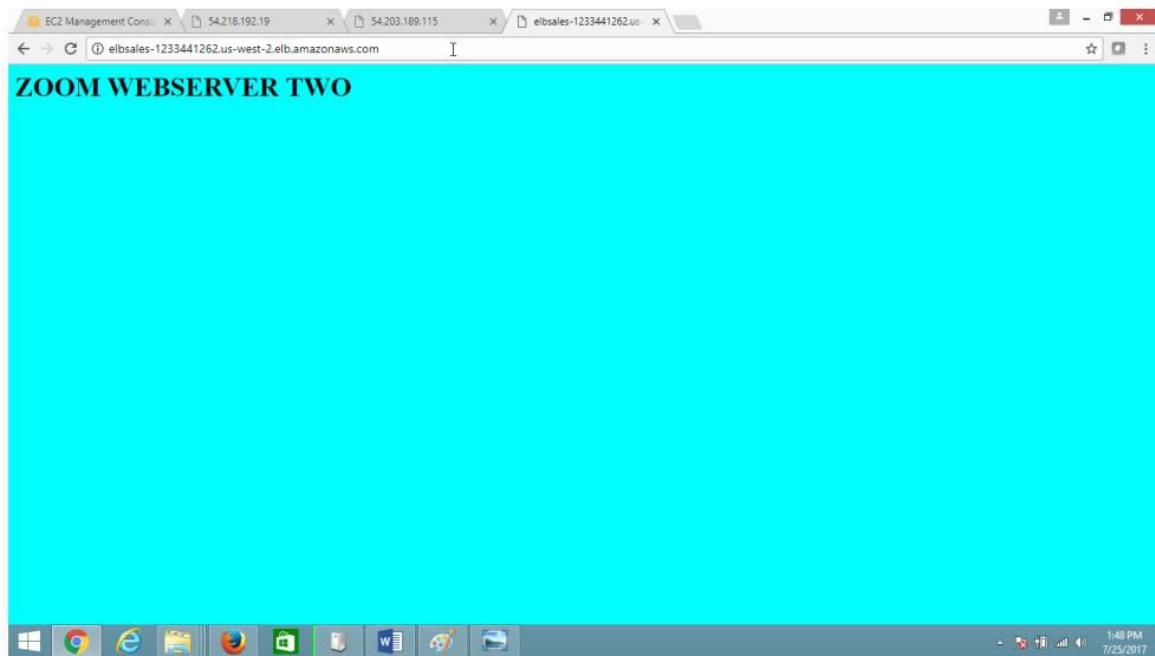
The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LoadBalancers>. The left sidebar includes 'Placement Groups', 'Key Pairs', 'Network Interfaces', 'LOAD BALANCING' (selected), 'Load Balancers' (highlighted), 'Target Groups', 'AUTO SCALING', 'Launch Configurations', 'Auto Scaling Groups', 'SYSTEMS MANAGER SERVICES', 'Run Command', 'State Manager', 'Automations', 'Patch Compliance', 'Patch Baselines', and 'SYSTEMS MANAGER'. The main content area displays a table for 'Load Balancers'. The table has columns: Name, DNS name, State, and VPC ID. One row is shown: 'Name' is 'ELBsales', 'DNS name' is 'ELBsales-1233441262.us-west-2.elb.amazonaws.com (A Record)', 'State' is 'provisioning', and 'VPC ID' is 'vpc-89c341ee'. Below the table, detailed information for the 'ELBsales' load balancer is provided: ARN, Hosted zone, DNS name, VPC, Scheme, Type, Availability, IP address type, AWS WAF Web ACL, and State. The 'DNS name' field is highlighted with a yellow box.

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.



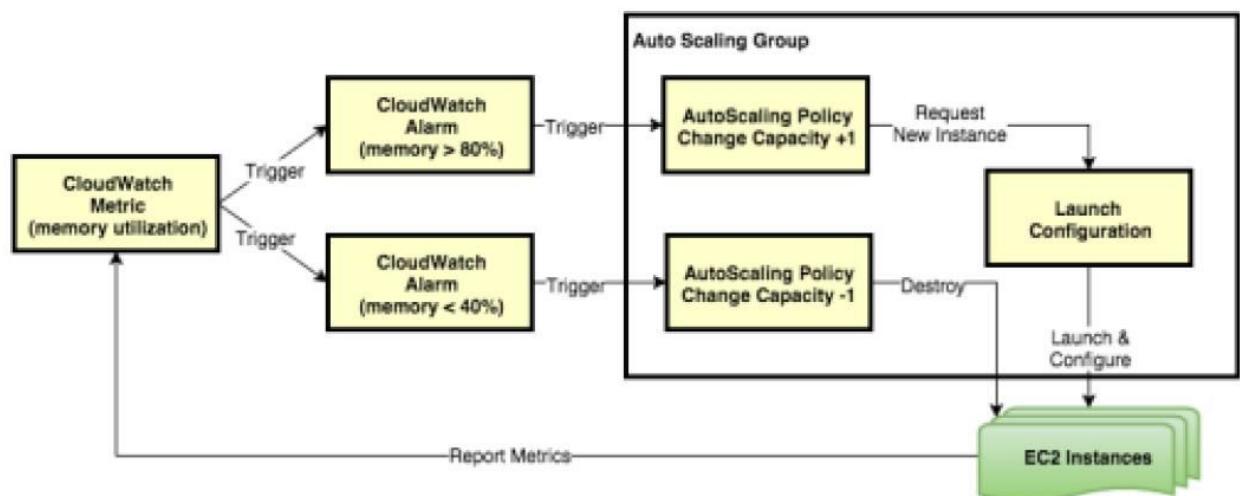
If you get this output, Congratulation your ELB configuration is successful.

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

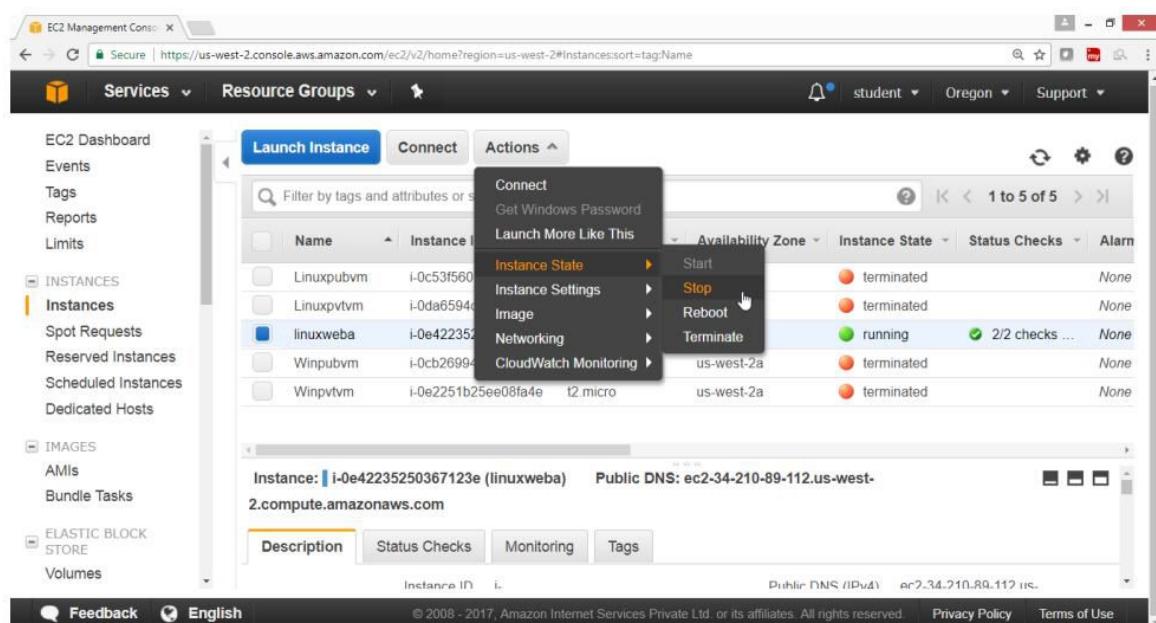
On “EC2 Dashboard” panel

Select the instance

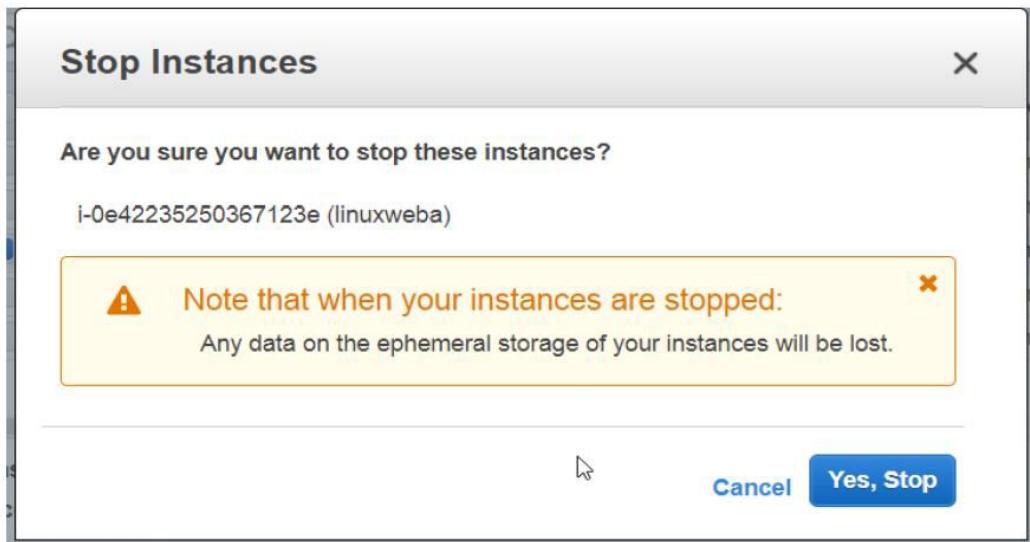
Click on **Action** button

Select Instance state

Click stop



Click on **Yes Stop** button

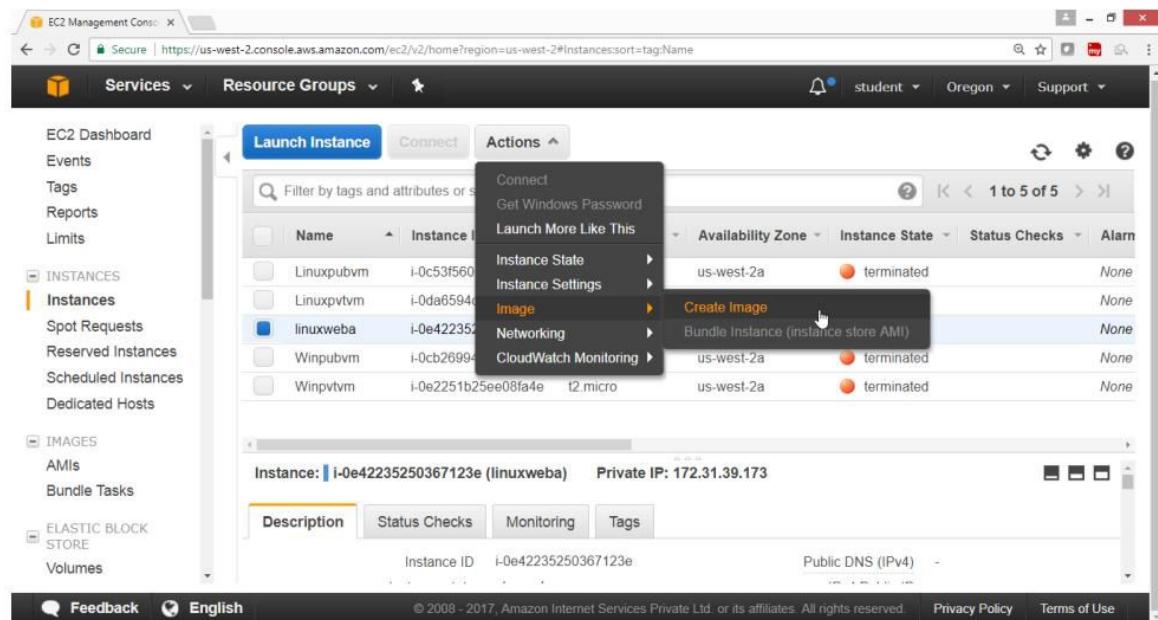


Select the stopped instance

Click on **Action** button

Select **image**

Click on **Create image** button

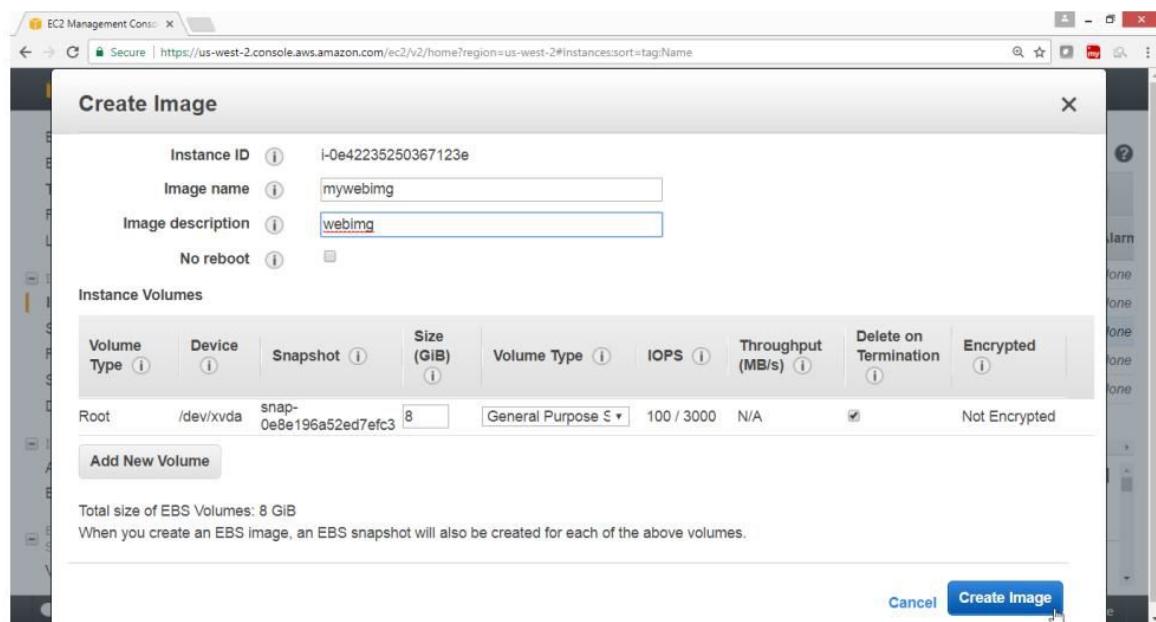


For Image name → mywebimg

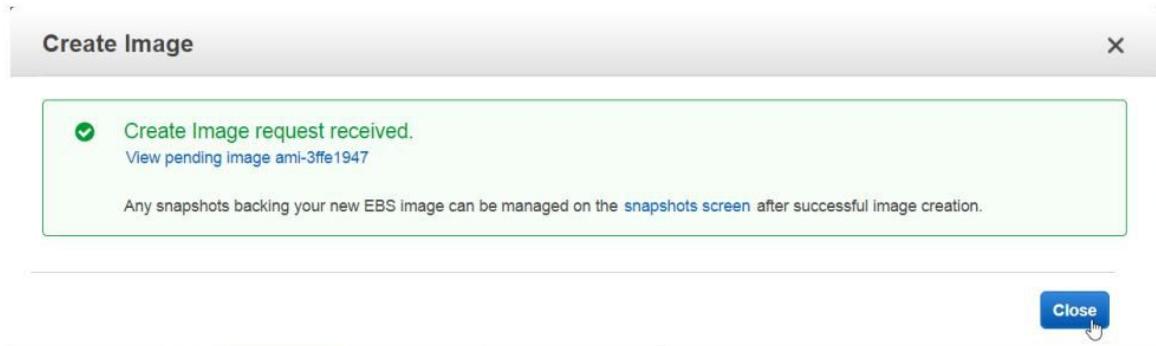
For Image description → webimg

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**

Name	AMI Name	AMI ID	Source	Owner	Visibility	Status
	mywebimg	ami-3ffe1947	523251683217...	523251683217	Private	available

3) To Configure Auto Scaling

On the **EC2 Dashboard** panel

Select “**AUTO SCALING**”

The screenshot shows the AWS EC2 Management Console interface. The left sidebar has a tree view with 'LOAD BALANCING' expanded, showing 'Load Balancers' and 'Target Groups'. 'AUTO SCALING' is selected and highlighted with a blue border, showing 'Launch Configurations' and 'Auto Scaling Groups'. Below this is 'SYSTEMS MANAGER SERVICES' with 'Run Command', 'State Manager', 'Automations', 'Patch Compliance', and 'Patch Baselines'. Further down is 'SYSTEMS MANAGER SHARED RESOURCES' with 'Managed Instances' and '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 in the center says: '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.' On the right, there's an 'Account Attributes' section with 'Supported Platforms' (VPC), 'Default VPC' (vpc-89c341ee), and 'Resource ID length management'. Below that is an 'Additional Information' section with links to 'Getting Started Guide', 'Documentation', 'All EC2 Resources', 'Forums', 'Pricing', and 'Contact Us'. At the bottom, there are links for 'Feedback', 'English', 'Privacy Policy', 'Terms of Use', and a date/time stamp '1:32 PM 8/9/2017'.

Click on “Launch Configuration”

The screenshot shows the AWS Management Console for Auto Scaling. The left sidebar has a tree view with 'Launch Configurations' selected under the 'Auto Scaling' category. The main content area is titled 'Welcome to Auto Scaling' and contains a 'Create Auto Scaling group' button. To the right is an 'Additional Information' sidebar with links like 'Getting Started Guide' and 'Documentation'. The bottom of the page includes standard AWS navigation links for feedback, language selection, and legal notices.

Click on “Create Auto Scaling Group” button

This screenshot is identical to the one above, but the 'Create Auto Scaling group' button is highlighted with a mouse cursor, indicating the next step in the process.

Click on “Create launch configuration” button

The screenshot shows the "Create Auto Scaling Group" wizard. The first step, "Step 1: Create launch configuration", is displayed. It features an icon of a person, a gear, and three server icons. The text explains that users need to choose a launch configuration template for their Auto Scaling group. A note says users can change their group's software later. At the bottom right, there are "Cancel" and "Create launch configuration" buttons, with the latter being highlighted by a mouse cursor.

Click on “My AMI”

The screenshot shows the "Create Launch Configuration" wizard. The "My AMIs" section is selected. It lists two AMIs: "Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-6df1e514" and "Red Hat Enterprise Linux 7.3 (HVM), SSD Volume Type - ami-b55a51cc". Both are marked as "Free tier eligible". On the right, there are "Select" buttons and "64-bit" options. The "Amazon Linux" row has a "Select" button highlighted with a mouse cursor. The navigation bar at the top includes tabs for "1. Choose AMI", "2. Choose Instance Type", "3. Configure details", "4. Add Storage", "5. Configure Security Group", and "6. Review".

Select the AMI which was created with Webserver.

Click on **Select** button

EC2 Management Console X

Secure | https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateLaunchConfiguration:CreationFlowType=linkToASGCreation

student | Oregon | Support

Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure details 4. Add Storage 5. Configure Security Group 6. Review

Create Launch Configuration

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

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Ownership

Owned by me

Shared with me

Search my AMIs

mywebimg - ami-3ffe1947

webimg

Root device type: ebs Virtualization type: hvm Owner: 523251683217

Select

Cancel and Exit

1 to 1 of 1 AMIs

64-bit

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

Choose instance Type,

General purpose, t2.micro free tier

Click on **Next : Configuration Details**

EC2 Management Console X

Secure | https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateLaunchConfiguration:CreationFlowType=linkToASGCreation

student | Oregon | Support

Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure details 4. Add Storage 5. Configure Security Group 6. Review

Create Launch Configuration

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

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

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
General purpose	t2.micro	1	1	EBS only	-	Low to Moderate
General purpose	t2.small	1	2	EBS only	-	Low to Moderate
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate

Cancel Previous Next: Configure details

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

On **Create launch Configuration** page

Name → mylaunchconf

Monitoring → Enable check box

Click on **Next : Add storage** button

The screenshot shows the 'Create Launch Configuration' wizard on the AWS Management Console. The current step is '3. Configure details'. The 'Name' field is populated with 'mylaunchconf'. Under 'Monitoring', the checkbox for 'Enable CloudWatch detailed monitoring' is checked. At the bottom, there are buttons for 'Cancel', 'Previous', 'Skip to review' (which is highlighted in blue), and 'Next: Add Storage'.

By default linux takes 8 GB EBS volume

Leave all values as default

Click on “ Next: Configure Security Group” button

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateLaunchConfiguration:CreationFlowType=linkToASGCreation>. The page is titled "Create Launch Configuration". The top navigation bar includes "Services", "Resource Groups", and tabs for "1. Choose AMI", "2. Choose Instance Type", "3. Configure details", "4. Add Storage", "5. Configure Security Group", and "6. Review". The "5. Configure Security Group" tab is highlighted.

The main content area is titled "Add New Volume". It shows a table with one row:

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput	Delete on Termination	Encrypted
Root	/dev/xvda	snap-090a9f2d57197bb89	8	General Purpose (SSD)	100 / 3000	N/A	<input checked="" type="checkbox"/>	No

A note below the table states: "Free tier eligible customers can get up to 30 GB of EBS storage. [Learn more](#) about free usage tier eligibility and usage restrictions."

At the bottom, there are buttons for "Cancel", "Previous", "Skip to review", and "Next: Configure Security Group" (which is highlighted). There are also links for "Feedback", "English", "Privacy Policy", and "Terms of Use".

On Create Launch Configuration page

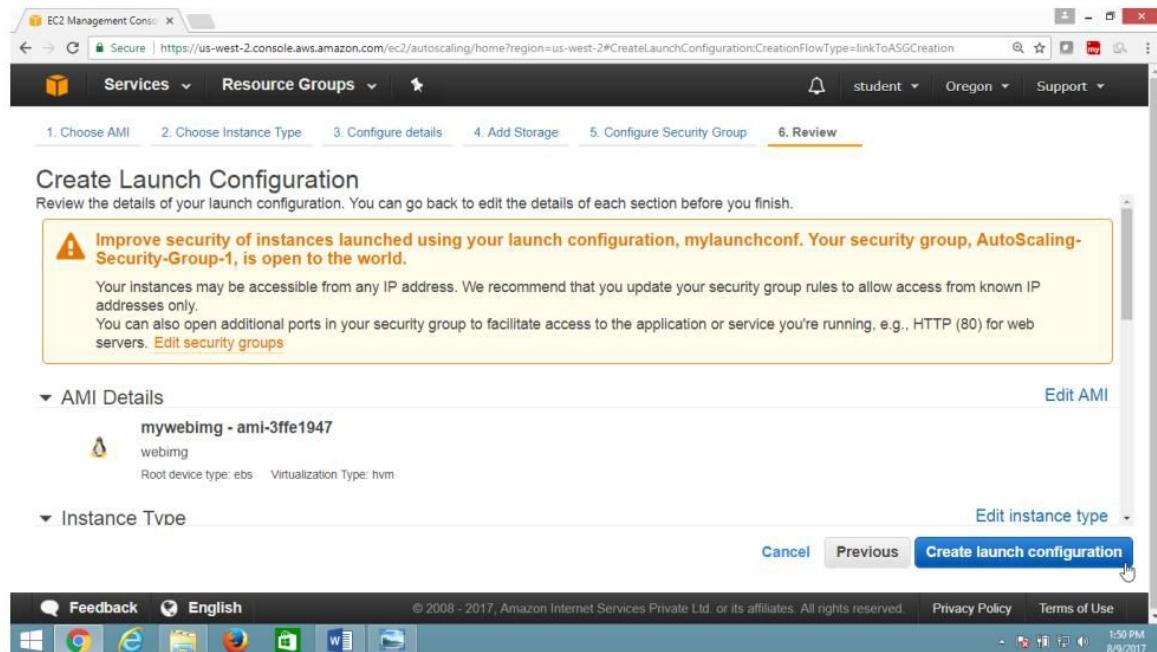
Select “Create a new security Group”

Click on Review

The screenshot shows the AWS EC2 Management Console interface for creating a launch configuration. The top navigation bar includes 'Services' (selected), 'Resource Groups', and account information ('student', 'Oregon', 'Support'). Below the navigation is a breadcrumb trail: '1. Choose AMI', '2. Choose Instance Type', '3. Configure details', '4. Add Storage', '5. Configure Security Group' (which is underlined in blue), and '6. Review'. The main content area is titled 'Create Launch Configuration' and describes security groups as sets of firewall rules. It asks to assign a security group, with the 'Create a new security group' option selected. A table shows a single rule: Type 'SSH', Protocol 'TCP', Port Range '22', and Source 'Anywhere'. At the bottom right of the form are 'Cancel', 'Previous', and a large blue 'Review' button.

Check the summary

Click on “Create launch configuraton” button



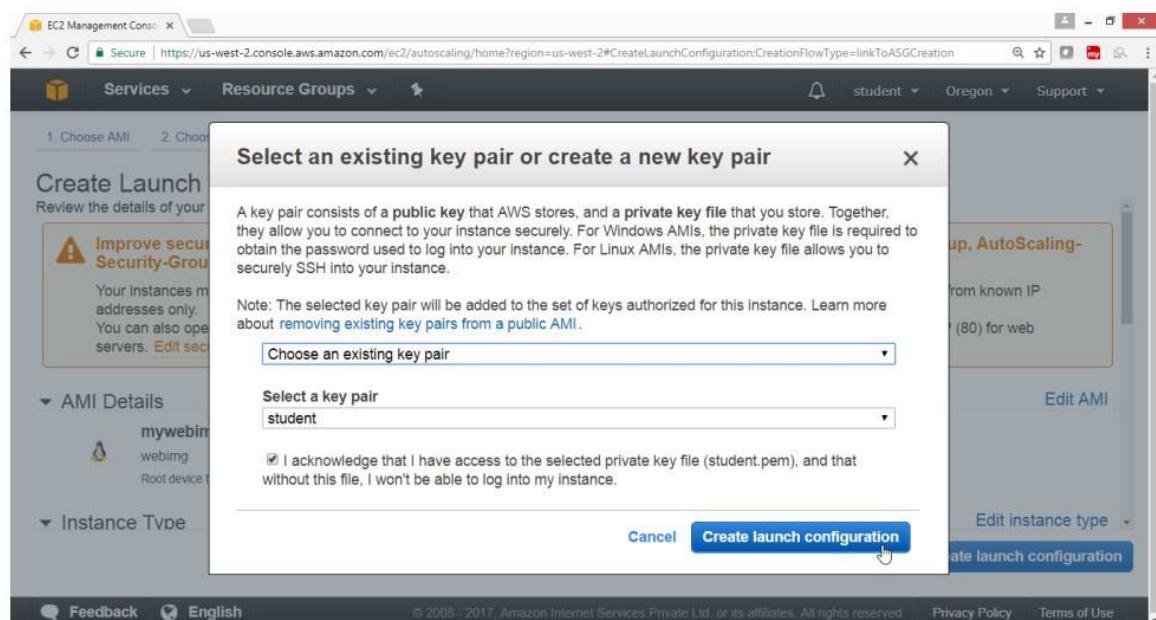
On “Select an existing key pair or create a new key pair” page

Select “Choose an existing key pair”

Select a key pair → student

Select Acknowledge check box

Click on “Create launch Configuration” button



On “Create Auto Scaling Group” page, give values as

Launch Configuration → mylaunchconf

Group name → myautoscalegrp

For Network → select default

Create Auto Scaling Group

Launch Configuration: mylaunchconf

Group name: myautoscalegrp

Group size: Start with 1 instances

Network: vpc-89c341ee (172.31.0.0/16) | default-vpc-oregon (d...)

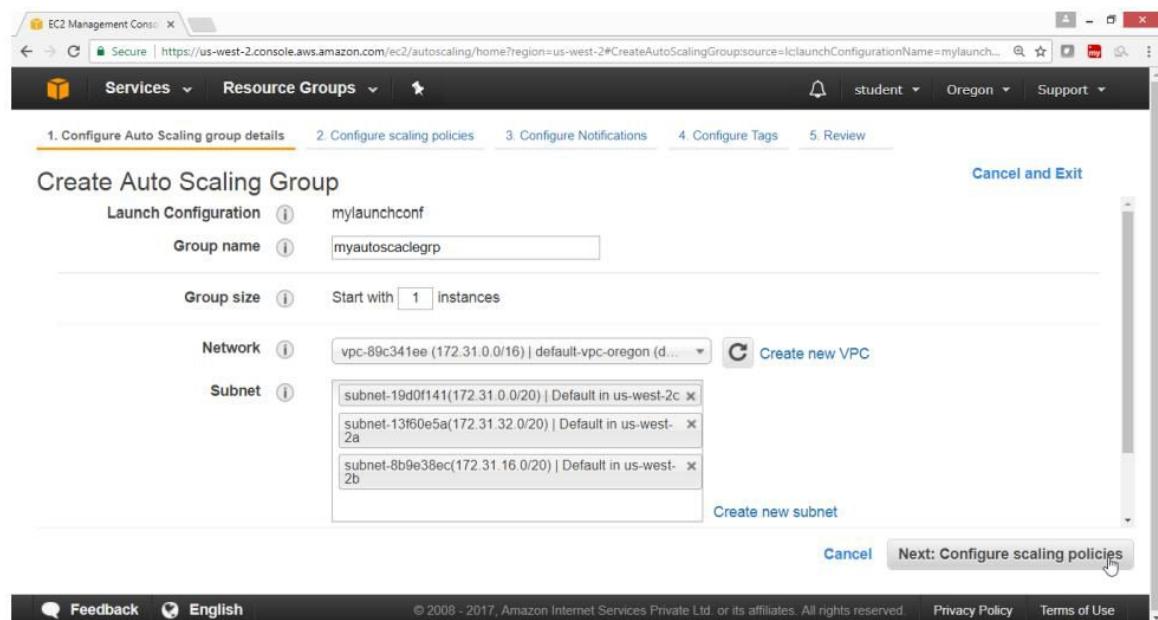
Subnet:

- subnet-19d0f141(172.31.0.0/20) | Default in us-west-2a
- subnet-13f60e5a(172.31.32.0/20) | Default in us-west-2a
- subnet-8b9e38ec(172.31.16.0/20) | Default in us-west-2b

Cancel Next: Configure scaling policies

Select ALL subnet one by one

Click on “Next Configure scaling policies” button



On “Create Auto Scaling Group” page

Select “Use scaling policies to adjust the capacity of this group”

Scale between [] and [] instances.

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateAutoScalingGroup:source=lc-launchConfigurationName=myLaunch...>. The top navigation bar includes 'Services', 'Resource Groups', and account information for 'student' in 'Oregon'. The main content area displays the 'Create Auto Scaling Group' wizard, step 2: Configure scaling policies. The second radio button, 'Use scaling policies to adjust the capacity of this group', is selected. Below it, a note says 'Scale between [1] and [3] instances. These will be the minimum and maximum size of your group.' A 'Scale Group Size' dialog box is overlaid, containing fields for 'Name' (Scale Group Size), 'Metric type' (Average CPU Utilization), 'Target value' (empty), and 'Instances need' (300). A message at the bottom of the dialog states 'Target value must be specified'. At the bottom of the wizard, buttons for 'Cancel', 'Previous', 'Review', and 'Next: Configure Notifications' are visible.

Drag Down

Click on “Scale the Auto Scaling group using step or simple scaling policies”

The screenshot shows the same AWS EC2 Management Console and wizard as the previous one, but the link 'Scale the Auto Scaling group using step or simple scaling policies' is now highlighted with a mouse cursor. The rest of the interface remains identical to the previous screenshot.

Select Increase Group Size

Click on "Add new alarm"

The screenshot shows the AWS Auto Scaling 'Create Auto Scaling Group' wizard, Step 2: Configure scaling policies. The 'Increase Group Size' policy is selected. The 'Execute policy when:' dropdown shows 'No alarm selected'. The 'Add new alarm' button is highlighted with a cursor. The 'Decrease Group Size' policy is also listed below.

Click on "create topic"

The screenshot shows the AWS CloudWatch 'Create Alarm' wizard. The 'Send a notification to:' dropdown shows 'No SNS topics found...' with a 'create topic' button highlighted with a cursor. A line chart titled 'CPU Utilization Percent' shows data for the period 04:00 to 08:00 on 8/9. The chart has three data series: 'myautoscalegrp', 'myautoscalegrp', and 'myautoscalegrp'. The 'Create Alarm' button is at the bottom right.

On “Create Alarm” box, give values as

Send a notification to → Cpuutiliazationabc
With this recipients → skmarhaan999@gmail.com
Whenever Average of CPU Utilization
is \geq → 30

Remaining value leave default

Click on “Create Alarm” button

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define. To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send a notification to: Cpuutiliazationabc [cancel](#)

With these recipients: skmarhaan999@gmail.com

Whenever: Average of CPU Utilization

Is: \geq 30 Percent

For at least: 1 consecutive period(s) of 5 Minutes

Name of alarm: awsec2-myautoscalegrp-High-CPU-Utilization

CPU Utilization Percent

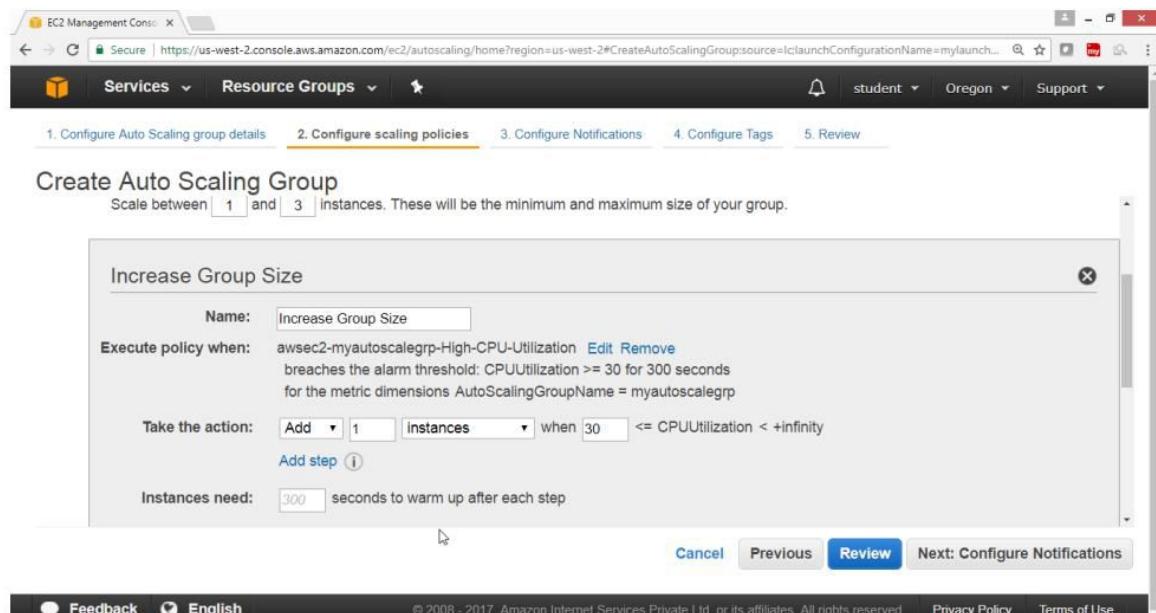
8/9 8/9 8/9
04:00 06:00 08:00

myautoscalegrp

[Cancel](#) [Create Alarm](#)

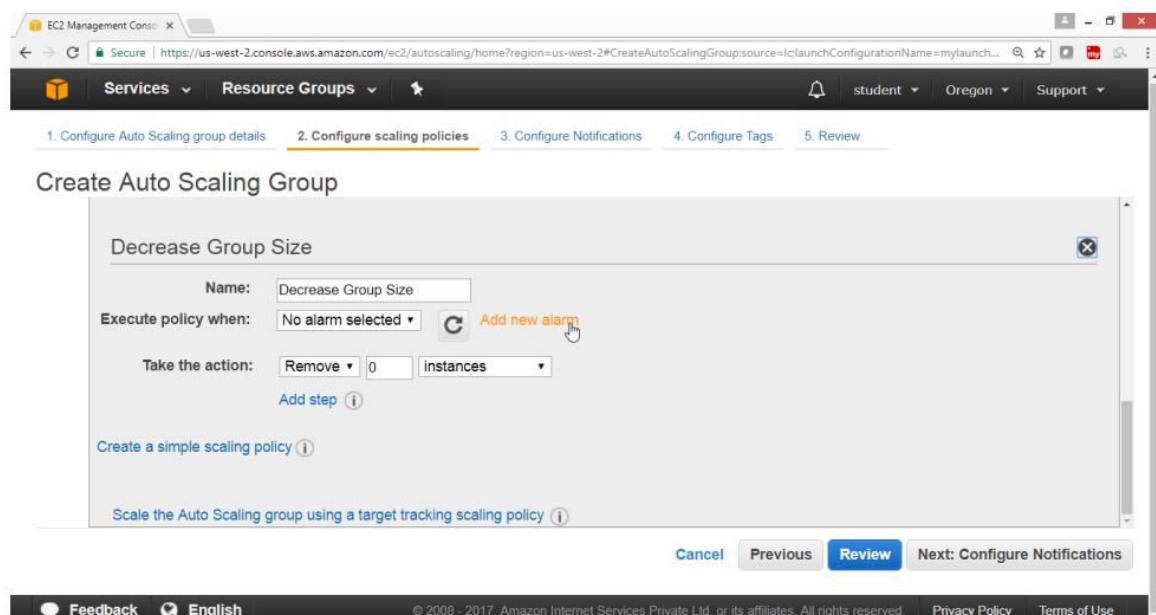
For Take the action → Add 1

Drag down and give Decrease policy parameters



In Decrease Group wizard

Click on "Add new alarm"



Select the topic “Cpuutilizationabc”

Whenever Average of CPU utilization is select “<=“

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define. To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send a notification to: Cpuutilizationabc (skmarhaan999@gmail) [create topic](#)

Whenever: Average of CPU Utilization

Is: >= Percent

For at least: consecutive period(s) of 5 Minutes

Name of alarm: awsec2-myautoscalegrp-High-CPU-Utilization

CPU Utilization Percent

8/9 04:00 8/9 06:00 8/9 08:00

myautoscalegrp

[Cancel](#) [Create Alarm](#)

Give the value → 20

Click on “Create Alarm” button

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define. To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send a notification to: Cpuutilizationabc (skmarhaan999@gmail) [create topic](#)

Whenever: Average of CPU Utilization

Is: <= 20 Percent

For at least: 1 consecutive period(s) of 5 Minutes

Name of alarm: awsec2-myautoscalegrp-High-CPU-Utilization

CPU Utilization Percent

8/9 04:00 8/9 06:00 8/9 08:00

myautoscalegrp

[Cancel](#) [Create Alarm](#)

Check the summary

Click on “Next: Configure Notificaiton”

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateAutoScalingGroup:source=lc:launchConfigurationName=mylaunch...>. The page title is "Create Auto Scaling Group". The navigation bar includes "Services", "Resource Groups", "student", "Oregon", and "Support". The main content area has tabs: "1. Configure Auto Scaling group details", "2. Configure scaling policies" (which is selected), "3. Configure Notifications", "4. Configure Tags", and "5. Review". Below the tabs, there's a section titled "Decrease Group Size" with a "Name" field set to "Decrease Group Size". Under "Execute policy when:", it shows "awsec2-myautoscalegrp-High-CPU-Utilization" with a description: "breaches the alarm threshold: CPUUtilization <= 20 for 300 seconds for the metric dimensions AutoScalingGroupName = myautoscalegrp". Under "Take the action:", it shows "Remove" followed by "1 instances" and "when 20 >= CPUUtilization > -infinity". There's also a link "Create a simple scaling policy". At the bottom right of the content area, there are buttons: "Cancel", "Previous", "Review" (which is highlighted in blue), and "Next: Configure Notifications". 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".

Click on “Add notification” button

The screenshot shows the AWS EC2 Management Console with the same URL as the previous screenshot. The page title is "Create Auto Scaling Group". The navigation bar and tabs are identical. The main content area has tabs: "1. Configure Auto Scaling group details", "2. Configure scaling policies", "3. Configure Notifications" (which is selected), "4. Configure Tags", and "5. Review". Below the tabs, there's a section with the heading "Create Auto Scaling Group" and a sub-instruction: "Configure your Auto Scaling group to send notifications to a specified endpoint, such as an email address, whenever a specified event takes place, including: successful launch of an instance, failed instance launch, instance termination, and failed instance termination." It also says "If you created a new topic, check your email for a confirmation message and click the included link to confirm your subscription. Notifications can only be sent to confirmed addresses." At the bottom left, there's a button "Add notification" with a cursor pointing at it. At the bottom right, there are buttons: "Cancel", "Previous", "Review" (highlighted in blue), and "Next: Configure Tags". The footer is the same as the previous screenshot.

Check the following output

Click on “Next: Configure tags”

The screenshot shows the AWS EC2 Management Console interface for creating an Auto Scaling group. The current step is "3. Configure Notifications". The configuration section allows sending notifications to an email address (Cpuutilizationabc (skmarhaan999@gmail.com)) and selecting events: launch, terminate, fail to launch, and fail to terminate. Below this is an "Add notification" button. At the bottom right are "Cancel", "Previous", "Review", and "Next: Configure Tags" buttons. The "Next: Configure Tags" button is highlighted with a mouse cursor.

For tag key → Name

For tag Value → WebAutoscale

Click on **Review** button

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2 autoscaling/home?region=us-west-2#CreateAutoScalingGroup:source=lc!launchConfigurationName=mylaunch...>. The page is titled 'Create Auto Scaling Group'. It's step 4 of 5, 'Configure Tags'. A table shows one tag: 'Name' with value 'WebAutoscale'. There are buttons for 'Add tag' and '49 remaining'. At the bottom right are 'Cancel', 'Previous', and a blue 'Review' button.

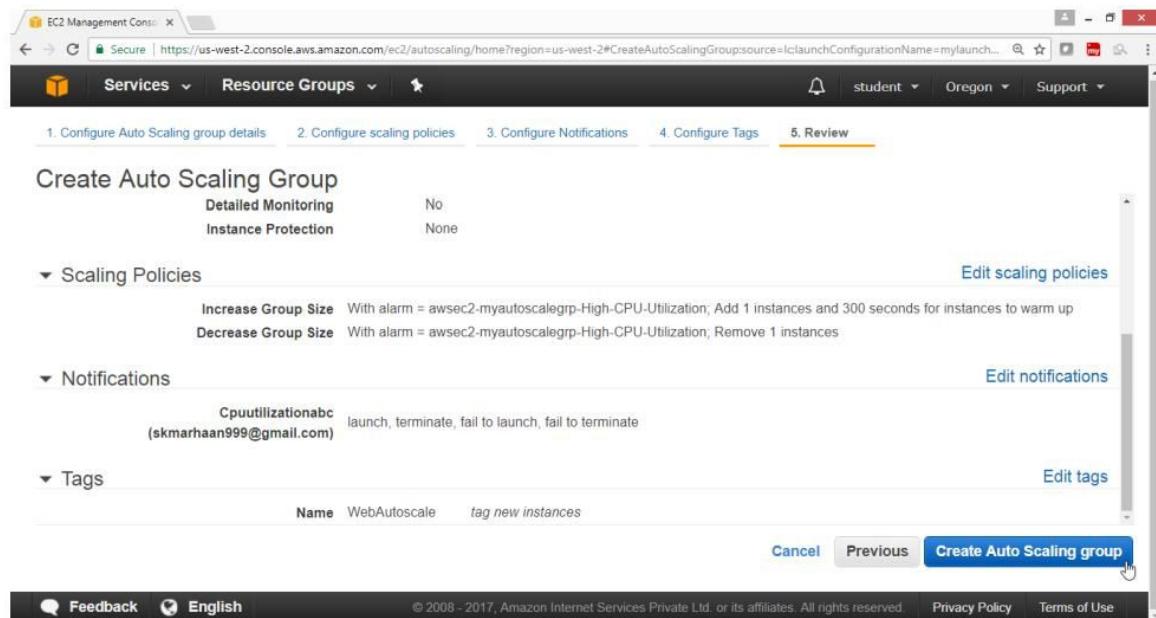
Check the summary

Drag down

The screenshot shows the AWS EC2 Management Console with the same URL as the previous screenshot. It's step 5 of 5, 'Review'. The summary section includes 'Auto Scaling Group Details' (Group name: myautoscalegrp, Group size: 1, Minimum Group Size: 1, Maximum Group Size: 3, Subnet(s): subnet-19d0f141, subnet-13f60e5a, subnet-8b9e38ec, Health Check Grace Period: 300, Detailed Monitoring: No, Instance Protection: None) and 'Scaling Policies' (Edit scaling policies). At the bottom right are 'Cancel', 'Previous', and a blue 'Create Auto Scaling group' button.

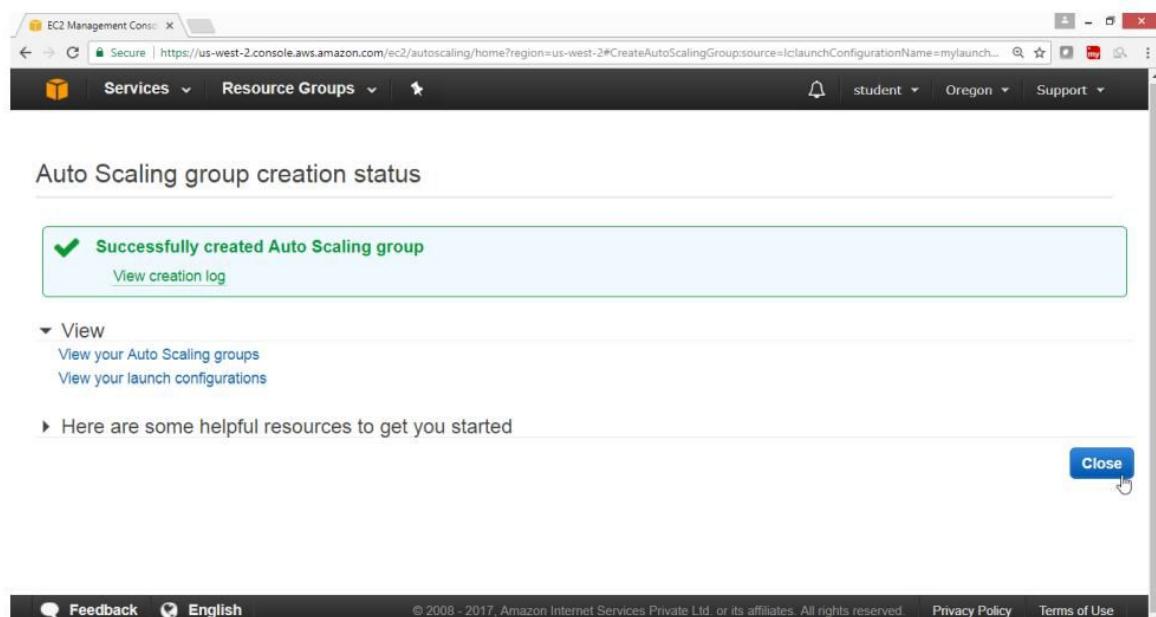
Drag down

Click on “Create Auto Scaling group” button



Successfully created

Click on **Close** button



Verification

Now go to EC2 Dash Board

Click on Instances

Observer that WebAutoscale instance got launched

The screenshot shows the AWS EC2 Management Console interface. The left sidebar has 'Instances' selected. The main area displays a table of instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
linuxweba	i-0e42235250367123e	t2.micro	us-west-2a	stopped	None	
WebAutoscale	i-0a7aaafe87044125e	t2.micro	us-west-2c	running	Initializing	None

A message at the bottom says "Select an instance above".

Now login to Web Autoscale instance

The screenshot shows the AWS EC2 Management Console interface, similar to the previous one, but with the 'WebAutoscale' instance selected. The 'Actions' tab is active. The main area shows the instance details:

Instance: i-0a7aaafe87044125e (WebAutoscale) Public DNS: ec2-54-244-159-247.us-west-2.compute.amazonaws.com

Below this, there are tabs for Description, Status Checks, Monitoring, and Tags. Under the Instance ID section, it shows "Instance ID: i-0a7aaafe87044125e" and "Public DNS (IPv4): ec2-54-244-159-247.us-west-2.compute.amazonaws.com".

Run the following command to increase the load

```
# yum install stress  
# stress --cpu --timeout 1000
```

Verification

After 15 minutes 3 instance got loaded automatically

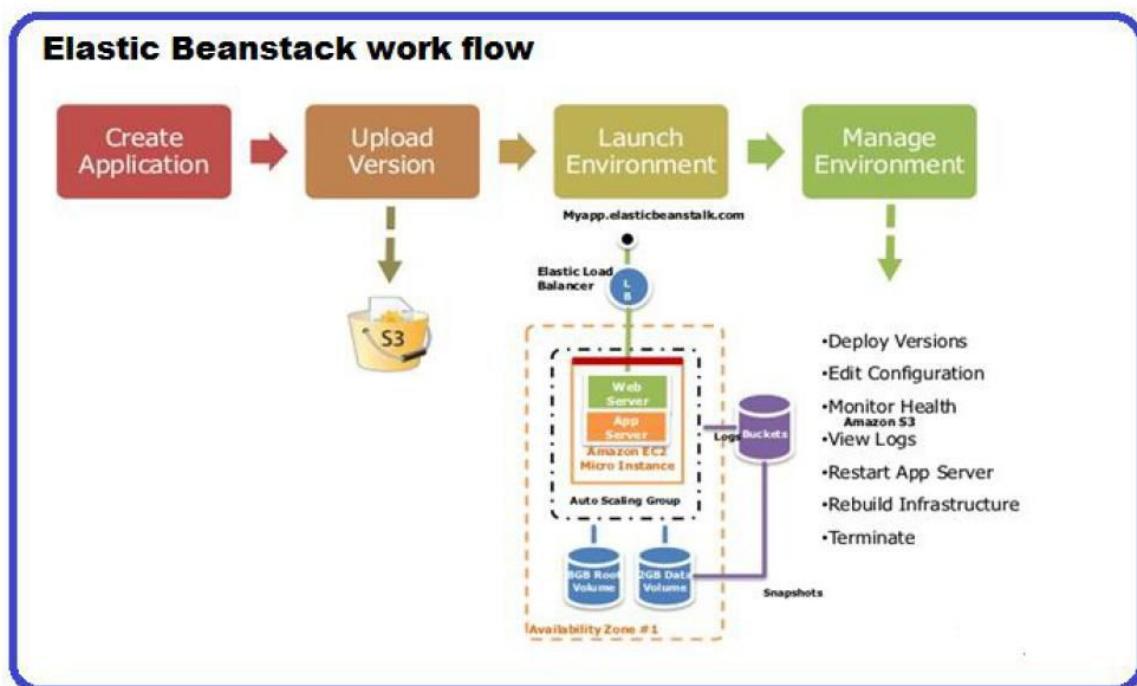
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
linuxweba	i-0e42235250367123e	t2.micro	us-west-2a	stopped	None	
WebAutoscale	i-045d526a506c6da75	t2.micro	us-west-2a	running	2/2 checks ...	None
WebAutoscale	i-0a7aaafe87044125e	t2.micro	us-west-2c	running	2/2 checks ...	None
WebAutoscale	i-0c07b9b3df34adc7c	t2.micro	us-west-2b	running	2/2 checks ...	None

Lab 14: To Configure an Elastic Beanstalk with Tomcat Application

OBJECTIVE

To configure Elastic Beanstalk in AWS

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with AWSElasticBeanstalkFullAccess

TASK :

Create Elastic Beanstalk Tomcat Application

Deploy java war files

Open Browser and check your web application

Practical Steps

1) To create Elastic Beanstalk Application

Open AWS Console

Select **Compute** service

Click on “**Elastic BeanStalk**”

The screenshot shows the AWS Management Console homepage with the URL <https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2>. The top navigation bar includes 'Services' and 'Resource Groups'. The main content area is titled 'Amazon Web Services' and features a 'Compute' section with icons for EC2, EC2 Container Service, Lightsail, Elastic Beanstalk, Lambda, and Batch. Below this are sections for 'Storage' (S3, EFS, Glacier, Storage Gateway), 'Developer Tools' (CodeStar, CodeCommit, CodeBuild, CodeDeploy, CodePipeline, X-Ray), 'Management Tools' (CloudWatch, CloudFormation, CloudTrail, Config), 'Internet of Things' (AWS IoT, AWS Greengrass), 'Contact Center' (Amazon Connect), 'Game Development' (Amazon GameLift), 'Mobile Services' (Mobile Hub, Cognito, Device Farm, Mobile Analytics), and 'Additional Resources' (AWS Console Mobile App, AWS Marketplace). A 'Resource Groups' sidebar on the right explains what they are and provides a 'Create a Group' button.

"Welcome to Amazon Elastic Beanstalk" page opens

Click on "Get started" button

The screenshot shows the AWS Elastic Beanstalk Management console. At the top, there's a navigation bar with tabs for Services, Resource Groups, and a search bar. Below the navigation is a sub-navigation bar with links for Create New Application, Services, Resource Groups, and Support. The main content area has a title "Welcome to AWS Elastic Beanstalk". It features a summary section with metrics: Average Latency (53.6 ms), Sum Requests (148K), CPU Utilization (65%), Max Network In (354KB), and Maximum Unavailable (12KB). Below this is a "Monitoring" section with two line graphs: "Average Latency in seconds" and "Auto Scaling in Count". A large blue "Get started" button is prominently displayed at the bottom of the main content area.

On “Create a Web app”, page, provide values

Application Name → Tomcatapp

Environment Name → Tomcatenv

Drag down

The screenshot shows the 'Create a web app' page in the AWS Elastic Beanstalk Management Console. The URL is https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2#/gettingStarted. The page has a header with 'Services', 'Resource Groups', and 'Elastic Beanstalk' tabs, and a 'Create New Application' button. The main content area is titled 'Create a web app' with a sub-section 'Application information'. It shows an 'Application name' field containing 'Tomcatapp' with a note: 'Up to 100 Unicode characters, not including forward slash (/)'. Below it is an 'Environment information' section with an 'Environment name' field containing 'tomcatenv' and a 'Domain' field showing '.us-west-2.elasticbeanstalk.com'. A note says 'Choose the name, subdomain, and description for your environment. These cannot be changed later.'

In Platform box select Tomcat

Drag down

The screenshot shows the 'Base configuration' section of the AWS Elastic Beanstalk console. The 'Platform' dropdown is open, displaying a list of options. 'Tomcat' is highlighted with a blue selection bar. Other options visible include '-- Choose a platform --', 'Preconfigured' (Node.js, PHP, Python, Ruby), '.NET (Windows/IIS)', 'Java', 'Go', 'Packer', 'Preconfigured – Docker' (GlassFish, Go, Python), 'Generic', 'Docker', and 'Multi-container Docker'. Below the dropdown, there is a note about moving to a new design and links for feedback and English language selection. At the bottom are 'Configure more options', 'Cancel', and 'Create application' buttons.

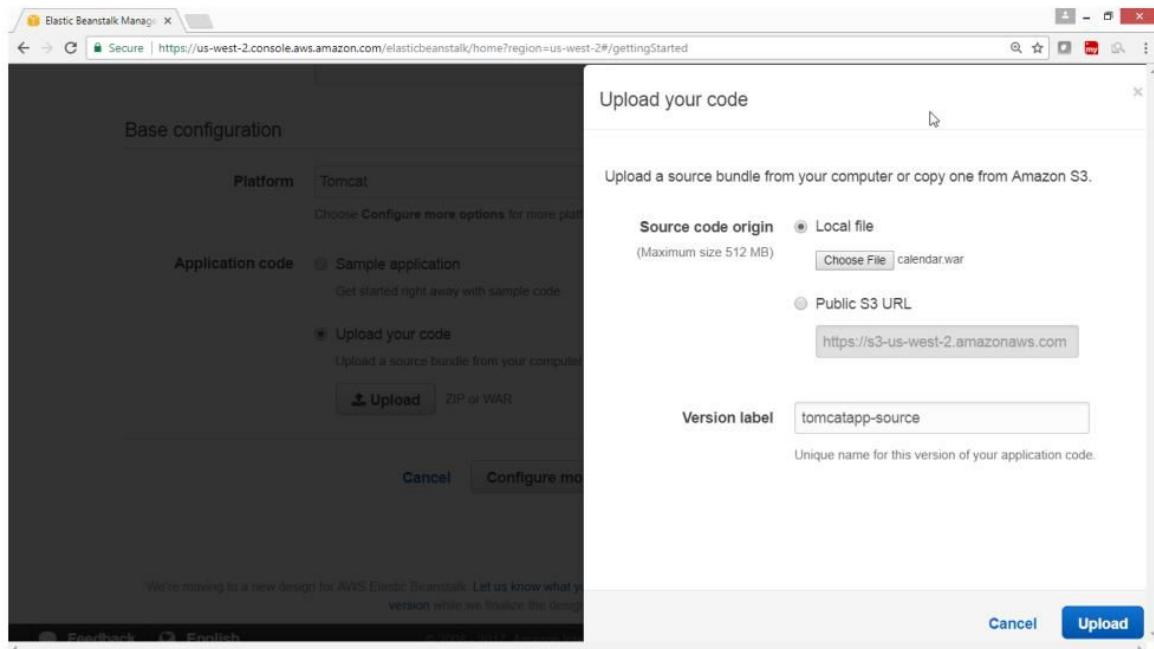
Select Upload your code

The screenshot shows the 'Base configuration' section with the 'Platform' set to 'Tomcat'. The 'Application code' section has a radio button selected for 'Upload your code'. A note says 'Get started right away with sample code.' Below it is a 'Upload' button with a file icon and the text 'ZIP or WAR'. At the bottom are 'Cancel', 'Configure more options', and 'Create application' buttons. A note at the bottom indicates a design change and links for feedback and English language selection.

Upload calendar.war file

Click on **Upload** button

Leave remaining fields as defaults



Verify that file is uploaded, beside **Upload** button

Click “Create Application” button

Base configuration

Platform: Tomcat

Choose [Configure more options](#) for more platform configuration options.

Application code:

- Sample application
- Upload your code

Get started right away with sample code.

Upload a source bundle from your computer or copy one from Amazon S3.

Upload tomcatapp-source.zip

Create application

Verification :

Tomcat application at background is getting created,

Progress on screen are displayed

Creating tomcatenv

This will take a few minutes..

4:28pm Using elasticbeanstalk-us-west-2-523251683217 as Amazon S3 storage bucket for environment data.

4:28pm createEnvironment is starting.

Learn More

- [Get started using Elastic Beanstalk](#)
- [Modify the code](#)
- [Create and connect to a database](#)
- [Add a custom domain](#)

Featured

[Create your own custom platform](#)

Command Line Interface (v3)

[Installing the AWS EB CLI](#)

[EB CLI Command Reference](#)

Verify

The screenshot shows a browser window titled 'Create Environment' with the URL <https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2#/environment?applicationName=Tomcatapp&environmentId=e-yg...>. The main content area displays a progress log for creating the environment 'tomcatenv'. The log entries are:

- 4:29pm Waiting for EC2 Instances to launch. This may take a few minutes.
- 4:28pm Created EIP: 34.213.99.251
- 4:28pm Environment health has transitioned to Pending. Initialization in progress (running for 29 seconds). There are no instances.
- 4:28pm Created security group named: awseb-e-ygqrzkbwwc-stack-AWSEBSecurityGroup-1NRF9H19B86AF
- 4:28pm Using elasticbeanstalk-us-west-2-523251683217 as Amazon S3 storage bucket for environment data.
- 4:28pm createEnvironment is starting.

To the right of the log, there is a 'Learn More' sidebar with links to 'Get started using Elastic Beanstalk', 'Modify the code', 'Create and connect to a database', and 'Add a custom domain'. Below that is a 'Featured' section with a link to 'Create your own custom platform', followed by a 'Command Line Interface (v3)' section and a link to 'Installing the AWS EB CLI'.

Note : This will take few minutes to start.

Wait until Tomcat Dashboard is displayed on the screen

Click on the URL link

The screenshot shows the 'Tomcatapp - Dashboard' page in the AWS Elastic Beanstalk console. The URL is <https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2#/environment/dashboard?applicationName=Tomcatapp&environmentId=e-yg...>. The dashboard provides an overview of the application's status, including:

- Overview:** Shows the environment ID (e-ygqrzkbwwc) and URL (tomcatenv.s9z85gpkn.k.us-west-2.elasticbeanstalk.com).
- Health:** Status is 'Ok' (indicated by a green checkmark icon).
- Running Version:** tomcatapp-source.
- Configuration:** Shows the operating system as '64bit Amazon Linux 2017.03' and the Java version as 'v2.6.2 running Tomcat 8 Java 8'.

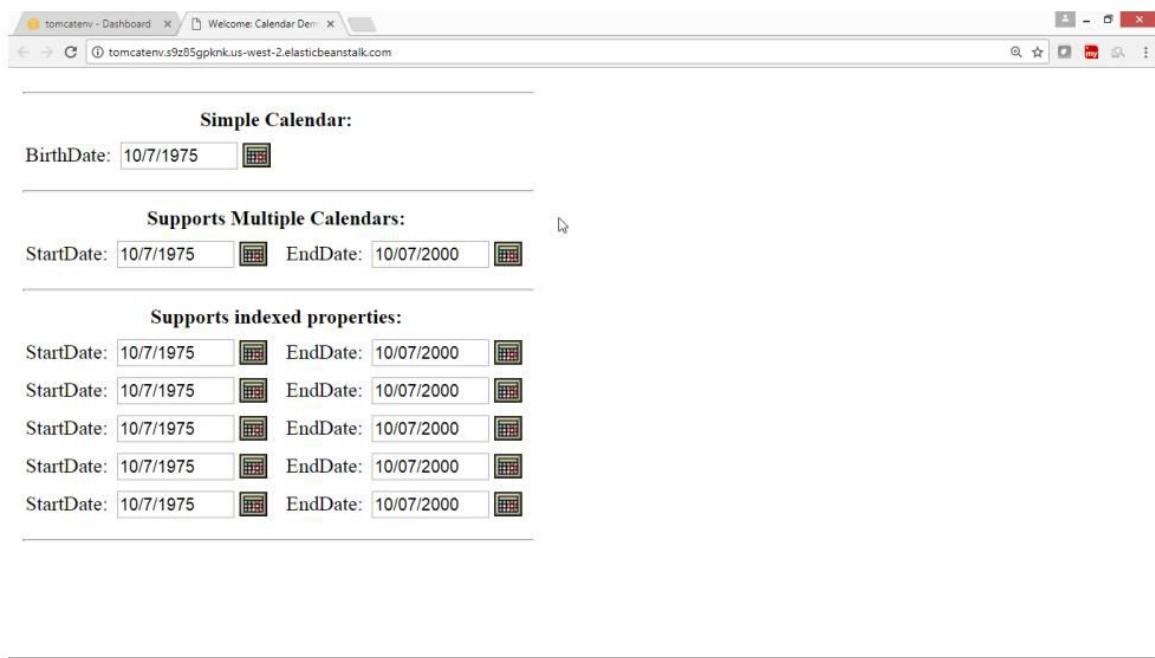
The left sidebar includes links for 'Dashboard', 'Overview', 'Configuration', 'Logs', 'Health', 'Monitoring', and 'Alarms'. A 'Managed' link at the bottom of the sidebar points to <https://tomcatenv.s9z85gpkn.k.us-west-2.elasticbeanstalk.com>.

Verification

Open any Browser

Click on URL link

Website is open



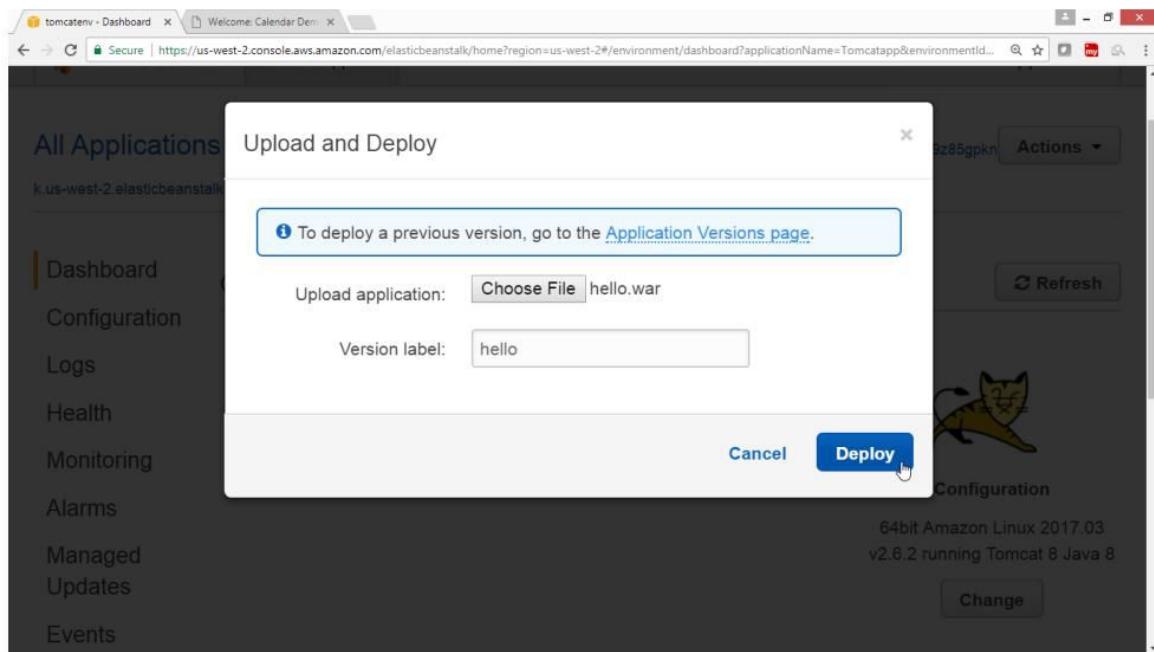
The screenshot shows a web browser window with the title "tomcatenv - Dashboard" and the URL "tomcatenv.s9z85gpknk.us-west-2.elasticbeanstalk.com". The page displays a "Simple Calendar:" section with a birth date input field containing "10/7/1975" and a calendar icon. Below it is a "Supports Multiple Calendars:" section with start and end date inputs both set to "10/7/1975" and calendar icons. Underneath is a "Supports indexed properties:" section containing five identical date input pairs, each with a start date of "10/7/1975", an end date of "10/07/2000", and calendar icons.

To Deploy another war file for eg hello.war

Go to Upload application

Choose file provide **hello.war** file name

Click **Deploy** button



Click on URL

The screenshot shows the AWS Elastic Beanstalk Dashboard for the Tomcatapp environment. The URL is https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2#environment/dashboard?applicationName=Tomcatapp&environmentId=... . The dashboard includes sections for Overview, Health (Ok), Running Version (hello), Configuration (with a cartoon cat icon), and Events. A sidebar on the left lists options like Dashboard, Configuration, Logs, Health, Monitoring, Alarms, Managed Updates, and Events.

Verify the website

The screenshot shows a web browser displaying the 'Hello Index' page from the Tomcatapp environment. The URL is tomcatenv.s9z85gpkn.us-west-2.elasticbeanstalk.com. The page content is "Hello Index".

Hello Index

Try the [servlet](#).

4) To Remove Elastic Bean stack

Select Action button

Click Delete application button

The screenshot shows the AWS Elastic Beanstalk console with the URL <https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2#applications>. The 'Resource Groups' tab is selected. On the left, there's a sidebar with links like 'Get started using Elastic Beanstalk', 'Modify the code', 'Create and connect to a database', 'Add a custom domain', 'Featured', 'Create your own custom platform', and 'Command Line Interface (v3)'. The main area displays a list of applications under 'All Applications'. The 'Tomcatapp' application is selected, showing its details: 'Environment tier: Web Server', 'Platform: 64bit Amazon Linux 2017.03 v2.6.2 running Tomcat 8 Java 8', 'Running versions: hello', 'Last modified: 2017-07-27 16:40:51 UTC+0530', and 'URL: tomcatenv.s9z85gpknk.us-west-2.elasticbeanst...'. A context menu is open over the 'Tomcatapp' card, with the 'Actions' dropdown expanded. The 'Delete application' option is highlighted with a blue background and white text.

The screenshot shows the AWS Elastic Beanstalk console with the same URL as the previous screenshot. A confirmation dialog box is overlaid on the page, asking 'Are you sure you want to delete the application: Tomcatapp?'. The dialog has two buttons: 'Cancel' and a red 'Delete' button. In the background, the 'Tomcatapp' application details are visible, identical to the previous screenshot.

Application will now get terminated

The screenshot shows the AWS Elastic Beanstalk console. In the top navigation bar, 'Services' and 'Resource Groups' are selected. Below the navigation, there's a search bar and a dropdown for 'student' and 'Oregon'. A 'Create New Application' button is visible. On the left, a sidebar titled 'Learn More' includes links for getting started with Elastic Beanstalk, modifying code, connecting to databases, and adding custom domains. A 'Featured' section links to creating custom platforms and the Command Line Interface (v3). The main content area is titled 'All Applications' and shows a single application named 'Tomcatapp'. A sub-section for 'tomcatenv (Terminated)' is displayed, showing details: Environment tier: Web Server, Platform: 64bit Amazon Linux 2017.03 v2.6.2 running Tomcat 8 Java 8, Running versions: hello, Last modified: 2017-07-27 16:48:14 UTC+0530, and URL: tomcatenv.s9z85gpknk.us-west-2.elasticbeanst... An 'Actions' dropdown menu is shown next to the application name.

Verification

After termination following screen will come

The screenshot shows the AWS Elastic Beanstalk console. The top navigation bar and sidebar are identical to the previous screenshot. The main content area displays a large 'Welcome to AWS Elastic Beanstalk' message. Below it, a sub-section for 'MobileBackend' provides monitoring statistics: Average Latency in milliseconds (53.6), Sum Requests (148K), CPU Utilization (65%), Max Network In (354KB), and Maximum Dwellseconds (12KB). It also features two line graphs: 'Average Latency in seconds' and 'Sum Requests by second'. To the right of the graphs, text explains the benefits of using Elastic Beanstalk: deploying, monitoring, and scaling applications quickly and easily. It also provides instructions for deploying existing web applications or sample applications using the EB CLI or Git.

3) To delete Elastic Beanstalk bucket policy is created in S3 bucket

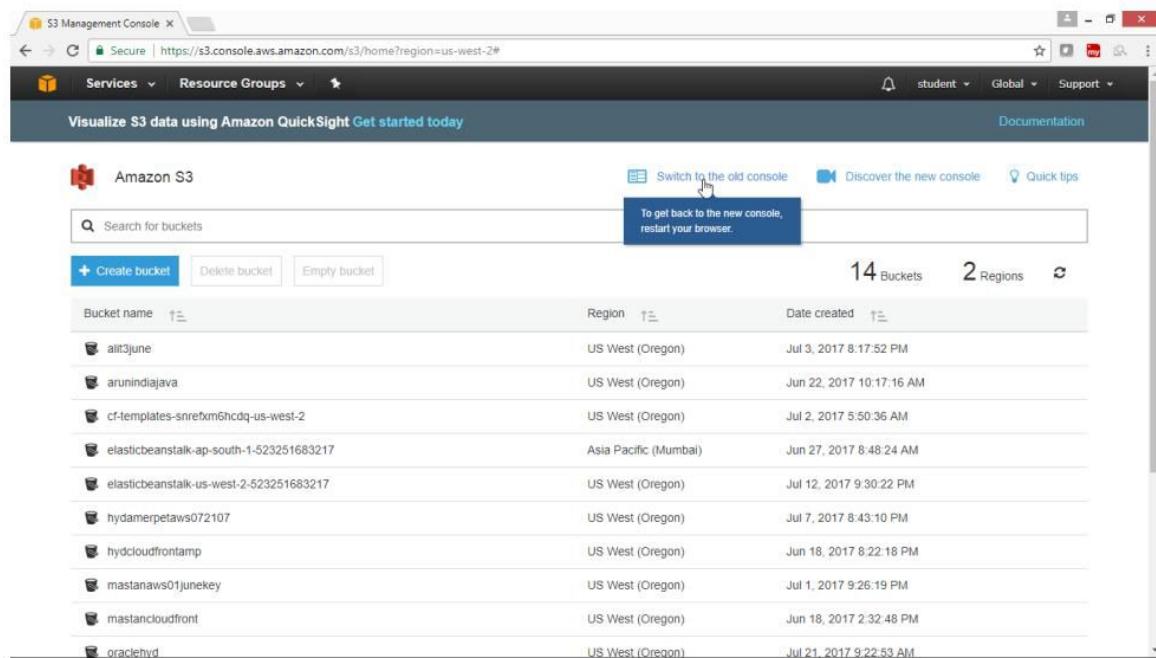
Note: S3 bucket created by Elastic Beanstalk is not deleted automatically.

It could be charged after free usage limits are over, so manually delete the beanstalk bucket

From console select “Storage”

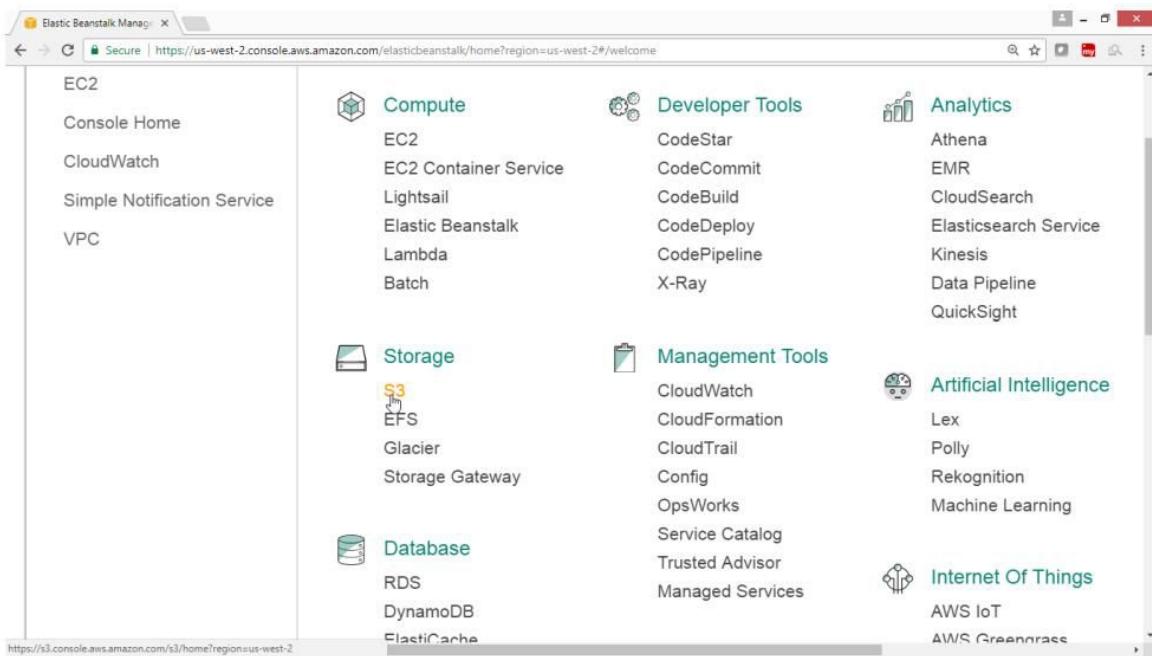
Select S3

Click on “Switch to old console”



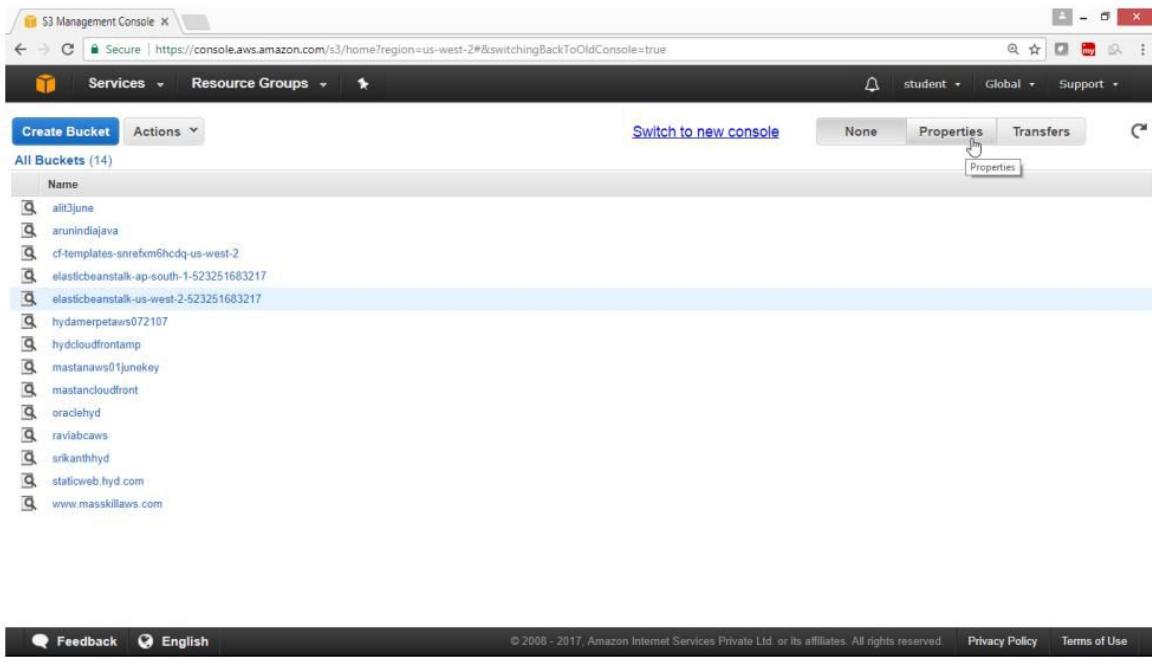
The screenshot shows the AWS S3 Management Console interface. At the top, there's a header bar with the AWS logo, user information (student), and navigation links (Services, Resource Groups). Below the header, a banner says "Visualize S3 data using Amazon QuickSight Get started today". The main area is titled "Amazon S3" and contains a search bar with placeholder "Search for buckets". Below the search bar are three buttons: "+ Create bucket", "Delete bucket", and "Empty bucket". To the right of these buttons, it shows "14 Buckets" and "2 Regions". A prominent blue button in the center says "Switch to the old console" with the sub-instruction "To get back to the new console, restart your browser." Below this, a table lists 14 buckets, each with a small icon, the bucket name, its region, and the date it was created. The buckets listed are:

Bucket name	Region	Date created
alit3june	US West (Oregon)	Jul 3, 2017 8:17:52 PM
arunindiajava	US West (Oregon)	Jun 22, 2017 10:17:16 AM
cf-templates-snrefxm6hcdq-us-west-2	US West (Oregon)	Jul 2, 2017 5:50:36 AM
elasticbeanstalk-ap-south-1-523251683217	Asia Pacific (Mumbai)	Jun 27, 2017 8:48:24 AM
elasticbeanstalk-us-west-2-523251683217	US West (Oregon)	Jul 12, 2017 9:30:22 PM
hydamerpetaws072107	US West (Oregon)	Jul 7, 2017 8:43:10 PM
hydcloudfrontamp	US West (Oregon)	Jun 18, 2017 8:22:18 PM
mastanaws01junekey	US West (Oregon)	Jul 1, 2017 9:26:19 PM
mastancloudfront	US West (Oregon)	Jun 18, 2017 2:32:48 PM
oraclehyd	US West (Oregon)	Jul 21, 2017 9:22:53 AM



Select elastic Beanstalk Bucket, Click Properties

Select Permissions



Click "Edit bucket policy"

The screenshot shows the AWS S3 Management Console. On the left, a sidebar lists 'All Buckets (14)' with various buckets. One bucket, 'elasticbeanstalk-us-west-2-523251683217', is selected and highlighted with a blue background. On the right, the main panel displays the details for this bucket, including its name, region (Oregon), creation date (Wed Jul 12 21:30:22 GMT+530 2017), and owner (skmval999). Below this, the 'Permissions' section is visible, featuring a 'Grantee' field set to 'skmval999' and several checkboxes for 'List', 'Upload/Delete', and 'View Permissions'. At the bottom of the permissions section, there are three buttons: 'Add more permissions', 'Edit bucket policy' (which is currently being edited), and 'Add CORS Configuration'. A 'Save' button is located at the bottom right of the main panel.

In Bucket Policy Editor wizard,

Click Delete to remove policy, click OK

The screenshot shows the AWS S3 Management Console with the 'Bucket Policy Editor' dialog box open. The dialog box contains the JSON policy for the selected bucket. The policy denies deletion from all principals and allows it from the principal 'arn:aws:iam::523251683217:role/elasticbeanstalk-ec2-role'. The dialog box includes a 'Cancel' button and a 'Delete' button, with the 'Delete' button highlighted with a yellow border. The rest of the interface is similar to the previous screenshot, showing the list of buckets on the left and the bucket details on the right.

Click on Save button

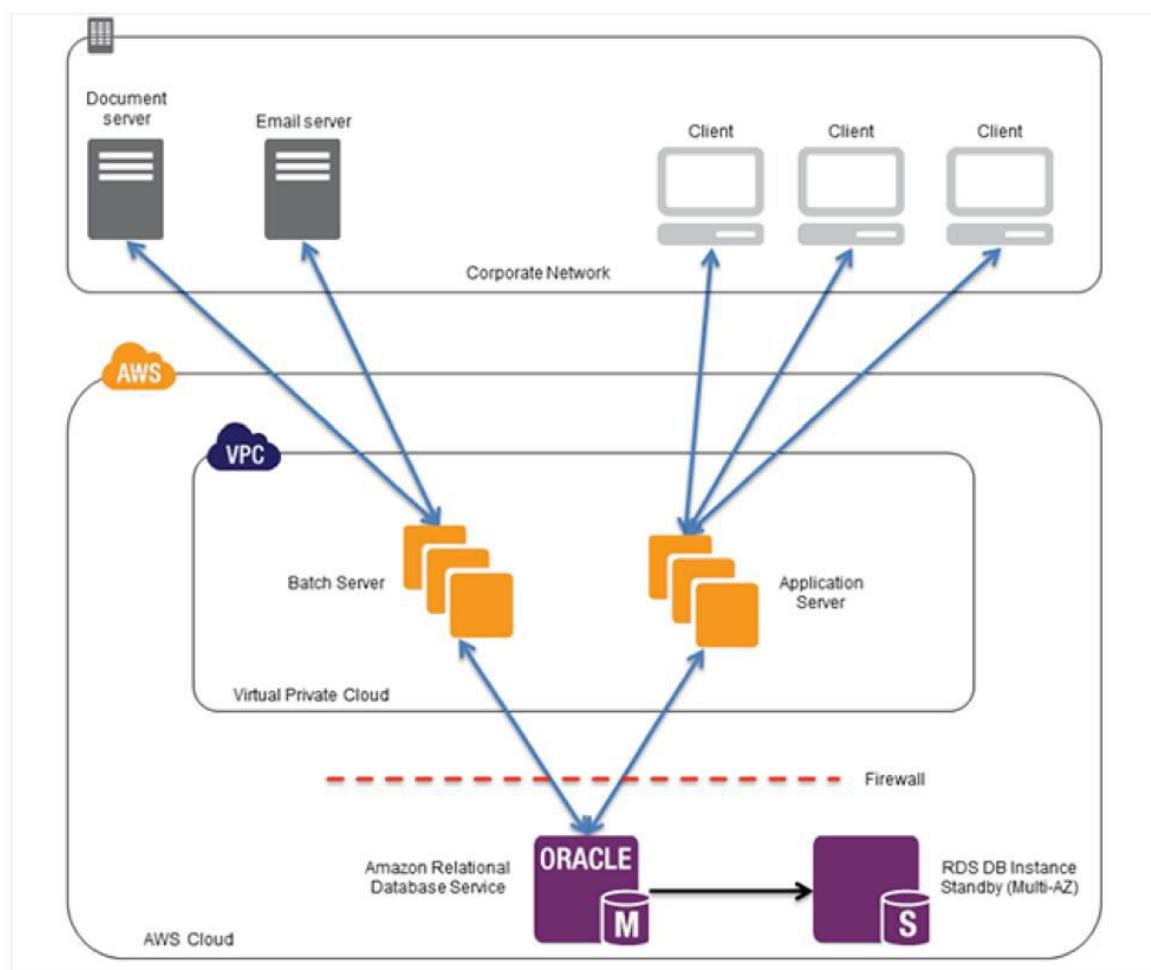
The screenshot shows the AWS S3 Management Console. On the left, a sidebar lists 'All Buckets (14)' with various bucket names. The bucket 'elasticbeanstalk-us-west-2-523251683217' is selected and shown in the main pane. The right pane displays the bucket details: Bucket: elasticbeanstalk-us-west-2-523251683217, Region: Oregon, Creation Date: Wed Jul 12 21:30:22 GMT+530 2017, Owner: skmval999. Below this, the 'Permissions' section is expanded, showing a grantee input field with 'skmval999' and several checkboxes: List, Upload/Delete, View Permissions, and Edit Permissions (which is checked). At the bottom of the permissions section are three buttons: 'Add more permissions', 'Add bucket policy', and 'Add CORS Configuration'. A prominent yellow arrow points to the 'Save' button at the bottom right of the permissions section.

Lab 15: To Configure an Amazon Relational Database Service

OBJECTIVE

To configure Amazon Relation Database service

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user withAmazonRDSFullAccess

Task

Create Amazon Relational Database Service

Verify connection from mysql client command line tool

Verify Connection using MySQL Workbench client application

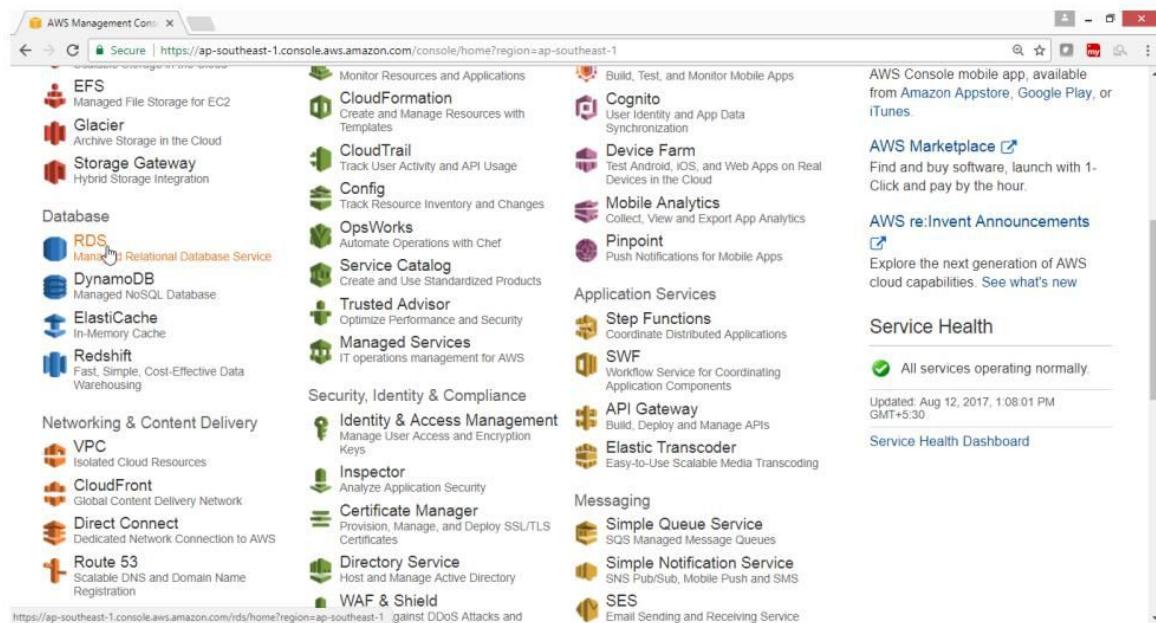
Practical Steps

To create Amazon Relational Database Service

From the AWS console

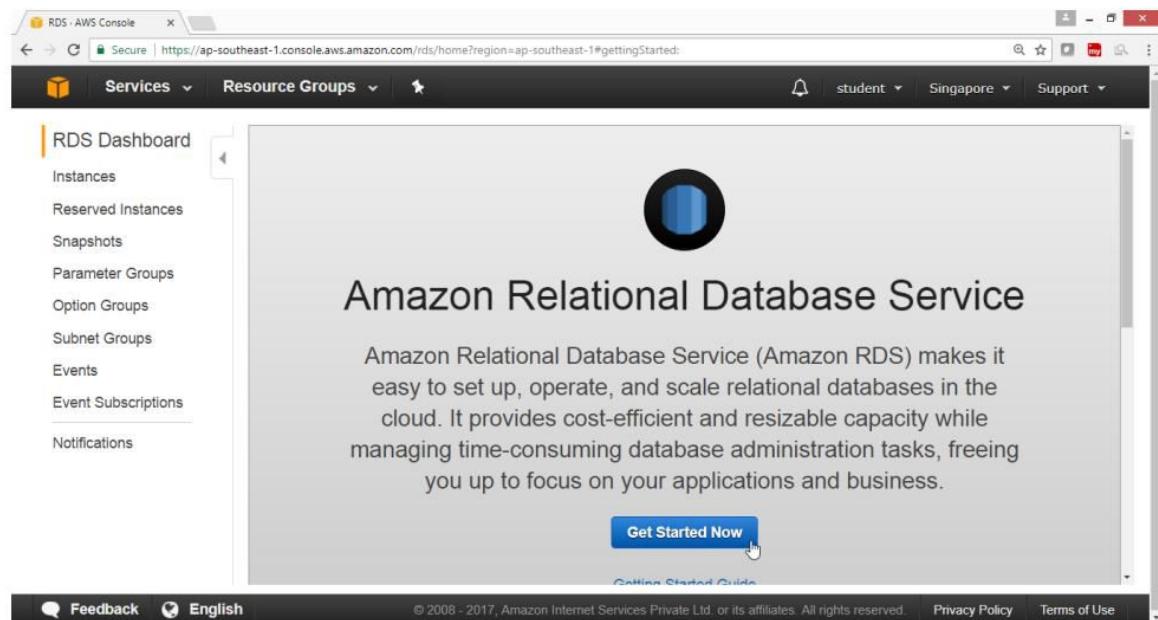
Select Database

Click on RDS service



In “RDS Dashboard”, wizard

Click “Get Started Now”, button



In Select Engine, wizard

Click on MySQL

Click on Select button

To get started, choose a DB Engine below and click Select.

MySQL
MySQL Community Edition

MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.

- Supports database size up to 6 TB.
- Instances offer up to 32 vCPUs and 244 GiB Memory.
- Supports automated backup and point-in-time recovery.
- Supports cross-region read replicas.
- Free tier eligible

Select

In Production wizard

select Dev/Test, Choose MySQL

Do you plan to use this database for production purposes?

Production

MySQL
Use Multi-AZ Deployment and Provisioned IOPS Storage as defaults for high availability and fast, consistent performance.

Dev/Test

MySQL
This instance is intended for use outside of production or under the RDS Free Usage Tier.

Billing is based on [RDS pricing](#).

Cancel **Previous** **Next Step**

In **Specify DB Details**, wizard provide following values

Instance Specifications

- For DB Engine → mysql
For License Model → general-public-license
For DB Engine Version → 5.6.27 [leave default]
For DB Instance Class → db.t2.micro
For Multi-AZ Deployment → No
For Storage Type → General Purpose SSD
For Allocated Storage → 5 GB

The screenshot shows the 'Specify DB Details' step of the AWS RDS wizard. On the left, a sidebar lists steps: Step 1: Select Engine, Step 2: Production?, Step 3: Specify DB Details (highlighted in blue), and Step 4: Configure Advanced Settings. Below the sidebar, a note says: 'Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#)'. The main panel has a title 'Specify DB Details' and a 'Free Tier' section with a note about the Free Tier providing a single db.t2.micro instance up to 20 GB of storage. There is a checkbox 'Only show options that are eligible for RDS Free Tier'. The 'Instance Specifications' section contains fields: 'DB Engine' set to 'mysql', 'License Model' set to 'general-public-license', and 'DB Engine Version' set to 'MySQL 5.6.35'. A tooltip for 'DB Engine Version' says: 'Version number of the database engine to be used for this instance.' At the bottom, there is a note: 'Review the Known Issues/Limitations to learn about potential compatibility issues with specific database versions.' and a dropdown for 'DB Instance Class' with the option '- Select One -'.

RDS - AWS Console

Secure | https://ap-southeast-1.console.aws.amazon.com/rds/home?region=ap-southeast-1#launch-dbinstance;ct=gettingStarted;

Services | Resource Groups

student | Singapore | Support

DB Engine: mysql
License Model: general-public-license
DB Engine Version: MySQL 5.6.35

DB Instance Class: db.t2.micro — 1 vCPU, 1 GiB RAM
Multi-AZ Deployment: No
Storage Type: General Purpose (SSD)
Allocated Storage*: 5 GB

Billing estimate is based on on-demand usage as described in [Amazon RDS Pricing](#). Estimate does not include costs for backup storage, I/Os (if applicable), or data transfer.

Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#).

Review the Known Issues/Limitations to learn about potential compatibility issues with specific database versions.

General Purpose (S) storage is suitable for broad range of data workloads. Provides baseline of 3 IOPS/ and ability to burst to 3,000 IOPS.

Provisioned IOPS (P) storage is suitable for I/O-intensive database workloads. Provides flexibility to provision ranging from 1,000 to 30,000 IOPS.

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

Under Settings

For Allocated Storage* → 5 GB

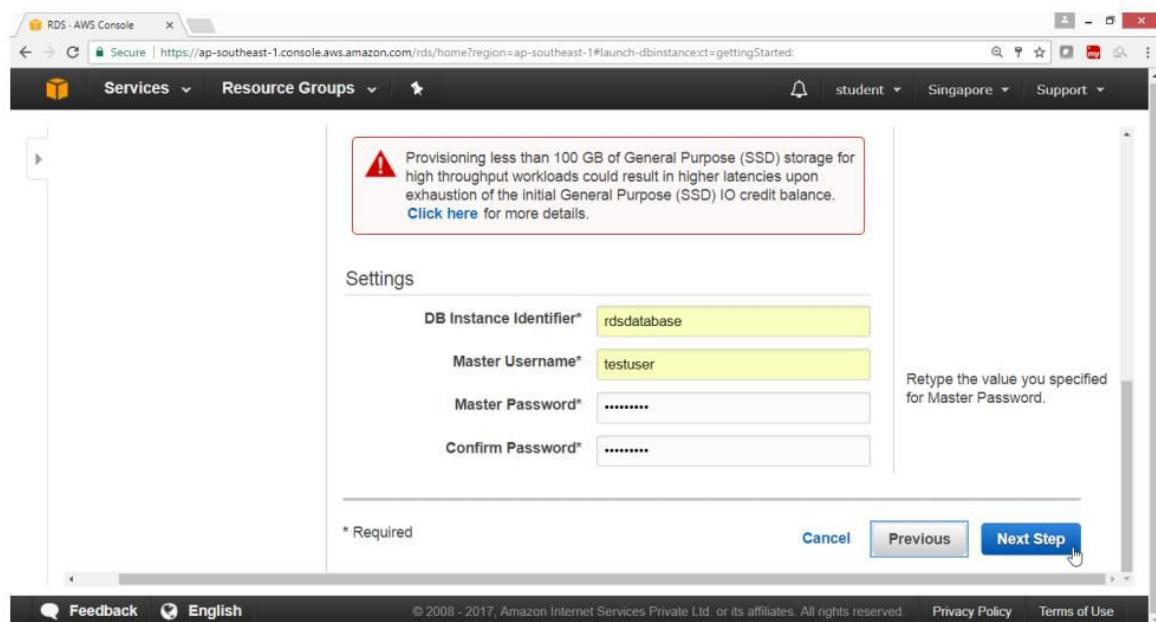
For DB Instance Identifier → rdsdatabase

For Master Username → testuser

For Master Password* → *****

For Confirm Password* → *****

Click on **Next** button.



In **Configure Advanced Settings**, wizard

Under **Network & Security**

Provide following Values

VPC*	→ Default VPC
Subnet Group	→ default
Publicly Accessible	→ Yes
Availability Zone	→ No Preference
VPC Security Group(s)	→ Create new Security Group

The screenshot shows the AWS RDS 'Configure Advanced Settings' wizard. On the left, a sidebar lists steps: Step 1: Select Engine, Step 2: Production?, Step 3: Specify DB Details, and Step 4: Configure Advanced Settings. The current step is Step 4. The main area is titled 'Configure Advanced Settings' under 'Network & Security'. It includes fields for VPC (Default VPC), Subnet Group (default), Publicly Accessible (Yes), Availability Zone (No Preference), and VPC Security Group(s). The 'VPC Security Group(s)' dropdown is open, showing options: Create new Security Group, default (VPC), launch-wizard-1 (VPC), and rds-launch-wizard (VPC). A tooltip on the right explains that security groups have rules authorizing connectivity of EC2 instances to the DB instance. At the bottom, there are links for Feedback, English, Privacy Policy, and Terms of Use.

Under Database Options

Provide following Values

Database Name	→ salesdba
Database Port	→ 3306
DB Parameter Group	→ default.mysql5.6
Option Group	→ default.mysql5.6
Copy Tags To Snapshots	→ leave blank
Enable IAM DB Authentication	→ No Preference
Enable Encryption	→ No

The screenshot shows the 'Database Options' configuration page in the AWS RDS console. The 'Database Name' is set to 'salesdba'. The 'Database Port' is set to '3306'. The 'DB Parameter Group' is set to 'default.mysql5.6'. The 'Option Group' is set to 'default.mysql5.6'. The 'Copy Tags To Snapshots' checkbox is unchecked. The 'Enable IAM DB Authentication' dropdown is set to 'No Preference'. The 'Enable Encryption' dropdown is set to 'No'. A note on the right side states: 'Specify a string of up to 63 alpha-numeric characters to define the name given to the database that Amazon RDS creates when it creates the DB instance, as in "mydb". If you do not specify a database name, Amazon RDS does not create a database when it creates the DB instance.' At the bottom, there are links for 'Feedback', 'English', 'Privacy Policy', and 'Terms of Use'.

Provider Following Values

Under Backup

- | | |
|-------------------------|-----------------|
| Backup Retention Period | → 7 days |
| Backup Window | → No Preference |

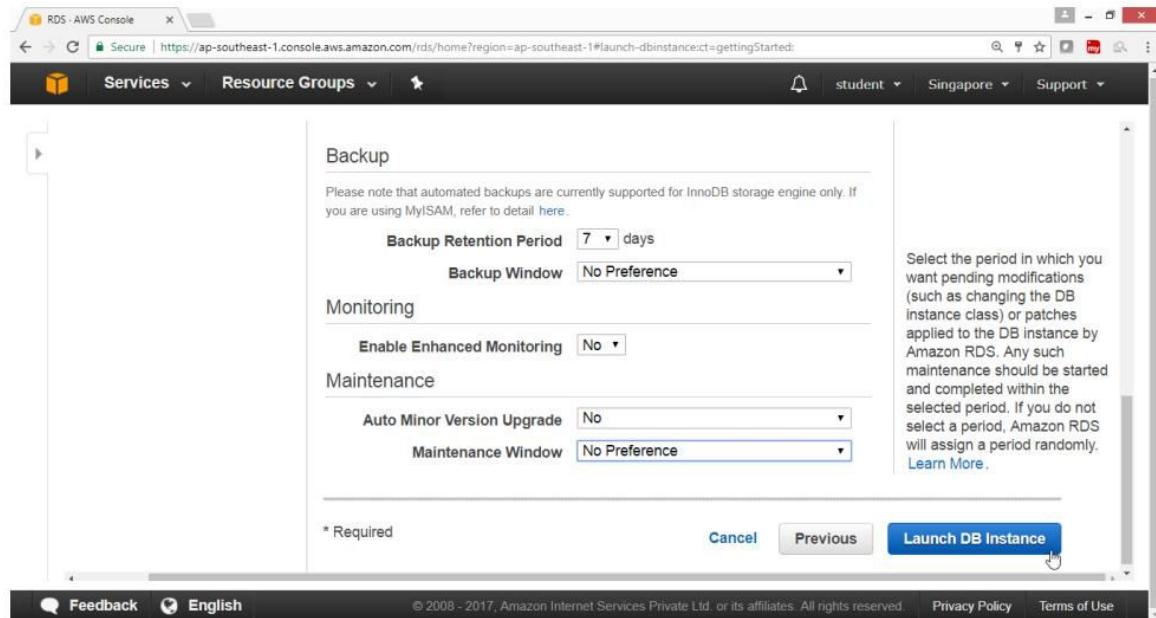
Under Monitoring

- | | |
|----------------------------|------|
| Enable Enhanced Monitoring | → No |
|----------------------------|------|

Under Maintenance

- | | |
|----------------------------|-----------------|
| Auto Minor Version Upgrade | → No |
| Maintenance Window | → No Preference |

Click on Launch DB Instance



Your DB Instance is being created.

Click on **View Your DB Instances** button

The screenshot shows the AWS RDS console with the URL <https://ap-southeast-1.console.aws.amazon.com/rds/home?region=ap-southeast-1#launch-dbinstance:ct=gettingStarted>. The page displays a progress bar with four steps: Step 1: Select Engine, Step 2: Production?, Step 3: Specify DB Details, and Step 4: Configure Advanced Settings. A green box highlights the message "Your DB Instance is being created." with a checkmark icon. Below it, a note says "Note: Your instance may take a few minutes to launch." Further down, there's a section titled "Connecting to your DB Instance" with a link "Learn about connecting to your DB instance". At the bottom right, a blue button labeled "View Your DB Instances" is visible, with a mouse cursor hovering over it.

Under status column

Verify **creating**

The screenshot shows the AWS RDS Dashboard with the URL <https://ap-southeast-1.console.aws.amazon.com/rds/home?region=ap-southeast-1#dbinstances:sf=all>. On the left, a sidebar lists options like Instances, Reserved Instances, Snapshots, Parameter Groups, Option Groups, Subnet Groups, Events, Event Subscriptions, and Notifications. The main area has tabs for "Launch DB Instance", "Show Monitoring", and "Instance Actions". It includes a filter for "All Instances" and a search bar for "Search DB Instances...". A table header shows columns for Engine, DB Instance, Status, CPU, Current Activity, Maintenance, Class, and VPC. A single row is shown with the following details: Engine: MySQL, DB Instance: rdsdatabase, Status: creating, CPU: None, Current Activity: None, Maintenance: None, Class: db.t2.micro, and VPC: vpc-ec2fe. The status "creating" is highlighted in orange. The footer includes links for Feedback, English, Privacy Policy, and Terms of Use.

Select MySQL Engine

The screenshot shows the AWS RDS console interface. On the left, there's a sidebar with options like Instances, Reserved Instances, Snapshots, Parameter Groups, Option Groups, Subnet Groups, Events, Event Subscriptions, and Notifications. The main area displays a table of DB instances. One instance is selected, showing details: Engine: MySQL, DB Instance: rdsdatabase, Status: creating, Current Activity: None, Class: db.t2.micro, VPC: vpc-ec2. Below the table, there are sections for Alarms and Recent Events and Monitoring. The Alarms and Recent Events table lists events such as 'DB instance deleted' and 'Finished DB Instance backup'. The Monitoring section shows CPU and Memory metrics with no data available.

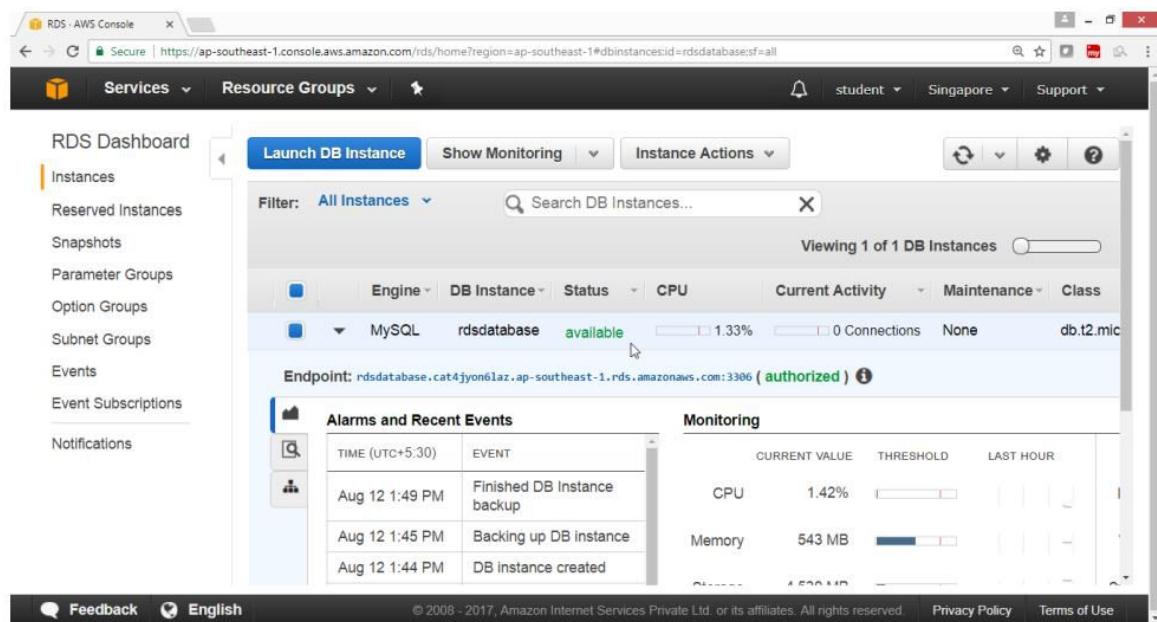
Under status column

Verify backing-up

This screenshot is similar to the previous one, showing the AWS RDS console. The instance status has changed to 'backing-up'. The endpoint now includes '(authorized)'. The monitoring section shows CPU and Memory metrics with no data available.

Under status column

Verify available



The screenshot shows the AWS RDS Dashboard. On the left, there's a sidebar with options like Instances, Reserved Instances, Snapshots, Parameter Groups, Option Groups, Subnet Groups, Events, Event Subscriptions, and Notifications. The main area has tabs for Launch DB Instance, Show Monitoring, and Instance Actions. A search bar and filter dropdown are also present. The main table displays one DB Instance:

Engine	DB Instance	Status	CPU	Current Activity	Maintenance	Class
MySQL	rdsdatabase	available	1.33%	0 Connections	None	db.t2.micro

Below the table, it says "Endpoint: rdsdatabase.cat4jyon6laz.ap-southeast-1.rds.amazonaws.com:3306 (authorized)". The "Monitoring" section shows CPU usage at 1.42% and Memory usage at 543 MB. The "Alarms and Recent Events" section lists recent events:

TIME (UTC+5:30)	EVENT
Aug 12 1:49 PM	Finished DB Instance backup
Aug 12 1:45 PM	Backing up DB instance
Aug 12 1:44 PM	DB instance created

Client Side

Go to linux box

Run mysql client command to connect to RDS database

Syt: \$ mysql -u <username> -h <End_point_of_RDS_Instance> -p <password>

```
shaikh@shaikh-virtual-machine:~$ mysql -u testuser -h rdsdatabase.clkyahad3ggx.ap-south-1.rds.amazonaws.com -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 31
Server version: 5.6.35-log MySQL Community Server (GPL)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
I
mysql> █
```

To see the list of databases;

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| innodb |
| mysql |
| performance_schema |
| salesdba |
| sys |
+-----+
6 rows in set (0.02 sec)

mysql> █
```

Use the database

Create table

Insert values in tables

```
mysql>
mysql> use salesdba;
Database changed
mysql>
mysql> create table tutorials_tbl(tutorial_id INT NOT NULL AUTO_INCREMENT,tutorial_title VARCHAR(100) NOT NULL,tutorial_author VARCHAR(40) NOT NULL,submission_date DATE,PRIMARY KEY ( tutorial_id ));
Query OK, 0 rows affected (0.04 sec) █

mysql>
mysql> INSERT INTO tutorials_tbl(tutorial_title, tutorial_author, submission_date) VALUES(
"Learn PHP", "John Poul", NOW());
Query OK, 1 row affected, 1 warning (0.02 sec)

mysql>
mysql> INSERT INTO tutorials_tbl(tutorial_title, tutorial_author, submission_date) VALUES(
"Learn MySQL", "Abdul S", NOW());
Query OK, 1 row affected, 1 warning (0.03 sec)

mysql>
mysql> INSERT INTO tutorials_tbl(tutorial_title, tutorial_author, submission_date) VALUES(
"JAVA Tutorial", "Sanjay", '2007-05-06');
Query OK, 1 row affected (0.02 sec)

mysql>
mysql>
mysql>
mysql>
mysql>
mysql> █
```

To see the structure of table;

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| innodb |
| mysql |
| performance_schema |
| salesdba |
| sys |
+-----+
6 rows in set (0.02 sec)

mysql> use salesdba;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> desc tutorials_tbl;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| tutorial_id | int(11) | NO | PRI | NULL | auto_increment |
| tutorial_title | varchar(100) | NO | | NULL | |
| tutorial_author | varchar(40) | NO | | NULL | |
| submission_date | date | YES | | NULL | |
+-----+-----+-----+-----+-----+-----+
4 rows in set (0.02 sec)

mysql> █
```

To see records in the tables;

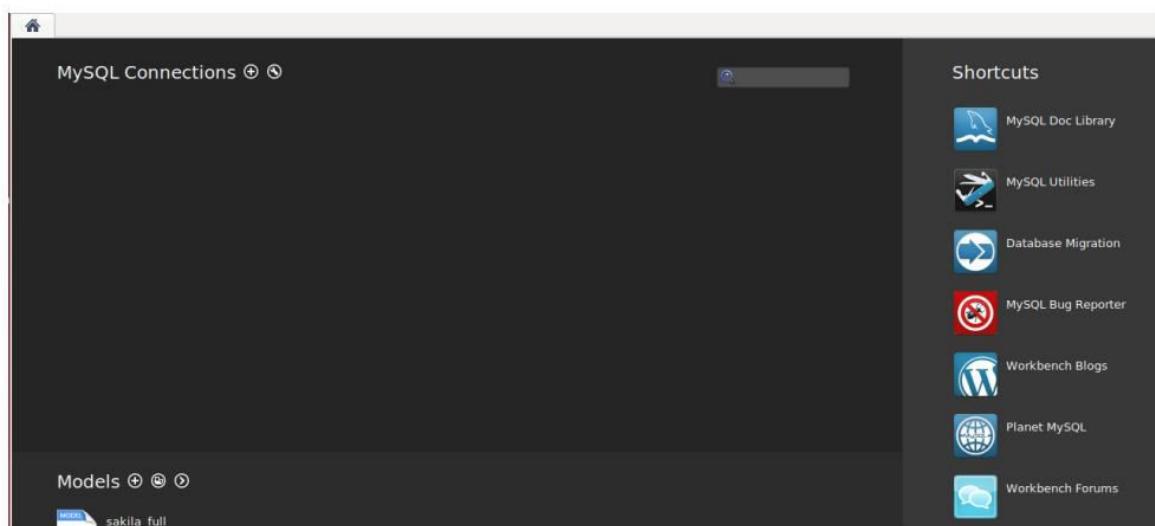
```
mysql> select * from tutorials_tbl;
+-----+-----+-----+-----+
| tutorial_id | tutorial_title | tutorial_author | submission_date |
+-----+-----+-----+-----+
| 1 | Learn PHP | John Poul | 2017-08-12 |
| 2 | Learn MySQL | Abdul S | 2017-08-12 |
| 3 | JAVA Tutorial | Sanjay | 2007-05-06 |
+-----+-----+-----+-----+
3 rows in set (0.02 sec)

mysql> █
```

2. To access RDS database through MYSQL WorkBenchclient application

Open MySQL WorkBench client Application, provide following details

On **MySQL Connection Tag**, click plus radio button



Provide the following values for

Connection Name: → testcon1

Connection Method: → Standard (TCP/IP)

Parameters

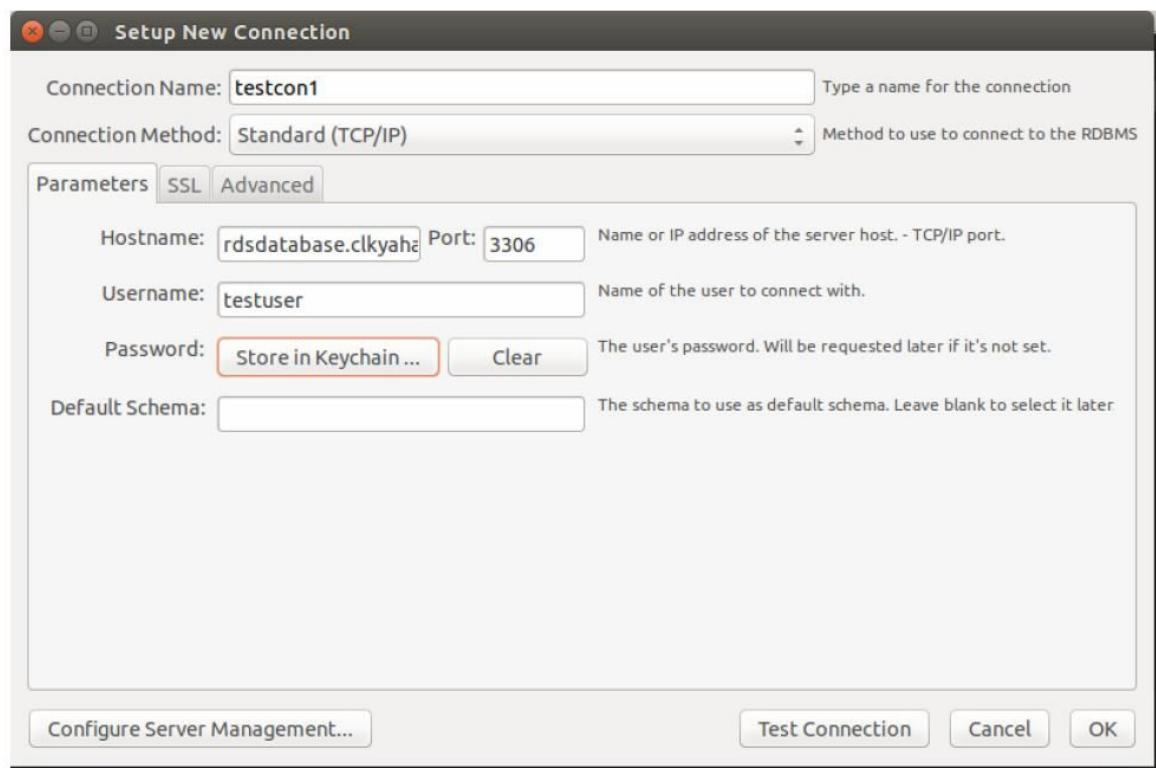
Hostname → copy RDS url

(<rdsdatabase.clkyahad3ggx.ap-south-1.rds.amazonaws.com>)

Port → 3306

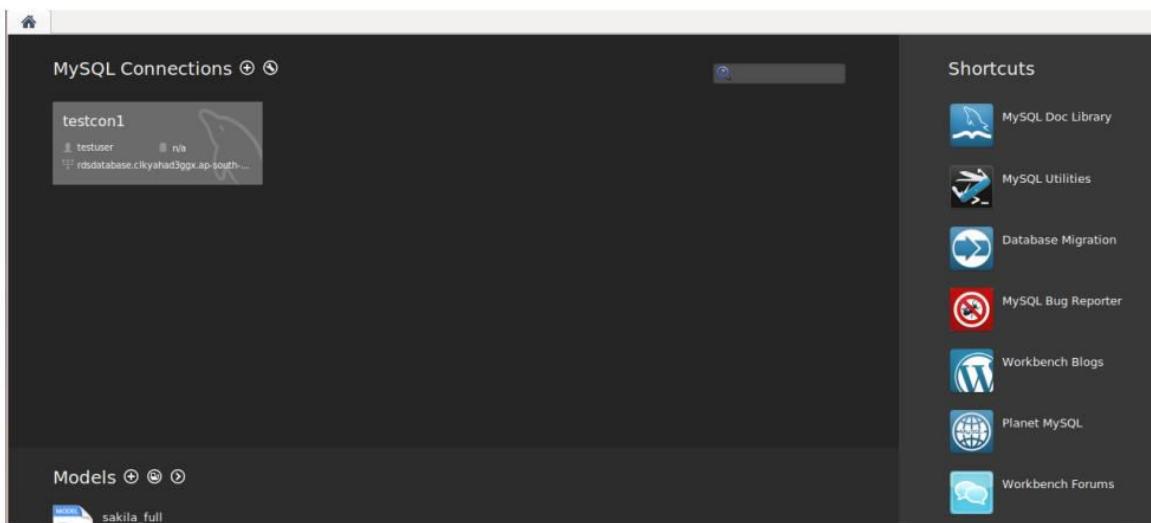
Username → testuser

Password → *****

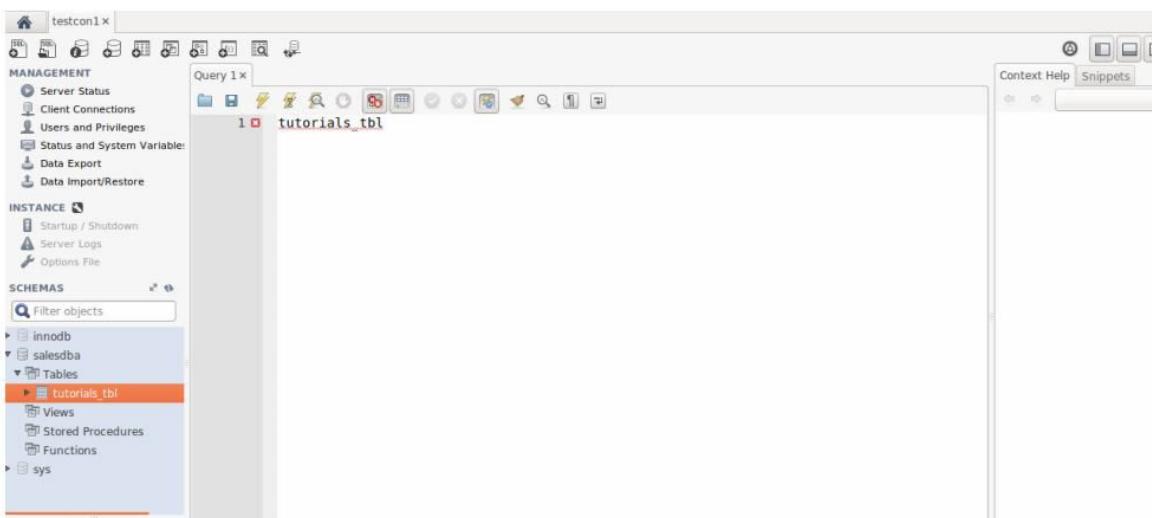


Verify

Connection is getting established.



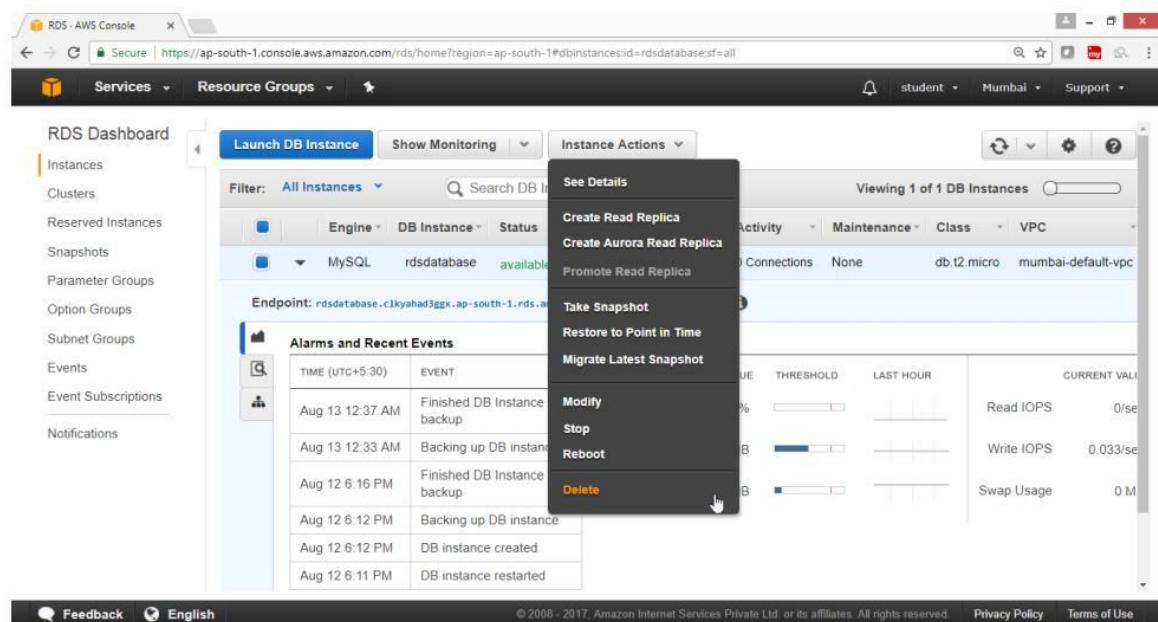
So we can see that tables are listed in MySQL clients.



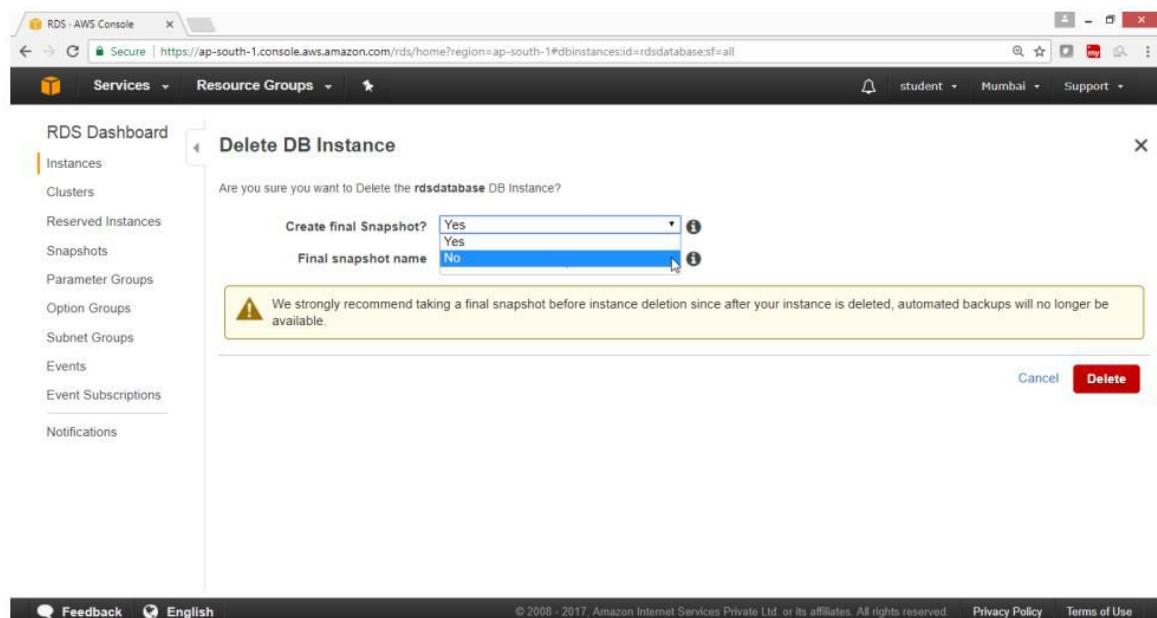
3. To Delete the RDS instance

3.1 Open RDS Dashboard , select instance

drop down Instance Action button, select Delete

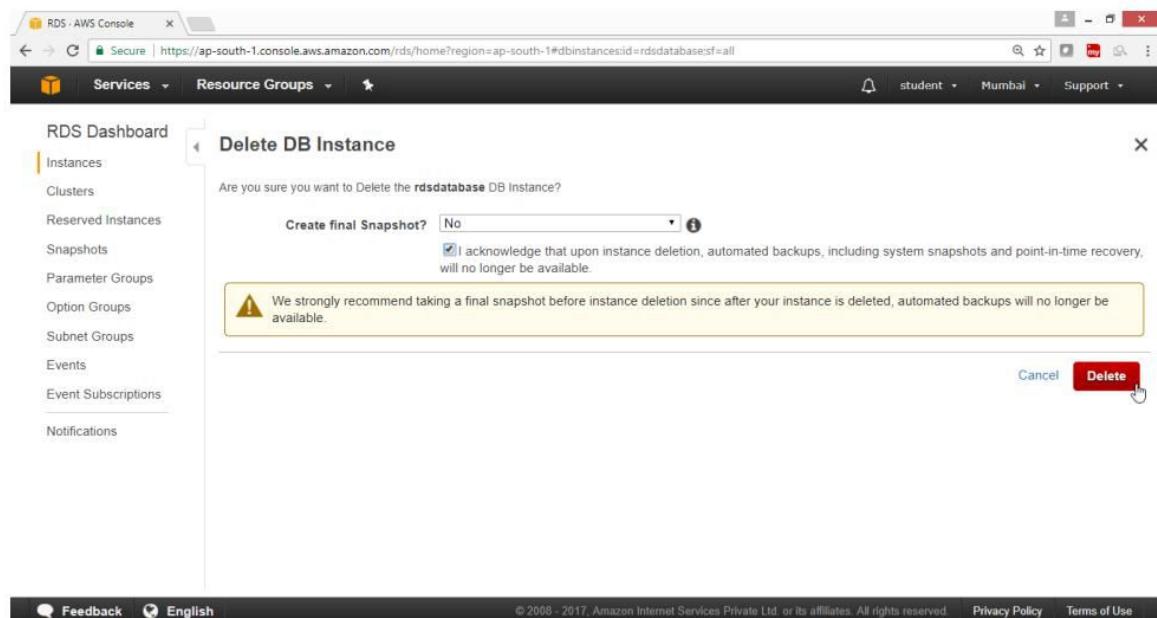


For Create final snapshot → No



Select acknowledge check box

Click on **Delete** button



Verify

In status column → deleting

The screenshot shows the AWS RDS console interface. On the left, there's a sidebar with options like Instances, Clusters, Reserved Instances, Snapshots, Parameter Groups, Option Groups, Subnet Groups, Events, Event Subscriptions, and Notifications. The main area has tabs for Launch DB Instance, Show Monitoring, and Instance Actions. A search bar at the top says "Search DB Instances...". Below it, a table lists one instance: Engine: MySQL, DB Instance: rdsdatabase, Status: deleting, CPU: 1.00%, Current Activity: None, Maintenance: None, Class: db.t2.micro, VPC: mumbai-default-vpc, Multi-AZ: No. A tooltip for the endpoint says "rdsdatabase.clykyahad3ggx.ap-south-1.rds.amazonaws.com:3306 (authorized)". Below the table, there are two sections: Alarms and Recent Events (listing events from Aug 13 and Aug 12) and Monitoring (showing CPU, Memory, Storage, Read IOPS, Write IOPS, and Swap Usage metrics). At the bottom, there are links for Feedback, English, Privacy Policy, and Terms of Use.

Delete Confirmed

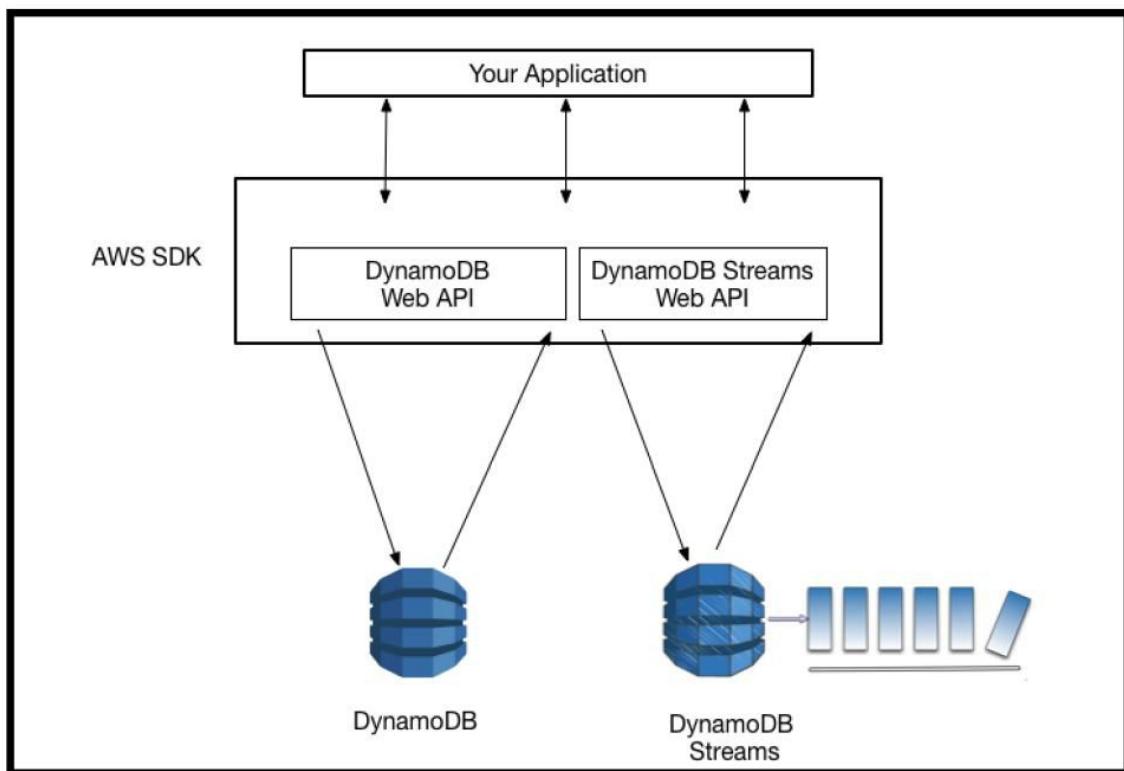
The screenshot shows the AWS RDS console after a deletion. The main area displays a message: "Relational Database Service (RDS) is a web service that makes it easy to set up, operate, and scale a relational database in the cloud. We currently offer MySQL, Oracle, PostgreSQL and Oracle engines, allowing you to use the code, application and tools you already use with your existing database with Amazon RDS. You can find pricing information for RDS here. Click the Launch DB Instance button to get started." Below this, a note says "Note: Your DB Instances will launch in the Asia Pacific (Mumbai) region." At the bottom, there are links for Feedback, English, Privacy Policy, and Terms of Use.

Lab 16: To Configure Amazon DynamoDB

OBJECTIVE

To configure a table create records in Amazon DynamoDB

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with AmazonDynamoDBFullAccess

TASK

Create DynamoDB table

Provide Provisioned Read/write capacity

Add the values to a table

Scan the table

Query table

Delete the table

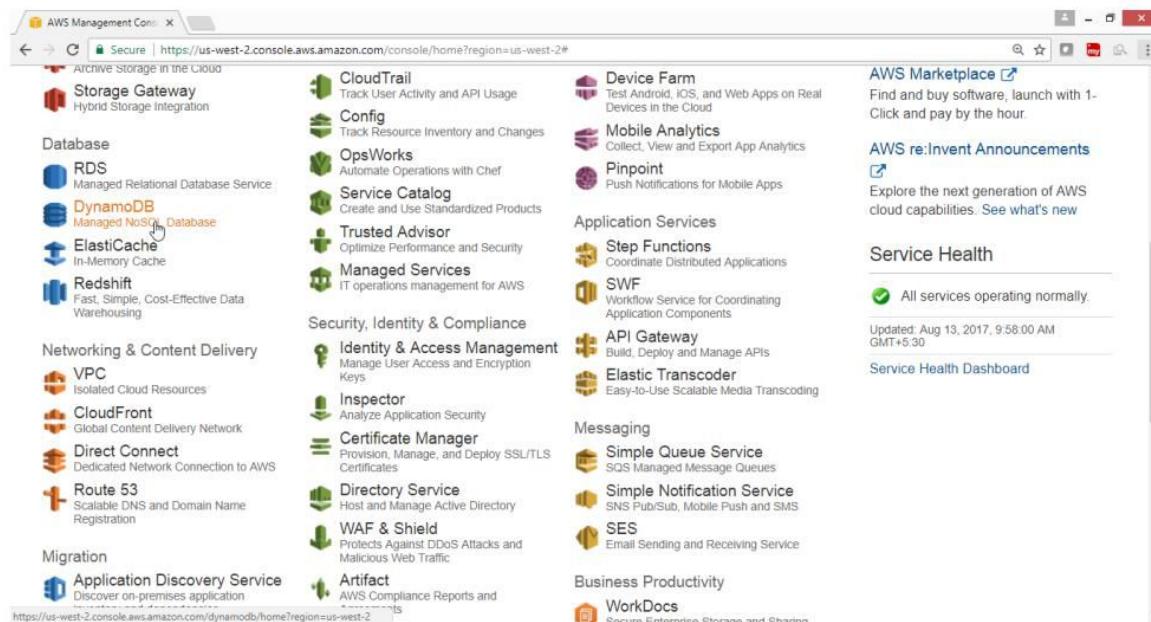
1) To Create an Amazon DynamoDB table

To Create Table

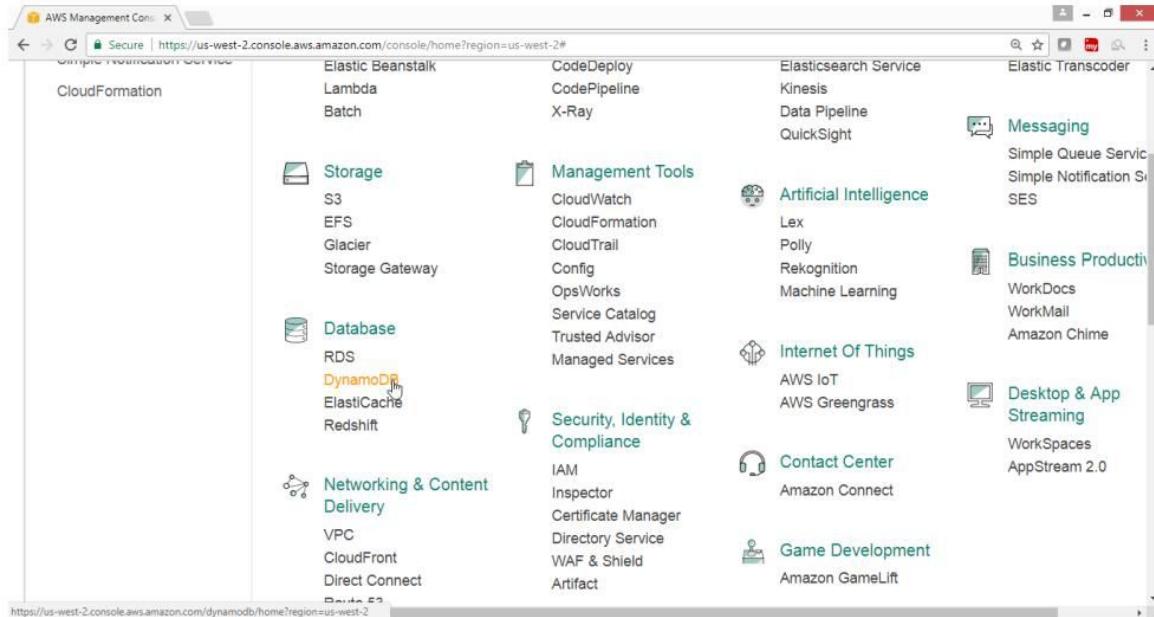
Open AWS console

Select services **Database**

Click on **DynamoDB**

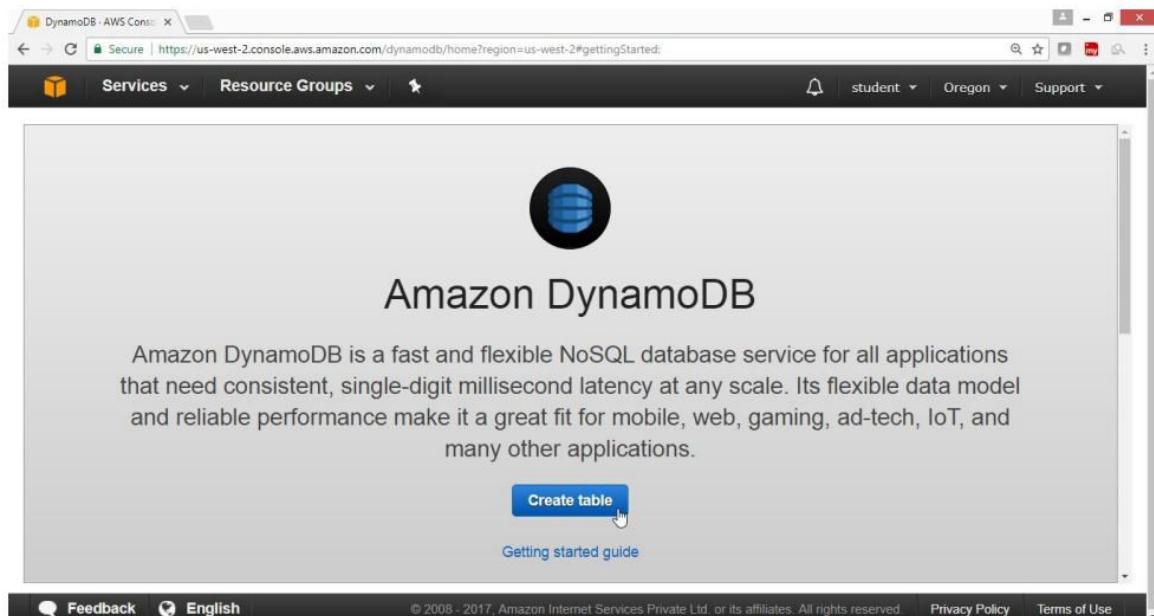


OR



From DynamoDB Dashboard

Click on **Create table** button



On “Create DynamoDB table” wizard

Provide following value

Table name* → Salestable

Partition Key → itemno, Select String

The screenshot shows the 'Create DynamoDB table' wizard in the AWS Management Console. The 'Table name*' field is set to 'Salestable'. The 'Primary key*' field is configured with 'Partition key' named 'itemno' of type 'String'. Below the primary key settings, there is an unchecked checkbox for 'Add sort key'. Under 'Table settings', the 'Use default settings' checkbox is checked, and the 'No secondary indexes.' option is selected. At the bottom of the page, there are links for 'Feedback', 'English', 'Privacy Policy', and 'Terms of Use'.

Under Table settings

Select “Use default settings” check box

click on **Create** button

The screenshot shows the 'Table settings' step of the 'Create Table' wizard. At the top, there is a checkbox labeled 'Use default settings' which is checked. Below it, three bullet points describe the default settings: 'No secondary indexes.', 'Provisioned capacity set to 5 reads and 5 writes.', and 'Basic alarms with 80% upper threshold using SNS topic "dynamodb"'.

A callout box highlights a message: 'You do not have the required role to enable Auto Scaling by default. Please refer to documentation.' Below this, a note states: 'Additional charges may apply if you exceed the AWS Free Tier levels for CloudWatch or Simple Notification Service. Advanced alarm settings are available in the CloudWatch management console.'

At the bottom right, there are 'Cancel' and 'Create' buttons, with 'Create' being highlighted.

Creating

The screenshot shows the 'Salestable' table details page. On the left, the navigation menu includes 'Create table' and 'Actions'. A search bar at the top of the main content area is set to 'Name' and contains the value 'Salestable'. The 'Overview' tab is selected, showing the message 'Table is being created'. Other tabs include 'Items', 'Metrics', 'Alarms', 'Capacity', 'Indexes', and 'More'. The 'Stream details' section shows 'Stream enabled: No', 'View type: -', and 'Latest stream ARN: -'. A 'Manage Stream' button is present. The 'Table details' section is partially visible at the bottom.

Verification

Salestable is created

The screenshot shows the AWS DynamoDB console interface. On the left, the navigation pane is visible with options like 'Dashboard', 'Tables' (which is selected), 'Reserved capacity', 'DAX', 'Clusters', 'Subnet groups', 'Parameter groups', and 'Events'. A 'Create table' button is also present. The main right panel displays the 'Salestable' table details. At the top, there are tabs for 'Overview', 'Items' (which is selected), 'Metrics', 'Alarms', 'Capacity', 'Indexes', and 'More'. Below the tabs, under 'Recent alerts', it says 'No CloudWatch alarms have been triggered for this table.' Under 'Stream details', it shows 'Stream enabled: No', 'View type: -', and 'Latest stream ARN: -'. A 'Manage Stream' button is available. The 'Table details' section shows a table with one row: 'Table name: Salestable'. At the bottom of the page, there are links for 'Feedback', 'English', and copyright information: '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' followed by 'Privacy Policy' and 'Terms of Use'.

Select Capacity

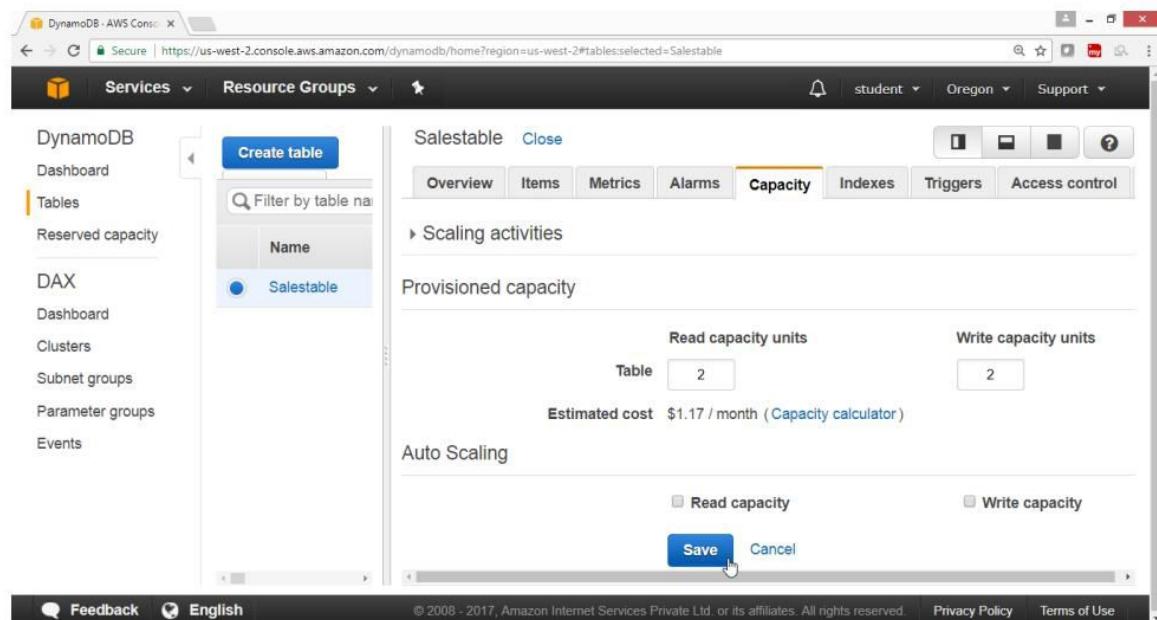
Under “**Provisioned capacity**”

Provide the following values

Read Capacity → 2

Write Capacity units → 2

Click on **Save** button



Select item

Click on Create item

The screenshot shows the AWS DynamoDB console interface. On the left, there's a sidebar with 'DynamoDB' selected under 'Tables'. A modal window titled 'Salestable' is open, showing the 'Items' tab. At the top of this modal, there's a 'Create Item' button. Below it, a search bar says 'Scan: [Table] Salestable: itemno ^'. A tooltip explains that items consist of attributes with names, data types, and values. The bottom of the modal has a note about primary keys and a 'More info' link.

To add, append, insert values in the table

Open DynamoDB Dashboard, select Tables

Select the tables from tables list

check status, by clicking on

Overview
Items
Metrics
Alarms
Capacity
Indexes
Triggers
Access control

Select Items, add tables field

Click on “Create Items”

On “Create Items” page

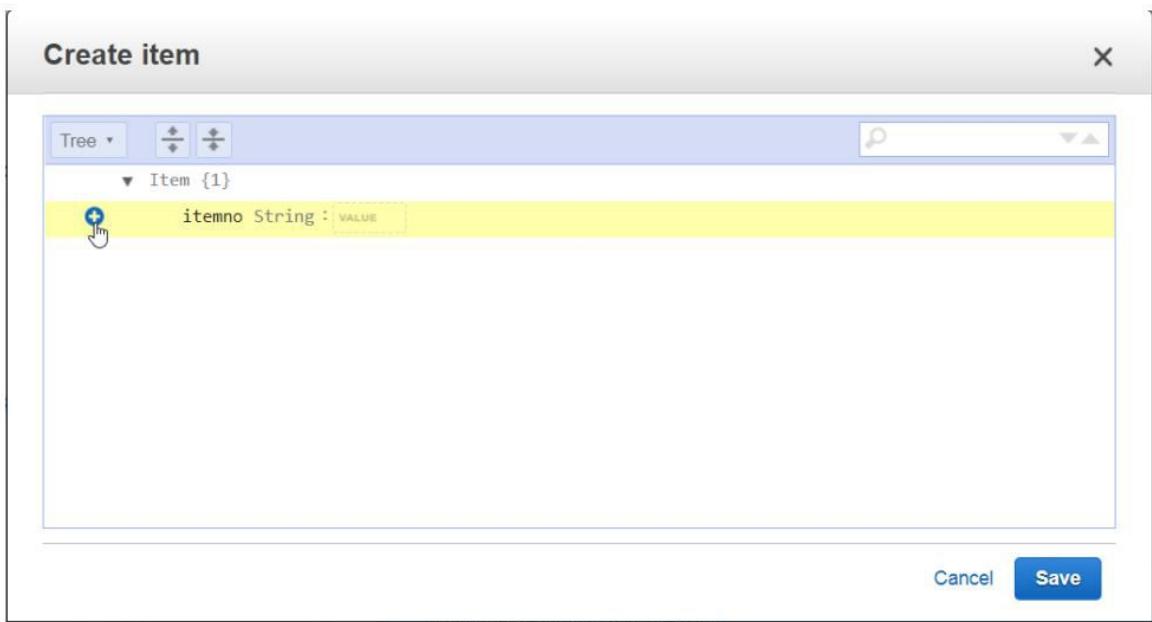
Click on Tree

Click on plus radio button

Provide

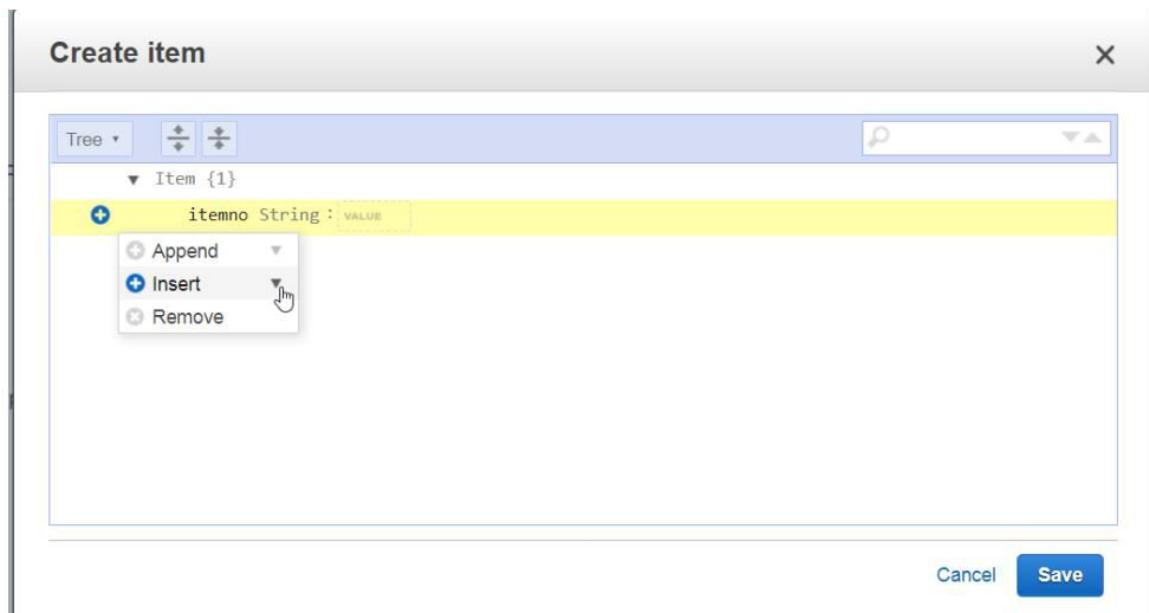
itemno String 1

Click on plus radio button

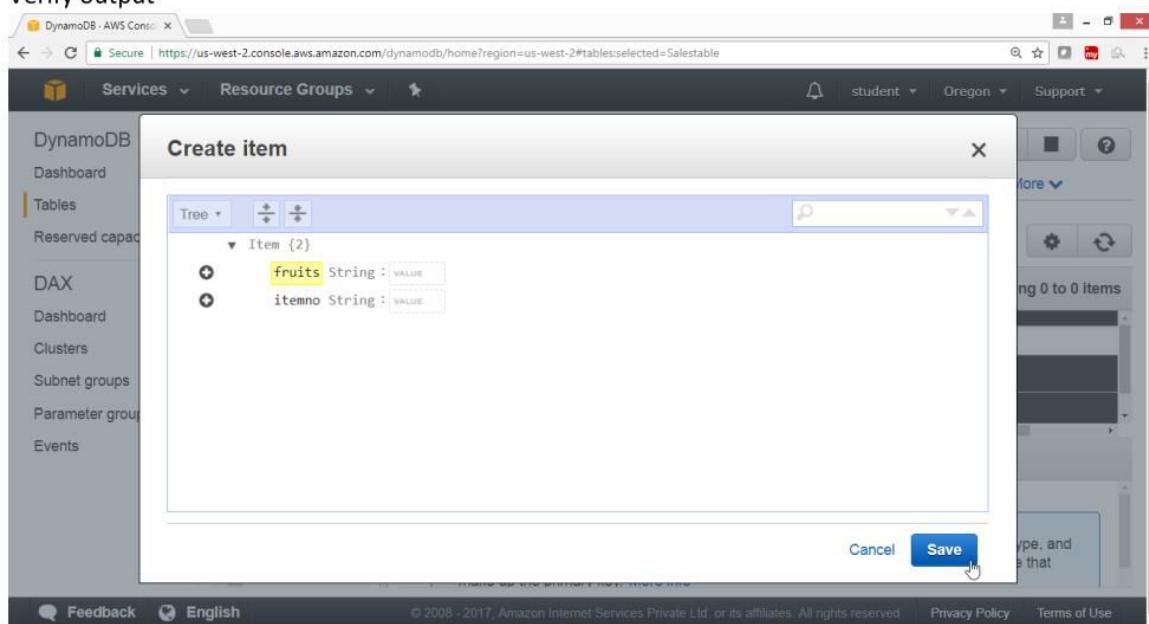


Select insert, select string

ItemName String fruits



Verify output

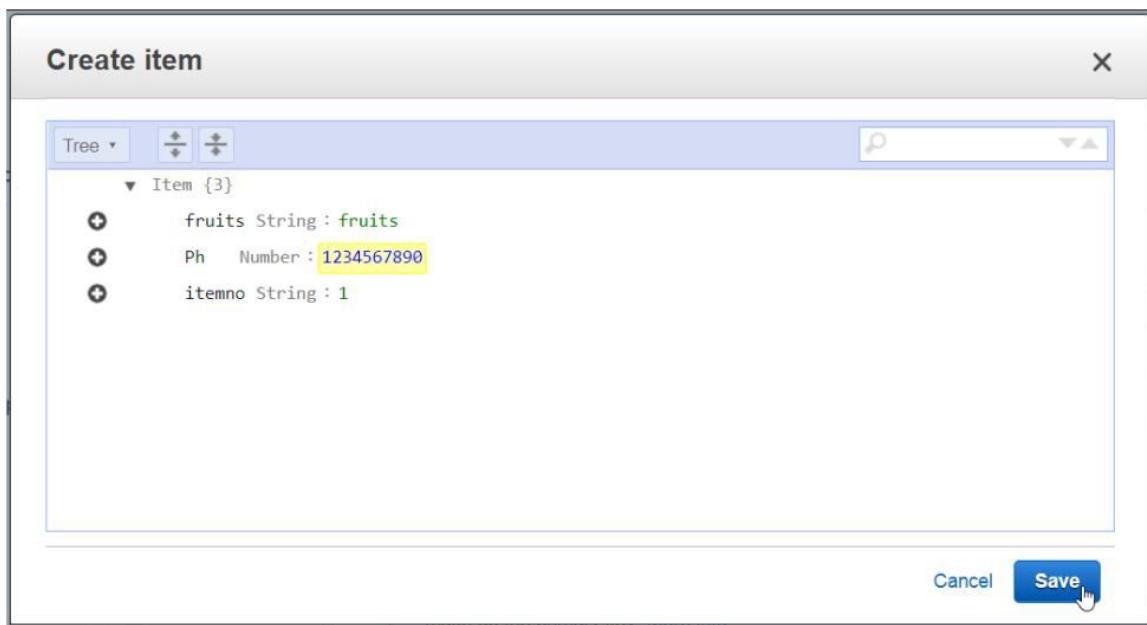


Click on plus radio button

select insert, select number

Ph → 123456789

click on **Save**



To View all entered data

select Scan , click start search

The screenshot shows the AWS DynamoDB console interface. On the left, the navigation pane is visible with options like DynamoDB, Dashboard, Tables, Reserved capacity, DAX, Clusters, Subnet groups, Parameter groups, and Events. A 'Create table' button is also present. The main area is titled 'Salestable' and shows the 'Items' tab selected. A search bar at the top says 'Scan: [Table] Salestable: itemno'. Below it, there's a 'Start search' button. The results table shows one item: itemno 1, Ph 1234567890, and fruits.

To add values in the created fields

Select the Table row, click **Action** button

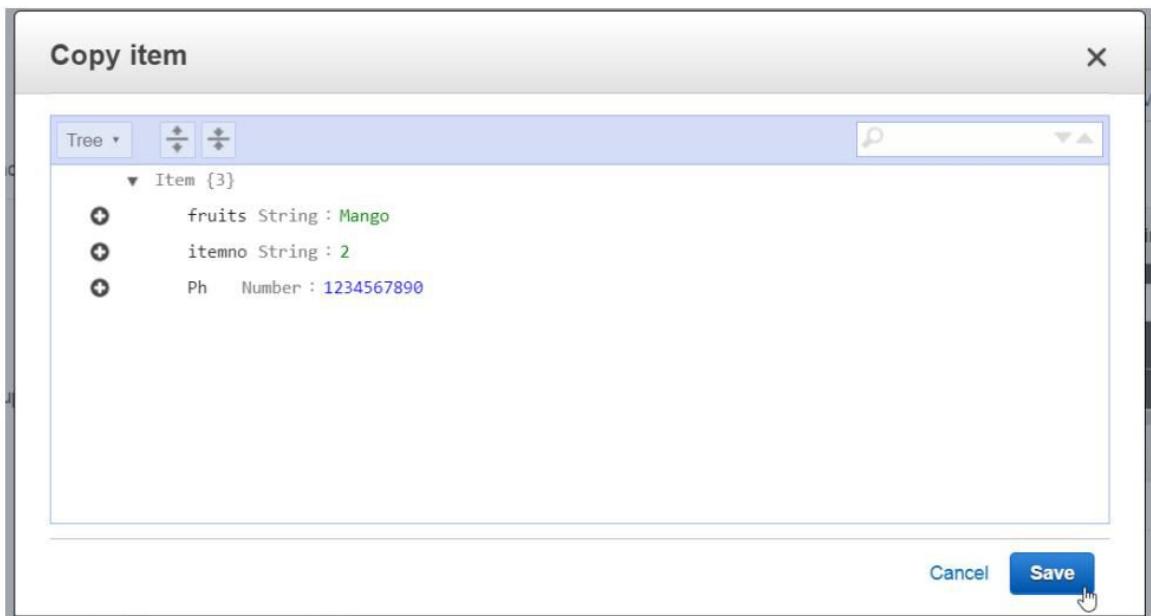
select **Duplicate**

This screenshot is similar to the previous one, showing the AWS DynamoDB console with the 'Salestable' table. The 'Actions' dropdown menu is open over the first item (itemno 1), and the 'Duplicate' option is highlighted with a cursor. The rest of the interface and data remain the same.

Now modify the values of the field

New row will be created

Click on save



Verify

itemno	Ph	fruits
2	1234567890	Mango
1	1234567890	fruits

To Delete the table permanently for DymoDB

From the AWS console

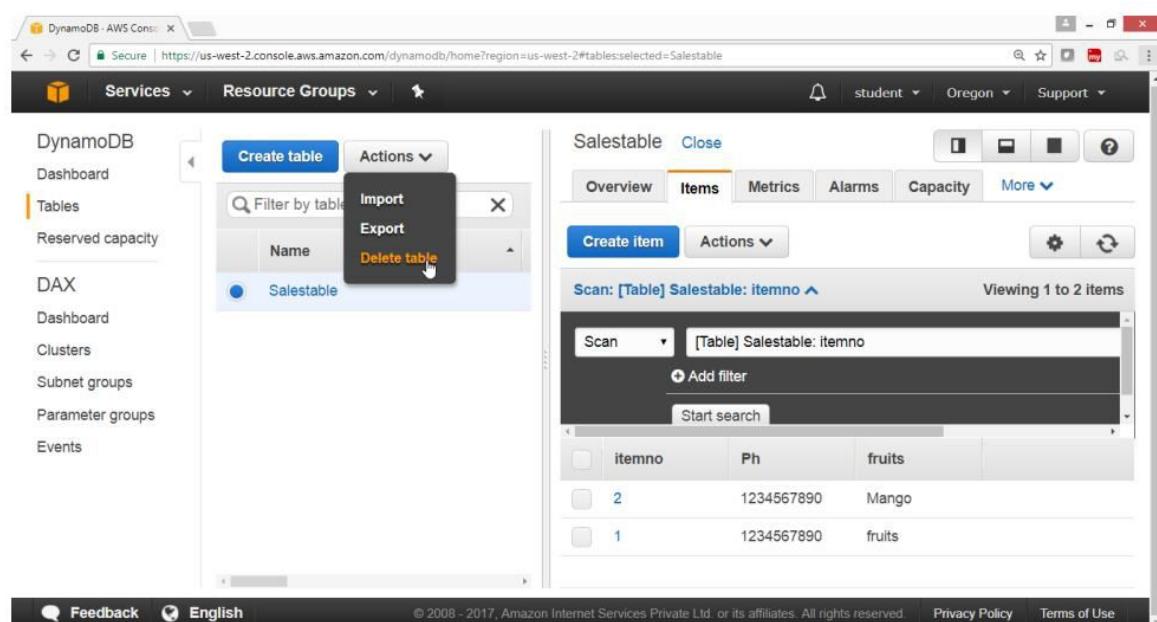
Select services **Database**

Choose **DynamoDB**

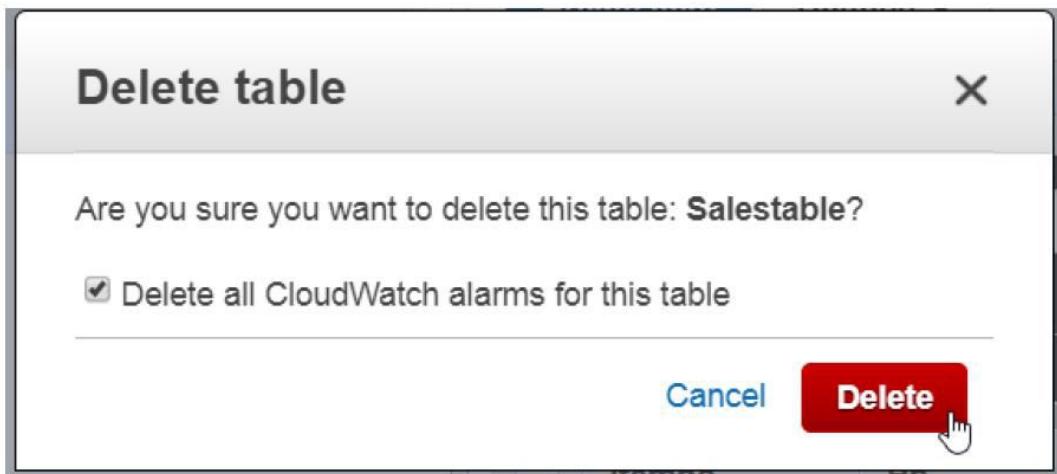
Under **Tables**, select the table for the list

click on Action button

Select “**Delete Table**”



Click on **Delete** button



Verify Table is deleted.

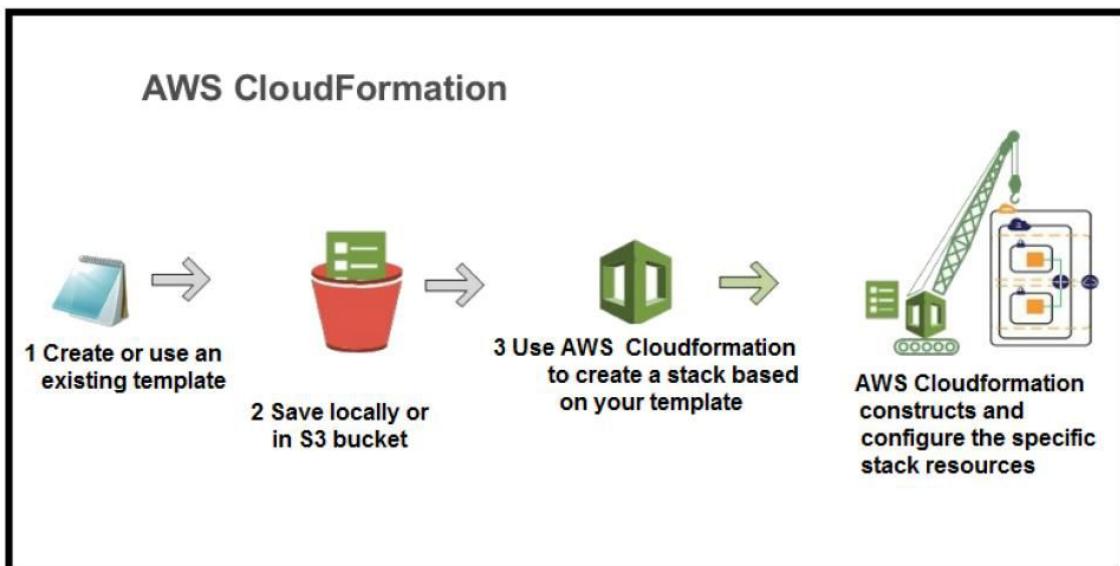
A screenshot of the AWS DynamoDB console. The left sidebar shows "Tables" selected. The main area has a search bar and a table header with "Name". A tooltip box is overlaid on the left side of the main area, containing information about DynamoDB and a "More info" link. The status bar at the bottom includes links for "Feedback", "English", "Privacy Policy", and "Terms of Use".

Lab 17: To Configure Amazon CloudFormation

OBJECTIVE

To configure AWS CloudFormation

Topology



PRE-REQUISITES

User should have AWS account, or IAM user with CloudFormationfullaccess

TASK

Creating EC2 instance using CloudFormation

Deleting all resources from CloudFormation

Practical Steps

1) To Launch Amazon EC2 instance in a security group using CloudFormation

Open AWS Console

Click on Services

In Management Tools services

Click on CloudFormation service

The screenshot shows the AWS Management Console homepage. The navigation bar at the top includes 'Services' and 'Resource Groups'. On the left, there's a sidebar with categories like Compute, Storage, and Management Tools. Under 'Management Tools', the 'CloudFormation' service is listed with a small icon and the text 'Create and Manage Resources with Templates'. To the right of the main content area, there's a 'Resource Groups' section with a 'Create a Group' button and a 'Tag Editor' button. Below that is an 'Additional Resources' section with links to 'Getting Started', 'AWS Console Mobile App', and 'AWS Marketplace'.

2) To create a new stack

On “Create Stack”, page

Click on “Create New Stack” button

The screenshot shows the AWS CloudFormation Manager interface. The top navigation bar includes 'Services', 'Resource Groups', 'CloudFormation', and 'Stacks'. Below the navigation is a search bar with 'Filter: Active' and 'By Stack Name'. A large central box titled 'Create a stack' contains text about CloudFormation and a 'Create new stack' button, which is highlighted with a mouse cursor. At the bottom of the page, there are links for 'Feedback', 'English', 'Privacy Policy', and 'Terms of Use'.

Under “Choose a template”

Select “Select a sample template”

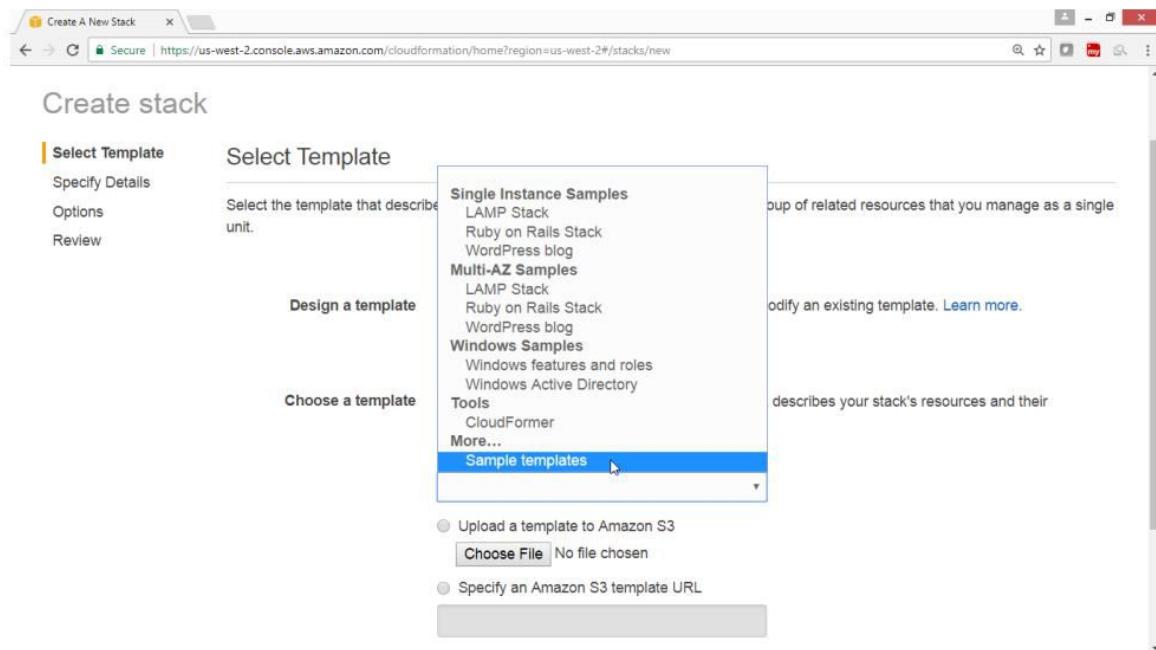
The screenshot shows the 'Create Stack' wizard. The left sidebar has tabs for 'Select Template', 'Specify Details', 'Options', and 'Review'. The main area is titled 'Select Template' with the sub-instruction 'Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.' Below this is a 'Design a template' section with a 'Design template' button. Further down, there's a 'Choose a template' section with the sub-instruction 'A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties.' It contains two options: a selected radio button for 'Select a sample template' and an unselected radio button for 'Upload a template to Amazon S3' with a 'Choose File' button.

On **Create stack** page

Select the “**Sample template**”

In the Drop Down box

Choose “**Sample templates**” option



On “AWS CloudFormation Templates” page

Click on “sample templates”

The screenshot shows the AWS CloudFormation Templates page. At the top, there's a navigation bar with links for 'Create A New Stack', 'AWS CloudFormation Templates', 'Products', 'Solutions', 'More', 'English', 'My Account', and 'Sign In to the Console'. Below the navigation bar, the title 'AWS CloudFormation Templates' is displayed in a large blue header. A brief introduction follows: 'AWS CloudFormation simplifies provisioning and management on AWS. You can create templates for the service or application architectures you want and have AWS CloudFormation use those templates for quick and reliable provisioning of the services or applications (called "stacks"). You can also easily update or replicate the stacks as needed.' A note below states: 'This collection of sample templates will help you get started with AWS CloudFormation and quickly build your own templates.' On the left, there are sections for 'Templates & Snippets by AWS Service' and 'Application Frameworks', each with links to sample templates. On the right, there are sections for 'Reference Implementations' (with a link to AWS Quick Start) and 'Sample Solutions' (with a link to AWS Test Drive). A footer at the bottom provides a URL: 'docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/sample-templates-services-us-west-2.html'.

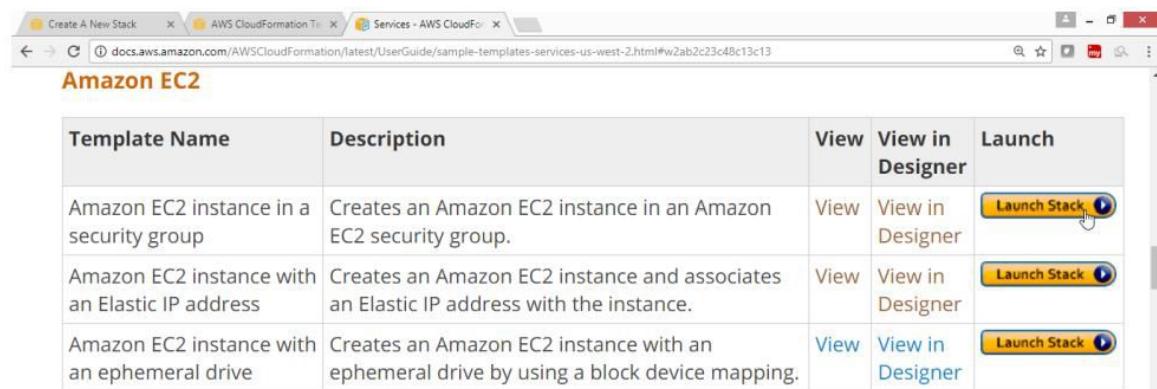
Under Topics

Select Amazon EC2

The screenshot shows the AWS CloudFormation User Guide page. The left sidebar contains a navigation menu with sections like 'Documentation - This Guide', 'Search', 'What is AWS CloudFormation?', 'Setting Up', 'Getting Started', 'Best Practices', 'Continuous Delivery', 'Working with Stacks', 'Working with Templates', and 'Working with AWS CloudFormation StackSets'. The main content area has a heading 'The service sample templates show you how you can use AWS CloudFormation with other AWS services.' Below this, there's a 'Topics' section with a list of items, where 'Amazon EC2' is highlighted in orange. The footer includes a 'Terms of Use' link, a feedback survey asking 'Did this page help you? Yes / No / Feedback', and a URL: 'docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/sample-templates-services-us-west-2.html#w2ab2c23c48c13c13'.

Select “Amazon EC2 instance in a security group”,

Click on “Launch stack”



Template Name	Description	View	View in Designer	Launch
Amazon EC2 instance in a security group	Creates an Amazon EC2 instance in an Amazon EC2 security group.	View	View in Designer	Launch Stack 
Amazon EC2 instance with an Elastic IP address	Creates an Amazon EC2 instance and associates an Elastic IP address with the instance.	View	View in Designer	Launch Stack 
Amazon EC2 instance with an ephemeral drive	Creates an Amazon EC2 instance with an ephemeral drive by using a block device mapping.	View	View in Designer	Launch Stack 

Amazon ElastiCache

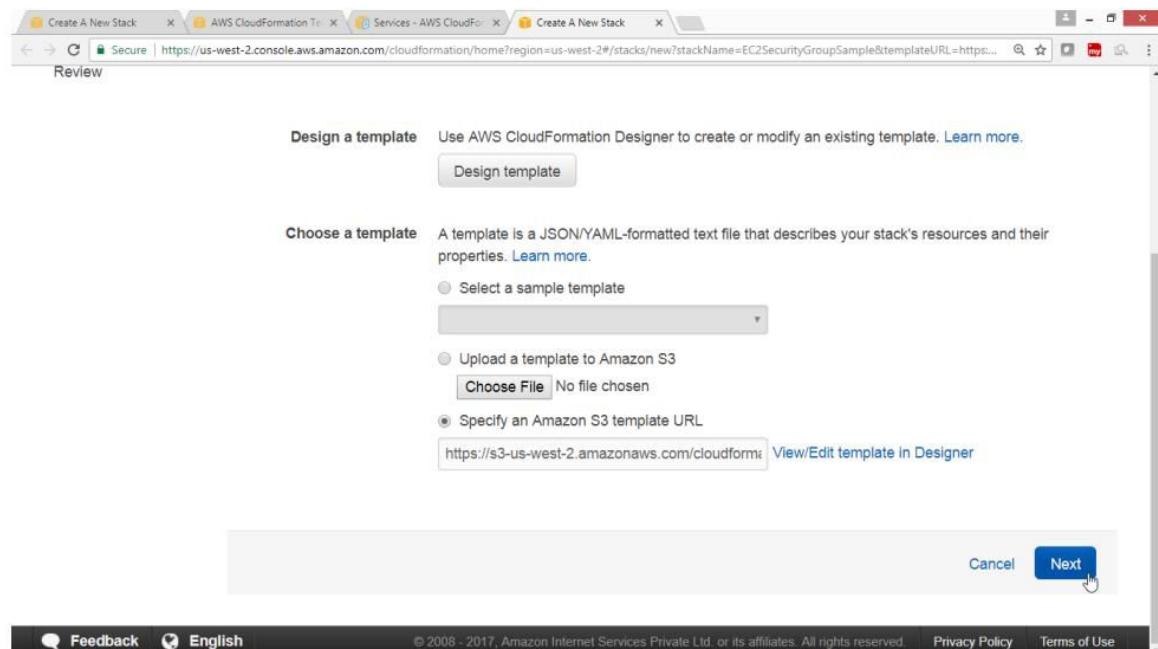


Template Name	Description	View	View in Designer	Launch
ElastiCache	Creates an ElastiCache cache cluster with the Memcached	View	View in Designer	Launch Stack 

In option “Specify an Amazon S3 template URL”

Verify template is loaded in S3

Click on **Next** button



On Specific Details page

Key Name → “key*.pem”

Click on Next button

The screenshot shows the 'Specify Details' step of a CloudFormation stack creation. On the left, a sidebar lists 'Select Template', 'Specify Details' (which is selected and highlighted in orange), 'Options', and 'Review'. The main area is titled 'Specify Details' with the sub-instruction: 'Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more](#)'. A 'Stack name' input field contains 'EC2SecurityGroupSample'. Below it is a 'Parameters' section with three fields: 'InstanceType' set to 't2.small' (with a tooltip 'WebServer EC2 instance type'), 'KeyName' set to '25july2017masorg' (with a tooltip 'Name of an existing EC2 KeyPair to enable SSH access to the instance'), and 'SSHLocation' set to '0.0.0.0/0' (with a tooltip 'The IP address range that can be used to SSH to the EC2 instances'). At the bottom right are 'Cancel', 'Previous', and a large blue 'Next' button.

Under Options Tag, provide values for

Key → Nameweb

Value → Web

Drag Down

Create stack

Select Template

Specify Details

Options

Review

Tags

You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. [Learn more.](#)

Key (127 characters maximum)	Value (255 characters maximum)
1 Nameweb	web

Permissions

You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. [Learn more.](#)

IAM Role Choose a role (optional)

Enter role arn

Click on Next

Key (127 characters maximum) Value (255 characters maximum)

1	Nameweb	web
---	---------	-----

Permissions

You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. [Learn more](#).

IAM Role Choose a role (optional)
Enter role arn

Advanced

You can set additional options for your stack, like notification options and a stack policy. [Learn more](#).

Cancel Previous **Next**

Review , check the summary

Create stack

Review

Template

Template URL <https://s3-us-west-2.amazonaws.com/cloudformation-templates-us-west-2/EC2InstanceWithSecurityGroupSample.template>

Description AWS CloudFormation Sample Template EC2InstanceWithSecurityGroupSample: Create an Amazon EC2 instance running the Amazon Linux AMI. The AMI is chosen based on the region in which the stack is run. This example creates an EC2 security group for the instance to give you SSH access.
WARNING This template creates an Amazon EC2 instance. You will be billed for the AWS resources used if you create a stack from this template.

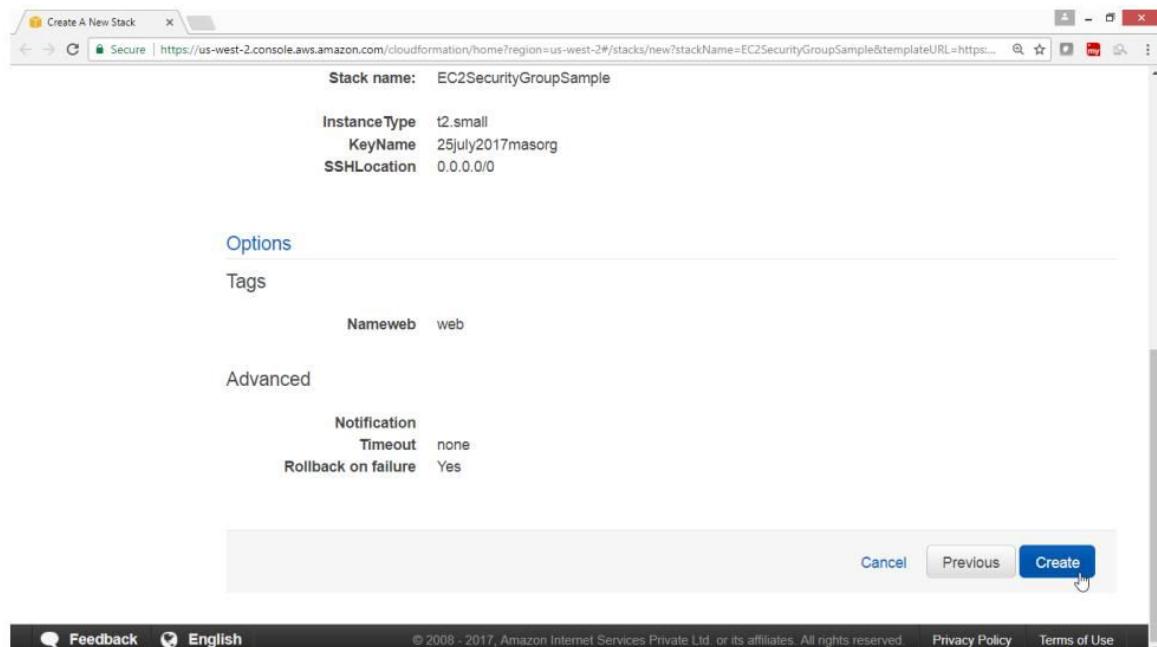
Estimate cost Cost

Details

Stack name: EC2SecurityGroupSample

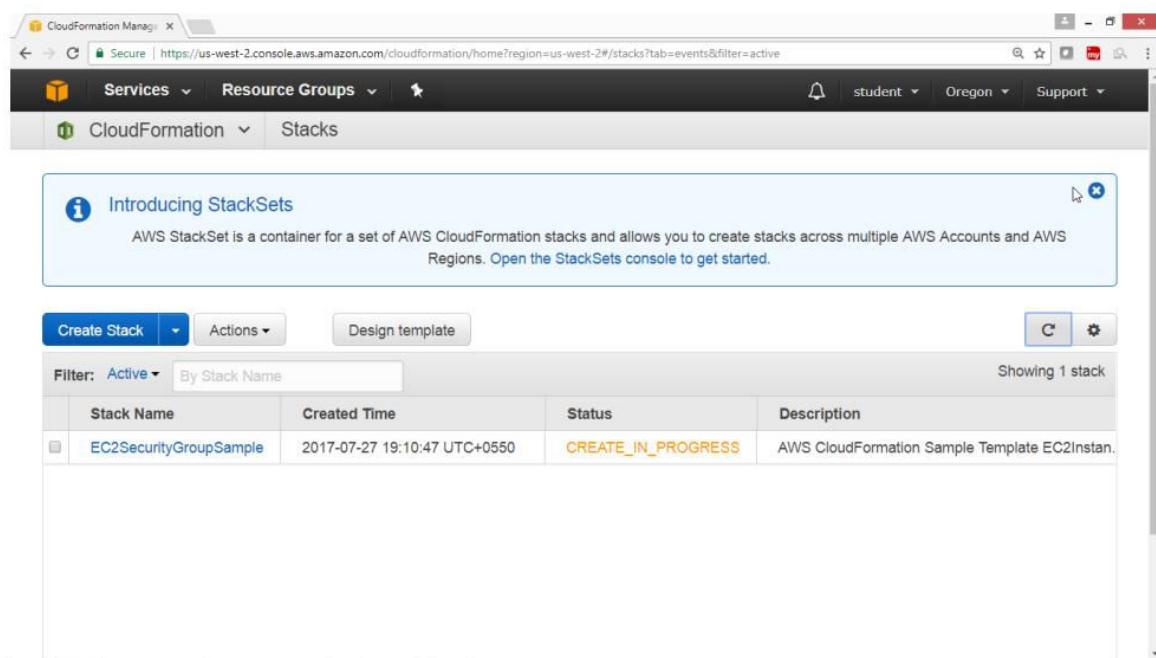
InstanceType: t2.small
KeyName: 25July2017masorg
SSHLocation: 0.0.0.0/0

Click **Create** button



Check the status

Cloudformation is in progress state.



Verify

Status is Create_Complete

The screenshot shows the AWS CloudFormation Manager interface. At the top, there is a banner stating: "AWS StackSet is a container for a set of AWS CloudFormation stacks and allows you to create stacks across multiple AWS Accounts and AWS Regions. Open the StackSets console to get started." Below the banner, there are navigation buttons for "Create Stack", "Actions", and "Design template". A filter bar shows "Filter: Active" and "By Stack Name". A table displays one stack entry:

	Stack Name	Created Time	Status	Description
<input type="checkbox"/>	EC2SecurityGroupSample	2017-07-27 19:10:47 UTC+0550	CREATE_COMPLETE	AWS CloudFormation Sample Template EC2Instan...

At the bottom of the page, there are links for "Feedback", "English", "Privacy Policy", and "Terms of Use".

Go to EC2 service

Check the instances

An instance with the Name “web” is launched

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block Store. The Instances section is currently selected. The main area displays a table of instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm S
web	i-0668c160a0f3daf41	t2.small	us-west-2c	running	2/2 checks ...	None
web1	i-081a441f51fc90525	t2.micro	us-west-2a	stopped	OK	

Below the table, it says "Instance: i-0668c160a0f3daf41 (web) Public DNS: ec2-34-212-227-98.us-west-2.compute.amazonaws.com". There are tabs for Description, Status Checks, Monitoring, and Tags. Under the Description tab, it shows Instance ID: i-0668c160a0f3daf41, Public DNS (IPv4): ec2-34-212-227-98.us-west-2.compute.amazonaws.com, Instance state: running, and IPv4 Public IP: 34.212.227.98.

3) To remove the Instances created by CloudFormation

From AWS console

Select services **Management tools**

Select **CloudFormation**

Select the Stack Name check box

The screenshot shows the AWS CloudFormation Management Console. At the top, there's a navigation bar with 'Services', 'Resource Groups', and 'CloudFormation' selected. Below it, a sub-navigation bar has 'CloudFormation' selected and 'Stacks' highlighted. A modal window titled 'Introducing StackSets' is open, explaining what StackSets are and how they allow creating stacks across multiple AWS Accounts and Regions. It includes a link to 'Open the StackSets console to get started.' The main content area shows a table of stacks. The table has columns: Stack Name, Created Time, Status, and Description. There is one row visible, representing the stack 'EC2SecurityGroupSample'. The 'Status' column shows 'CREATE_COMPLETE'. The 'Description' column indicates it's a 'AWS CloudFormation Sample Template EC2Instan...'. Below the table, there are tabs for Overview, Outputs, Resources, Events, Template, Parameters, Tags, Stack Policy, and Change Sets. The 'Overview' tab is selected. At the bottom of the page, it says 'Stack name: EC2SecurityGroupSample'.

Stack Name	Created Time	Status	Description
EC2SecurityGroupSample	2017-07-27 19:10:47 UTC+0550	CREATE_COMPLETE	AWS CloudFormation Sample Template EC2Instan...

Click on **Actions** button

Select “Delete stack”

The screenshot shows the AWS CloudFormation Manager interface. At the top, there's a banner about StackSets. Below it, the main area has tabs like 'Create Stack', 'Actions', and 'Design template'. A dropdown menu under 'Actions' is open, showing options: 'Create Change Set For Current Stack', 'Update Stack', 'Delete Stack' (which is highlighted with a mouse cursor), and 'View/Edit template in Designer'. The main table below shows one stack named 'EC2SecurityGroupSample' with status 'CREATE_COMPLETE'. At the bottom, there's a summary of the stack details.

Click on “Yes, Delete”

This screenshot shows a confirmation dialog box titled 'Delete Stack'. It asks if you're sure you want to delete the stack 'EC2SecurityGroupSample'. It also states that deleting a stack deletes all stack resources. At the bottom of the dialog are two buttons: 'Cancel' and a red 'Yes, Delete' button, which is being clicked by a mouse cursor. The background shows the same CloudFormation interface as the previous screenshot, with the stack details visible.

Verify

Deletion is in progress

The screenshot shows the AWS CloudFormation Management Console. The top navigation bar includes 'Services', 'Resource Groups', 'CloudFormation', and 'Stacks'. A modal window titled 'Introducing StackSets' provides information about StackSets. Below it, the main interface displays a table of stacks. The table has columns: Stack Name, Created Time, Status, and Description. One row is selected, showing 'EC2SecurityGroupSample' as the Stack Name, '2017-07-27 19:10:47 UTC+0550' as the Created Time, 'DELETE_IN_PROGRESS' as the Status, and 'AWS CloudFormation Sample Template EC2Instan...' as the Description. The status 'DELETE_IN_PROGRESS' is highlighted in orange. The table also shows 'Showing 1 stack'.

Verification

After deletion again starting screen of CloudFormation is displayed

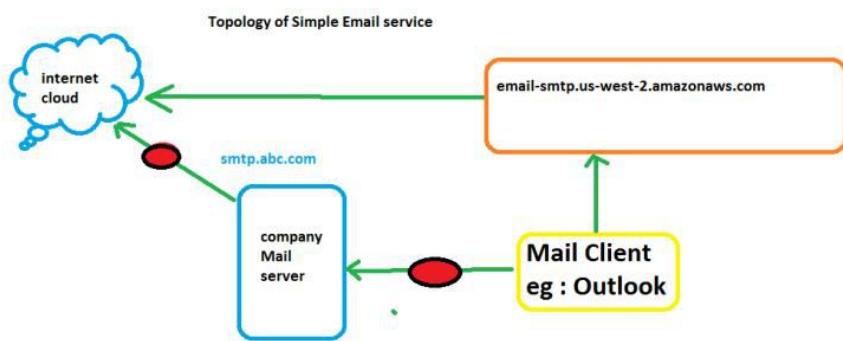
The screenshot shows the AWS CloudFormation Management Console. The top navigation bar includes 'Services', 'Resource Groups', 'CloudFormation', and 'Stacks'. The main area displays a 'Create a stack' wizard. It contains a descriptive text block about AWS CloudFormation and a button labeled 'Create new stack'.

Lab 18: To Configure Amazon Simple E-Mail Service (SES)

Objective

TO configure and use Simple Email Service (SES)

Topology



PRE-REQUISITES

User should have AWS account, or IAM user with AmazonSESFullAccess

To Configure SES with following task:

- Provide valid Mail Account
- Verify Email Address
- Configure SMTP settings
- Download the credentials, keep at safe place
- Configure Mail client for eg Outlook

To use Amazon Simple E-Mail Service SES

1. Create SES account

From the AWS console select service “**Messaging**”, choose SES service

The screenshot shows the AWS Management Console Services page. The navigation bar at the top includes tabs for SES Manager, Inbox - studio, ses aws diag, Sending Email, aws ses ppt, (SDD412) A..., aws-amazon, Getting Start..., SMTP Setup, and others. The main content area has a search bar and filters for Group and A-Z. The services are categorized into groups: Compute, Developer Tools, Analytics, Application Services, Storage, Management Tools, Artificial Intelligence, Business Productivity, and Messaging. The **Simple Email Service** is highlighted in orange and selected, indicated by a mouse cursor icon.

From SES Home, panel

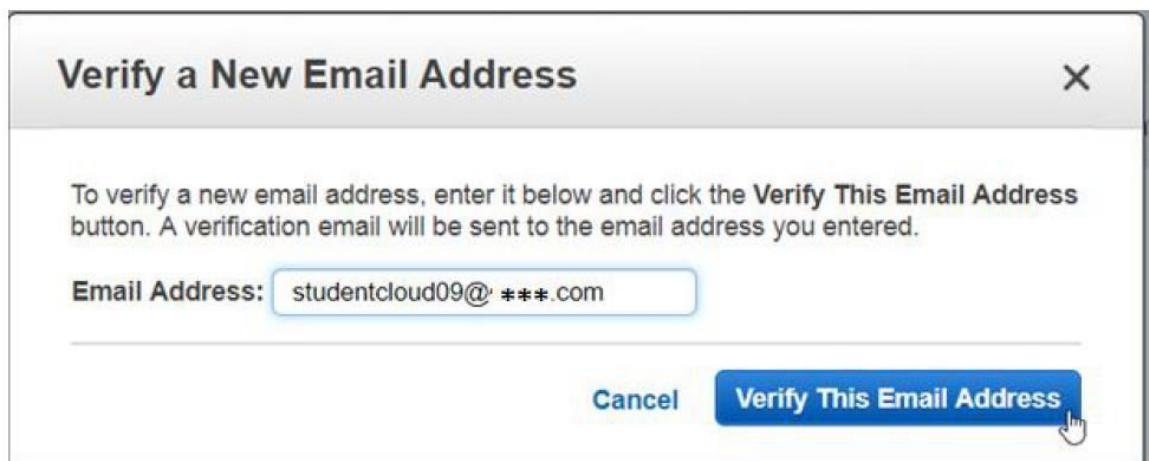
select "Email Addresses"

The screenshot shows the AWS Simple Email Service (SES) home page. The left sidebar has a navigation menu with options like SES Home, Identity Management, Domains, Email Addresses (which is highlighted in orange), Email Sending, Sending Statistics, Reputation Dashboard, Dedicated IPs, Configuration Sets, SMTP Settings, Suppression List Removal, and Cross-Account Notifications. The main content area features the Amazon logo and the text "Amazon Simple Email Service". It also includes three icons: a user profile with a plus sign, a computer monitor with a chart and envelope, and two interlocking gears. Below these icons is the text "Amazon Simple Email Service enables you to send and receive email using a reliable and scalable email platform." and a link to "Read the documentation". At the bottom of the page, there are links for Feedback, English (US), Privacy Policy, and Terms of Use.

Select "Verify a New Email Address" button

The screenshot shows the "Email Addresses" page under the SES service. The left sidebar is identical to the previous screenshot. The main content area has a header with "Verify a New Email Address" in blue, followed by "Send a Test Email", "Remove", and "View Details" buttons. Below this is a search bar with "Search email addresses" and a dropdown for "All Identities". A message states "You have not verified any email addresses. To verify a email address, click the Verify a New Email Address button above." At the bottom of the page are links for Feedback, English (US), Privacy Policy, and Terms of Use.

In “Verify a New Email Address”, wizard provide email id
click “Verify This Email Address” button



2. Now login to your companies mail account, to confirm your email address

Click on “**confirm the address using this URL. This link expires 24 hours after your original verification request.**”

Go back to your Amazon Console, select **SES** service

Under SES home dashboard select “**Email Address**”

Check your email is **verified**

Note: If mail is not received check in spam box, you should have a valid email ID.

Email Address Identities	Status
studentcloud09@*****com	verified

3. To configure SMTP settings

From SES Home panel

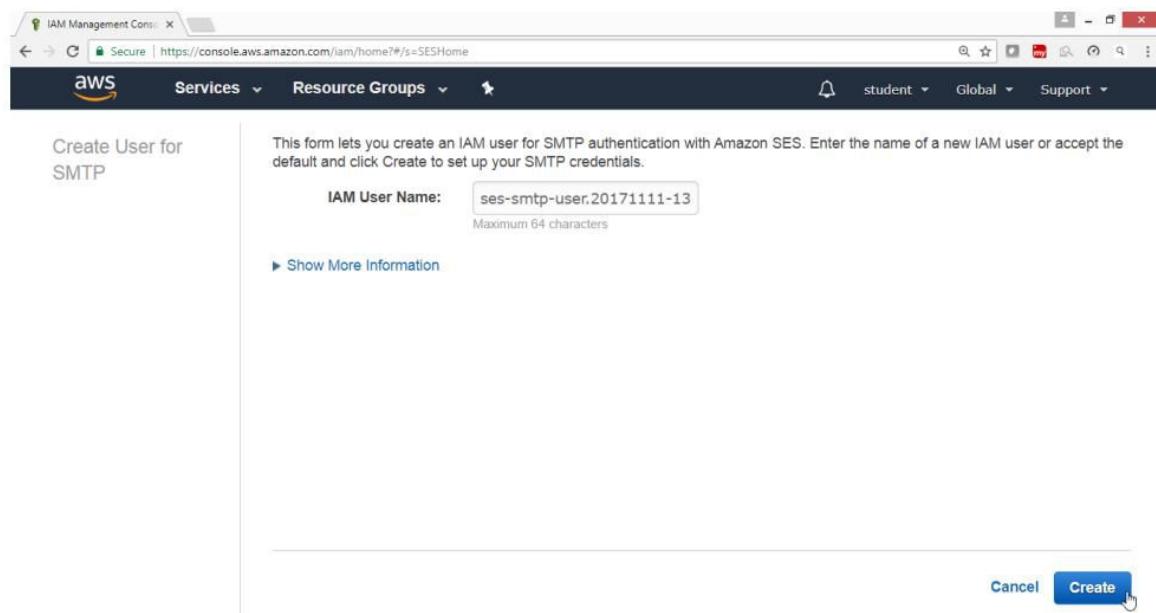
Select “SMTP Setting”

Click on “Create My SMTP Credentials” button

The screenshot shows the AWS SES Management Console interface. The left sidebar has a navigation menu with options like SES Home, Identity Management, Domains, Email Addresses, Email Sending, Sending Statistics, Reputation Dashboard, Dedicated IPs, Configuration Sets, and **SMTP Settings**. The **SMTP Settings** option is currently selected. The main content area is titled "Using SMTP to Send Email with Amazon SES". It contains instructions for sending email via SMTP, including the server name (email-smtp.us-west-2.amazonaws.com), port (25, 465 or 587), and TLS support (Yes). It also mentions that SMTP credentials are required and provides a note about the difference between AWS credentials and SMTP user credentials. A prominent blue button at the bottom of this section is labeled "Create My SMTP Credentials", which is being pointed to by a cursor.

Default **IAM user Name** will be provided

Click **Create** button



This form lets you create an IAM user for SMTP authentication with Amazon SES. Enter the name of a new IAM user or accept the default and click Create to set up your SMTP credentials.

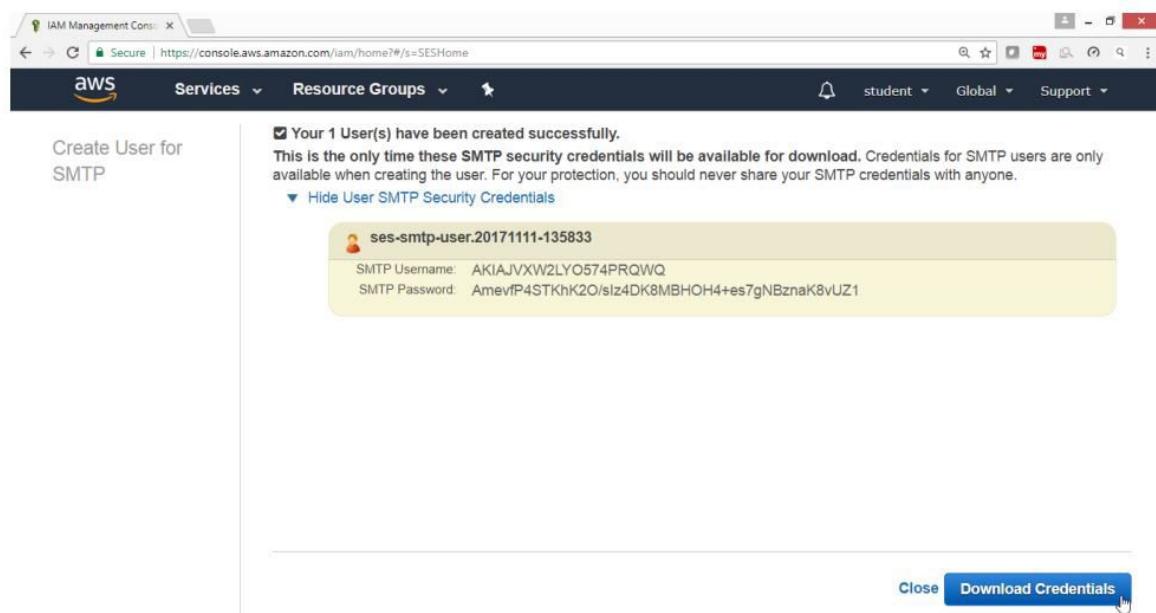
IAM User Name: ses-smtp-user.20171111-13
Maximum 64 characters

[Show More Information](#)

Create

User SMTP Security Credentials will be displayed

click "**Download Credentials**" keep at safe place



Your 1 User(s) have been created successfully.
This is the only time these SMTP security credentials will be available for download. Credentials for SMTP users are only available when creating the user. For your protection, you should never share your SMTP credentials with anyone.

[Hide User SMTP Security Credentials](#)

 ses-smtp-user.20171111-135833
SMTP Username: AKIAJVXW2LYO574PRQWQ
SMTP Password: AmevfP4STKhK2O/slz4DK8MBHOH4+es7gNBznaK8vUZ1

Download Credentials

Verify credentials

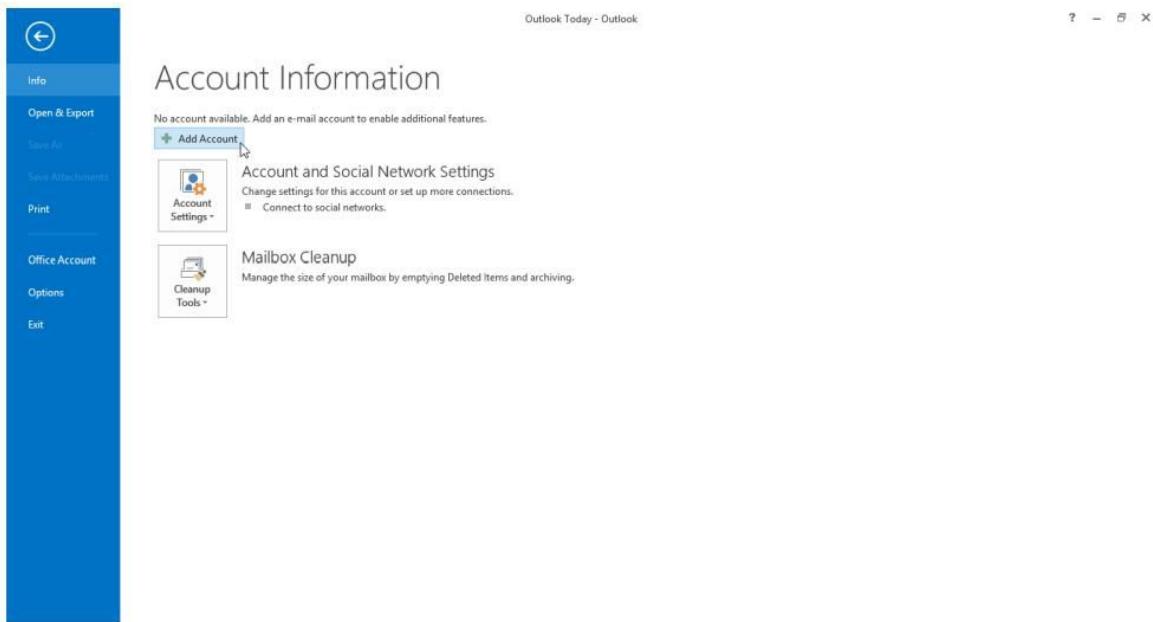
The screenshot shows the AWS IAM Management Console at <https://console.aws.amazon.com/iam/home#/sesHome>. A success message states: "Your 1 User(s) have been created successfully. This is the only time these SMTP security credentials will be available for download. Credentials for SMTP users are only available when creating the user. For your protection, you should never share your SMTP credentials with anyone." Below the message, a yellow box displays the user details: "ses-smtp-user.20171111-135833", "SMTP Username: AKIAJV...QWQ", and "SMTP Password: AmevfP4...gNBznaK8vUZ1".

Open Outlook

The screenshot shows the Microsoft Outlook application window titled "Outlook Today - Outlook". The ribbon menu is visible with tabs like FILE, HOME, SEND / RECEIVE, FOLDER, and VIEW. The HOME tab is selected. The main area shows a calendar for "Saturday, November 11, 2017" with no events listed. To the right, there are sections for "Tasks" and "Messages". The "Messages" section shows a summary of inbox, drafts, and outbox items.

Folder	Count
Inbox	0
Drafts	1
Outbox	0

Click Add Account



Select Manual Setup

Add Account X

Auto Account Setup
Manual setup of an account or connect to other server types.

E-mail Account

Your Name:
Example: Ellen Adams

E-mail Address:
Example: ellen@contoso.com

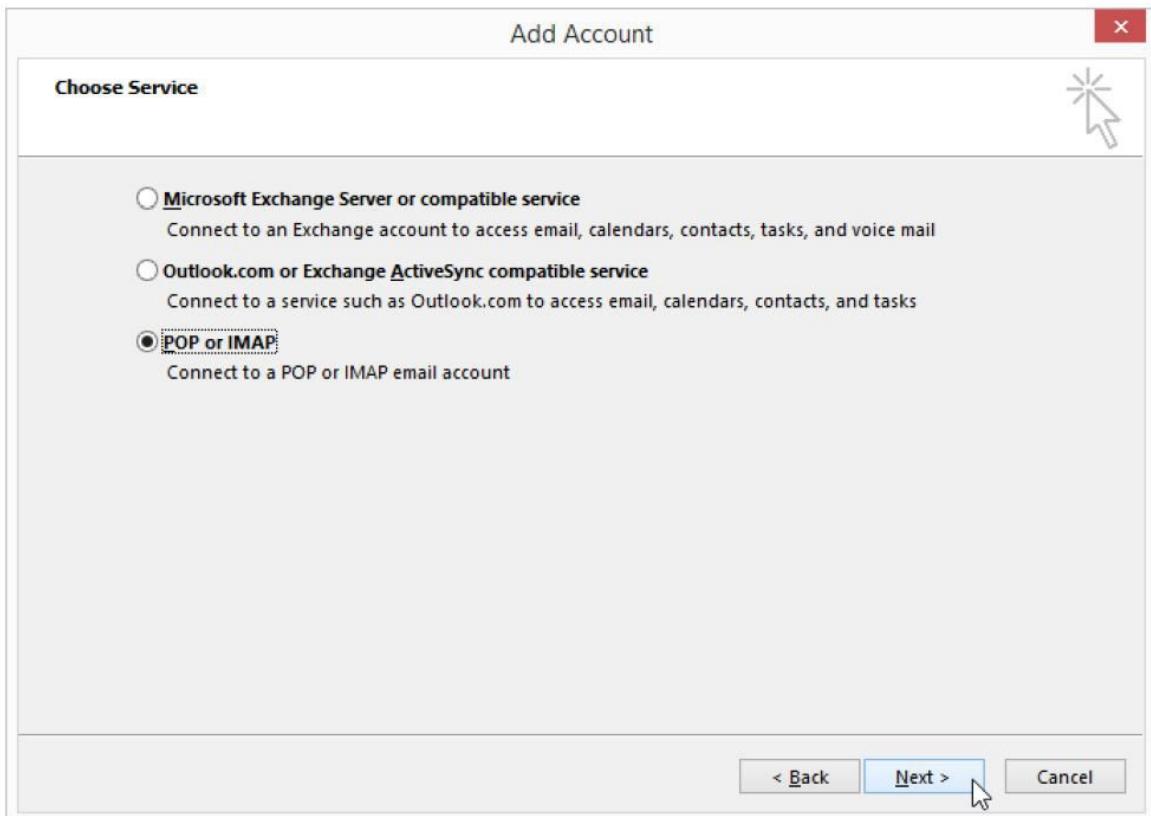
Password:

Retype Password:
Type the password your Internet service provider has given you.

Manual setup or additional server types

[< Back](#) [Next >](#) [Cancel](#)

Select POP or IMAP, click on next



Provide following details

Add Account X

POP and IMAP Account Settings
Enter the mail server settings for your account.

User Information

Your Name: studentcloud09
Email Address: studentcloud09@***.com

Server Information

Account Type: IMAP
Incoming mail server: imap.***.com
Outgoing mail server (SMTP): email-smtp.us-west-2.amazo

Logon Information

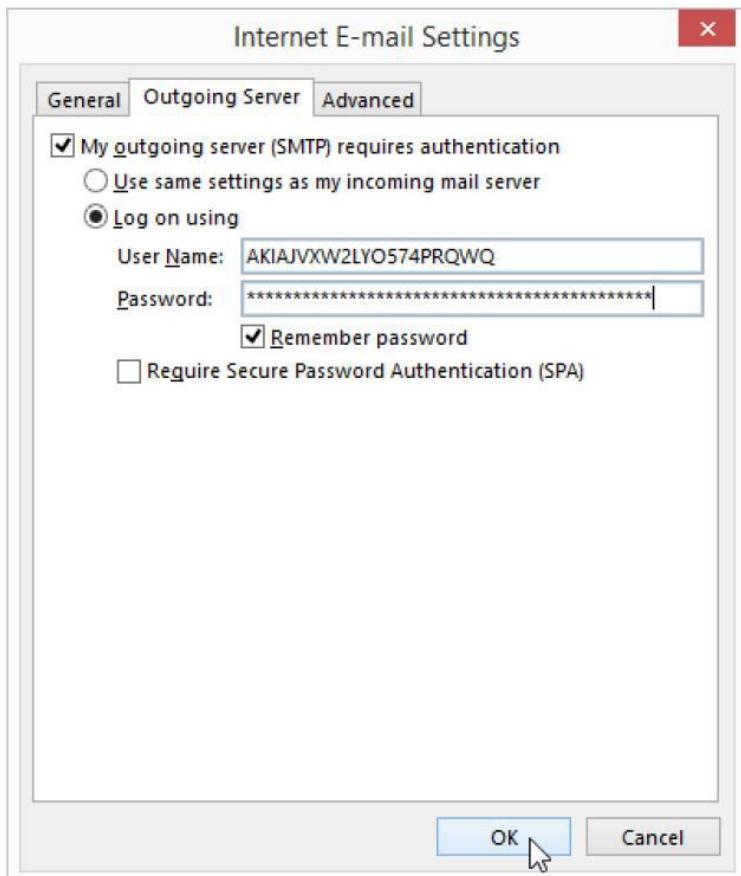
User Name: studentcloud09@***.com
Password: *****

Remember password
 Require logon using Secure Password Authentication (SPA)

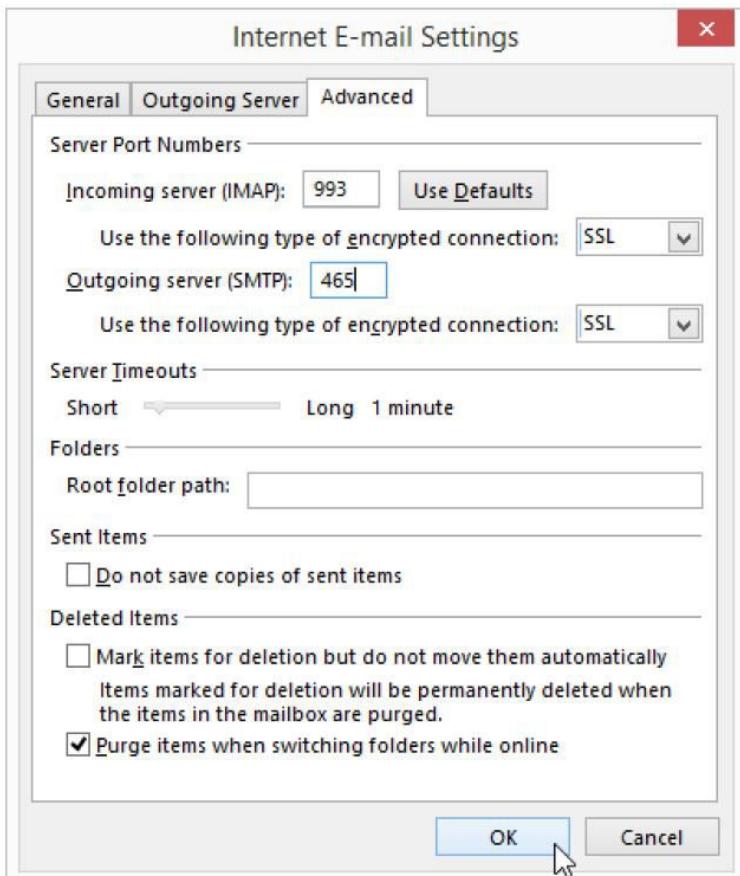
[More Settings ...](#)

[< Back](#) [Next >](#) [Cancel](#)

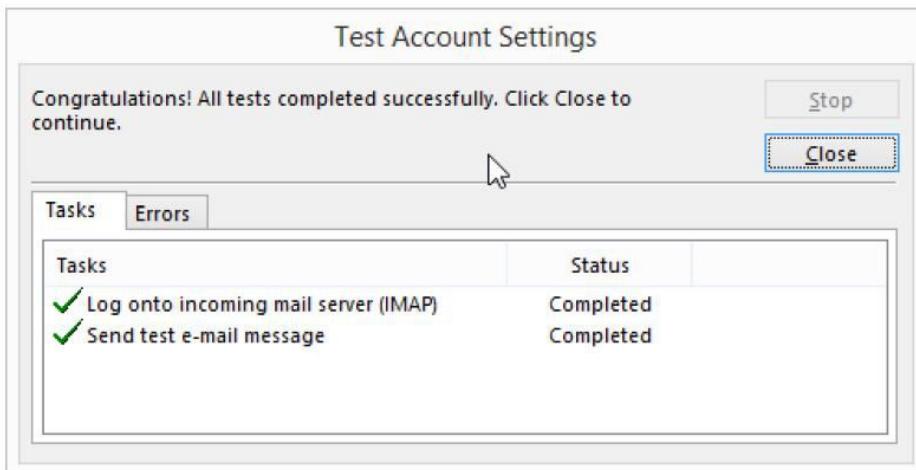
Provide following details in Outgoing Server



Provide following details in Advance



Verify successfully connected

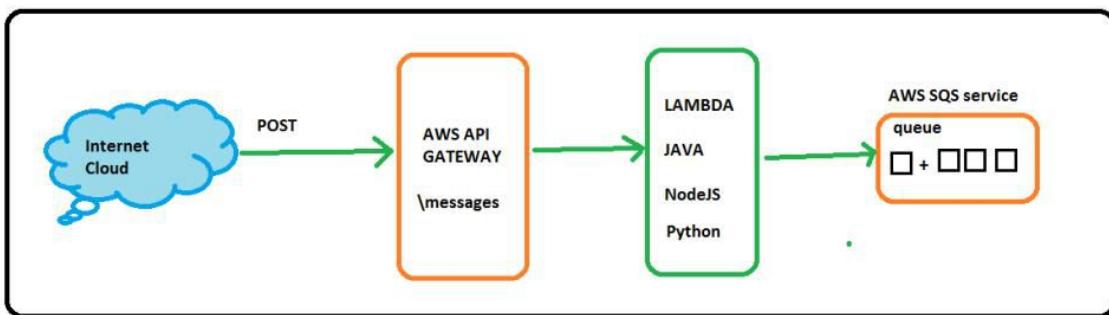


Lab 19: To Configure Amazon Simple QUEUE Service SQS

Objective

TO configure and use Simple Queue Service (SQS)

SQS Topology



PRE-REQUISITES

User should have AWS account, or IAM user with SQSfullaccess

To Configure SQS with following task:

Create the Queue

Send the message

Pool the queue

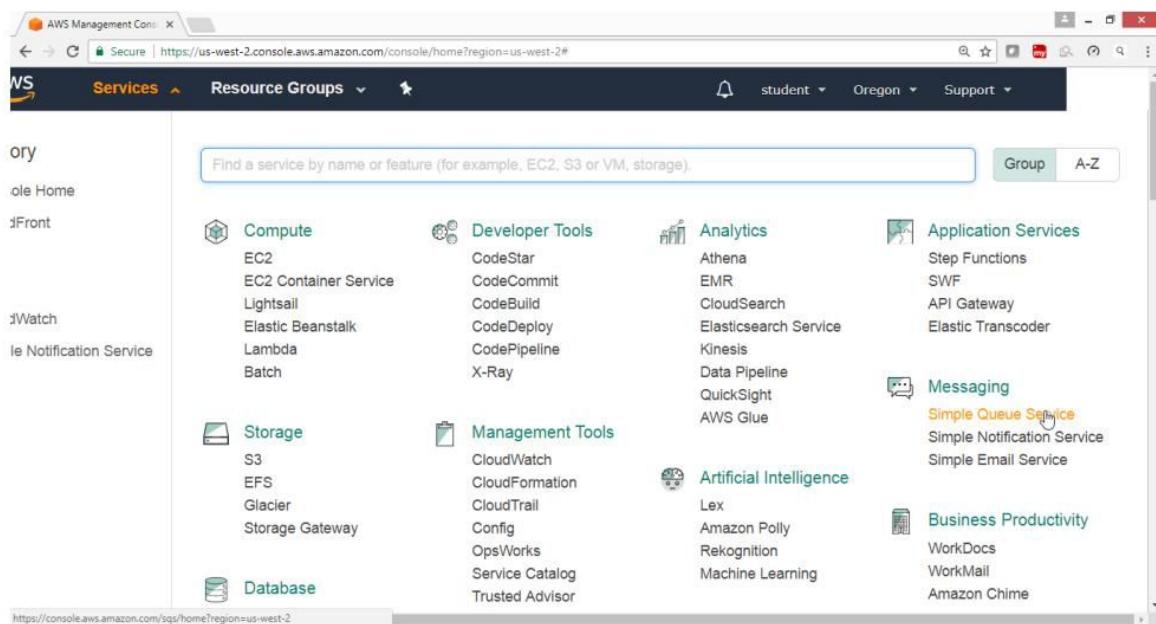
View the message

Delete the message

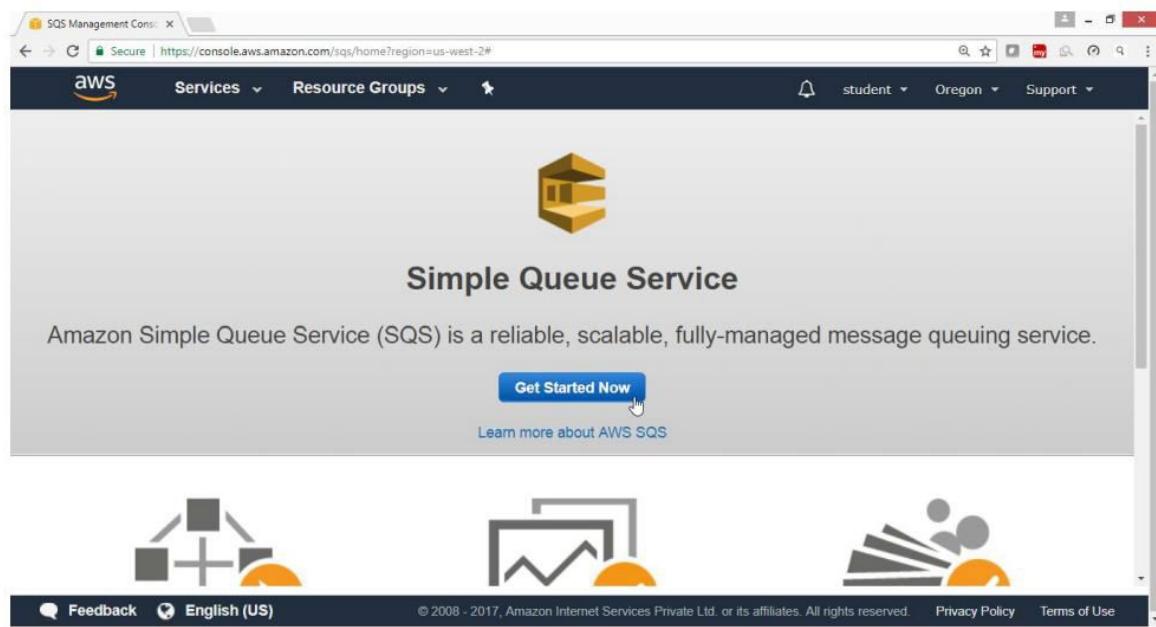
1) To Configure Amazon Simple Queue Service SQS

From the AWS console select service **Messaging** service

Select Simple Queue service



Click on **Get started on**

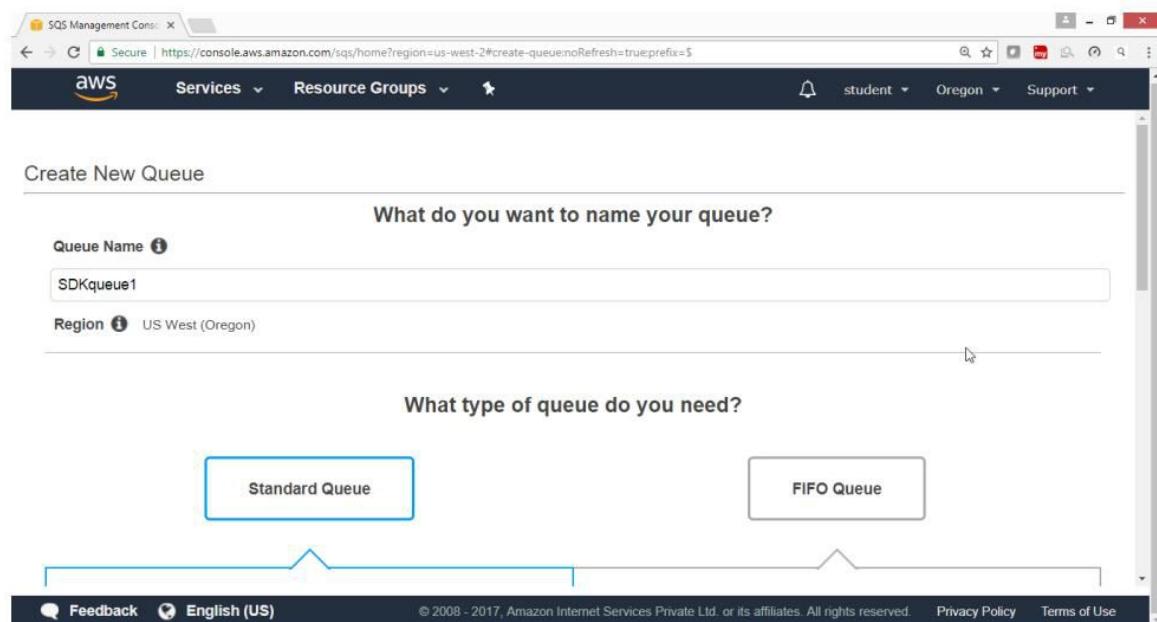


In “Create New Queue” wizard

Provide following values

Queue Name => SDKqueue1
Region => US West (Oregon)

leave the remaining values as default



Click on “Quick-Create Queue” button

The screenshot shows the AWS SQS Management Console home page. At the top, there are two large callout boxes. The left box discusses throughput and examples like decoupling user requests from background work. The right box discusses ordering and examples like ensuring command execution order. Below these boxes, a note says "For more information, see the Amazon SQS FAQs and the [Amazon SQS Developer Guide](#)". A prominent blue button at the bottom right is labeled "Quick-Create Queue".

Verify Queue is Created

The screenshot shows the AWS SQS Management Console after creating a queue. The main table lists one queue: "SDKqueue1" (Standard type, N/A content-based deduplication, 0 messages available, 0 messages in flight, created on 2017-11-12 18:42:48 GMT+05:30). Below the table, a detailed view of "SDKqueue1" is shown with tabs for Details, Permissions, Redrive Policy, Monitoring, Tags, and Encryption. The Details tab displays the queue's name, URL, ARN, creation date, last update date, and delivery delay. To the right, configuration details are listed: Default Visibility Timeout (30 seconds), Message Retention Period (4 days), Maximum Message Size (256 KB), Receive Message Wait Time (0 seconds), and Messages Available (Visible) (0).

Select the Queue

Drop down “Queue Action” button

select “Send message”

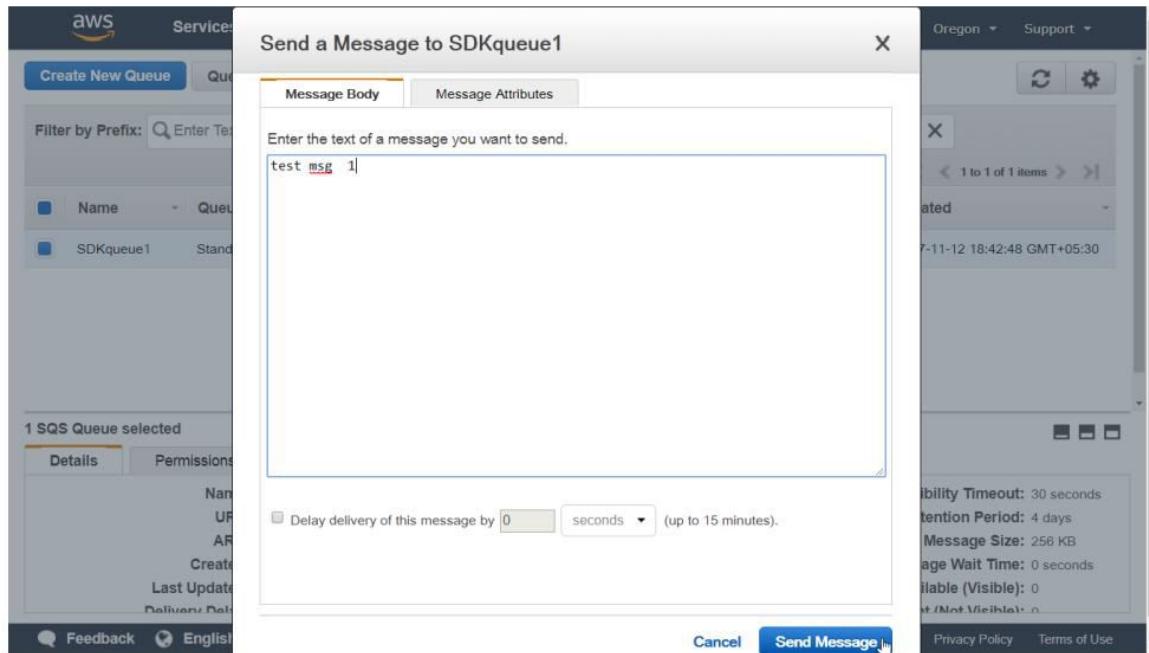
The screenshot shows the AWS SQS Management Console interface. At the top, there's a navigation bar with 'Services', 'Resource Groups', and user information. Below it, a sidebar lists 'Create New Queue' and 'Queue Actions'. A dropdown menu is open under 'Queue Actions', showing options like 'Send a Message' (which is highlighted in orange), 'View/Delete Messages', 'Configure Queue', 'Add a Permission', 'Purge Queue', 'Delete Queue', and 'Subscribe Queue to SNS Topic'. The main content area shows a table for 'SDKqueue1' with columns for 'Name', 'Created', 'Messages Available', 'Messages in Flight', and 'Created'. The table shows 0 messages in all categories. On the left, a sidebar shows '1 SQS Queue selected' with tabs for 'Details', 'Permissions', 'Redrive Policy', 'Monitoring', 'Tags', and 'Encryption'. The 'Details' tab is active, displaying queue details such as Name: SDKqueue1, URL: https://sqs.us-west-2.amazonaws.com/523251683217/SDKqueue1, ARN: arn:aws:sqs:us-west-2:523251683217:SDKqueue1, Created: 2017-11-12 18:42:48 GMT+05:30, Last Updated: 2017-11-12 18:42:48 GMT+05:30, and Delivery Delay: 0 seconds. To the right of these details are configuration parameters: Default Visibility Timeout: 30 seconds, Message Retention Period: 4 days, Maximum Message Size: 256 KB, Receive Message Wait Time: 0 seconds, Messages Available (Visible): 0, and Messages in Flight (Not Visible): 0. At the bottom, there are links for 'Feedback', 'English (US)', 'Privacy Policy', and 'Terms of Use'.

From “Send a Message to SDKqueue” Wizard

In Message Body type the Message

Note: Message size should not be more than 64K

click on “Send Message” then elect close

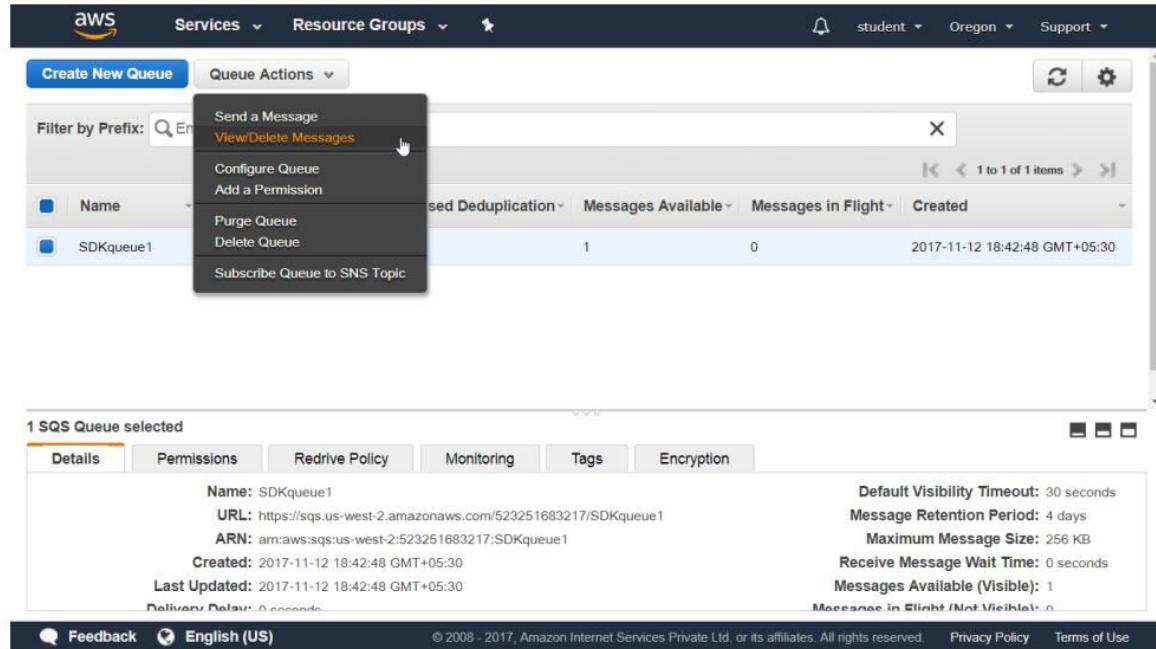


2) To View the message

Select the Queue

Drop down **Queue Action** button

Select the option “**View/Delete Message**”



The screenshot shows the AWS SQS console. A dropdown menu titled "Queue Actions" is open, with the "View/Delete Messages" option highlighted. Below the menu, a table displays a single queue named "SDKqueue1". The table includes columns for "Messages Available", "Messages in Flight", and "Created". The "Messages Available" column shows a value of 1. At the bottom of the page, there is a summary section for the selected queue, listing details like Name, URL, ARN, and visibility timeout.

Name	URL	ARN	Default Visibility Timeout	Message Retention Period	Maximum Message Size
SDKqueue1	https://sns.us-west-2.amazonaws.com/523251683217/SDKqueue1	arn:aws:sns:us-west-2:523251683217:SDKqueue1	30 seconds	4 days	256 KB

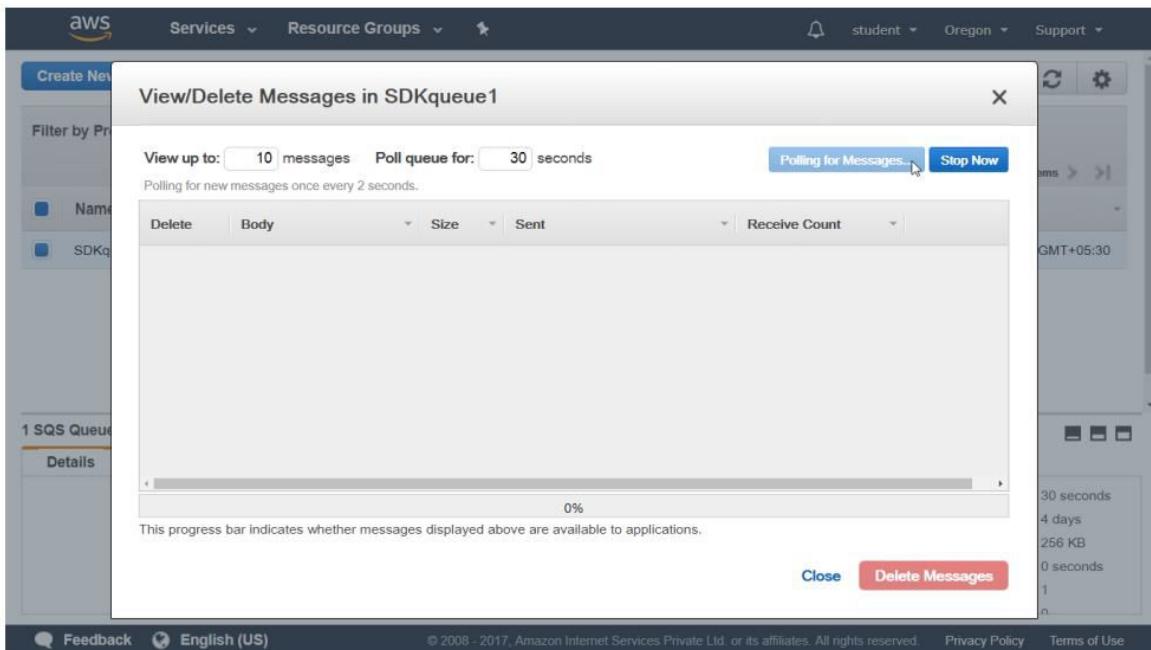
SDKqueue1

1 to 1 of 1 items

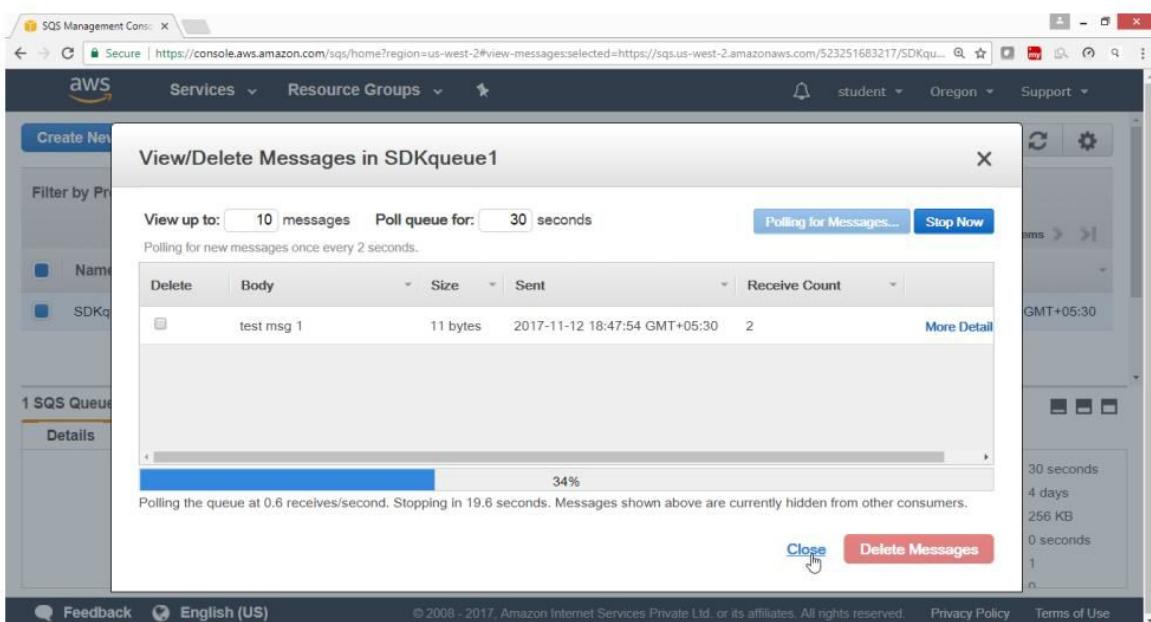
1 0 2017-11-12 18:42:48 GMT+05:30

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

Click "Start Polling for Message"



Verify message is in the queue



3) To delete the message

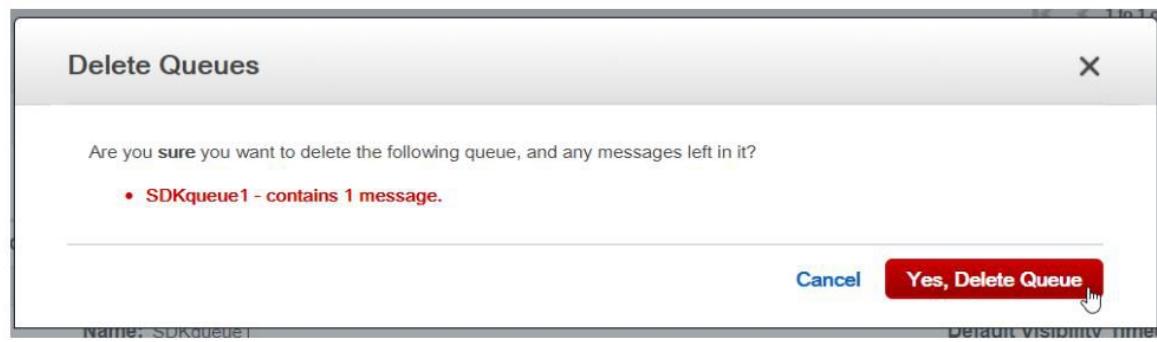
Select the Queue

Drop Down Queue Action

Select “Delete Message”

The screenshot shows the AWS SQS Management Console interface. In the center, there is a table with one item: 'SDKqueue1'. The 'Actions' column for this item has a dropdown menu open, with 'Delete Queue' highlighted. The main pane below shows details for 'SDKqueue1', including its name, URL, ARN, creation and update times, and visibility timeout settings. A confirmation message at the bottom of the page reads: "Are you sure you want to delete the following queue, and any messages left in it? • SDKqueue1 - contains 1 message."

Confirm

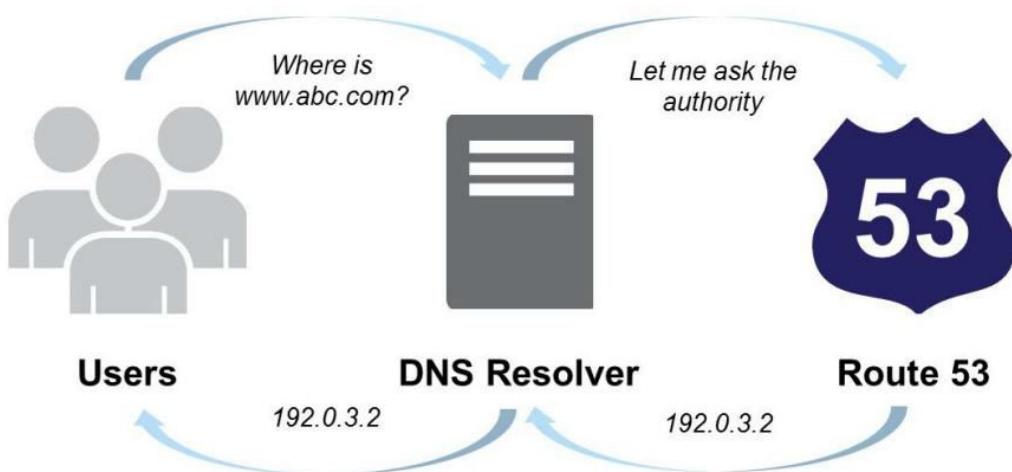


Lab 20: To Configure Amazon Route 53

OBJECTIVE

To configure and use AWS Route53 service

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with AmazonRoute53FullAccess

By default AWS does not provide to Register Domain Name with AWS

You should have a registered domain name one with your ISP

To Configure Route53 with following task:

To Transfer existing DNS service from your ISP to Amazon Route 53

Creating record set

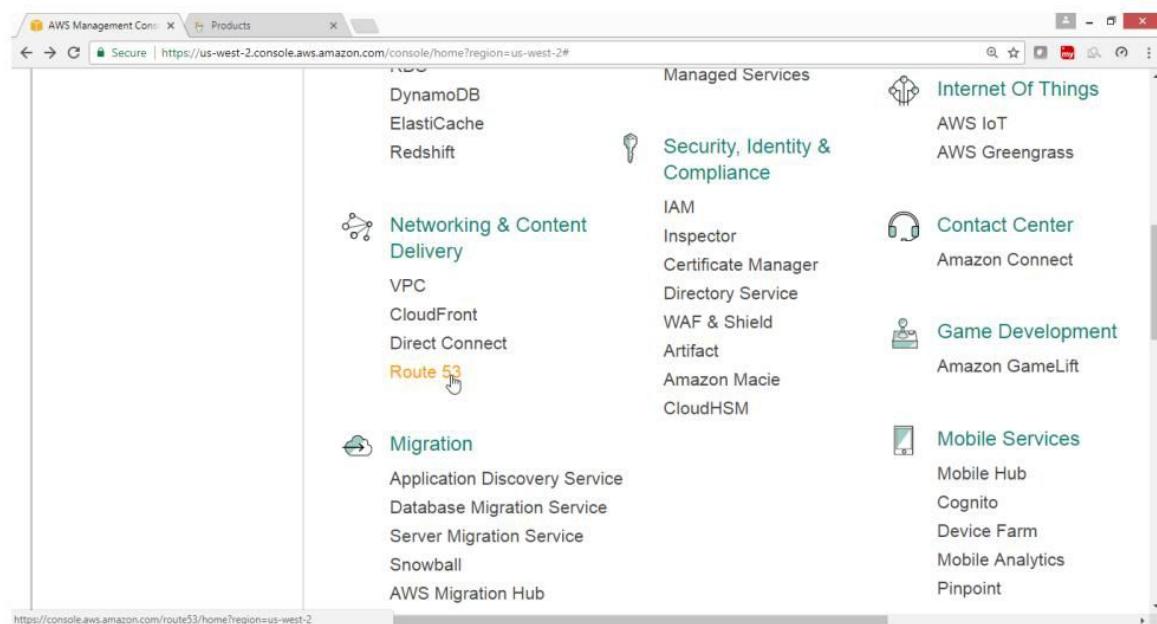
Creating CNAME record set

Step-1: Configuration of Route53 for your Domain Name

Open AWS console

Select “Networking & Content Delivery”

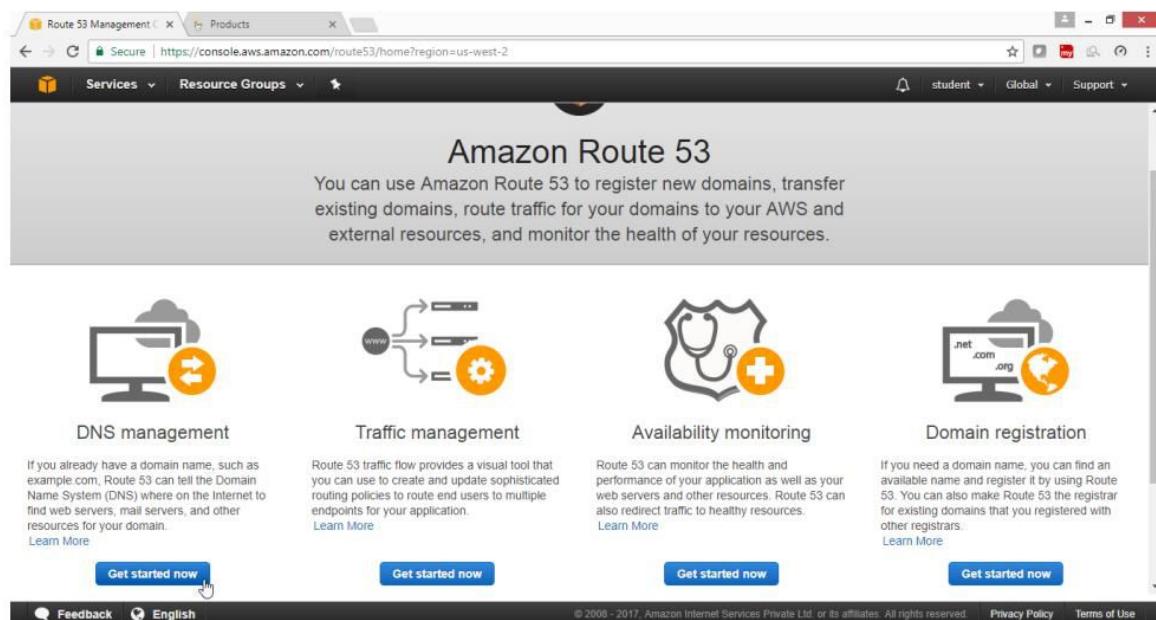
Click on **Route 53** services



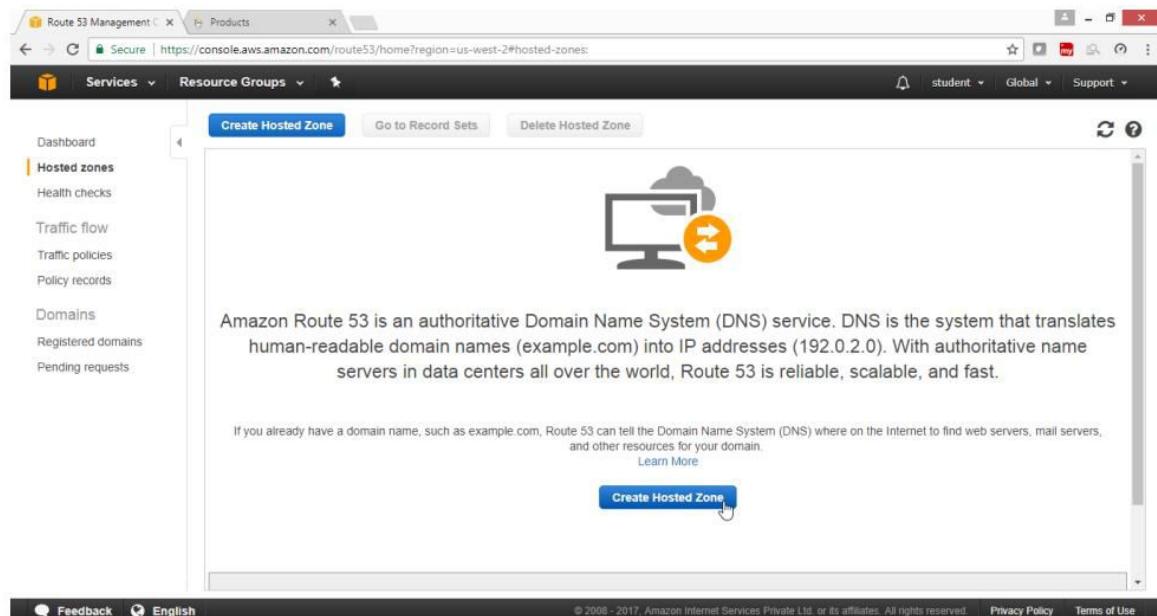
Route53 DashBoard wizard opens

Under DNS management

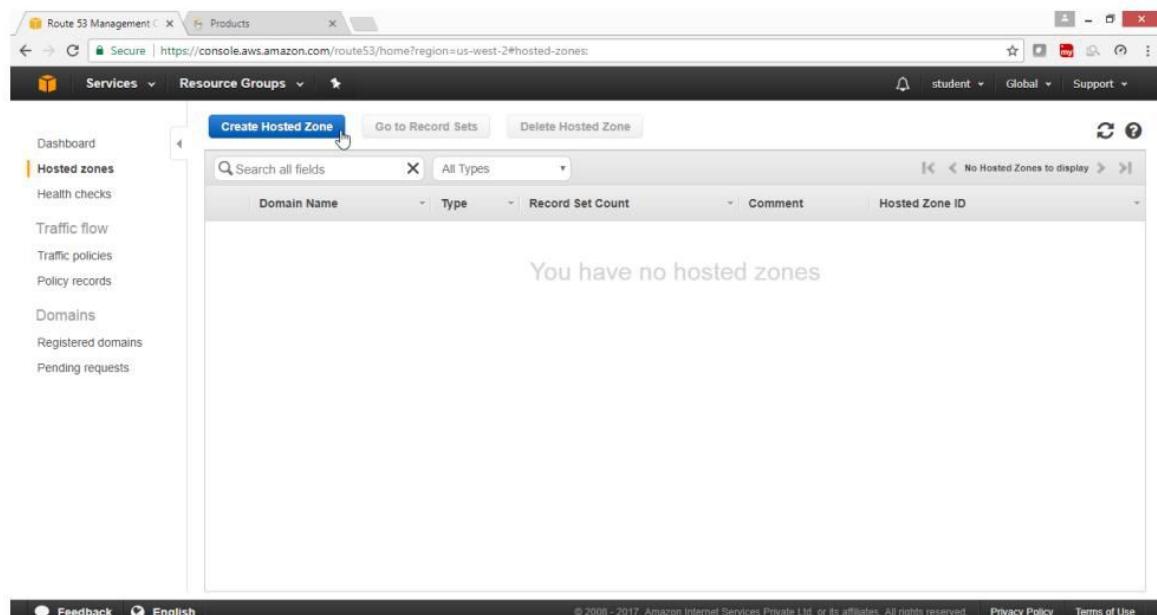
Click on “Get started Now” button



Click on “Created Hosted Zone” button



Again Click on Create Hosted Zone button



Under “**Created Hosted Zone**”, wizard

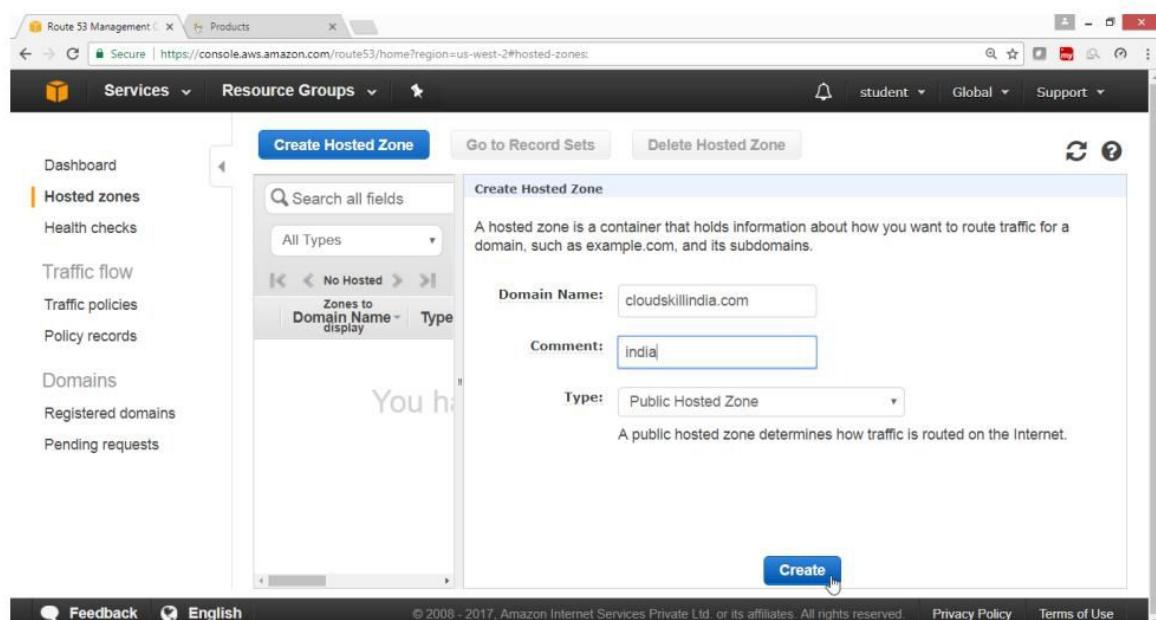
On right side panel provide following values

For Domain Name: → cloudskillindia.com

For Comment → india

For Type → Public Hosted Zone

Click on **Create** button



Now the list of AWS NS records will appear

Now add all AWS NS record to your local DNS NS record (godaddy.com)

The screenshot shows the AWS Route 53 Management console. On the left, there's a sidebar with options like Dashboard, Hosted zones, Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The main area is titled 'Edit Record Set' for a zone named 'cloudskillindia.com.'. It shows a table with two entries: one for NS type with values ns-140.awsdns-17.com., ns-1565.awsdns-03.co.uk., ns-726.awsdns-26.net., and ns-1286.awsdns-32.org.; and another for SOA type with value ns-140.awsdns-17.com.. The TTL is set to 172800 seconds. A note says 'The domain name of a name server. Enter multiple name servers on separate lines.' and provides an example: ns1.amazon.com, ns2.amazon.org, ns3.amazon.net.

Step-2: Now copy these DNS NS record in godaddy.com for cloudskillindia.com domain.

ns-140.awsdns-17.com

ns-1565.awsdns-03.co.uk

ns-726.awsdns-26.net

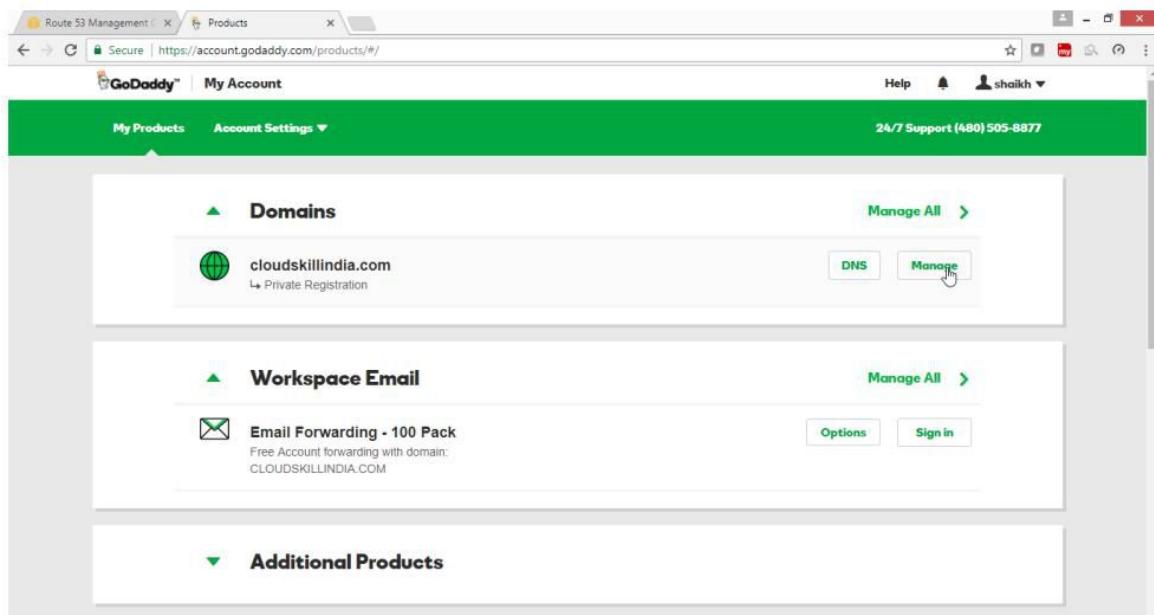
ns-1286.awsdns-32.org

Open the browser

Go to godaddy.com site

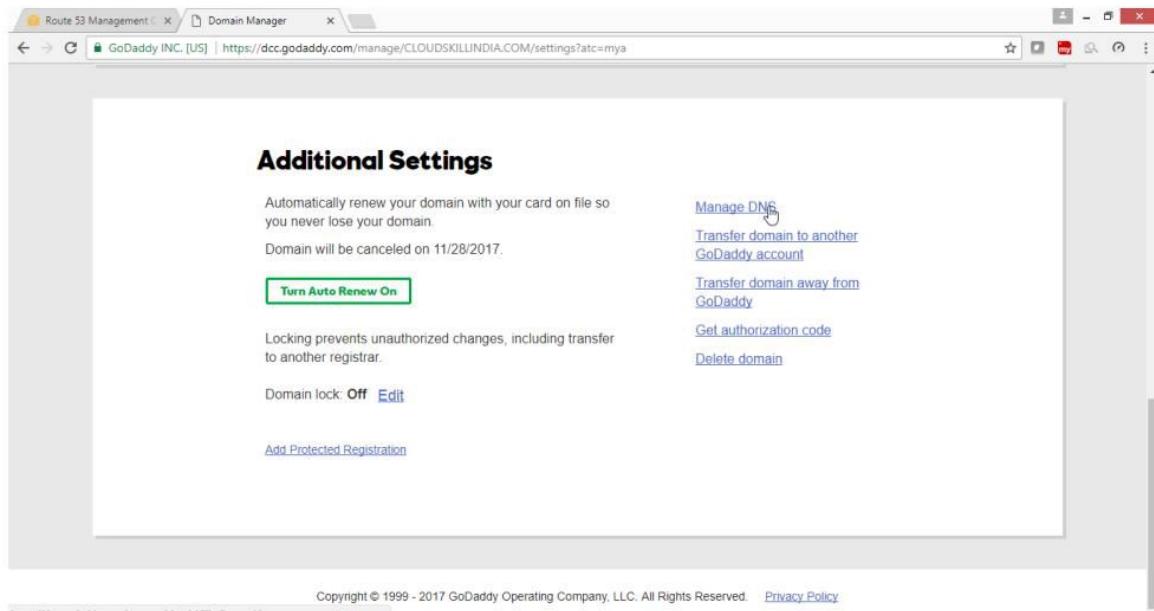
Login and select your domain name

Click on **Manage**



Drag Down

Click on **Manage DNS**



Click on change

Add latest entries provided by Route53 NS records

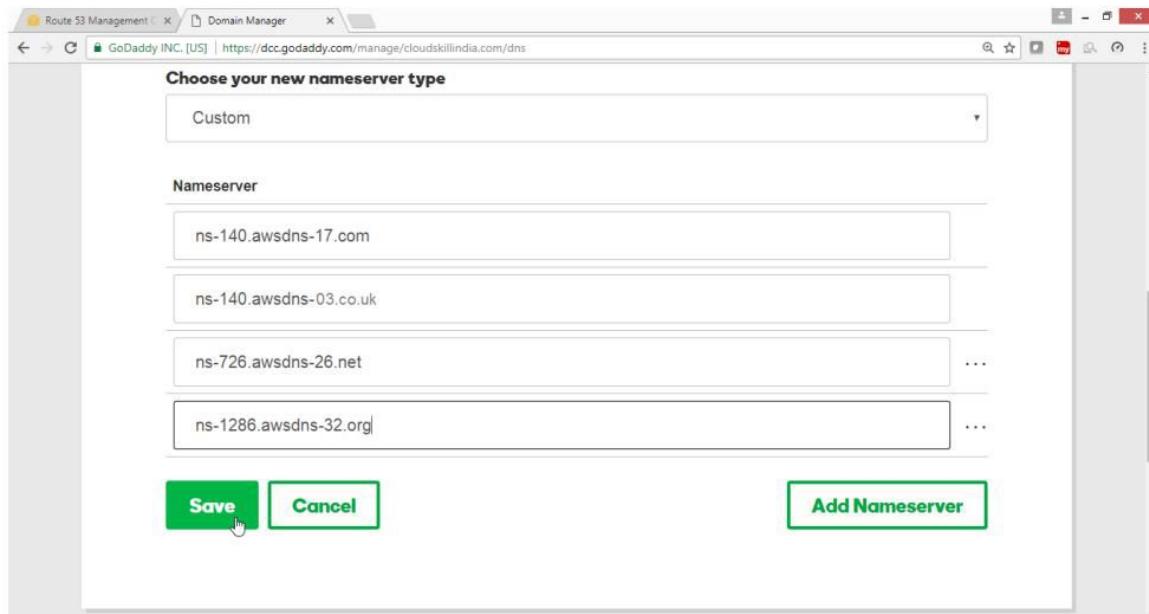
The screenshot shows a web browser window titled "Route 53 Management" with a tab labeled "Domain Manager". The URL is https://dcc.godaddy.com/manage/cloudskillindia.com/dns. The main content area is titled "Nameservers". It displays a list of nameservers under the heading "Using custom nameservers" with a "Change" button. The listed nameservers are:

- ns-652.awsdns-17.net
- ns-1796.awsdns-32.co.uk
- ns-1378.awsdns-44.org
- ns-351.awsdns-43.com

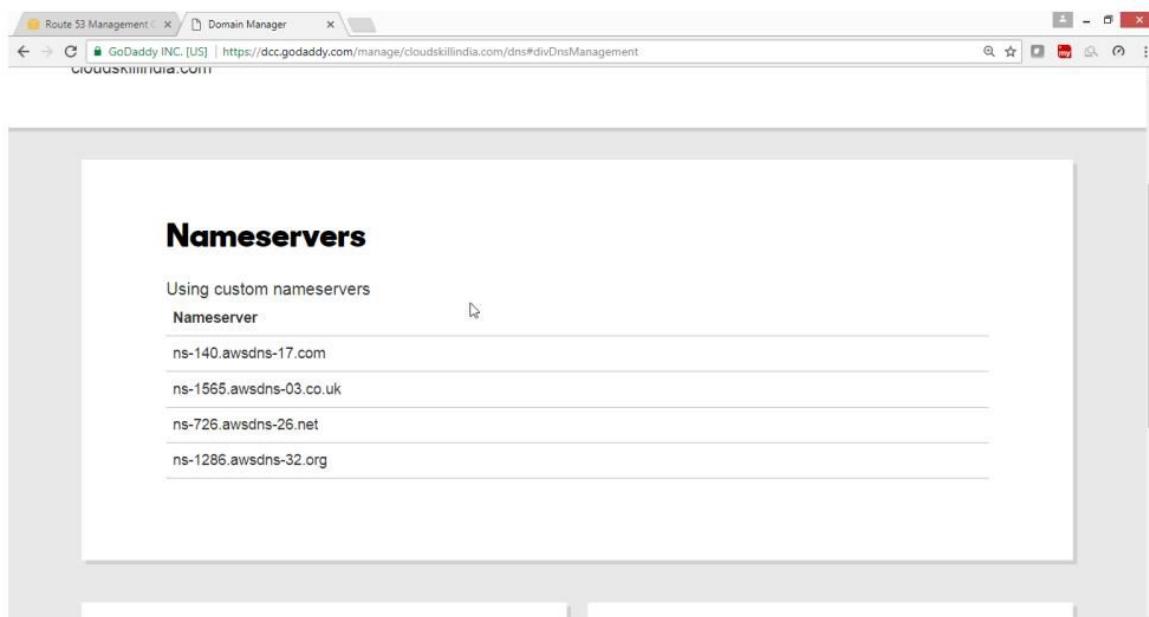
For Choose your new name server → Custom

Replace old NS records with latest NS records

Click on Save button



Verify New names got updated.



Step-3. Launch an instance Configure it as a webserver.

Launch an Amazon linux Instance

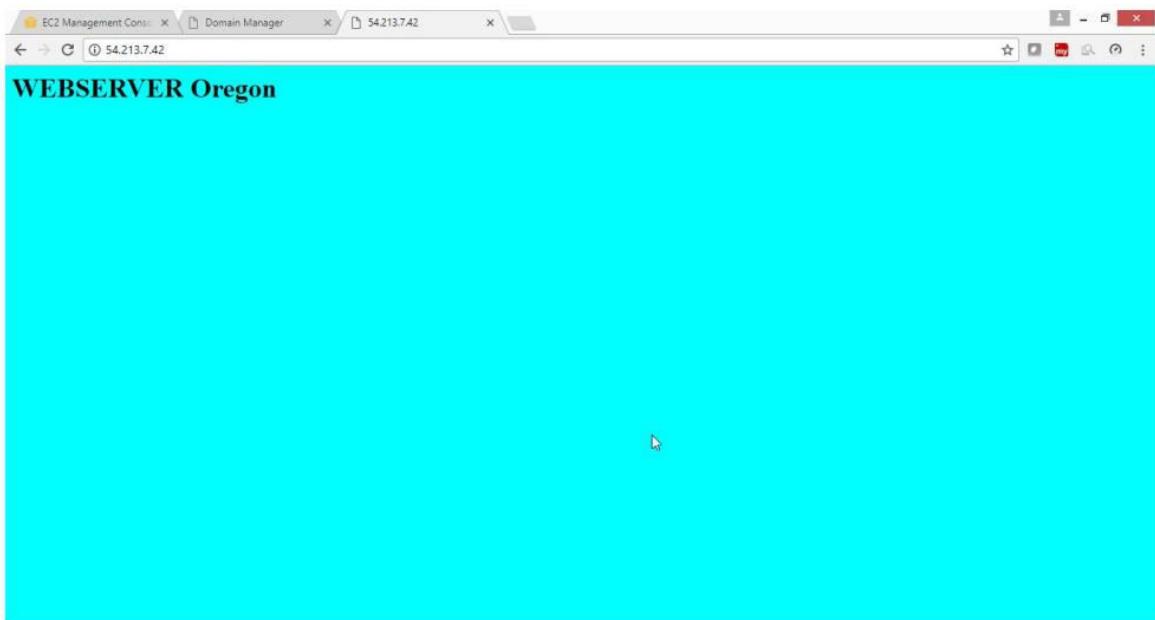
Configure it as a Web Server

Note: Repeat LAB Hosting webserver on linux.

Copy the public IP and type in Browser

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block Store. The main area displays a table of instances. One instance, named 'linuxvm1', is selected. Below the table, detailed information is shown for this instance, including its Instance ID (i-0986868cc14262f26), Instance Type (t2.micro), Availability Zone (us-west-2a), and State (running). The Public DNS is listed as 'ec2-54-213-7-42.us-west-2.compute.amazonaws.com'. The Public IPv4 IP is highlighted in blue as '54.213.7.42'. Other details shown include Instance state (running), Instance type (t2.micro), and Elastic IPs.

Verify Website is accessible



Step-4: To add a A record and CNAME record in Route53

From **Route 53 Dashboard**

Click on “**Hosted Zones**”

Select **Domain Name**

Click on “**cloudskillindia.com**”

The screenshot shows the AWS Route 53 Management console. In the top navigation bar, there are tabs for 'Route 53 Management', 'Domain Manager', and '54.213.742'. The URL in the address bar is <https://console.aws.amazon.com/route53/home?region=us-west-2#hosted-zones>. The main interface has a sidebar with options like 'Dashboard', 'Hosted zones' (which is selected and highlighted in orange), 'Health checks', 'Traffic flow', 'Traffic policies', 'Policy records', 'Domains', 'Registered domains', and 'Pending requests'. The main content area is titled 'Hosted Zone Details' for the domain 'cloudskillindia.com'. It shows the following details:

- Domain Name:** cloudskillindia.com.
- Type:** Public Hosted Zone
- Hosted Zone ID:** Z3IBZ8DEZM6NPV
- Record Set Count:** 2
- Comment:** India
- Name Servers:** ns-140.awsdns-17.com, ns-1565.awsdns-03.co.uk, ns-726.awsdns-26.net, ns-1286.awsdns-32.org

A note at the bottom states: "Before the Domain Name System will start to route queries for this domain to Route 53 name servers, you must update the name server records either with the current DNS service or with the registrar for the domain, as applicable. For more information, click the ? icon above."

Click on **Create Record set** button

The screenshot shows the AWS Route 53 Domain Manager interface. The left sidebar is titled "Hosted zones" and lists several options: Dashboard, Hosted zones (which is selected and highlighted in orange), Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The main content area has a header with "Back to Hosted Zones", "Create Record Set" (which is highlighted with a blue box and a cursor arrow), "Import Zone File", and "Delete Record Set". Below this is a search bar with "Record Set Name" and a dropdown menu set to "Any Type". There are two checkboxes: "Aliases Only" and "Weighted Only", with "Aliases Only" being checked. A note below the search bar says: "To get started, click Create Record Set button or click an existing record set." A table displays two record sets for the domain "cloudskillindia.com." The first record set is of type NS and points to four nameservers: ns-140.awsdns-17.com, ns-1565.awsdns-03.co.uk, ns-726.awsdns-26.net, and ns-1286.awsdns-32.org. The second record set is of type SOA and points to ns-140.awsdns-17.com and awsc. The table has columns for "Name", "Type", and "Value". At the bottom of the page, there are links for "Feedback", "English", "© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.", "Privacy Policy", and "Terms of Use".

To add A record

On right side Under **Create Record set**

Provide following values

NAME	→ org.cloudskillindia.com
Type	→ A-Ipv4 address
Alias	→ No
Value	=> 54.213.7.42 [Give your Instance Public IP]

Click on “Create” button

The screenshot shows the AWS Route 53 Management console with the 'Domain Manager' tab selected. On the left, there's a sidebar with options like Dashboard, Hosted zones, Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The 'Hosted zones' option is currently selected. In the main area, there's a 'Create Record Set' dialog. The 'Record Set Name' field contains 'org.cloudskillindia.com.'. The 'Type' dropdown is set to 'A - IPv4 address'. The 'Value' field contains '54.213.7.42'. Below the value field, there's a note: 'IPv4 address. Enter multiple addresses on separate lines.' and an example: '192.0.2.235 198.51.100.234'. At the bottom of the dialog is a 'Create' button, which is highlighted with a cursor. Above the dialog, there are tabs for 'Back to Hosted Zones', 'Import Zone File', and 'Delete Record Set'.

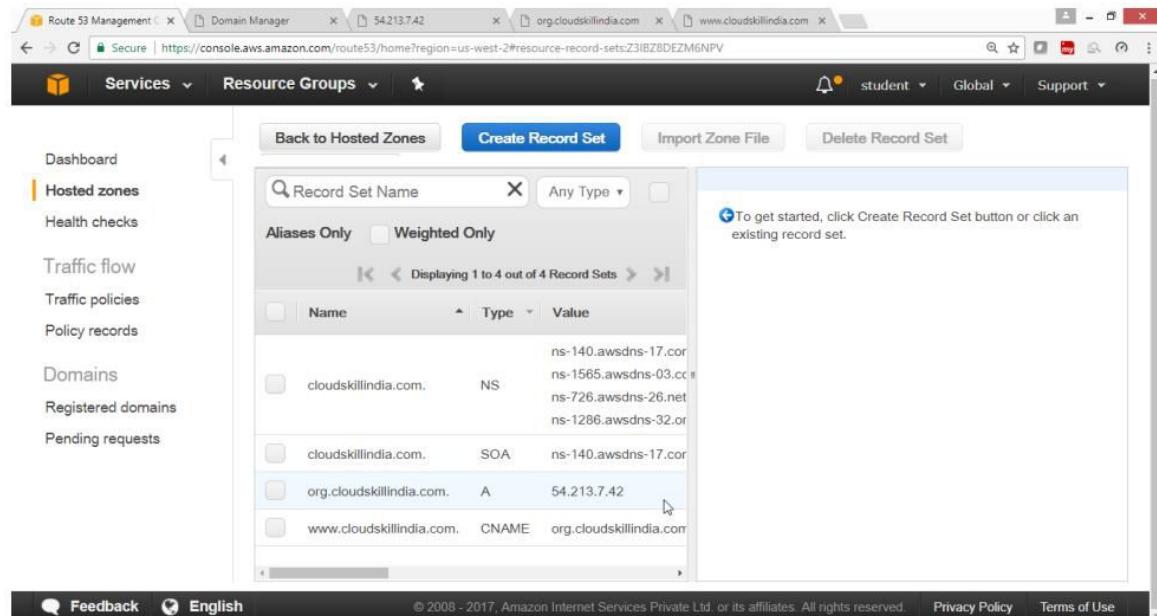
Verify the A record got created

The screenshot shows the AWS Route 53 Management console. On the left, there's a sidebar with options like Dashboard, Hosted zones, Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The 'Hosted zones' option is selected. In the main area, there's a table of existing record sets. To the right of the table, a form for creating a new record set is displayed. The 'Name' field contains 'org.cloudskillindia.com.', the 'Type' dropdown is set to 'A - IPv4 address', and the 'Value' field contains '54.213.7.42'. Below the table, there's a note about entering multiple addresses on separate lines, followed by examples: '192.0.2.235' and '198.51.100.234'. At the bottom right of the form is a 'Save Record Set' button.

Create Alias record

This screenshot shows the same AWS Route 53 Management console interface. The sidebar and table of existing record sets are identical to the previous screenshot. To the right of the table, a 'Create Record Set' form is shown. The 'Name' field is filled with 'www', the 'Type' dropdown is set to 'CNAME – Canonical name', and the 'Value' field contains 'org.cloudskillindia.com.'. Below the 'Value' field is a note explaining what it means: 'The domain name that you want to resolve to instead of the value in the Name field.' It includes an example: 'www.example.com'. At the bottom right of the form is a 'Create' button, which has a mouse cursor hovering over it.

Verify the CNAME record got created

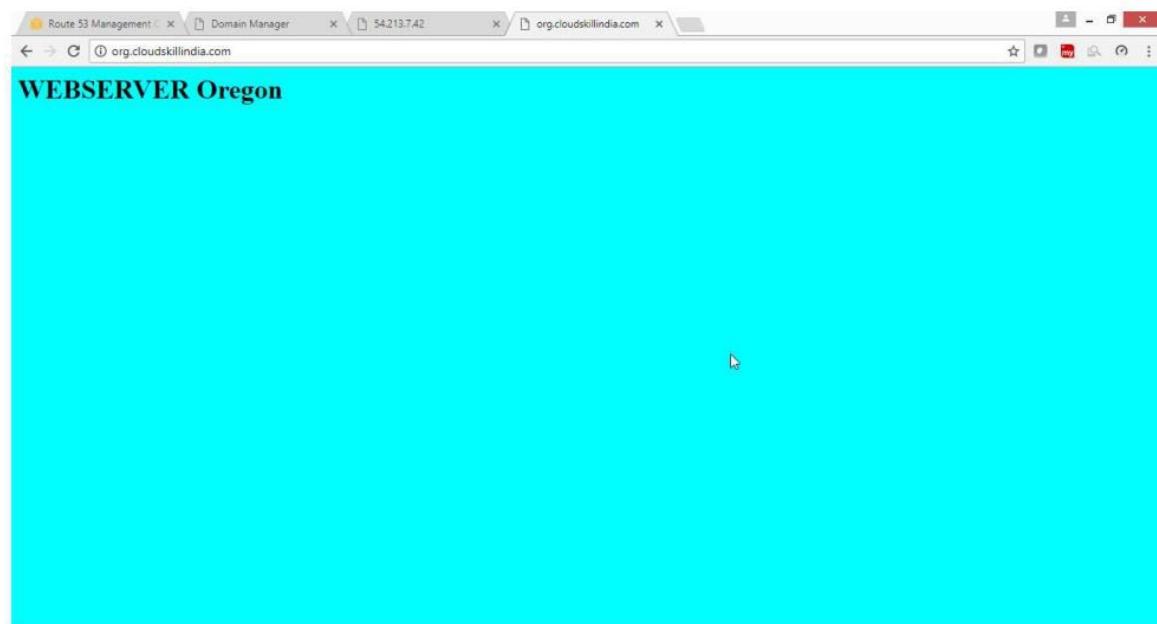


The screenshot shows the AWS Route 53 Management console. In the left sidebar, under the 'Hosted zones' section, the 'org.cloudskillindia.com' zone is selected. The main area displays a table of record sets. One record set is highlighted, showing the following details:

Name	Type	Value
cloudskillindia.com.	NS	ns-140.awsdns-17.cor ns-1565.awsdns-03.cc ns-726.awsdns-26.net ns-1286.awsdns-32.or
cloudskillindia.com.	SOA	ns-140.awsdns-17.cor
org.cloudskillindia.com.	A	54.213.7.42
www.cloudskillindia.com.	CNAME	org.cloudskillindia.com

Verification

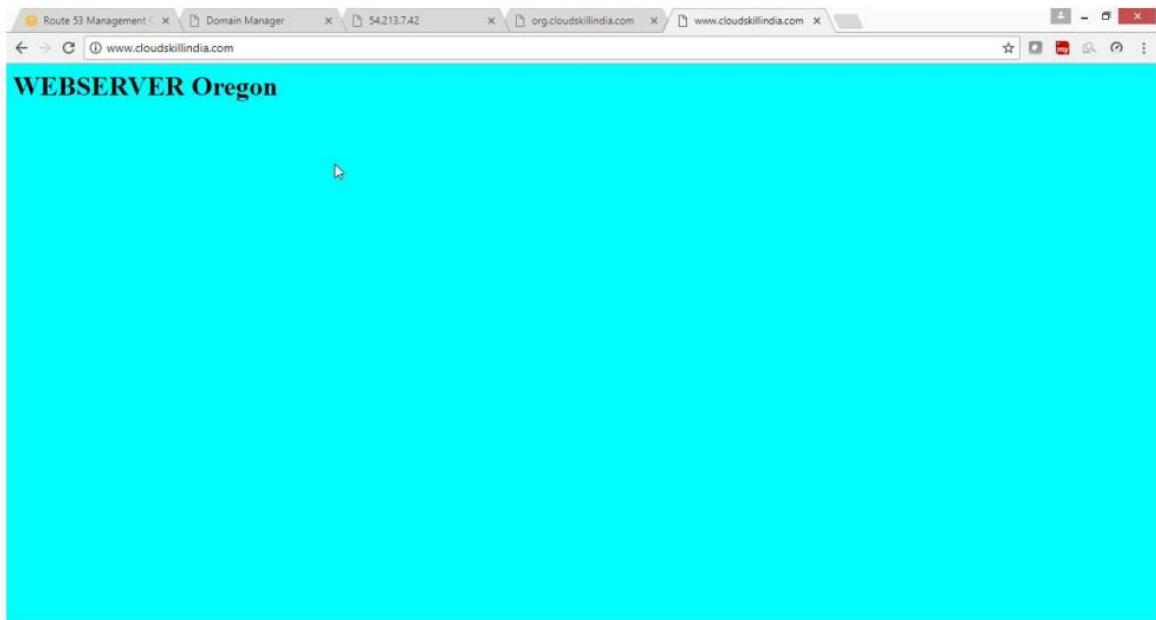
Now access the website with A record → org.cloudskillindia.com



The screenshot shows a web browser window with the URL 'org.cloudskillindia.com'. The page content is a solid teal color. At the top left, the text 'WEB SERVER Oregon' is visible in white. The rest of the page is a uniform teal color.

Verification

Now access the website with CNAME record → www.cloudskillindia.com

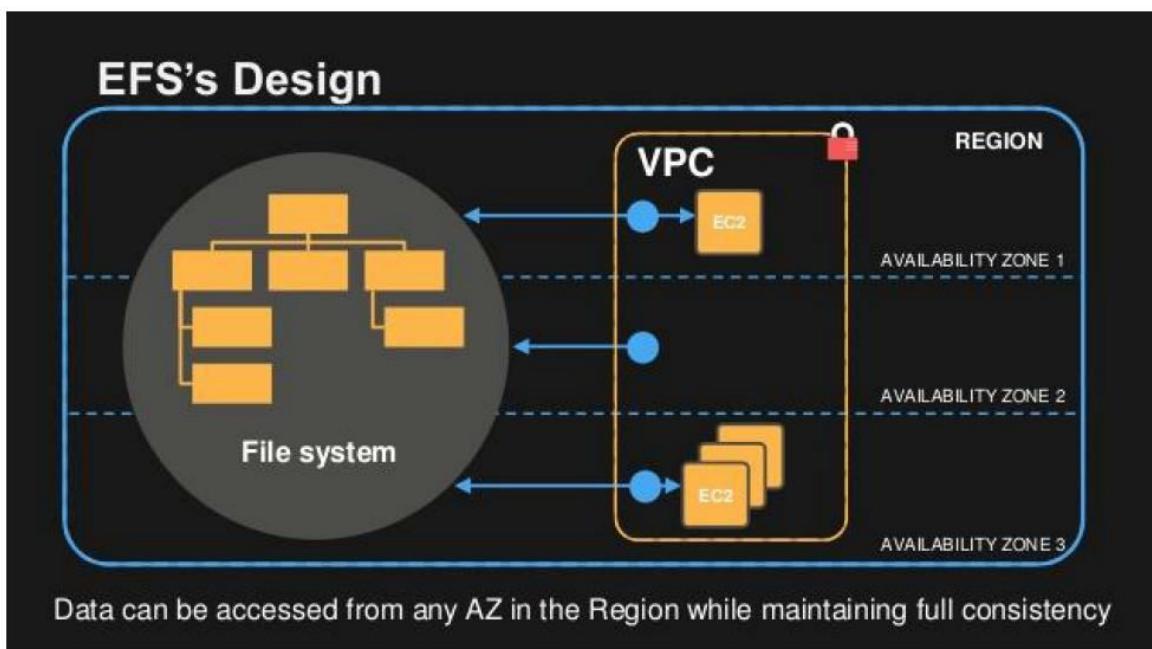


Lab 21: To configure Amazon EFS Service

OBJECTIVE

To configure and use AWS EFS Service.

TOPOLOGY



PRE-REQUISITES

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

To configure EFS with following task.

Create a security group for EFS access

Create Your Amazon EFS File System

Launch Your EC2 Instance

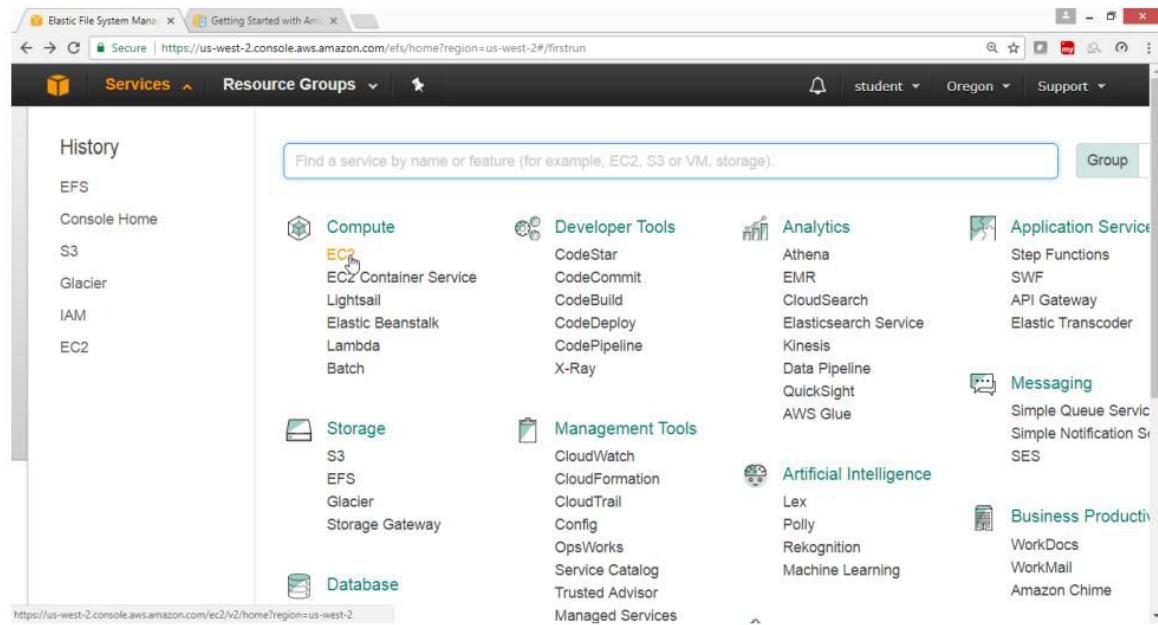
Create Your Amazon EFS File System

Mount the Amazon EFS File System in your linux launch instance

1) Create a security group for EFS access

Open AWS Console go for **Ec2 Service**

Click on **EC2**



Under EC2 Dashboard go for **Network & Security**

Select **Security Groups**

Click on **Create Security Group**

The screenshot shows the AWS EC2 Management Console interface. On the left, there is a navigation sidebar with several categories: Services (selected), Resource Groups, Bundle Tasks, ELASTIC BLOCK STORE (Volumes, Snapshots), NETWORK & SECURITY (Security Groups selected, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), LOAD BALANCING (Load Balancers, Target Groups), and AUTO SCALING (Launch Configurations). At the top, there are tabs for 'Create Security Group' (highlighted) and 'Actions'. Below the tabs is a search bar with the placeholder 'Filter by tags and attributes or search by keyword'. A table displays four security groups: sg-275b205d (Group Name: launch-wizard-1, VPC ID: vpc-89c341ee, Description: launch-wizard-1), sg-38265c42 (Group Name: launch-wizard-2, VPC ID: vpc-89c341ee, Description: launch-wizard-2), sg-a2344dd8 (Group Name: launch-wizard-3, VPC ID: vpc-89c341ee, Description: launch-wizard-3), and default (Group Name: default, VPC ID: vpc-89c341ee, Description: default VPC security group). Below the table, a message says 'Select a security group above'. At the bottom of the page, 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.

Under “Create Security Group” wizard

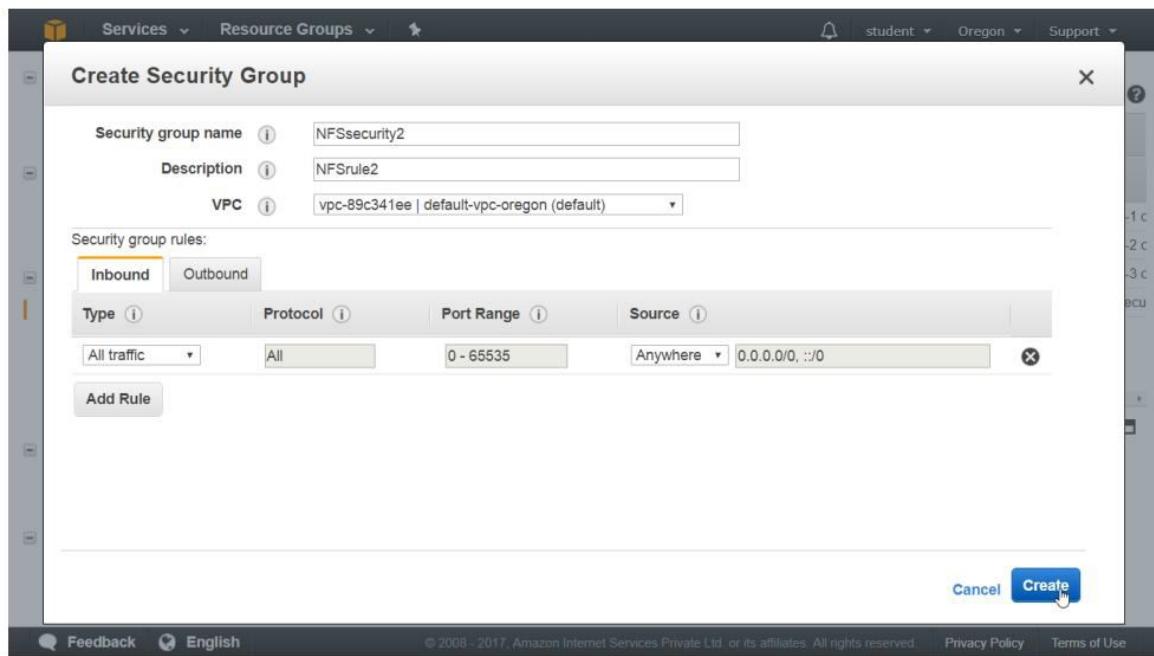
Give Following values

Security group name → NFSsecurity2
Description → NFSrule2
VPC → take default

Select Inbound

Type → All traffic
Source → Anywhere

Click on **Create** button



2) Create Your Amazon EFS File System

The screenshot shows the AWS Management Console with the 'Services' navigation bar selected. In the main content area, there is a grid of service icons. The 'Storage' category is expanded, showing 'S3', 'EFS' (which is highlighted with a yellow circle), and 'Glacier'. Below the Storage section, there is a 'Database' section.

Click on “Create file system” button

The screenshot shows the 'Amazon Elastic File System (EFS)' landing page. It features a large central icon of a red cube with a black outline. Below the icon, the text 'Amazon Elastic File System (EFS)' is displayed. A blue button labeled 'Create file system' is centered at the bottom of the page. Below this button, there is a link 'Getting started guide'.



Select Default VPC

The screenshot shows the 'Create file system' wizard in the AWS EFS console. The first step, 'Step 1: Configure file system access', is selected. A note says: 'An Amazon EFS file system is accessed by EC2 instances running inside one of your VPCs. Instances connect to a file system by using a network interface called a mount target. Each mount target has an IP address, which we assign automatically or you can specify.' Below this is a table header with columns: Availability Zone, Subnet, IP address, and Security groups.

Remove all Security Groups

The screenshot shows the 'Create mount targets' wizard in the AWS EFS console. It lists three availability zones: us-west-2a, us-west-2b, and us-west-2c. For each zone, it shows a dropdown for the subnet and a checkbox for a security group named 'sg-a3a41edb-default'. A tooltip for the security group shows its full name: 'sg-a3a41edb-default'.

Verify that all security groups go deleted

Create mount targets

Instances connect to a file system by using mount targets you create. We recommend creating a mount target in each of your VPC's Availability Zones so that EC2 instances across your VPC can access the file system.

Availability Zone	Subnet	IP address	Security groups
us-west-2a	subnet-13f60e5a (default)	Automatic	Select Security
us-west-2b	subnet-8b9e38ec (default)	Automatic	Select Security
us-west-2c	subnet-19d0f141 (default)	Automatic	

Cancel Next Step

Now add NFSsecurity2 group in all A.Z

Create mount targets

Instances connect to a file system by using mount targets you create. We recommend creating a mount target in each of your VPC's Availability Zones so that EC2 instances across your VPC can access the file system.

Availability Zone	Subnet	IP address	Security groups
us-west-2a	subnet-13f60e5a (default)	Automatic	
us-west-2b	subnet-8b9e38ec (default)	Automatic	
us-west-2c	subnet-19d0f141 (default)	Automatic	

Cancel

Verify that all Security Groups are added.

Click on **Next Step**

Create mount targets

Instances connect to a file system by using mount targets you create. We recommend creating a mount target in each of your VPC's Availability Zones so that EC2 instances across your VPC can access the file system.

	Availability Zone	Subnet	IP address	Security groups
<input checked="" type="checkbox"/>	us-west-2a	subnet-13f60e5a (default)	Automatic	sg-28652152 * - NFSsecurity2
<input checked="" type="checkbox"/>	us-west-2b	subnet-8b9e38ec (default)	Automatic	sg-28652152 * - NFSsecurity2
<input checked="" type="checkbox"/>	us-west-2c	subnet-19d0f141 (default)	Automatic	sg-28652152 * - NFSsecurity2

[Cancel](#) [Next Step](#)

Provide tags

Key → Name

Value → NFShyd1

Drag Down

The screenshot shows the AWS EFS wizard at Step 3: Review and create. In the 'Add tags' section, there is one tag defined: Key 'Name' with Value 'NFShyd1'. In the 'Choose performance mode' section, 'General Purpose (default)' is selected. The browser address bar shows the URL <https://us-west-2.console.aws.amazon.com/efs/home?region=us-west-2#/wizard/2>.

Key	Value	Remove
Name	NFShyd1	X

Choose performance mode

We recommend **General Purpose** performance mode for most file systems. **Max I/O** performance mode is optimized for applications where tens, hundreds, or thousands of EC2 instances are accessing the file system — it scales to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations.

General Purpose (default) Max I/O

Select General Purpose

Click on **Next Step**

We recommend **General Purpose** performance mode for most file systems. Max I/O performance mode is optimized for applications where tens, hundreds, or thousands of EC2 instances are accessing the file system — it scales to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations.

General Purpose (default)
 Max I/O

Enable encryption

If you enable encryption for your file system, all data on your file system will be encrypted at rest. You can select a KMS key from your account to protect your file system, or you can provide the ARN of a key from a different account. Encryption can only be enabled during file system creation. [Learn more](#)

Enable encryption

Cancel **Previous** **Next Step**

NFShyd1 filesystem got selected

Click on **Create File System**

VPC	Zone	Subnet	IP address	Security groups
vpc-89c341ee - default-vpc-oregon (default)	us-west-2a	subnet-13f60e5a (default)	Automatic	sg-28652152 - NFSsecurity2
	us-west-2b	subnet-8b9e38ec (default)	Automatic	sg-28652152 - NFSsecurity2
	us-west-2c	subnet-19d0f141 (default)	Automatic	sg-28652152 - NFSsecurity2

Optional settings

Tags
Performance mode General Purpose (default)
Encrypted No

Create File System

Verify

The screenshot shows the AWS EFS console with a success message: "You have created a file system. You can mount your file system from an EC2 instance with an NFSv4.1 client installed. You can also mount your file system from an on-premises server over an AWS Direct Connect connection. Click [here](#) for EC2 mount instructions, and [here](#) for on-premises mount instructions." Below this, a table lists the newly created file system "NFShyd1". The table includes columns for Name, File system ID, Metered size, Number of mount targets, and Creation date. The "NFShyd1" row has values: Name - NFShyd1, File system ID - fs-53f822fa, Metered size - 6.0 KIB, Number of mount targets - 3, and Creation date - 2017-08-15T06:16:55Z. Under "Other details", the Owner ID is listed as 523251683217 and the Life cycle state is Available. A tag named "Name: NFShyd1" is attached to the file system.

Drag Down

Verify that Life cycle state is **Creating**, it takes few minutes.

The screenshot shows the AWS EFS console for the file system "fs-53f822fa". It displays the DNS name as fs-53f822fa.under.us-west-2.amazonaws.com. Below this, there are links for "Amazon EC2 mount instructions" and "AWS Direct Connect mount instructions". The "Mount targets" section lists three targets in a table. The table columns are VPC, Availability Zone, Subnet, IP address, Mount target ID, Network interface ID, Security groups, and Life cycle state. The targets are associated with the VPC "vpc-89c341ee - default-vpc-oregon (default)". The first target is in "us-west-2c" with subnet "subnet-19d0f141 (default)", IP "172.31.7.82", Mount target ID "fsmt-86a0072f", Network interface ID "eni-7adcc27a", and Life cycle state "Creating". The second target is in "us-west-2a" with subnet "subnet-13f60e5a (default)", IP "172.31.40.66", Mount target ID "fsmt-87a0072e", Network interface ID "eni-e8d884d6", and Life cycle state "Creating". The third target is in "us-west-2b" with subnet "subnet-8b9e38ec (default)", IP "172.31.27.220", Mount target ID "fsmt-98a00731", Network interface ID "eni-eec553c1", and Life cycle state "Creating".

Verify that Life cycle state is Available

The screenshot shows the AWS Elastic File System Management console. The URL in the browser is <https://us-west-2.console.aws.amazon.com/efs/home?region=us-west-2#filesystems/fs-53f822fa>. The page displays the DNS name as fs-53f822fa.efs.us-west-2.amazonaws.com. Below it, there are links for "Amazon EC2 mount instructions" and "AWS Direct Connect mount instructions". The main content is a table titled "Mount targets" with the following data:

VPC	Availability Zone	Subnet	IP address	Mount target ID	Network Interface ID	Security groups	Life cycle state
vpc-89c341ee - default-vpc-oregon (default)	us-west-2c	subnet-19d0f141 (default)	172.31.7.82	fsmt-86a0072f	eni-7adcc27a	sg-28652152 - NFSsecurity2	Available
	us-west-2a	subnet-13f60e5a (default)	172.31.40.66	fsmt-87a0072e	eni-e8d884d6	sg-28652152 - NFSsecurity2	Available
	us-west-2b	subnet-8b9e38ec (default)	172.31.27.220	fsmt-98a00731	eni-eec553c1	sg-28652152 - NFSsecurity2	Available

Step 3. Now launch linux instance & Mount the Amazon EFS File System.

Login to linux instance by using mobaxterm client

```
[2017-08-15 12:01.25] /drives/e/awskeys
[shaikh_pc_mas] > ssh -i "studentorg.pem" ec2-user@ec2-54-213-7-42.us-west-2.compute.amazonaws.com
```

Run the following commands

```
[ec2-user@ip-172-31-45-138 ~]$ sudo su
[root@ip-172-31-45-138 ec2-user]#
[root@ip-172-31-45-138 ec2-user]# yum install nfs-utils
[root@ip-172-31-45-138 ec2-user]#
[root@ip-172-31-45-138 ec2-user]# mkdir /opt/oracledata
[root@ip-172-31-45-138 ec2-user]# mount -t nfs4 fs-53f822fa.efs.us-west-2.amazonaws.com:/ /opt/oracledata
[root@ip-172-31-45-138 ec2-user]#
```

Verify is it mounted

Check the last line

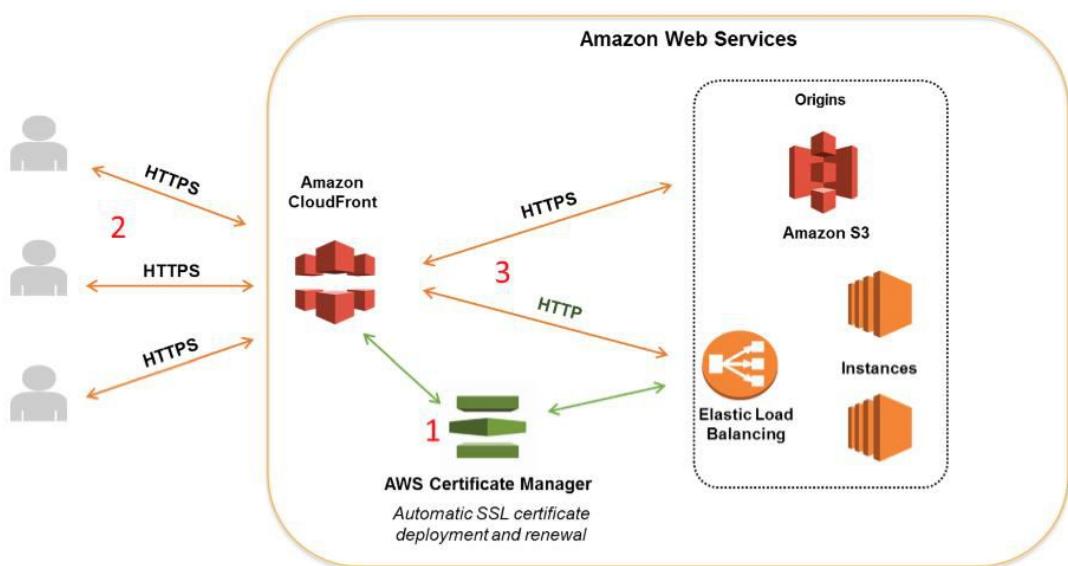
```
proc on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
devtmpfs on /dev type devtmpfs (rw,relatime,size=499756k,nr_inodes=124939,mode=755)
devpts on /dev/pts type devpts (rw,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /dev/shm type tmpfs (rw,relatime)
/dev/xvda1 on / type ext4 (rw,noatime,data=ordered)
devpts on /dev/pts type devpts (rw,relatime,gid=5,mode=620,ptmxmode=000)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
fs-53f822fa.efs.us-west-2.amazonaws.com:/ on /opt/oracledata type nfs4 (rw,relatime,vers=4.0,rsize=1048576,wsize
=1048576,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=172.31.45.138,local_lock=none,addr=172
.31.40.66)
[root@ip-172-31-45-138 ec2-user]#
```

Lab 22: To Configure Amazon CloudFront Service

OBJECTIVE

To configure and use AWS CloudFront Service.

TOPOLOGY



PRE-REQUISITES

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

To configure Cloudfront with following task.

Configure a Website with Amazon S3 bucket by uploading your content

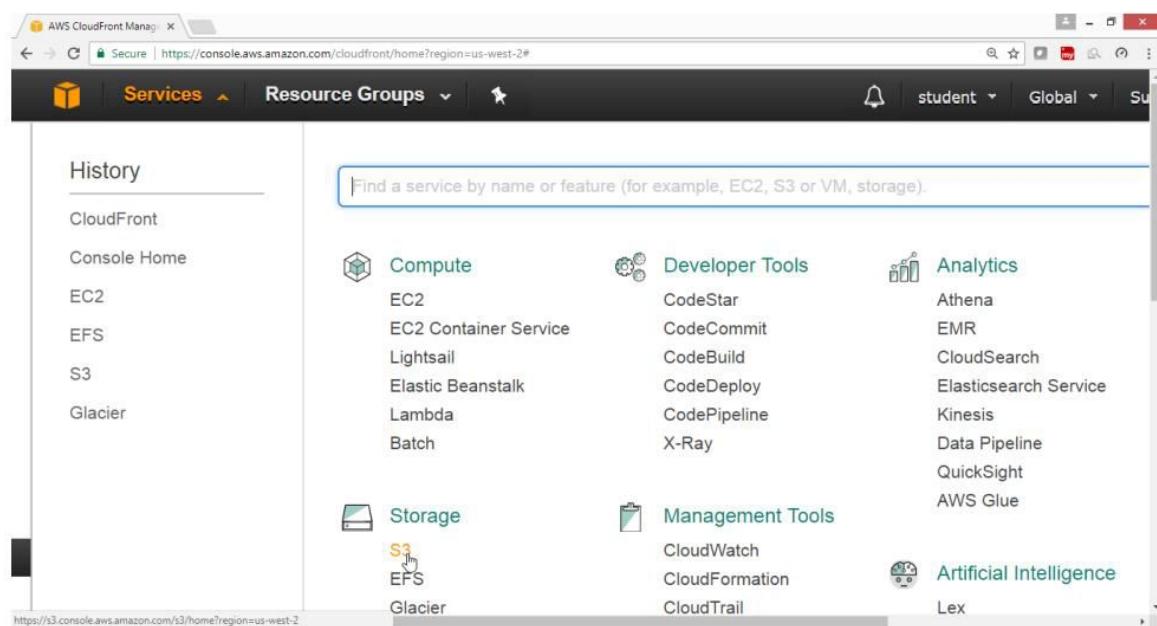
Create a CloudFront Web Distribution

Verify your site by providing cloudfont DNS link

1) Configure a Website with Amazon S3 bucket by uploading your content

Open AWS Console go for **S3** Service

Follow the lab steps of Website Hosting in S3



Check the S3 bucket content

The screenshot shows the AWS S3 Management Console interface. At the top, there are tabs for 'Upload', 'Create Folder', and 'Actions'. A search bar is labeled 'Search by prefix'. Below the search bar, there are buttons for 'Switch to new console', 'None', 'Properties', and 'Transfers'. The main area displays a table of objects in the 'Bucket: www.cloudskillhyd.com'.

	Name	Storage Class	Size
<input type="checkbox"/>	404.html	Standard	6 KB
<input type="checkbox"/>	about-us.html	Standard	5.8 KB
<input type="checkbox"/>	article.html	Standard	5.3 KB
<input type="checkbox"/>	articles.html	Standard	4.8 KB
<input type="checkbox"/>	contact-us.html	Standard	4.7 KB
<input type="checkbox"/>	css	--	--
<input type="checkbox"/>	images	--	--
<input type="checkbox"/>	index.html	Standard	6 KB
<input type="checkbox"/>	js	--	--
<input type="checkbox"/>	sitemap.html	Standard	4.8 KB

To the right of the table, detailed information about the bucket is shown:

- Bucket:** www.cloudskillhyd.com
- Region:** Oregon
- Creation Date:** Tue Aug 15 08:44:43 GMT+530 2017
- Owner:** skmvali999

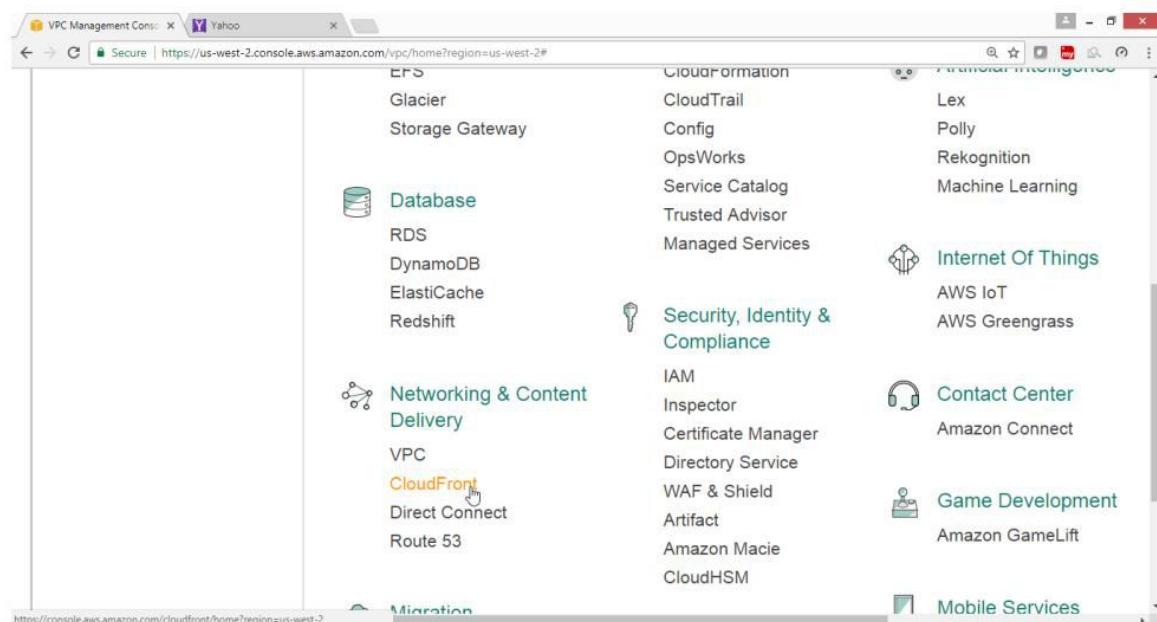
Below this, there are sections for 'Permissions' and 'Static Website Hosting'. Under 'Static Website Hosting', it says: 'You can host your static website entirely on Amazon S3. Once you enable static website hosting for your bucket, all your content is accessible from web browsers via the Amazon S3 website endpoint for your bucket.' The 'Endpoint' link is highlighted with a mouse cursor.

Step-2. Create a CloudFront Web Distribution

Open AWS Console

Select Networking and Content Delivery

Click on **CloudFront** service



Click on **Create Distribution** button

The screenshot shows the AWS CloudFront Management Console. On the left, there's a sidebar with various links like 'Distributions', 'Reports & Analytics', and 'Private Content'. The main area is titled 'CloudFront Distributions' and shows a table with one row. The first column is 'Delivery Method' (Web), the second is 'ID' (E3MBZACTGBE5OL), the third is 'Domain Name' (d2sxq5lo2sebu2.cloudfront.net), and the fourth is 'Comment' (empty) and 'Origin' (www.cfameerpet.com.s3.amazonaws.com). At the top, there's a blue 'Create Distribution' button, which is the focus of the instruction.

Under "Select a delivery method for your content" Wizard

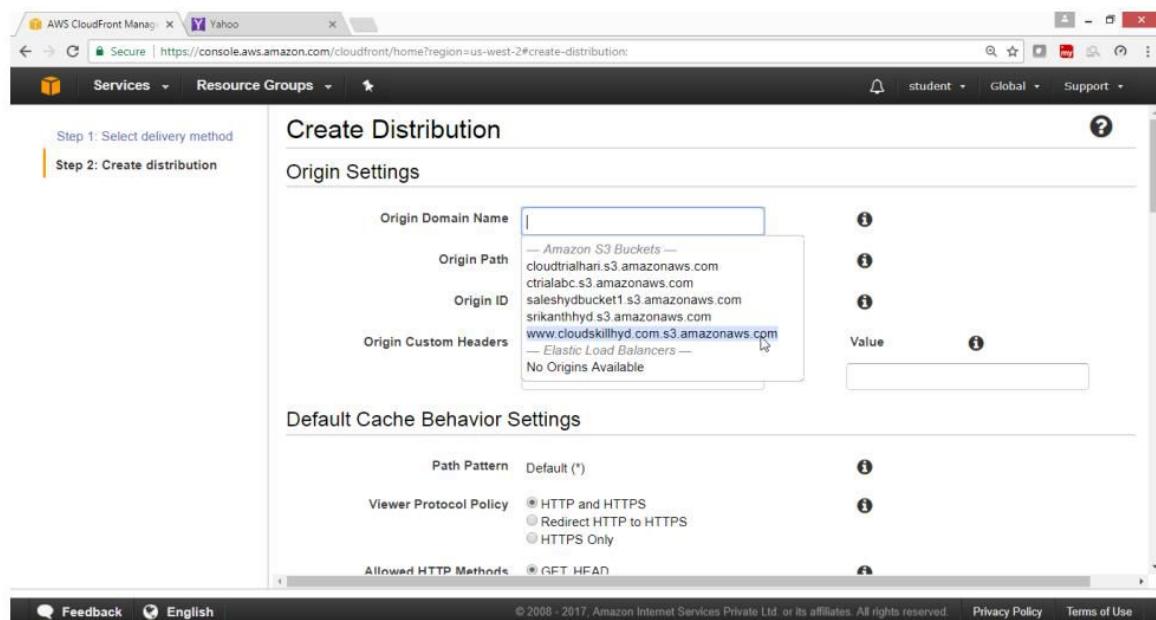
Under Web

Click on **Get Started** button

This screenshot shows the 'Select a delivery method for your content' wizard. It's step 1 of 2, specifically for a 'Web' distribution. The page explains that a web distribution speeds up static and dynamic content. It also notes that files are stored in an origin (Amazon S3 bucket or web server). A large blue 'Get Started' button is prominently displayed at the bottom left of the main content area.

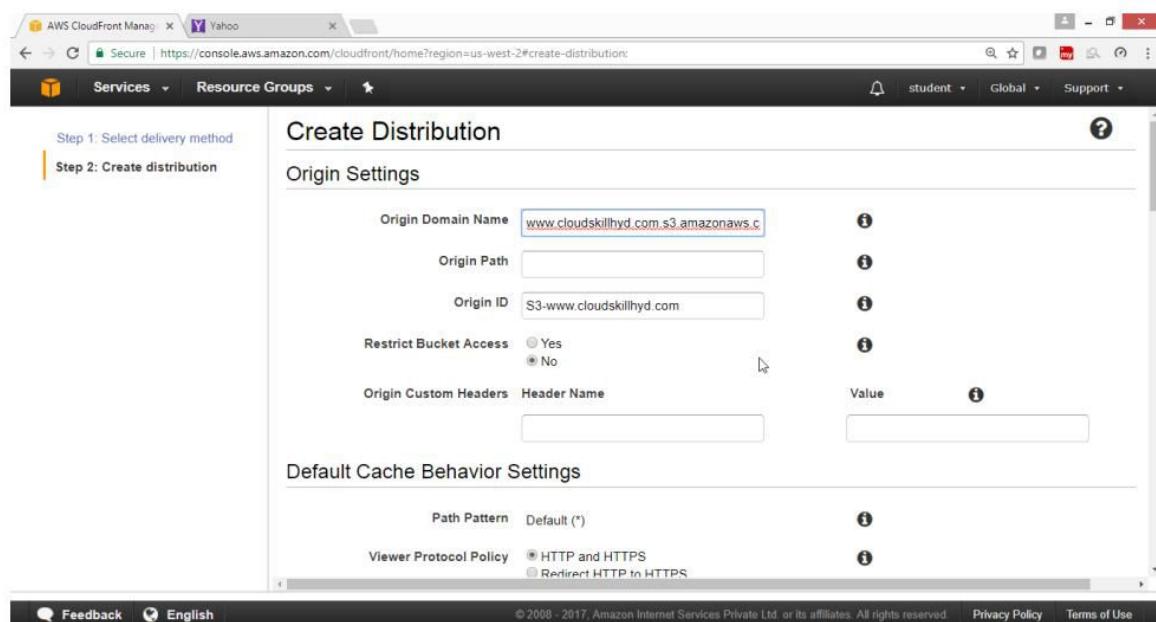
Under Create Distribution

For Origin Domain Name → Drop down → www.cloudskill.com.s3.amazonaws.com



The screenshot shows the 'Create Distribution' wizard on the 'Step 2: Create distribution' page. In the 'Origin Settings' section, the 'Origin Domain Name' dropdown is expanded, displaying a list of available origins. The item 'www.cloudskillhyd.com.s3.amazonaws.com' is highlighted, indicating it has been selected. Other items in the list include 'Amazon S3 Buckets' (such as 'cloudtrialhari.s3.amazonaws.com', 'ctrilabc.s3.amazonaws.com', 'saleshydbucket1.s3.amazonaws.com', 'srikanthhyd.s3.amazonaws.com') and 'Elastic Load Balancers'.

Verify Origin Domain Name got selected



The screenshot shows the 'Create Distribution' wizard on the 'Step 2: Create distribution' page. In the 'Origin Settings' section, the 'Origin Domain Name' field is populated with 'www.cloudskillhyd.com.s3.amazonaws.com'. The 'Origin Path' and 'Origin ID' fields are also filled. The 'Restrict Bucket Access' section shows 'No' selected. The 'Default Cache Behavior Settings' section is partially visible below.

Drag Down

Go for **Distribution Settings**

For **Price Class**

Select **Edge location**

The screenshot shows the 'Distribution Settings' page in the AWS CloudFront Manager. The top navigation bar includes 'Services' (selected), 'Resource Groups', and other global navigation links. The main content area is titled 'Distribution Settings' and displays the following configuration:

- Price Class:** Use All Edge Locations (Best Performance) (selected)
- AWS WAF Web ACL:** None
- Alternate Domain Names (CNAMEs):** (empty input field)
- SSL Certificate:** Default CloudFront Certificate (*.cloudfront.net)
Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as <https://d111111abcdef8.cloudfront.net/logo.jpg>).
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.
- Custom SSL Certificate (example.com)
Choose this option if you want your users to access your content by using an alternate domain name, such as <https://www.example.com/logo.jpg>. You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

At the bottom, there are links for 'Feedback', 'English', 'Privacy Policy', and 'Terms of Use'.

Price Class → Use only Canada and Europe

Distribution Settings

Step 1: Select delivery method
Step 2: Create distribution

Price Class: Use Only US, Canada and Europe

AWS WAF Web ACL: None

Alternate Domain Names (CNAMEs):

SSL Certificate: Default CloudFront Certificate (* cloudfront.net)

Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d11111abcdef0.cloudfront.net/logo.jpg). Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

No certificates available

Request or Import a Certificate with ACM

Drag Down

Click on Create Distribution

Default Root Object:

Logging: On Off

Bucket for Logs:

Log Prefix:

Cookie Logging: On Off

Enable IPv6:

Comment:

Distribution State: Enabled Disabled

Create Distribution

Verify the status

The screenshot shows the AWS CloudFront Management console with the URL <https://console.aws.amazon.com/cloudfront/home?region=us-west-2#distributions>. The left sidebar is collapsed, and the main area displays the 'CloudFront Distributions' page. At the top, there are buttons for 'Create Distribution', 'Distribution Settings', 'Delete', 'Enable', and 'Disable'. Below these are dropdown menus for 'Viewing' (set to 'Any Delivery Method') and 'Any State'. A search bar is also present. The main table lists two distributions:

Delivery Method	ID	Domain Name	Comment	Origin
Web	E3MBZACTGBE5OL	d2sxq5lo2sebu2.cloudfront.net	-	www.cfameerpet.com.s3.amazonaws.com
Web	E1PZW95RSB3Y79	d3hv6v1ag4tvcy.cloudfront.net	-	www.cloudskillhyd.com.s3.amazonaws.com

At the bottom of the page, there is a note: "© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved." and links to "Privacy Policy" and "Terms of Use".

Check column Status

Shows → In Progress

The screenshot shows the same AWS CloudFront Management console interface. The left sidebar is collapsed, and the main area displays the 'CloudFront Distributions' page. The 'Status' column is highlighted in yellow. The table data remains the same as in the previous screenshot.

Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
Web	E3MBZACTGBE5OL	d2sxq5lo2sebu2.cloudfront.net	-	www.cfameerpet.com.s3.amazonaws.com	-	Deployed	Enabled	2017-08-12 11:4
Web	E1PZW95RSB3Y79	d3hv6v1ag4tvcy.cloudfront.net	-	www.cloudskillhyd.com.s3.amazonaws.com	-	In Prog	Enabled	2017-08-15 14:2

At the bottom of the page, there is a note: "© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved." and links to "Privacy Policy" and "Terms of Use".

Wait for status to gen **Enable**

Note : It takes around 15 minutes

The screenshot shows the AWS CloudFront Manager interface. On the left, there's a sidebar with links like 'Distributions', 'Reports & Analytics', 'Cache Statistics', etc. The main area displays a table of distributions. The table has columns: Comment, Origin, CNAMEs, Status, State, and Last Modified. There are two entries:

Comment	Origin	CNAMEs	Status	State	Last Modified
-	www.cfameerpet.com.s3.amazonaws.com	-	Deployed	Enabled	2017-08-12 11:4
-	www.cloudskillhyd.com.s3.amazonaws.com	-	Deployed	Enabled	2017-08-15 14:2

Verify the Site with DNS name "d3hv6v1ag4tvcy.cloudfront.net"

The screenshot shows the 'CloudFront Distributions' page. The sidebar is identical to the previous one. The main area has a 'Create Distribution' button and a table of distributions. The table has columns: Delivery Method, ID, Domain Name, Comment, and Origin. There are two entries:

Delivery Method	ID	Domain Name	Comment	Origin
Web	E3MBZACTGBE5OL	d2sxq5lo2sebu2.cloudfront.net	-	www.cfameerpet.com.s3.amazonaws.com
Web	E1PZW95RSB3Y79	d3hv6v1ag4tvcy.cloudfront.net	-	www.cloudskillhyd.com.s3.amazonaws.com

Verify

Now Open the Browser and type

<http://d3hv6v1ag4tvcy.cloudfront.net/index.html>

The screenshot shows the AWS CloudFront Management Console. On the left, there's a sidebar with 'Services' and 'Resource Groups' dropdowns, and a 'Distributions' section. Below that are sections for 'Reports & Analytics', 'Private Content', and 'How-to Guide'. The main area is titled 'CloudFront Distributions > E1PZW95RSB3Y79'. It has tabs for 'General', 'Origins', 'Behaviors', 'Error Pages', 'Restrictions', 'Invalidations', and 'Tags'. Under 'General', the Distribution ID is E1PZW95RSB3Y79, ARN is am.aws.cloudfront: 523251683217:distribution/E1PZW95RSB3Y79, Log Prefix is -, Delivery Method is Web, Cookie Logging is Off, Distribution Status is InProgress, and Comment is -. Price Class is Use Only US, Canada and Europe. AWS WAF Web ACL is not present. State is Enabled. Alternate Domain Names (CNAMEs) include *.cloudfront.net and d3hv6v1ag4tvcy.cloudfront.net. SSL Certificate is Default CloudFront Certificate (*.cloudfront.net). Domain Name is d3hv6v1ag4tvcy.cloudfront.net. Custom SSL Client Support is -. Supported HTTP Versions are HTTP/2, HTTP/1.1, HTTP/1.0. IPv6 is Enabled. Default Root Object is -. Last Modified is 2017-08-15 14:28 UTC+5:30. Log Bucket is -. At the bottom, there are links for 'Feedback', 'English', 'Privacy Policy', and 'Terms of Use'.

This Website is coming from CloudFront Service

The screenshot shows a website for 'Car Club'. The header includes a navigation menu with links for HOME, ABOUT, ARTICLES, CONTACTS, SITE MAP, Help, and FAQ. The main feature is a large image of a purple sports car. Below the car, there's a search bar labeled 'SEARCH'. On the left, there's a 'Latest News' section with two items: one from 10.08.2010 and another from 03.08.2010. On the right, there's a 'Welcome to Our Club' section with a brief description of the template and a sidebar with a list of bullet points. At the bottom, there's a note about the website template being deliverable in two packages.

MCSE-2012 Full Course

MICROSOFT CERTIFIED SOLUTIONS EXPERT

Practicals in real-time environment. Detailed curriculum with all 5 papers

Duration: 1 Month | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 8.30 to 10.30 • Afternoon: 2.00 to 4.00 • Evening: 7.30 to 9.30

CCNA (v 3.0) Full Course

CISCO CERTIFIED NETWORK ASSOCIATE

Cisco Routers with BSNL/TELCO MUX & Live Channelised E1

Duration: 1 Month | 4 Hrs Per Day (starts on 7th, 15th & 30th of every month)

Batches: Morning: 8.30 to 10.30 • Afternoon: 2.00 to 4.00 • Evening: 7.30 to 9.30

LINUX ADMINISTRATION

COMPLETE RHCE LINUX

Practicals on Live Web Administration + Integration of Windows with Linux/Unix (Samba Server)

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 8.30 • Afternoon: 2.00 • Evening: 7.30

EMERGING TECHNOLOGIES - AN INSIGHT

NETWORKING AND NETWORK SECURITY

Free MCSE & CCNA Exam Practice Questions

EHCE | Ethical Hacking & Countermeasures Expert

Course is mapped to EHCE course from US-Council (www.us-council.com)
(Pre requisite is CCNA / MCSE / LINUX)

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 7.30 or Evening: 7.30

CCNP R&S

CISCO CERTIFIED NETWORK PROFESSIONAL

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 • Afternoon: 2.00 • Evening: 7.00

• Labs on latest routers with IOS version 15.X

Monitoring, Diagnostics & Troubleshooting Tools

• PRTG • Wireshark • SolarWinds, etc.

Exam Practice Challenge Labs

CCIE R&S

CISCO CERTIFIED INTERNETWORK EXPERT

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 • Evening: 6.00

• Individual Rack For Every Student
• Real time scenarios by 20+ years experienced CCIE certified industry expert who has worked on critical projects worldwide.

Written + Lab Exam Focus

FREE Full Scale 8 Hours Exam Lab Included

Unlimited Lab Access For 1 Year

Complete Package for Only

Fees: ₹ 5,900/-

+ 18% GST

**Duration: 3 Months
4 Hrs Per Day**

100% GUARANTEED JOB ASSISTANCE

**Fees: ₹ 9,500/-
+ 18% GST**

~~₹ 10,000/-~~

Introductory Special Offer

**Fees: ₹ 6,500/-
+ 18% GST**

**Fees: ₹ 25,500/-
+ 18% GST**

MICROSOFT EXCHANGE SERVER-2013

Duration: 2 Weeks | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

**Fees: ₹ 2,500/-
+ 18% GST**

MICROSOFT PRIVATE CLOUD

(Microsoft Certified Solutions Expert [MCSE] Private Cloud

Duration: 2 Weeks | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

**Fees: 4,500/-
+ 18% GST**

ADVANCED LINUX

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 8.30 or Evening: 7.30

**Fees: ₹ 3,000/-
+ 18% GST**

CCNA SECURITY

(Pre requisite is CCNA R&S)

CISCO CERTIFIED NETWORK ASSOCIATE - SECURITY

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 or Evening: 6.00

**Fees: ₹ 5,500/-
+ 18% GST**

CCNP SECURITY

(Pre requisite is CCNA sSECURITY AT ZOOM)

CISCO CERTIFIED NETWORK PROFESSIONAL - SECURITY

Duration: 2 Weeks | 4 Hrs Per Day (starts on 30th of every month)

Batches: Morning: 7.30 or Evening: 6.00

**Fees: ₹ 7,500/-
+ 18% GST**

CCIE SECURITY

(Pre requisite is CCNA & CCNP Security at ZOOM)

CISCO CERTIFIED INTERNETWORK - SECURITY

Duration: 1 Month | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

**Fees: ₹ 15,500/-
+ 18% GST**

VMware vSphere

(Pre requisite is MCSE)

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 and Evening: 7.30

**Fees: ₹ 5,950/-
+ 18% GST**

VMware vCloud

(Pre requisite is VMware vSphere)

Duration: 1 Week | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 9.30 to 11.30

**Fees: ₹ 2,500/-
+ 18% GST**

CHECKPOINT FIREWALL

Duration: 2 Weeks | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

**Fees: ₹ 5,500/-
+ 18% GST**

CISCO ASA FIREWALL+CISCO IPS

(CCNA Security + CCNP Security)

Duration: 2 Weeks | (Starts on 15th of every month)

Batches: Morning: 7.30 am or Evening 7.30 pm

**Fees: ₹ 10,500/-
+ 18% GST**

We also offer the following courses (Contact the Counselors for the next available batch)

- › **CCNA Voice** @ ₹7,500/-
- › **CCNP Voice** @ ₹9,500/-
- › **CCIE Collaboration** @ ₹15,500/-
- › **CCNA Data Center** @ ₹7,500/-
- › **CCNP Data Center** @ ₹9,500/-
- › **CCIE Data Center** @ ₹15,500/-
- › **IPv6 Migration** @ ₹5,500/-

FACULTY

- › All Senior Engineers of Zoom working on Live projects
- › Training Engineers of British Army, CISCO, CMC, GE, BSNL, Tata Teleservices and Several Corporates etc for 18 Years.

FREE Training

Zoom Technologies offers a number of free resources for the professional development of network engineers.

Register on our website to get access to the video recordings of live sessions on:

- **MCSE – Windows Server 2012**
 - **Cisco – CCNA**
 - **Cisco – CCNP**
 - **Cisco – CCIE**
 - **Exchange Server 2013**
 - **Linux**
 - **Advanced Linux**
 - **Ethical Hacking and Countermeasure Expert (www.us-council.com)**
- All Tracks (R & S, Security and Voice)
All Flavors

Find us at: www.zoomgroup.com

Like us on Facebook and get access to free online webinars as well as special offers and discounts.
<https://www.facebook.com/ZoomTechnolgies>

Online Training

Online Training at Zoom is a cost effective method of learning new networking skills from the convenience of your home or workplace.

Taking an online training course has many advantages for everyone (Freshers / Working Professionals). Zoom offers online training for the highly coveted CCNA, CCNP and CCIE courses as well as MCSE, Linux, VMware, Ethical Hacking and Firewalls, IPv6 with more courses planned for the near future. These are live instructor led courses, using Cisco WebEX. Check out our online course offerings at: http://zoomgroup.com/online_course

Job Opportunities

There is a high demand for network and security professionals at all times. Apart from job opportunities in India and the Middle East, network and security administrators are also sought-after in the US and Europe.

If you do not have the right skills, then get them now! Choose the experts in network and security training, an organization which has already trained over one hundred thousand engineers.

For the latest job openings in networking and security, register and upload your resume on: <http://zoomgroup.com/careers> or visit zoom to choose job offering from several multinational companies.

ABOUT US

ZOOM Technologies India Pvt. Ltd. is a pioneering leader in network and security training, having trained over two hundred thousand engineers over the last two decades.

We offer a world class learning environment, with state-of-the-art labs which are fully equipped with high-end routers, firewalls, servers and switches. All our courses are hands-on so you'll get much needed practical experience.

The difference between us and the competition can be summed up in one simple sentence. Our instructors are real-time network professionals who also teach.

Zoom has designed, developed and provided network and security solutions as well as training to all the big names in the Indian industry, for the public sector as well as corporate leaders. Some of our clients are:

- TATA
- BSNL
- VSNL
- Indian Railways
- National Police Academy
- Air Force Academy
- IPCL - Reliance Corporation
- CMC
- British Army

No other training institute can boast of a customer base like this. This is the reason for the resounding success of our networking courses. If you do not have the right skills, then get them now. Come, join the experts!



TELANGANA

Hyderabad

Ameerpet

203 to 206, 2nd Floor,
HUDA Maitrivanam.
Tel: +91-40-2374 5252 / 2374 5259
eMail: ameerpet@zoomgroup.com

Banjara Hills

Above HDFC Bank, Road No. 12.
Tel: +91-40-2339 4150 / 2330 3160
eMail: banjara@zoomgroup.com



ANDHRA PRADESH

Vijayawada

64-9-2, Second Floor,
SBH Building, Patamata,
NTR Circle.
Mobile: +91 733 744 5253
733 744 5254
eMail: vijayawada@zoomgroup.com



GUJARAT

Surat

40/A, 3rd Floor,
River Front Building,
Opp. Dutch Garden,
Nanpura.
Mobile: +91 964 233 8901
eMail: surat@zoomgroup.com