

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 instance3
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

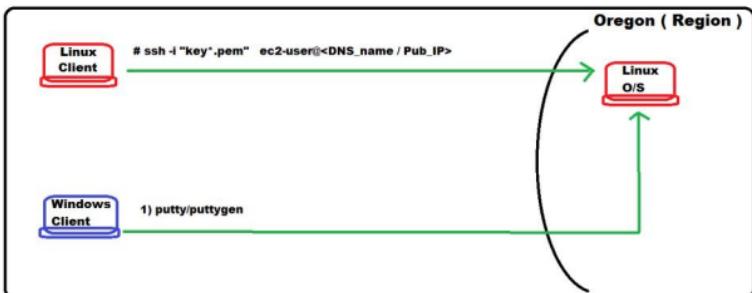
Lab 15: To Configure an Amazon Relational Database Service	337
Lab 16: To Configure Amazon DynamoDB.....	360
Lab 17: To Configure Amazon CloudFormation.....	377
Lab 18: To Configure Amazon Simple E-Mail Service (SES).....	393
Lab 19: To Configure Amazon Simple QUEUE Service SQS.....	408
Lab 20: To Configure 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

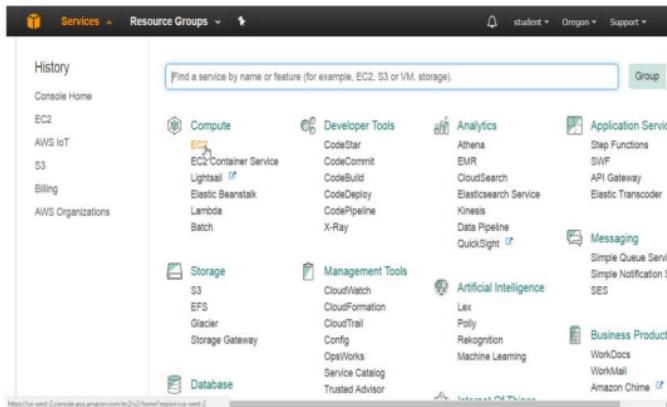
Start/stop/terminate instance

1. To Launch Amazon Linux instance in default VPC

Open the Amazon EC2 console

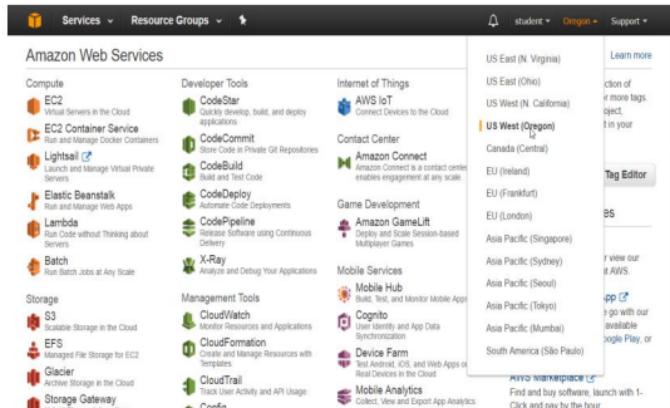
Select **Compute**

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 links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, and Bundle Tasks. The main panel is titled "Service Health". It shows "Service Status" for "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"). At the bottom of the main panel is a link to "Service Health Dashboard". To the right, there's a section titled "Scheduled Events" with the message "No events".

From the "**EC2 Dashboard**" panel

Select Instance

Click on "**Launch Instance**" button

The screenshot shows the AWS EC2 Dashboard. The sidebar is identical to the previous one. The main panel has a large "Launch Instance" button at the top. Below it is a search bar and a table listing two instances: "linuxvma" and "linuxvmb". The table columns include Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Both instances are currently in a "shutting down" state. At the bottom of the main panel, there's a "Description" tab showing details for the selected instances: "i-04ca59221f3ac80ba" and "i-05b8f1f94d4924dd". There are also tabs for "Status Checks", "Monitoring", and "Tags". At the very bottom of the page, there are links for "Feedback", "English", and other AWS services.

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 Management Console interface for selecting an AMI. 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 1 is highlighted: 'Step 1: Choose an Amazon Machine Image (AMI)'. A sub-header states: '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.' The main content area is titled 'Quick Start' and lists several AMI options:

- Amazon Linux**: Free tier eligible. Description: '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.' It has a 'Select' button and '64-bit' link.
- Red Hat Enterprise Linux 7.3 (HVM)**: Free tier eligible. Description: 'Red Hat Enterprise Linux version 7.3 (HVM). EBS General Purpose (SSD) Volume Type' It has a 'Select' button and '64-bit' link.

At the bottom of the page, there are links for 'Feedback', 'English', '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 EC2 instance selection interface. At the top, there are tabs for Services, Resource Groups, and a navigation bar with student, Oregon, Support, and other links. Below the tabs, a breadcrumb trail shows the current step: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. A sub-header "Step 2: Choose an Instance Type" is displayed. A descriptive text explains that Amazon EC2 provides a wide selection of instance types optimized to fit different use cases, mentioning CPU, memory, storage, and networking capacity, and encouraging users to choose the appropriate mix of resources for their applications. A link to learn more about instance types and how they can meet your computing needs is provided. A filter bar at the top of the table allows filtering by instance type, generation, and columns. The main area displays a table of instance types:

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 <small>(Free tier eligible)</small>	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

At the bottom of the table, there are buttons for Cancel, Previous, Review and Launch (which is highlighted in blue), and Next: Configure Instance Details. The footer includes links for Feedback, English, and various AWS terms and policies.

On "Configure Instance Details", page

Leave all values as default

Click on "Next: Add storage" button

Step 3: Configure Instance Details

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

Number of instances: 1 Launch into Auto Scaling Group ⓘ

Purchasing option: Request Spot instances

Network: vpc-0fc34f6e | default-vpc-oregon (default) Create new VPC

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

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

IAM role: None Create new IAM role

Shutdown behavior: Stop

Enable termination protection: Protect against accidental termination

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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-0ce0f7735518cbdd	8	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Below the table is a button labeled "Add New Volume". A callout box highlights the "Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and terms of use." At the bottom right, there are buttons for "Cancel", "Previous", "Review and Launch" (which is highlighted in blue), and "Next: Add Tags".

On "Add Tags", page

Provide following values

Key → Name

Value → linuxvm

Click on "Next: Configure Security Group" button

The screenshot shows the AWS EC2 instance creation wizard at Step 5: Add Tags. The navigation bar includes Services, Resource Groups, student, Oregon, Support, and tabs for Choose All, Choose Instance Type, Configure Instance, Add Storage, Add Tags (highlighted in orange), Configure Security Group, and Review. The main area shows a table for adding tags. A single tag is present with Key 'Name' and Value 'linuxvm'. Below the table is a button 'Add another tag' with the note '(Up to 50 tags maximum)'. At the bottom are 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Configure Security Group'.

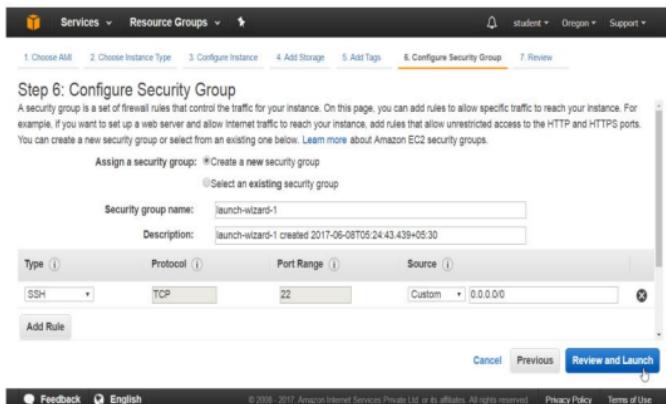
On “Configure Security Group” page

Select → Create a new security group

Leave all values as default.

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

Click “Review and Launch” button



On "Review Instance Launch", page

Leave all values as default.

Verify the summary, then drag down

The screenshot shows the AWS Lambda 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 highlighted. Below the tabs, the heading is "Step 7: Review Instance Launch". A note 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." A warning message in a yellow box says: "⚠ 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 "AMI Details" section shows "Amazon Linux AMI 2017.03.0 (HVM), SSD Volume Type - ami-4836a428". The "Instance Type" section shows "t2.micro" selected. The "Security Groups" section shows "launch-wizard-1" selected. At the bottom right, there are "Cancel", "Previous", and "Launch" buttons. The "Launch" button is highlighted with a blue border.

Verify the summary

Click on **Launch** button

The screenshot shows the AWS Lambda Step 7: Review Instance Launch page. The interface is identical to the previous one, but the "Launch" button at the bottom right is now highlighted with a blue border, indicating it is the next step to be clicked.

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

Select "Create a new key pair"

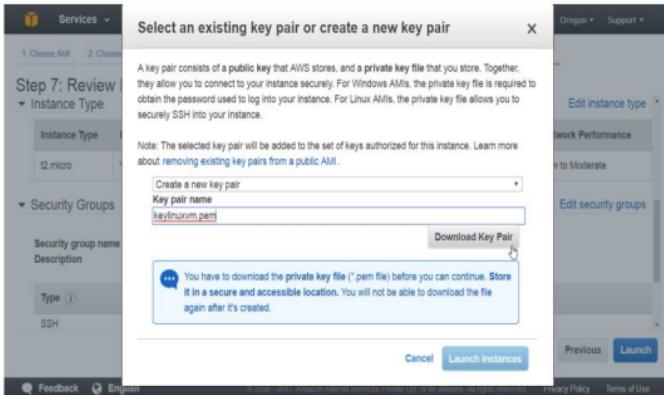
Enter Key pair name → keylinuxvm.pem

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 user profile (student, Oregon, Support). Below the navigation bar, the title "Launch Status" is displayed. A note below the title states: "instances will start immediately and continue to accrue until you stop or terminate your instances." A link "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." is provided. Below this, there is a section titled "Here are some helpful resources to get you started" with 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, there is a section titled "While your instances are launching you can also" with links to "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 of the page, there is a blue button labeled "View Instances". The footer of the page includes links for Feedback, English, and various AWS terms and policies.

On EC2 Dashboard panel

Click on Instances,

Select instances

Check instance status → running

The screenshot shows the AWS EC2 Dashboard with the 'Instances' section selected. A single instance named 'linuxvm' is listed. The instance details are as follows:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
linuxvm	i-0dad392c31958bef6	t2.micro	us-west-2b	running	Initing	None

To check instance details like

Description, Status check, Monitoring, Tags

The screenshot shows the AWS EC2 Dashboard with the 'Instances' section selected. An instance named 'linuxvm' is selected, and its details are displayed. The 'Description' tab is active, showing the instance ID and public DNS.

Instance Details:

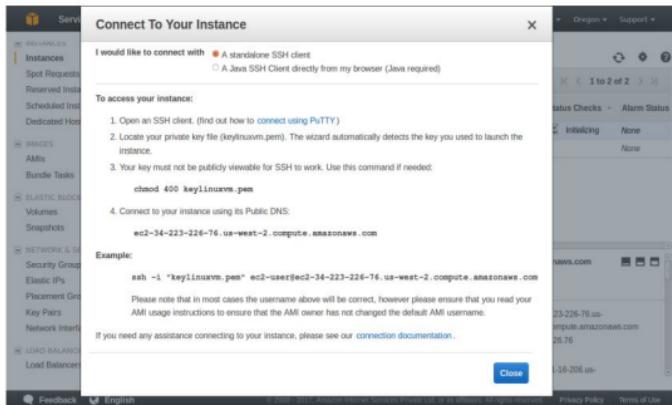
Instance ID	Public DNS
i-0dad392c31958bef6 (linuxvm)	ec2-54-149-138-51.us-west-2.compute.amazonaws.com

Below the tabs, detailed information is shown for the instance:

Instance state	Instance type	Public DNS (IPv4)	IPv4 Public IP
running	t2.micro	ec2-54-149-138-51.us-west-2.compute.amazonaws.com	54.149.138.51
		IPv6 IPs	-
		Private DNS	p-172-31-23-254.us-

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

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



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

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

eg : keylinuxvmm.pem

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

The screenshot shows a terminal window with the following content:

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

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

To know current user in linux

```
$ whoami
```

To switch to root user in linux

```
$ sudo su
```

Verify (root user)

```
# whoami
```

To logout

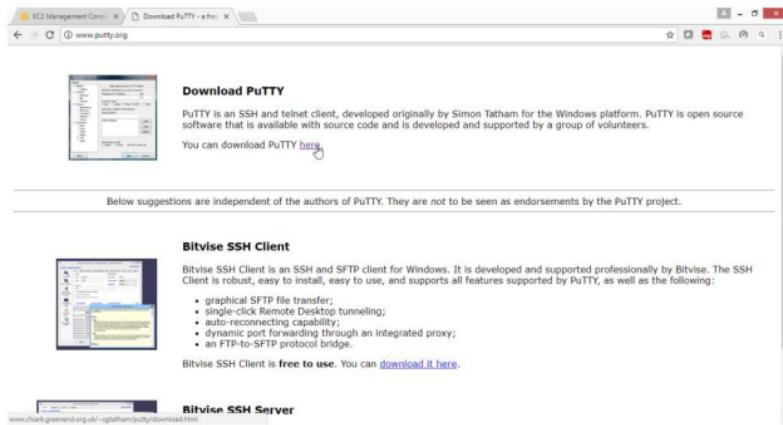
```
# exit
```

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

I

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

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



The screenshot shows a web browser window with the URL www.putty.org. The main content is titled "Download PuTTY". It describes PuTTY 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 volunteers. A link to download Putty is provided. Below the main content, 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, "Bitvise SSH Client", is shown with its own description and download link.

Download PuTTY

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

You can download PuTTY [here](#).

Bitvise SSH Client

Bitvise SSH Client is an SSH and SFTP client for Windows. It is developed and supported professionally by Bitvise. The SSH Client is robust, easy to install, easy to use, and supports all features supported by PuTTY, as well as the following:

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

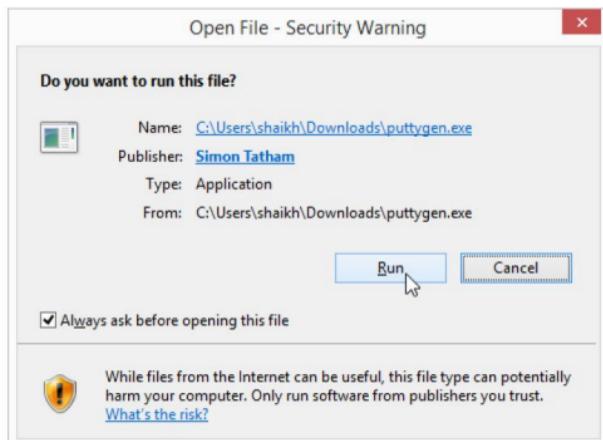
Bitvise SSH Client is **free to use**. You can [download it here](#).



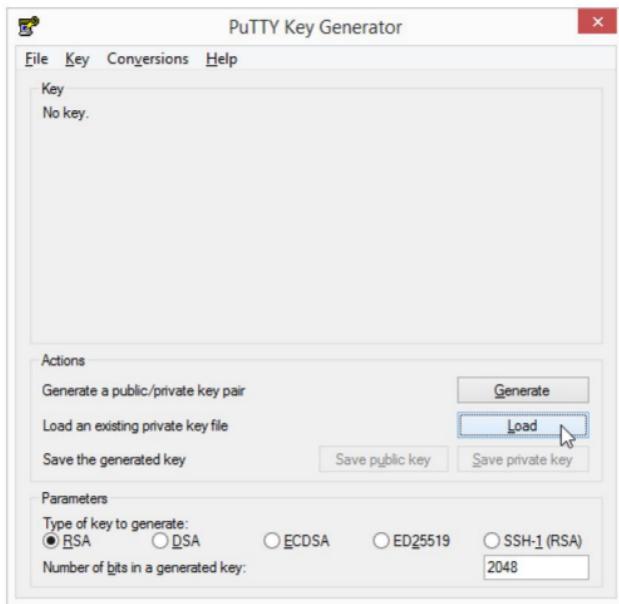
Note: Because putty cannot understand .pem file format, so use puttygen.exe to converting *.pem file into *.ppk format

Click on puttygen.exe file in windows operating system

Click on Run



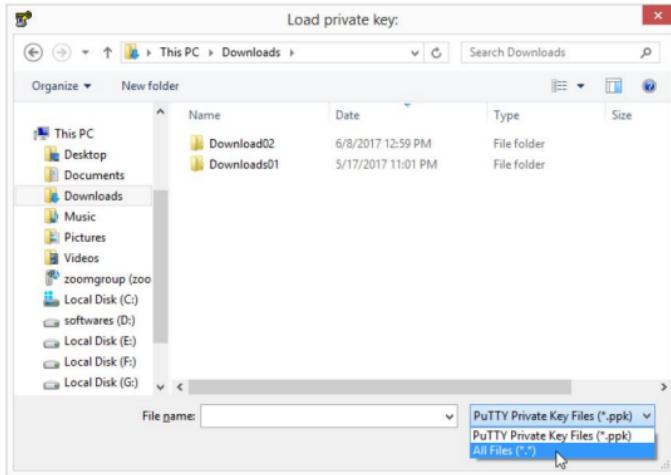
Click on **Load** button



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

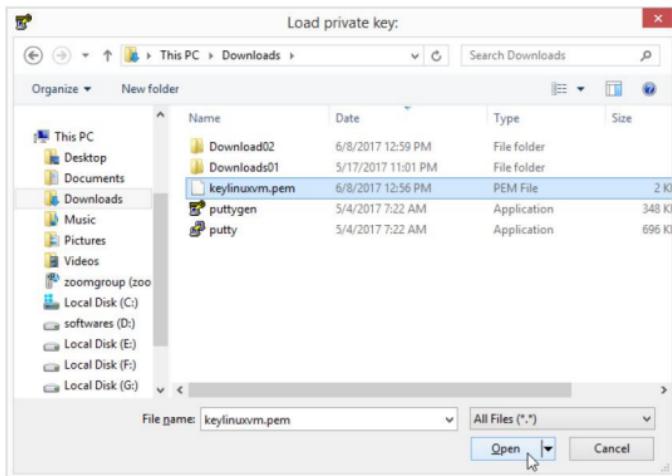
So to locate your .pem file

On file names Select →All files (*.*)

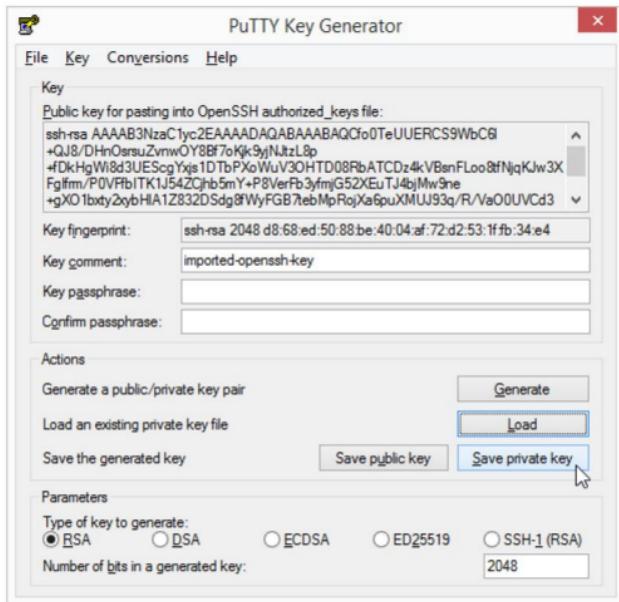


Locate keylinuxvm.pem in your folder

Click on open

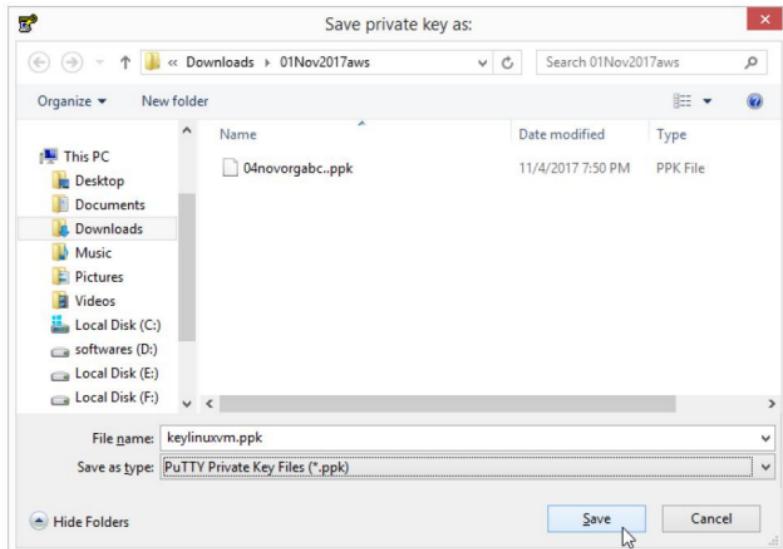


Click on "Save private key" button



Save the file → keylinuxvm.ppk

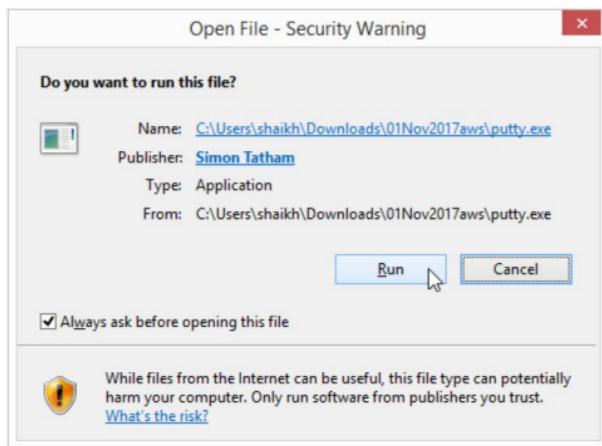
Click on Save button



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

Run putty.exe

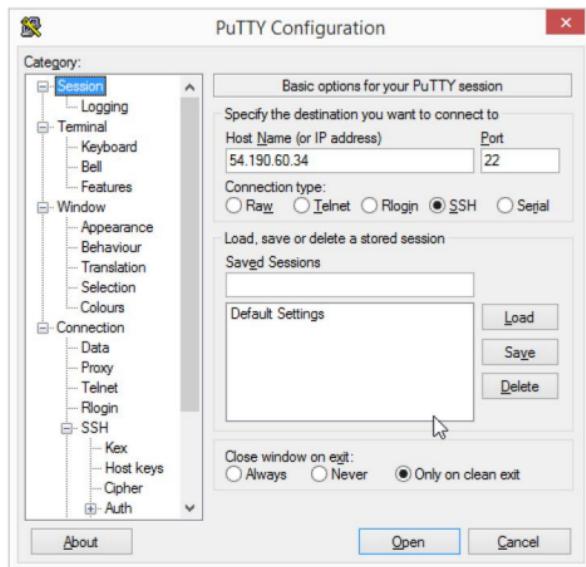
Click on Run



On **Category** page provide following values

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

Port → 22

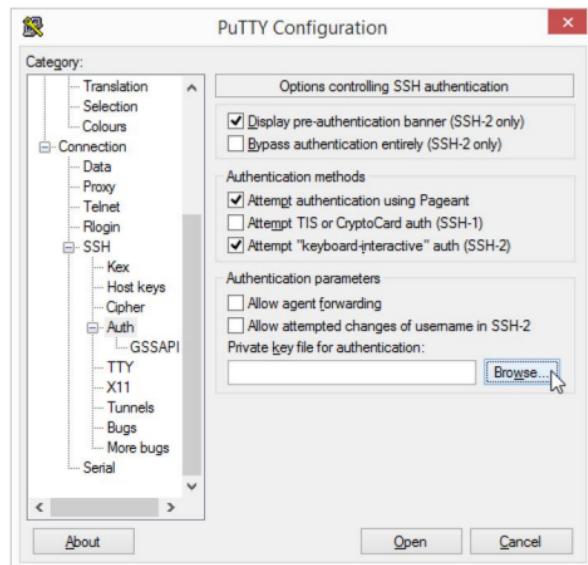


Under Connection expand

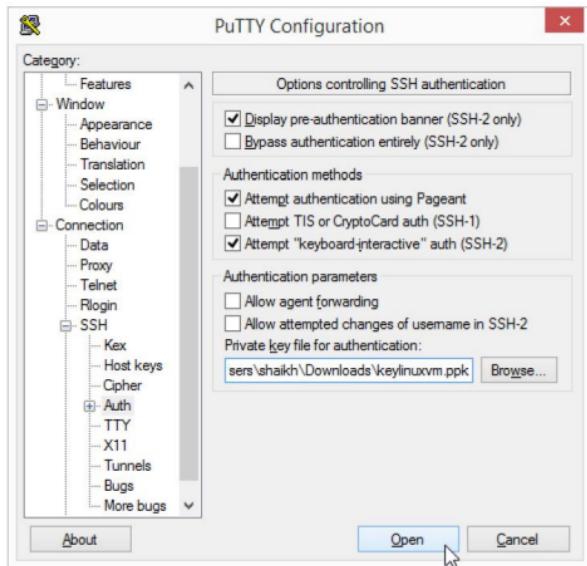
Click on SSH → Auth

Select Browse button

Provide the path of *.ppk file



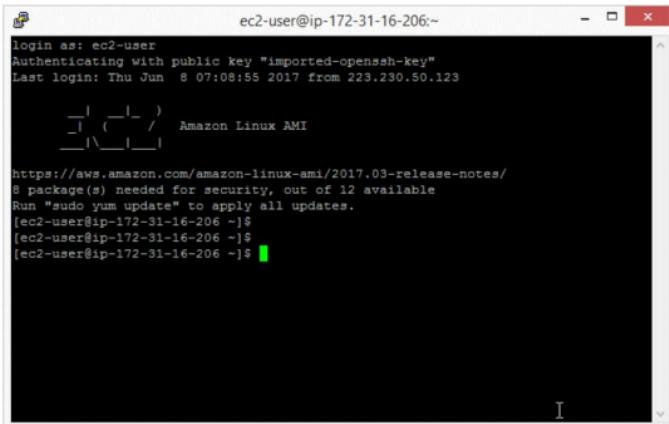
Click on Open button



Verify

Putty login screen is for linux

Provide user name **ec2-user**



The screenshot shows a Windows-style terminal window titled "Putty". The title bar displays "ec2-user@ip-172-31-16-206:~". The terminal content 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 ~]$ _|_(_|_) / Amazon Linux AMI
[ec2-user@ip-172-31-16-206 ~]$ https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
[ec2-user@ip-172-31-16-206 ~]$ 8 package(s) needed for security, out of 12 available
[ec2-user@ip-172-31-16-206 ~]$ Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-16-206 ~]$ [ec2-user@ip-172-31-16-206 ~]$ [ec2-user@ip-172-31-16-206 ~]$
```

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

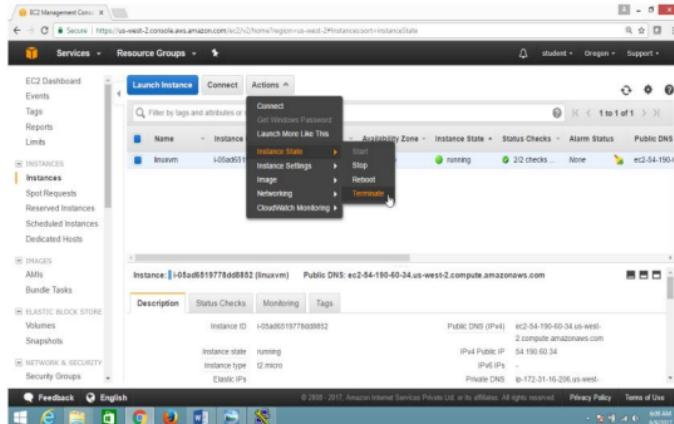
To start/stop/terminate instance

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,

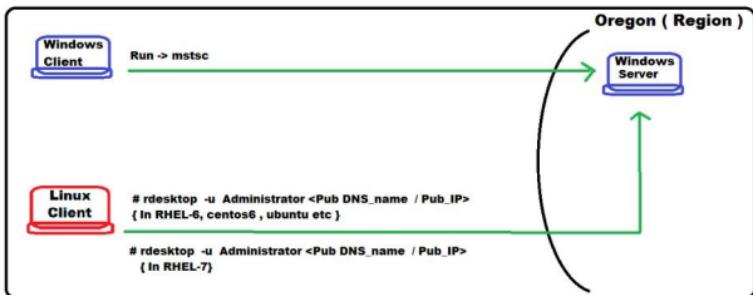
Otherwise it will be charged if the limit is over after free tier usage.

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

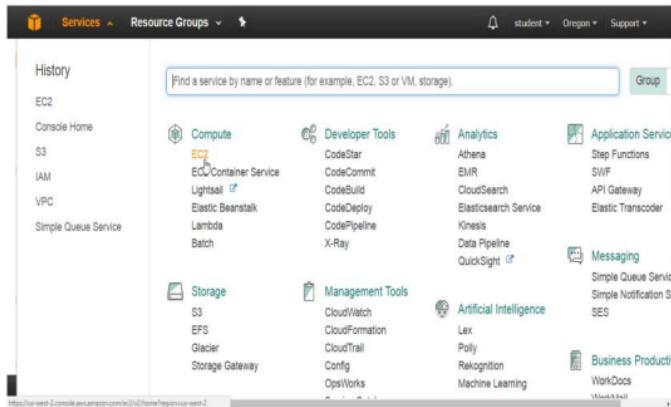
Start/stop/terminate instance

1. To Launch Windows instance in default VPC

Open the Amazon EC2 console

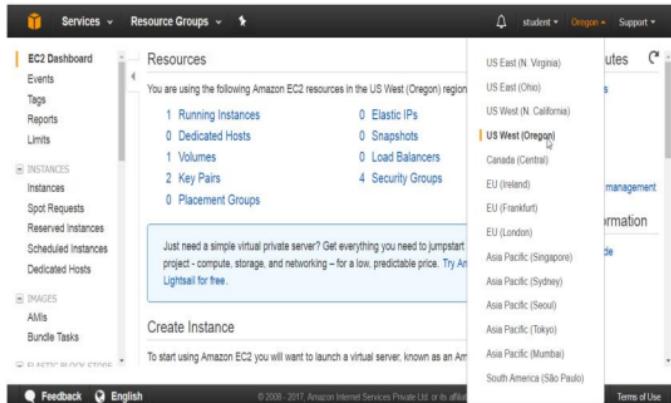
Select **Compute**

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. In the left sidebar, under the "Service Health" section, it says "This service is operating normally". Under "Availability Zone Status:", there are three entries: "us-west-2a" (operating normally), "us-west-2b" (operating normally), and "us-west-2c" (operating normally). To the right, there are promotional cards for Barracuda NextGen Firewall F-Series - PAYG and VM-Series Next-Generation Firewall Bundle 2.

From the “EC2 Dashboard” panel

Select Instance

Click on “Launch Instance” button

The screenshot shows the AWS EC2 Dashboard with the "Launch Instance" button highlighted. Below the search bar, a table lists an instance: "linuxvm" (Instance ID: i-05ad6519778dd8852, Instance Type: t2.micro, Availability Zone: us-west-2b, State: running). At the bottom, there are tabs for "Description", "Status Checks", "Monitoring", and "Tags".

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

Select “Quick start”

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

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

Step 1: Choose an Amazon Machine Image (AMI)

Image	Name	Description	Select	64-bit
Windows	Microsoft Windows Server 2012 with SQL Server Standard - ami-dd914bd	Microsoft Windows Server 2012 Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Standard edition [English] Root device type: ebs Virtualization type: hvm	Select	64-bit
Windows	Microsoft Windows Server 2008 R2 Base - ami-0381e463	Microsoft Windows 2008 R2 SP1 Datacenter edition, 64-bit architecture, [English] Root device type: ebs Virtualization type: hvm	Select	64-bit
Windows	Microsoft Windows Server 2008 R2 with SQL Server Express and IIS - ami-3483e654	Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft Root device type: ebs Virtualization type: hvm	Select	64-bit

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 "Step 2: Choose an Instance Type" page. At the top, there are tabs: 1. Choose AMI, 2. Choose Instance Type (which is selected), 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the tabs, there is a filter section with "Filter by: All instance types" and "Current generation". A note says "Currently selected: t2.micro (Variable ECUs, 1 vCPU, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)". There is a table with columns: Family, Type, vCPUs, Memory (GiB), Instance Storage (GiB), EBS-Optimized Available, Network Performance, and IPv6 Support. The table contains four rows:

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

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

On “Configure Instance Details” page

Leave all values as default

Click on “Next : Add storage” button

The screenshot shows the "Step 3: Configure Instance Details" page. At the top, there are tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance (which is selected), 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the tabs, there is a heading "Step 3: Configure Instance Details" with a sub-instruction: "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." There are several configuration fields:

- Number of Instances:** 1 Launch into Auto Scaling Group
- Purchasing option:** Request Spot instances
- Network:** vpc-89c341ee | default-vpc-oregon (default) Create new VPC
- Subnet:** No preference (default subnet in any Availability Zone) Create new subnet
- Auto-assign Public IP:** Use subnet setting (Enable)
- Domain join directory:** None Create new directory

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

On “Add Storage”, page

Leave all values as default

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

The screenshot shows the 'Add Storage' step 4 configuration page. At the top, there are tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (which is highlighted), 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the tabs, the heading 'Step 4: Add Storage' is displayed. A note states: '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.' The main configuration table has the following columns: Volume Type, Device, Snapshot, Size (GiB), Volume Type, IOPS, Throughput (MB/s), Delete on Termination, and Encrypted. One row is shown for the 'Root' volume: /dev/sda1, snap-05c5aa21237b4e6c8, 30, General Purpose SSD, 100, 1000, N/A, Not Deleted, and Not Encrypted. There is a 'Add New Volume' button below the table. A note at the bottom left says: '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, there are buttons for Cancel, Previous, Review and Launch (which is highlighted in blue), and Next: Add Tags.

On "Add Tags" page

Provide following values

Key → Name

Value → winserver

Click on "Next: Configure Security Group" button

The screenshot shows the AWS Step 5: Add Tags configuration page. At the top, there are tabs for 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (which is highlighted in orange), 6. Configure Security Group, and 7. Review. Below the tabs, there is a section titled "Step 5: Add Tags". It contains a note: "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." There is 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)". In the "Value" column, the word "winserver" is typed. To the right of the table, there are two buttons: "Instances" and "Volumes", each with a question mark icon. Below the table, there is a button labeled "Add another tag" with the note "(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 is also highlighted in blue). There is also a feedback link, a language selection for English, and copyright information from 2008.

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

Step 6: Configure Security Group

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

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

Security group name:

Description:

Type	Protocol	Port Range	Source
RDP	TCP	3389	Custom 0.0.0.0

Add Rule

Cancel Previous Review and Launch

On "Review Instance Launch", page

Leave all values as default.

Verify the summary, then drag down

Step 7: Review Instance Launch

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

⚠ 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](#)

AMI Details

Microsoft Windows Server 2008 R2 Base - ami-0381e463

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

Free tier Root Device Type: ebs Virtualization type: hvm

[Edit AMI](#)

[Cancel](#) [Previous](#) **Launch**

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

Verify the summary

Click on **Launch** button

Step 7: Review Instance Launch

Security Groups

Type	Protocol	Port Range	Source
RDP	TCP	3389	0.0.0.0/0

Instance Details

[Edit instance details](#)

Storage

[Edit storage](#)

Tags

[Edit tags](#)

[Cancel](#) [Previous](#) **Launch**

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

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

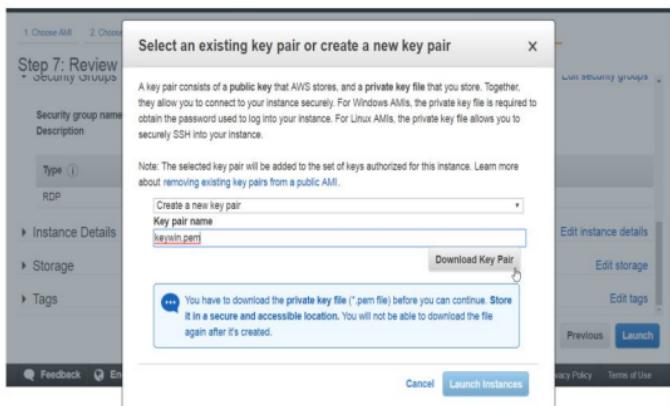
Select "Create a new key pair"

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”

The screenshot shows the AWS Step 7: Review screen. On the left, there's a sidebar with "Step 7: Review" and a "Security Groups" section. The main area displays a modal dialog titled "Select an existing key pair or create a new key pair". Inside the dialog, there's a note about key pairs, a dropdown menu set to "Create a new key pair", a text input field for "Key pair name" containing "keywin.pem", a "Download Key Pair" button, and a message box stating: "You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created." At the bottom of the dialog are "Cancel" and "Launch Instances" buttons.

On **Launch Status** page, go to right bottom corner

Click “View instances” button

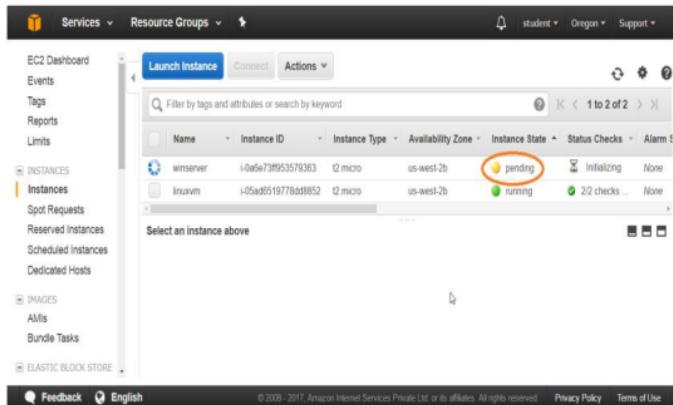
The screenshot shows the AWS Launch Status page. It has a header with "Services", "Resource Groups", and user information. Below the header, there's a section titled "Launch Status" with a note about instances starting immediately. It includes a "View Instances" link and a "Help" section with links to EC2 User Guide and Discussion Forum. Further down, there's a section for launching instances with links to status check alarms and EBS volumes, along with a "Manage security groups" link. At the bottom right of the page is a prominent blue "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 options like Services, Resource Groups, EC2 Dashboard, Events, Tags, Reports, Limits, Instances (which is selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, and Bundle Tasks. Below the sidebar is a search bar and a table of instances. The table has columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. There are two rows: one for 'winserver' (pending) and one for 'Inuvm' (running). A yellow circle highlights the 'pending' status of the first instance. At the bottom of the dashboard, there are links for Feedback, English, Privacy Policy, and Terms of Use.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
winserver	i-0f6e73ff953579363	t2.micro	us-west-2b	pending	Initializing	None
Inuvm	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, 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, 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 rows are listed: "Inuxvm" and "winserver". Both instances are in the "running" state, indicated by green dots. The "winserver" row has a red circle around its "running" status. Below the table, it says "Instance: i-0a6e73f953579363 (winserver) Public DNS: ec2-54-214-137-73.us-west-2.compute.amazonaws.com". At the bottom, there are tabs for Description, Status Checks, Monitoring, and Tags, with "Description" being the active tab.

To check instance details like

Description, Status check, Monitoring, Tags

This screenshot is identical to the one above, showing the AWS EC2 Instances page. The "Description" tab is now highlighted with a red circle. The rest of the interface is the same, showing the two instances and their details.

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

Open Ec2 Dashboard Console

Go to instance

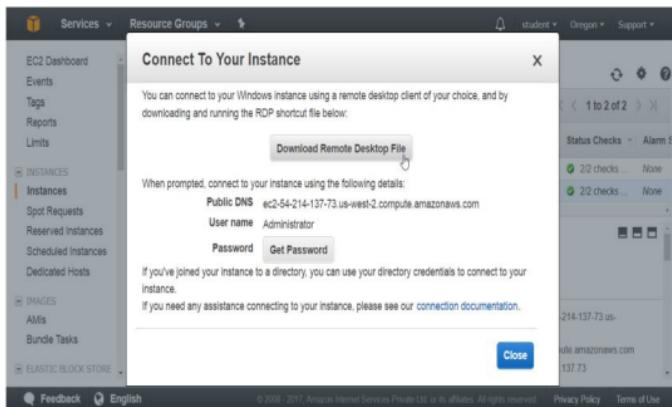
Select the instance you want to connect

Click **Connect** button

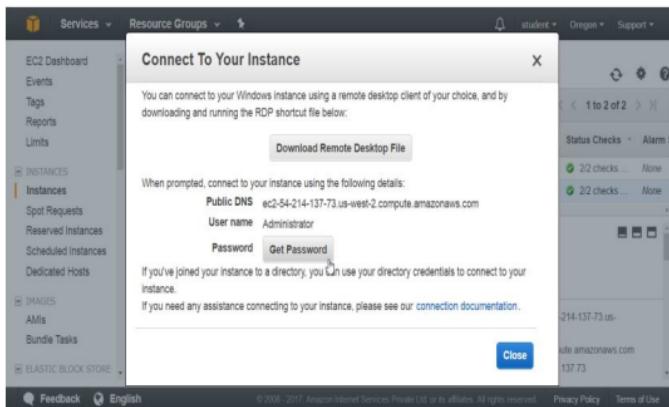
The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with navigation links: Services, Resource Groups, Events, Tags, Reports, Limits, Instances (which is selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, and Elastic Block Store. The main area has tabs for Launch Instance, Connect (which is highlighted with a mouse cursor), and Actions. Below these are search and filter fields. A table lists two instances: 'linuxvm' and 'winserver'. The 'winserver' row is selected. The table columns include Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Below the table, it says 'Instance: i-0a6e73f953579363 (winserver) Public DNS: ec2-54-214-137-73.us-west-2.compute.amazonaws.com'. At the bottom of the main area, there are tabs for Description, Status Checks, Monitoring, and Tags. The status checks tab is active, showing details for the selected instance: Instance ID i-0a6e73f953579363, Public DNS (IPv4) ec2-54-214-137-73.us-west-2.compute.amazonaws.com, and IPv4 Public IP 54.214.137.73. At the very bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use.

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

Click on “Download Remote Desktop file” button



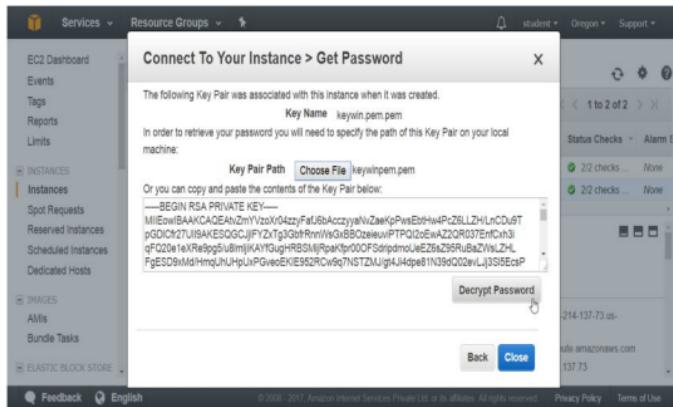
Click on “Get Password” button



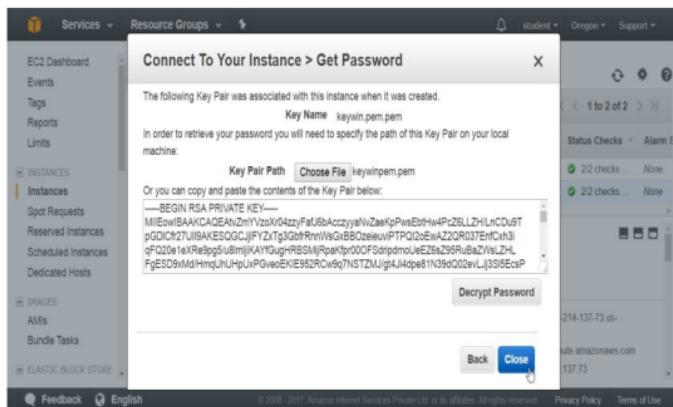
Click on "Choose file" button

Provide the path of key file

Click on "Decrypt Password" button



Click on Close button



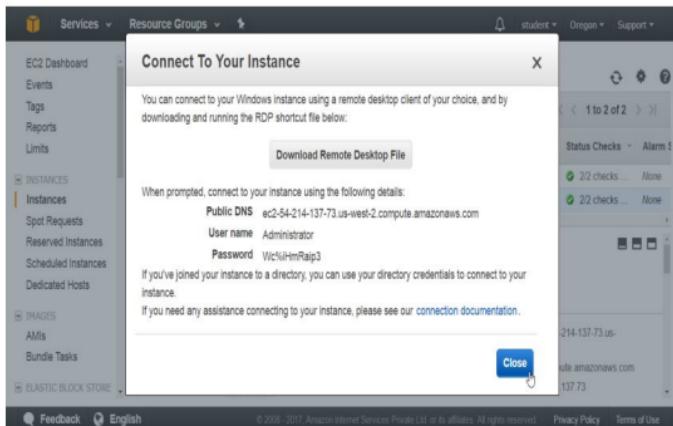
Copy your instance Detail in Notepad

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

User name Administrator

Password *****

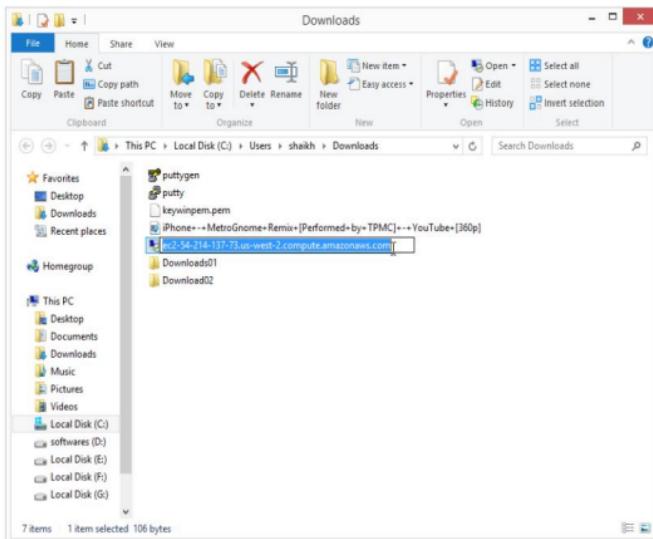
Click on **Close** button.



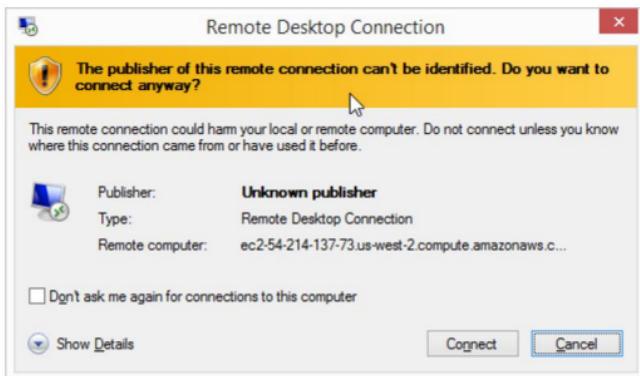
3) Now you can login to Amazon Windows instance

Double click on downloaded RDP file

Provide username as Administrator and give Password.

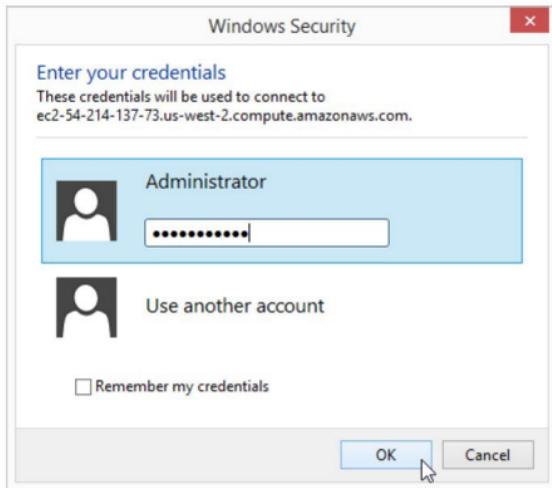


Click on connect

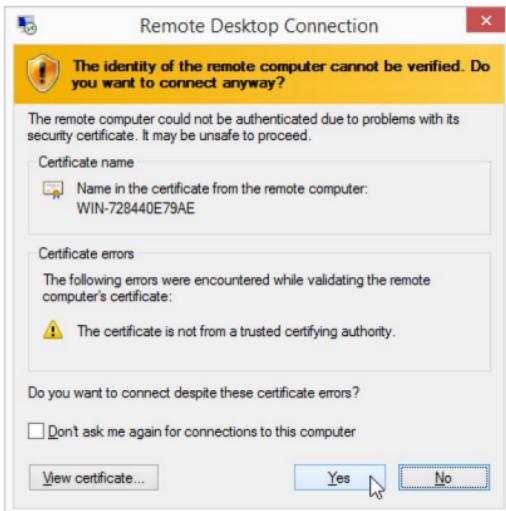


Provide username Administrator and Password

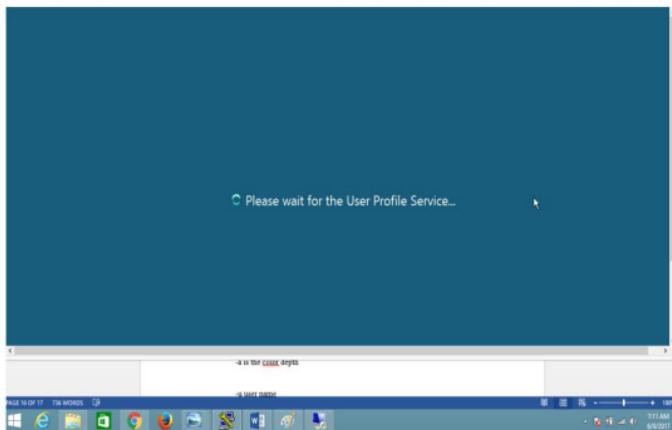
Click on OK



Click on Yes button



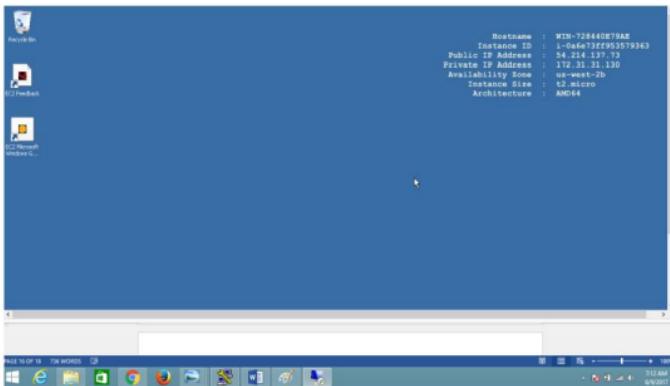
Wait for a movement



Verify

Successfully Logged in to windows instance

Check Public and Private IP of Windows instance



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

Login to Linux client operating system

Open linux terminal

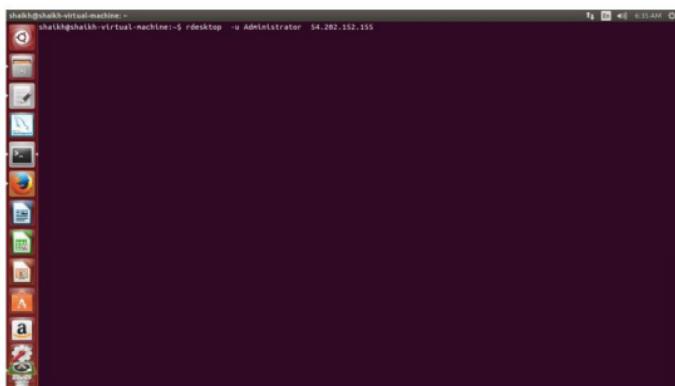
Note: rdesktop or xfreerdp { RHEL-6,7 } package should be installed

\$ rdesktop -u Administrator <Pub_DNS_name / Public_IP>

or

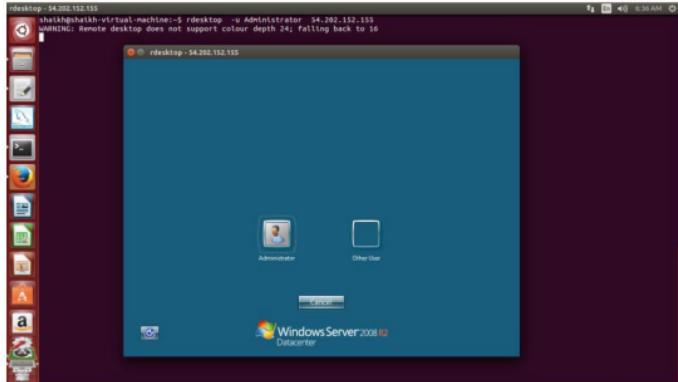
\$ xfreerdp -u Administrator <Pub_DNS_name / Public_IP> { in RHEL 6,7 }

-u → user name



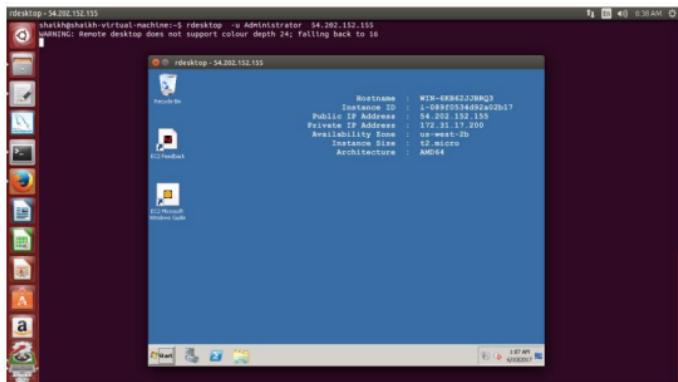
Click on Administrator

Provide the password



Verify:

Once Logged in Windows Desktop is available



Note:

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

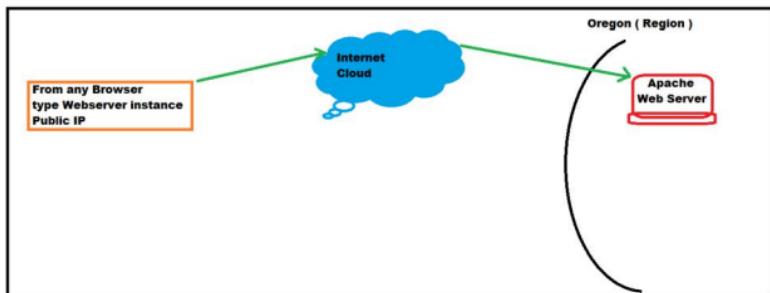
Otherwise it will be charged if the limit is over after free tier usage.

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

OBJECTIVE

To configure Webserver and to verify using Elastic public IP

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

TASK :

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

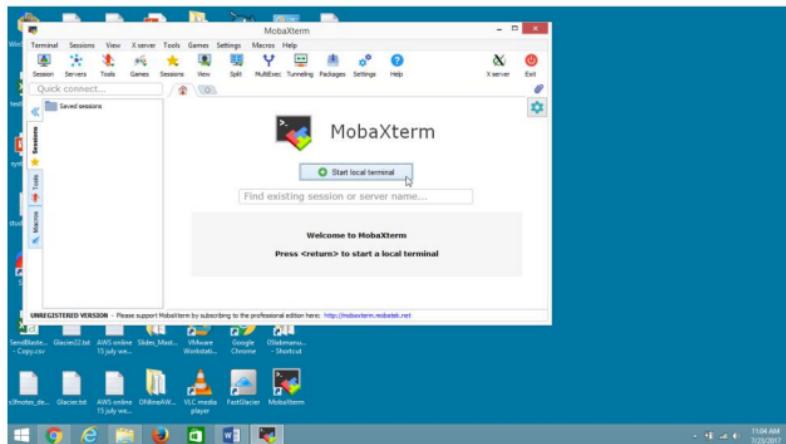
1) Launch Amazon linux instance and login to your instance

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

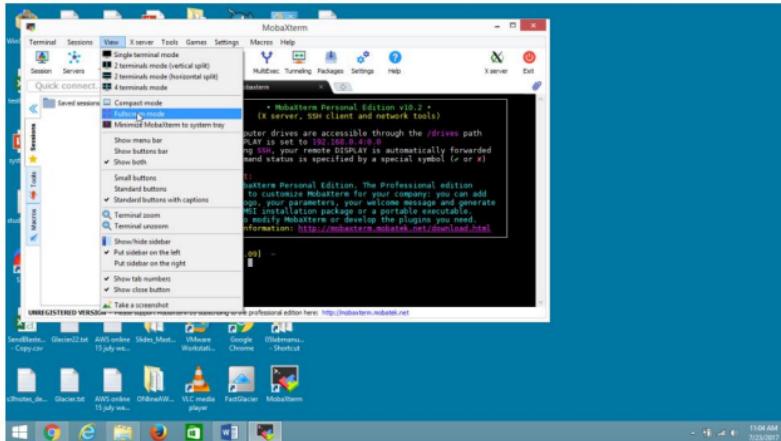
2) Connect to linux instance from windows using MobaXterm

Open **MobaXterm**

Click on **Start local terminal**



[Go to Full Screen mode](#)



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

Eg : cd e:/awskeys

- Mohabekas Personal Edition v3.2 - 1x Server, SSM client and network tools
- Your computer drives are accessible through the /drives path
- Your DISPLAY is set to 192.168.0.4:0.0
- Each connection status is indicated by a special symbol (x or *)

Important:
This is Mohabekas Personal Edition, The Professional edition allows you to customize Mohabekas for your company; you can add your logo, change colors, and much more.

To install Mohabekas Personal Edition, you must download either an MSI installation package or a portable executable, you can download it from the following link:
For more information: <http://mohabekas.muhakat.com/download.htm>

[2017-07-23 11:04.09] -> [shashikn-pc.mast] > cd e:/zavkayal

Login to linux instance by typing the following command

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

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

 _|_(-|- )
 _\|_|_ | Amazon Linux AMI

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

Switch to root user

Type “sudo su”

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

Configure Apache Webserver run following commands as shown in the screen

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

To use vi editor

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

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

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 sidebar with navigation links: Services (selected), Resource Groups, EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images (AMIs, Bundle Tasks), and Elastic Block Store (Volumes, Snapshots). The main content area is titled "Instances" and shows a table with two rows. The first row is for a "Linuxwebserver..." instance, which is currently running. The second row is for another instance. The table includes columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, and Public DNS. Below the table, a detailed view for the "Linuxwebserver..." instance is shown. It includes tabs for Description, Status Checks, Monitoring, and Tags. Under the Description tab, it shows the Instance ID (i-09e8a7e3ce9a9561), Instance state (running), Instance type (t2.micro), and Flavour (t2.micro). It also lists Public DNS (ec2-54-186-180-140.us-west-2.compute.amazonaws.com), Public IP (54.186.180.140), IPv4 Public IP (54.186.180.140), and Private IP (10.177.54.10.9.8.41). A "Details" link is present. At the bottom of the main content area, there are links for Feedback, English, and a footer with copyright information (© 2008-2017, Amazon Web Services Private Ltd or its affiliates. All rights reserved.), Privacy Policy, Terms of Use, and a Show all link. The status bar at the bottom right shows the date and time (10:02 AM 10/26/2017).

Go to the right end

Select Security Groups

Click on launch-wizard-1

The screenshot shows the AWS Management Console interface for the EC2 service. On the left, there's a navigation sidebar with links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block Store. The main content area is titled 'Launch Instance' and shows a table of instances. One instance, 'i-09e8a71e3ce9a9561 (Linuxwebserver)', is highlighted. The 'Security Groups' column for this instance displays 'launch-wizard-1'. The browser's address bar at the top contains the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2&instances.sortBy=tagName>.

Click on Inbound button

The screenshot shows the AWS Management Console interface for the Security Groups service. On the left, there's a navigation sidebar with links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block Store. The main content area is titled 'Create Security Group' and shows a table of security groups. One security group, 'sg-6ab60510' (with the name 'launch-wizard-1'), is selected. The 'Inbound' tab is highlighted in the 'Security Group: sg-6ab60510' panel. The browser's address bar at the top contains the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2&SecurityGroups=search+sg-6ab60510sort+groupID>.

Click on Edit button

The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with various navigation links like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area is titled 'Create Security Group' and shows a search bar with 'sg-6abb0510'. Below it, a table lists a single security group: 'sg-6abb0510' with 'Group Name' 'launch-wizard-1', 'VPC ID' 'vpc-89c34tee', and 'Description' 'launch-wizard-1 created 2017-07-23T09:27'. There are tabs for 'Description', 'Inbound' (which is selected), 'Outbound', and 'Tags'. A large button labeled 'Edit' is visible. The 'Inbound' table has columns for 'Type', 'Protocol', 'Port Range', and 'Source'. One row is shown: 'SSH', 'TCP', '22', and '0.0.0.0/0'. At the bottom right of the main window, there's a status bar with '10:00 AM 7/23/2017'.

Click on Add Rule button

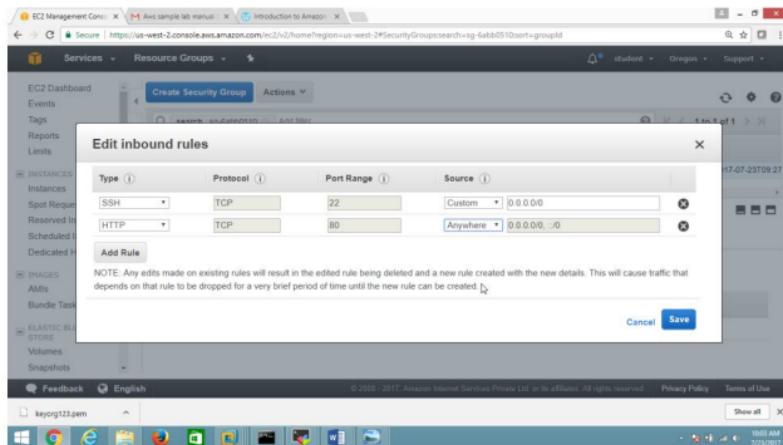
This screenshot shows the 'Edit inbound rules' dialog box overlaid on the EC2 Management Console. The dialog has fields for 'Type' (set to 'SSH'), 'Protocol' (set to 'TCP'), 'Port Range' (set to '22'), and 'Source' (set to 'Custom 0.0.0.0/0'). A prominent button labeled 'Add Rule' is highlighted with a mouse cursor. A note below the form states: 'NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.' At the bottom right of the dialog are 'Cancel' and 'Save' buttons. The background shows the same EC2 interface as the previous screenshot, with the status bar at the bottom indicating '10:00 AM 7/23/2017'.

Add HTTP Rule

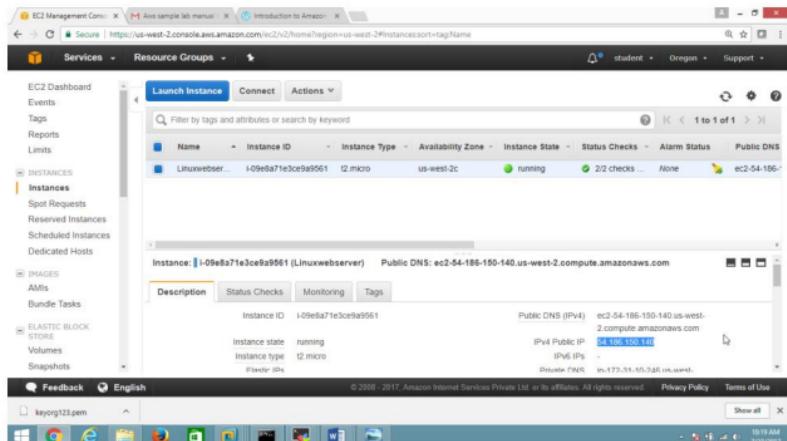
Under **Type** column select **HTTP**

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

Click Save button



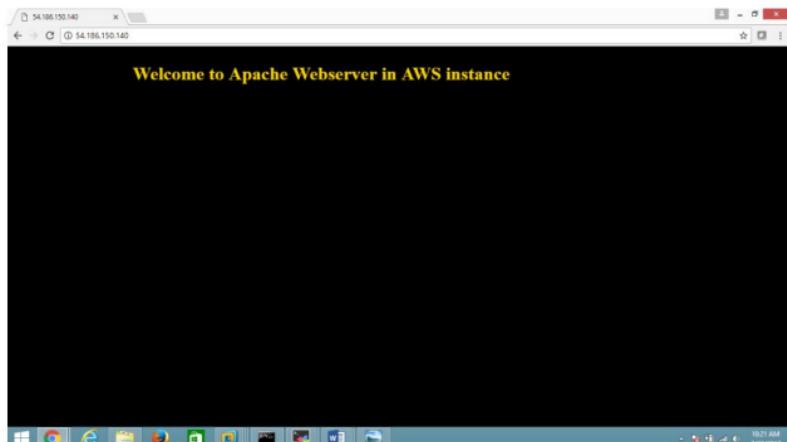
4) Open Browser and provide Webserver instance DNS_name or Public IP



The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, and Elastic Block Store. The Instances section is currently selected. In the main content area, there's a search bar and a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, and Public DNS. One row is highlighted for 'Linuxwebserver'. Below this, a detailed view of the selected instance is shown with tabs for Description, Status Checks, Monitoring, and Tags. The instance's public DNS is listed as ec2-54-186-150-140.us-west-2.compute.amazonaws.com. The status checks show 2/2 checks passed. The instance state is running, and it's an t2.micro type in us-west-2c. The browser's address bar displays the URL https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#instances:sort+tagName. The taskbar at the bottom has icons for various applications.

Verify

Website is running



The screenshot shows a web browser window with the URL 54.186.150.140 in the address bar. The main content of the browser shows the text "Welcome to Apache Webserver in AWS instance". The browser's title bar also displays the same URL. The taskbar at the bottom of the screen shows icons for various Windows applications like File Explorer, Task View, and Control Panel.

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 navigation menu includes 'Services' (selected), 'Resource Groups', 'Launch Instance', 'Connect', and 'Actions'. Under 'NETWORK & SECURITY', 'Elastic IP' is selected and highlighted with a blue border. The main content area displays a table of instances. One row is selected, showing details for an instance named 'Linuxwebser...'. The 'Public DNS' field shows 'ec2-54-186-150-140.us-west-2.compute.amazonaws.com'. Below the table, there are tabs for 'Description', 'Status Checks', 'Monitoring', and 'Tags'. At the bottom of the page, there are links for 'Privacy Policy' and 'Terms of Use', along with a copyright notice from 2017.

Click on Allocate new address button

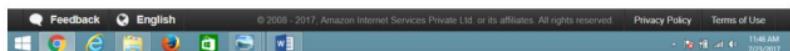
The screenshot shows the EC2 Management Console interface. The top navigation bar includes 'Services', 'Resource Groups', and user information ('student', 'Oregon', 'Support'). The left sidebar has sections for 'Networking & Security' (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), 'Load Balancing' (Load Balancers, Target Groups), 'Auto Scaling' (Launch Configurations, Auto Scaling Groups), and 'Systems Manager Services'. The main content area is titled 'Allocate new address' and displays a message: 'You do not have any Addresses in this region. Click the Create Address button to create your first Address.' A prominent blue button labeled 'Allocate new address' is centered, with a cursor pointing at it.

Click Allocate button

The screenshot shows the 'Allocate new address' dialog box. At the top, it says 'Addresses > Allocate new address'. Below that is the title 'Allocate new address'. A sub-instruction reads 'Allocate a new Elastic IP address by selecting the scope in which it will be used'. A required field is marked with an asterisk (*). At the bottom right are 'Cancel' and 'Allocate' buttons, with the 'Allocate' button highlighted by a cursor.

Click on **Close** 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#AllocateAddress>. The page title is "Allocate new address". A green success message box contains the text "New address request succeeded" with a checkmark icon. Below it, the "Elastic IP" is listed as "52.42.166.202". In the bottom right corner of the message box, there is a blue "Close" button.



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

Verify website is running with elastic IP.

A screenshot of a Microsoft Edge browser window. The address bar shows the URL "52.42.166.202". The main content area displays the text "Welcome to Apache Webserver in AWS instance" in yellow font against a black background. The browser's taskbar at the bottom shows other pinned sites like Google, YouTube, and the AWS console. The system tray indicates the date and time as "11:54 AM 7/23/2017".

To releasing Elastic IP

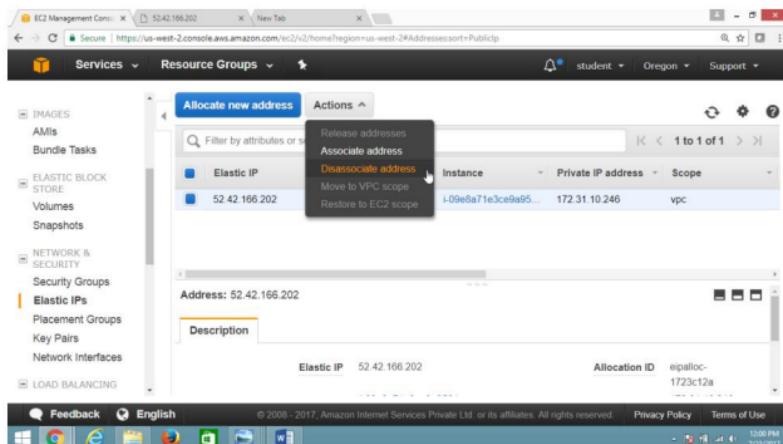
Open the console **EC2 Dashboard**

Expand "Network Security"

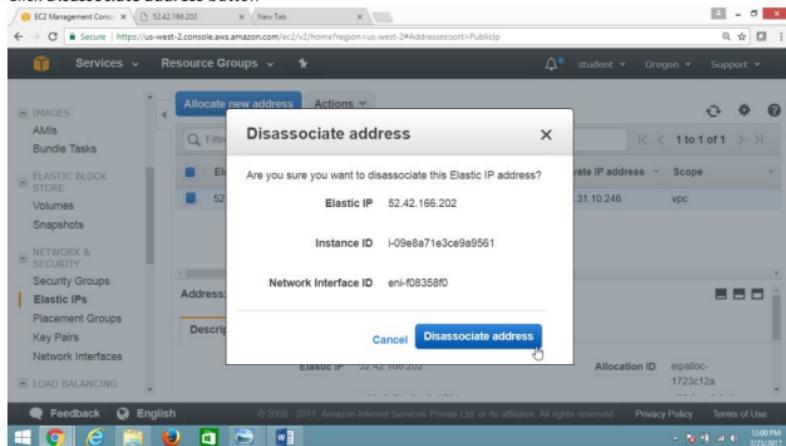
Select **Elastic IP**

Click **Action** button

Select **Disassociate Address**

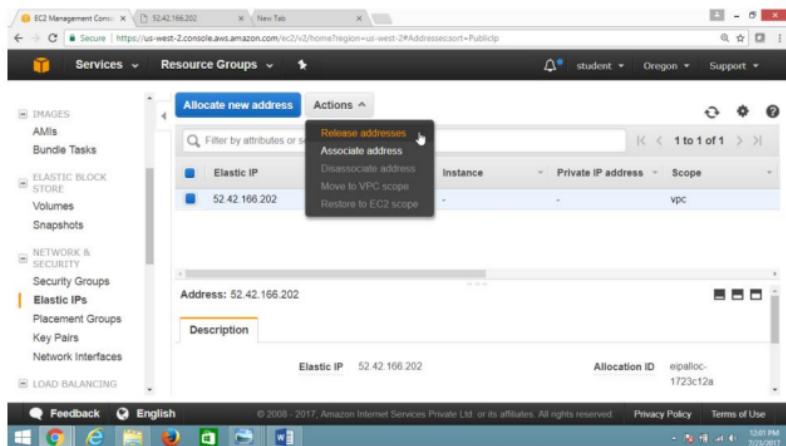


Click Disassociate address button

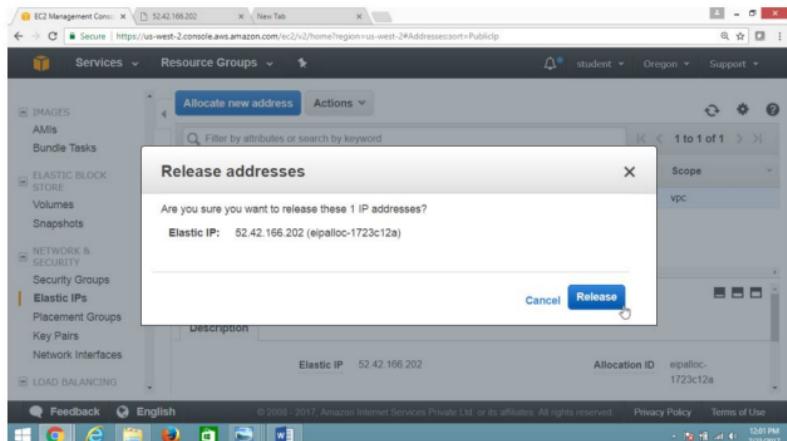


Click Action button

Select Release Addresses



Click Release button



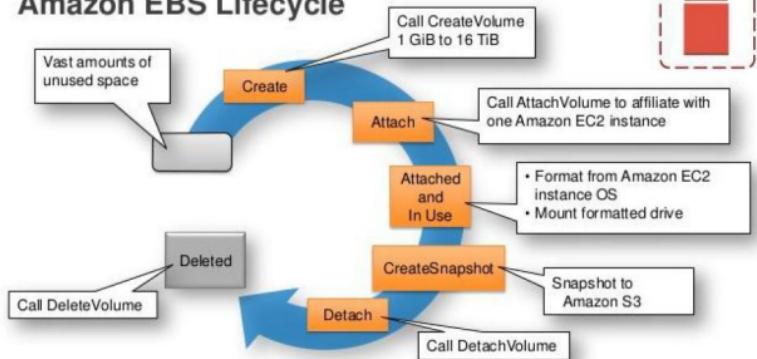
Lab 5: To Manage Elastic Block Store (EBS)

OBJECTIVE

To configure and use AWS EBS service

TOPOLOGY

Amazon EBS Lifecycle



© 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" option is highlighted with a red circle. The main content area displays resource counts: 0 Running Instances, 0 Dedicated Hosts, 0 Volumes, 0 Key Pairs, 0 Placement Groups, 0 Elastic IPs, 0 Snapshots, 0 Load Balancers, and 1 Security Groups. A callout box highlights the "Volumes" link with the text: "Just need a simple virtual private server? Get everything you need to jumpstart your project - compute, storage, and networking – for a low, predictable price. Try Amazon Lightsail for free." Below this, there's a "Create Instance" section with a "Launch Instance" button, and a note stating "To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance." At the bottom, there are links for "Service Health" and "Scheduled Events". The top right corner shows account attributes like "Supported Platforms", "Default VPC", and "Resource ID length management". The bottom right corner features the "AWS Marketplace" section.

Click on **Create Volumes** button

The screenshot shows the AWS EBS Management Console interface. On the left, there's a sidebar with navigation links: Instances, Scheduled Instances, Dedicated Hosts, IMAGES, AMIs, Bundle Tasks, ELASTIC BLOCK STORE (with Volumes selected), Snapshots, NETWORK & SECURITY (with Security Groups, Elastic IPs, Placement Groups, and Key Pairs). At the top, there are tabs for 'Creating an Amazon EBS Volume' and 'EC2 Management Console'. The main area has a search bar and a message: 'You do not have any EBS volumes in this region. Click the Create Volume button to create your first volume.' A large blue 'Create Volume' button is centered. Below it, there's a section titled 'Select a volume above' with three small icons. At the bottom, there are links for Feedback, English (US), and copyright information: '© 2006 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy 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 'Volume Type' is set to 'General Purpose SSD (GP2)'. The 'Size (GiB)' is set to '2'. The 'IOPS' setting is '300 / 3000' with a note: '(Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)'. The 'Availability Zone' is 'us-west-2a'. The 'Throughput (MB/s)' is 'Not applicable'. The 'Snapshot ID' dropdown is set to 'Select a snapshot'. The 'Encryption' checkbox is checked. Below the form, there's a 'Tags' section with a note: 'Add tags to your volume'. At the bottom right, there are 'Cancel' and 'Create Volume' buttons, with 'Create Volume' being highlighted by a blue border.

Verify Volume successfully created

Click **Close** button

The screenshot shows a browser window with the AWS EC2 Management Console. The URL is [https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2CreateVolume](https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2>CreateVolume). The page title is "Creating an Amazon EBS Volume". The main content area displays a green success message box with the text "Volume created successfully" and the Volume ID "vol-0d040899c111aceec". A blue "Close" button is visible at the bottom right of the message box. The top navigation bar includes "Services" and "Resource Groups". The top right corner shows user information: "student", "Oregon", and "Support". The footer contains links for "Feedback", "English (US)", "Privacy Policy", and "Terms of Use".

To Monitoring the State of Your Volumes

Select Volume check state → available

The screenshot shows a browser window with the AWS EC2 Management Console. The URL is <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2Volumesort=desccreateTime>. The main content area displays a table of volumes. One row is highlighted, showing the following details:

Name	Volume ID	Size	Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Status
vol-08ba155...	vol-08ba155...	2 GiB	gp2	100 / 3000		November 10, 2017...	us-west-2a	available	None

The "State" column for this volume shows a blue circle with the word "available". The footer contains links for "Feedback", "English (US)", "Privacy Policy", and "Terms of Use".

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

The screenshot shows the AWS EC2 Management Console with the 'Create Volume' tab selected. A search bar at the top right contains the text '2 to 2 of 2'. Below it is a table with the following data:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	Stat
Wlmrm1	vol-0b2580a	30 GB	gp2	100 / 3000	snap-04e2c21...	November 10, 2017...	us-west-2a	green dot
2gb2a		2 GB	gp2	100 / 3000		November 10, 2017...	us-west-2a	blue dot

Below the table, there is a section titled 'Volumes' with a single item listed: 'vol-08ba155bd2df3cbcc'. At the bottom of the page, there are tabs for 'Description', 'Status Change', 'Monitoring', and 'Tags', with 'Description' being the active tab.

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**.

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with links like Spot Requests, Reserved Instances, 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 has tabs for Description, Status Checks, Monitoring, and Tags. A modal window is open over the table of volumes, showing a dropdown menu with options: Modify Volume, Delete Volume, Attach Volume (which is highlighted with a cursor), Detach Volume, Force Detach Volume, Create Snapshot, and Change Auto-Enable IO Setting. The table lists three volumes: gp2, 100 / 3000, snap-0a2a00d... (Created: November 10, 2017, Availability Zone: us-west-2a); gp2, 100 / 3000, snap-04e2c21... (Created: November 10, 2017, Availability Zone: us-west-2a); and 2gt02a, 100 / 3000, snap-04e2c21... (Created: November 10, 2017, Availability Zone: us-west-2a). At the bottom of the modal, there are buttons for Add/Edit Tags and Cancel.

Select instance → Winvm1

The screenshot shows the AWS EC2 Management Console with the 'Volumes' section selected. A modal dialog box titled 'Attach Volume' is open. Inside the dialog, a volume is selected ('vol-08ba15bd2df3ccbc (2gb2a)') and is being attached to an instance ('i-0515c735f8bfa071 (Winvm1 (running))'). The device is set to '/dev/sda1'. At the bottom right of the dialog is a blue 'Attach' button.

Click on Attach

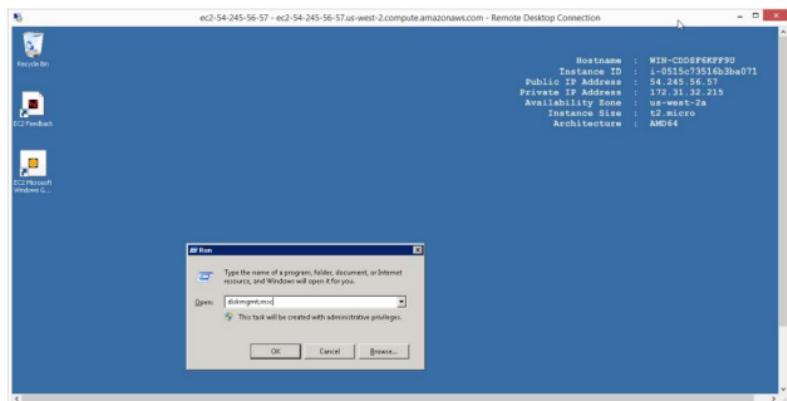
The screenshot shows the AWS EC2 Management Console with the 'Volumes' section selected. A modal dialog box titled 'Attach Volume' is open. Inside the dialog, a volume is selected ('vol-08ba15bd2df3ccbc (2gb2a)') and is being attached to an instance ('i-0515c735f8bfa071'). The device is set to 'xvdf'. At the bottom right of the dialog is a blue 'Attach' button.

Verify the Availability of new volume

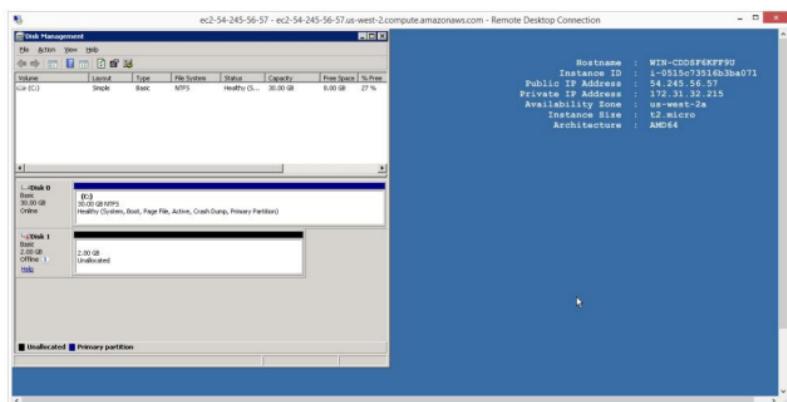
3. To check availability of new drive login to your Windows instance.

Login to windows instance

Run → diskmgmt.msc

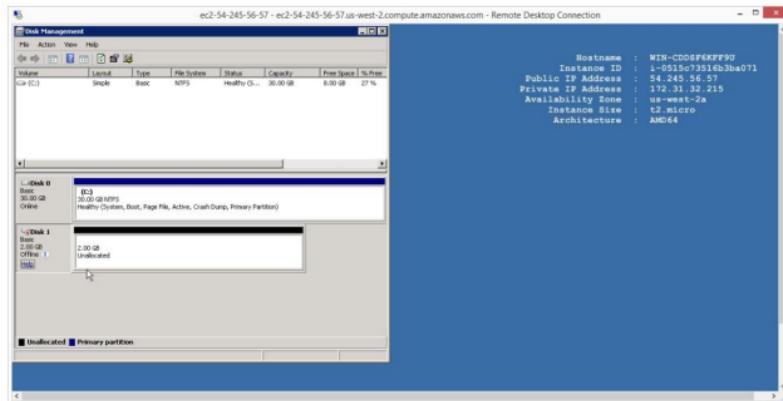


Verifies that 2 GB volume available as unallocated space

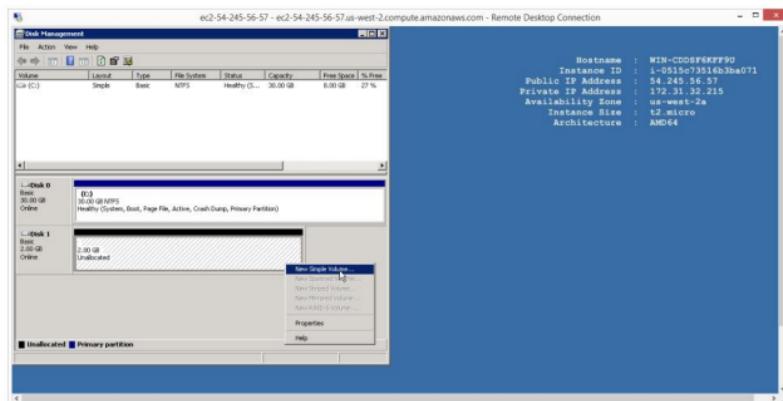


New disk is offline,

So turn it to online by right clicking and select online

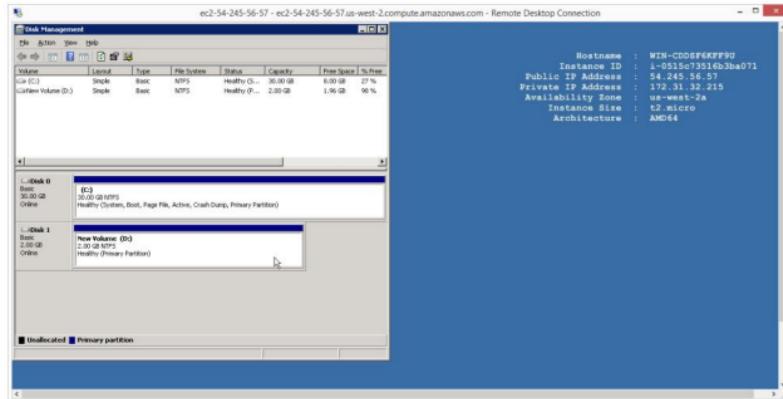


Format the unallocated disk



Verify

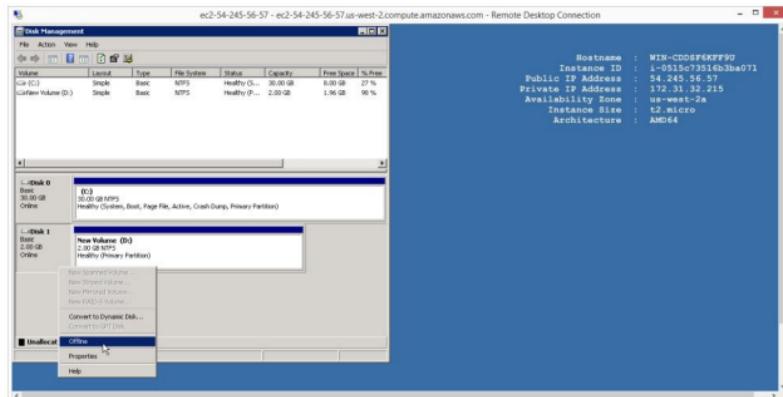
New Volume to 2GB is available to use



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

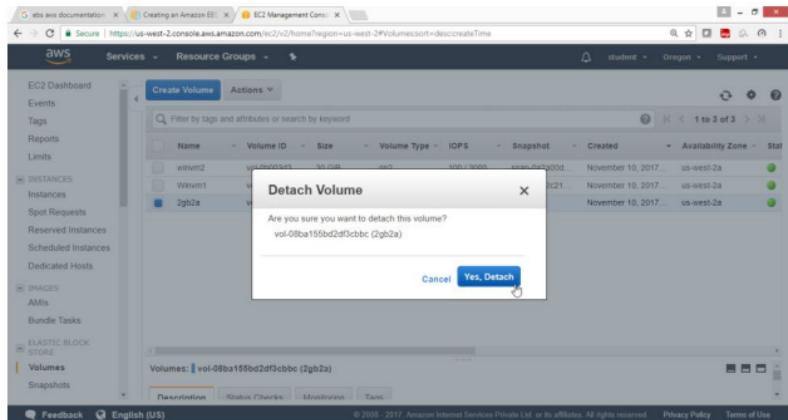
Select volume to be detached under Name column.

Drop Down Action button

Select "Detach Volume"

Name	Type	IOPS	Snapshot	Created	Availability Zone	Stat
www2	gp2	100 / 3000	snap-0a2a00d	November 10, 2017	us-west-2a	green
wwwm2	gp2	100 / 3000	snap-04e2c21	November 10, 2017	us-west-2a	green
2gb2a	gp2	100 / 3000		November 10, 2017	us-west-2a	green

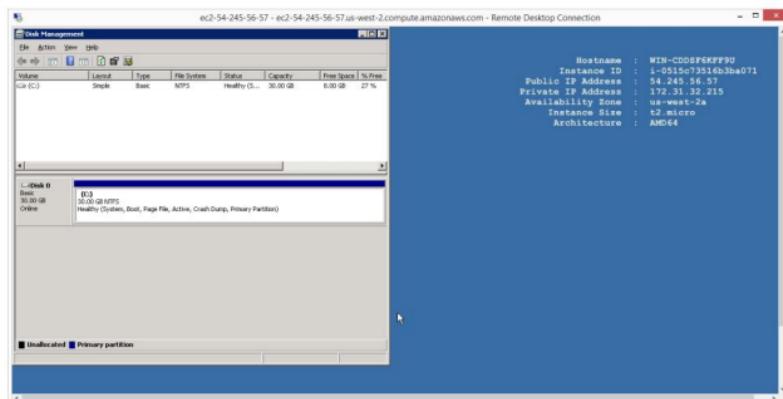
Click on "Yes, Detach" button



Verification

Login to windows instance

Check that D: drive is removed

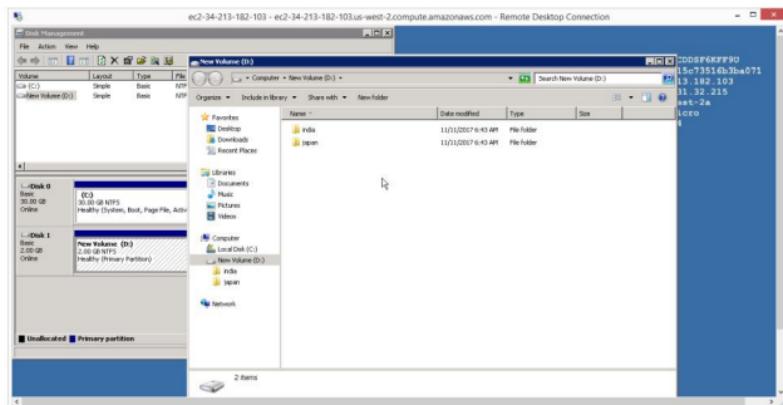


5. To Create Snapshot and Restore EBS volume.

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, there's a sidebar with various services like Scheduled Instances, Dedicated Hosts, and Elastic Block Store. Under EBS, 'Volumes' is selected. In the main area, a table lists three volumes: gp2, gp2, and gp2. A context menu is open over the first gp2 volume, with 'Actions' expanded. The 'Create Snapshot' option is highlighted with a cursor. The table has columns for Volume Type, IOPS, Snapshot, and Created.

Provide snapshot details

Click **Create** button

The screenshot shows the 'Create Snapshot' dialog box. It contains fields for Volume (selected), Name (snapvol1), Description (snapvol1_des), and Encrypted (No). At the bottom are 'Cancel' and 'Create' buttons.

Volume	vol-08ba155bd2df3cbbc (2gb2a)
Name	snapvol1
Description	snapvol1_des
Encrypted	No

Cancel **Create**

Verify that snapshot is created.

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#SnapshotList#snapshotId>. The left sidebar is collapsed, and the main area displays the 'Snapshots' section. A table lists one snapshot entry:

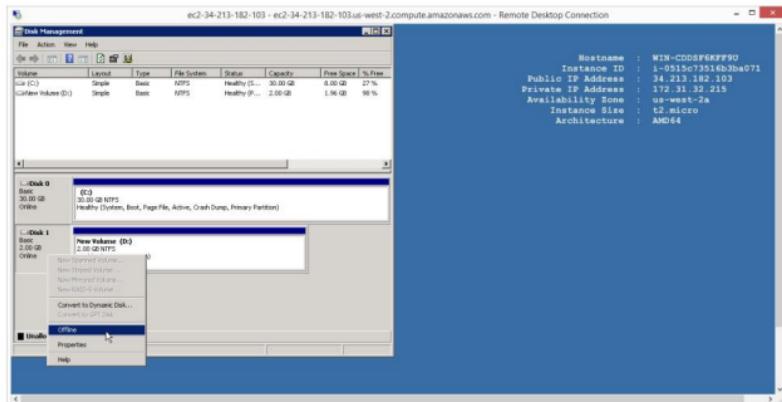
Name	Snapshot ID	Size	Description	Status
snapvol1	snap-08ff48c354563cba0	2 GiB	snapvol1_des	Completed

Below the table, the snapshot details are shown: **Snapshot: snap-08ff48c354563cba0 (snapvol1)**. There are three tabs at the bottom: **Description**, **Permissions**, and **Tags**. The **Description** tab is selected.

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.

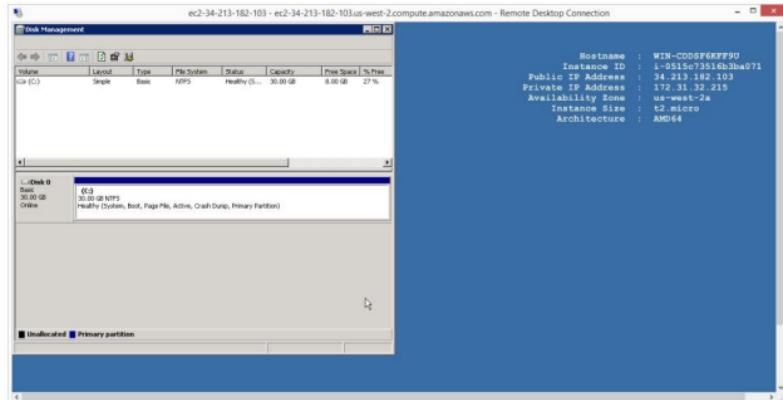
Drop Down Action button, Select “**Delete Volume**”

The screenshot shows the AWS EC2 Management Console interface. On the left, the navigation pane is open, showing various services like Scheduled Instances, Dedicated Hosts, and the selected "ELASTIC BLOCK STORE" which has "Volumes" highlighted. In the main content area, a list of volumes is displayed in a table. One volume, "2gb2a", is selected and highlighted with a blue border. A context menu is open over this volume, with the "Actions" option expanded. The "Actions" menu contains several options: "Delete Volume", "Attach Volume", "Detach Volume", "Force Detach Volume", "Create Snapshot", "Change Auto-Enable IO Setting", and "Add/Edit Tags". The "Detach Volume" option is currently being selected, indicated by a mouse cursor icon. The table below the menu lists three volumes: gp2, gp2, and gp2, with their respective details: IOPS (100 / 3000), Snapshot (snap-0a2a00d... and snap-0e4e2c1...), and Created (November 10, 2017...).

Volume Type	IOPS	Snapshot	Created
gp2	100 / 3000	snap-0a2a00d...	November 10, 2017...
gp2	100 / 3000	snap-0e4e2c1...	November 10, 2017...
gp2	100 / 3000		November 10, 2017...

Verify from windows instance open disk Management tool

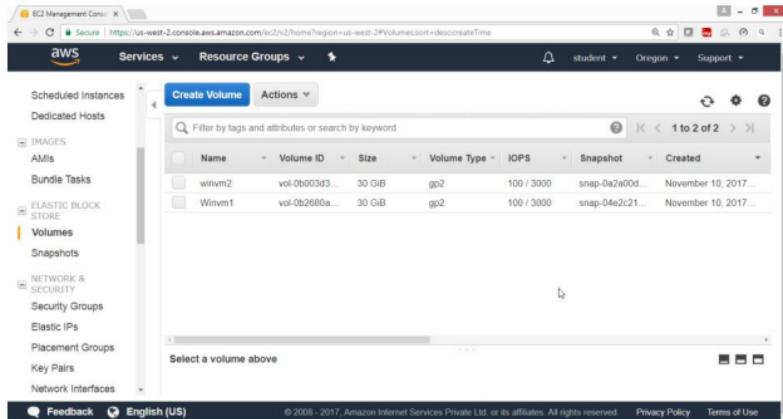
Now D drive is detached



Now delete the volume

A screenshot of the AWS Management Console for the EC2 service. On the left, the navigation pane shows 'Scheduled Instances', 'Dedicated Hosts', 'IMAGES', 'AMIs', 'Bundle Tasks', 'ELASTIC BLOCK STORE', 'Volumes' (which is selected and highlighted in orange), and 'Snapshots'. In the main content area, there's a 'Create Volume' button and an 'Actions' dropdown menu. A context menu is open over a volume named '2gb2a', with the 'Delete Volume' option highlighted. To the right, a table lists three volumes: 'wimv2' (gp2, 100 / 3000, snap-0a00d...), 'Wimmt' (gp2, 100 / 3000, snap-04e02c21...), and '2gb2a' (gp2, 100 / 3000, snap-08ba155bd2df3ccb...). At the bottom of the table, there are buttons for 'Add/Edit Tags' and 'Change Auto-Enable IO Setting'. The status bar at the bottom of the page includes links for 'Feedback', 'English (US)', '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Verify volume is deleted.



The screenshot shows the AWS Management Console interface for the EC2 service. The left sidebar has 'Scheduled Instances' and 'Dedicated Hosts' collapsed, and 'IMAGES', 'AMIs', 'Bundle Tasks', and 'ELASTIC BLOCK STORE' expanded. Under 'ELASTIC BLOCK STORE', 'Volumes' is selected, and 'Snapshots' is collapsed. The main content area shows a table titled 'Create Volume' with 'Actions' dropdown. A search bar at the top of the table says 'Filter by tags and attributes or search by keyword'. The table has columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, and Created. There are two entries:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
wimvm2	vol-0b000d3...	30 GiB	gp2	100 / 3000	snap-0a2a00d...	November 10, 2017...
Wimvmf	vol-0b2680a...	30 GiB	gp2	100 / 3000	snap-04e2c21...	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)', and copyright information: '© 2006 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' followed by 'Privacy Policy' and 'Terms of Use'.

7. To Restore the volume.

From the console **EC2 Dashboard**

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

Select the snapshot

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

The screenshot shows the AWS 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 and Snapshots selected), NETWORK & SECURITY (with Security Groups, Elastic IPs, Placement Groups, Key Pairs, and Network Interfaces). In the center, a modal window titled "Create Snapshot" is open over a list of snapshots. One snapshot, "snapvol1", is selected. A dropdown menu labeled "Actions" is open, and the option "Create Volume" is highlighted with a cursor arrow. Below the modal, the main content area shows a table for the selected snapshot, with details like "Snapshot: snap-08ff48c354563cba0 (snapvol1)", "Description", "Permissions", and "Tags". At the bottom of the page, there are links for Feedback, English (US), and footer information including copyright notice, Privacy Policy, and Terms of Use.

Accept the defaults values in wizard

Note: Check the right availability zone.

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

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

At the bottom, there is a note: "Tags" with a link to "Add tags to your volume". Below that is a required field indicator: "* Required". On the right, there are "Cancel" and "Create Volume" buttons. The footer includes links for "Feedback", "English (US)", "Privacy Policy", and "Terms of Use".

Verify Volume is created

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

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
vol-0cd5da3c...	vol-0cd5da3c...	2 GiB	gp2	100 / 3000	snap-08ff48c3...	November 11, 2017
wimvm2	vol-0b003d5...	30 GiB	gp2	100 / 3000	snap-0a2a00d...	November 10, 2017...
Wimvm1	vol-0b2680a...	30 GiB	gp2	100 / 3000	snap-04e2c21...	November 10, 2017...

At the bottom, there are tabs for "Description", "Status Checks", "Monitoring", and "Tags". The footer includes links for "Feedback", "English (US)", "Privacy Policy", and "Terms of Use".

7) To expanding the size of EBS volume.

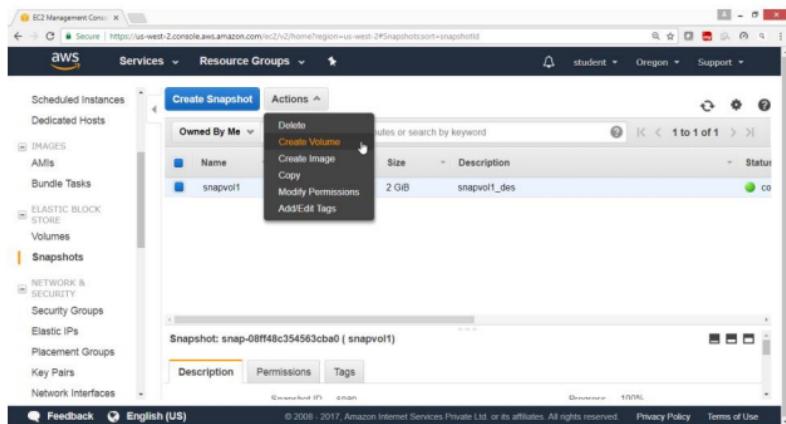
To expand EBS volume first take **snapshot**, now select the snapshot

On the **EC2 Dashboard** panel

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

Drop Down **Action** button

Select **Create Volume**



Give the required size → 4 GB

Check the right Availability Zone

click **Create Volume** button

The screenshot shows the 'Create Volume' wizard on 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

At the bottom, there is a 'Tags' section with a link to 'Add tags to your volume'. A note says '* Required'. On the right, there are 'Cancel' and 'Create Volume' buttons. The 'Create Volume' button is highlighted with a blue border.

Verify that 4 GB is created

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

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
vol-034d700...	4 GiB	gp2	100 / 3000	snap-08ff48c3...	November 11, 2017...	
vol-0cd5da3c...	2 GiB	gp2	100 / 3000	snap-08ff48c3...	November 11, 2017...	
wimv2	vol-0b0003d3...	30 GiB	gp2	100 / 3000	snap-02a2e0d...	November 10, 2017...
Wimv1	vol-0b2680a...	30 GiB	gp2	100 / 3000	snap-04e2c21...	November 10, 2017...

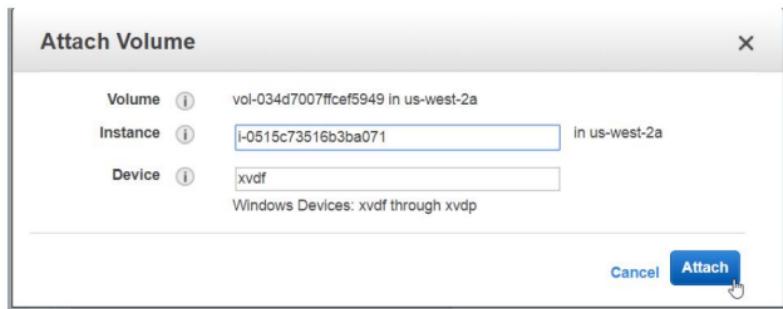
Now attach this expanded volume to your instance.

The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with various services like Scheduled Instances, Dedicated Hosts, AMIs, and Volumes. The 'Volumes' section is currently selected. In the main area, there's a table of volumes with columns for Name, Volume Type, IOPS, Snapshot, and Created. One volume, 'vol-034d7007ffcef5949', is selected. A context menu is open over this volume, with 'Attach Volume' highlighted. Other options in the menu include Modify Volume, Delete Volume, Detach Volume, Force Detach Volume, Create Snapshot, Change Auto-Enable IO Setting, and Add/Edit Tags. At the bottom of the screen, there are tabs for Description, Status Checks, Monitoring, and Tags, along with a feedback link and language selection for English (US).

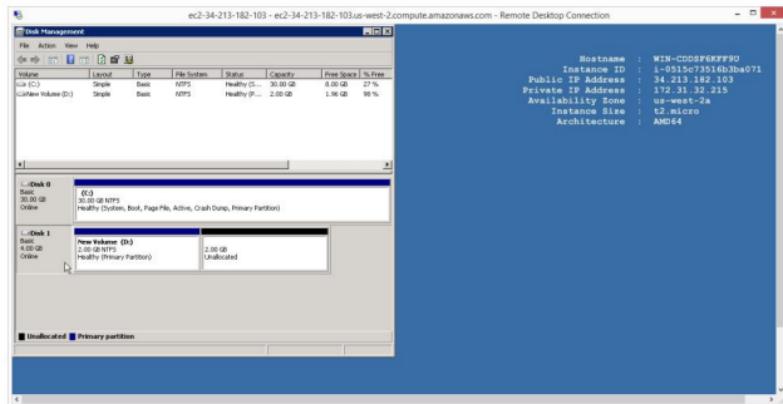
Select instance

The 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' with 'In us-west-2a'), and 'Device' (a dropdown list showing two options: 'i-0515c73516b3ba071 (winvm1) (running)' and 'i-04bd24ef0affeed12 (winvm2) (running)'). The second option in the list is highlighted with a cursor. At the bottom right are 'Cancel' and 'Attach' buttons.

Click **Attach** button

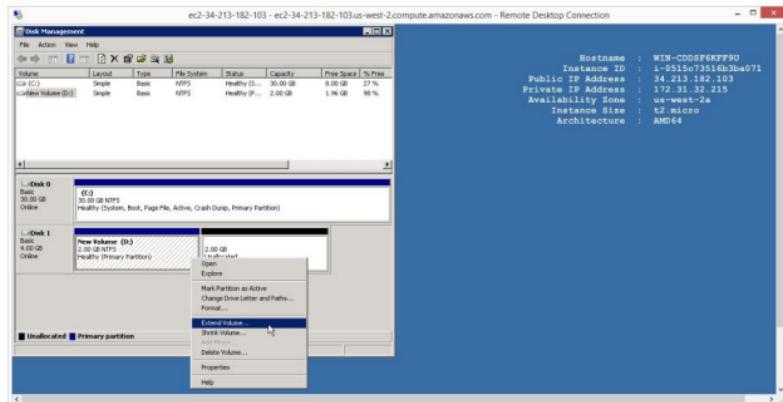


Verify 4 GB drive is available

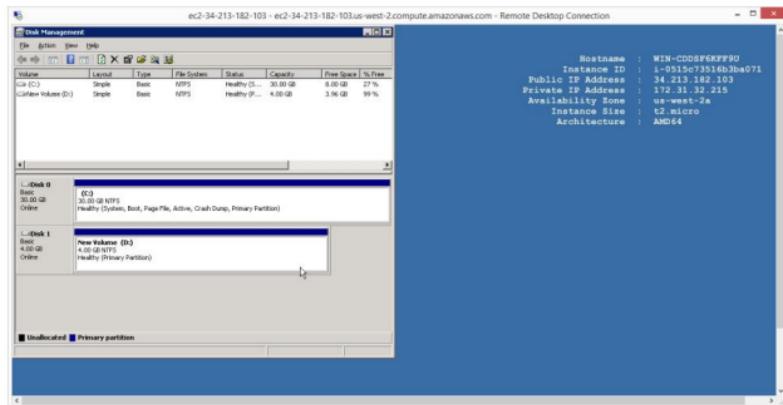


Now with respect to Windows operating system

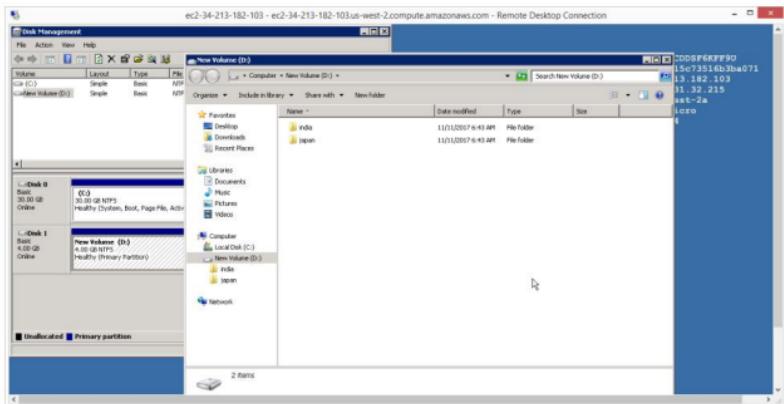
Right click on D drive extend your volume to your desired size



Verified that 4 GB volume available

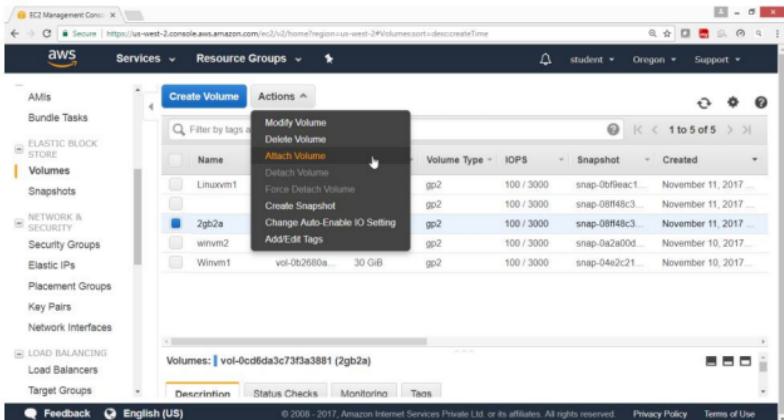


Verified that D drive contains two folders that was there in 2B drive earlier.

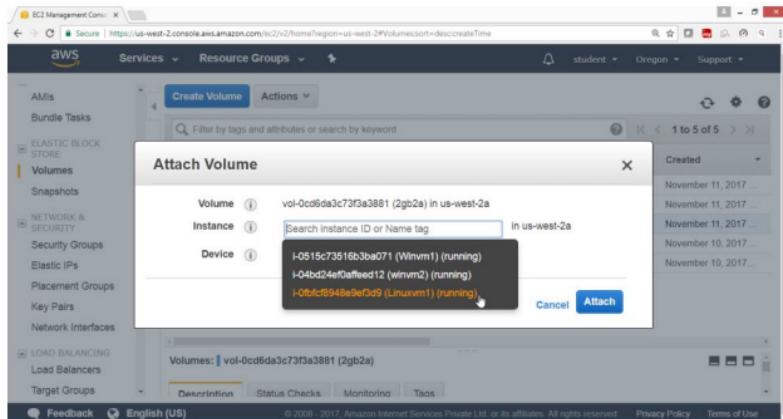


Similarly check volume in linux instance

From Action select **Attach volume**



Select Linux instance



Now connect to Linux instance

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

```
Amazon Linux AMI
```

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

To verify

Switch to root user and run fdisk -l

\$ sudo su

To check list of drives and partitions

fdisk -l

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

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

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

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

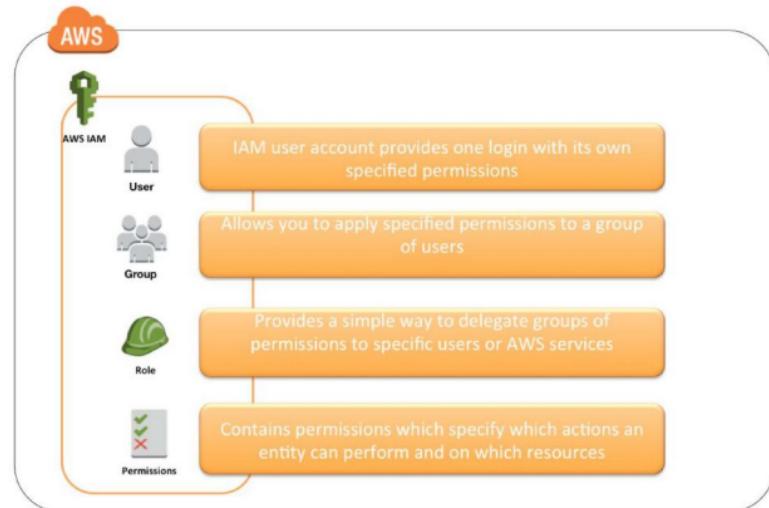
Lab 6: To Manage IAM Users, Groups and Policies

OBJECTIVE

To configure and use AWS IAM Service.

TOPOLOGY

AWS IAM Identities



PRE-REQUISITES

User should have AWS root account

To configure IAM with following task.

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

Create IAM groups.

Add users to a group.

Add policies to Groups and Users.

Create your own policies.

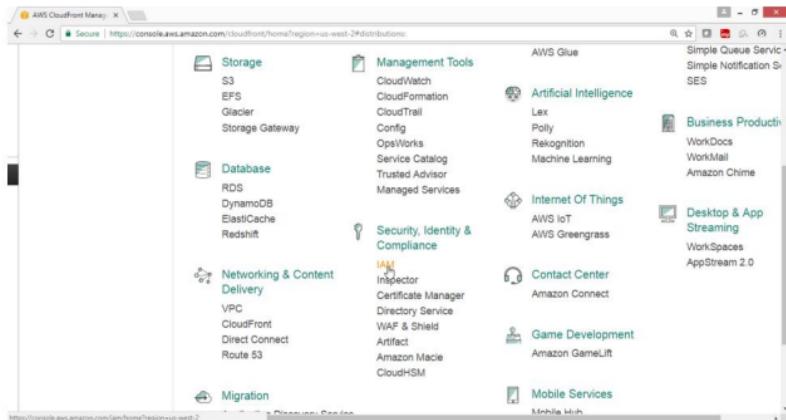
Users Login to sign-in page.

Deleting users and groups.

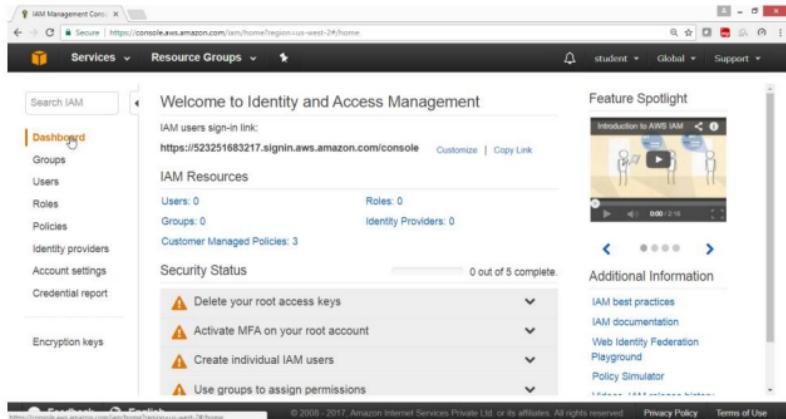
1) To create user, assign password, change password policy.

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

Click on IAM service



IAM Dashboard panel available



2) To Mange Groups and applying policies

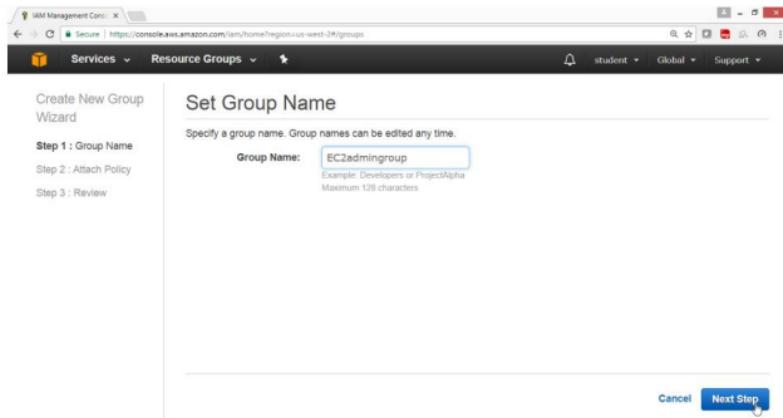
From IAM dashboard, select **Groups**

Click on **Create New Group** button

The screenshot shows the AWS IAM Groups page. On the left, there's a sidebar with links: Dashboard, Groups (which is selected and highlighted in orange), Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area has a header with 'Create New Group' and 'Group Actions'. Below that is a table with columns: Group Name, Users, Inline Policy, and Creation Time. A filter input field is above the table. The table displays the message 'No records found.' At the bottom of the page, there are footer links for Feedback, English, Privacy Policy, and Terms of Use.

Give Group Name → EC2admingroup

Click on **Next Step** button



In Filter type → EC2f

Select check box for **AmazonEC2FullAccess**

Click on **Next Step** button

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Attach Policy

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

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 ...

Showing 2 results

Cancel Previous Next Step

Click on **Create Group**

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Review

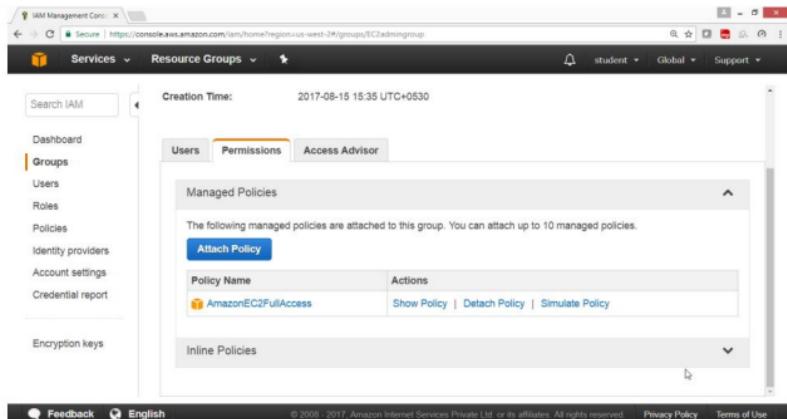
Review the following information, then click **Create Group** to proceed.

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

Cancel Previous Create Group

Verify

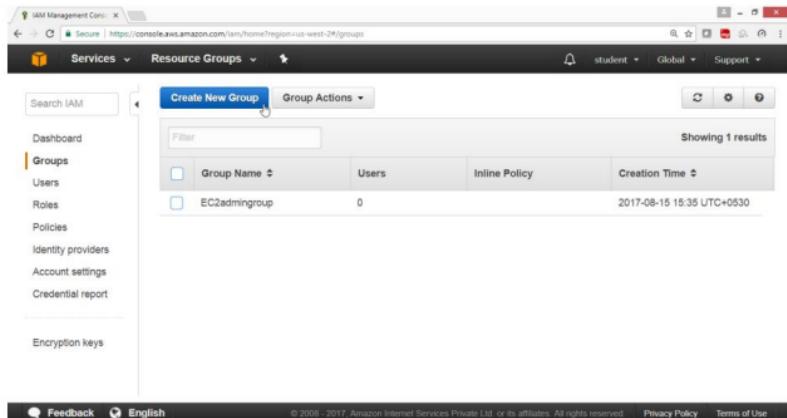
Group EC2admingrp got created with AmazonEC2FullAccess policy



The screenshot shows the AWS IAM Management Console. On the left, there's a sidebar with links like Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main area has tabs for Services (selected), Resource Groups, and a search bar. Below these, a 'Creation Time:' label is followed by '2017-08-15 15:35 UTC+0530'. There are three tabs: 'Users' (selected), 'Permissions', and 'Access Advisor'. Under 'Permissions', the 'Managed Policies' section is shown with a table. The table has columns for 'Policy Name' and 'Actions'. One row shows 'AmazonEC2FullAccess' with options 'Show Policy', 'Detach Policy', and 'Simulate Policy'. Below this is an 'Inline Policies' section.

Now again create Another Group

Click on **Create Group** button



The screenshot shows the 'Create New Group' page in the AWS IAM Management Console. The left sidebar is identical to the previous screenshot. The main area has a 'Create New Group' button highlighted with a red circle. Below it is a 'Group Actions' dropdown. A 'Filter' input field is present. A table titled 'Showing 1 results' lists one group: 'EC2admingroup' with '0' users, 'Inline Policy' (empty), and 'Creation Time' as '2017-08-15 15:35 UTC+0530'.

To create a group With S3FullAccess

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Set Group Name

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

Group Name: Example: Developers or ProjectAlpha
Maximum 128 characters

Cancel **Next Step**

In Filter type → S3f

Select check box for **AmazonS3FullAccess**

Click on **Next Step** button

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Attach Policy

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

Filter: Policy Type ▾ s3f Showing 2 results

Policy Name	Attached Entities	Creation Time	Edited Time
<input checked="" type="checkbox"/> AmazonS3FullAccess	0	2015-02-07 00:10 UTC...	2015-02-07 00:10 ...
<input type="checkbox"/> AmazonS3FullAccess...	0	2017-06-05 21:24 UTC...	2017-06-05 21:24 ...

Cancel Previous **Next Step**

Click on **Create Group** button

Review

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

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

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

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

Verify EC2admingroup & S3admingrp groups got created

Groups

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

Verify S3 policy is attached

The screenshot shows the AWS IAM Groups page. On the left, a sidebar lists navigation options: Dashboard, Groups (which is selected and highlighted in orange), Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area has tabs for 'Users', 'Permissions' (which is selected and highlighted in orange), and 'Access Advisor'. Under the 'Permissions' tab, there's a section titled 'Managed Policies' with the sub-section 'AmazonS3FullAccess'. A table shows one managed policy:

Policy Name	Actions
AmazonS3FullAccess	Show Policy Detach Policy Simulate Policy

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

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 interface. The left sidebar has 'Users' selected. The main area has a search bar and two buttons: 'Add user' (highlighted with a blue box) and 'Delete user'. Below these are filters for 'User name' and 'Groups'. A message at the bottom states 'There are no IAM users. Learn more'. The URL in the address bar is <https://console.aws.amazon.com/iam/home?region=us-west-2#/users>.

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. At the top, there are navigation links: Services, Resource Groups, student, Global, and Support. Below the header, a progress bar indicates four steps: 1. Details (highlighted in blue), 2. Permissions, 3. Review, and 4. Complete. The main section is titled 'Set user details'. It asks for a user name ('tom') and provides an option to 'Add another user'. A note states: 'You can add multiple users at once with the same access type and permissions.' Below this, the 'Select AWS access type' section is shown. It notes: 'Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step.' It lists two options: 'Programmatic access' (unchecked) and 'AWS Management Console access' (checked). A note for 'AWS Management Console access' says: 'Enables a password that allows users to sign-in to the AWS Management Console.' At the bottom of the page, there are links for Feedback, English, Copyright information (© 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

The screenshot shows the AWS IAM Management Console interface. A user named 'student' is logged in. The 'Resource Groups' tab is selected. A new user named 'tom' is being created. Under the 'AWS Management Console access' section, the 'Custom password' option is selected, and a password is entered. Below it, the 'Require password reset' checkbox is checked. At the bottom right, the 'Next: Permissions' button is highlighted.

Under Group column

Select EC2admingroup

Click on Next Review

The screenshot shows the 'Attached policies' step in the IAM user creation process. It lists two groups: 'EC2admingroup' and 'S3admingrp'. The 'EC2admingroup' checkbox is checked, and its attached policy 'AmazonEC2FullAccess' is listed. At the bottom right, the 'Next: Review' button is highlighted.

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	EC2admin

Create user

Down the .csv file

Success

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

Users with AWS Management Console access can sign-in at: <https://S23251683217.sigin.aws.amazon.com/console>

Download .csv

User	Email login instructions
tom	Send email

Details **Permissions** **Review** **Complete**

Close

Click on **close** button

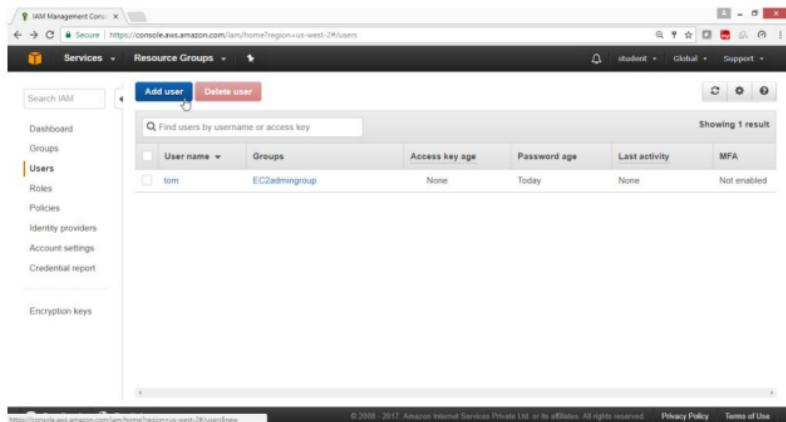
The screenshot shows the AWS IAM Management Console interface. At the top, there's a navigation bar with tabs like 'Services', 'Resource Groups', and 'Complete'. Below the navigation bar, there are four buttons: 'Details', 'Permissions', 'Review', and 'Complete'. A green success message box is displayed, stating: '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. It also mentions that users with AWS Management Console access can sign-in at <https://signin.aws.amazon.com/console>. Below this message, there's a 'Download.csv' button. On the left, there's a sidebar with a 'User' section containing a list item 'tom'. To the right of the user list, there are 'Email login instructions' and a 'Send email' button. In the bottom right corner of the main content area, there is a 'Close' button with a circular arrow icon. At the very 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'.

Scenario 2)

Create user john and join to S3admingroup

Select user

Click on Add user button



The screenshot shows the AWS IAM Management Console. The left sidebar has 'Users' selected. The main area displays a table of users. One user, 'tom', is listed with the following details:

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

At the top of the main area, there are 'Add user' and 'Delete user' buttons. The 'Add user' button is highlighted with a red box.

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

Drag down

User name*

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

Console password* Autogenerated password
 Custom password

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

Click on Next Permission 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**

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

Select S3admingrp

Click on **Next Review** button

The screenshot shows the AWS IAM Management Console. In the top navigation bar, 'Services' is selected under 'Resource Groups'. The main content area displays a table titled 'Attached policies' with two rows. The first row, 'EC2admingrp', has a checkbox next to it and the policy 'AmazonEC2FullAccess'. The second row, 'S3admingrp', also has a checkbox next to it and the policy 'AmazonS3FullAccess'. A blue border surrounds the 'S3admingrp' row. At the bottom right of the table, there are three buttons: 'Cancel', 'Previous', and 'Next: Review'. The 'Next: Review' button is highlighted with a blue border.

Verify user details

Click on **Create user** button

The screenshot shows the 'Create user' step in the AWS IAM Management Console. At the top, a message says 'Review your choices. After you create the user, you can view and download the autogenerated password and access key.' Below this, the 'User details' section is shown with the following settings:

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

Under 'Permissions summary', it states 'The user shown above will be added to the following groups.' A table shows one group entry:

Type	Name
Group	S3admingrp

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create user'. The 'Create user' button is highlighted with a blue border.

Download .csv file

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 'student'. Below the navigation bar, a progress bar shows four steps: 'Details', 'Permissions', 'Review', and 'Complete'. Step 4 is highlighted with a blue circle. The main area displays a 'Success' message: 'You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.' Below this message, it says 'Users with AWS Management Console access can sign-in at: https://523251683217.signin.aws.amazon.com/console'. There's a 'Download.csv' button with a file icon, which is also circled in blue. A table lists a single user named 'User' with the value 'john'. To the right of the table, there are 'Email login instructions' and a 'Send email' button. At the bottom of the page, there are links for 'Feedback', 'English', and 'Close'.

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. The left sidebar has a 'Users' section selected. The main area shows a table with two users: 'john' and 'tom'. The 'Add user' button is highlighted with a mouse cursor. The URL in the browser is <https://console.aws.amazon.com/iam/home?region=us-west-2#users>.

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* Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

Console password* Autogenerated password
 Custom password

 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

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&loginUserNames=sai&passwordType=manual>. The page title is "Add user". The top navigation bar includes "Services", "Resource Groups", "student", "Global", "Support", and tabs for "Details", "Permissions", "Review", and "Complete". The "Permissions" tab is selected. Below it, three options are shown: "Add user to group" (with a group icon), "Copy permissions from existing user" (with a user and document icon), and "Attach existing policies directly" (with a document icon). A note below says: "Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)". At the bottom, there are "Feedback", "English", and links to "Privacy Policy" and "Terms of Use".

In Filter type search for ec2f

Select AmazonEC2FullAccess check box

The screenshot shows the "Attach existing policies directly" step of the IAM wizard. The URL is <https://console.aws.amazon.com/iam/home?region=us-west-2#/users/new?step=permissions&loginUserNames=sai&passwordType=manual&permissionsFilter=ec2f>. The search filter "existing user" is selected. The results table shows two policies:

Policy name	Type	Attachments	Description
AmazonEC2FullAccess	AWS managed	1	Provides full access to Amazon EC2 via the AWS Man...
AmazonEC2FullAcces...	Customer managed	0	Provides full access to Amazon EC2 via the AWS Man...

At the bottom, there are "Create policy", "Refresh", "Feedback", "English", and links to "Privacy Policy" and "Terms of Use".

In Filter type search for s3f

Select AmazonS3FullAccess check box

Click on **Next Review** button

The screenshot shows the AWS IAM Management Console. A policy named 'AmazonS3FullAccess' is selected. The 'Next: Review' button is visible at the bottom.

Verify users detail

Click on Create user button

The screenshot shows the 'Create user' step in the AWS IAM Management Console. The 'User details' section is filled out. The 'Permissions summary' section shows policies attached. The 'Create user' button is highlighted at the bottom.

Download .csv file

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 'student'. Below it, a progress bar shows four steps: 'Details', 'Permissions', 'Review', and 'Complete' (which is highlighted with a blue circle). The main area displays a success message: "Success: You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time." Below this message, a table lists two users: 'User' and 'sai'. For each user, there's a 'Download .csv' button, an 'Email login instructions' link, and a 'Send email' button. At the bottom of the page, there are links for 'Feedback', 'English', and 'Close'.

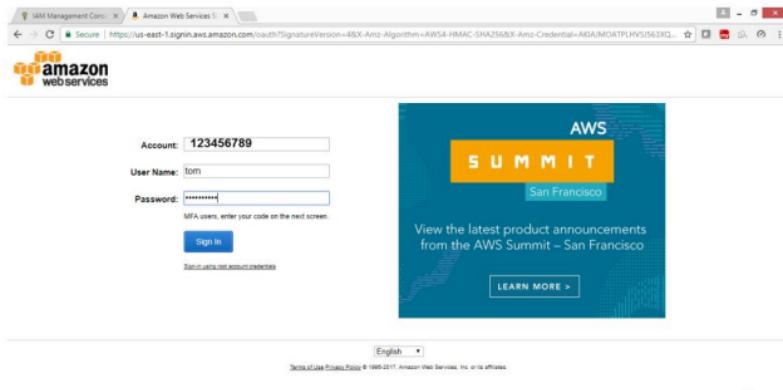
To verify whether users can access particular Service

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

Verification

Error Access Denied

The screenshot shows the AWS S3 Management Console. At the top, it says 'Identify optimal storage classes with S3 Analytics - Storage Class Analysis. Learn More ». Below that, there's a navigation bar with 'Services', 'Resource Groups', and other options. The main area has a red header bar with 'Amazon S3'. It includes buttons for '+ Create bucket', 'Delete bucket', and 'Empty bucket'. A large error message box is displayed, containing a red exclamation mark icon and the text 'Error' followed by 'Access Denied'.

Now select EC2 service

The screenshot shows the AWS Management Console homepage. On the left, there's a sidebar with links to History, S3, Console Home, IAM, CloudFront, VPC, and EC2. The main area has a search bar at the top with placeholder text "Find a service by name or feature (for example, EC2, S3 or VM, storage)." Below the search bar are several service categories represented by icons and lists:

- 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, AWS Glue.
- 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, Managed Services.
- Artificial Intelligence:** Lex, Polly, Rekognition, Machine Learning.
- Messaging:** Simple Queue Service, Simple Notification Service, SES.
- Database:** RDS, DynamoDB.
- Business Productivity:** WorkDocs, WorkMail, Amazon Chime.
- Internet Of Things:** AWS IoT.
- Desktop & App:** (represented by a monitor icon).

Verification

User tom can access EC2 service.

The screenshot shows the EC2 Management Console. In the top navigation bar, it says "EC2 Management Console". The main content area is divided into sections:

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

1 Running Instances	0 Elastic IPs
0 Dedicated Hosts	1 Snapshots
1 Volumes	0 Load Balancers
3 Key Pairs	6 Security Groups
0 Placement Groups	
- Account Attributes:**
 - Supported Platforms: VPC
 - Default VPC: vpc-89c341ee
 - Resource ID length management
- Create Instance:** A section with the text "To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance."
- Additional Information:**
 - [Getting Started Guide](#)
 - [Documentation](#)

At the bottom, there are links for "Feedback", "English", "Privacy Policy", "Terms of Use", and copyright information: "© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved." and the URL "https://docs.amazonaws.net/console/ec2/GetStarted.html".

Similarly check for user john

To Delete users and groups

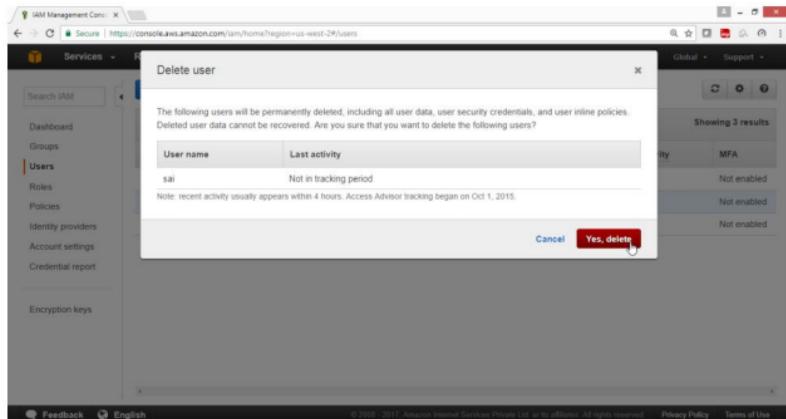
From IAM dashboard, select **Users**

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

Click on **Delete Users** button

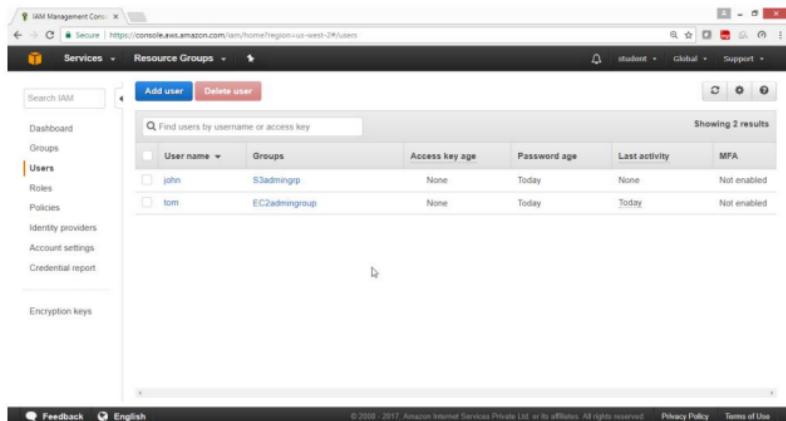
The screenshot shows the AWS IAM Management Console. On the left, there's a sidebar with options like Dashboard, Groups, Users (which is selected and highlighted in orange), Roles, Policies, Identity providers, Account settings, and Credential report. Below that is an Encryption keys section. The main area has tabs for Services (selected) and Resource Groups. At the top right, there are buttons for student, Global, Support, and a bell icon. A search bar says 'Search IAM'. Below it, there's a 'Find users by username or access key' input field. A large red button labeled 'Delete user' is prominently displayed. To its left is a blue button labeled 'Add user'. A table titled 'Showing 3 results' lists three users: John, S3admingrp, None, Today, None, Not enabled; Sai, None, None, Today, None, Not enabled; and Tom, EC2admingroup, None, Today, Today, Not enabled. The 'User name' column has checkboxes, and the 'Sai' checkbox is checked. The entire screenshot is framed by a black border.

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. On the left, there's a sidebar with links like Dashboard, Groups (which is selected), Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main area is titled 'Resource Groups' and shows two groups: 'EC2admingrp' and 'S3admingrp'. A context menu is open over the 'S3admingrp' group, with 'Delete Group' highlighted. The menu also includes 'Add Users to Group', 'Edit Group Name', and 'Remove Users from Group'. At the bottom of the screen, there are links for Feedback, English, and some legal notices.

Click Yes, Delete button

The screenshot shows the AWS IAM Groups page. A modal dialog box is open, prompting the user to confirm the deletion of a group named 'S3admingrp'. The dialog contains the message: 'All users and permissions belonging to the following groups will be removed from the group first. Are you sure you want to delete the following groups?' followed by a list item 'S3admingrp'. At the bottom of the dialog are two buttons: 'Cancel' and a red 'Yes, Delete' button, which is highlighted with a mouse cursor.

Verification

Group is deleted

The screenshot shows the AWS IAM Groups page after the group 'S3admingrp' has been deleted. The table now displays one result: 'EC2admingroup' with 1 user associated with it. The 'Yes, Delete' button from the previous screen is visible at the bottom right of the table area.

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 has a 'Users' section selected. The main area displays a table of users:

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

A blue selection box highlights the row for the user 'tom'. At the top of the main area, there are 'Add user' and 'Delete user' buttons.

Click on Security credentials

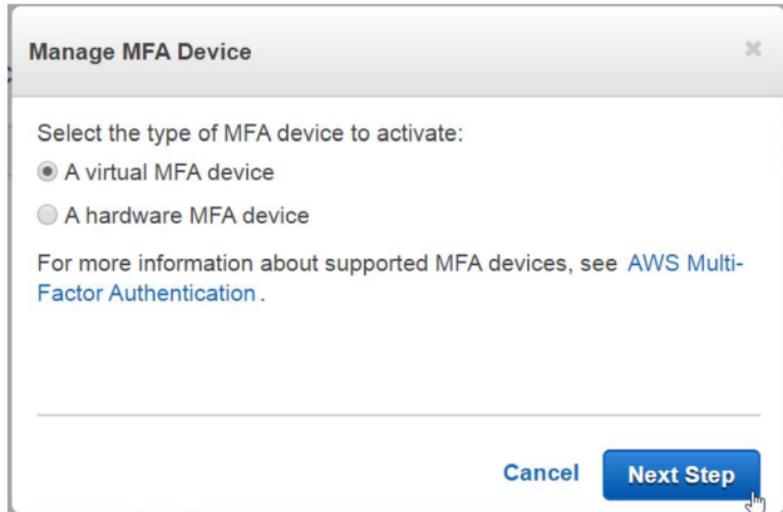
The screenshot shows the AWS IAM Management Console. On the left, there's a sidebar with links like Dashboard, Groups, Users (which is selected), Roles, Policies, Identity providers, Account settings, and Credential report. The main area is titled 'Summary' for the user 'tom'. It shows the User ARN (arn:aws:iam:::user/tom), 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 yellow box), and Access Advisor. Under the Security credentials tab, it says 'Attached policies: 1'. At the bottom, there are fields for Policy name and Policy type.

Click on pen sign for "Assigned MFS device"

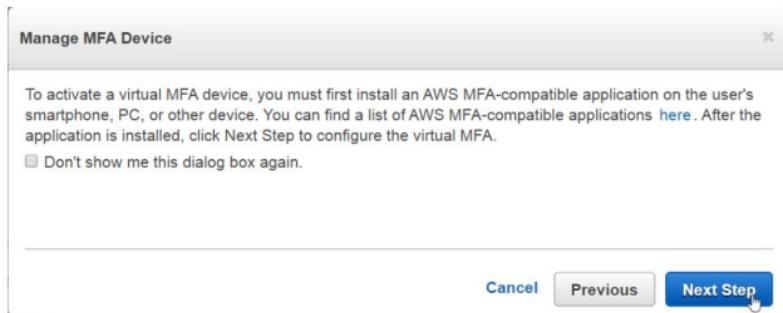
This screenshot is similar to the one above, showing the user 'tom' summary page in the AWS IAM Management Console. The 'Security credentials' tab is selected. In the 'Sign-in credentials' section, there is a row for 'Assigned MFA device' which has a blue edit/pencil icon next to the value 'No'. The rest of the page includes sections for Path (/), Creation time (2017-08-15 22:09 UTC+0530), and other tabs for Permissions, Groups (1), and Access Advisor.

Select → “A virtual MFA device”

Click on **Next Step** button



Click on **Next Step** button



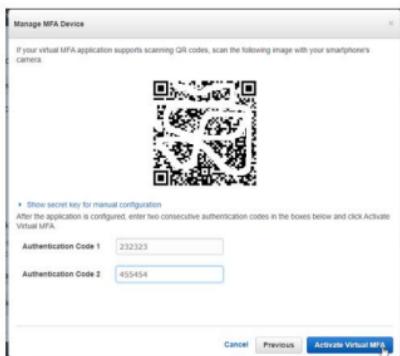
Bar code will be created

Scan this bar code from your mobile Google Authenticator application.

Now type 6 digit bar code in Authentication code 1

Once the bar code changes

Retype 6 digit bar code in Authentication code 2



Click on Finish



Now login as tom user

A screenshot of a web browser showing the AWS Management Console login screen. The URL in the address bar is https://us-west-2.signin.aws.amazon.com/. The page features the AWS logo and fields for "Account" (123456789), "User Name" (tom), and "Password". Below these fields is a link for "MFA users, enter your code on the next screen." A "Sign In" button is centered below the password field. To the right of the login form is a promotional banner for the "AWS SUMMIT San Francisco". The banner includes the text "View the latest product announcements from the AWS Summit – San Francisco" and a "LEARN MORE >" button. At the bottom of the page, there are links for "English", "Terms of Use", "Privacy", and "© 1999-2017, Amazon Web Services, Inc. or its affiliates".

https://us-west-2.signin.aws.amazon.com/.auth?SignatureVersion=4&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIMQATPjHVS5GZIQ&X-Amz-Date=2017-08-15T17%3A46%3A06.042Z&X-Amz-Signature=7d6497161f96fa057

Once the user types the MFA 6 digit code

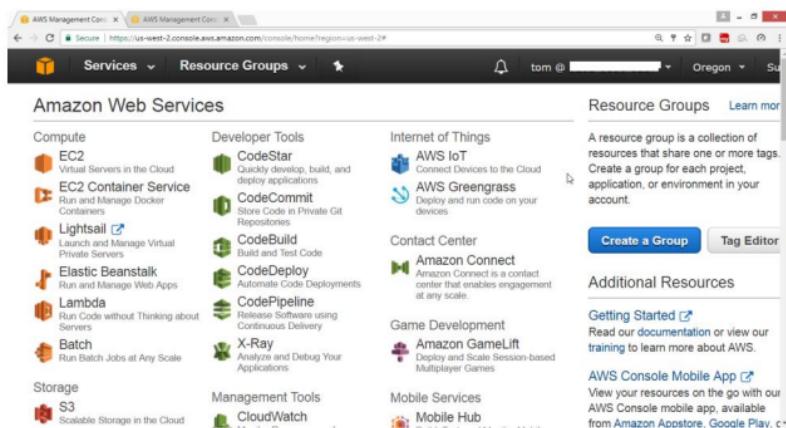
Click on submit



The screenshot shows the AWS Multi-factor Authentication sign-in page. At the top, there's a logo for "amazon web services". Below it, the title "Multi-factor Authentication" is displayed. A sub-instruction "Please enter an MFA code to complete sign-in." is present. A text input field contains the MFA code "132432". Below the input field are two buttons: "Submit" (highlighted in blue) and "Cancel". At the bottom of the page, there's a language selection dropdown set to "English" and a small footer note: "Developer Terms | Privacy | © 1999-2017, Amazon Web Services, Inc. or its affiliates."

<https://us-west-2.console.aws.amazon.com/auth/Tsignature?version=48X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJQATHV5G63Q8X&X-Amz-Date=2017-08-15T17%3A40%3A06.024Z&X-Amz-Signature=7i6497161ef9f6ad37>

Verify user had successfully logged in.



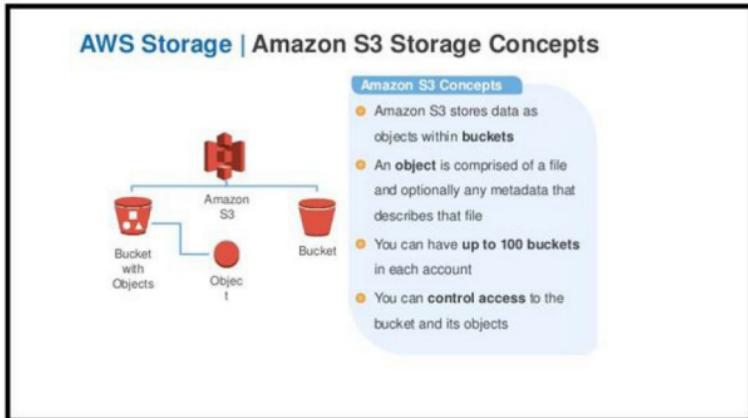
The screenshot shows the AWS Management Console Home Page. The top navigation bar includes links for "AWS Management Console", "AWS Management Console", "Services", "Resource Groups", and a user profile for "tom". The main content area is titled "Amazon Web Services". It features several service categories with icons and links: Compute (EC2, EC2 Container Service, Lightsail, Elastic Beanstalk, Lambda, Batch), Developer Tools (CodeStar, CodeCommit, CodeBuild, CodeDeploy, CodePipeline, X-Ray), Internet of Things (AWS IoT, AWS Greengrass), Contact Center (Amazon Connect), Game Development (Amazon GameLift), Management Tools (CloudWatch), and Mobile Services (Mobile Hub). On the right side, 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 a "Getting Started" link and a "AWS Console Mobile App" link.

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. On the left, there's a sidebar with 'History' and links to various AWS services like DynamoDB, RDS, EC2, CloudWatch, and Simple Notification Service. The 'Storage' section is expanded, showing 'S3' as the selected service. Other options in 'Storage' include 'Amazon FSx', 'Glacier', and 'Storage Gateway'. Below 'Storage' are 'Database' services like Amazon RDS, Amazon Aurora, Amazon Neptune, and Amazon DynamoDB. The main content area has a search bar at the top: 'Find a service by name or feature (example, EC2, S3 or VM, storage)'. It's divided into several categories: 'Compute' (EC2, 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), 'Messaging' (Simple Queue Service, Simple Notification Service, SES), 'Management Tools' (CloudWatch, CloudFormation, CloudTrail, Config, OpsWorks, Service Catalog, Trusted Advisor), 'Artificial Intelligence' (Lex, Polly, Rekognition, Machine Learning), and 'Business Productivity' (WorkDocs, WorkMail, Amazon Chime). At the bottom, there's a 'CloudWatch Metrics' section.

On Amazon S3 page

Click on **Create Bucket**

The screenshot shows the AWS S3 Management Console. At the top, it says 'Identify optimal storage classes with S3 Analytics - Storage Class Analysis. Learn More ». Documentation' and has links for 'Switch to the old console', 'Discover the new console', and 'Quick tips'. Below that is the 'Amazon S3' logo and a search bar with 'Search for buckets'. There are three buttons: '+ Create bucket', 'Delete bucket', and 'Empty bucket'. To the right, it shows '4 Buckets' and '2 Regions'. A table lists four buckets: 'alitjune' (Region: US West (Oregon), Date created: Jul 3, 2017 8:17:52 PM), 'elasticbeanstalk-us-west-2-523251683217' (Region: US West (Oregon), Date created: Jul 12, 2017 9:30:22 PM), 'srikanthhyd' (Region: US West (Oregon), Date created: Apr 13, 2017 5:46:10 PM), and 'www.cfameerpet.com' (Region: Asia Pacific (Singapore), Date created: Aug 11, 2017 8:34:03 PM).

Bucket name	Region	Date created
alitjune	US West (Oregon)	Jul 3, 2017 8:17:52 PM
elasticbeanstalk-us-west-2-523251683217	US West (Oregon)	Jul 12, 2017 9:30:22 PM
srikanthhyd	US West (Oregon)	Apr 13, 2017 5:46:10 PM
www.cfameerpet.com	Asia Pacific (Singapore)	Aug 11, 2017 8:34:03 PM

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

Provide following values

Bucket Name → saleshydbucket

Region → Oregon

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

Create a Bucket - Select a Bucket Name and Region

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

Bucket Name: saleshydbucket1

Region: Oregon

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

Verify that bucket is created.

The screenshot shows the AWS Management Console interface for creating a new S3 bucket. On the left, there's a sidebar with 'Services' and 'Resource Groups'. The main area has tabs for 'Create Bucket' (which is selected), 'Actions', and 'Switch to new console'. Below these are buttons for 'None', 'Properties', and 'Transfers'. A list titled 'All Buckets (4)' shows existing buckets: 'cloudtrialhari', 'ctrilabc', 'saleshydbucket1' (which is highlighted with a blue selection bar), and 'srikanthhyd'. To the right, a detailed view for the selected bucket 'Bucket: saleshydbucket1' is displayed. It shows the bucket's name, region (Oregon), creation date (Tue Aug 15 08:00:06 GMT+530 2017), and owner (skmv@99). There are also links for 'Permissions', 'Static Website Hosting', 'Logging', 'Events', and 'Versioning'.

To upload files of any type

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

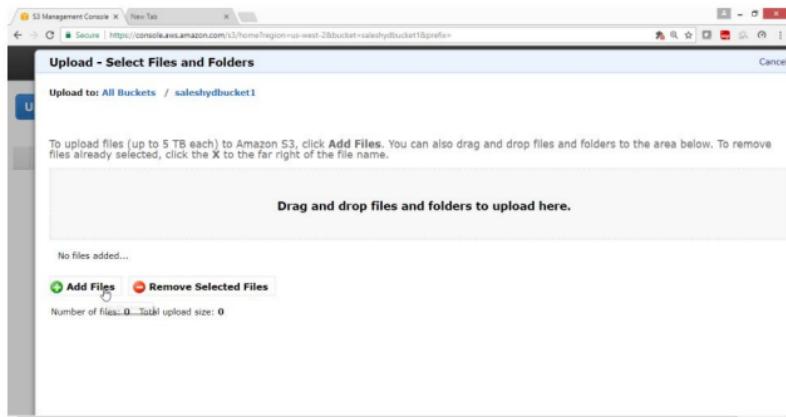
Note: 5 GB can be uploaded

It will be charged if crossed free tier usage.

Click on Created bucket

The screenshot shows the AWS S3 Management Console interface. In the top navigation bar, there are tabs for 'Services', 'Resource Groups', and other account details. Below the navigation, there are buttons for 'Create Bucket', 'Actions', 'None', 'Properties', and 'Transfers'. A link to 'Switch to new console' is also present. On the left, a sidebar lists 'All Buckets (4)' with names: 'cloudtrialhari', 'ctrilabc', 'saleshydbucket1' (which is selected and highlighted in blue), and 'srikanthhyd'. The main content area is titled 'Bucket: saleshydbucket1' and displays the following details:
Bucket: saleshydbucket1
Region: Oregon
Creation Date: Tue Aug 15 08:00:06 GMT+530 2017
Owner: skmvall999
Below these details, there are several expandable sections: 'Permissions', 'Static Website Hosting', 'Logging', 'Events', and 'Versioning'.

Click on Add files

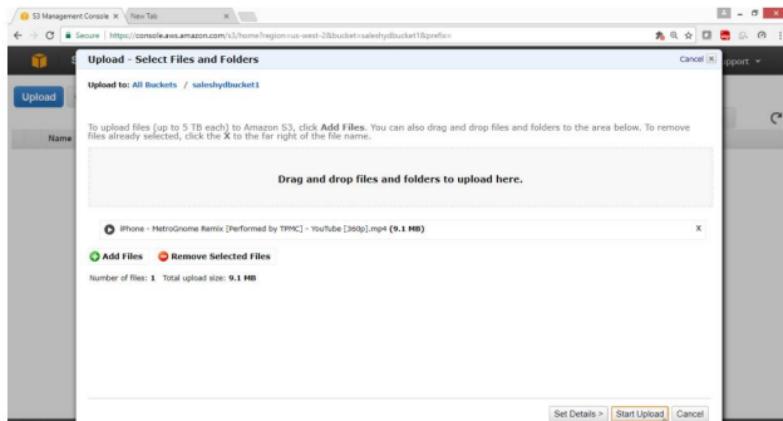


In the upload Wizard

Click on **Add files**

Select some txt, pdf, video files

Click "start upload" button



Verify that the file got uploaded.

S3 Management Console < New Tab

Services Resource Groups

Upload Create Folder Actions

Search by prefix

Switch to new console

Name Storage Class Size Last M

iPhone - MetroGnome Remix [Perf... Standard 9.1 MB Tue Aug

Transfers

Automatically clear finished transfers

Select the file, Click on Properties on Right Panel,

Click on the link

S3 Management Console < New Tab

Services Resource Groups

Upload Create Folder Actions

Search by prefix

Switch to new console None Properties Transfers

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

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

Bucket: saleshybucket1
Name: iPhone - MetroGnome Remix [Performed by TPMYC] - YouTube [950].mp4
Last Modified: Tue Aug 15 08:04:56 GMT+530 2017
Owner: skmval999
File Type: video/mp4
Expires: Never
Expiration Rule: None

Details Permissions Metadata Tags

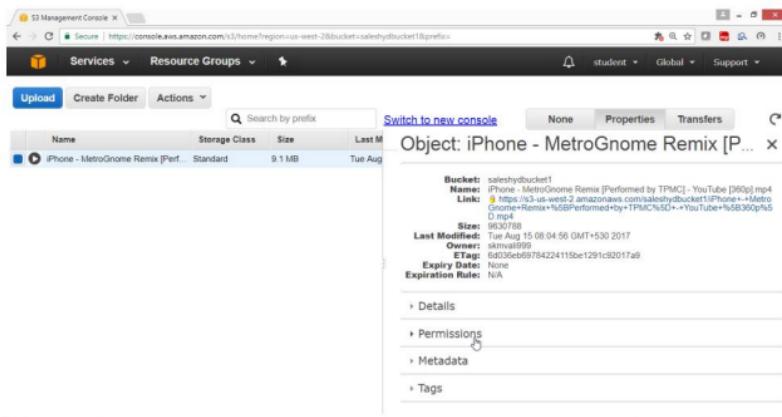
Verification : Cannot access due to lack of permission

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>572AA441F3766B385</RequestId>
  <HostId>
    1Pz8E0Qestv0USxIMM54p6jy2pJt7zHwT1QYmZPiIjg/7dW+UT/t/F0xR9VrUTeBlqjlyEqbQ=
  </HostId>
</Error>
```

To allow users to Download, or view give permission

Select, Permission tag



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

Drop down Grantee Button

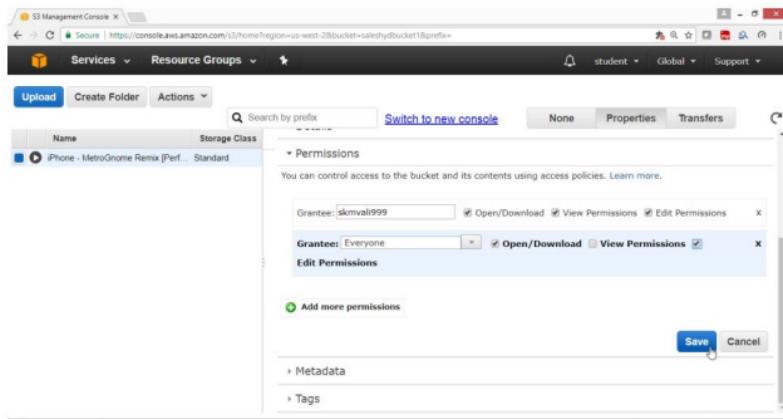
Select **Everyone** to make it public

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

Enable the check box to **View Permission**

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

Click on **Save** button



Verify file is accessible.

The screenshot shows the AWS S3 Management Console interface. A file named "iPhone - MetroGnome Remix [Performed by TPMC] [300x300].mp4" is selected. The file's thumbnail image is a black grid with white dots, representing a video frame. The file details pane on the right shows the full path: "https://s3-us-west-2.amazonaws.com/saleshybucket1/iPhone - MetroGnome Remix [Performed by TPMC] [300x300].mp4". Below the file name 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 interface again. A file named "iPhone - MetroGnome Remix [Performed by TPMC] [300x300].mp4" is selected. A context menu is open over the file, with the "Copy" option highlighted. The menu also includes options like Open, Download, Make Public, Rename, Delete, and Initiate Restore.

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 tabs for 'Services' and 'Resource Groups'. Below the navigation bar, a search bar says 'Switch to new console'. To the right of the search bar are buttons for 'None' and 'Properties'. A dropdown menu is open, showing 'Create Bucket' and 'Actions'. The main area is titled 'All Buckets (5)' and lists five buckets: 'cloudtrialhari', 'trialabc', 'finshydbucket1' (which is highlighted in orange), '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. The URL in the address bar indicates a specific bucket has been selected. The navigation bar and search bar are similar to the previous screenshot. The 'Actions' dropdown menu is open, showing options: 'Upload', 'Create Folder', and 'Paste'. The 'Paste' option is highlighted in orange. Below the dropdown, a message says 'The bucket 'finshydbucket1' is empty'. A large, semi-transparent black box covers the bottom half of the screen, obscuring the file list.

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

The screenshot shows the AWS S3 Management Console interface. The left sidebar shows 'All Buckets / finshydbucket1'. The main area lists a single file: 'iPhone - MetroGnome Remix [Performed by TP...]' with a size of '9.1 MB' and 'Last Modified' on 'Tue Aug 15 08:23:54 GMT+530 2017'. A context menu is open over this file, with the 'Delete' option highlighted.

3) To delete a file from a bucket

Right click on it, select Delete

The screenshot shows the AWS S3 Management Console interface. The left sidebar shows 'All Buckets / finshydbucket1'. The main area lists a single file: 'iPhone - MetroGnome Remix [Performed by TP...]' with a size of '9.1 MB' and 'Last Modified' on 'Tue Aug 15 08:23:54 GMT+530 2017'. A context menu is open over this file, with the 'Delete' option highlighted.

To Delete a bucket

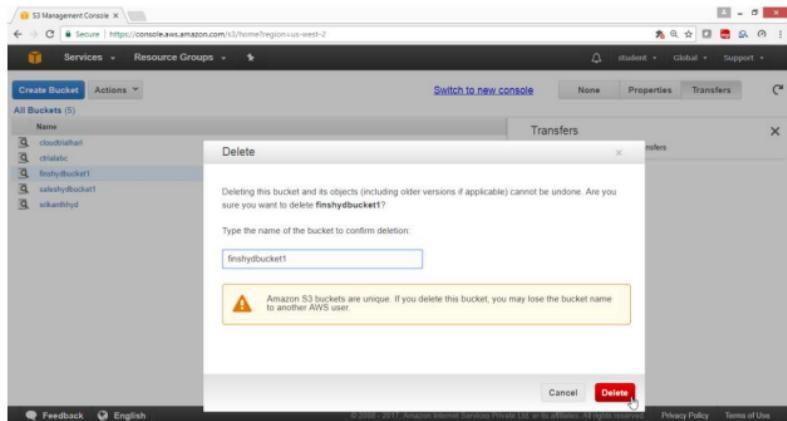
Select the bucket, right click select **Delete Bucket**

The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with tabs for 'Services' and 'Resource Groups'. Below the navigation bar, a main content area displays a table titled 'All Buckets (5)'. The table has a column header 'Name' and lists five buckets: 'cloudtrialhari', 'ctrialabc', 'finshydbucket1', 'saleshydbucket1', and 'srikanthhy'. To the right of the table, there's a sidebar titled 'Transfers' with an option to 'Automatically clear fin'. A context menu is open over the 'srikanthhy' bucket, listing options: 'Create Bucket...', 'Delete Bucket' (which is highlighted in orange), 'Empty Bucket', 'Paste Into', and 'Properties'. The URL in the browser address bar is <https://console.aws.amazon.com/s3/home?region=us-west-2>.

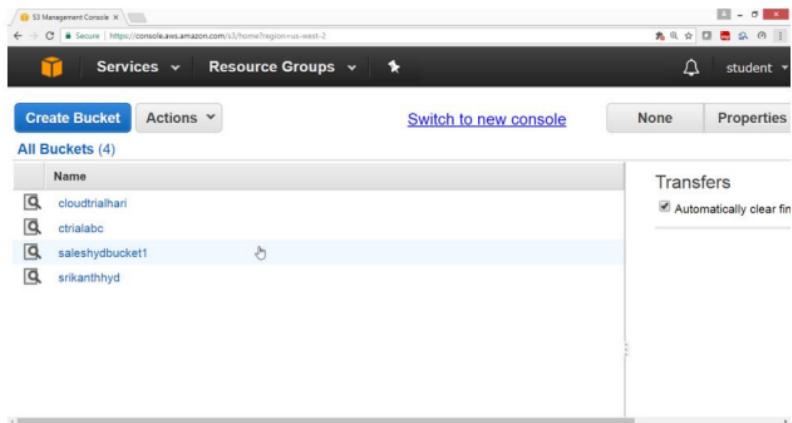
To Delete Bucket

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 tabs for 'Services' and 'Resource Groups'. On the right side of the header, there's a user profile section labeled 'student'. Below the header, there are two main buttons: 'Create Bucket' and 'Actions'. To the right of these buttons is a link 'Switch to new console'. Further to the right are 'None' and 'Properties' buttons. The main content area is titled 'All Buckets (4)' and contains a table with four rows. The columns are 'Name' and 'Transfers'. The 'Name' column lists bucket names: '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	

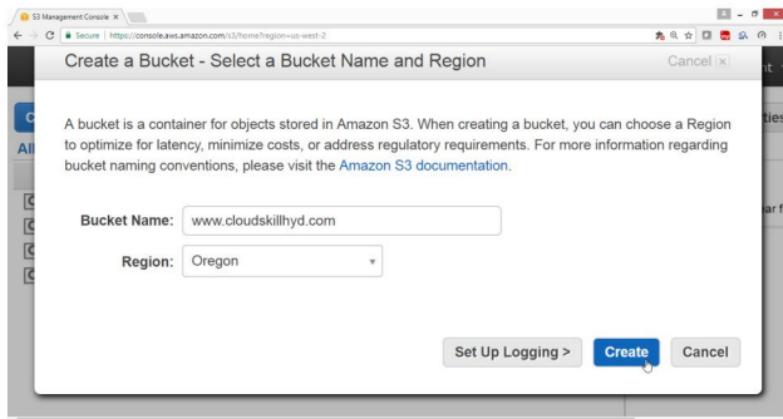
On "Create a Bucket - Select a Bucket Name and Region" page

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 with the URL <https://console.aws.amazon.com/s3/home?region=us-west-2>. The top navigation bar includes 'Services', 'Resource Groups', and a user dropdown for 'student'. Below the navigation is a toolbar with 'Create Bucket', 'Actions', 'Switch to new console', 'None', and 'Properties' buttons. A link 'All Buckets (4)' is visible. The main content area displays a table with columns 'Name' and 'Actions'. The buckets listed are: cloudtrialhari, ctrialabc, saleshydbucket1, srikanthyd, and www.cloudskillhyd.com. On the right side, there is a 'Transfers' section with a checkbox for 'Automatically clear finished transfers'.

Upload all website contents in this bucket.

The screenshot shows the AWS S3 Management Console with the URL <https://console.aws.amazon.com/s3/home?region=us-west-2&bucket=www.cloudskillhyd.com&prefix=www>. The top navigation bar includes 'Services', 'Resource Groups', and a user dropdown for 'student'. Below the navigation is a toolbar with 'Upload', 'Create Folder', 'Actions', 'Search by prefix', 'Switch to new console', 'None', 'Properties', and 'Transfers' buttons. A link 'All Buckets | www.cloudskillhyd.com' is visible. The main content area displays a table with columns 'Name', 'Storage Class', 'Size', and 'Last Modified'. The objects listed are: 404.html, about-us.html, article.html, articles.html, contact-us.html, css, images, index.html, js, and sitemap.html. All objects are in the Standard storage class, with sizes ranging from 6 KB to 5.3 KB and last modified on Tue Aug 15 08:46:32 GMT+530 2017. On the right side, there is a 'Transfers' section with a checkbox for 'Automatically clear finished transfers'.

Select the bucket and click on properties button

The screenshot shows the AWS S3 Management Console. In the top navigation bar, 'Services' is selected. Below it, 'Resource Groups' is shown. On the left, there's a 'Create Bucket' button and an 'Actions' dropdown. To the right, there are tabs for 'None', 'Properties' (which is highlighted in blue), and 'Transfers'. A bell icon and user information ('student', 'Global', 'Support') are also present. The main area is titled 'All Buckets (4)' and lists four buckets: 'cloudtrialhari', 'ctrlalabc', 'saleshydbucket1', and 'www.cloudskillhyd.com'. On the right side, under 'Transfers', there is a checkbox for 'Automatically clear finished transfers'.

On the **Properties** panel

Click **Static Website Hosting**

Drag Down

This screenshot shows the same AWS S3 Management Console interface as the previous one, but with the 'Properties' tab selected. The 'All Buckets (5)' list includes the previously listed buckets plus 'www.cloudskillhyd.com'. On the right, the 'Properties' panel is expanded to show details for the selected bucket. It displays the bucket name 'www.cloudskillhyd.com', its region 'Oregon', creation date 'Tue Aug 15 08:44:43 GMT+530 2017', and owner 'skmvai999'. Below this, the 'Permissions' and 'Static Website Hosting' sections are visible. The 'Static Website Hosting' section contains a note about hosting static websites and provides the endpoint 'Endpoint: www.cloudskillhyd.com.s3-website-us-west-2.amazonaws.com'. A note at the bottom explains how each bucket serves a website namespace and can route requests to its contents.

Select the **Enable website hosting**

Provide following values for

Index Document box → index.html

Error Document box → 404.html

Click on **Save** button

The screenshot shows the AWS S3 Management Console. On the left, there is a sidebar with 'Services' and 'Resource Groups'. Below it, a list of buckets is shown, including 'ame', 'doutrialhari', 'trialabc', 'jaleshhydbucket1', 'irikanthyd', and 'www.cloudskillhyd.com'. The 'www.cloudskillhyd.com' bucket is selected. On the right, a configuration dialog is open under the 'Properties' tab. It has two main sections: 'Enable website hosting' and 'Edit Redirection Rules'. Under 'Enable website hosting', the 'Index Document' is set to 'index.html' and the 'Error Document' is set to '404.html'. There is also a note about 'Edit Redirection Rules'. Below that, there is an option to 'Redirect all requests to another host name'. At the bottom right of the dialog are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted.

Note down the Endpoint.

The screenshot shows the AWS S3 console interface. In the top navigation bar, there are links for Services, Resource Groups, and a user dropdown for 'student'. Below the navigation, there are buttons for Create Bucket, Actions, and a link to Switch to new console. The main area displays a list of buckets under 'All Buckets (5)'. One bucket, 'www.cloudskilbyd.com', is selected and highlighted with a blue background. To the right of the bucket list, there is a configuration panel for the selected bucket's endpoint.

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

Each bucket serves a website namespace (e.g., "www.example.com"). Requests for your host name (e.g., "example.com" or "www.example.com") can be routed to the contents in your bucket. You can also redirect requests to another host name (e.g., redirect "example.com" to "www.example.com"). See our walkthrough for how to set up an Amazon S3 static website with your host name.

Do not enable website hosting

Enable website hosting

Index Document: index.html

Error Document: 404.html

Edit Redirection Rules You can set custom rules to automatically redirect web page requests for specific content.

Redirect all requests to another host name

Save **Cancel**

At the bottom of the page, there is a footer with links for Feedback, English, © 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved., Privacy Policy, and Terms of Use.

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

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

Click on **Add Bucket Policy**.

The screenshot shows the AWS S3 console. In the top navigation bar, 'Services' is selected. On the left sidebar, 'Create Bucket' is highlighted. The main area displays a list of buckets under 'All Buckets (5)'. The bucket 'www.cloudskillhyd.com' is selected, shown in a larger preview pane on the right.

Bucket: www.cloudskillhyd.com

Bucket: www.cloudskillhyd.com
Region: Oregon
Creation Date: Tue Aug 15 08:44:43 GMT+530 2017
Owner: skmvali999

Permissions

You can control access to the bucket and its contents using access policies. [Learn more](#)

Grantee: skmvali999 **List** **Upload/Delete**
[View Permissions](#) [Edit Permissions](#)

[Add more permissions](#) [Add bucket policy](#) [Add CORS Configuration](#)

Save **Cancel**

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 'Enable website hosting' option is selected. The 'Index Document' field is set to 'index.html' and the 'Error Document' field is set to '404.html'. The URL 'Endpoints: https://www.cloudskillhyd.com.s3-website-us-west-2.amazonaws.com' is displayed above the configuration fields.

Verify the website which is coming from S3 Bucket

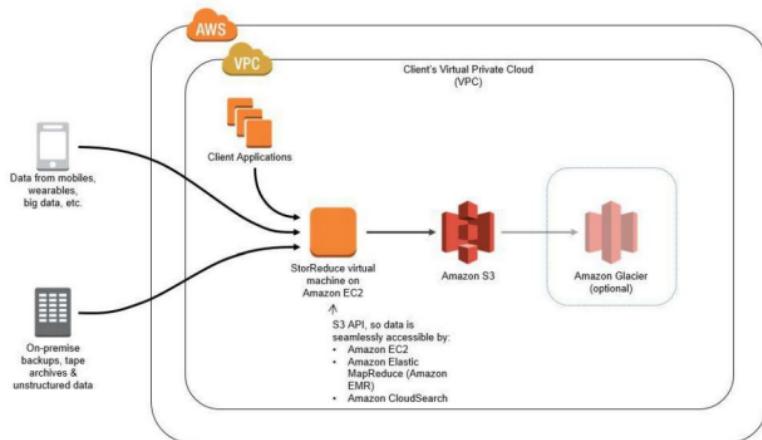
The screenshot shows a web browser displaying the 'Car Club' website template. The page features a dark header with navigation links for HOME, ABOUT, ARTICLES, CONTACTS, SITE MAP, Help, and FAQ. Below the header is a large image of a purple sports car. To the left of the car is a search bar and a 'Latest News' section with two items. To the right of the car is a 'Welcome to Our Club' section with a brief introduction and a list of bullet points. At the bottom of the page, there is a note about the website template's delivery options.

Lab 8: To configure Amazon Glacier

OBJECTIVE

To configure and use AWS Glacier Service.

TOPOLOGY



PRE-REQUISITES

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

To configure Glacier with following task.

Transfer files from S3 to Glacier

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

use s3 or third party tools to archive or restore.

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

Select S3 bucket

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

Select the bucket,

Go to properties

Click on **Lifecycle**

The screenshot shows the AWS S3 Management Console interface. On the left, there's a sidebar with 'Create Bucket' and 'Actions'. Below it, a list of buckets: 'All Buckets (5)' including 'cloudnathan', 'ctrlabc', 'saleshydbucket1', 'sriramhyd', and 'www.cloudskillhyd.com'. The 'www.cloudskillhyd.com' bucket is selected. On the right, a detailed view for this bucket is shown. At the top right of this view, there are tabs: 'None', 'Properties', and 'Transfers'. The 'Properties' tab is selected. In the main area, the 'Bucket' is identified as 'www.cloudskillhyd.com'. Below that, the 'Region' is listed as 'Oregon'. The 'Creation Date' is 'Tue Aug 15 08:44:43 GMT+530 2017' and the 'Owner' is 'skmval999'. A vertical navigation menu on the right lists several options: 'Permissions', 'Static Website Hosting', 'Logging', 'Events', 'Versioning', 'Lifecycle' (which is currently selected), and 'Cross-Region Replication'. The 'Lifecycle' section likely contains the configuration for archiving files to Glacier.

Click on Add rule

The screenshot shows the AWS S3 Management Console interface. In the top navigation bar, there are tabs for 'None', 'Properties', and 'Transfers'. Below the navigation bar, there is a list of buckets: 'All Buckets (5)' including 'cloudrathan', 'cratabc', 'saileshybucket1', 'srikanthyd', and 'www.cloudskillhyd.com'. On the right side of the screen, a modal window titled 'Add rule' is open. The modal contains a note about enabling Versioning and a section for 'Lifecycle Rules' with several options: 'Cross-Region Replication', 'Tags', 'Requester Pays', 'Transfer Acceleration', and 'Storage Management'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Under Lifecycle Rules

select **Choose Rule Target**

Apply the Rule to → Whole Bucket

The screenshot shows the 'Lifecycle Rules' configuration dialog. On the left, there are three steps: 'Step 1: Choose Rule Target', 'Step 2: Configure Rule', and 'Step 3: Review and Name'. On the right, under 'Apply the Rule to:', there are two options: 'Whole Bucket: www.cloudskillhyd.com' (selected) and 'A Prefix: e.g. MyFolder/ or MyObject'. At the bottom right of the dialog is a 'Configure Rule >' button.

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

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

click on **Review**

How to add multiple do... 53 Management Console

Services Resource Groups

Lifecycle Rules

Step 1: Choose Rule Target Step 2: Configure Rule Step 3: Review and Name

Transition to Standard - Infrequent Access Storage Class Days after the object's creation date
Standard - Infrequent Access has a 30-day minimum retention period and a 120KB minimum object size. Lifecycle policy will not transition objects that are less than 120KB. Refer here to learn more about Standard - Infrequent Access

Archive to the Glacier Storage Class 7 Days after the object's creation date
This rule could reduce your storage costs. Refer here to learn more about Glacier pricing. Note that objects archived to the Glacier Storage Class are not immediately accessible.

Permanently Delete 372 Days after the object's creation date

EXAMPLE:

August 15, 2017 (Day 0) → Object Uploaded → August 22, 2017 (Day 7) → Rule Archive to Glacier → Object Storage Class Glacier → August 22, 2018 (Day 372) → Rule Expire → Object Deleted

Action on Incomplete Multipart Uploads

< Set Target Review >

Provide Rule Name → Testbackup

click on “Create and Activate Rule” button

How to add multiple do... 53 Management Console

Services Resource Groups

Lifecycle Rules

Step 1: Choose Rule Target Step 2: Configure Rule Step 3: Review and Name

Rule Name: Testbackup (Optional)

Rule Target
This rule will apply to the whole bucket: www.cloudskillhyd.com

Rule Configuration

Action on Objects

Archive to the Glacier Storage Class 7 days after the object's creation date.
This rule could reduce your storage costs. Refer here to learn more about Glacier pricing. Note that objects archived to the Glacier Storage Class are not immediately accessible.

Permanently Delete 372 days after the object's creation date
As versioning is not enabled, lifecycle delete rule will permanently delete the objects with no recovery.

Create and Activate Rule

Click on Save button

The screenshot shows the AWS S3 Management Console with the 'Lifecycle' tab selected. A lifecycle rule named 'Testbackup' is configured to move objects to the 'Standard-Infrequent Access' storage class after 30 days. The 'Enabled' checkbox is checked. A 'Save' button is highlighted with a red circle.

Verify Storage Class is Standard

The screenshot shows the AWS S3 Management Console displaying the contents of a bucket. The table lists files such as 404.html, about-us.html, article.html, articles.html, contact-us.html, css, images, index.html, js, and sitemap.html. All files are listed under the 'Standard' storage class column.

Name	Storage Class	Size	Last Modified
404.html	Standard	6 KB	Tue Aug 15 08:46:32 GMT+05:30 2015
about-us.html	Standard	5.8 KB	Tue Aug 15 08:46:33 GMT+05:30 2015
article.html	Standard	5.3 KB	Tue Aug 15 08:46:34 GMT+05:30 2015
articles.html	Standard	4.8 KB	Tue Aug 15 08:46:34 GMT+05:30 2015
contact-us.html	Standard	4.7 KB	Tue Aug 15 08:46:35 GMT+05:30 2015
css	--	--	--
images	--	--	--
index.html	Standard	6 KB	Tue Aug 15 08:46:36 GMT+05:30 2015
js	--	--	--
sitemap.html	Standard	4.8 KB	Tue Aug 15 08:46:37 GMT+05:30 2015

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

The screenshot shows the AWS S3 Management Console interface. At the top, there are tabs for 'Services' (selected), 'Resource Groups', and other account information like 'student', 'Global', and 'Support'. Below the tabs, there's a search bar with 'Search by prefix' and a button 'Switch to new console'. A toolbar includes 'Upload', 'Create Folder', 'Actions', 'Versions', 'Hide', and 'Show'. There are also buttons for 'None', 'Properties', and 'Transfers'. A table lists two objects:

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

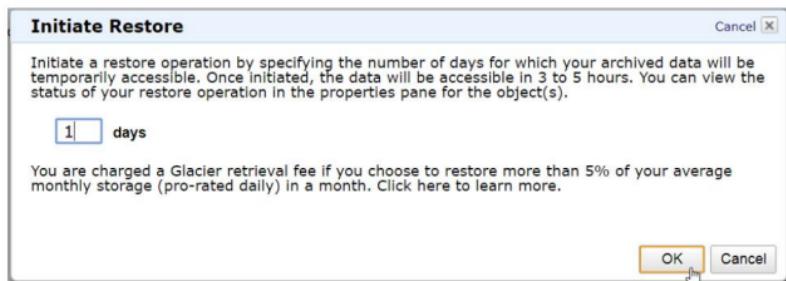
To Restore go to the bucket select the file

Right click and select **Initiate Restore**

The screenshot shows the AWS S3 Management Console interface. A file named "How I Lowered My Cholesterol From 266 to 151 Without Drugs - YouTube (360p).mp4" is selected and listed in the main pane. The file is in the "Glacier" storage class, has a size of 6.4 MB, and was last modified on Thu Apr 13 20:37:27 GMT+5. A context menu is open over the file, with the "Initiate Restore" option highlighted in red. Other options visible in the menu include Open, Download, Make Public, Rename, Delete, Cut, and Copy.

Provide number of days → 1

Click on OK



Verify

File will get restored after 1 Day

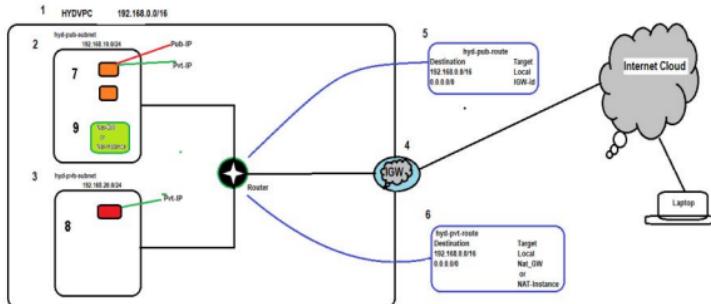
Storage class will become Standard.

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

The screenshot shows the AWS Management Console with the URL <https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2#>. The left sidebar has a tree view of services under 'Networking & Content Delivery'. The 'VPC' service is highlighted with a yellow box. Other services listed include CloudFront, Direct Connect, Route 53, AWS WAF, and others. The right side of the screen displays a grid of service cards with icons and brief descriptions. A banner at the top right says 'Explore the next generation of AWS cloud capabilities. See what's new.' and shows an 'Updated: Jul 28, 2017, 4:49:00 AM GMT+5:30' timestamp.

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		dhcp-e404ff180

Select a VPC above

https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#vpc: © 2018 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

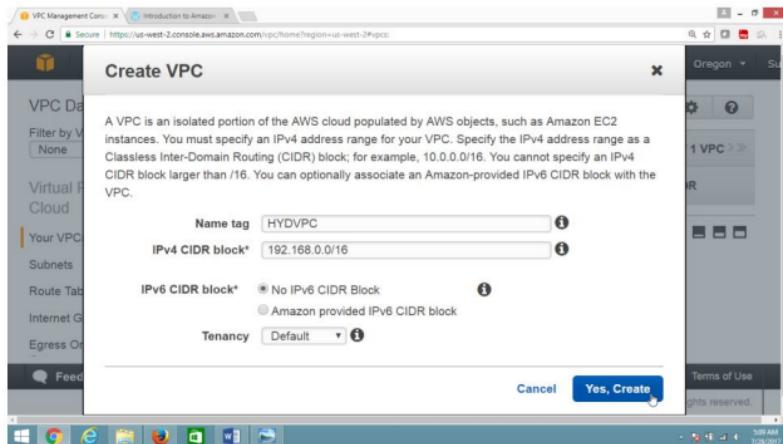
On "Create VPC", page

For Name tag → HYDVPC

For IPv4 CIDR block → 192.168.0.0/16

Leave remaining field as default

Click on "Yes Create" button



Verify

HYDVPN is created

VPC Management Cons... Introduction to Amazon... https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#vpcs:

Services Resource Groups

Create VPC Actions

Search VPCs and their properties

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

vpc-7d934d1b | HYDVPN

Summary Flow Logs Tags

VPC ID: vpc-7d934d1b Network ACL: acl-
acl-7d934d1b

Feedback English Privacy Policy Terms of Use

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

2) To create public subnet

Click on **Subnet**

Click on **Create Subnet** button

VPC Management Cons... Introduction to Amazon... https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#subnets:

Services Resource Groups

Create Subnet Subnet Actions

Search Subnets and their properties

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

Select a subnet above

Feedback English Privacy Policy Terms of Use

https://us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#subnets

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

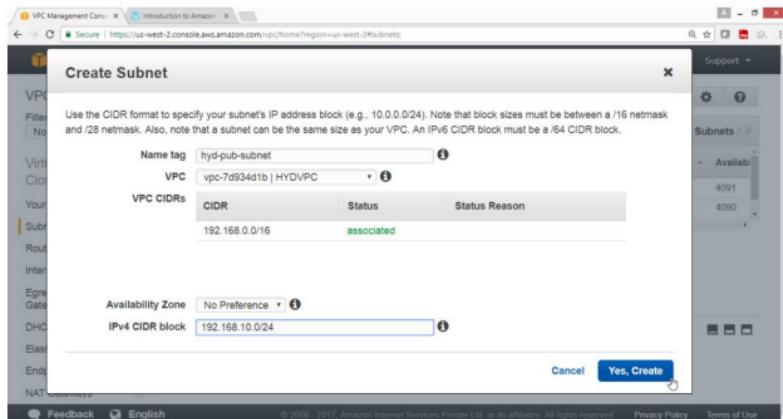
On Create Subnet, page

For Name tag → hyd-pub-subnet

For VPC → HYDVPC

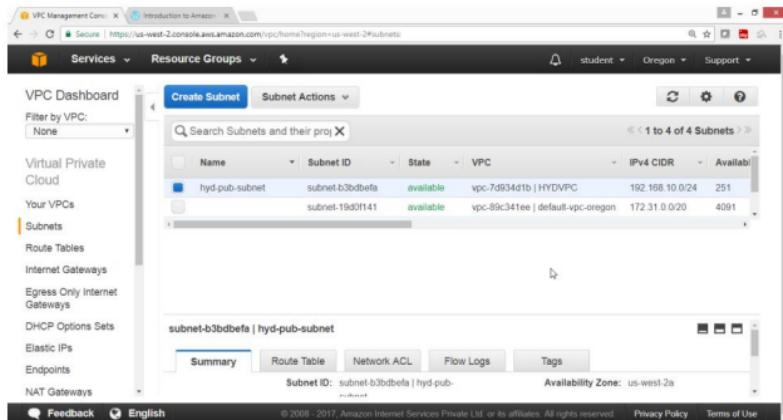
For IPv4 CIDR block → 192.168.10.0/24

Click on Yes Create button



Verify

hyd-pub-subnet got created



The screenshot shows the AWS VPC Management Console. In the left sidebar, under 'Your VPCs', 'Subnets' is selected. The main area displays a table of subnets. A new subnet, 'hyd-pub-subnet' (subnet-b3bdbefb), has been added and is listed with the following details:

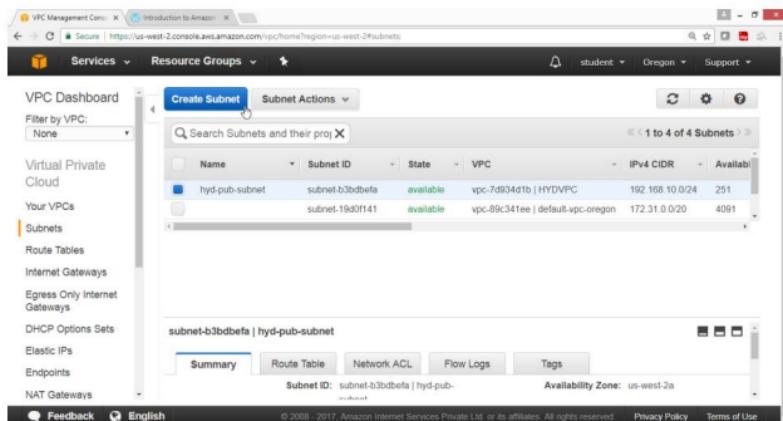
Name	Subnet ID	State	VPC	IPv4 CIDR	Available
hyd-pub-subnet	subnet-b3bdbefb	available	vpc-7d934d1b HYDVPC	192.168.10.0/24	251
	subnet-19d0f141	available	vpc-89c341ee default-vpc-oregon	172.31.0.0/20	4091

Below the table, a detailed view of the 'hyd-pub-subnet' is shown. The 'Summary' tab is selected, displaying the subnet ID as 'subnet-b3bdbefb | hyd-pub-' and the availability zone as 'us-west-2a'.

3) To create private subnet

Click on **Subnet**

Click on **Create Subnet** button



The screenshot shows the AWS VPC Management Console. The 'Create Subnet' button in the top navigation bar is highlighted with a red circle. The rest of the interface is identical to the previous screenshot, showing the list of existing subnets and the detailed view of the 'hyd-pub-subnet'.

On Create Subnet, page

For Name tag → hyd-pvt-subnet

For VPC → HYDVPC

For IPv4 CIDR block → 192.168.20.0/24

Click on Yes Create button



Verify

hyd-pvt-subnet got created

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with options like VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The 'Subnets' option is selected. The main area has a table titled 'Create Subnet' with columns: Name, Subnet ID, State, VPC, IPv4 CIDR, and Available. There are 5 subnets listed:

Name	Subnet ID	State	VPC	IPv4 CIDR	Available
hyd-pvt-subnet	subnet-6abcbf23	available	vpc-7df034d1b HYDVPC	192.168.20.0/24	251
hyd-pub-subnet	subnet-b3bdfbfa	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-1380e5a		available	vpc-89c341ee default-vpc-oregon	172.31.32.0/20	4090
subnet-89e03bec		available	vpc-89c341ee default-vpc-oregon	172.31.16.0/20	4091

Below the table, a specific subnet is selected: 'subnet-6abcbf23 | hyd-pvt-subnet'. The 'Summary' tab is active, showing the Subnet ID as 'subnet-6abcbf23 | hyd-pvt-' and the Availability Zone as 'us-west-2a'. Other tabs include Route Table, Network ACL, Flow Logs, and Tags.

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

In VPC Dashboard panel

Click on Internet Gateway

This screenshot is identical to the one above, showing the AWS VPC Management Console. The 'Internet Gateways' link in the sidebar is highlighted with a blue arrow. The main content area displays the same subnet list and the selected subnet details for 'hyd-pvt-subnet'.

Click on **Create Internet Gateway** button

The screenshot shows the AWS VPC Management Console. On the left sidebar, under the 'Internet Gateways' section, the 'Create Internet Gateway' button is highlighted with a cursor. The main pane displays a table of existing Internet Gateways, with one entry visible: 'igw-6ea7f10a' attached to 'vpc-89c34fee | default-vpc-oregon'. Below the table, there's a section titled 'Select an Internet gateway above' with three small icons.

In **Create Internet Gateway**, box

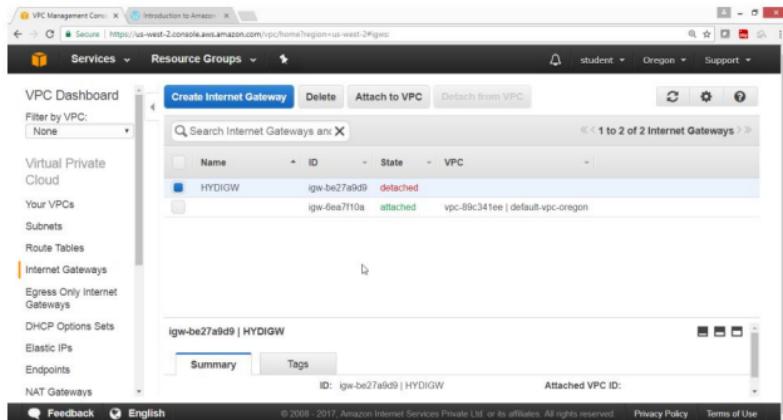
For **Name tag** → HYDIGW

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

This screenshot shows the 'Create Internet Gateway' dialog box. It contains a brief description: 'An Internet gateway is a virtual router that connects a VPC to the Internet.' Below this, the 'Name tag' field is populated with 'HYDIGW'. At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Yes, Create', with the latter being highlighted by a cursor.

Verify

Internet gateway is created

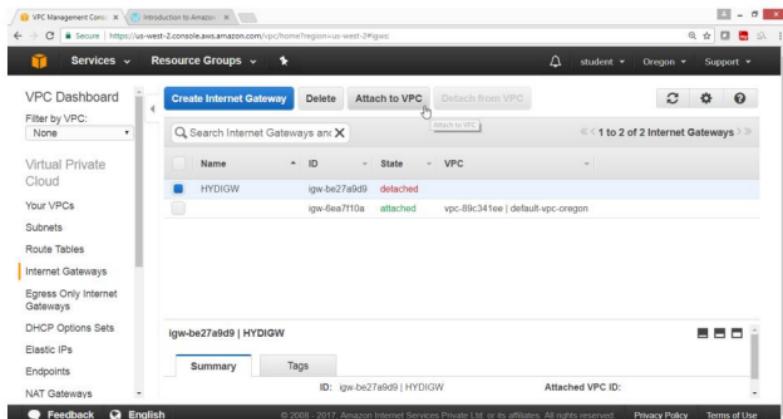


The screenshot shows the AWS VPC Management Console. In the left sidebar, under the 'Internet Gateways' section, there is a single entry: 'HYDIGW'. This entry is highlighted with a blue selection bar. To the right of the table, a modal window titled 'igw-be27a9d9 | HYDIGW' is open, showing the 'Summary' tab. The summary table includes columns for ID, State, and Attached VPC ID. The ID is 'igw-be27a9d9', the state is 'detached', and the Attached VPC ID is 'None'.

Name	ID	State	VPC
HYDIGW	igw-be27a9d9	detached	
	igw-bea7f10a	attached	vpc-89c341ee default-vpc-oregon

Select HYDIGW

Click "Attach to VPC"



This screenshot is identical to the one above, showing the AWS VPC Management Console. The 'HYDIGW' internet gateway is selected. A mouse cursor is hovering over the 'Attach to VPC' button in the top navigation bar of the modal window.

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 left sidebar lists 'Virtual Private Cloud', 'Your VPCs', 'Subnets', 'Route Tables', and 'Internet Gateways' (which is highlighted). The main area displays a table of 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 of the first Internet Gateway (igw-be27a9d9) is shown with tabs for 'Summary' (selected) and 'Tags'. The summary includes the ID, name, and attached VPC information.

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. In the left sidebar, under 'Route Tables', the 'Internet Gateways' option is selected. The main area displays a table of Internet Gateways:

Name	ID	State	VPC
HYDIGW	igw-be27af9d9	attached	vpc-7d934d1b HYDVPN
	igw-6ea7f10a	attached	vpc-89c341ee default-vpc-oregon

Below the table, a specific gateway is selected: 'igw-be27af9d9 | HYDIGW'. The 'Summary' tab is active, showing the ID 'igw-be27af9d9 | HYDIGW' and the attached VPC 'vpc-7d934d1b | HYDVPN'.

Click on "Create Route table" button

The screenshot shows the AWS VPC Management Console. In the left sidebar, under 'Route Tables', the 'Create Route Table' button is highlighted. The main area displays a table of existing Route Tables:

Name	Route Table ID	Explicitly Associated Subnets	Main	VPC
	rtb-1996c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYDVPN

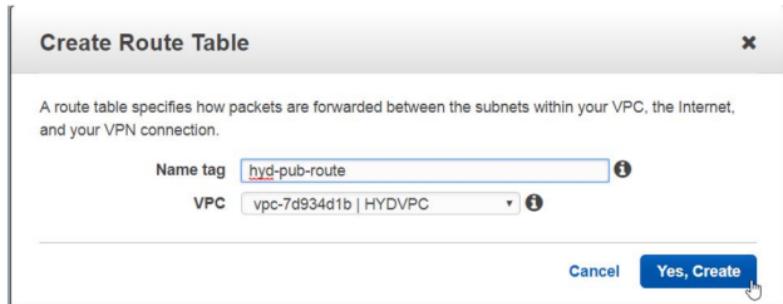
A message at the bottom says 'Select a route table above'.

On "Create Route Table" box

For Name tag → hyd-pub-route

For VPC → HYDVPC

Click on "Yes, Create" button



Verify

hyd-pub-route table is created

The screenshot shows the AWS VPC Management Console with the 'Route Tables' section selected. On the left sidebar, there are links for 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 displays a table of route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	0 Subnets	No	vpc-7d934d1b HYDVPC
	rtb-1996c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYDVPC

Below the table, the details for the selected route table ('rtb-234b6445 | hyd-pub-route') are shown in a summary tab. The summary tab includes tabs for Summary, Routes, Subnet Associations, Route Propagation, and Tags. The Route Table ID is listed as 'rtb-234b6445 | hyd-pub-route'. The 'Summary' tab is active, showing the Route Table ID and the status '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 (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, 'rtb-234b6445 | hyd-pub-route', is selected. Below it, the details for this route table are shown, including tabs for Summary, Routes, Subnet Associations (which is highlighted with a cursor), Route Propagation, and Tags. At the bottom of the route table details, it says 'Main: no'.

Click on **Edit** button

This screenshot is similar to the previous one, showing the details for the 'rtb-234b6445 | hyd-pub-route' route table. The 'Edit' button on the Subnet Associations tab is highlighted with a cursor. The tab bar also includes Summary, Routes, Subnet Associations (highlighted), Route Propagation, and Tags. Below the tabs, there's a note: '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:' followed by a list of subnets.

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

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... 1 to 3 of 3 Route Tables

Name	Routes Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	0 Subnets	No	vpc-7d934d1b HYDVPC

rtb-234b6445 | hyd-pub-route

Summary Routes Subnet Associations Route Propagation Tags

Associate Subnet IPv4 CIDR IPv6 CIDR Current Route Table

Cancel Save

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input checked="" type="checkbox"/>	subnet-b3dbfbfa hyd-pub-subnet	192.168.10.0/24	-	Main
<input type="checkbox"/>	subnet-6abcbf23 hyd-pvt-subnet	192.168.20.0/24	-	Main

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

Verify

hyd-pub-subnet is associated with routing 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... 1 to 3 of 3 Route Tables

Name	Routes Table ID	Explicitly Associated	Main	VPC
rtb-1996c27e	rtb-1996c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
rtb-847d52e2	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYDVPC

rtb-234b6445 | hyd-pub-route

Summary Routes Subnet Associations Route Propagation Tags

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-b3dbfbfa hyd-pub-subnet	192.168.10.0/24	-

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

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

Click on **Route** Button

Click on **Edit** button

The screenshot shows the AWS VPC Management Console. In the left sidebar, under 'Route Tables', the 'rtb-234b6445 | hyd-pub-route' table is selected. The main area displays the table's details: Name (rtb-234b6445), Route Table ID (rtb-234b6445), Explicitly Associated Subnets (0 Subnets), Main (Yes), and VPC (vpc-89c341ee | default-vpc-oregon). Below this, there are tabs for Summary, Routes, Subnet Associations (which is active), Route Propagation, and Tags. Under the Subnet Associations tab, there is a 'Summary' section showing one subnet: 'subnet-03b0fbfa | hyd-pub-subnet 192.168.0.2/24'. A note below states: 'The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:'. At the bottom of the table view, there are 'Edit' and 'Delete' buttons.

Click on "Add another route" button

This screenshot is similar to the previous one, showing the 'rtb-234b6445 | hyd-pub-route' table. The 'Routes' tab is active. Below the table summary, there is a 'View: All rules' section. It shows one existing rule: 'Destination 192.168.0.0/16 Target local Status Active Propagated No Remove'. Below this, there is a button labeled 'Add another route' with a cursor hovering over it. Other buttons visible include 'Cancel' and 'Save'.

For Destination → 0.0.0.0/0

For Target → select HYDIGW

Click on **Save** button

The screenshot shows the AWS VPC Management Console with the 'Create Route Table' tab selected. In the 'Routes' section, a new route is being defined:

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

The 'Save' button is highlighted in blue at the bottom left of the route table configuration area.

Verification

Public route is added through internet gateway

The screenshot shows the AWS VPC Management Console with the 'Create Route Table' tab selected. In the 'Routes' section, the newly created route is listed:

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

The 'Save' button is highlighted in blue at the bottom left of the route table configuration area.

Verify

Status column show Active

VPC Management Console - Introduction to Amazon VPC

Services Resource Groups

VPC Dashboard

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 Routes Table ID Explicitly Associated Main VPC

rtb-1998c27e 0 Subnets Yes vpc-89c341ee | default-vpc-oregon

rtb-234b6445 | hyd-pub-route

Summary Routes Subnet Associations Route Propagation Tags

Edit View: All rules

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

Feedback English

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

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 sidebar, under 'Route Tables', there is a 'Create Route Table' button. The main area displays a table of existing route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	1 Subnet	No	vpc-7d934d1b HYDVPC
	rtb-1986c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYDVPC

Below the table, a specific route table 'rtb-234b6445 | hyd-pvt-route' is selected. Its details page shows tabs for Summary, Routes, Subnet Associations, Route Propagation, and Tags. The 'Edit' button is visible. The 'Routes' tab is selected, showing a table with columns: Destination, Target, Status, and Propagated.

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'. Below it is a descriptive text: 'A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.' There are two input fields: 'Name tag' containing 'hyd-pvt-route' and 'VPC' containing 'vpc-7d934d1b | HYDVPC'. At the bottom are 'Cancel' and 'Yes, Create' buttons, with 'Yes, Create' being highlighted with a mouse cursor icon.

Verify

hyd-pvt-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', and 'NAT Gateways'. The 'Route Tables' section is currently selected. The main area displays a table of 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	rtb-1998c27e	0 Subnets	Yes	vpc-89c341ee default-vpc-oregon
rtb-847d52e2	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYDVPC

Below the table, a specific route table 'rtb-ac446bca | hyd-pvt-route' is selected. The 'Routes' tab is active. At the bottom of the page, there are buttons for 'Edit', 'View: All rules', and tabs for 'Destination', 'Target', 'Status', and 'Propagated'.

Click on Subnet Association button

This screenshot shows the same VPC Management Console interface as the previous one, but with a different focus. The 'Subnet Associations' tab is now selected for the 'hyd-pvt-route' table. The table data remains the same as in the previous screenshot.

Click on Edit button

VPC Dashboard
Filter by VPC:
None

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

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Routes 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-59c341ee default-vpc-oregon
	rtb-847d52e2	0 Subnets	Yes	vpc-7d934d1b HYDVPC

rtb-ac446bca | hyd-pvt-route

Summary Routes Subnet Associations Route Propagation Tags

Edit Subnet IPv4 CIDR IPv6 CIDR

You do not have any subnet associations.

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

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

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	Routes 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-ac446bca | hyd-pvt-route

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/>	subnet-53bd1fba hyd-pvt-subnet	192.168.10.0/24	-	rtb-234b6445 hyd-pub-route
<input checked="" type="checkbox"/>	subnet-8abcbf23 hyd-pvt-subnet	192.168.20.0/24	-	Main

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

Click on Save button

The screenshot shows the AWS VPC Management Console. In the left sidebar, under 'Route Tables', the 'hyd-pvt-route' table is selected. On the main page, there is a table listing route tables. The 'hyd-pvt-route' table is highlighted. Below the table, a message states: 'The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table.' A 'Save Successful' message is displayed at the bottom.

Verify

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

This screenshot is identical to the previous one, showing the AWS VPC Management Console. The 'hyd-pvt-route' table is selected. The 'Subnet Associations' tab is active, showing the 'subnet-6abcfb23' subnet is associated with the route table. The same message about implicit association is present.

Click on Route 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 page displays a list of route tables. The 'hyd-pvt-route' table is selected, and its details are shown in the main pane. The 'Routes' tab is active, showing a single route entry:

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No

Note: No need to add IGW in pvt route

The screenshot shows the same AWS VPC Management Console interface. The 'Routes' tab is still active, but the table below it is empty, indicating no explicit routes have been added.

7) To launch Windows instance in Public subnet

Open the AWS console

Click on Services

Click on Ec2 services

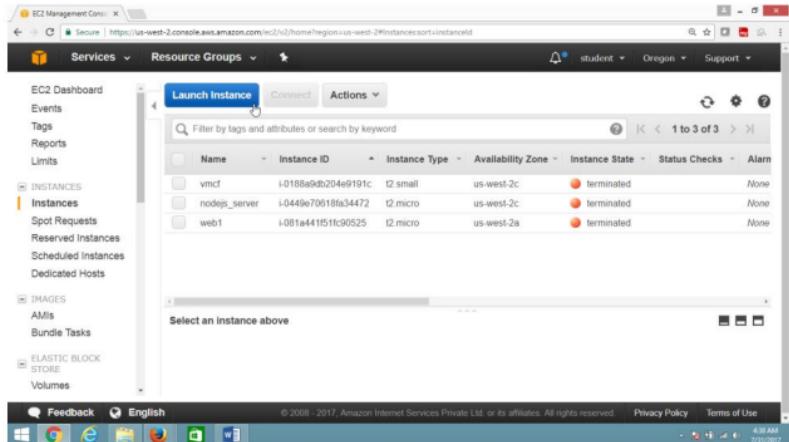
The screenshot shows the AWS Management Console with the URL <https://us-west-2.console.aws.amazon.com/>. The Services menu is open, showing various service categories: History, Compute, Developer Tools, Analytics, Application Services, Storage, Management Tools, Artificial Intelligence, Messaging, Database, and Business Products. A search bar at the top right says "Find a service by name or feature (for example, EC2, S3 or VM, storage)." The sidebar on the left lists EC2 and VPC under the "Compute" section.

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>. The left sidebar has sections for EC2 Dashboard, Instances (with sub-options like Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), Images (AMIs, Bundle Tasks), and Elastic Block Store (Volumes). The main area shows "Resources" with a list of EC2 resources: 0 Running Instances, 0 Dedicated Hosts, 0 Volumes, 0 Key Pairs, 0 Placement Groups, 0 Elastic IPs, 0 Snapshots, 0 Load Balancers, and 2 Security Groups. A callout box 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." Below this is a "Create Instance" section with a "Launch Instance" button. On the right, there's an "Account Attributes" section with details like Supported Platforms (VPC), Default VPC (vpc-8c341ee), and Resource ID length management. An "Additional Information" section includes links to Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, and Contact Us.

On the EC2 dashboard panel

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 navigation links: EC2 Dashboard, Events, Tags, Limits, INSTANCES (with sub-links: Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), IMAGES (with sub-links: AMIs, Bundle Tasks), and ELASTIC BLOCK STORE (with sub-links: Volumes). The main content area is titled 'Instances' and shows a table of running instances. The table has columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Three instances are listed:

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-0449e70618f8a34472	t2.micro	us-west-2c	terminated	None	
web1	i-091a44f15fc90525	t2.micro	us-west-2a	terminated	None	

Below the table, a message says 'Select an instance above'. At the top of the main content area, there's a blue button labeled 'Launch Instance' with a cursor pointing to it. The browser address bar shows the URL: https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#instances;sort=instanceId.

Select AMI “Microsoft Windows Server 2012 Base - ami-a1c1ddd8”

Free tier eligible

Step 1: Choose an Amazon Machine Image (AMI)

Microsoft Windows Server 2012 Base - ami-a1c1ddd8
Microsoft Windows Server 2012 Standard edition with 64-bit architecture. [English]
Root device type: ebs Virtualization type: hvm
Select 64-bit

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]
Root device type: ebs Virtualization type: hvm
Select 64-bit

Microsoft Windows Server 2012 with SQL Server Web - ami-f2c6da8b
Select

On the “Choose an Instance Type” page

Select “General purpose t2.micro”

Click on “Next Configure Instance Details” button

Step 2: Choose an Instance Type

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

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	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

Cancel Previous Review and Launch Next: Configure Instance Details

On the "Configuration Instance Details" page

For "Number of instances" → 1

For "Network" → HYDVPC

For "Subnet" → hyd-pub-subnet

For "Auto-assign Public IP" → Enable

Click on "Next: Add Storage" button

The screenshot shows the AWS EC2 Management Console interface for launching a new instance. The top navigation bar includes 'Services' and 'Resource Groups'. The main title is 'Step 3: Configure Instance Details'. Below it, a sub-instruction says: '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.' The configuration section has the following settings:

- Number of instances:** 1
- Purchasing option:** Request Spot Instances
- Network:** vpc-7df34d1b | HYDVPC
- Subnet:** subnet-b3cdbea | hyd-pub-subnet | us-west-2a
- Auto-assign Public IP:** Enable
- Domain join directory:** None

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

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-01e5be77f81e7266	30	General Purpose SSD	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 of use](#).

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

Click on “Add tag” button

Step 5: Add Tags

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

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

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

Add Tag (Up to 50 tags maximum)

Cancel Previous [Review and Launch](#) Next: Configure Security Group

For "Key" → Name

For Value → Winpubvm

Click on "Next: Configure Security Group"

EC2 Management Console

Services Resource Groups

student Oregon Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 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.

Key	(127 characters maximum)	Value	(255 characters maximum)	Instances	Volumes
Name		Winpubvm		(1)	(1)

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Feedback English © 2006-2017, Amazon Internet Services Private Ltd or its affiliates. All rights reserved. Privacy Policy 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

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

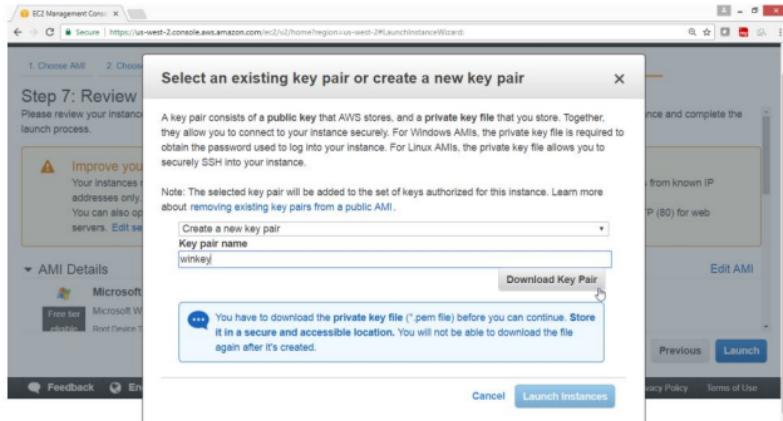
Microsoft Windows Server 2012 Base - ami-a1c1ddd8
Free tier eligible Microsoft Windows 2012 Standard edition with 64-bit architecture. [English]
Root Device Type: ebs Virtualization type: hvm

Cancel Previous Launch Define key pair and launch

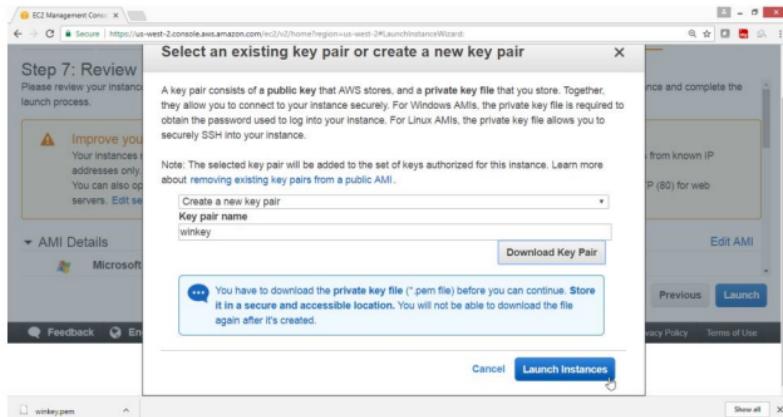
Select "Create a new key pair"

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 AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#launchInstanceWizard>. The browser tabs include "EC2 Management Console" and "Secure". The navigation bar has "Services" and "Resource Groups" dropdowns, and user information "student" and "Oregon". The main content area is titled "Launch Status" with a sub-instruction: "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, Microsoft Windows Guide, and Discussion Forum. Further down, instructions for creating status check alarms and managing security groups are provided. At the bottom right is a blue "View Instances" button.

Verify that instance is Running

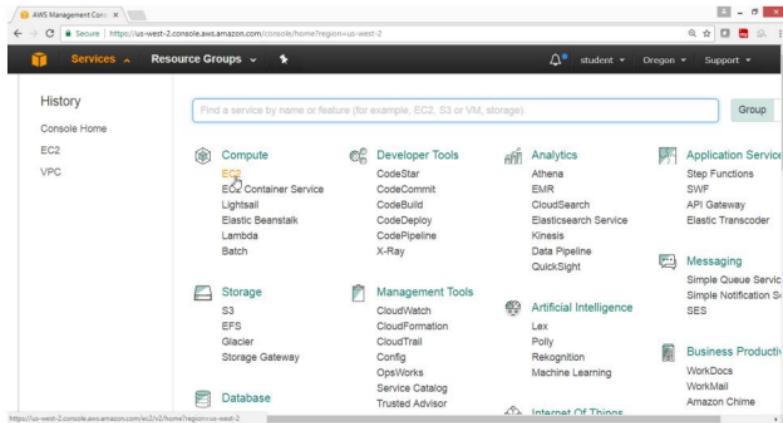
The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#instances?sort=instanceId>. The browser tabs and navigation bar are identical to the previous screenshot. The left sidebar shows "Instances" selected under "INSTANCES", with sub-options: Spot Requests, Reserved Instances, Scheduled Instances, and Dedicated Hosts. The main content area displays a table of instances. One row is highlighted for "Winpubvm" with the instance ID "i-0cb26994e13174e85", type "t2.micro", availability zone "us-west-2a", and status "running". Below the table, a detailed view for "Winpubvm" shows its Public IP (54.202.132.130) and Public DNS (IPv4). The bottom of the page includes standard AWS footer links: "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 a tree view with 'Instances' selected. The main content area shows a table of instances. One instance is listed:

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

Below the table, the instance details are shown: Instance: i-0cb26994e13174e85 (Winpubvm), Public IP: 54.202.132.130. There are tabs for Description, Status Checks, Monitoring, and Tags. The Status Checks tab is active, showing Instance ID: i-0cb26994e13174e85 and Public DNS (IPv4): -.

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 interface. At the top, there's a navigation bar with tabs like 'Services', 'Resource Groups', and 'Launch Instance Wizard'. Below the navigation bar, a progress bar indicates 'Step 1: Choose an Amazon Machine Image (AMI)'. The main content area displays a list of available AMIs under the 'Windows' category. One AMI is highlighted with a blue border and a 'Select' button:

AMI Name	Description	Action
Microsoft Windows Server 2016 with SQL Server Standard - ami-39fae640	Microsoft Windows 2016 Datacenter edition, Microsoft SQL Server 2016 Standard. [English]	Select
Microsoft Windows Server 2012 R2 Base - ami-3dcbd744	Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]	Select
Microsoft Windows Server 2012 R2 with SQL Server Express - ami-3bc8d442	Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]	Select

At the bottom of the page, there are links for 'Feedback', 'English', '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 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', 'Resource Groups', and tabs for 'student', 'Oregon', and 'Support'. Below the navigation is a breadcrumb trail: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, 7. Review. A dropdown menu 'Filter by:' is set to 'All instance types' and 'Current generation'. The main content area is titled 'Step 2: Choose an Instance Type' with a sub-instruction 'Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz. Intel Xeon Family, 1 GiB memory, EBS only)'. A table lists various 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 <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

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

On the "Configuration Instance Details" page

For "Number of instances" → 1

For "Network" → HYDVPC

For "Subnet" → hyd-pvt-subnet

For "Auto-assign Public IP" → Disabled

Click on "Next: Add Storage" button

The screenshot shows the 'Configure Instance Details' step of the EC2 instance creation wizard. The 'Number of instances' is set to 1. Under 'Purchasing option', 'Request Spot Instances' is selected. In the 'Network' section, 'vpc-7d934d1b | HYDVPC' is chosen. In the 'Subnet' section, 'subnet-6abcbf23 | hyd-pvt-subnet | us-west-2a' is selected, with 'Create new subnet' and '251 IP Addresses available' options shown. The 'Auto-assign Public IP' dropdown is set to 'Disable'. The 'Domain join directory' field is empty. At the bottom, there are 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Add Storage' buttons.

On the "Add Storage" page

Take default values

Click on "Next: Add tags" button

The screenshot shows the 'Add Storage' step of the EC2 instance creation wizard. It displays a table for adding storage volumes. A single row is present for the 'Root' volume, which is attached to the '/dev/sda1' device and has a size of 30 GiB. The volume type is 'General Purpose S', IOPS is 100 / 3000, and throughput is N/A. The 'Delete on Termination' checkbox is checked, and 'Encrypted' is set to 'Not Encrypted'. Below the table, a note 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 terms of service.' At the bottom, there are 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Add Tags' buttons.

Click on “Add tag” button

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#launchInstanceWizard>. The page is titled "Step 5: Add Tags". It includes a note about tag formats and permissions. A table for adding tags is shown with columns for Key (127 characters maximum), Value (255 characters maximum), Instances, and Volumes. Below the table, a message says "This resource currently has no tags". A note at the bottom says "Choose the Add tag button or click to add a Name tag. Make sure your IAM policy includes permissions to create tags." 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

The screenshot shows the same EC2 Launch Instance Wizard page as before, but the "Review and Launch" button is now highlighted in blue. The rest of the interface remains the same, including the "Add Tag" button, the note about IAM permissions, and the navigation buttons.

Take Default Values

Click on “Review and Launch” button

EC2 Management Console < Services < Resource Groups < student < Oregon < Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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-2

Description: launch-wizard-2 created 2017-07-31T08:27:45.080+05:30

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

Add Rule Cancel Previous Review and Launch

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

Drag down

Click on “Launch” button

EC2 Management Console < Services < Resource Groups < student < Oregon < Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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]
Instance Type: m3.2xlarge | Virtualization type: hvm

Cancel Previous Launch

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

Select "Choose an existing key pair"

For "Key pair name" → winkey

Select I acknowledge check box

Click on "Launch Instance" button

EC2 Management Console Secure | https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#launchInstanceWizard:

1. Choose AMI 2. Choose Security Groups

Step 7: Review

Security group name:

Description:

Type: RDP

Instance Details

Storage

Tags

Select an existing key pair or create a new key pair

Choose an existing key pair

Select a key pair

winkey

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

Cancel Launch Instances

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

Check summary, Drag down

Click on "View Instance" button

EC2 Management Console Secure | https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#launchInstanceWizard:

Services Resource Groups

Launch Status

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.

Here are some helpful resources to get you started

- Amazon EC2 User Guide
- Amazon EC2: Microsoft Windows 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

View Instances

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

Verify that instance is Running

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 more. The Instances section is currently selected. In the main content area, there's a search bar at the top followed by a table of instances. The table has columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Two instances are listed:

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

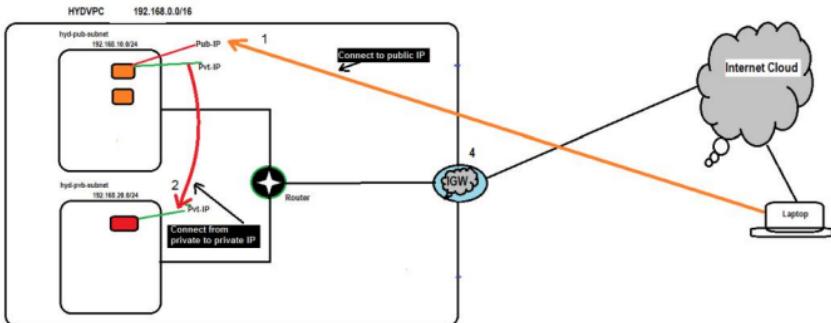
Below the table, a specific instance is selected: Winpvtvm (i-0e2251b25ee08fa4e). A detailed view shows its Private IP (192.168.20.87) and Public DNS (IPv4). The status indicates it's running with 2/2 checks and no alarm.

Verification

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

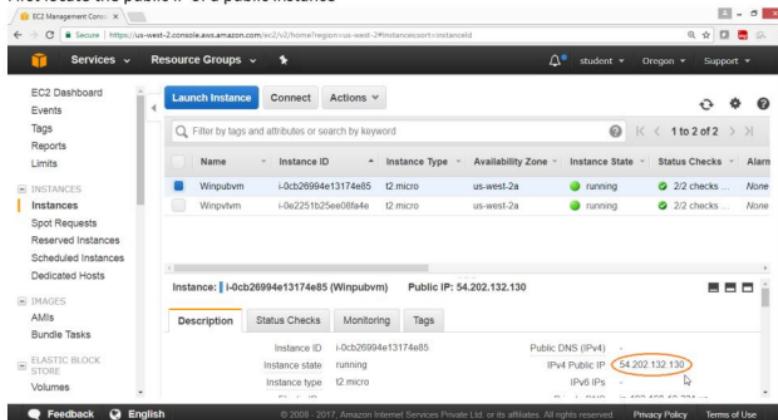
This screenshot is identical to the one above, showing the AWS EC2 Management Console. It displays the same sidebar, instance list, and detailed view for the selected instance (Winpvtvm). The status remains "running" with 2/2 checks and no alarm.

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



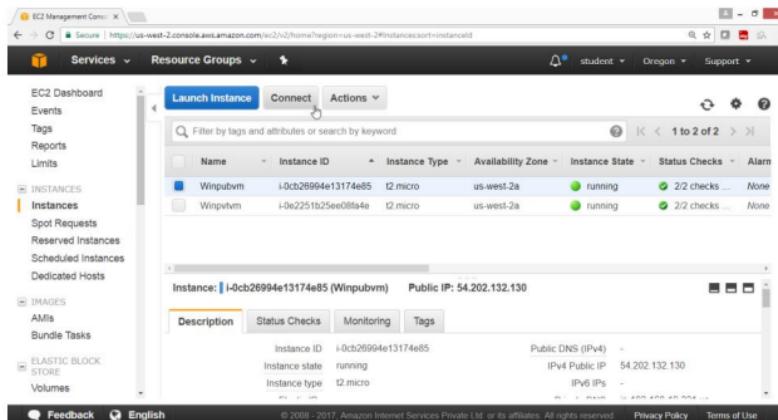
9) To Connect to Public subnet instance

First locate the public IP of a public instance



The screenshot shows the AWS EC2 Management Console. On the left sidebar, under the 'Instances' section, the 'Instances' option is selected. In the main content area, there is a table of running instances. One instance, 'Winpubvm' (Instance ID: i-0cb26994e13174e85), is highlighted. Below the table, a detailed view for this instance is shown. The 'Description' tab is selected. In the 'Public DNS (IPv4)' field, the value '54.202.132.130' is displayed and circled in red. The 'IPv4 Public IP' field also contains '54.202.132.130'. At the bottom of the window, the footer includes the text '© 2008 - 2017, Amazon Internet Services Private Ltd, or its affiliates. All rights reserved.' and links for 'Privacy Policy' and 'Terms of Use'.

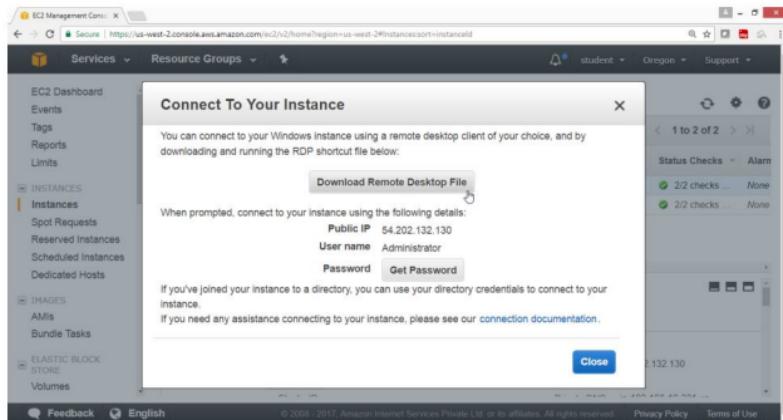
Click on "Connect" button



This screenshot is identical to the one above, showing the AWS EC2 Management Console. The 'Instances' section is selected on the left. A single instance, 'Winpubvm', is highlighted. In the 'Description' tab of the detailed view, the 'IPv4 Public IP' field is circled in red. The footer at the bottom of the window includes the copyright notice and links for 'Privacy Policy' and 'Terms of Use'.

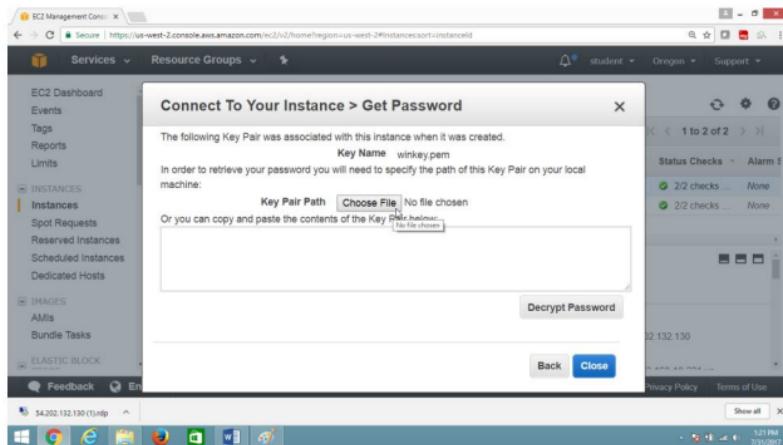
Click on "Download Remote Desktop file"

Click on "Get Password"



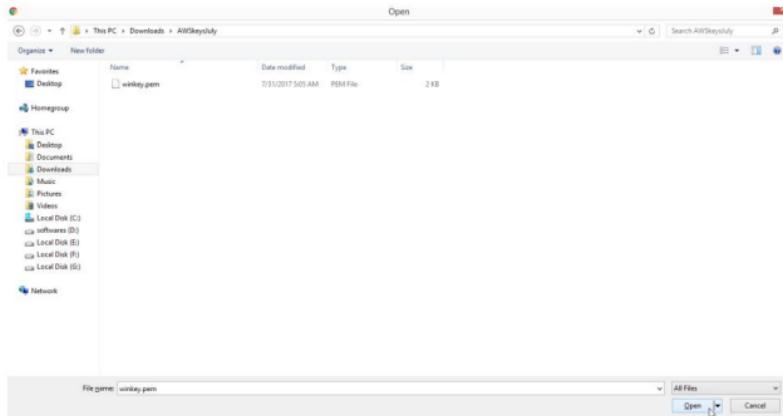
Provide the path of key file

Click on Choose file button

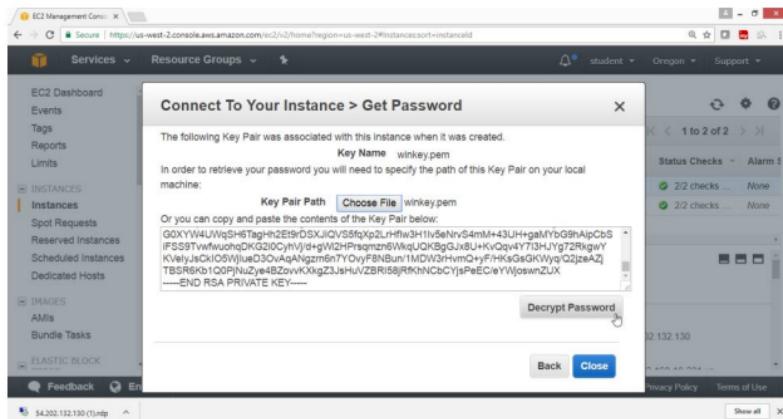


Select the key file

Click on **Open** button



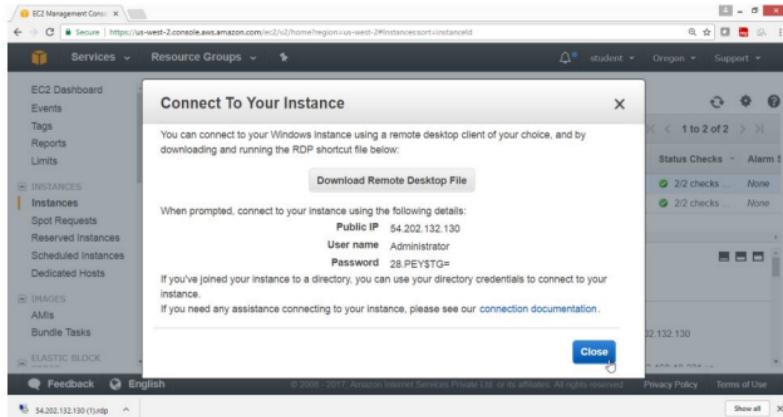
Now click on “Decrypt Password” button



Verification

Password is generated copy in notepad

Click on **Close** button



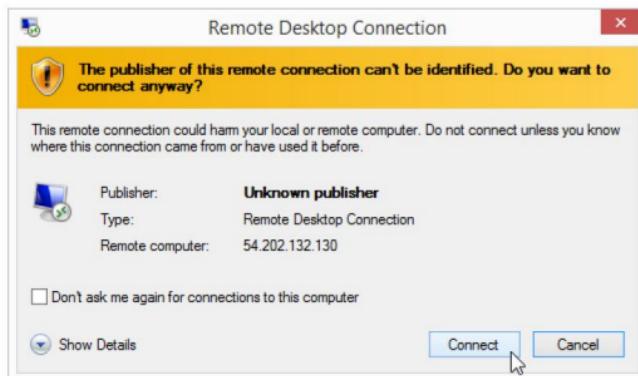
Double Click on RDP file

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 navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Dedicated Hosts. The main area is titled 'Launch Instance' and shows a table of instances. One instance, 'Winpubvm' (Instance ID: i-0cb26994e13174e85), is selected. Below the table, there's a detailed view for this instance. At the bottom of the main window, there's a toolbar with various icons. The status bar at the bottom right shows the IP address (54.202.132.130) and the date/time (11/25 PM 11/29/2017).

Click on “Connect” button

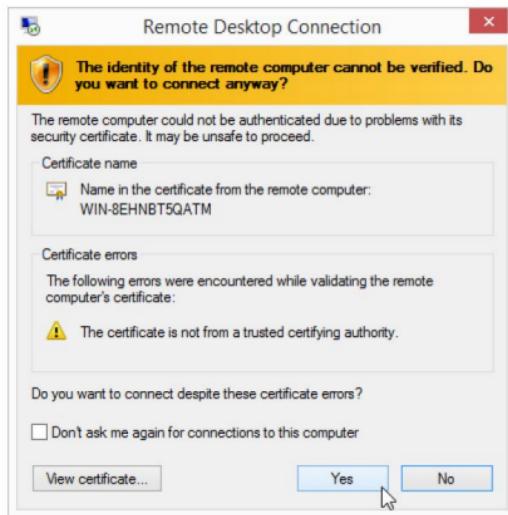


Paste the password

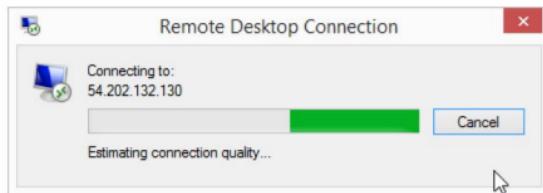
Click on **OK** button



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

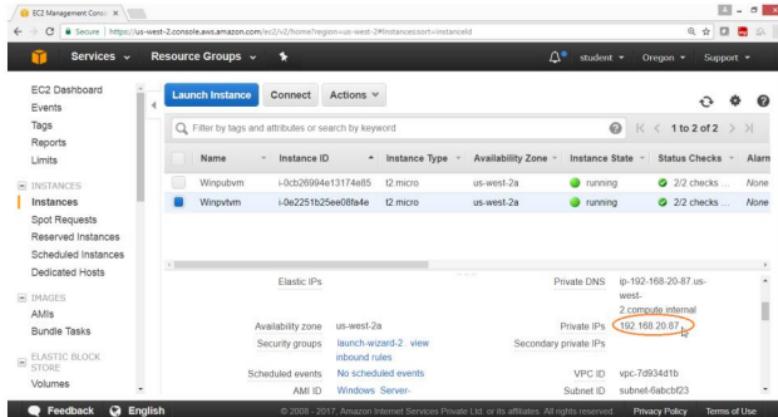


10) To Connect to Private subnet instance

Go to Ec2 Dashboard

Select private instance

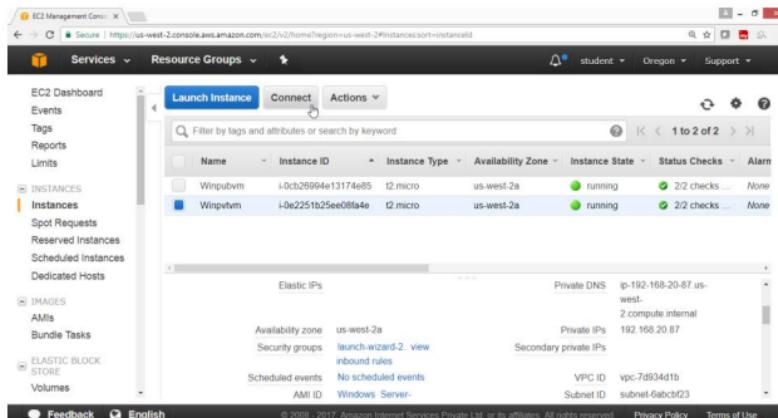
Get the private IP of the instance



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
Winpvvm	i-0e2251b25ee0f8a4e	t2.micro	us-west-2a	running	2/2 checks ...	None

Elastic IPs Private DNS ip-192.168.20.87.us-west-2.compute.internal
Availability zone us-west-2a Private IPs 192.168.20.87
Security groups launch-wizard-2, view inbound rules
Scheduled events No scheduled events
AMI ID Windows Server-
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
Winpvvm	i-0e2251b25ee0f8a4e	t2.micro	us-west-2a	running	2/2 checks ...	None

Elastic IPs Private DNS ip-192.168.20.87.us-west-2.compute.internal
Availability zone us-west-2a Private IPs 192.168.20.87
Security groups launch-wizard-2, view inbound rules
Scheduled events No scheduled events
AMI ID Windows Server-
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-----
MIIEowlBAAKCAQEAshLs36UXn01ILHgG/mv0QHxJMq6p3NPPFedListup5gUUYge2zj8QQf1sn2AKs
Ye9PBAwBxIwlhdUpy0GbIRuBS17CY0cTkdxJipuhTg2Ynkpxuq0BYKw3n9B3AMDmVbSyvsrenC
Lcg05A1sSSm0tTrBqUjqkoANQZa+uZO7xDEkQS3G6rTf6XTtcjOl5Vp4erJfMPneJYCdg7ul/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:

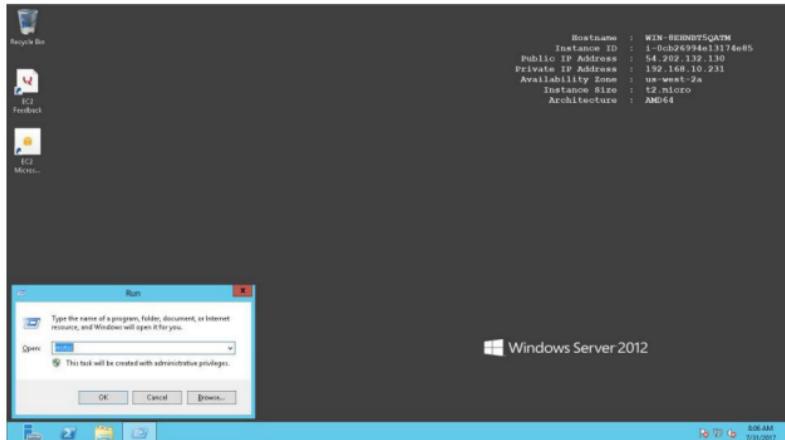
Private IP 192.168.20.87
User name Administrator
Password G-oV;n\$@!

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](#).

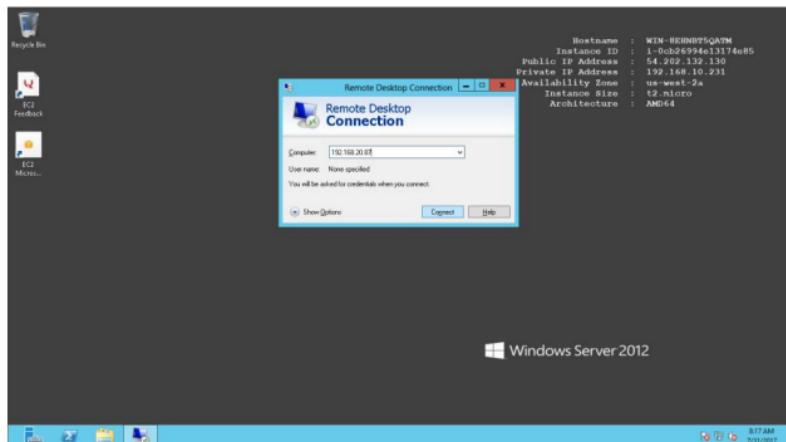
Now logging to public instance

Open Run and type mstsc to connect to window private instance

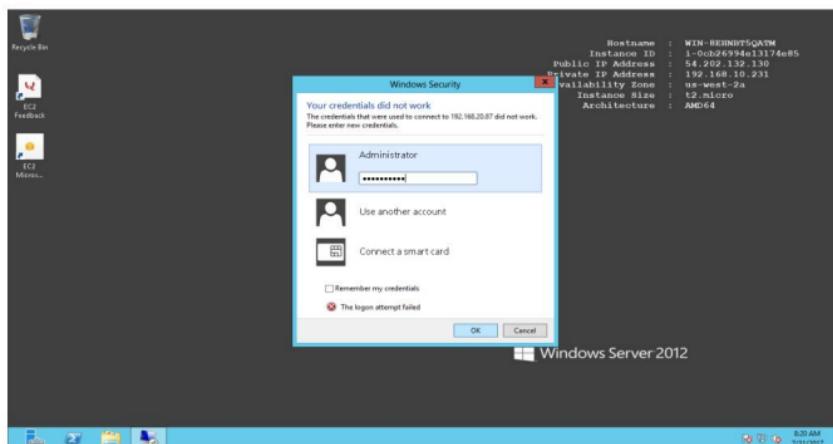


Provide private instance

Private IP → 192.168.20.87
Username → Adminsitritor
Password → G-oV;n\$.(@)



Now Provide Username & password



Verification

Check private IP at Right top corner

Now you are connected to windows private instance.



11) To connect to linux instance in private subnet

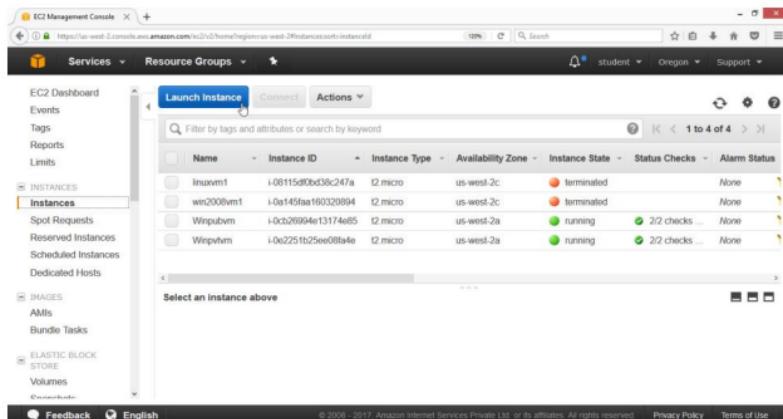
Launch linux instance in public subnet → hyd-pub-subnet

Open the AWS console

Click on Services

Click on Instance

Click on “Launch Instance” button



The screenshot shows the AWS Management Console interface for the EC2 service. The left sidebar navigation bar includes 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES' (with 'Instances' selected), 'Images', 'AMIs', 'Bundle Tasks', and 'ELASTIC BLOCK STORE'. The main content area displays a table of running instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
inuvm1	i-08115d0bd38c247a	t2.micro	us-west-2c	terminated	None	None
win2008vm1	i-0a145faa160320894	t2.micro	us-west-2c	terminated	None	None
Winpubvm	i-0cb26994e1317465	t2.micro	us-west-2a	running	2/2 checks	None
Winpvvm	i-0e225fb25eed0f6a4e	t2.micro	us-west-2a	running	2/2 checks	None

Below the table, there is a message: "Select an instance above". At the bottom of the page, there are links for "Feedback", "English", "© 2006–2017 Amazon Internet Services Private Ltd. or its Affiliates. All rights reserved.", "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

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

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.

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

SUSE Linux Enterprise Server 12 Service Pack 2 (HVM), FRS General Purpose (SSD)

Select

Cancel and Exit

1 to 33 of 33 AMIs

64-bit

64-bit

Feedback English

© 2006–2017, Amazon Internet Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

On the “Choose an Instace Type” page

Select “General purpose”

Type →t2.micro

Click on “Next: Configure Instance Details”

The screenshot shows the AWS Management Console EC2 Launch Instance Wizard. The second step, "Choose an Instance Type", is active. A table lists various instance types across different families. The "t2.micro" row is highlighted with a green background, indicating it has been selected. The "Free tier eligible" status is also highlighted in green. The table includes columns for Family, Type, vCPUs, Memory (GiB), Instance Storage (GB), EBS-Optimized Available, Network Performance, and IPv6 Support.

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
General purpose	t2.xlarge	4	16	EBS only	-	Medium	No

Below the table, there are buttons for "Cancel", "Previous", "Review and Launch", and "Next: Configure Instance Details". The "Review and Launch" button is highlighted in blue.

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

Step 3: Configure Instance Details

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

Number of Instances: 1

Purchasing option: Request Spot Instances

Network: vpc-7d934d1b | HYDVPC

Subnet: subnet-b30dbefb | hyd-pub-subnet | us-west-2a
250 IP Addresses available

Auto-assign Public IP:

IAM role: None

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 with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#launchInstanceWizard>. The page is titled "Step 4: Add Storage". It displays a table for adding storage volumes. A single row is present in the table:

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

Below the table is a button labeled "Add New Volume". At the bottom of the page, there is a note about free tier usage: "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." Below the note are several buttons: "Cancel", "Previous", "Review and Launch" (which is highlighted in blue), and "Next: Add Tags".

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: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (which is highlighted in blue), 6. Configure Security Group, and 7. Review. Below the navigation bar, the main content area has a heading "Step 5: Add Tags". It contains a note: "A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver." and "A copy of a tag can be applied to volumes, instances or both." It also states "Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources." There is a table with two columns: "Key" and "Value". In the "Key" column, there is a placeholder "(127 characters maximum)". In the "Value" column, there is a placeholder "(255 characters maximum)". Below the table, there is a dropdown menu labeled "Name" with the value "Linuxpubvm" selected. To the right of the table, there are two buttons: "Instances" and "Volumes", each with a count of 1. Below the table, there is a button labeled "Add another tag" with the note "(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 is also highlighted in blue). At the very bottom of the page, there are links for "Feedback", "English", "© 2006-2011, Amazon Internet Services Private Ltd or its affiliates. All rights reserved.", "Privacy Policy", 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:

Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere <input type="button" value="Edit"/>

Add Rule

[Cancel](#) [Previous](#) [Review and Launch](#)

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

On the “Review Instance Launch” page

Click on **Launch** button

Step 7: Review Instance Launch

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

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

▼ AMI Details [Edit AMI](#)

Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-6df1e514
Free tier available
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

[Cancel](#) [Previous](#) [Launch](#)

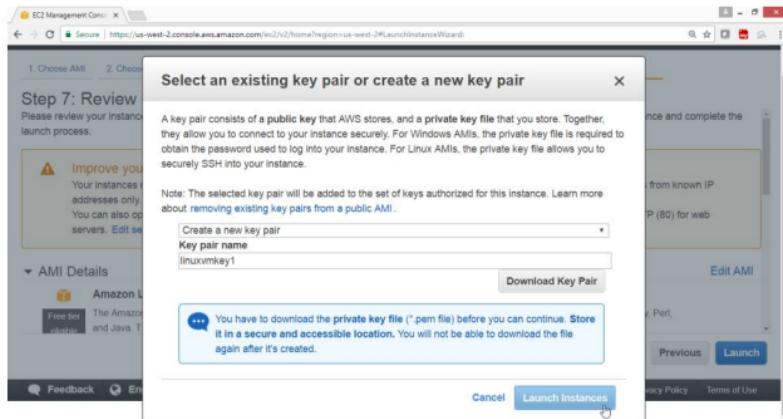
[Feedback](#) [English](#)

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

Select **Create a new key pair**

Key pair name → linuxvmkey1

Click on “Launch Instance” button



Check the summary

Click on **View Instance** button

The screenshot shows the EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#launchInstanceWizard>. The page displays the 'Launch Status' section, which includes instructions on how to connect to instances and lists helpful resources like the Amazon EC2 User Guide and Discussion Forum. Below this, there's a note about status check alarms and options to attach EBS volumes or manage security groups. A blue 'View Instances' button is highlighted with a red circle.

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=1>tagName>. The left sidebar shows navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, and Elastic Block. The main area is titled 'Launch Instance' and shows a table of instances. One row is selected: 'Linuxpubvm' (Instance ID: i-0c53f560c48fd5f80, Public IP: 54.202.241.190). The table includes columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Below the table, detailed information for the selected instance is shown in tabs: Description, Status Checks, Monitoring, and Tags. The 'Status Checks' tab is active, showing the instance ID, state, type, and its public DNS and IP addresses.

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 navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, AMIs, Bundle Tasks, and Elastic Block. The main area has tabs for Services and Resource Groups, with the Services tab selected. A large blue "Launch Instance" button is prominently displayed. Below it, there's a search bar and a table listing three instances: Linuxpubvm, linuzvm1, and Winpubvm. The table includes columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. The instance "Linuxpubvm" is currently running. At the bottom, there's a detailed view of the selected instance (Linuxpubvm), showing its Instance ID, Instance state, and Instance type.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Linuxpubvm	i-0c53f560c48fd5f80	t2.micro	us-west-2a	running	1/2 checks	None
linuzvm1	i-08115df0bd38c247a	t2.micro	us-west-2c	terminated	-	None
Winpubvm	i-0cb26964e13174e85	t2.micro	us-west-2a	running	2/2 checks	None

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

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

Click on **Select** button

Step 1: Choose an Amazon Machine Image (AMI)

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

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Free tier only ⓘ

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

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

SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami-00000000

Select Cancel and Exit

Feedback English

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

Show all ×

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 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', 'Resource Groups', and tabs for 'student', 'Oregon', and 'Support'. Below the navigation is a breadcrumb trail: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, 7. Review.

Step 2: Choose an Instance Type

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	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	SSD only	-	Low to Moderate	Yes

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

On the “Configure Instance Details” page

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

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 browser window title is "EC2 Management Console". The navigation bar includes "Services", "Resource Groups", and "student Oregon Support". Below the navigation bar, a progress bar shows steps 1 through 7: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance (which is highlighted), 4. Add Storage, 5. Add Tags, 6. Configure Security Group, 7. Review.

Step 3: Configure Instance Details

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

Number of Instances: 1

Purchasing option: Request Spot Instances

Network: vpc-7d934d1b | HYDVPC

Subnet: subnet-6abccb23 | hyd-pvt-subnet | us-west-2a

250 IP Addresses available

Auto-assign Public IP: Disable

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

Footer: Feedback, English, © 2006-2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved., Privacy Policy, Terms of Use, Show all

On the “Add Storage” page

Leave the values as default

Click on “Next: Add Tags” button

Step 4: Add Storage

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

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

Add New Volume

Cancel Previous Review and Launch Next: Add Tags

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

Click on Add Tag

Step 5: Add Tags

A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key	(127 characters maximum)	Value	(255 characters maximum)	Instances	Volumes
-----	--------------------------	-------	--------------------------	-----------	---------

This resource currently has no tags

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

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

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

On the "Add Tags" page

Key → Name

Value → Linuxpvvm

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: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (which is highlighted in orange), 6. Configure Security Group, and 7. Review. Below the tabs, the title "Step 5: Add Tags" is displayed. A sub-instruction says: "A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver." It also notes: "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." On the left, there's a "Key" input field with "(127 characters maximum)" placeholder text. To its right is a "Value" input field with "(255 characters maximum)" placeholder text. Further right are two buttons: "Instances" and "Volumes". Below these fields is a "Name" input field containing "Linuxpvvm". Underneath the "Name" field is a "Add another tag" button with "(Up to 50 tags maximum)" text. 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 mouse cursor hovering over it). At the very bottom of the page, there are links for "Feedback", "English", and legal notices: "© 2006-2011, Amazon Internet Services Private Ltd or its affiliates. All rights reserved.", "Privacy Policy", 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:
Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere <input type="button" value="Edit"/>

Add Rule

On the “Review Instance Launch” page

Click on **Launch** button

Step 7: Review Instance Launch

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

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

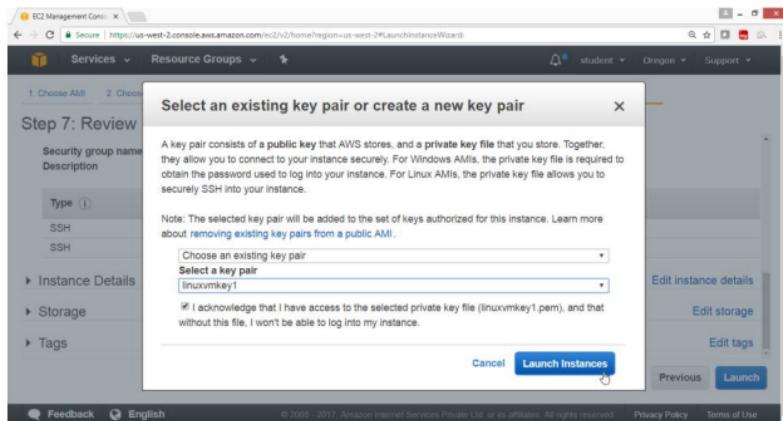
Instance Details
Storage
Tags

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

Select **Create a new key pair**

Key pair name → linuxvmkey1

Click on “Launch Instance” button



Check the summary

Click on **View Instance** button

The screenshot shows the AWS EC2 Management Console. At the top, it says "Launch Status". Below that, a note states: "Your instances are starting now. You can start them immediately or continue to accrue until you stop or terminate your instances." A link "Check View Instances" is provided to monitor instance status. A section titled "Here are some helpful resources to get you started" lists links to the User Guide, Free Usage Tier, and Discussion Forum. Below this, a note says "While your instances are launching you can also..." followed by links to Create status check alarms and Create and attach additional EBS volumes. A "Manage security groups" link is also present. At the bottom right, there is a blue "View Instances" button.

Verification

Linux instance in public subnet is launched

The screenshot shows the AWS EC2 Management Console with the "Instances" tab selected. The left sidebar lists "EC2 Dashboard", "Events", "Tags", "Reports", "Limits", "INSTANCES" (which is expanded to show "Instances", "Spot Requests", "Reserved Instances", "Scheduled Instances", and "Dedicated Hosts"), "IMAGES", "AMIs", "Bundle Tasks", and "ELASTIC BLOCK". The main pane displays a table of instances with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, and Status Checks. Four instances are listed: "Wlnpvhm", "Wlnpubvm", "Linuxpvvm" (which is selected), and "Linuxpubvm". The "Linuxpvvm" instance has a status of "running" and "Initializing". The bottom panel shows detailed information for the selected instance: "Instance: i-0da6594c71079c242 (Linuxpvvm)", "Private IP: 192.168.20.101", and a table with rows for "Description", "Status Checks", "Monitoring", and "Tags". The "Status Checks" row shows "Instance ID: i-0da6594c71079c242" and "Public DNS (IPv4):". The "Tags" row shows "Instance state: running" and "IPv4 Public IP: -".

To connect to linux private instance

First copy the key to linux instance in public subnet

Now connect to linux instance in public

Then connect to linux instance in private

Open Mobaxterm

Coping *.pem file to linux instance in public

Select public linux instance click on connect

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Linuxpubvm	i-0c5f560c48fd5f80	t2.micro	us-west-2a	running	2/2 checks	None
Linusprivvm	i-0da6594c71079c242	t2.micro	us-west-2a	running	2/2 checks	None
Winpubvm	i-0cb26994e13174e65	t2.micro	us-west-2a	running	2/2 checks	None
Winprivvm	i-0e2251b25ee08fa4e	t2.micro	us-west-2a	running	2/2 checks	None

View the guide lines

I would like to connect with A standalone SSH client
 A Java SSH Client directly from my browser (Java required)

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 Public IP:
54.202.241.198

Example:

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

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.

Feedback

Region: us-west-2 | Support

1 to 4 of 4

Status Checks

2/2 checks ... None

2/2 checks ... None

2/2 checks ... None

2/2 checks ... None

241.198

EC2 Policy Terms of Use

Use the above public ip of linux instance in mobaxterm

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

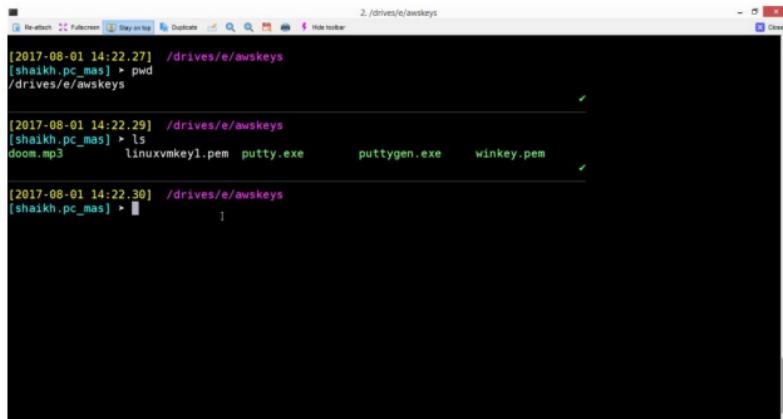
```
[2017-08-01 14:21.18] /drives/e/awskeys
[shaikh.pc_mas] > ls
doom.mp3      linuxvmkey1.pem  putty.exe      puttygen.exe  winkey.pem

[2017-08-01 14:21.20] /drives/e/awskeys
[shaikh.pc_mas] > scp -i "linuxvmkey1.pem" linuxvmkey1.pem ec2-user@54.202.241.198:/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

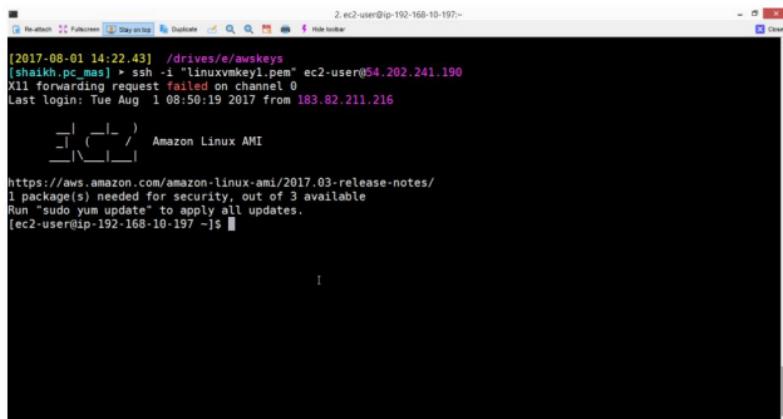


```
[2017-08-01 14:22:27] ./drives/e/awskeys
[shaikh.pc_mas] > pwd
/drives/e/awskeys

[2017-08-01 14:22:29] ./drives/e/awskeys
[shaikh.pc_mas] > ls
doom.mp3      linuxvmkeyl.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 "linuxvmkeyl.pem" ec2-user@54.202.241.190
X11 forwarding request failed on channel 0
Last login: Tue Aug  1 08:50:19 2017 from 183.82.211.216
[REDACTED]
[REDACTED] | (   )  Amazon Linux AMI
[REDACTED] | \___|___|
https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
1 package(s) needed for security, out of 3 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-10-197 ~]$ [REDACTED]
```

Select private instance and get private ip

EC2 Management Con... Secure | https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#instances:sort+tagName

Services Resource Groups

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

1 to 4 of 4

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Linregubvm	i-0c51f50c4f8d5f80	t2.micro	us-west-2a	running	2/2 checks	None
Linuxpvvm	i-0da6594c71079c242	t2.micro	us-west-2a	running	2/2 checks	None
Winregubvm	i-0cb26994e13174e65	t2.micro	us-west-2a	running	2/2 checks	None
Winpvvm	i-0e2251b25ee08fa4e	t2.micro	us-west-2a	running	2/2 checks	None

Instance: i-0da6594c71079c242 (Linuxpvvm) Private IP: 192.168.20.101

Description Status Checks Monitoring Tags

Instance ID: i-0da6594c71079c242 Public DNS (IPv4): -

Instance state: running IPv4 Public IP: -

Instance type: t2.micro IPv6 IPs: -

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

View the details of private instance

EC2 Management Con... Secure | https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#instances:sort+tagName

tags Reports Limits

INSTANCES Instances Spot Requests Reserved Instances Scheduled Instances Dedicated Hosts

IMAGES AMIs Bundle Tasks

ELASTIC BLOCK STORE Volumes

Feedback English

To access your instance:

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

Example:

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

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

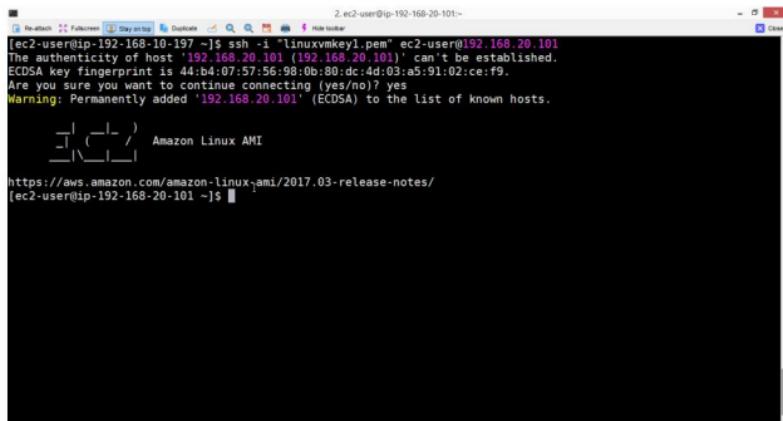
If you need any assistance connecting to your instance, please see our [connection documentation](#).

Close

Verification

Run ssh command to login to private instance

Now you are connected to private instance in private subnet



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

```
[ec2-user@ip-192-168-197-] $ 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:b1:07:57:56:98:0b: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 dark background and light-colored text. It includes standard Linux terminal icons at the top: a file icon, a folder icon, a trash icon, a search icon, a refresh icon, and a help icon. The title bar also displays the terminal session details.

Lab 10: To Configure Amazon CloudWatch

OBJECTIVE

To configure CloudWatch to monitor CPU Utilization

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

TASK :

Creating Alarm

Select Notification

Check mail to verify

1) To Configure Amazon CloudWatch Service

Launch a Amazon linux instance, then

Open AWS Console

Click on Services

In the Management Tools section

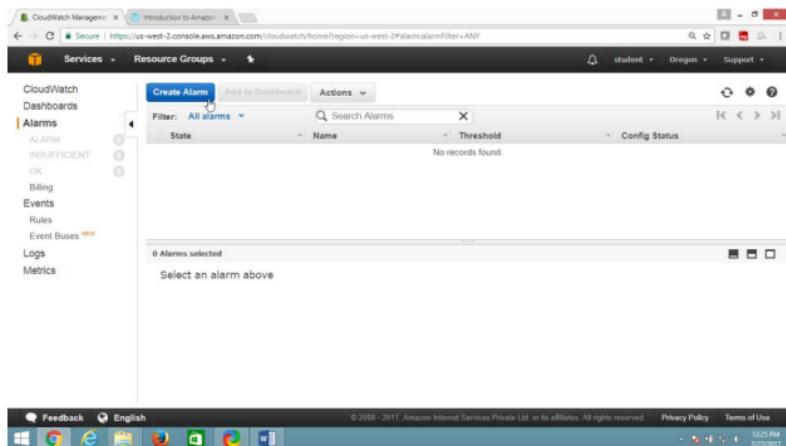
Click on CloudWatch

The screenshot shows the AWS Management Console with the URL <https://us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2>. The page displays the CloudWatch service interface, which includes sections for Developer Tools, Internet of Things, Contact Center, Game Development, Mobile Services, and Additional Resources. On the left, there is a sidebar with links to various AWS services like Compute, Storage, and Database. The top navigation bar shows the user is signed in as 'student' with a 'Oregon' region selected. The bottom right corner shows the date and time as '12:09 PM 3/21/2015'.

On "CloudWatch", panel

Select Alarms

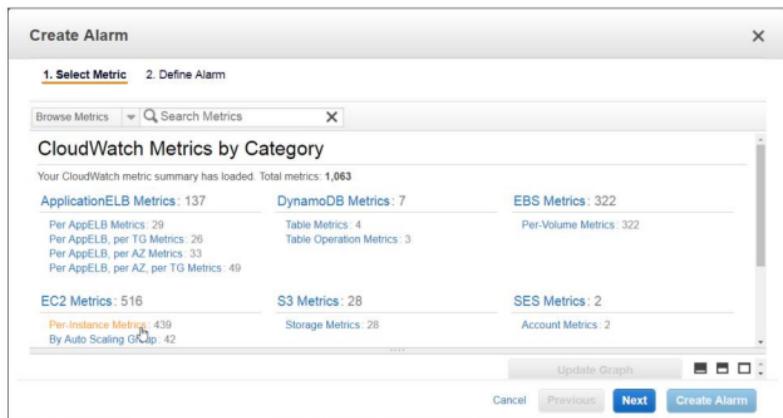
Click on "Create Alaram" button



In “Create Alarm” page

Select “EC2 Metrics”

Click on “Per-instance Metrics”



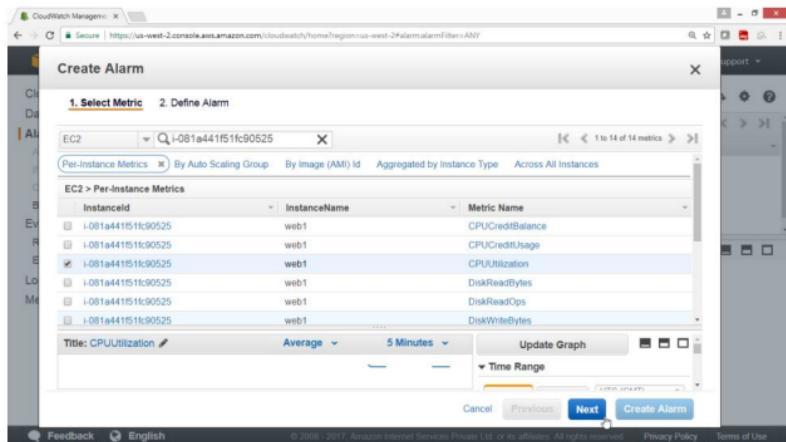
From "Create Alarm" page

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 → testcpuitilization

Description→ cputest

Under Whenever CPUUtilization

is >= 30

for 1 consecutive period(s)

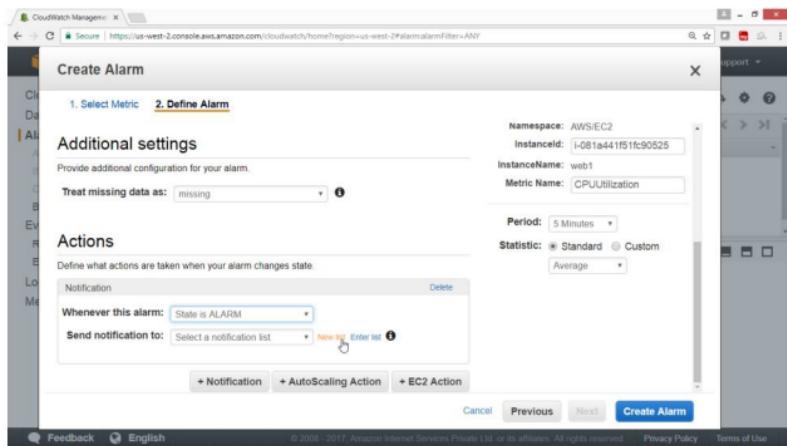
Drag Down

The screenshot shows the AWS CloudWatch Metrics 'Create Alarm' interface. The 'Define Alarm' step is active. In the 'Alarm Threshold' section, the 'Name' is set to 'testcpuitilization' and the 'Description' is 'cputest1'. Under 'Whenever', 'CPUUtilization' is selected with the condition 'is: >= 30' and 'for: 1 consecutive period(s)'. To the right, the 'Alarm Preview' displays a graph titled 'CPUUtilization >= 0'. The graph shows a sharp blue spike reaching a value of approximately 1.5 at 05:00 on 7/27, which then drops back down to near zero. A red horizontal line represents the threshold. A text overlay next to the graph states: 'This alarm will trigger when the blue line goes up to or above the red line for a duration of 5 minutes.' Below the preview, the 'Namespace' is listed as 'AWS/EC2', 'InstanceId' as 'i-081a441f51fc90525', and 'InstanceName' as 'web1'. At the bottom, there are 'Cancel', 'Previous', 'Next', and 'Create Alarm' buttons.

Under Actions

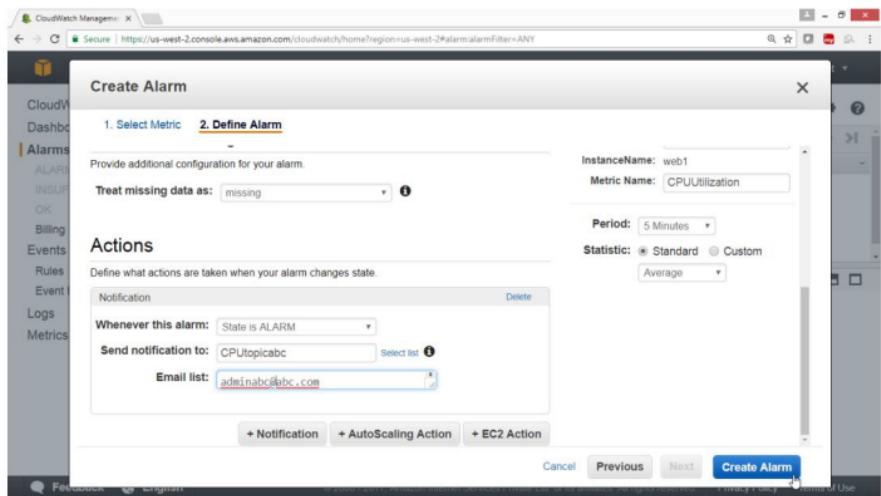
Whenever this alarm → State is Alaram

Send notification to → Click on New list

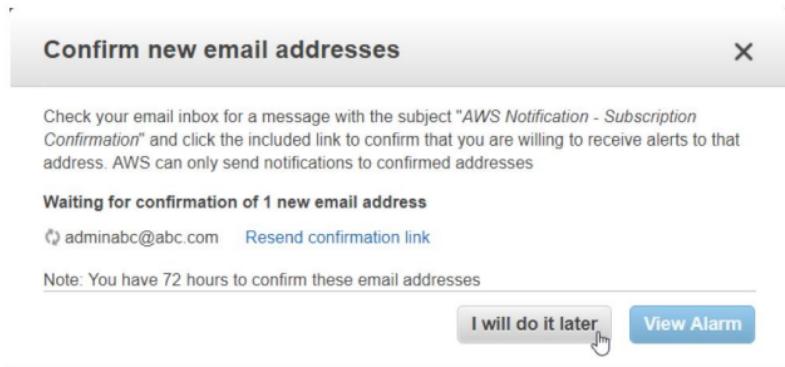


Send notification to → CPUpicabc
Email → adminabc@abc.com

Click on "Create Alaram" button



Click on "I will do it Later" button.



Go to your Email account and check the Mail

Once mail is been checked

Config status → Pending confirmation

Verify the link from your Email

The screenshot shows the AWS CloudWatch Metrics console. On the left sidebar, under the 'Alarms' section, there is a link labeled 'Pending confirmation'. The main area displays a success message: 'Your alarm testcpuutilization has been saved.' Below this, the alarm configuration is shown: State 'OK', Name 'testcpuutilization', Threshold 'CPUUtilization >= 30 for 5 minutes', and Config Status 'Pending confirmation'. A note at the bottom says 'Select an alarm above'.

Open your email

The screenshot shows a Gmail inbox with 113 messages. The top navigation bar includes a search bar, a 'Compose' button, and a notifications icon. The inbox header shows tabs for 'Primary', 'Social', 'Promotions', and 'Inbox (113)'. An email from 'AWS Notifications' is visible in the inbox, with the subject 'AWS Notification - Subscript' and a timestamp of '1:26 pm'.

Click on "Confirm subscription"

=====

AWS Notification - Subscription Confirmation Inbox x

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

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 AWS Notification - Subscription Confirmation - You have chosen to subscribe to the topic: arn:aws:sns:us-west-2:523251683217:CPUtopicabc 1:26 pm

=====

Verified by this output

=====



Subscription confirmed!

You have subscribed adminabc@abc.com to the topic:
CPUtopicabc.

Your subscription's id is:
arn:aws:sns:us-west-2:523251683217:CPUtopicabc:8e548f92-5474-4587-8105-64022c49ebf6

If it was not your intention to subscribe, [click here to unsubscribe](#).

=====

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

Now login to Instance using mobaxterm

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

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

Switch to root user and install stress command

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

Login to another terminal-2

Run top command

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

Verify output

CPU status is 100% idle

```
top - 08:56:26 up 1:53, 2 users, load average: 0.00, 0.00, 0.00
Tasks: 94 total, 1 running, 93 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.0%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	5	0.0	0.2	0:00.00	init
2	root	20	0	0	0	0	5	0.0	0.0	0:00.00	xthreadd
3	root	20	0	0	0	0	5	0.0	0.0	0:00.00	ksftiirqd/0
4	root	20	0	0	0	0	5	0.0	0.0	0:00.00	kworker/0:0
5	root	0	-20	0	0	0	5	0.0	0.0	0:00.00	kworker/0:0H
6	root	20	0	0	0	0	5	0.0	0.0	0:00.00	kworker/u30:0
7	root	20	0	0	0	0	5	0.0	0.0	0:00.03	rcu_sched
8	root	20	0	0	0	0	5	0.0	0.0	0:00.00	rcu_bh
9	root	RT	0	0	0	0	5	0.0	0.0	0:00.00	migration/0
10	root	0	-20	0	0	0	5	0.0	0.0	0:00.00	lru-add-drain
11	root	20	0	0	0	0	5	0.0	0.0	0:00.00	cpuhp/0
12	root	20	0	0	0	0	5	0.0	0.0	0:00.00	kddevtmpfs
13	root	0	-20	0	0	0	5	0.0	0.0	0:00.00	netns
16	root	20	0	0	0	0	5	0.0	0.0	0:00.01	xenwatch
17	root	20	0	0	0	0	5	0.0	0.0	0:00.02	kworker/u30:2
21	root	20	0	0	0	0	5	0.0	0.0	0:00.00	xenbus
139	root	20	0	0	0	0	5	0.0	0.0	0:00.00	khungtaskd
140	root	20	0	0	0	0	5	0.0	0.0	0:00.00	oom_reaper
141	root	0	-20	0	0	0	5	0.0	0.0	0:00.00	writelock
143	root	20	0	0	0	0	5	0.0	0.0	0:00.00	kcompactd0
144	root	25	5	0	0	0	5	0.0	0.0	0:00.00	ksmd
145	root	39	19	0	0	0	5	0.0	0.0	0:00.00	khugepaged
146	root	0	-20	0	0	0	5	0.0	0.0	0:00.00	crypto
147	root	0	-20	0	0	0	5	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: 101.572K 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	:00:73	stress
3147	root	20	0	7260	96	0	R	2.7	0.0	:00:73	stress
3179	root	20	0	7260	96	0	R	2.7	0.0	:00:73	stress
3141	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3142	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3144	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3145	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3146	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3148	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3149	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3150	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3151	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3152	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3153	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3154	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3155	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3156	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3157	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3158	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3159	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3160	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3161	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3162	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress
3163	root	20	0	7260	96	0	R	2.3	0.0	:00:72	stress

Go to CloudWatch service

Check the status

The screenshot shows the AWS CloudWatch Metrics interface. On the left sidebar, under the CloudWatch section, the 'Metrics' option is selected. In the main content area, the 'Alarm Summary' section displays a chart titled 'testcpuutilization' with the metric 'CPUUtilization >= 30'. The chart shows a sharp spike from approximately 30 to 40 at 09:00 on 7/27. Below the chart, a message states 'All your alarms are in OK state in US West (Oregon) region.' A 'Create Alarm' button is visible. The 'Service Health' section shows a single entry for 'Amazon CloudWatch Service' with a green checkmark and the status 'Service is operating normally'. A link to 'View complete service health details' is provided. At the bottom of the page, there are links for 'Feedback', 'English', 'Privacy Policy', and 'Terms of Use'.

After 5 minutes Alarm is generated

This screenshot is identical to the one above, but it is taken 5 minutes later. The 'Metrics' option is still selected in the sidebar. The 'Alarm Summary' section now shows a red alarm icon and the message 'You have 1 alarm in ALARM state in US West (Oregon) region.' The chart for 'testcpuutilization' now shows a constant value of 60 from 07:00 to 09:00 on 7/27. The 'Service Health' section remains the same, indicating normal operation. The footer links are also present.

Go to email and check mail

The screenshot shows a Gmail inbox with 113 messages in the inbox. Two messages from 'AWS Notifications' are visible:

From	Subject	Date
AWS Notifications	ALARM: "testcpuitilization" in US West - Oregon	2:39 pm
AWS Notifications	AWS Notification - Subscription Confirmation - You h...	2:02 pm

Click on mail

Verify output

The email subject is 'AWS Notifications' from 'no-reply@sns.amazonaws.com' at 2:39 PM (2 minutes ago). The recipient is 'to me'. The email body contains the following text:

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

View this alarm in the AWS Management Console:

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

Alarm Details:

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

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

Threshold:

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

Monitored Metric:

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

State Change Actions:

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

↳ State Change Actions:

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

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

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

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

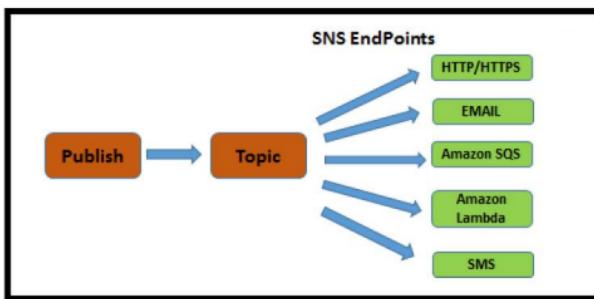
===== END OF OUTPUT =====

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

OBJECTIVE

To configure Amazon Simple Service (SNS)

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with AmazonSNSFullAccess

TASK :

Create a Topic

Subscribe your topic

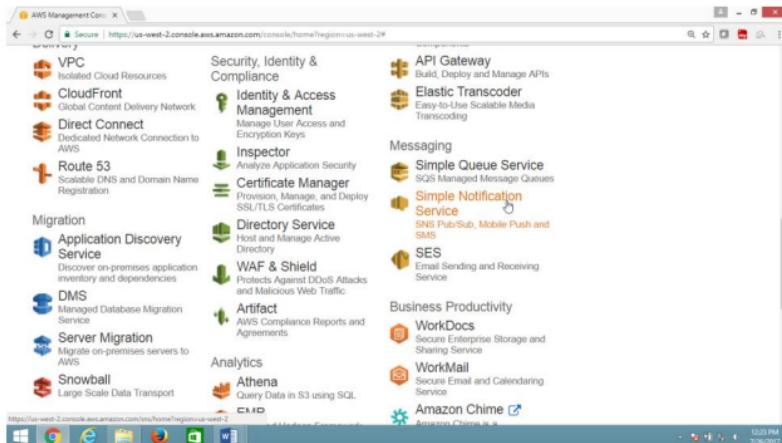
Verify in your mail account

1) To configure Amazon Simple Notification Service (SNS)

Open AWS console

Select “Messaging” service

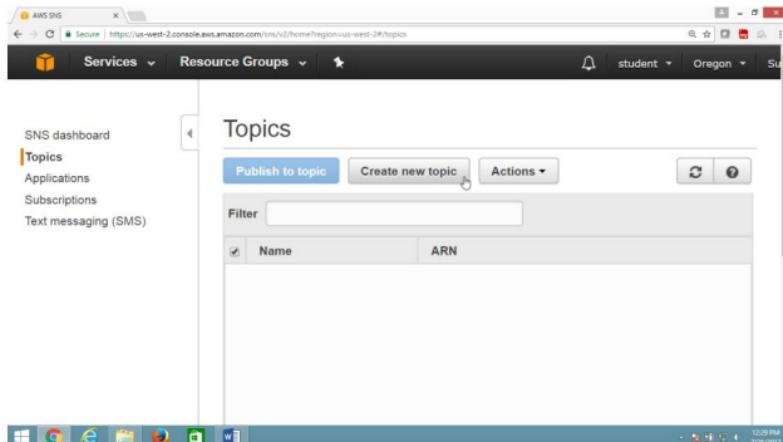
Click on “Simple Notification service”



From "SNS Dashboard" panel

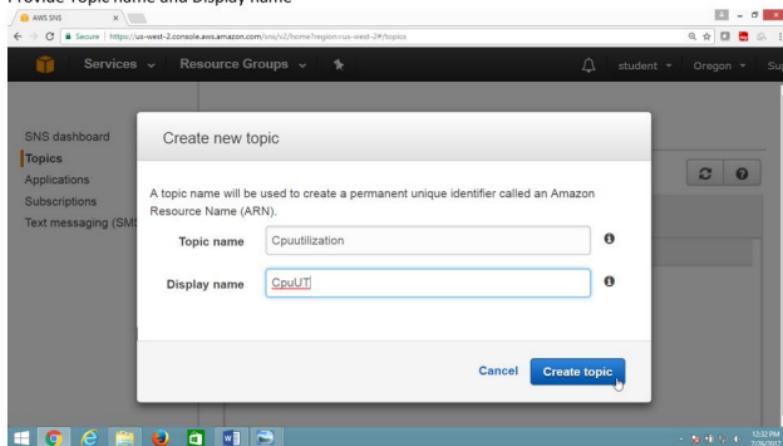
Select Topic

Click on "Create new topic" button



In "Create new topic" box

Provide Topic name and Display name



Click of ARN link

The screenshot shows the AWS SNS Topics page. A red box highlights the ARN link in the 'CpuUtilization' topic row. The URL in the browser is <https://us-west-2.console.aws.amazon.com/sns/v2/home?region=us-west-2#/topics>.

2) To create Subscription

Click on “Createsubscription” button

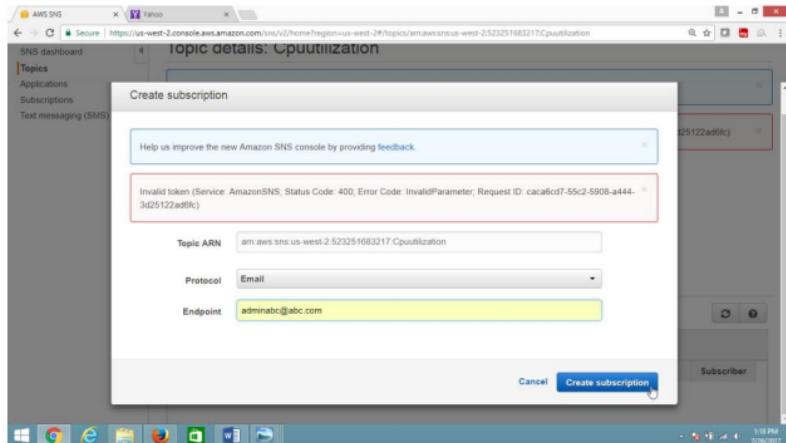
The screenshot shows the AWS SNS Topic details page for 'CpuUtilization'. A red box highlights the 'Create subscription' button. The URL in the browser is <https://us-west-2.console.aws.amazon.com/sns/v2/topics/am.avis.sns.us-west-2.523251683217.CpuUtilization>.

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 for the us-west-2 region. A single subscription named 'CpuUT' is listed under the 'PendingConfirmation' status. The 'Confirm subscription' button is highlighted.

Subscription ID	Protocol	Endpoint	Subscriber
PendingConfirmation	email	adminabc...	

Go to your mail account

Click on the mail

The screenshot shows an AWS notification email in the Gmail inbox. The subject is 'AWS Notification - Subscription Confirmation'. The message body indicates a subscription to the topic 'arn:aws:sns:us-west-2:523251683217:CpuUtilization'.

Click on "Confirm message"

The screenshot shows the contents of the AWS notification email. It includes a 'Confirm subscription' link and instructions for confirming the subscription.

You have chosen to subscribe to the topic:
arn:aws:sns:us-west-2:523251683217:CpuUtilization
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-unsub@amazonaws.com.

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 this, 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", "Enabled", and "Status". The single entry is: Subscription ID (arn:aws:sns:us-west-2:523251683217:CpuUtilization:b5f880a3-4631-405e-b5e1-a37209c3...), Protocol (email), Enabled (Yes), and Status (52%). There are also "Create subscription", "Request confirmations", "Confirm subscription", and "Other subscription actions" buttons.

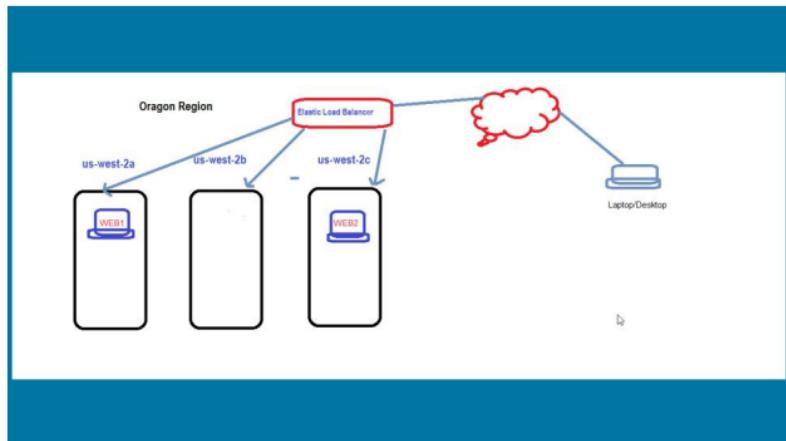
Subscription ID	Protocol	Enabled	Status
arn:aws:sns:us-west-2:523251683217:CpuUtilization:b5f880a3-4631-405e-b5e1-a37209c3...	email	Yes	52%

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. On the left, there's a sidebar with navigation links for Services, Resource Groups, EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, Elastic Block Store, Volumes, and Snapshots. The main content area has tabs for Launch Instance, Connect, and Actions. A search bar at the top says "Filter by tags and attributes or search by keyword". Below it is a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Two instances are listed: web1 (Instance ID: i-081a441f51fc90525, Instance Type: t2.micro, Availability Zone: us-west-2a, State: running, Status Checks: Initializing, Alarm: None) and web2 (Instance ID: i-090dfbcc632605047, Instance Type: t2.micro, Availability Zone: us-west-2c, State: running, Status Checks: Initializing, Alarm: None). At the bottom, there's a summary section for Instances: i-081a441f51fc90525 (web1), i-090dfbcc632605047 (web2), with tabs for Description, Status Checks, Monitoring, and Tags. The status checks table shows the public IP addresses for each instance: i-081a441f51fc90525: ec2-54-218-192-19.us-west-2.compute.amazonaws.com and i-090dfbcc632605047: ec2-54-203-189-115.us-west-2.compute.amazonaws.com. The bottom of the screen includes standard browser controls (Back, Forward, Home, Stop, Refresh) and links for Feedback, English, Privacy Policy, Terms of Use, and copyright information (© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.).

Verify Public IP of both instance

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with navigation links: EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, Elastic Block Store, Volumes, Snapshots, Feedback, and English. The main content area has tabs for Launch Instance, Connect, and Actions. A search bar at the top says "Filter by tags and attributes or search by keyword". Below it is a table with the following data:

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...	54.218.192.19	-
running	2/2 checks ...	None	ec2-54-203-189-115.us...	54.203.189.115	-

Below the table, a section titled "Instances" lists two instances: i-081a441f1fc90525 (web1) and i-090dfbcc632605047 (web2). There are tabs for Description, Status Checks, Monitoring, and Tags. The Description tab shows the public DNS names for both instances.

At the bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use. The status bar at the bottom right shows the time as 10:46 PM and the date as 10/29/2017.

Verify

Output of Webserver one



Verify

Output of Webserver two



3) To Configure Elastic Load Balancer.

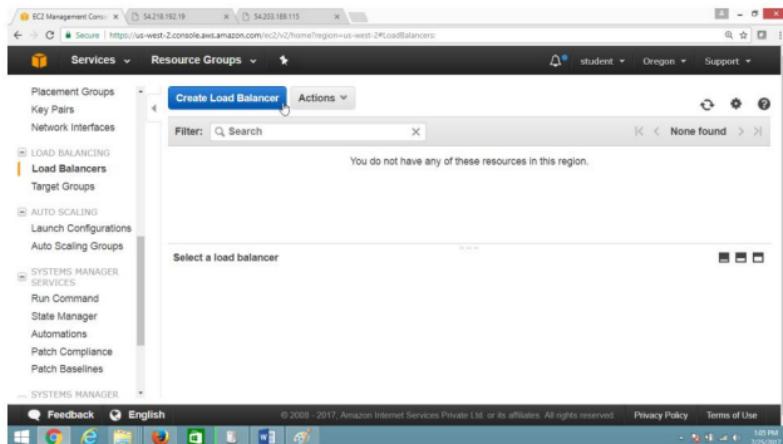
Open the AWS console

On **EC2 Dashboard** panel

Expanding “**LOAD BALANCING**”

Select **Load Balancer**,

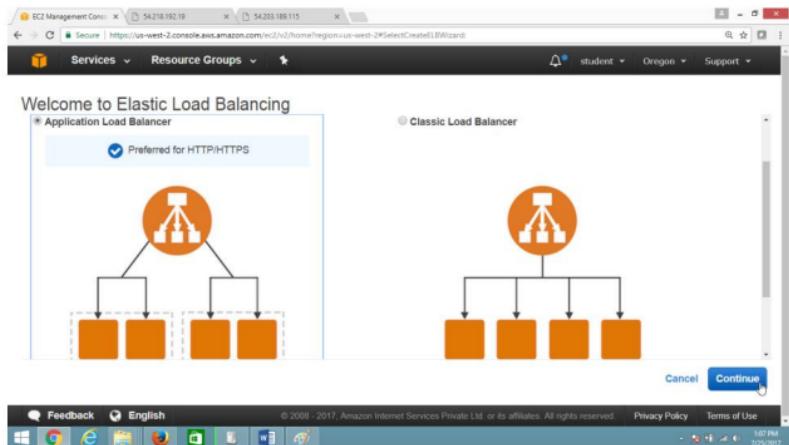
Click on “**Create Load Balancer**” button



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/home?region=us-west-2#V2CreateLBWizard>. The browser tabs include 'EC2 Management Console', '54.218.192.19', and '54.203.189.115'. The main content area is titled 'Step 1: Configure Load Balancer' under 'Basic Configuration'. It contains fields for 'Name' (set to 'ELBsales'), 'Scheme' (radio buttons for 'internet-facing' and 'internal' with 'internet-facing' selected), and 'IP address type' (set to 'ipv4'). Below these fields is a 'Listeners' section with a note: 'A listener is a process that checks for connection requests, using the protocol and port that you configured.' At the bottom right of the form are 'Cancel' and 'Next: Configure Security Settings' buttons.

Under **Listeners**, Provide

Load Balancer Protocol → **HTTP**

Load Balancer Port as → **80**

Drag down

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

Cancel Next: Configure Security Settings

Under Availability Zones

Select all zones

Click on “Next:Configure Security Settings” button

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

VPC	vpc-89c341ee (172.31.0.0/16) default-vpc-oregon (default)		
Availability Zone	Subnet ID	Subnet IPv4 CIDR	Name
us-west-2a	subnet-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

The screenshot shows a browser window with three tabs open: 'EC2 Management Cons...', '56.218.192.19', and '54.203.189.115'. The main content area is titled 'Step 2: Configure Security Groups'. A navigation bar at the top includes 'Services', 'Resource Groups', and links for 'student', 'Oregon', and 'Support'. Below the navigation bar, a horizontal menu bar shows steps 1 through 6: '1. Configure Load Balancer', '2. Configure Security Settings' (which is highlighted in blue), '3. Configure Security Groups', '4. Configure Routing', '5. Register Targets', and '6. Review'. A callout box with a warning icon and the text 'Improve your load balancer's security. Your load balancer is not using any secure listener.' is displayed. The text continues: 'If your traffic to the load balancer needs to be secure, use the HTTPS protocol for your front-end connection. You can go back to the first step to add/configure secure listeners under Basic Configuration section. You can also continue with current settings.' At the bottom right of the page, there are 'Cancel', 'Previous', and 'Next: Configure Security Groups' buttons. The 'Next' button is highlighted with a mouse cursor. The footer of the page includes links for 'Feedback', 'English', 'Privacy Policy', 'Terms of Use', and copyright information: '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.'

On "Configure Security Groups" page

Under Assign a security group

Select "Create a new security group"

click on Configure Routing button

The screenshot shows a browser window with three tabs open: 'EC2 Management Console', '54.218.192.19', and '54.203.189.115'. The main content area is titled 'Step 3: Configure Security Groups'. It displays a form for creating a new security group named 'load-balancer-wizard-2' with a description 'load-balancer-wizard-2 created on 2017-07-25T13:35:42.009+05:30'. A table lists a single rule: 'Custom TCP Rule' (Type), 'TCP' (Protocol), port '80' (Port Range), and 'Custom [0.0.0.0/:0]' (Source). At the bottom right of the form, there are 'Cancel', 'Previous', and 'Next: Configure Routing' buttons, with the 'Next' button being the target of a mouse cursor.

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 new load balancer. The current step is "Configure Routing".
Target group settings:

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

Health checks settings:

- Protocol: HTTP
- Path: /

Buttons at the bottom:

- Cancel
- Previous
- Next: Register Targets

On Register Targets page, Drag down

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

Click on “Add to register” button, Drag down

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#V2CreateLBWizard>. The page is titled "Step 5: Register Targets". A table lists instances with columns: Instance, Name, State, Security, Zone, Subnet ID, and Subnet CIDR. Two instances are listed: web1 (running) and web2 (running). A search bar above the table contains "Add to registered on port 80". Below the table are buttons for "Cancel", "Previous", and "Next: Review". The status bar at the bottom shows "Feedback English" and the date "© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use".

Verify that running instances are registered

Click on “Next: Review” 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#V2CreateLBWizard>. The page is titled "Step 5: Register Targets". A table titled "Registered targets" shows the registered instances: web1 and web2. Both are listed with port 80 and state "running". Below this is a table titled "Instances" which is currently empty. At the bottom are buttons for "Cancel", "Previous", and "Next: Review". The status bar at the bottom shows "Feedback English" and the date "© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use".

Verify

Check the summary

Drag Down

Step 6: Review

Please review the load balancer details before continuing.

Load balancer

- Name: ELBSales
- Scheme: Internet-facing
- Listeners: Port 80 - Protocol: HTTP
- IP address type: ipv4
- VPC: vpc-8fc3c41ee (default-vpc-oregon)
- Subnets: subnet-13f60e5a, subnet-8b9e38ec, subnet-19d0f141
- Tags

Security settings

- Certificate name
- Security policy name

Cancel Previous Create

Click on “Create” button

Step 6: Review

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

Targets

Instances: i-081a441f51fc90525 (web1):80, i-090dfbcc632605047 (web2):80

Cancel Previous Create

Verify

Load balancer successfully created.

The screenshot shows a browser window with three tabs open: 'EC2 Management Console', '54.218.192.19', and '54.203.188.115'. The main content area displays a success message: 'Successfully created load balancer ELBsales was successfully created. Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks.' A 'Close' button is visible in the bottom right corner of this message box. At the bottom of the screen, the AWS navigation bar includes links for Feedback, English, Privacy Policy, Terms of Use, and a timestamp of 7/25/2013.

4) Verification

To verify Websites are coming through Load Balancer

Go to **EC2 Dashboard** panel

Expanding **LOAD BALANCING**

Select **Load Balancer**.

Copy Load Balancer DNS Name

Name	DNS name	State	VPC ID
ELBsales	ELBsales-123441262.us-west-2.elb.amazonaws.com (A Record)	provisioning	vpc-89c341ee

In browser type load balancer DNS name

Verify website by frequently refreshing browser (press F5)



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



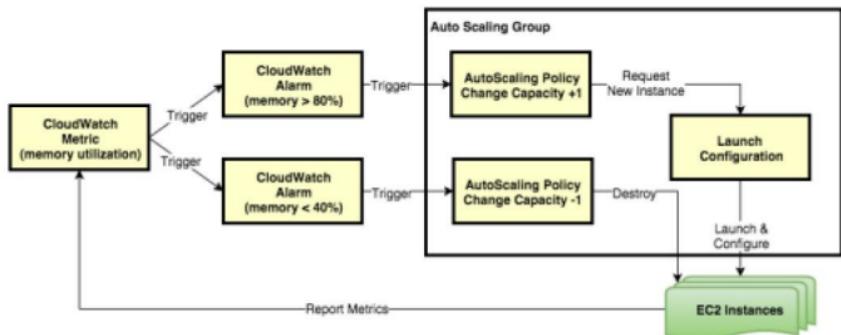
If you get this output, Congratulation your ELB configuration is successful.

Lab 13: To Configure Auto Scaling With Load Balancer

OBJECTIVE

To configure Auto Scaling in AWS

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

TASK

Launch Amazon linux instance

Configure web server

Stop the instance

Create AMI image of above instance

Configure Autoscaling launch configuration and autoscaling group

Configure Load balancer with Autoscaling

Practical Steps

1) First launch Amazon linux Instance and configure webserver

2) Create AMI image

To create AMI from this instance

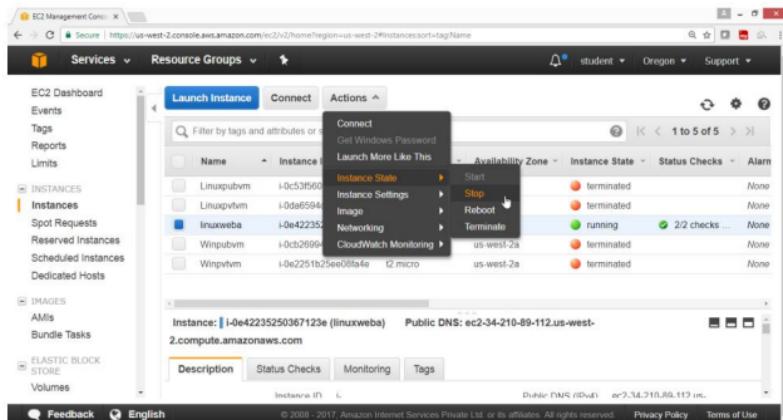
On “EC2 Dashboard” panel

Select the instance

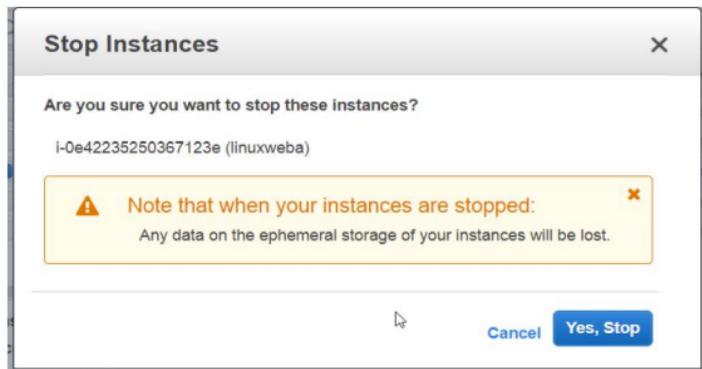
Click on **Action** button

Select Instance state

Click stop



Click on **Yes Stop** button

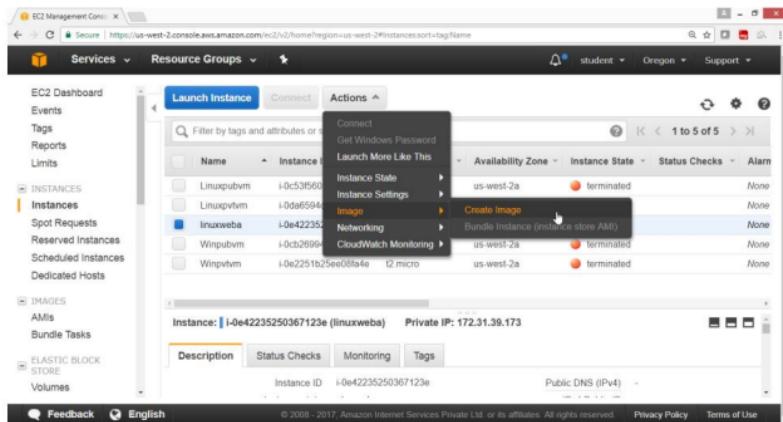


Select the stopped instance

Click on **Action** button

Select **image**

Click on **Create image** button

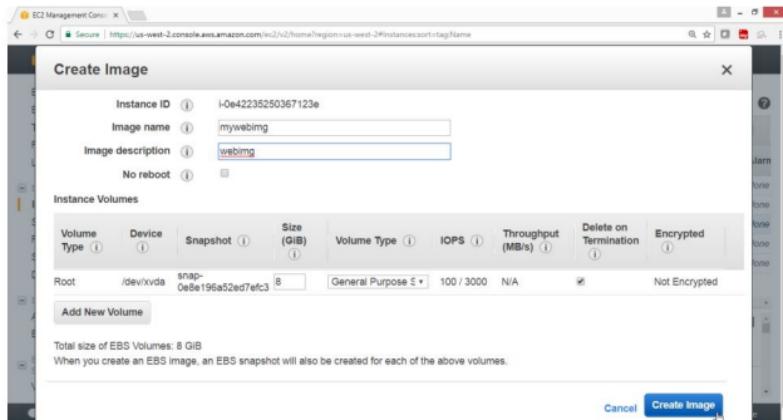


For Image name → mywebimg

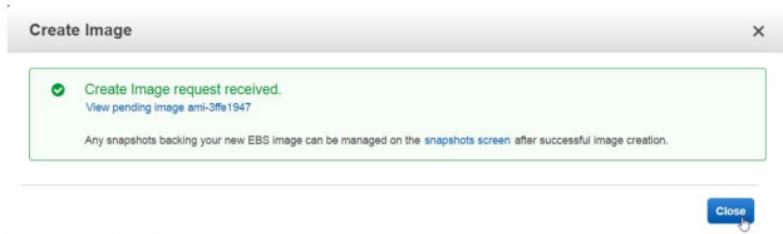
For Image description → webimg

Leave remaining default

Click on **Create image** button



Click on **Close** button



Verify AMI is created

On the **EC2 Dashboard** panel

Select **IMAGES**

Click on **AMIs**

Check the status is **available**

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation bar includes 'Services' (selected), 'Resource Groups', and several other options like 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES' (with sub-options like 'Instances', 'Spot Requests', 'Reserved Instances', 'Scheduled Instances', 'Dedicated Hosts'), 'IMAGES' (with sub-options like 'AMIs' - selected, 'Bundle Tasks'), and 'ELASTIC BLOCK STORE' (with sub-options like 'Volumes'). The main content area is titled 'Launch' and shows a table of AMIs. The table has columns: Name, AMI Name, AMI ID, Source, Owner, Visibility, and Status. One row is visible: 'mywebimg' (AMI Name), ami-3ffe1947 (AMI ID), 523251683217... (Source), 523251683217 (Owner), Private (Visibility), and available (Status). Below the table, a modal window is open for the AMI 'mywebimg', showing tabs for 'Details', 'Permissions', and 'Tags'. The 'Details' tab is active.

3) To Configure Auto Scaling

On the **EC2 Dashboard** panel

Select “**AUTO SCALING**”

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with sections like Load Balancing, Systems Manager, and Auto Scaling. The Auto Scaling section is currently selected. The main content area displays a summary of resources in the US West (Oregon) region:

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

Below this, there's a promotional message about Amazon Lightsail. To the right, there's a sidebar titled "Account Attributes" listing VPC, Default VPC, and Resource ID length management. At the bottom, there's an "Additional Information" section with links to Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, and Contact Us.

Create Instance

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

Launch Instance

Click on “Launch Configuration”

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#LaunchConfigurations>. The left sidebar has 'Launch Configurations' selected under the 'AUTO SCALING' section. The main content area displays the 'Welcome to Auto Scaling' page, which includes sections for 'Benefits of Auto Scaling' and three icons representing 'Reusable Instance Templates', 'Automated Provisioning', and 'Adjustable Capacity'. On the right, there's an 'Additional Information' sidebar with links like 'Getting Started Guide', 'Documentation', and 'Contact Us'.

Click on “Create Auto Scaling Group” button

This screenshot is identical to the one above, showing the 'Welcome to Auto Scaling' page. However, the 'Create Auto Scaling group' button in the center of the page is highlighted with a yellow box, indicating the user action required.

Click on “Create launch configuration” button

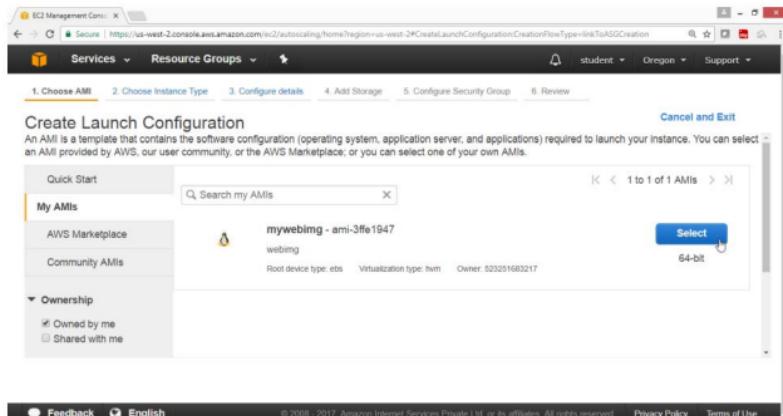
The screenshot shows the "Create Auto Scaling Group" wizard. Step 1: Create launch configuration. It features a diagram where a user icon and a gear icon combine to form three stacked instances. Below the diagram, text explains: "First, define a template that your Auto Scaling group will use to launch instances. You can change your template later." At the bottom right, there are "Cancel" and "Create launch configuration" buttons.

Click on “My AMI”

The screenshot shows the "Create Launch Configuration" wizard, step 1: Choose AMI. It lists two AMIs: "Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-6df1e514" and "Red Hat Enterprise Linux 7.3 (HVM), EBS General Purpose (SSD) Volume Type - ami-b55a51cc". Both have "Select" and "64-bit" buttons. On the left, a sidebar shows "Quick Start" with options: "My AMIs" (selected), "AWS Marketplace", and "Community AMIs". A "Free tier only" checkbox is also present. At the bottom, there are "Feedback", "English", and navigation links.

Select the AMI which was created with Webserver.

Click on **Select** button

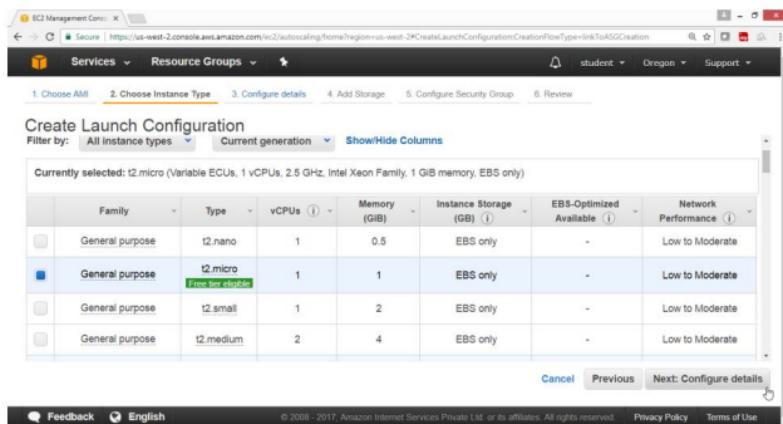


The screenshot shows the 'Create Launch Configuration' wizard. Step 1: Choose AMI is selected. A list of AMIs is shown, with one entry: 'mywebimg - ami-3ffe1947'. This entry includes a thumbnail of a penguin icon, the name 'mywebimg', the ID 'ami-3ffe1947', the root device type 'ebs', the virtualization type 'hvm', and the owner '523251683217'. To the right of the list is a blue 'Select' button. On the left, there are filters for 'My AMIs', 'AWS Marketplace', and 'Community AMIs', and a section for 'Ownership' with checkboxes for 'Owned by me' and 'Shared with me'. At the top right are 'Cancel and Exit' and 'Next Step' buttons.

Choose instance Type,

General purpose, t2.micro free tier

Click on **Next : Configuration Details**



The screenshot shows the 'Create Launch Configuration' wizard. Step 2: Choose Instance Type is selected. A table lists available instance types. The 't2.micro' row is highlighted with a green background and has a green 'Free tier eligible' label next to it. Other rows include 't2.nano', 't2.small', and 't2.medium'. The table has columns for Family, Type, vCPUs, Memory (GiB), Instance Storage (GB), EBS-Optimized Available, and Network Performance. At the bottom of the table are 'Cancel', 'Previous', and 'Next: Configure details' buttons. The 'Next: Configure details' button is highlighted with a blue border.

On Create launch Configuration page

Name → mylaunchconf

Monitoring → Enable check box

Click on **Next : Add storage** button

The screenshot shows the 'Create Launch Configuration' page in the AWS Management Console. The 'Name' field is set to 'mylaunchconf'. The 'Monitoring' section has the 'Enable CloudWatch detailed monitoring' checkbox checked. A note below says: 'Later, if you want to use a different launch configuration, you can create a new one and apply it to any Auto Scaling group. Existing launch configurations cannot be edited.' Navigation buttons at the bottom include 'Cancel', 'Previous', 'Skip to review' (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

Create Launch Configuration

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.

<https://docs.aws.amazon.com/console/ec2/launchinstance/storage> about storage options in Amazon EC2.

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

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Skip to review Next: Configure Security Group

Feedback English © 2006 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy 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 with the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2&createLaunchConfigurationCreationFlowType=linkToASGCreation>. The page is titled "Create Launch Configuration". The 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 "Configure Security Group" tab is selected. A sub-section titled "Create a new security group" is shown, with a radio button selected for "Create a new security group". Below it is a "Select an existing security group" link. The "Security group name" field contains "AutoScaling-Security-Group-1". The "Description" field shows "AutoScaling-Security-Group-1 (2017-08-09 13:47:40 +05:30)". A table displays a single security rule: "Type" is "SSH", "Protocol" is "TCP", "Port Range" is "22", and "Source" is "Anywhere". An "Add Rule" button is visible. At the bottom right are "Cancel", "Previous", and "Review" buttons, with "Review" being highlighted.

Check the summary

Click on “Create launch configuraton” button

EC2 Management Con... 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

Review the details of your launch configuration. You can go back to edit the details of each section before you finish.

⚠ Improve security of Instances launched using your launch configuration, mylaunchconf. Your security group, AutoScaling-Security-Group-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

mywebimg - ami-3ffe1947

ami-3ffe1947

Root device type: ebs Virtualization Type: hvm

Instance Type

t2.micro

Edit AMI Edit Instance type

Cancel Previous Create launch configuration

Feedback English © 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use 1:56 PM 6/8/2017

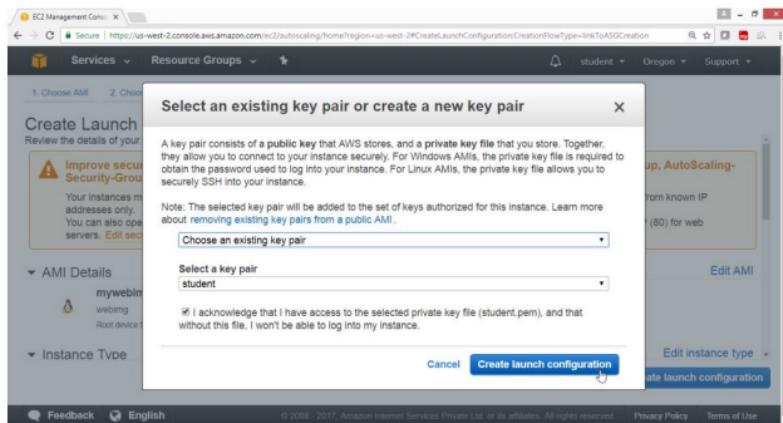
On "Select an existing key pair or create a new key pair" page

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 Congiration → 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-19400141 (172.31.0.0/20) | Default in us-west-2a
- subnet-13f60e5a (172.31.32.0/20) | Default in us-west-2a
- subnet-bb0e38ec (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

Create Auto Scaling Group

Launch Configuration mylaunchconf

Group name myautoscalinggrp

Group size Start with 1 instances

Network vpc-89c341ee (172.31.0.0/16) | default-vpc-oregon (d... [Create new VPC](#)

Subnet

- subnet-19d0f141(172.31.0.0/20) | Default in us-west-2c
- subnet-13f60e5a(172.31.32.0/20) | Default in us-west-2a
- subnet-8t9e38ec(172.31.16.0/20) | Default in us-west-2b

Create new subnet

Cancel [Next: Configure scaling policies](#)

On “Create Auto Scaling Group” page

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

Scale between [] and [] instances.

EC2 Management Console Secure https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateAutoScalingGroupSource=1&launchConfigurationName=myLaunch... student Oregon Support

Services Resource Groups

1. Configure Auto Scaling group details 2. Configure scaling policies 3. Configure Notifications 4. Configure Tags 5. Review

Create Auto Scaling Group

Keep this group at its initial size
 Use scaling policies to adjust the capacity of this group

Scale between and instances. These will be the minimum and maximum size of your group.

Scale Group Size

Name: Scale Group Size
Metric type: Average CPU Utilization
Target value:
Instances need: 300 seconds to warm up after scaling

Cancel Previous Review Next: Configure Notifications

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

Drag Down

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

EC2 Management Console Secure https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#CreateAutoScalingGroupSource=1&launchConfigurationName=myLaunch... student Oregon Support

Services Resource Groups

1. Configure Auto Scaling group details 2. Configure scaling policies 3. Configure Notifications 4. Configure Tags 5. Review

Create Auto Scaling Group

Scale Group Size

Name: Scale Group Size
Metric type: Average CPU Utilization
Target value:
Instances need: 300 seconds to warm up after scaling
Disable scale-in:

Scale the Auto Scaling group using step or simple scaling policies ⓘ

Cancel Previous Review Next: Configure Notifications

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

Select Increase Group Size

Click on "Add new alarm"

1. Configure Auto Scaling group details 2. Configure scaling policies 3. Configure Notifications 4. Configure Tags 5. Review

Create Auto Scaling Group

Increase Group Size

Name: Increase Group Size
Execute policy when: No alarm selected Add new alarm

Take the action: Add 0 instances

Add step

Instances need: 300 seconds to warm up after each step

Create a simple scaling policy

Decrease Group Size

Name: Decrease Group Size

Cancel Previous Review Next: Configure Notifications

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

Click on "create topic"

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: No SNS topics found...

Whenever: Average of CPU Utilization

Is: >= Percent

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

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

CPU Utilization Percent

0 10 20 30

04.00 06.00 08.00

myautoscalegrp

Cancel Create Alarm

On “Create Alarm” box, give values as

Send a notification to → Cpuutilizationabc

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: Cpuutilizationabc [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

Cancel Create Alarm

For Take the action → Add 1

Drag down and give Decrease policy parameters

Create Auto Scaling Group

Scale between and instances. These will be the minimum and maximum size of your group.

Increase Group Size

Name: Increase Group Size

Execute policy when: awsec2-myautoscalegrp-high-CPUUtilization Edit Remove
breaches the alarm threshold: CPUUtilization >= 30 for 300 seconds for the metric dimensions AutoScalingGroupName = myautoscalegrp

Take the action: Add instances when <= CPUUtilization < +infinity

Add step ⓘ

Instances need: seconds to warm up after each step

Cancel Previous Review Next: Configure Notifications

In Decrease Group wizard

Click on "Add new alarm"

Create Auto Scaling Group

Decrease Group Size

Name: Decrease Group Size

Execute policy when: No alarm selected ⏪

Take the action: Remove instances

Add step ⓘ

Create a simple scaling policy ⓘ

Scale the Auto Scaling group using a target tracking scaling policy ⓘ

Cancel Previous Review Next: Configure Notifications

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.com) create topic

Whenever: Average of CPU Utilization

Is: \leq 20 Percent

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

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

CPU Utilization Percent

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.com) create topic

Whenever: Average of CPU Utilization

Is: \leq 20 Percent

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

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

CPU Utilization Percent

Cancel Create Alarm

Check the summary

Click on “Next: Configure Notificaion”

Create Auto Scaling Group

Decrease Group Size

Name: Decrease Group Size

Execute policy when: awsEC2-myautoscalegrp-High-CPUUtilization [Edit](#) [Remove](#)
breaches the alarm threshold: CPUUtilization <= 20 for 300 seconds
for the metric dimensions AutoScalingGroupName = myautoscalegrp

Take the action: Remove instances when >= CPUUtilization > -infinity

Add step ⓘ

Create a simple scaling policy ⓘ

Cancel Previous Review Next: Configure Notifications

Click on “Add notification” button

Create Auto Scaling Group

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.

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.

Add notification

Cancel Previous Review Next: Configure Tags

Check the following output

Click on “Next: Configure tags”

The screenshot shows the 'Create Auto Scaling Group' wizard at step 3: 'Configure Notifications'. The 'Send a notification to:' field contains 'cputilizationabc (skmarhaan999@gmail.com)'. Below it, under 'Whenever instances:', several checkboxes are checked: 'launch', 'terminate', 'fail to launch', and 'fail to terminate'. A button labeled 'Add notification' is visible. At the bottom, there are 'Cancel', 'Previous', 'Review', and 'Next: Configure Tags' buttons. The 'Review' button is highlighted in blue.

For tag key → Name

For tag Value → WebAutoscale

Click on **Review** button

Create Auto Scaling Group

A tag consists of a case sensitive key-value pair that you can use to identify your group. For example, you could define a tag with Key = Environment and Value = Production. You can optionally choose to apply these tags to instances in the group when they launch. [Learn more](#).

Key	Value
Name	WebAutoscale

Add tag 49 remaining

Cancel Previous Review

Check the summary

Drag down

Create Auto Scaling Group

Please review your Auto Scaling group details. You can go back to edit changes for each section. Click **Create Auto Scaling group** to complete the creation of an Auto Scaling group.

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

Scaling Policies

Edit scaling policies

Create Auto Scaling group

Drag down

Click on “Create Auto Scaling 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>CreateAutoScalingGroup\[source=LaunchConfigurationName=mylaunchconfig&autoScalingGroupName=autoScalingGroup1\]](https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2>CreateAutoScalingGroup[source=LaunchConfigurationName=mylaunchconfig&autoScalingGroupName=autoScalingGroup1]). The page is titled "Create Auto Scaling Group". Step 5, "Review", is selected. The configuration includes:

- Scaling Policies:** Increase Group Size (With alarm = awsec2-myautoscalegrp-High-CPU.Utilization, Add 1 instances and 300 seconds for instances to warm up) and Decrease Group Size (With alarm = awsec2-myautoscalegrp-High-CPU.Utilization, Remove 1 instances).
- Notifications:** Cpuutilizationabc (skmarhaan99@gmail.com) with events launch, terminate, fail to launch, fail to terminate.
- Tags:** Name: WebAutoscale, Tag new instances.

At the bottom right, there is a large blue button labeled "Create Auto Scaling group".

Successfully created

Click on Close 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\[source=LaunchConfigurationName=mylaunchconfig&autoScalingGroupName=autoScalingGroup1\]](https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2>CreateAutoScalingGroup[source=LaunchConfigurationName=mylaunchconfig&autoScalingGroupName=autoScalingGroup1]). The page is titled "Auto Scaling group creation status". A green box at the top left says "Successfully created Auto Scaling group" with a link "View creation log". Below it, there are sections for "View" (View your Auto Scaling groups, View your launch configurations) and "Helpful resources" (Here are some helpful resources to get you started). At the bottom right, there is a blue button labeled "Close".

Verification

Now go to EC2 Dash Board

Click on Instances

Observer that WebAutoscale instance got launched

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
linuxweba	i-042235250367123e	t2.micro	us-west-2a	stopped	None	None
WebAutoscale	i-0a7aaafe87044125e	t2.micro	us-west-2c	running	Initializing	None

Now login to Web Autoscale instance

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

Description	Status Checks	Monitoring	Tags
Instance ID: i-0a7aaafe87044125e	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

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with navigation links: EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, and Elastic Block Store Volumes. 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 titled "Instances" with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. There are four rows in the table:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
linuzwba	i-0e42235250367123e	t2.micro	us-west-2a	stopped	None	None
WebAutoscale	i-0456526a506cdda75	t2.micro	us-west-2a	running	2/2 checks	None
WebAutoscale	i-0a7aaaef67044125e	t2.micro	us-west-2c	running	2/2 checks	None
WebAutoscale	i-07bb6b3d034adc7c	t2.micro	us-west-2b	running	2/2 checks	None

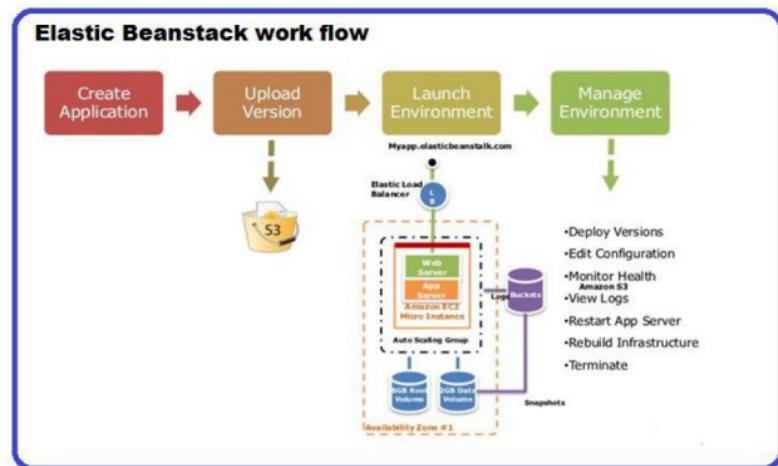
Below the table, a message says "Select an Instance above". At the bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use.

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 interface. At the top, there's a navigation bar with tabs for Services, Resource Groups, and other account details. Below the navigation is a search bar and a 'Create a Group' button. The main content area is titled 'Amazon Web Services' and lists various services under categories like Compute, Storage, Developer Tools, Internet of Things, Game Development, and Mobile Services. The 'Compute' category is expanded, showing EC2, EC2 Container Service, Lightsail, and Elastic Beanstalk. The 'Elastic Beanstalk' icon is highlighted with a red box. The 'Resource Groups' section on the right provides information about what a resource group is and how to create one. Other sections include 'Getting Started' with links to documentation and the AWS Marketplace.

https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2

"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-header with the Elastic Beanstalk logo and a 'Create New Application' button. The main content area is titled 'Welcome to AWS Elastic Beanstalk'. It features a summary card with metrics: 53.6 (Average response time), 148K (Sum Requests), 65% (CPU Utilization), 354KB (Avg Network In), and 12KB (Avg Network Out). Below this is a 'Monitoring' section with two line graphs showing CPU utilization and network traffic over time. At the bottom of the page is a blue 'Get started' button.

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

Application Name → Tomcatapp

Environment Name → Tomcatenv

Drag down

The screenshot shows the AWS Elastic Beanstalk Management console with the URL <https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2&gettingStarted>. The page title is "Create a web app". It has sections for "Application information" and "Environment information". In the Application information section, the "Application name" is set to "Tomcatapp". In the Environment information section, the "Environment name" is set to "tomcatenv" and the "Domain" field contains "Leave blank for autogenerated value" and "us-west-2.elasticbeanstalk.com".

Elastic Beanstalk Manager

Secure | https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2&gettingStarted

Services Resource Groups

Elastic Beanstalk

Create New Application

Create a web app

Create a new application and environment with a sample application or your own code. By creating an environment, you allow AWS Elastic Beanstalk to manage AWS resources and permissions on your behalf.

Learn more

Application information

Application name Up to 100 Unicode characters, not including forward slash (/)

Environment information

Choose the name, subdomain, and description for your environment. These cannot be changed later.

Environment name

Domain us-west-2.elasticbeanstalk.com

In Platform box select **Tomcat**

Drag down

The screenshot shows the 'Base configuration' section of the AWS Elastic Beanstalk console. The 'Platform' dropdown menu is open, displaying options like 'Choose a platform', 'Preconfigured', and 'Tomcat'. The 'Tomcat' option is highlighted with a blue selection bar. Below the dropdown, there's a note about moving to a new design and links for feedback and terms of use.

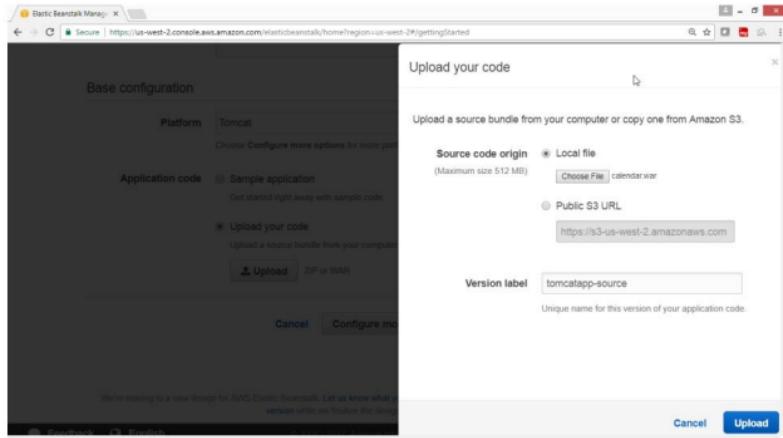
Select **Upload your code**

The screenshot shows the 'Base configuration' section with 'Tomcat' selected in the 'Platform' dropdown. The 'Application code' section has 'Upload your code' selected. A note at the bottom indicates a design change and provides links for feedback and terms of use.

Upload calendar.war file

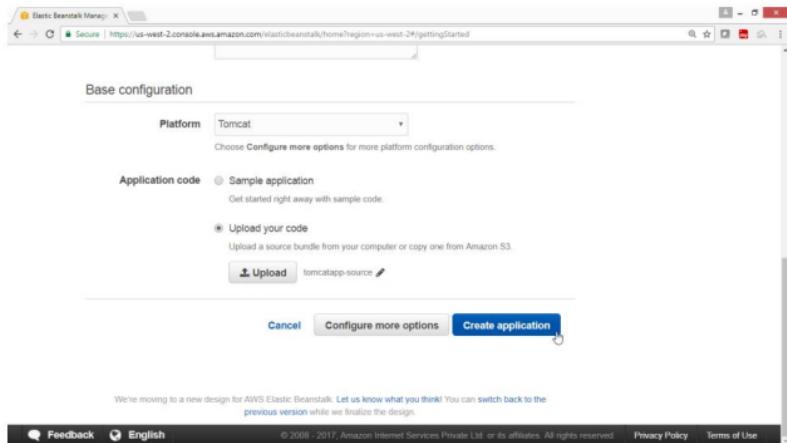
Click on **Upload** button

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

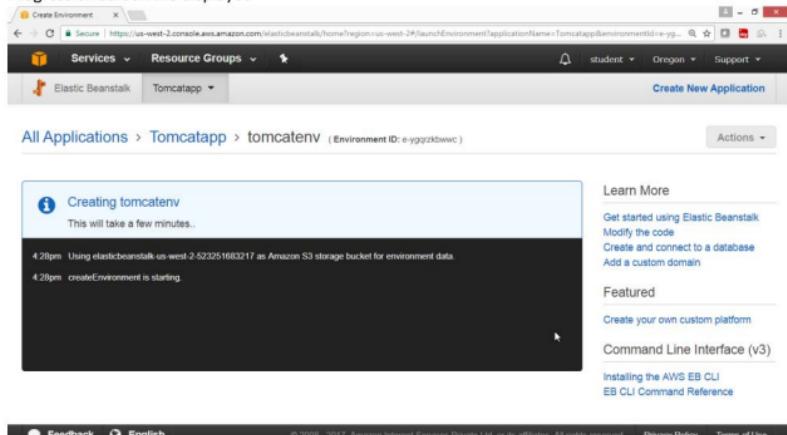
Create application

We're moving to a new design for AWS Elastic Beanstalk. Let us know what you think! You can switch back to the previous version while we finalize the design.

Verification :

Tomcat application at background is getting created,

Progress on screen are displayed



Creating tomatcatenv

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

[Create Environment](#)

[https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2&launchEnvironment?applicationName=Tomcatapp&environmentId=e-39...\[Secure\]\(#\)](#)

k.us-west-2.elasticbeanstalk.com

i Creating tomcatenv

This will take a few minutes..

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:
aws-e-3grzkbwc-stack-AWSEBSecurityGroup-1NRF9H19B86AF

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

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 AWS Elastic Beanstalk console with the following details:

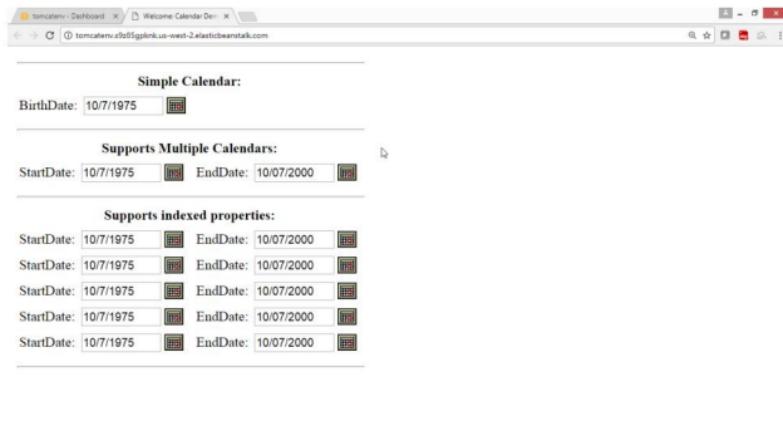
- Region:** us-west-2
- Environment ID:** e-ygqrzkbwwc
- URL:** tomcatenv.s9z85pkn.us-west-2.elasticbeanstalk.com
- Health Status:** Ok
- Running Version:** tomcatapp-source
- Actions:** Create New Application, Actions (dropdown)

Verification

Open any Browser

Click on URL link

Website is open

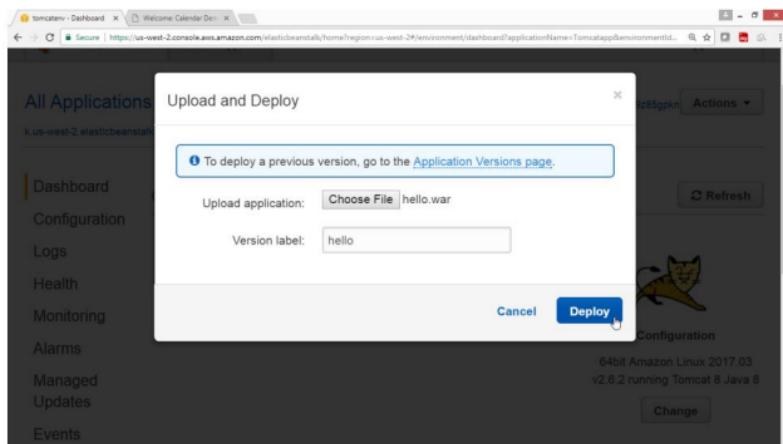


To Deploy another war file for eg hello.war

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 'tomcatenv' application. The URL is https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2&environmentName=Tomcatapp&environmentId=e-yqqrzkbwwc. The page displays the 'Overview' section with a green health status icon (checkmark), the running version 'hello', and a yellow cat icon representing configuration. It also shows system details: '64bit Amazon Linux 2017.03 v2.6.2 running Tomcat 8 Java 8'. A 'Change' button is visible for configuration.

Verify the website

The screenshot shows a browser window displaying the 'Hello Index' page at https://tomcatenv.sflfsgplnk.us-west-2.elasticbeanstalk.com. The page content includes the heading 'Hello Index' and a note to 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 main area displays a list of applications under 'All Applications'. One application, 'Tomcatapp', is selected and highlighted with a green box. A context menu is open next to it, listing options: 'Create environment', 'Delete application' (which is highlighted in blue), 'View application versions', 'View saved configurations', and 'Restore terminated environment'. On the left sidebar, there are sections for 'Learn More' (links to get started, modify code, connect to database, add custom domain) and 'Featured' (link to create a custom platform). Below the sidebar is a 'Command Line Interface (v3)' section.

This screenshot shows a confirmation dialog box titled 'Delete Application'. The question inside the box is 'Are you sure you want to delete the application: Tomcatapp?'. At the bottom right of the dialog are two buttons: 'Cancel' and a red 'Delete' button, which has a mouse cursor hovering over it. The background of the dialog shows the same application details as the previous screenshot, including the green-highlighted 'Tomcatapp' entry with its configuration information. The overall interface is identical to the one in the first screenshot, with the addition of the modal dialog.

Application will now get terminated

The screenshot shows the AWS Elastic Beanstalk Applications page. The top navigation bar includes 'Services' (selected), 'Resource Groups', 'student', 'Oregon', and 'Create New Application'. Below the navigation is a search bar labeled 'Filter by Application Name:' and a 'Actions' button. The main content area is titled 'All Applications' with a back arrow. It lists 'Tomcatapp' with a status of 'terminated'. A detailed box for 'tomcatenv (Terminated)' provides information: 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.elasticbean...'. On the left sidebar, there are sections for '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), and 'Command Line Interface (v3)'.

Verification

After termination following screen will come

The screenshot shows the AWS Elastic Beanstalk Welcome page. The top navigation bar is identical to the previous page. The main content features a large 'Welcome to AWS Elastic Beanstalk' heading. To the left is a screenshot of a browser displaying the Elastic Beanstalk Metrics dashboard, which shows various performance metrics like CPU Utilization, Network In, and Network Out. To the right of the heading is a descriptive text block: 'With Elastic Beanstalk, you can **deploy, monitor, and scale** an application quickly and easily. Let us do the heavy lifting so you can focus on your business.' Below this is another text block: 'To deploy your existing web application, create an application source bundle and then **create a new application**. If you’re using Git and would prefer to use it with our command line tool, please see [Getting Started with the EB CLI](#).' At the bottom, there is a final note: 'To deploy a **sample application**, click [Get started](#), choose a name, select a platform and'. The bottom of the page has a footer with 'Create New Application' and other navigation links.

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 links for Global and Support. Below the header, a navigation bar has 'Services' and 'Resource Groups' dropdowns, along with 'Documentation' and 'Quick tips'. The main content area is titled 'Amazon S3' and features a search bar with placeholder 'Search for buckets'. Below the search bar are three buttons: '+ Create bucket', 'Delete bucket', and 'Empty bucket'. A tooltip 'Switch to the old console' is displayed over the '+ Create bucket' button. The main table lists 14 buckets across 2 regions. The columns are 'Bucket name', 'Region', and 'Date created'. The buckets listed are:

Bucket name	Region	Date created
alt3jane	US West (Oregon)	Jul 3, 2017 8:17:52 PM
arunindajava	US West (Oregon)	Jun 22, 2017 10:17:16 AM
cf-templates-smithmincsg-us-west-2	US West (Oregon)	Jul 2, 2017 9:50:36 AM
elasticbeanstalk-ap-south-1-522351683217	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
hydamerpetas072107	US West (Oregon)	Jul 7, 2017 8:43:10 PM
hydcisoumontamp	US West (Oregon)	Jun 18, 2017 8:22:19 PM
mastanav07junekey	US West (Oregon)	Jul 1, 2017 9:26:19 PM
mastanciousfront	US West (Oregon)	Jun 18, 2017 2:32:48 PM
oracleutd	US West (Oregon)	Jul 21, 2017 9:22:53 AM

The screenshot shows the AWS Elastic Beanstalk Management Console interface. On the left, there's a sidebar with links for EC2, Console Home, CloudWatch, Simple Notification Service, and VPC. The main area is organized into several sections:

- Compute**: EC2, 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.
- Storage**: S3, EFS, Glacier, Storage Gateway.
- Management Tools**: CloudWatch, CloudFormation, CloudTrail, Config, OpsWorks, Service Catalog, Trusted Advisor, Managed Services.
- Artificial Intelligence**: Lex, Polly, Rekognition, Machine Learning.
- Internet Of Things**: AWS IoT, AWS Greengrass.
- Database**: RDS, DynamoDB, ElastiCache.

At the bottom of the page, the URL is https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2#/welcome.

Select elastic Beanstalk Bucket, Click Properties

Select Permissions

The screenshot shows the AWS S3 Management Console. At the top, it says "Services" and "Resource Groups". Below that, there are tabs for "Create Bucket" and "Actions". A dropdown menu shows "All Buckets (14)". The main list shows various buckets:

- el13ame
- arunadasra
- ctemplates-streamlit-hd.us-west-2
- elasticbeanstalk-ap-west-1-523251683217
- elasticbeanstalk-us-west-2-523251683217
- hydarometeo72107
- hydcloudfronting
- mastanav0719rekky
- mastancloudfront
- oraclehyd
- ravibacaws
- orkanthyd
- stationwhyd.com
- www.mawakilaw.com

The bucket "elasticbeanstalk-us-west-2-523251683217" is highlighted. At the top right, there are tabs for "None", "Properties", and "Transfers", with "Properties" being the active tab. At the bottom, there are links for "Feedback", "English", and copyright information from 2008-2017.

Click "Edit bucket policy"

The screenshot shows the AWS S3 Management Console. On the left, a sidebar lists 'All Buckets (14)' with various bucket names. On the right, the main panel displays details for the bucket 'elasticbeanstalk-us-west-2-523251683217'. The 'Permissions' section is selected, showing a grantee 'skmval999' with permissions 'List', 'Upload/Delete', and 'View Permissions'. Below this are buttons for 'Add more permissions', 'Edit bucket policy' (which is highlighted with a cursor), and 'Add CORS Configuration'. At the bottom are links for 'Static Website Hosting' and 'Logging', and a 'Save' button.

In Bucket Policy Editor wizard,

Click Delete to remove policy, click OK

The screenshot shows the 'Bucket Policy Editor' dialog. It displays a JSON policy document with one statement. The 'Delete' button is highlighted with a cursor. The policy document is as follows:

```
{ "Version": "2008-10-17", "Statement": [ { "Sid": "eb-58950adbc-fc6b-11e2-89e0-0800277d041b", "Effect": "Deny", "Principal": "*", "Action": "s3:DeleteObject", "Resource": "arn:aws:s3:::elasticbeanstalk-us-west-2-523251683217/*" } ] }
```

Click on Save button

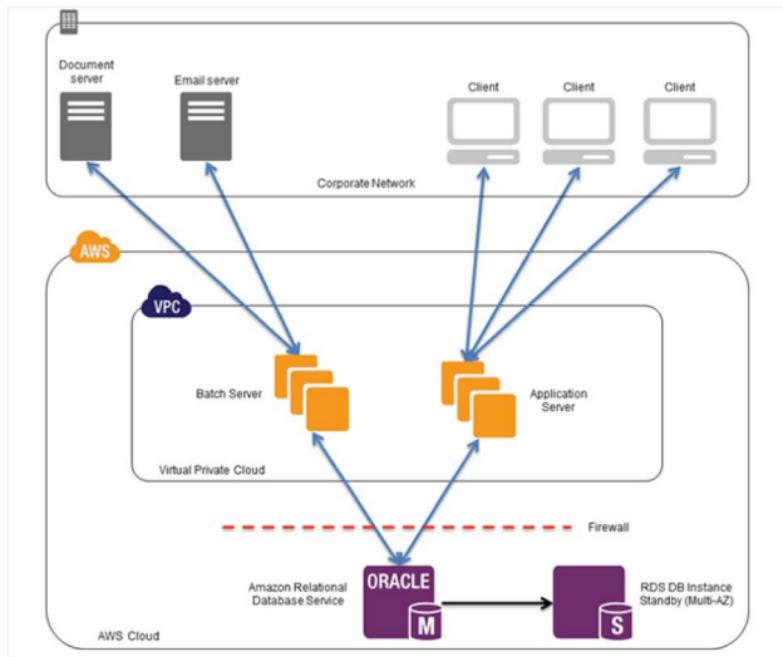
The screenshot shows the AWS S3 Management Console. On the left, there's a sidebar titled 'Services' with 'Resource Groups' selected. Below it, a 'Create Bucket' button and an 'Actions' dropdown are visible. The main area is titled 'All Buckets (14)' and lists various buckets. One bucket, 'elasticbeanstalk-us-west-2-523251683217', is highlighted with a blue selection bar. To the right, a detailed view of this bucket is shown. The bucket name is 'elasticbeanstalk-us-west-2-523251683217'. It was created in the 'Oregon' region on 'Wed Jul 12 21:30:22 GMT+0300 2017' by the owner 'skmval999'. Under the 'Permissions' section, there's a grantee input field with 'skmval999' and several checkboxes for permissions: 'List', 'Upload/Delete', and 'View Permissions'. Below this are buttons for 'Add more permissions', 'Add bucket policy', and 'Add CORS Configuration'. At the bottom of the permissions section is a 'Save' button, which is highlighted with a mouse cursor. Other sections visible include 'Static Website Hosting' and 'Logging'.

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 with `AmazonRDSFullAccess`

Task

Create Amazon Relational Database Service

Verify connection from mysql client command line tool

Verify Connection using MySQL Workbench client application

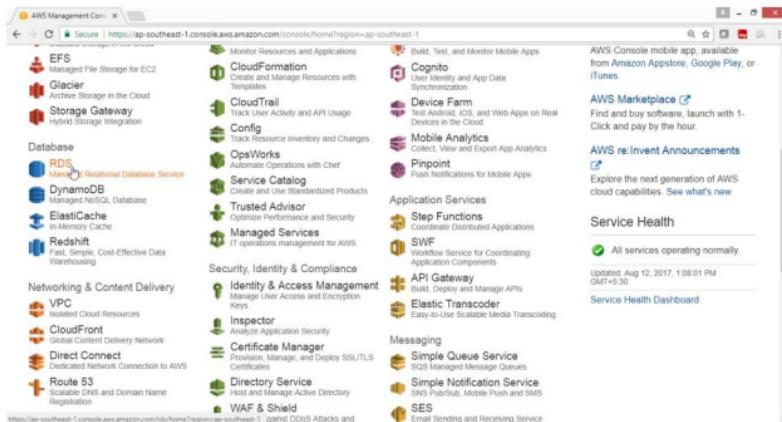
Practical Steps

To create Amazon Relational Database Service

From the AWS console

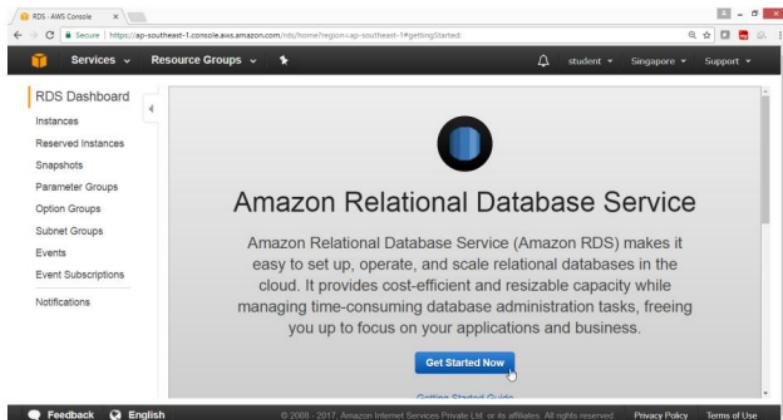
Select Database

Click on RDS service



In “RDS Dashboard”, wizard

Click “Get Started Now”, button



In Select Engine, wizard

Click on MySQL

Click on Select button

The screenshot shows the AWS RDS console with the "Select Engine" step open. A message at the top says "To get started, choose a DB Engine below and click Select." Below this, there are five engine options: MySQL (selected), MariaDB, PostgreSQL, Oracle, and SQL Server. Each option has a small icon and a brief description. The MySQL section includes a note about free tier eligibility. On the right side of the MySQL card is a blue "Select" button.

In Production wizard

select Dev/Test, Choose MySQL

The screenshot shows the AWS RDS console with the "Production" step of the "Production" wizard open. On the left, a sidebar lists steps: Step 1: Select Engine, Step 2: Production? (selected), Step 3: Specify DB Details, Step 4: Configure Advanced Settings. The main area has two sections: "Production" and "Dev/Test". Under "Production", there is a radio button for "MySQL" which is selected. Under "Dev/Test", there is also a radio button for "MySQL" which is unselected. A note next to the "Dev/Test" MySQL button states: "This instance is intended for use outside of production or under the RDS Free Usage Tier." At the bottom, there are "Cancel", "Previous", and "Next Step" buttons.

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 (which is active), and Step 4: Configure Advanced Settings. Below the sidebar, there's a note about estimating monthly costs using the AWS Simple Monthly Calculator.

The main panel is titled 'Specify DB Details' and has a 'Free Tier' section. It describes the Free Tier benefits and includes a checkbox for 'Only show options that are eligible for RDS Free Tier'. The 'Instance Specifications' section contains the following fields:

- DB Engine: mysql
- License Model: general-public-license
- DB Engine Version: MySQL 5.6.35
- DB Instance Class: Select One (dropdown menu)

A callout box points to the DB Engine Version field with the text: "Version number of the database engine to be used for this instance." At the bottom of the panel, there's a link to review known issues/limitations: "Review the Known Issues/Limitations to learn about potential compatibility issues with specific database versions."

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

RDS - AWS Console

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

Services Resource Groups

student Singapore Support

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](#).

DB Instance	18.98 USD
Storage	0.69 USD
Total	19.67 USD

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

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

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

⚠ Provisioning less than 100 GB of General Purpose (SSD) storage for high throughput workloads could result in higher latencies upon exhaustion of the initial General Purpose (SSD) IO credit balance. Click here for more details.

- General Purpose (S) storage is suitable for broad range of data workloads. Provides up to 3 IOPS and ability to burst to 3,000 IOPS.
- Provisioned (IOPS) storage is suitable for I/O-intensive data 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

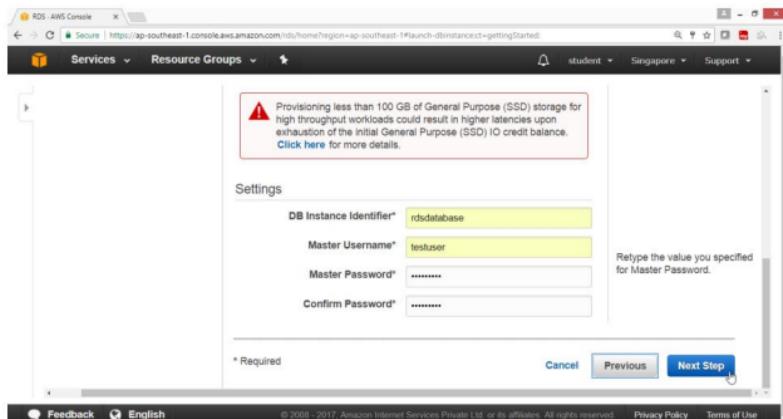
For DB Instance Identifier → rdsdatabase

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)	→ <u>Create new Security Group</u>

The screenshot shows the AWS RDS console with the 'Configure Advanced Settings' wizard open. The current step is 'Step 4: Configure Advanced Settings'. The 'Network & Security' section is displayed. In the 'VPC Security Group(s)' dropdown, 'Create new Security Group' is selected. A tooltip on the right side of the screen provides information about security groups, stating they have rule sets that authorize connections from EC2 instances or devices that need to access data stored in the DB. It also notes that by default, security groups do not authorize any connections and must define rules for specific instances and devices to connect to the DB.

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 '3306'. The 'DB Parameter Group' is 'default.mysql5.6'. The 'Option Group' is 'default.mysql-5-6'. 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 an instance, as in "mydb". Amazon RDS does not create a database when it creates an instance.' At the bottom, there is a note about automated backups and a link to the MySQL documentation.

Provider Following Values

Under Backup

Backup Retention Period → 7 days

Backup Window → No Preference

Under Monitoring

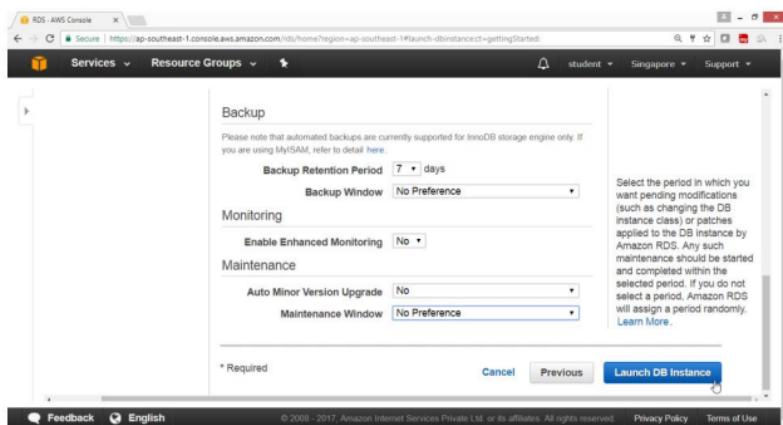
Enable Enhanced Monitoring → No

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 interface. On the left, a vertical navigation bar lists steps: Step 1: Select Engine, Step 2: Production?, Step 3: Specify DB Details, and Step 4: Configure Advanced Settings. To the right, a main panel displays a green checkmark icon and the text "Your DB Instance is being created." Below this, a note says "Note: Your instance may take a few minutes to launch." Underneath, a section titled "Connecting to your DB Instance" contains the text "Once Amazon RDS finishes provisioning your DB instance, you can use a SQL client application or utility to connect to the instance." A link "Learn about connecting to your DB instance" is provided. At the bottom right of the main panel is a blue button labeled "View Your DB Instances".

Under status column

Verify creating

The screenshot shows the AWS RDS Dashboard. On the left, a sidebar menu includes "Instances", "Reserved Instances", "Snapshots", "Parameter Groups", "Option Groups", "Subnet Groups", "Events", "Event Subscriptions", and "Notifications". The main content area has tabs "Launch DB Instance", "Show Monitoring", and "Instance Actions". It features a search bar "Search DB Instances..." and a filter dropdown "Filter: All Instances". Below this, a table header includes columns: Engine, DB Instance, Status, CPU, Current Activity, Maintenance, Class, and VPC. A single row is visible in the table, showing "MySQL" as the Engine, "rdsdatabase" as the DB Instance, "creating" as the Status, and "None" as the Current Activity. The table footer indicates "Viewing 1 of 1 DB Instances".

Select MySQL Engine

The screenshot shows the AWS RDS Dashboard. On the left sidebar, under the 'Instances' section, there is a single entry for a MySQL database named 'rdsdatabase'. The status of this instance is listed as 'creating'. Below the instance list, there is a table titled 'Alarms and Recent Events' showing three recent events: 'DB Instance deleted' at 10:07 PM, 'DB Instance shutdown' at 10:03 PM, and 'Finished DB Instance backup' at 9:05 PM. To the right of the instance list, there is a 'Monitoring' section with tabs for CPU and Memory, both showing 'No Data'.

Under status column

Verify backing-up

This screenshot is identical to the one above, but the status of the MySQL database 'rdsdatabase' has changed to 'backing-up'. The 'Alarms and Recent Events' table now shows a new event: 'DB Instance backup' at 9:05 PM. The monitoring section remains the same, showing 'No Data' for both CPU and Memory.

Under status column

Verify available

The screenshot shows the AWS RDS Dashboard. On the left, a sidebar lists various options: 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 highlighted: Engine: MySQL, DB Instance: rdsdatabase, Status: available, CPU: 1.33%, Current Activity: 0 connections, Maintenance: None, Class: db.t2.micro. Below the table, there are two sections: 'Alarms and Recent Events' and 'Monitoring'. The 'Alarms and Recent Events' section shows three events: 'Aug 12 1:49 PM Finished DB Instance backup', 'Aug 12 1:45 PM Backing up DB Instance', and 'Aug 12 1:44 PM DB Instance created'. The 'Monitoring' section shows CPU usage at 1.42% and Memory usage at 543 MB.

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.
mysql> █
```

To see the list of databases;

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

mysql> █
```

Use the database

Create table

Insert values in tables

```
mysql>
mysql> use salesdb;
Database changed
mysql>
mysql> create table tutorials_tbl(tutorial_id INT NOT NULL AUTO_INCREMENT,tutorial_title V
ARCHAR(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 |
| salesdb |
| sys |
+-----+
6 rows in set (0.02 sec)

mysql> use salesdb;
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;

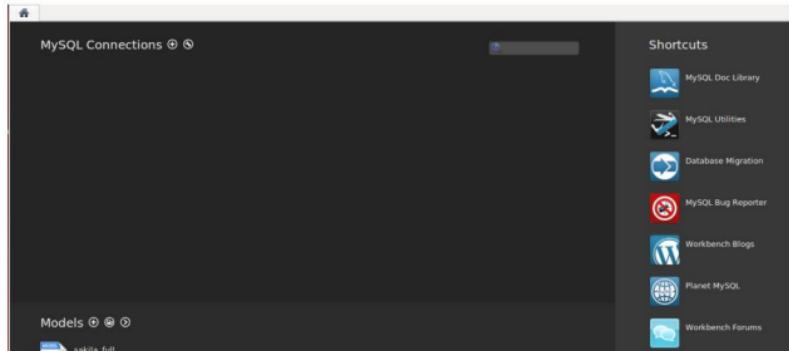
```
mysql> select * from tutorials_tbl;
+-----+-----+-----+-----+
| tutorial_id | tutorial_title | tutorial_author | submission_date |
+-----+-----+-----+-----+
| 1 | Learn PHP | John Poul | 2017-08-12 |
| 2 | Learn MySQL | Abdul S | 2017-08-12 |
| 3 | JAVA Tutorial | Sanjay | 2007-05-06 |
+-----+-----+-----+-----+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

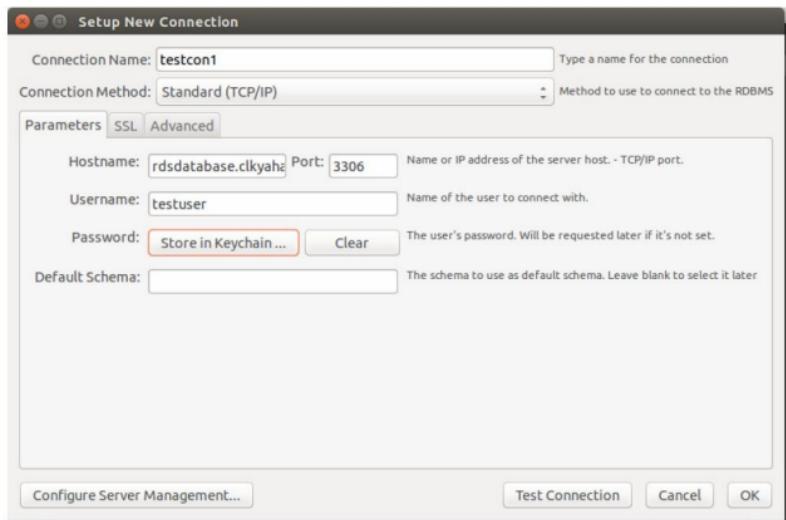
Hostname → copy RDS url

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

Port → 3306

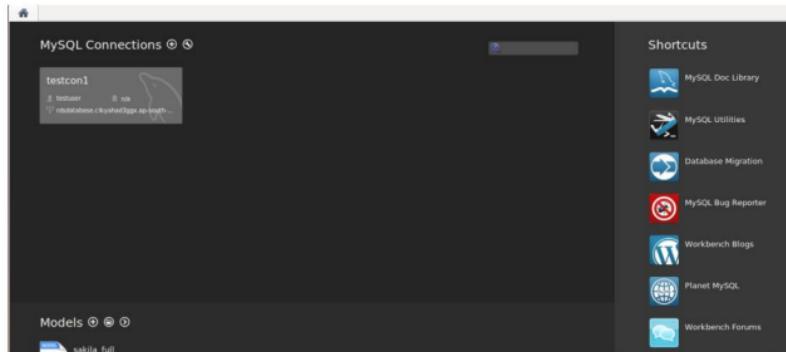
Username → testuser

Password → *****

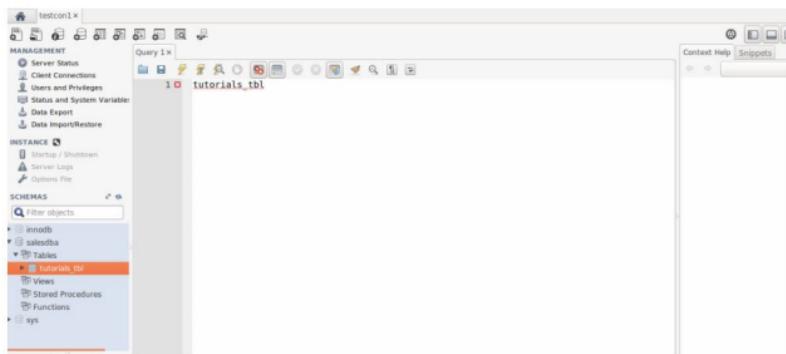


Verify

Connection is getting established.



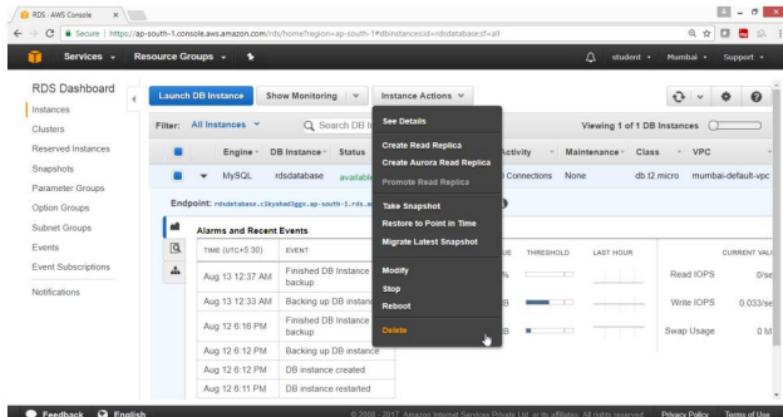
So we can see that tables are listed in Mysql clients.



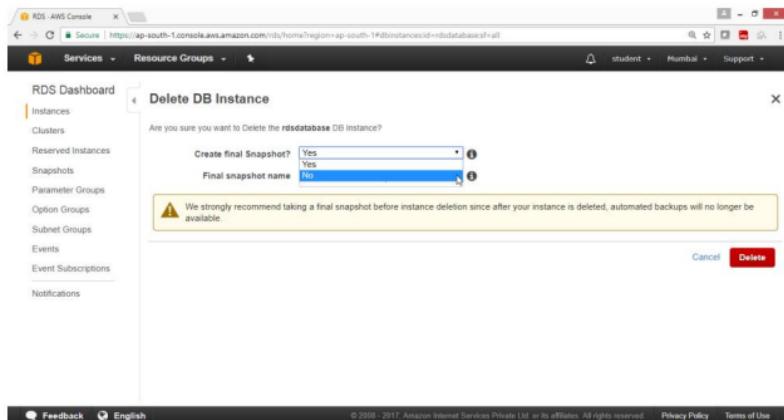
3. To Delete the RDS instance

3.1 Open RDS Dashboard , select instance

drop down Instance **Action button**, select **Delete**

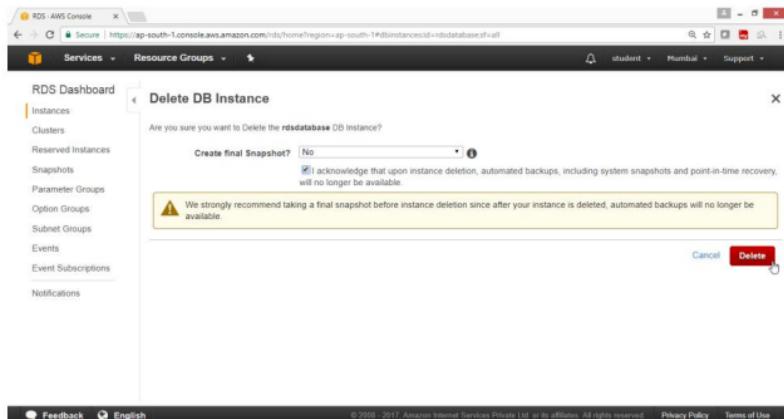


For Create final snapshot → No



Select acknowledge check box

Click on Delete button



Verify

In status column → deleting

The screenshot shows the AWS RDS Dashboard. On the left, there's a sidebar with 'Instances' selected under 'RDS Dashboard'. The main area has tabs for 'Launch DB Instance', 'Show Monitoring', and 'Instance Actions'. A search bar says 'Search DB Instances...'. Below it, a table lists one instance:

Engine	DB Instance	Status	CPU	Current Activity	Maintenance	Class	VPC	Multi-AZ
MySQL	rdsdatabase	deleting	1.00%	0 Connections	None	db.t2.micro	mumbai-default-vpc	No

Below the table, the 'ndpoint' is listed as `rdsdatabase.ckiyahalggx.ap-south-1.rds.amazonaws.com:3306 (authorized)`. There are two sections: 'Alarms and Recent Events' and 'Monitoring'. The 'Alarms and Recent Events' section shows several events:

TIME (UTC+5:30)	EVENT
Aug 13 12:37 AM	Finished DB Instance backup
Aug 13 12:33 AM	Backing up DB instance
Aug 12 6:16 PM	Finished DB Instance backup
Aug 12 6:12 PM	Backing up DB instance
Aug 12 6:12 PM	DB instance created
Aug 12 6:11 PM	DB instance restarted

The 'Monitoring' section displays four metrics: CPU, Memory, Storage, and Swap Usage, each with current values and thresholds.

Delete Confirmed

The screenshot shows the AWS RDS Dashboard. The sidebar is identical to the previous one. The main area now displays a confirmation message:

elational 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, 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.

Note: Your DB Instances will launch in the Asia Pacific (Mumbai) region.

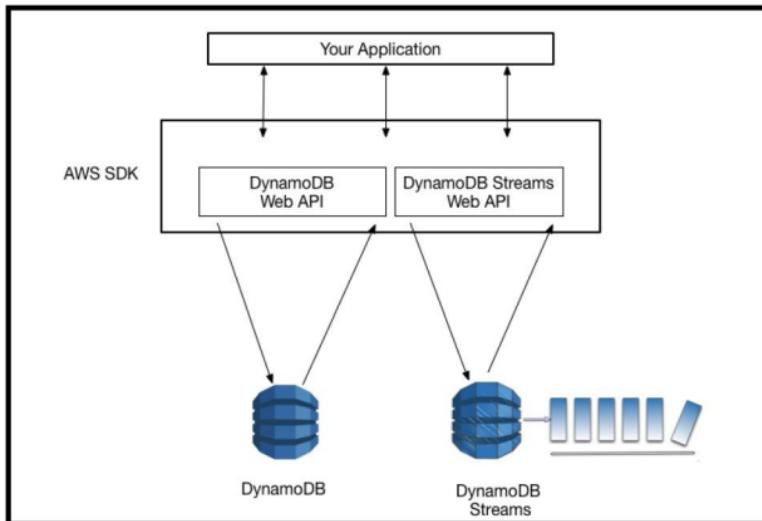
A progress bar at the bottom indicates the process is 1% complete.

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

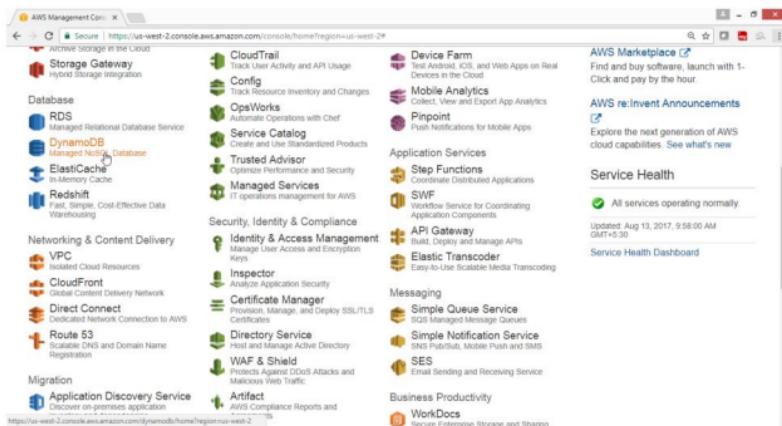
1) To Create an Amazon DynamoDB table

To Create Table

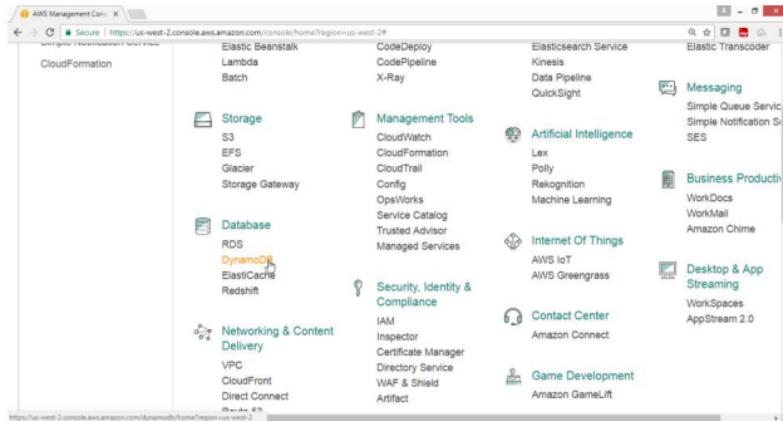
Open AWS console

Select services Database

Click on **DynamoDB**

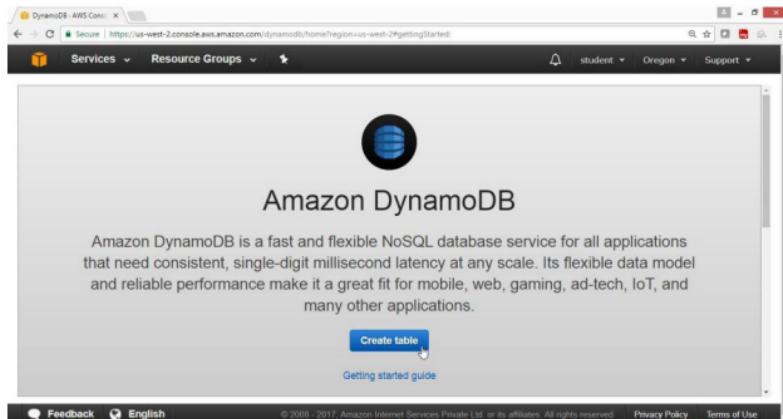


OR



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 interface. At the top, there's a header bar with the AWS logo, 'Services', 'Resource Groups', and user information ('student', 'Oregon', 'Support'). Below the header is a 'Tutorial' button and a help icon. The main form has a title 'Create DynamoDB table'. It contains fields for 'Table name*' (set to 'Salestable') and 'Primary key*' (set to 'Partition key' with 'itemno' selected as a 'String' type). There's also an option to 'Add sort key'. Under 'Table settings', it says 'Default settings provide the fastest way to get started with your table. You can modify these default settings now or after your table has been created.' A checkbox for 'Use default settings' is checked, with a note below stating 'No secondary indexes.' At the bottom, there are links for 'Feedback', 'English', '© 2006–2011 Amazon Internet Services Private Ltd or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Under Table settings

Select “Use default settings” check box

click on **Create** button

DynamoDB - AWS Console Secure https://us-west-2.console.aws.amazon.com/dynamodb/home?region=us-west-2#createtable

Services Resource Groups

Add sort key

Table settings

Default settings provide the fastest way to get started with your table. You can modify these default settings now or after your table has been created.

Use default settings

- No secondary indexes.
- Provisioned capacity set to 5 reads and 5 writes.
- Basic alarms with 80% upper threshold using SNS topic "dynamodb".

Info You do not have the required role to enable Auto Scaling by default.
Please refer to documentation.

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.

Cancel Create

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

Creating

DynamoDB - AWS Console Secure https://us-west-2.console.aws.amazon.com/dynamodb/home?region=us-west-2#tableselected=Saleable

Services Resource Groups

Create table

Tables

Reserved capacity

DAX

Dashboard Clusters Subnet groups Parameter groups Events

Filter by table name

Name Saleable

Saleable Close

Overview Items Metrics Alarms Capacity Indexes More

Table is being created

Recent alerts

No CloudWatch alarms have been triggered for this table.

Stream details

Stream enabled: No
View type: -
Latest stream ARN: -

Manage Stream

Table details

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

Verification

Salestable is created

The screenshot shows the AWS DynamoDB console interface. On the left, the navigation pane lists services like DynamoDB, DAX, and Events. Under the 'Tables' section, a search bar is present, and the table 'Salestable' is selected, indicated by a blue dot. The main content area is titled 'Salestable' and contains tabs for Overview, Items, Metrics, Alarms, Capacity, and Indexes. The 'Overview' tab is selected. It displays information such as 'Recent alerts' (none), 'Stream details' (Stream enabled: No, View type: -, Latest stream ARN: -), and 'Table details' (Table name: Salestable). At the bottom, there are links for Feedback, English, and footer text: © 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

Select Capacity

Under “**Provisioned capacity**”

Provide the following values

Read Capacity → 2

Write Capacity units → 2

Click on **Save** button

The screenshot shows the AWS DynamoDB console with the URL <https://us-west-2.console.aws.amazon.com/dynamodb/home?region=us-west-2&tableSelected=Salestable>. The left sidebar is collapsed. The main area shows a table named "Salestable". The "Capacity" tab is selected. Under "Provisioned capacity", the "Table" dropdown is set to "2". Below it, the "Estimated cost" is listed as "\$1.17 / month (Capacity calculator)". At the bottom, there are "Read capacity" and "Write capacity" checkboxes, both of which are checked. A blue "Save" button is at the bottom right, with a cursor pointing directly at it.

Select item

Click on **Create item**

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 contains tabs for 'Overview', 'Items', 'Metrics', 'Alarms', 'Capacity', 'Indexes', 'Triggers', and 'Access control'. The 'Items' tab is selected. Below this, there's a 'Create item' button and an 'Actions' dropdown. A search bar at the top right says 'Scan: [Table] Salestable: itemno ^'. The main content area displays a table with one row, labeled 'itemno'. A tooltip explains what an item is: 'An item consists of one or more attributes. Each attribute consists of a name, a data type, and a value. When you read or write an item, the only attributes that are required are those that make up the primary key.' At the bottom, 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'.

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

Create item

X

Tree ▾ ▾ Item {1}

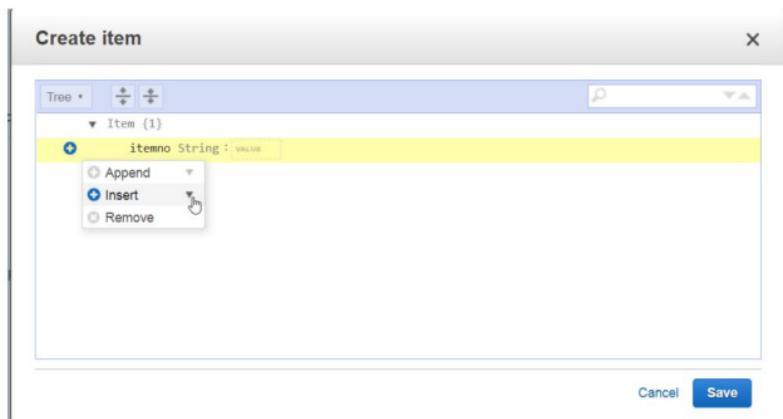
itemno	String : value
--------	----------------

Cancel

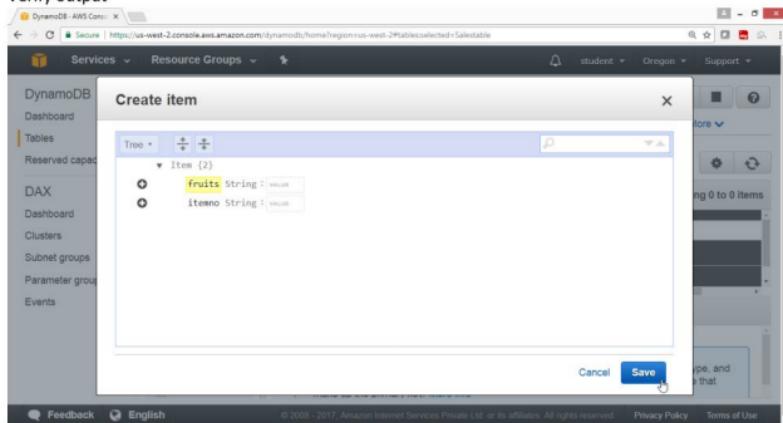
Save

Select insert, select string

ItemName String fruits



Verify output

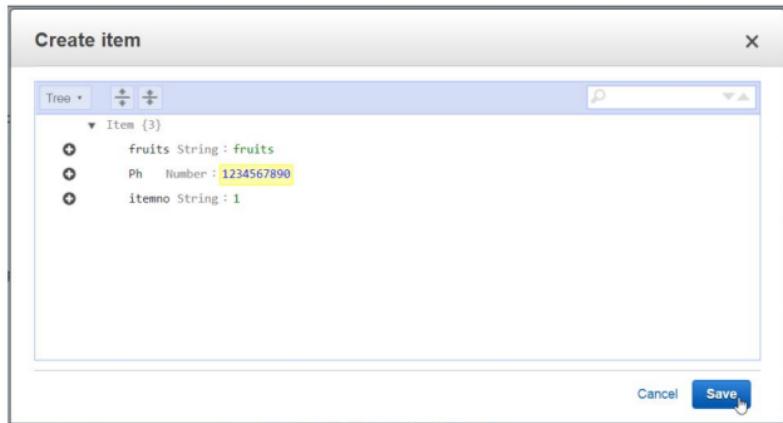


Click on plus radio button

select insert, select number

Ph → 123456789

click on **Save**



To View all entered data

select Scan , click start search

DynamoDB - AWS Console https://us-west-2.console.aws.amazon.com/dynamodb/home?region=us-west-2#tableSelected=Salestable

Services Resource Groups

Salestable Close

Overview Items Metrics Alarms Capacity Indexes Triggers More

Create item Actions

Scan: [Table] Salestable: itemno Viewing 1 to 1 items

Scan Add filter Start search

itemno	Ph	fruits
1	1234567890	fruits

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

To add values in the created fields

Select the Table row, click Action button

select Duplicate

DynamoDB - AWS Console https://us-west-2.console.aws.amazon.com/dynamodb/home?region=us-west-2#tableSelected=Salestable

Services Resource Groups

Salestable Close

Overview Items Metrics Alarms Capacity Indexes Triggers More

Create item Actions

Scan: [Table] Salestable: itemno Viewing 1 to 1 items

Scan Edit Delete Export to .csv Manage TTL

itemno Ph fruits

1 1234567890 fruits

Duplicate

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

Now modify the values of the field

New row will be created

Click on save



Verify

The screenshot shows the AWS DynamoDB console for the 'Saleable' table. On the left, there's a sidebar with 'Services' and 'Resource Groups' tabs, and a main area with 'Create table' and 'Tables' sections. The main area has tabs for 'Overview', 'Items', 'Metrics', 'Alarms', 'Capacity', 'Indexes', 'Triggers', and 'More'. The 'Items' tab is selected. It shows a 'Scan' operation with the query '[Table] Saleable: itemno'. There are two items listed: one with itemno 2 and Ph 1234567890, and another with itemno 1 and Ph 1234567890. Both items also have the value 'Mango' for the 'fruits' attribute.

To Delete the table permanently for DymonaDb

From the AWS console

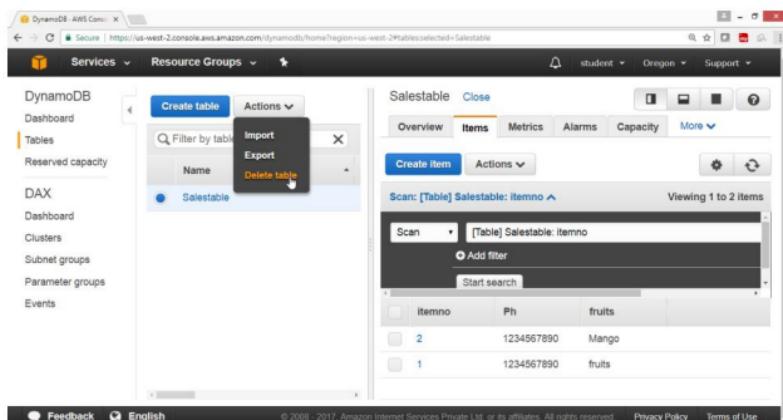
Select services **Database**

Choose **DynamoDB**

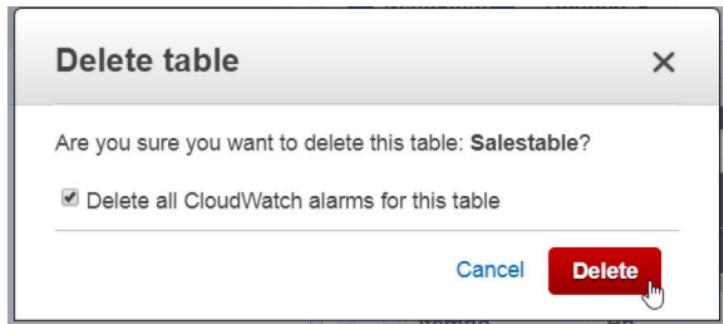
Under **Tables**, select the table for the list

click on Action button

Select "**Delete Table**"



Click on **Delete** button



Verify Table is deleted.

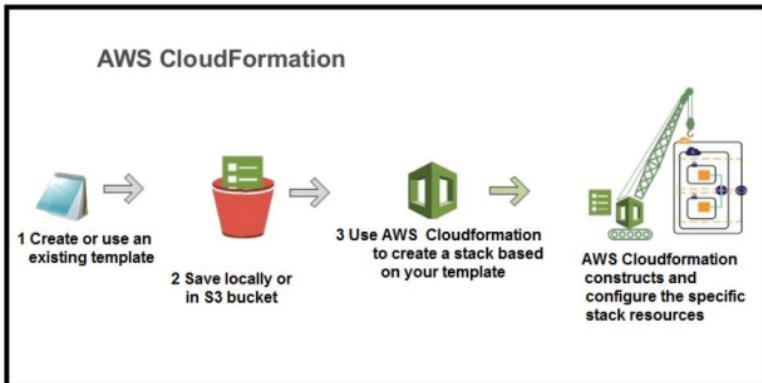
The screenshot shows the AWS DynamoDB service dashboard. On the left, there's a sidebar with "Tables" selected. The main area shows a table named "Salestable" with a small "X" icon next to it, indicating it has been deleted. A tooltip for the "Salestable" table provides information about DynamoDB. At the bottom, there are 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 interface. At the top, there's a navigation bar with tabs for Services, Resource Groups, and other account details. Below the navigation is a search bar and a 'Create a Group' button. The main content area is titled 'Amazon Web Services' and contains several sections:

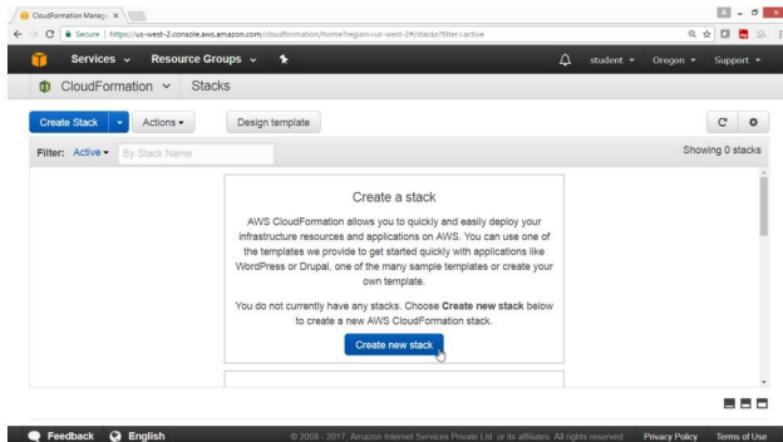
- Compute**: Includes EC2, EC2 Container Service, Lightsail, Elastic Beanstalk, Lambda, and Batch.
- Developer Tools**: Includes CodeStar, CodeCommit, CodeBuild, CodeDeploy, CodePipeline, and X-Ray.
- Internet of Things**: Includes AWS IoT and AWS Greengrass.
- Contact Center**: Includes Amazon Connect.
- Game Development**: Includes Amazon GameLift.
- Storage**: Includes S3, EFS, Glacier, and Storage Gateway.
- Management Tools**: Includes CloudWatch, CloudFormation, CloudTrail, Config, and AWS CloudTrail Metrics.
- Mobile Services**: Includes Mobile Hub, Cognito, Device Farm, and Mobile Analytics.
- Additional Resources**: Includes Getting Started, AWS Console Mobile App, AWS Marketplace, and AWS Launch Announcements.
- Resource Groups**: A section describing what resource groups are and how to create them, with 'Create a Group' and 'Tag Editor' buttons.

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

2) To create a new stack

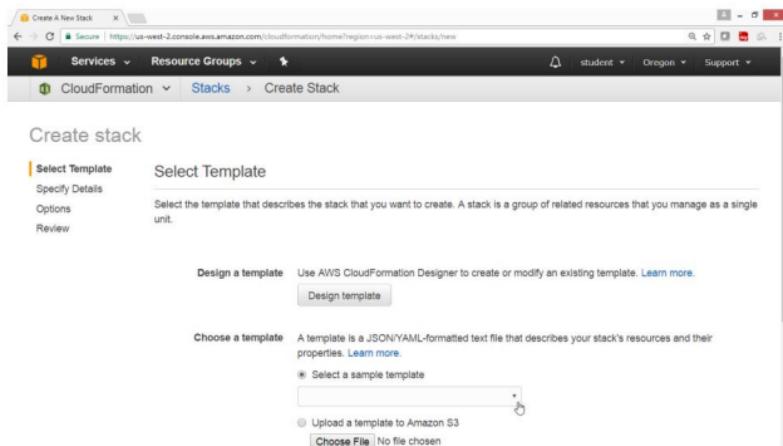
On “Create Stack”, page

Click on “Create New Stack” button



Under “Choose a template”

Select “Select a sample template”

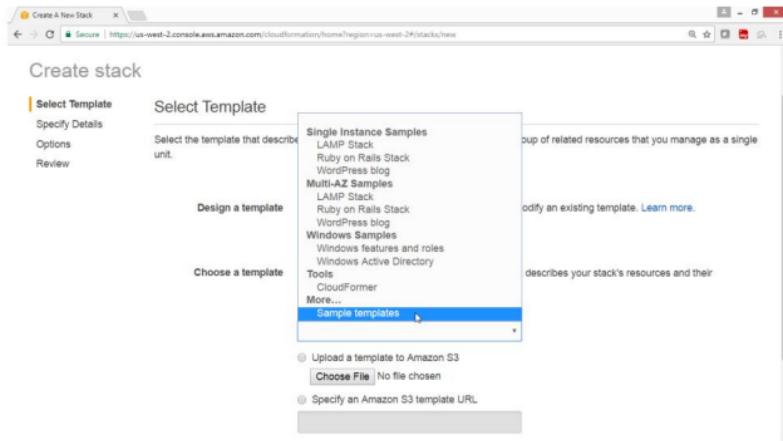


On **Create stack** page

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 Tr", "Menu", "Amazon Web Services logo", "Products", "Solutions", "More", "English", "My Account", and "Sign In to the Console". The main title is "AWS CloudFormation Templates". Below the title, a paragraph explains what CloudFormation is and how it can be used. It then states: "This collection of sample templates will help you get started with AWS CloudFormation and quickly build your own templates." There are two main sections: "Templates & Snippets by AWS Service" and "Reference Implementations". The "Templates & Snippets by AWS Service" section contains links to "Browse sample templates by AWS service." and "Browse template snippets by AWS service.". It also includes a link to "Refer to our developer documentation for more examples and references.". The "Reference Implementations" section contains a link to "AWS Quick Start offers AWS CloudFormation templates and detailed deployment guides for popular IT workloads such as Microsoft Windows Server and SAP HANA.". Below these sections, there's a "Application Frameworks" section with a link to "Application framework templates demonstrate how to use AWS CloudFormation to provision popular frameworks such as LAMP and Ruby on Rails.". At the bottom, there's a "Sample Solutions" section with a link to "Sample solution templates show how to create an end-to-end solution with common applications. AWS does not support or maintain the applications in these examples. These examples are code for demonstrating the capabilities of AWS CloudFormation." The URL in the browser is <https://aws.amazon.com/cloudformation/templates/>.

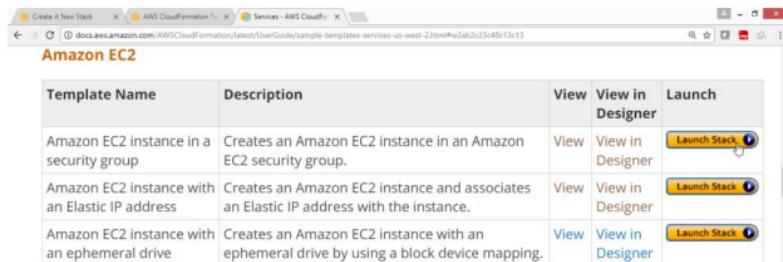
Under Topics

Select Amazon EC2

The screenshot shows the AWS CloudFormation User Guide for Amazon EC2. At the top, there's a navigation bar with links for "Create A New Stack", "AWS CloudFormation Tr", "Services - AWS CloudFormation", "Menu", "Amazon Web Services logo", "English", and "Sign In to the Console". The main title is "AWS CloudFormation". Below it, a sub-section title is "User Guide (API Version 2010-05-15)". On the left, there's a sidebar with a search bar and a list of topics: "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 starts with a heading "Topics" and a bulleted list of services: "Auto Scaling", "AWS Config", "Amazon DynamoDB", "Amazon EC2", "Amazon ElastiCache", "AWS Elastic Beanstalk", "Elastic Load Balancing", "AWS Identity and Access Management", "AWS OpsWorks", "Amazon Relational Database Service", "Amazon Redshift", "Amazon Route 53", "Amazon Simple Storage Service", and "Amazon Simple Queue Service". At the bottom of the page, there are links for "Terms of Use | © 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.", "Did this page help you?", "Yes", "No", and "Feedback". The URL in the browser is <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/sample-templates-services-us-west-2.html>.

Select “Amazon EC2 instance in a security group”,

Click on “Launch stack”



The screenshot shows the AWS CloudFormation console with the URL <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/sample-templates-services-us-west-2.html#web-234b13e13>. The page displays three sample templates under the 'Amazon EC2' section:

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

Below the table, there is a section titled 'Amazon ElastiCache' with a single template entry:

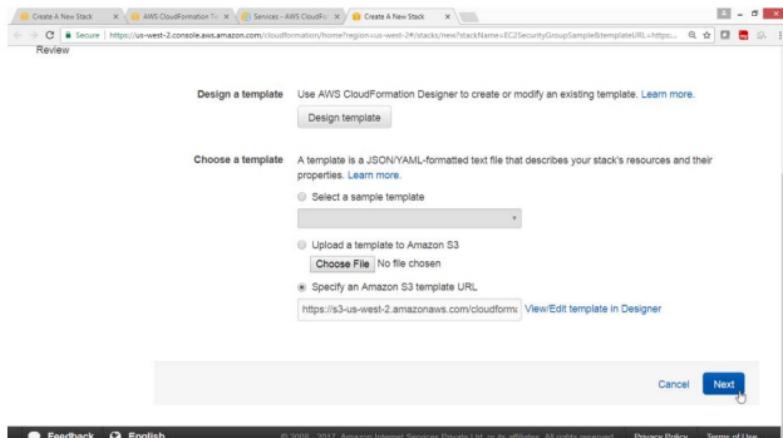
Template Name	Description	View	View in Designer	Launch
ElastiCache	Creates an ElastiCache cache cluster with the Memcached.	View	View in Designer	Launch Stack

At the bottom of the page, there are links for 'Terms of Use', 'Feedback', and a 'Did this page help you?' poll with options 'Yes' and 'No'.

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 the 'Create A New Stack' wizard. The browser URL is <https://us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/new?stackName=EC2SecurityGroupSample&templateURL=https://s3.amazonaws.com/zoomgroup-public/CloudFormation/EC2SecurityGroupSample.yaml>.

Specify Details (highlighted)

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](#).

Stack name: EC2SecurityGroupSample

Parameters

InstanceType	i2.small	WebServer EC2 instance type
KeyName	25July2017masorg	Name of an existing EC2 KeyPair to enable SSH access to the instance
SSHLocation	0.0.0.0/0	The IP address range that can be used to SSH to the EC2 instances

Buttons at the bottom: Cancel, Previous, **Next Step** (highlighted).

Under Options Tag, provide values for

Key → Nameweb

Value → Web

Drag Down

The screenshot shows the 'Create stack' wizard in the AWS CloudFormation console. The current step is 'Options'. On the left, there are tabs: 'Select Template', 'Specify Details', 'Options' (which is selected), and 'Review'. The main area is titled 'Tags' with the sub-instruction: '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.' Below this, there is a table for adding tags:

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

At the bottom of the 'Tags' section is a blue '+' button. Below the tags section is another section titled 'Permissions' with the instruction: '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.' It includes a dropdown for 'IAM Role' (set to 'Choose a role (optional)') and a text input field for '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

Select Template
Specify Details
Options
Review

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

Instance Type t2.small
Key Name 25July2017masorg
SSH Location 0.0.0.0

Click Create button

The screenshot shows the 'Create A New Stack' wizard in the AWS CloudFormation console. The stack configuration includes:

- Stack name:** EC2SecurityGroupSample
- InstanceType:** t2.small
- KeyName:** 25July2017masorg
- SSHLLocation:** 0.0.0.0

Below the configuration, there are tabs for **Options**, **Tags**, and **Advanced**. Under Advanced, the following settings are shown:

- Notification:** none
- Timeout:** none
- Rollback on failure:** Yes

At the bottom right of the wizard, there are 'Cancel', 'Previous', and 'Create' buttons. The 'Create' button is highlighted.

Check the status

Cloudformation is in progress state.

The screenshot shows the AWS CloudFormation Manager interface. The top navigation bar includes 'Services', 'Resource Groups', 'CloudFormation', and 'Stacks'. The main area displays a message about StackSets, followed by a table of stacks.

Filter: Active | By Stack Name

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

Verify

Status is Create_Complete

The screenshot shows the AWS CloudFormation Manager interface. At the top, there's a header bar with tabs for 'CloudFormation Manager' and 'AWS Lambda'. Below the header, a message says '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.' There are three buttons: 'Create Stack', 'Actions', and 'Design template'. A filter dropdown is set to 'Active' and a search bar is empty. The main area shows a table with one row:

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

At the bottom, there are links for 'Feedback', 'English', and legal notices: '© 2008 - 2017, Amazon Internet Services Private LLC or its affiliates. All rights reserved.', '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 navigation links for EC2 Dashboard, Events, Tags, Report Requests, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, and Elastic Block Store Volumes, Snapshots. The main content area has tabs for Launch Instance, Connect, and Actions. A search bar at the top says "Filter by tags and attributes or search by keyword". Below it is a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. Two instances are listed:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
web0	i-0668c160a0f3da41	t2.small	us-west-2c	running	2/2 checks ...	None
web1	i-081a44151fc0525	t2.micro	us-west-2a	stopped	0/0 checks ...	OK

Below the table, there's a detailed view for the first instance (web0). It shows the Public DNS (ec2-34-212-227-98.us-west-2.compute.amazonaws.com), Instance ID (i-0668c160a0f3da41), 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 tabs for Services, Resource Groups, CloudFormation, and Stacks. Below the navigation bar, a modal window titled "Introducing StackSets" provides information about StackSets. The main content area displays a table of stacks. The table has columns for Stack Name, Created Time, Status, and Description. One row is visible, showing "EC2SecurityGroupSample" as the Stack Name, "2017-07-27 19:10:47 UTC+0550" as the Created Time, "CREATE_COMPLETE" as the Status, and "AWS CloudFormation Sample Template EC2Instan" as the Description. The table includes filters for Active and By Stack Name, and actions like Create Stack, Actions, and Design template. 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, it shows the 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 header bar with tabs like 'Create Stack', 'Actions', and 'Design template'. Below this is a search/filter bar with 'Filter: Active' and a dropdown for 'Stack Name'. A table lists one stack: 'EC2SecurityGroupSample' with Status 'CREATE_COMPLETE' and Description 'AWS CloudFormation Sample Template EC2Instan...'. An 'Actions' dropdown menu is open over the stack row, with 'Delete Stack' highlighted. Other options in the dropdown include 'Create Change Set For Current Stack', 'Update Stack', and 'View/Edit template in Designer'. Below the table is a navigation bar with tabs like 'Overview', 'Outputs', 'Resources', etc.

Click on "Yes, Delete"

This screenshot shows the same AWS CloudFormation Manager interface as above, but with a modal dialog box in the foreground titled 'Delete Stack'. The dialog contains the message: 'Are you sure you want to delete this stack? EC2SecurityGroupSample'. It also states 'Deleting a stack deletes all stack resources.' At the bottom of the dialog are two buttons: 'Cancel' and 'Yes, Delete'. The 'Yes, Delete' button is highlighted with a red border. The background of the manager interface is dimmed.

Verify

Deletion is in progress

The screenshot shows the AWS CloudFormation Management Console. At the top, there's a banner titled "Introducing StackSets" with a subtext explaining what AWS StackSets are. Below this, a table lists a single stack named "EC2SecurityGroupSample". The status of this stack is "DELETE_IN_PROGRESS". The table has columns for Stack Name, Created Time, Status, and Description. The "Status" column for the stack shows the current state. At the bottom of the table, there are tabs for Overview, Outputs, Resources, Events, Template, Parameters, Tags, Stack Policy, and Change Sets. The "Overview" tab is selected.

Verification

After deletion again starting screen of CloudFormation is displayed

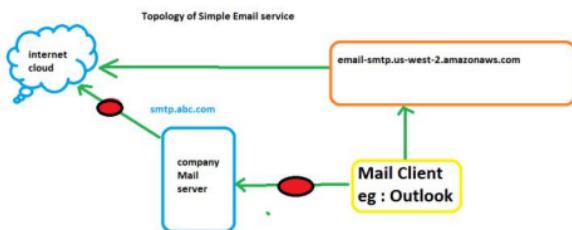
The screenshot shows the AWS CloudFormation Management Console. The interface is identical to the previous one, but the table below the banner is now empty, indicating "Showing 0 stacks". A large callout box titled "Create a stack" provides instructions for creating a new stack. It states that AWS CloudFormation allows users to quickly deploy infrastructure resources and applications. It offers to use sample templates like WordPress or Drupal or to create their own. It also mentions that no stacks are currently present and provides a "Create new stack" button. At the bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use.

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

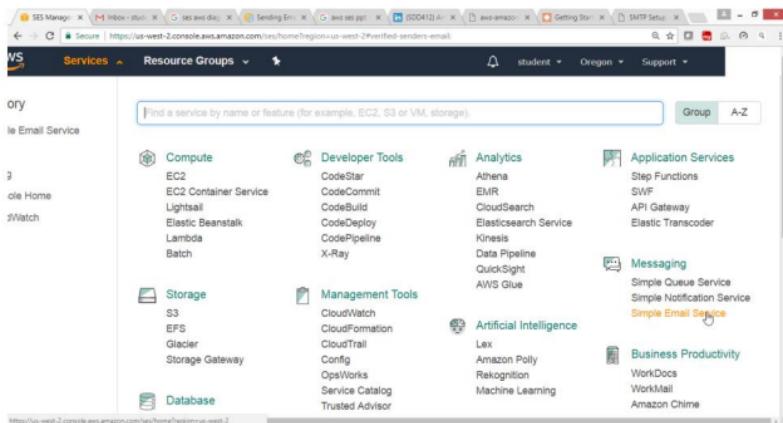
To Configure SES with following task:

- 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

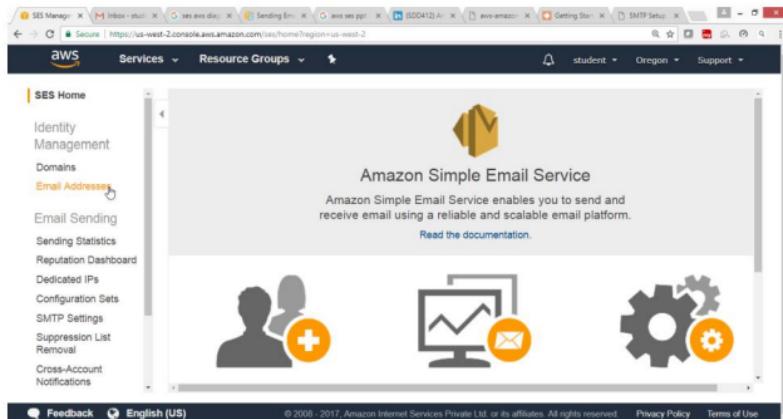
1. Create SES account

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



From SES Home,panel

select "Email Addresses"



SES Home

Identity Management

Domains

Email Addresses

Email Sending

Sending Statistics

Reputation Dashboard

Dedicated IPs

Configuration Sets

SMTP Settings

Suppression List Removal

Cross-Account Notifications

Amazon Simple Email Service

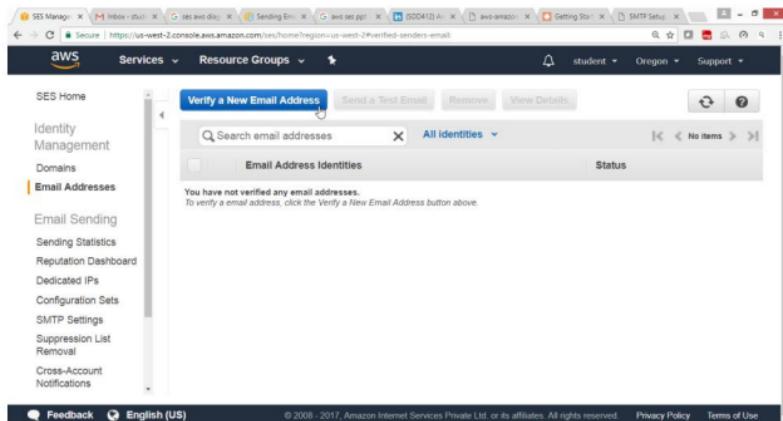
Amazon Simple Email Service enables you to send and receive email using a reliable and scalable email platform.

Read the documentation.

Feedback English (US)

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

Select "Verify a New Email Address" button



SES Home

Identity Management

Domains

Email Addresses

Email Sending

Sending Statistics

Reputation Dashboard

Dedicated IPs

Configuration Sets

SMTP Settings

Suppression List Removal

Cross-Account Notifications

Verify a New Email Address

Send a Test Email Remove View Details

Search email addresses All identities

Email Address Identities Status

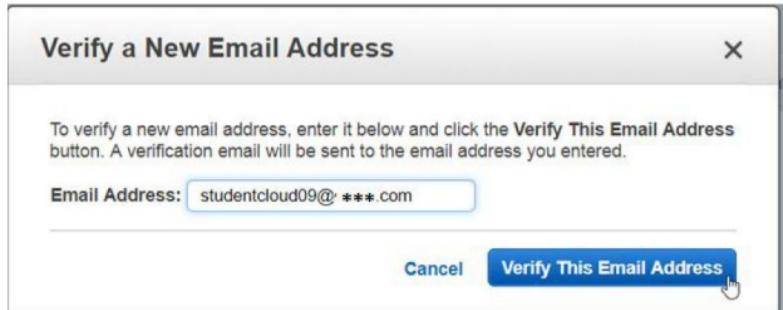
You have not verified any email addresses.
To verify a email address, click the Verify a New Email Address button above.

Feedback English (US)

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

The screenshot shows the AWS SES Management Console. The left sidebar has links for SES Home, Identity Management, Domains, Email Addresses (which is selected and highlighted in orange), Email Sending, Sending Statistics, Reputation Dashboard, Dedicated IPs, and Configuration Sets. The main content area has a header "Verify a New Email Address" with buttons for "Send a Test Email", "Remove", and "View Details". Below this is a search bar and a dropdown menu set to "All identities". A table lists email addresses with their status. One row is shown in detail: "studentcloud09@*****.com" with a status of "verified".

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

SES Management Console

Services Resource Groups

student Oregon Support

SES Home

Identity Management

Domains

Email Addresses

Email Sending

Sending Statistics

Reputation Dashboard

Dedicated IPs

Configuration Sets

SMTP Settings

Suppression List Removal

Cross-Account Notifications

Using SMTP to Send Email with Amazon SES

You can send email through Amazon SES by using a variety of SMTP-enabled programming languages and software. To learn more about the Amazon SES SMTP interface, [click here](#).

To send email using SMTP, you will need to know the following:

Server Name: `email-smtp.us-west-2.amazonaws.com`

Port: 25, 465 or 587

Use Transport Layer Security (TLS): Yes

Authentication: Your SMTP credentials - see below.

To send email through Amazon SES using SMTP, you must create SMTP credentials. SMTP credentials are a username and password that you use when you connect to the Amazon SES SMTP endpoint. You can use the same set of SMTP credentials for all regions in which Amazon SES is available.

To obtain your SMTP credentials, click the button below. For more information about SMTP credentials, [click here](#).

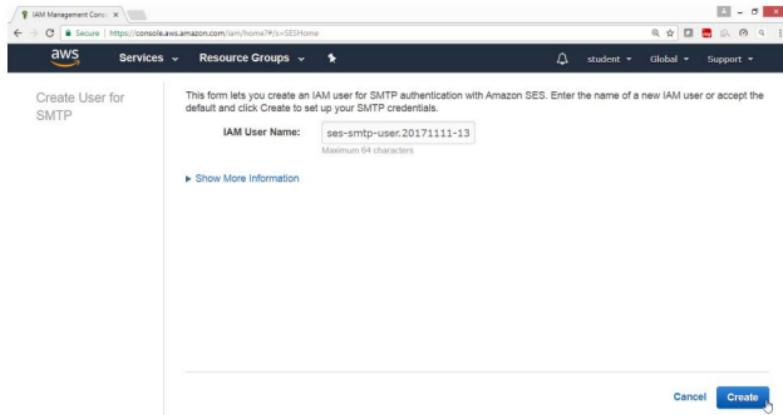
Create My SMTP Credentials

Note: Your SMTP user name and password are not the same as your AWS access key ID and secret access key. Do not attempt to use your AWS credentials to authenticate yourself against the SMTP endpoint. For more information about credential types, [click here](#).

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

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.

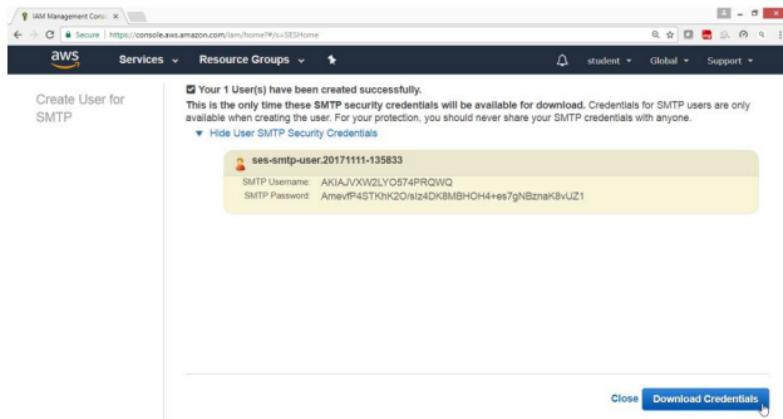
IAM User Name: ses-smtp-user.20171111-13
Maximum 64 characters

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: AKIAJVXWZLY0574PRQWQ
SMTP Password: AmevfP45TKhK2GisIz4DK8MBHOH4+es7gNBzaK8vUZJ

Close Download Credentials

Verify credentials

The screenshot shows the AWS IAM Management Console. A message box displays: "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 highlights the "Hide User SMTP Security Credentials" link and the generated SMTP credentials: Username: AKIAJUV...2WQ, Password: AmeyvP4...es/gNBznaKBvUZ1.

Open Outlook

The screenshot shows the Microsoft Outlook 2016 interface. The ribbon tabs include FILE, HOME, SEND / RECEIVE, FOLDER, and VIEW. The main area displays the "Outlook Today - Outlook" calendar view for Saturday, November 11, 2017. On the right side, there are three panes: "Tasks" (empty), "Messages" (with sections for Inbox, Drafts, and Outbox), and "Categorize Outlook Today".

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

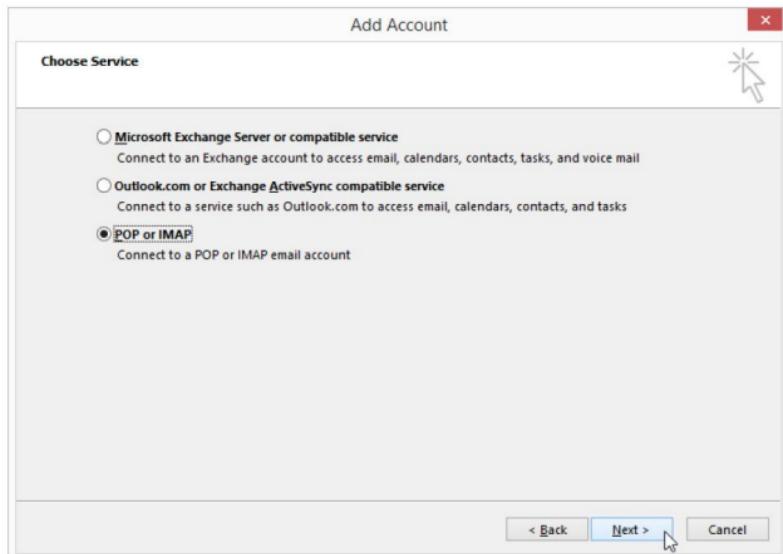
Password:

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

Mail to keep offline: All (progress bar)

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

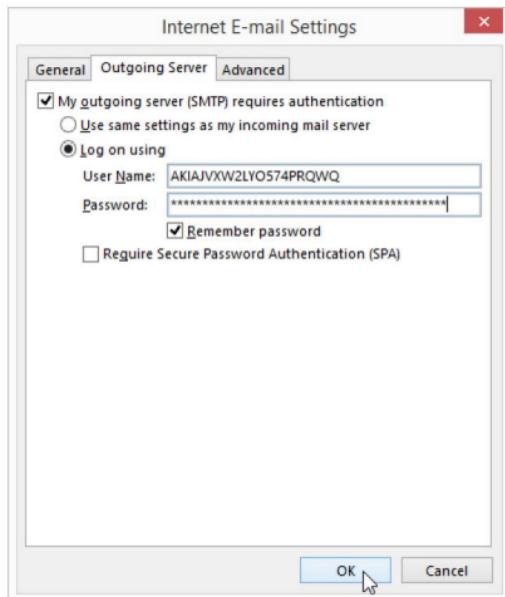
Password: *****

Remember password

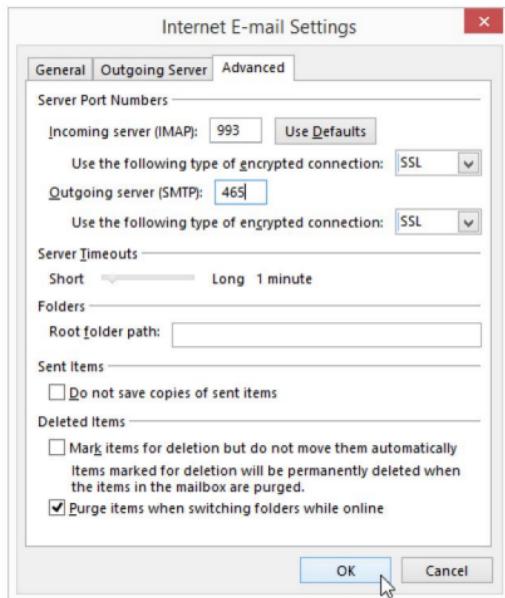
Require logon using Secure Password Authentication (SPA) [More Settings ...](#)

< Back Next > Cancel

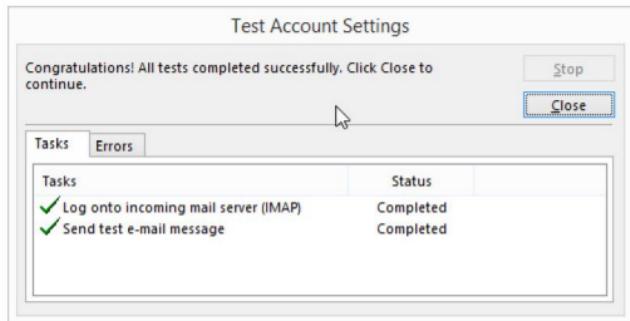
Provide following details in Outgoing Server



Provide following details in Advance



Verify successfully connected

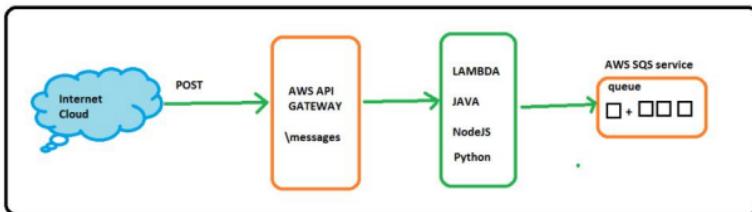


Lab 19: To Configure Amazon Simple QUEUE Service SQS

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

The screenshot shows the AWS Management Console Services page. The navigation bar at the top includes the AWS logo, a search bar, and links for student, Oregon, Support, Group, and A-Z. The main content area is titled "Find a service by name or feature (for example, EC2, S3 or VM, storage)." Below this is a grid of service icons and names. The "Messaging" section is highlighted with a yellow box, and "Simple Queue Service" is specifically pointed to with a red arrow. Other services listed in the Messaging section include Simple Notification Service and Simple Email Service.

Click on **Get started on**

The screenshot shows the AWS Simple Queue Service (SQS) landing page. The navigation bar at the top is identical to the previous screenshot. The main content features a large yellow 3D cube icon. Below it, the text "Simple Queue Service" is displayed in bold. A blue "Get Started Now" button is centered below the text. At the bottom of the page, there is a link "Learn more about AWS SQS".



Feedback English (US)



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



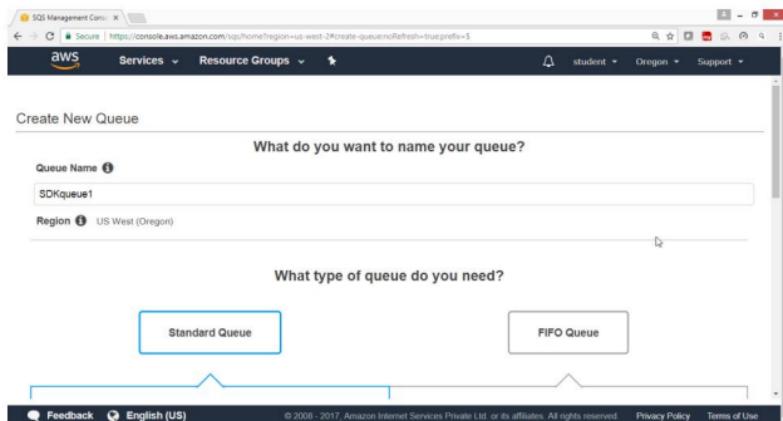
Privacy Policy Terms of Use

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 with the URL <https://console.aws.amazon.com/sqs/home?region=us-west-2&create-queue=refresh=true&profile=5>. The page is titled "Quick-Create Queue". It has two main sections:

- Send data between applications when the throughput is important, for example:**
 - Decouple live user requests from intensive background work: let users upload media while resizing or encoding it.
 - Allocate tasks to multiple worker nodes: process a high number of credit card validation requests.
 - Batch messages for future processing: schedule multiple entries to be added to a database.
- Send data between applications when the order of events is important, for example:**
 - Ensure that user-entered commands are executed in the right order.
 - Display the correct product price by sending price modifications in the right order.
 - Prevent a student from enrolling in a course before registering for an account.

At the bottom, there is a note: "For more information, see the [Amazon SQS FAQs](#) and the [Amazon SQS Developer Guide](#)". Below that, a note says: "To create a new queue, choose Quick-Create Queue. To configure your queue's parameters, choose Configure Queue." There are three buttons at the bottom: "Cancel", "Configure Queue", and "Quick-Create Queue" (which is highlighted).

Verify Queue is Created

The screenshot shows the AWS SQS Management Console with the URL <https://console.aws.amazon.com/sqs/home?region=us-west-2&queue-browserselected=https://sqs.us-west-2.amazonaws.com/523251683217/SDKqueue1>. The page title is "SQS Queue selected".

Create New Queue **Queue Actions**

Filter by Prefix: Enter Text...

Name	Queue Type	Content-Based Deduplication	Messages Available	Messages in Flight	Created
SDKqueue1	Standard	N/A	0	0	2017-11-12 18:42:48 GMT+05:30

1 SQS Queue selected

Details **Permissions** **Redrive Policy** **Monitoring** **Tags** **Encryption**

SDKqueue1

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

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
Messages in Flight (Last 1000): 0

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

Select the Queue

Drop down “Queue Action” button

select “Send message”

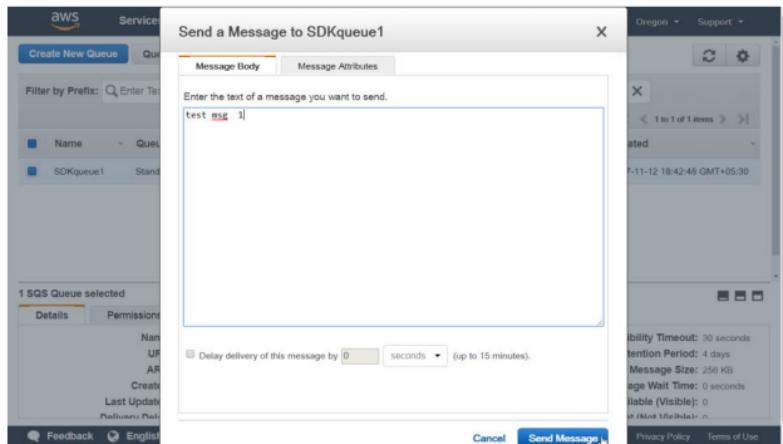
The screenshot shows the AWS SQS Management Console interface. At the top, there's a navigation bar with the AWS logo, Services, Resource Groups, and Support. Below the navigation is a search bar and a filter section labeled "Filter by Prefix: Q". A dropdown menu titled "Queue Actions" is open, showing options: "Send a Message" (which is highlighted with a mouse cursor), "View/Delete Messages", "Configure Queue", "Add a Permission", "Purge Queue", "Delete Queue", and "Subscribe Queue to SNS Topic". The main content area displays a table for the selected queue, "SDKqueue1". The table has columns: Name, URL, ARN, Created, and Last Updated. The "Created" column shows the timestamp "2017-11-12 18:42:48 GMT+05:30". To the right of the table, there are details about the queue: 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). At the bottom of the page, 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

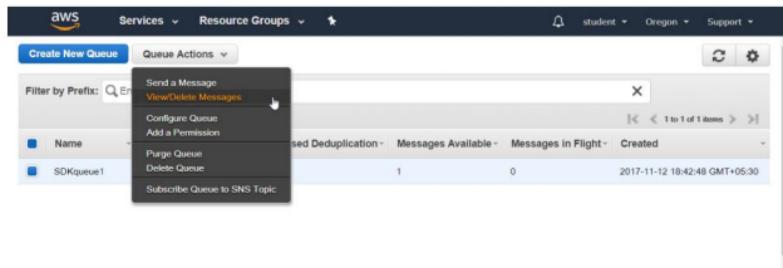


2) To View the message

Select the Queue

Drop down **Queue Action** button

Select the option “View/Delete Message”



The screenshot shows the AWS Management Console interface for an SQS queue named "SDKqueue1". A context menu is open over the queue name, with the "Queue Actions" option selected. The submenu includes "Send a Message", "View/Delete Messages" (which is highlighted with a cursor), "Configure Queue", "Add a Permission", "Purge Queue", "Delete Queue", and "Subscribe Queue to SNS Topic". Below the menu, the queue details are displayed: 1 message available, 0 messages in flight, and a creation date of 2017-11-12 18:42:48 GMT+05:30.

1 SQS Queue selected

Details Permissions Redrive Policy Monitoring Tags Encryption

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

Default Visibility Timeout: 30 seconds
Message Retention Period: 4 days
Maximum Message Size: 256 KB
Receive Message Wait Time: 0 seconds
Messages Available (Visible): 1
Messages In Flight (Not Available)

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"

View/Delete Messages in SDKqueue1

View up to: 10 messages Poll queue for: 30 seconds

Polling for new messages once every 2 seconds.

Delete	Body	Size	Sent	Receive Count

0%

This progress bar indicates whether messages displayed above are available to applications.

Close **Delete Messages**

Verify message is in the queue

View/Delete Messages in SDKqueue1

View up to: 10 messages Poll queue for: 30 seconds

Polling for new messages once every 2 seconds.

Delete	Body	Size	Sent	Receive Count
<input type="checkbox"/>	test msg 1	11 bytes	2017-11-12 18:47:54 GMT+05:30	2

34%

Polling the queue at 0.6 receives/second. Stopping in 19.6 seconds. Messages shown above are currently hidden from other consumers.

Close **Delete Messages**

3) To delete the message

Select the Queue

Drop Down Queue Action

Select "Delete Message"

The screenshot shows the AWS SQS Management Console. In the center, there is a table titled "SQS Queue selected" with one item listed: "SDKqueue1". The "Actions" column for this queue contains a dropdown menu. The menu is open, showing several options: "Send a Message", "View/Delete Messages", "Configure Queue", "Add a Permission", "Purge Queue", and "Delete Queue". The "Delete Queue" option is highlighted with a red box. At the bottom of the dropdown menu, there is a small "Subscribe Queue to SNS Topic:" link.

1 SQS Queue selected

Actions	SDKqueue1
Send a Message View/Delete Messages Configure Queue Add a Permission Purge Queue Delete Queue Subscribe Queue to SNS Topic:	1 0 2017-11-12 18:42:48 GMT+05:30

Details Permissions Redrive Policy Monitoring Tags Encryption

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

Default Visibility Timeout: 30 seconds Message Retention Period: 4 days Maximum Message Size: 256 KB Receive Message Wait Time: 0 seconds Messages Available (Visible): 1 Messages in Flight (Not Visible): 0

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

Confirm

The screenshot shows a modal dialog box titled "Delete Queues". The text inside the dialog asks if the user is sure they want to delete the following queue, and any messages left in it. A red bullet point lists "SDKqueue1 - contains 1 message.". At the bottom right of the dialog, there are two buttons: "Cancel" and "Yes, Delete Queue". The "Yes, Delete Queue" button is highlighted with a red box and has a small circular arrow icon next to it. At the very bottom of the dialog, there is a note: "WARNING: This action cannot be undone." and "Default Visibility Timeout".

Are you sure you want to delete the following queue, and any messages left in it?

- SDKqueue1 - contains 1 message.

Cancel Yes, Delete Queue

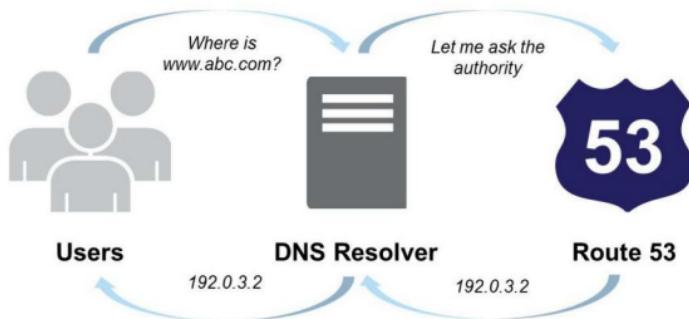
WARNING: This action cannot be undone. Default Visibility Timeout

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 provides 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

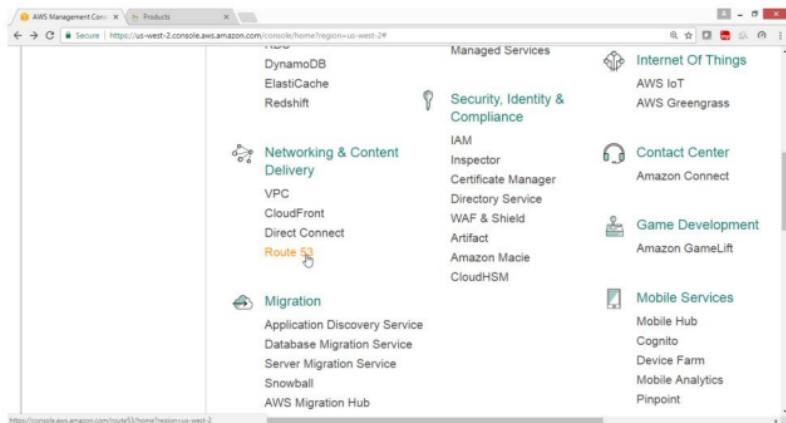
Creating CNAME record set

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

The screenshot shows the Amazon Route 53 Management console. At the top, there's a navigation bar with tabs for 'Route 53 Management' and 'Products'. Below the navigation, there are four main service cards:

- DNS management**: Shows a computer monitor icon with a cloud and two orange circular arrows. A subtext explains it can register new domains and route traffic to AWS and external resources.
- Traffic management**: Shows a network diagram with a central gear and three arrows pointing to different resources. A subtext explains it can route traffic to multiple endpoints for an application.
- Availability monitoring**: Shows a shield with a stethoscope and a green plus sign. A subtext explains it monitors the health and performance of web servers and other resources.
- Domain registration**: Shows a computer monitor icon with '.com' and '.org' suffixes. A subtext explains it can find and register available domain names.

At the bottom of each card is a 'Get started now' button. The footer includes links for 'Feedback', 'English', and legal notices like '© 2006–2017 Amazon Internet Services Inc. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Click on “Created Hosted Zone” button

The screenshot shows the AWS Route 53 Management console. The left sidebar has 'Hosted zones' selected. The main area has a large icon of a computer monitor with a gear. Below it, text explains what Route 53 does: translating human-readable domain names into IP addresses. A 'Create Hosted Zone' button is at the bottom. A cursor arrow points to this button.

Again Click on Create Hosted Zone button

The screenshot shows the same AWS Route 53 Management console interface. The 'Hosted zones' section is still selected. The main area displays the message 'You have no hosted zones'. The 'Create Hosted Zone' button is visible at the top of the list.

Under "Created Hosted Zone", wizard

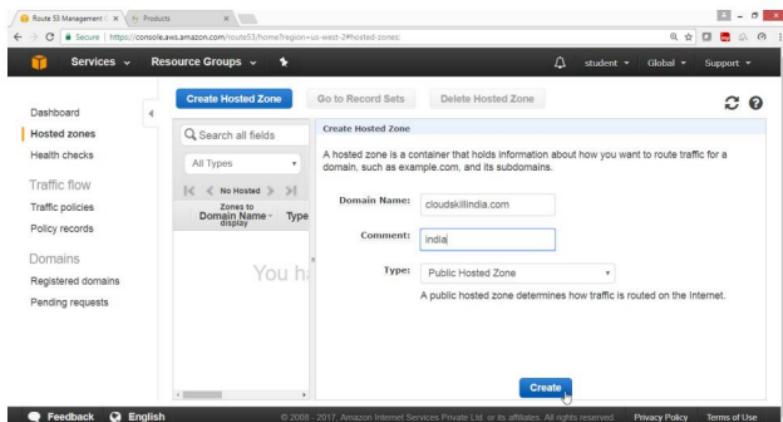
On right side panel provide following values

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 sidebar, under 'Hosted zones', 'cloudskillindia.com' is selected. In the main area, a 'Create Record Set' dialog is open. The 'Record Set Name' is 'cloudskillindia.com.' and the 'Type' is 'NS - Name server'. The 'Value' field contains four entries: 'ns-140.awsdns-17.com.', 'ns-1565.awsdns-03.co.uk.', 'ns-726.awsdns-26.net.', and 'ns-1286.awsdns-32.org.'. The 'TTL (Seconds)' is set to 172800. The 'Save Record Set' button is visible at the bottom right.

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

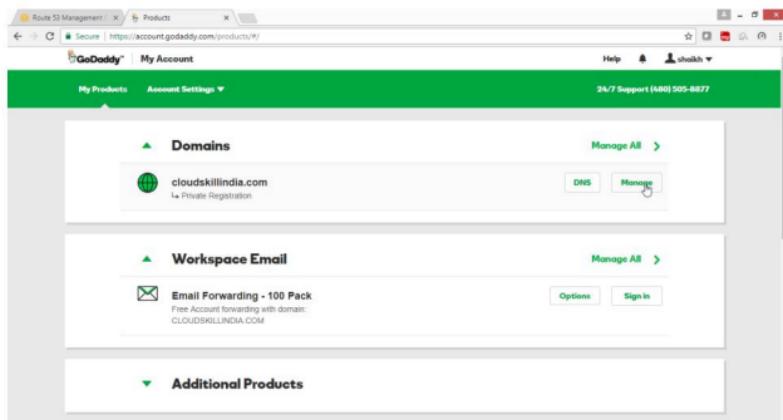
ns-1286.awsdns-32.org

Open the browser

Go to godaddy.com site

Login and select your domain name

Click on **Manage**



Drag Down

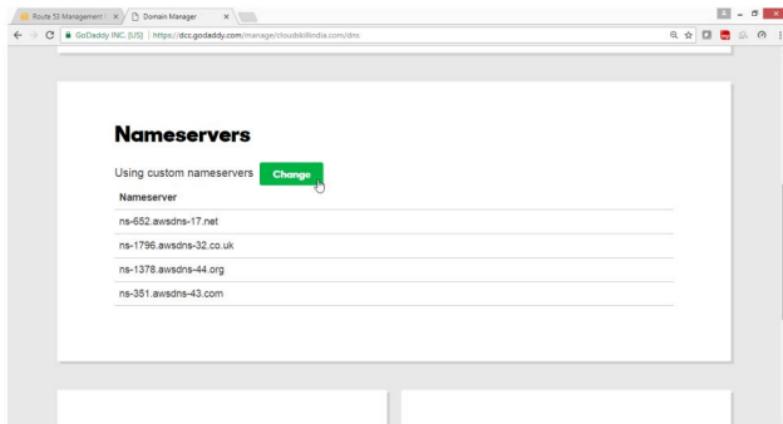
Click on **Manage DNS**

The screenshot shows a web browser window with two tabs open: 'Route 53 Management' and 'Domain Manager'. The 'Domain Manager' tab is active, displaying the 'Additional Settings' page for the domain 'cloudskillINDIA.COM'. The page includes options to automatically renew the domain, transfer it to another GoDaddy account, or delete it. It also features a 'Locking' section and a link to add protected registration. At the bottom, there's a copyright notice and a privacy policy link.

Copyright © 1999 - 2017 GoDaddy Operating Company, LLC. All Rights Reserved. [Privacy Policy](#)

Click on change

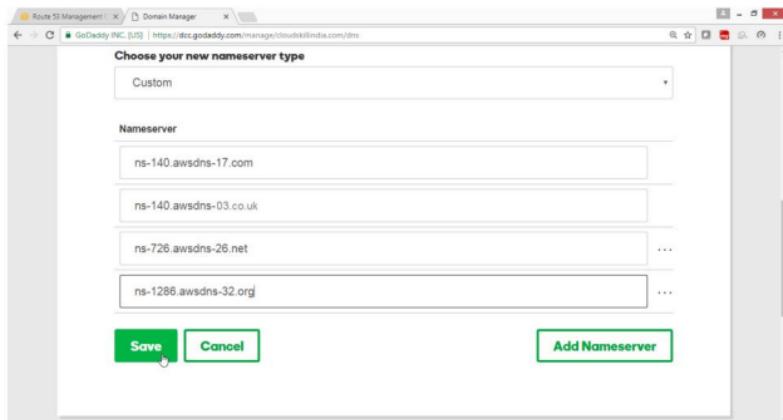
Add latest entries provided by Route53 NS records



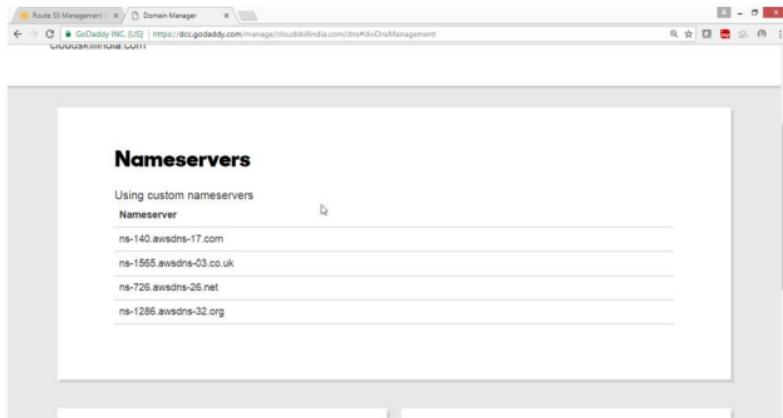
For Choose your new name server → Custom

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

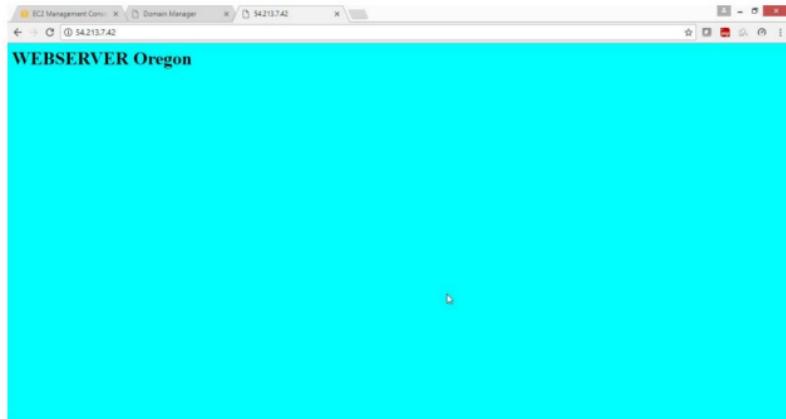
Configure it as a Web Server

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 for Services, Resource Groups, and various EC2 categories like Instances, Images, and Elastic Block Store. The main content area is titled 'Launch Instance' and displays a table of instances. One instance is selected: 'linuxvm1' (Instance ID: i-0986868cc14262f6). The Public DNS is listed as 'ec2-54-213-7-42.us-west-2.compute.amazonaws.com'. Below the table, there are tabs for Description, Status Checks, Monitoring, and Tags. Under the 'Description' tab, detailed information is provided: Instance ID (i-0986868cc14262f6), Public DNS (IPv4) (ec2-54-213-7-42.us-west-2.compute.amazonaws.com), Instance state (running), Instance type (t2.micro), and Elastic IPs. The Public DNS (IPv4) is also listed as 54.213.7.42. At the bottom of the page, there are links for Feedback, English, Copyright notice (© 2006 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

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 Domain Manager interface. On the left sidebar, under 'Hosted zones', the 'cloudskillindia.com' domain is selected. In the main content area, the 'Record Sets' tab is active, showing two entries:

- A record for 'cloudskillindia.com' pointing to IP address 128.111.12.123.
- CNAME record for 'www.cloudskillindia.com' pointing to 'www'.

Click on Create Record set button

The screenshot shows the AWS Route 53 Domain Manager interface. On the left, there's a sidebar with options like Dashboard, Hosted zones (which is selected), Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The main area has tabs for Back to Hosted Zones, Create Record Set (which is highlighted in blue), Import Zone File, and Delete Record Set. A search bar at the top says "Record Set Name" and "Any Type". Below it, there are two radio buttons: "Aliases Only" and "Weighted Only", with "Weighted Only" being selected. A note says "To get started, click Create Record Set button or click an existing record set." There's a table displaying two record sets for the domain "cloudskillindia.com.". The first record set is of type NS, with values ns-140.awsdns-17.com., ns-1565.awsdns-03.co.uk., ns-726.awsdns-26.net., and ns-1266.awsdns-32.org. The second record set is of type SOA, with value ns-140.awsdns-17.com. The table has columns for Name, Type, and Value.

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. On the left, there's a sidebar with options like Services, Resource Groups, Dashboard, Hosted zones, Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The 'Hosted zones' section is currently selected. In the main area, there's a 'Create Record Set' dialog box. The 'Record Set Name' field contains 'org.cloudskillindia.com'. The 'Type' dropdown is set to 'A - IPv4 address'. The 'TTL (Seconds)' dropdown has '300' selected. The 'Value' field contains '54.213.7.42'. Below the value field, there's a note: 'IPv4 address. Enter multiple addresses separated by commas.' and an example: '192.0.2.235, 192.51.100.234'. At the bottom of the dialog, there's a 'Create' button. Above the dialog, there are buttons for 'Back to Hosted Zones', 'Import Zone File', and 'Delete Record Set'. The top of the page shows tabs for 'Route 53 Management', 'Domain Manager', and '54.213.7.42'. The URL in the address bar is 'https://console.aws.amazon.com/route53/home?region=us-west-2#resource-record-sets/Z3BZSDZMNPV'. The bottom of the page includes links for 'Feedback', 'English', '© 2006-2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Verify the A record got created

The screenshot shows the AWS Route 53 Domain Manager interface. In the left sidebar, 'Hosted zones' is selected. On the right, under 'Create Record Set', a new record set named 'org.cloudskillindia.com.' is being created. The type is set to 'A - IPv4 address'. The value is '54.213.7.42'. The TTL is set to 300 seconds. The routing policy is 'Simple'. The 'Save Record Set' button is visible at the bottom.

Create Alias record

The screenshot shows the AWS Route 53 Domain Manager interface. In the left sidebar, 'Hosted zones' is selected. On the right, under 'Create Record Set', a new record set named 'www' for the domain 'cloudskillindia.com.' is being created. The type is set to 'CNAME - Canonical name'. The alias is set to 'Yes' and points to 'org.cloudskillindia.com.'. The TTL is set to 300 seconds. The routing policy is 'Simple'. The 'Create' button is visible at the bottom.

Verify the CNAME record got created

The screenshot shows the AWS Route 53 Domain Manager interface. In the left sidebar, 'Hosted zones' is selected. On the right, under 'Create Record Set', a table lists four record sets. The fourth row, 'www.cloudskillindia.com.', is highlighted with a blue border. It is defined as a CNAME record pointing to 'org.cloudskillindia.com.'.

Name	Type	Value
cloudskillindia.com.	NS	ns-140.awsdns-17.co... ns-1565.awsdns-03.co... ns-726.awsdns-26.net ns-1298.awsdns-32.or...
cloudskillindia.com.	SOA	ns-140.awsdns-17.co...
www.cloudskillindia.com.	A	54.213.7.42
org.cloudskillindia.com.	CNAME	org.cloudskillindia.com

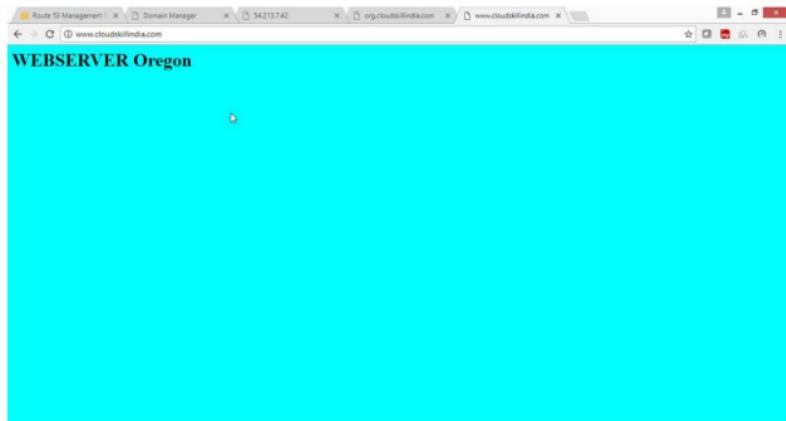
Verification

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

The screenshot shows a web browser window displaying the URL 'org.cloudskillindia.com'. The page content is a solid cyan color with the text 'WEB SERVER Oregon' centered in white.

Verification

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

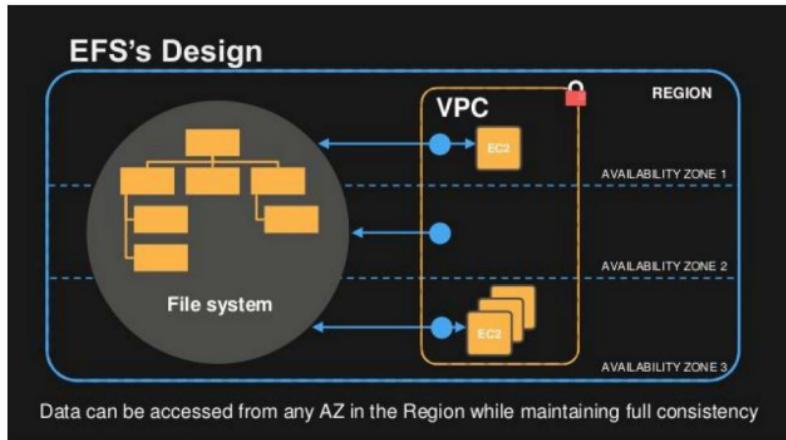


Lab 21: To configure Amazon EFS Service

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**

The screenshot shows the AWS Cloud Services Catalog interface. On the left, there's a sidebar with links to History, EFS, Console Home, S3, Glacier, IAM, and EC2. The main area is titled "Find a service by name or feature (for example, EC2, S3 or VM, storage)." It lists various services under categories: Compute, Developer Tools, Analytics, Application Services, Storage, Management Tools, Artificial Intelligence, Messaging, and Database. The "Compute" category is expanded, showing EC2 Container Service, Lightsail, Elastic Beanstalk, Lambda, and Batch. The "Database" category is also expanded, showing Amazon RDS, Amazon Aurora, Amazon Neptune, and Amazon DynamoDB. The "EC2" link in the sidebar is highlighted in blue, indicating it is the active service.

Under EC2 Dashboard go for Network & Security

Select Security Groups

Click on Create Security Group

Name	Group ID	Group Name	VPC ID	Description
sg-275b205d		launch-wizard-1	vpc-89c341ee	launch-wizard-1
sg-38265c42		launch-wizard-2	vpc-89c341ee	launch-wizard-2
sg-a2344dd8		launch-wizard-3	vpc-89c341ee	launch-wizard-3
sg-a3affec6		default	vpc-89c341ee	default VPC security group

Under “Create Security Group” wizard

Give Following values

Security group name → NFSsecurity2

Description → NFSrule2

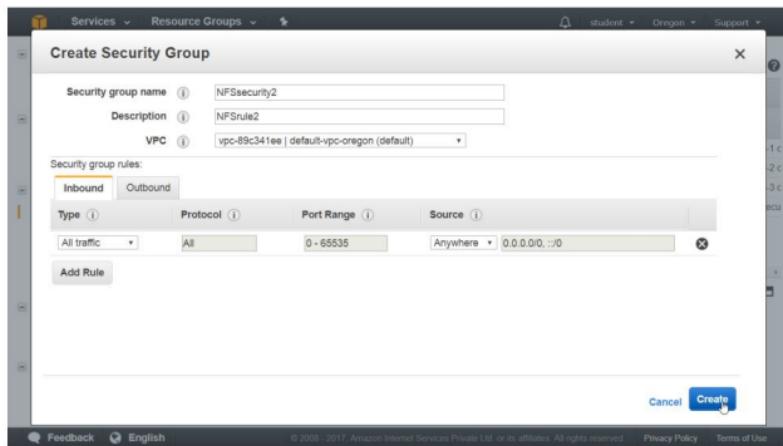
VPC → take default

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 menu open. Under the Storage category, the EFS icon is highlighted. Other services listed include S3, Glacier, IAM, EC2, and various developer tools like CloudWatch, CloudFormation, and CloudTrail.

Click on “Create file system” button

The screenshot shows the Amazon EFS landing page. It features a large red circular icon with a white 'E' and the text "Amazon Elastic File System (EFS)". Below the icon, it says "Amazon EFS provides file storage for use with your EC2 instances." A prominent blue button labeled "Create file system" is centered at the bottom. Below the button, there is a link to "Getting started guide".



Select Default VPC

Step 1: Configure file system access

Step 2: Configure optional settings

Step 3: Review and create

Configure file system access

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.

VPC vpc-89c341ee - default

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-12f60e5a (default)	Automatic	sg-a3a41edb - default
us-west-2b	subnet-8b9e38ec (default)	Automatic	sg-a3a41edb - default
us-west-2c	subnet-19d0f141 (default)	Automatic	sg-a3a41edb - default

Remove all Security Groups

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-12f60e5a (default)	Automatic	sg-a3a41edb - default
us-west-2b	subnet-8b9e38ec (default)	Automatic	sg-a3a41edb - default
us-west-2c	subnet-19d0f141 (default)	Automatic	sg-a3a41edb - default

Verify that all security groups go deleted

VPC vpc-89c341ee - default... ⓘ

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-13f50e5a (default)	Automatic ⓘ	Select Security ⓘ
us-west-2b	subnet-8b9e38ec (default)	Automatic ⓘ	Select Security ⓘ
us-west-2c	subnet-19d0f141 (default)	Automatic ⓘ	[] ⓘ

Cancel Next Step

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

Now add NFSsecurity2 group in all A.Z

VPC vpc-89c341ee - default... ⓘ

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-13f50e5a (default)	Automatic ⓘ	sg-275b205d - launch-wizard-1
us-west-2b	subnet-8b9e38ec (default)	Automatic ⓘ	sg-28652152 - NFSsecurity2
us-west-2c	subnet-19d0f141 (default)	Automatic ⓘ	

Cancel

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

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
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

[Cancel](#)

[Next Step](#)

Provide tags

Key → Name

Value → NFShyd1

Drag Down

Elastic File System Manager Getting Started with An... https://us-west-2.console.aws.amazon.com/ebs/home?region=us-west-2#wizard/2

Step 3: Review and create

Add tags

You can add tags to describe your file system. A tag consists of a case-sensitive key-value pair. (For example, you can define a tag with key-value pair with key = Corporate Department and value = Sales and Marketing.) At a minimum, we recommend a tag with key = Name.

Key	Value	Remove
Name	NFShyd1	<input type="button" value="Remove"/>

Add New Key

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	<input type="text"/> Name: NFShyd1
Performance mode	General Purpose (default)
Encrypted	No

Create File System

Verify

The screenshot shows the AWS EBS File System Manager interface. A success message box is displayed, stating: "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 created file system: Name: NFShydr1, File system ID: fs-53f822fa, Metered size: 6.0 KB, Number of mount targets: 3, Creation date: 2017-08-15T06:16:55Z. Under "Other details", Owner ID is listed as 523251683217 and Life cycle state is Available. There is a "Tags" section with a single tag named "Name: NFShydr1".

Drag Down

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

The screenshot shows the AWS EFS Mount Targets page for the file system fs-53f822fa. It displays three mount targets with their details:

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		Creating
	us-west-2a	subnet-13f60e5a (default)	172.31.40.66	fsmt-87a0072e	eni-e8d884d6		Creating
	us-west-2b	subnet-8b93a8ec (default)	172.31.27.220	fsmt-98a00731	eni-eecc553c1		Creating

Verify that Life cycle state is Available

The screenshot shows the AWS EBS File System Manager interface. At the top, there are tabs for 'Elastic File System Manager' and 'Getting Started with Amazon FSx'. The URL in the address bar is <https://us-west-2.console.aws.amazon.com/fsx/home?region=us-west-2#filesystems/fs-53f622fa>. Below the tabs, there are two sections: 'Amazon EC2 mount instructions' and 'AWS Direct Connect mount instructions'. Under 'Mount targets', there is a table 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-19c0f141 (default)	172.31.7.82	fsmnt-86a0072f	eni-7adcc27a	sg-28652152 - NFSsecurity2	Available
	us-west-2a	subnet-13f60e5a (default)	172.31.40.66	fsmnt-87a0072e	eni-8bd884d6	sg-28652152 - NFSsecurity2	Available
	us-west-2b	subnet-8b9e38ec (default)	172.31.27.220	fsmnt-98a00731	eni-eec553c1	sg-28652152 - NFSsecurity2	Available

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'.

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_masi] > 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

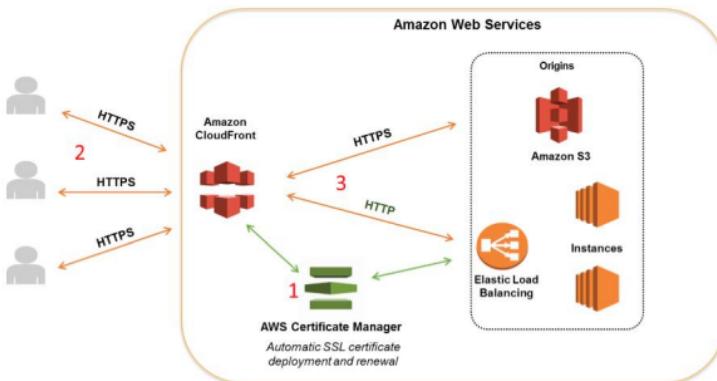
```
proc on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
devtmpfs on /dev type devtmpfs (rw,relatime,size=499756k,nr_inodes=124939,mode=755)
devpts on /dev/pts type devpts (rw,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs /dev/shm type tmpfs (rw,relatime)
/dev/xvda1 on / type ext4 (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 cloudfront 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

The screenshot shows the AWS CloudFront Manager interface. At the top, there's a navigation bar with tabs for 'CloudFront', 'Console Home', 'EC2', 'EFS', 'S3', and 'Glacier'. Below this is a search bar labeled 'Find a service by name or feature (for example, EC2, S3 or VM, storage.)'. The main area is titled 'Services' and contains several categories: 'Compute' (EC2, 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, AWS Glue), 'Storage' (S3, EFS, Glacier), 'Management Tools' (CloudWatch, CloudFormation, CloudTrail), and 'Artificial Intelligence' (Lex). The 'S3' icon is highlighted with a red box.

Check the S3 bucket content

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 other account-related options. Below the navigation is a search bar labeled 'Search by prefix' and a link to 'Switch to new console'. To the right of the search bar are buttons for 'None', 'Properties', and 'Transfers'. The main content area is titled 'Bucket: www.cloudskillhyd.com'. It displays a list of objects within the bucket:

Name	Storage Class	Size
404.html	Standard	6 KB
about-us.html	Standard	5.8 KB
article.html	Standard	5.3 KB
articles.html	Standard	4.8 KB
contact-us.html	Standard	4.7 KB
css	--	--
images	--	--
index.html	Standard	6 KB
js	--	--
sitemap.html	Standard	4.8 KB

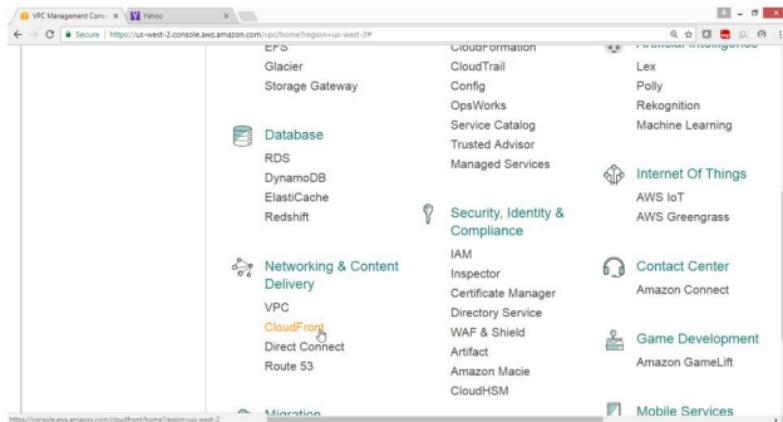
On the right side of the bucket details, there are sections for 'Permissions' and 'Static Website Hosting'. Under 'Static Website Hosting', it says you can host your static website entirely on Amazon S3, and provides the endpoint: www.cloudskillhyd.com.s3-website-us-west-2.amazonaws.com.

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 sidebar, under 'Services', 'CloudFront' is selected. The main area is titled 'CloudFront Distributions'. At the top of this section is a blue 'Create Distribution' button. Below it are tabs for 'Viewing', 'Any Delivery Method', and 'Any State'. A table lists one distribution entry:

Delivery Method	ID	Domain Name	Comment	Origin
Web	E3MBZACTGBE5OL	d2sq5lo2sebu2.cloudfront.net	-	www.cflameper.com s3.amazonaws.com

Under "Select a delivery method for your content" Wizard

Under Web

Click on **Get Started** button

The screenshot shows the 'Select a delivery method for your content' wizard. Step 1: Select delivery method is completed. Step 2: Create distribution is in progress. The 'Web' delivery method is selected. The 'RTMP' delivery method is also listed. A note states: 'You store your files in an origin - either an Amazon S3 bucket or a web server. After you create the distribution, you can add more origins to the distribution.' A large blue 'Get Started' button is at the bottom.

Under Create Distribution

For Origin Domain Name → Drop down → www.cloudskill.com.s3.amazonaws.com

The screenshot shows the 'Create Distribution' wizard at Step 2: Create distribution. In the 'Origin Settings' section, the 'Origin Domain Name' dropdown is open, displaying a list of available origins. The item 'www.cloudskillhyd.com.s3.amazonaws.com' is highlighted. Other options in the list include 'Amazon S3 Buckets', 'cloudmahan1.s3.amazonaws.com', 'crislacat.s3.amazonaws.com', 'saleshydbucket1.s3.amazonaws.com', 'srikanthhyd.s3.amazonaws.com', and 'Elastic Load Balancers'. Below the dropdown, there is a 'Value' input field and a 'Default Cache Behavior Settings' section.

Verify Origin Domain Name got selected

The screenshot shows the 'Create Distribution' wizard at Step 2: Create distribution. In the 'Origin Settings' section, the 'Origin Domain Name' dropdown is now closed, and the selected value 'www.cloudskillhyd.com.s3.amazonaws.com' is displayed in the input field. The other fields in the 'Origin Settings' section remain the same as in the previous screenshot. Below the dropdown, there is a 'Value' input field and a 'Default Cache Behavior Settings' section.

Drag Down

Go for **Distribution Settings**

For **Price Class**

Select **Edge location**

Step 1: Select delivery method

Step 2: Create distribution

Distribution Settings

Price Class: Use All Edge Locations (Best Performance)

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. For example, https://111111111111.cloudfront.net/logo.jpg.
Important: If you choose this option, CloudFront requires that browsers or devices support TLS 1.2 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 upload a certificate from AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

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

Price Class → Use only Canada and Europe

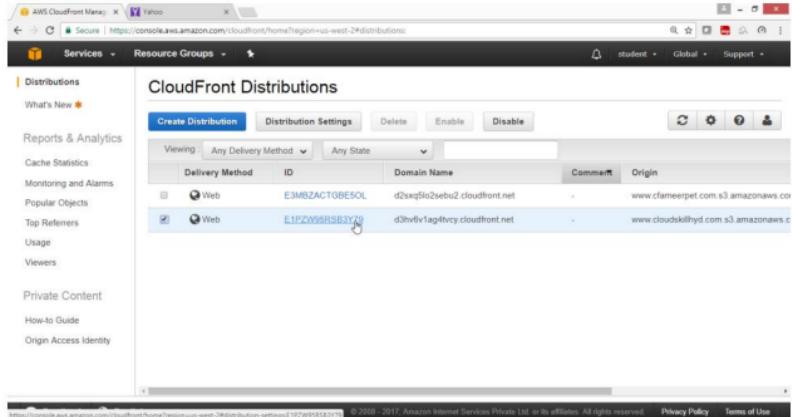
The screenshot shows the 'Distribution Settings' page in the AWS CloudFront console. Under 'Step 2: Create distribution', the 'Price Class' dropdown is set to 'Use Only US, Canada and Europe'. Other settings shown include 'AWS WAF Web ACL' (None), 'Alternate Domain Names (CNAMEs)' (empty), and 'SSL Certificate' (Default CloudFront Certificate). A note about SSL certificates is present, mentioning that users can use HTTPS or HTTP to access content via the CloudFront domain name (e.g., https://11111abcc0f8.cloudfront.net/logo.jpg) or their own alternate domain name. It also notes that CloudFront requires TLS 1.2 or later to access your content. There are options for 'Custom SSL Certificate' and 'Request or Import a Certificate with ACM'.

Drag Down

Click on **Create Distribution**

The screenshot shows the 'Distribution Settings' page in the AWS CloudFront console. Under 'Step 2: Create distribution', several configuration options are listed: 'Default Root Object' (empty), 'Logging' (On selected), 'Bucket for Logs' (empty), 'Log Prefix' (empty), 'Cookie Logging' (Off selected), 'Enable IPv6' (selected), 'Comment' (empty), and 'Distribution State' (Enabled selected). At the bottom right, there are 'Cancel', 'Back', and a large blue 'Create Distribution' button, which is the target of the mouse cursor.

Verify the status

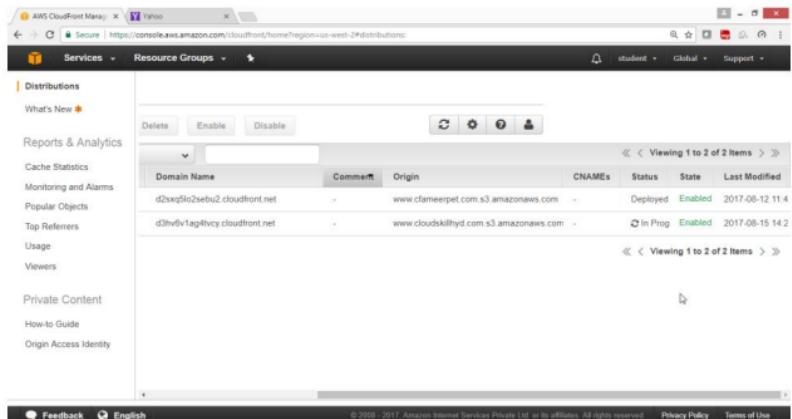


The screenshot shows the AWS CloudFront Distributions page. On the left, there's a sidebar with links like Services, Resource Groups, Distributions, Reports & Analytics, Cache Statistics, Monitoring and Alarms, Popular Objects, Top Referrers, Usage, Viewers, Private Content, How-to Guide, and Origin Access Identity. The main area has tabs for Create Distribution, Distribution Settings, Delete, Enable, and Disable. A search bar is above a table with columns: Delivery Method, ID, Domain Name, Comment, and Origin. Two rows are visible: one for a Web distribution with ID E3MBZACT0BE5OL and another for a Web distribution with ID E1PZW96RSBY3Q.

Delivery Method	ID	Domain Name	Comment	Origin
Web	E3MBZACT0BE5OL	d2xq5lo2sebu2.cloudfront.net	-	www.cloudflare.com s3.amazonaws.com
Web	E1PZW96RSBY3Q	d3hv6vtagltvcy.cloudfront.net	-	www.cloudskilhyd.com s3.amazonaws.com

Check column Status

Shows → In Progress



This screenshot is similar to the previous one but includes explicit status labels for each row. The first distribution's status is 'Deployed' and 'Enabled'. The second distribution's status is 'In Prog' and 'Enabled'. The table structure is identical to the first screenshot.

Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
d2xq5lo2sebu2.cloudfront.net	-	www.cloudflare.com s3.amazonaws.com	-	Deployed	Enabled	2017-08-12 11:4
d3hv6vtagltvcy.cloudfront.net	-	www.cloudskilhyd.com s3.amazonaws.com	-	In Prog	Enabled	2017-08-15 14:2

Wait for status to gen **Enable**

Note : It takes around 15 minutes

The screenshot shows the AWS CloudFront Management Console with the 'Distributions' tab selected. The main area displays a table of distribution configurations. Two distributions are listed:

Comment	Origin	CNAMEs	Status	State	Last Modified
-	www.cfameerpet.com.s3.amazonaws.com	-	Deployed	Enabled	2017-08-12 11:42
-	www.cloudskillhyd.com.s3.amazonaws.com	-	Deployed	Enabled	2017-08-15 14:22

At the bottom of the table, there is a message: "Viewing 1 to 2 of 2 items".

Verify the Site with DNS name "d3hv6v1ag4tvcy.cloudfront.net"

The screenshot shows the AWS CloudFront Management Console with the 'CloudFront Distributions' page. The main area displays a table of distribution configurations. Two distributions are listed:

Delivery Method	ID	Domain Name	Comment	Origin
Web	E3MBZACTGBE50L	d2sxq5lo2sebu2.cloudfront.net	-	www.cfameerpet.com
Web	E1PZW95RSB3Y79	d3hv6v1ag4tvcy.cloudfront.net	-	www.cloudskillhyd.com

At the bottom of the table, there is a message: "Viewing 1 to 2 of 2 items".

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 links like 'Services', 'Resource Groups', 'Distributions', 'Reports & Analytics', 'Private Content', and 'How-to Guide'. The main area is titled 'CloudFront Distributions > E1PZW95RSB3Y79' and contains tabs for 'General', 'Origins', 'Behaviors', 'Error Pages', 'Restrictions', 'Invalidations', and 'Tags'. Under the 'General' tab, detailed information is provided for the distribution:

- Distribution ID:** E1PZW95RSB3Y79
- ARN:** arn:aws:cloudfront:523251683217:distribution/E1PZW95RSB3Y79
- Log Prefix:** -
- Delivery Method:** Web
- Cookie Logging:** Off
- Distribution Status:** InProgress
- Comment:** -
- Price Class:** Use Only US, Canada and Europe
- AWS WAF Web ACL:** -
- State:** Enabled
- Alternate Domain Names (CNAMEs):** -
- SSL Certificate:** Default CloudFront Certificate (* cloudfront.net)
- Domain Name:** d3hv6v1ag4tvcy.cloudfront.net
- Custom SSL Client Support:** -
- Supported HTTP Versions:** HTTP/2, HTTP/1.1, HTTP/1.0
- IPv6:** Enabled
- Default Root Object:** -
- Last Modified:** 2017-08-15 14:28 UTC+5:30
- Log Bucket:** -

At the bottom, there are links for 'Feedback', 'English', and copyright information: '© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' and links to 'Privacy Policy' and 'Terms of Use'.

This Website is coming from CloudFront Service

The screenshot shows a website for 'Car Club'. The header features a navigation menu with links for 'HOME', 'ABOUT', 'ARTICLES', 'CONTACTS', 'SITE MAP', 'Help', and 'FAQ'. Below the menu is a large image of a purple sports car. A search bar is located below the car image. The main content area includes sections for 'Latest News' and 'Welcome to Our Club'. The 'Latest News' section displays two news items with small thumbnail images and dates (10.08.2010 and 03.08.2010). The 'Welcome to Our Club' section contains a brief welcome message and a list of social media links. At the bottom, there's a note about the website template and a footer with links to 'AWS Lab Manual', 'Page | 458', and 'www.zoomgroup.com'.

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

**Complete Package
for Only**

Fees: ₹ 5,900/-

+ 18% GST

**Duration: 3 Months
4 Hrs Per Day**

**100%
GUARANTEED
JOB
ASSISTANCE**

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

Fees: ₹ 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/-
- › CCNA Data Center @ ₹7,500/-
- › IPv6 Migration @ ₹5,500/-
- › CCNP Voice @ ₹9,500/-
- › CCNP Data Center @ ₹9,500/-
- › CCIE Collaboration @ ₹15,500/-
- › CCIE Data Center @ ₹15,500/-

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.