

ZOOM
TECHNOLOGIES



Lab Manual

A Practical Guide to Configuring

AWS

(Amazon Web Services)

Cloud Platform

Lab Manual

© 2017 Zoom Technologies India Pvt. Ltd.

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

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

Introduction

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

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

Each of the exercises is divided into four sections:

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

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

Table of Contents

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

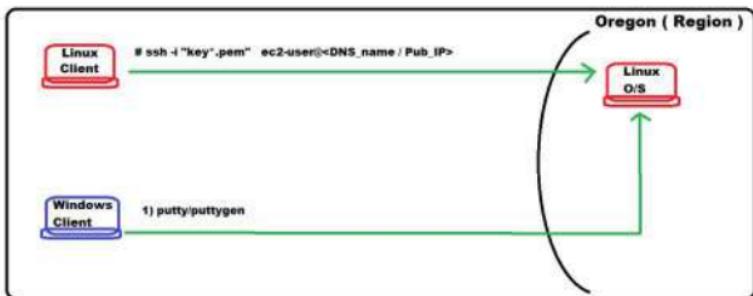
Lab 15: To Configure an Amazon Relational Database Service	337
Lab 16: To Configure Amazon DynamoDB.....	360
Lab 17: To Configure Amazon CloudFormation.....	377
Lab 18: To Configure Amazon Simple E-Mail Service (SES).....	393
Lab 19: To Configure Amazon Simple QUEUE Service SQS.....	408
Lab 20: To Configure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

Lab 1: To Launch Amazon Linux EC2 instance

OBJECTIVE

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

TOPOLOGY



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

PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

TASK :

Launch Amazon Linux instance

Select Region

Select Amazon Machine Image (AMI)

Create key pair

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

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

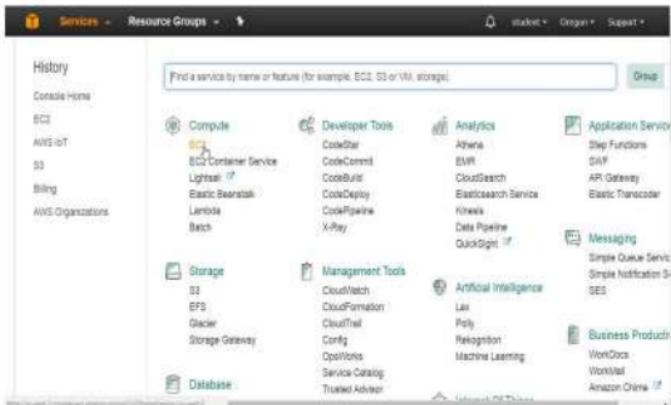
Start/stop/terminate instance

1. To Launch Amazon Linux instance in default VPC

Open the Amazon EC2 console

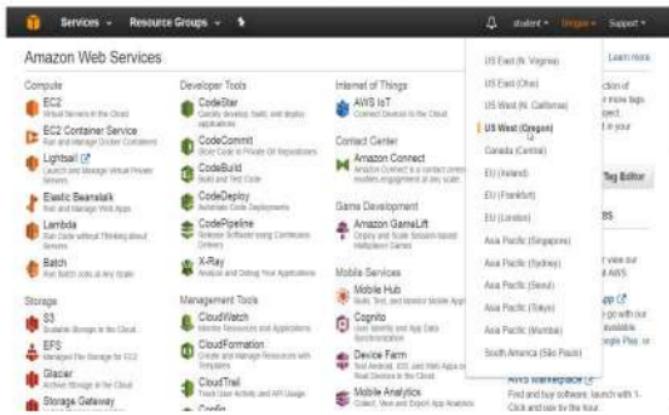
Select Compute

Click on EC2 service



Select the Region, " US West (Oregon) "

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



To check Service Health

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

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Instances, Images, and Elastic Block Store. The main area is titled "Service Health". It shows "Service Status: US West (Oregon): This service is operating normally". Below that is "Availability Zone Status:" with three items: "us-west-2a: Availability zone is operating normally", "us-west-2b: Availability zone is operating normally", and "us-west-2c: Availability zone is operating normally". To the right, there's a section for "Scheduled Events" under "US West (Oregon):" which says "No events". At the bottom right of the main area, it says "Service Health Dashboard".

From the "EC2 Dashboard" panel

Select Instance

Click on "Launch Instance" button

The screenshot shows the AWS EC2 Instances page. The sidebar on the left includes links for EC2 Dashboard, Events, Tags, Reports, Instances, Images, and Elastic Block Store. The main content area has a search bar and a table with two rows of instance data. The columns are Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. The first instance is named "instname" with Instance ID i-04ca59221f1ac0ba, Instance Type t2.micro, Availability Zone us-west-2b, Instance State running, Status Checks healthy, and Alarm None. The second instance is named "instname2" with Instance ID i-056bf5f194e0d24dd, Instance Type t2.micro, Availability Zone us-west-2c, Instance State running, Status Checks healthy, and Alarm None. Below the table, there are tabs for Description, Status Checks, Monitoring, and Tags. Under the Description tab, it lists two instance IDs: i-04ca59221f1ac0ba (instname) and i-056bf5f194e0d24dd (instname2). At the bottom, there are links for Feedback, English, and a footer with copyright information.

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

Select "Quick start"

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

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

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and 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

Cancel and Exit

1 to 21 of 31 AMIs

Image	AMI Name	Type	Size
	Amazon Linux AMI 2017.03.0 (HVM), SSD Volume Type - ami-4c35a426	Select	64 GB
	Red Hat Enterprise Linux 7.3 (HVM), SSD Volume Type - ami-088cf0f	Select	64 GB

Feedback English

© 2016, 2017 Amazon.com Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

On "Choose an Instance Type" page

Select type "**t2.micro**", eligible for the free tier.

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

The screenshot shows the AWS CloudFormation console with the "Step 2: Choose an Instance Type" step selected. The table lists various instance types, with the **t2.micro** row highlighted. The t2.micro row has the following details:

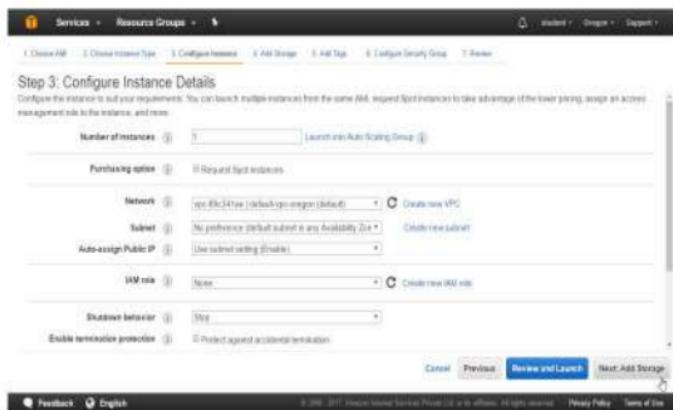
Family	Type	vCPUs	Memory (GB)	Instance Storage (GB)	EBI-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.micro	1	0.5	388.000	-	Low to Moderate	Yes
General purpose	t2.micro <small>(selected)</small>	1	0.5	388.000	-	Low to Moderate	Yes
General purpose	t2.small	1	2	388.000	-	Low to Moderate	No
General purpose	t2.medium	2	4	1920.000	-	Low to Moderate	No

At the bottom, the "Review and Launch" button is visible, indicating the next step in the process.

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 in Auto Scaling Group:

Purchasing option: Reserve Spot Instances

Network: vpc-fbc54f8e (default-type: private, default) Create new VPC

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

Auto-assign Public IP: Use subnet setting (Enable) Create new IAM role

IAM role: Amazon Lambda Create new IAM role

Shutdown behavior: Stop 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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MiB/s)	Delete on Termination	Encrypted
General Purpose SSD	/dev/xvda	snap-0ca9f75735518cbef	8	General Purpose SSD	100 / 3000	N/A	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 limits.

CANCEL PREVIOUS **Review and Launch** Next: Add Tags

On "Add Tags" page

Provide following values

Key → Name

Value → linuxvm

Click on "Next: Configure Security Group" 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	(33 characters maximum)	Instances	Volumes
Name		linuxvm		1	0

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Feedback English © 2014-2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

On "Configure Security Group" page

Select → Create a new security group

Leave all values as default.

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

Click "Review and Launch" button

Step 6: Configure Security Group

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

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

Security group name:

Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	Custom <input type="text" value="0.0.0.0"/>

Add Rule

Cancel Previous Review and Launch

On "Review Instance Launch", page

Leave all values as default.

Verify the summary, then drag down

The screenshot shows the AWS Step 7: Review Instance Launch page. At the top, there are tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. The 7. Review tab is selected. Below the tabs, a yellow warning box says: "Improve your instances' security. Your security group, launch-wizard-1, is open to the world." It continues: "Your instance 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 group".
The main content area has sections for AMI Details, Instance Type, and Storage. The Instance Type section shows: Instance Type: t2.micro, ECU: 0.25, vCPUs: 1, Memory (GiB): 1.0, Instance Storage (GiB): 16, EBS-Optimized Available, and Network Performance. Buttons at the bottom right of this section are 'Cancel', 'Previous', and 'Launch'.
At the bottom of the page, there are links for 'Feedback', 'English', and 'AWS 2017 - Amazon Web Services Privacy Policy Terms of Use'.

Verify the summary

Click on **Launch** button

This screenshot is identical to the one above, showing the AWS Step 7: Review Instance Launch page. The 'Launch' button is highlighted with a red box at the bottom right of the Instance Type section. The rest of the interface, including the summary and other configuration options, remains the same.

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

Select "Create a new key pair"

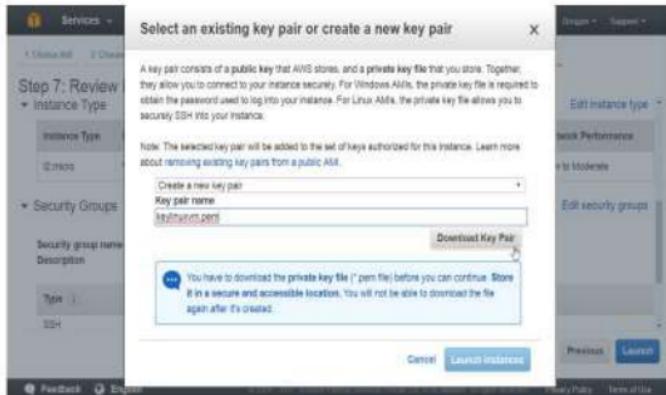
Enter Key pair name → keylinuxvms.pem

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

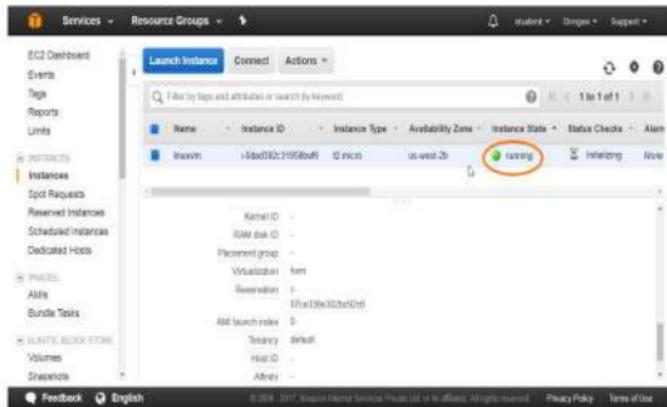
The screenshot shows the AWS Launch Status page. At the top, there is a navigation bar with icons for Services, Resource Groups, and links for Student, Logout, and Support. Below the navigation bar, the title "Launch Status" is displayed. A note below the title states: "Instances we start immediately and continue to accrue until you stop or terminate your instances." There is 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." Below this, there is a section titled "Here are some helpful resources to get you started" with three items: "How to connect to your Linux instance" (with a link to the Amazon EC2 User Guide), "Learn about AWS Free Usage Tier" (with a link to the Amazon EC2 Discussion Forum), and "Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)" (with a link to the Create and attach additional EBS volumes (Additional charges may apply)). There is also a link "Manage security groups". At the bottom right of the main content area, there is a blue button labeled "View instances". At the very bottom of the page, there are links for Feedback, English, Copyright information (© 2014-2017 Amazon Internet Services Private Ltd. All Rights Reserved.), Privacy Policy, and Terms of Use.

On EC2 Dashboard panel

Click on Instances,

Select instances

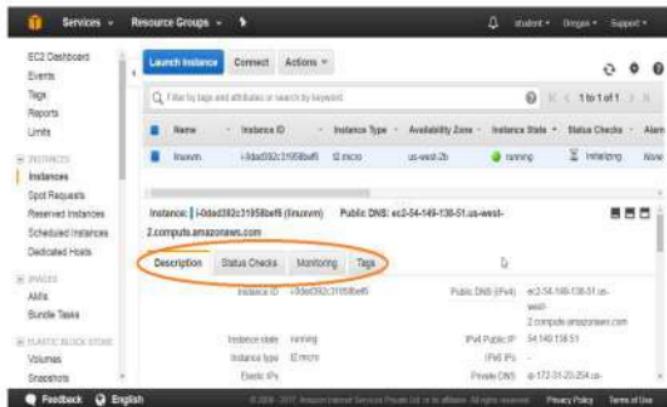
Check instance status → running



The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Units, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, and more. The Instances link is highlighted. In the main pane, there's a search bar and a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. One row is visible for an instance named 'Inuvnm' with the status 'running' circled in red.

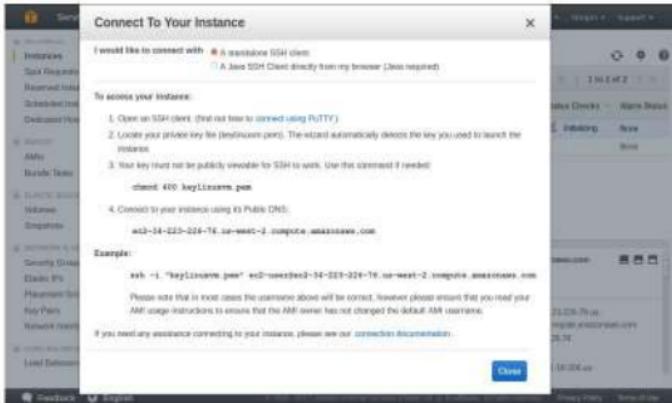
To check instance details like

Description, Status check, Monitoring, Tags



This screenshot is similar to the previous one, showing the EC2 Dashboard with the Instances section selected. An instance named 'Inuvnm' is selected. At the bottom of the instance card, there are four tabs: 'Description', 'Status Checks', 'Monitoring', and 'Tags'. The 'Description' tab is highlighted and circled in red. It displays the instance ID and its public DNS name.

1a) To connect to “Amazon linux instance” from linux client operating system.
On “[Connect To Your Instance](#)” page see the guide lines to connect to linux instance.



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

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

eg : keylinuxvm.pem

```
# ls
```

```
# ll
```

```
# chmod 400 keylinuxvm.pem
```

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

The screenshot shows a terminal window on a Linux desktop environment. The terminal output is as follows:

```
$ ls -l keylinuxvm.pem
-rw-r--r-- 1 sheikh sheikh 1692 Jun  8 12:30 keylinuxvm.pem
$ chmod 400 keylinuxvm.pem
$ ls -l keylinuxvm.pem
-r----- 1 sheikh sheikh 1692 Jun  8 12:30 keylinuxvm.pem
$ 
$ ssh -i "keylinuxvm.pem" ec2-user@ec2-34-223-226-76.us-west-2.compute.amazonaws.com
The authenticity of host 'ec2-34-223-226-76.us-west-2.compute.amazonaws.com (34.223.226.76)' can't be established.
ECDSA key fingerprint is 90:9e:db:17:4b:f1:c5:0b:a2:38:98:8b:93: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' (EDSA) 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
```

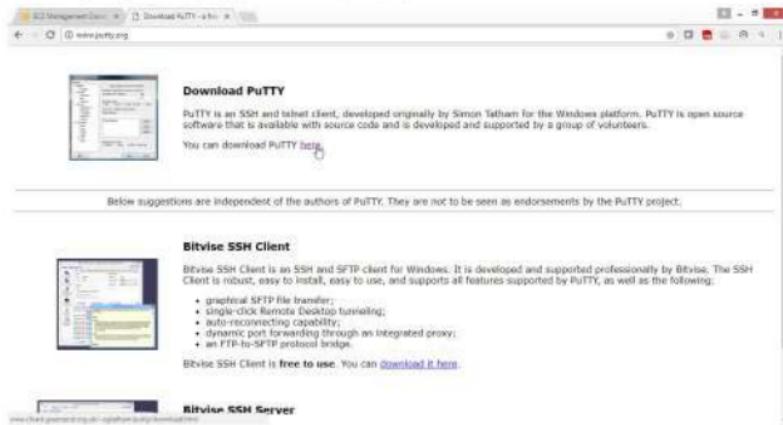
To logout

```
# 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
```

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

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



The screenshot shows a Microsoft Edge browser window with 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 latest" is provided. Below this, a note states: "Below suggestions are independent of the authors of PuTTY. They are not to be seen as endorsements by the PuTTY project;". A section titled "Bitvise SSH Client" follows, featuring a screenshot of the software interface and a brief description: "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:". A bulleted list includes: "graphical SFTP file transfer", "single-click Remote Desktop tunneling", "auto-reconnecting capability", "dynamic port forwarding through an integrated proxy", and "an FTP-to-SFTP protocol bridge". It also mentions that the client is "free to use" and provides a link to download it.

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



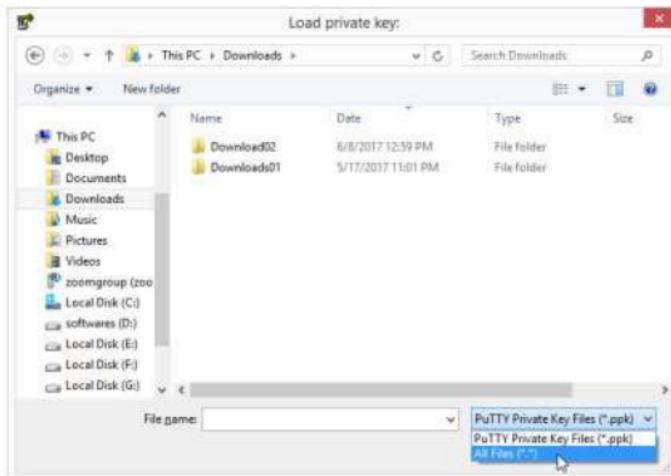
Click on Load button



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

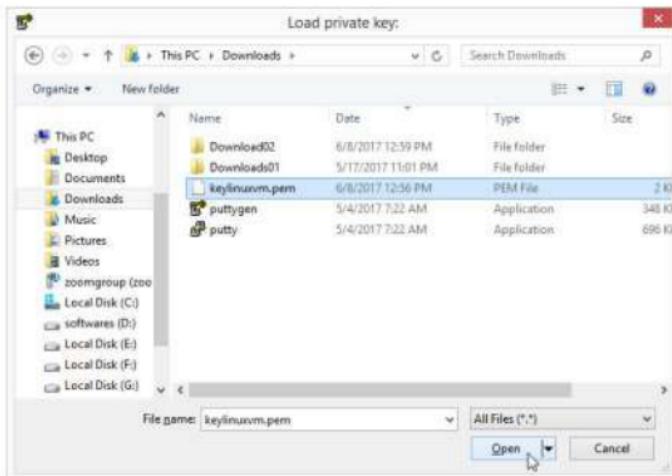
So to locate your .pem file

On file names Select →All files (*.*)

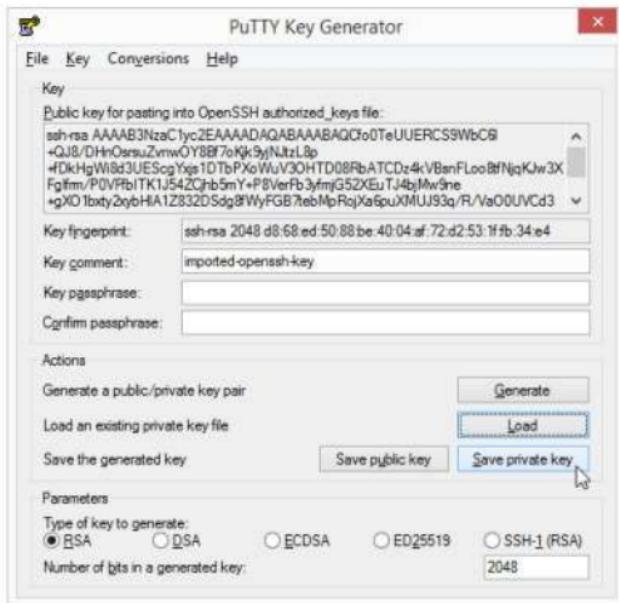


Locate keylinuxvm.pem in your folder

Click on open

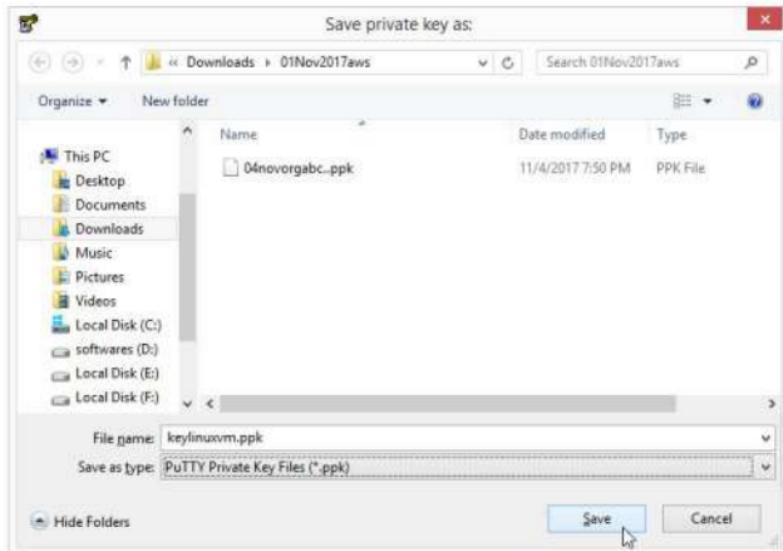


Click on "Save private key" button



Save the file → keylinuxvm.ppk

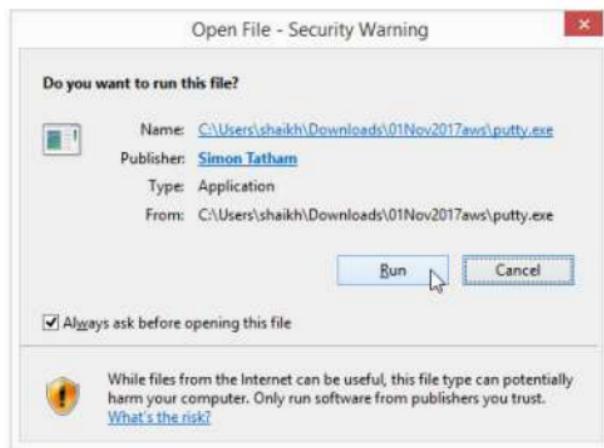
Click on Save button



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

Run putty.exe

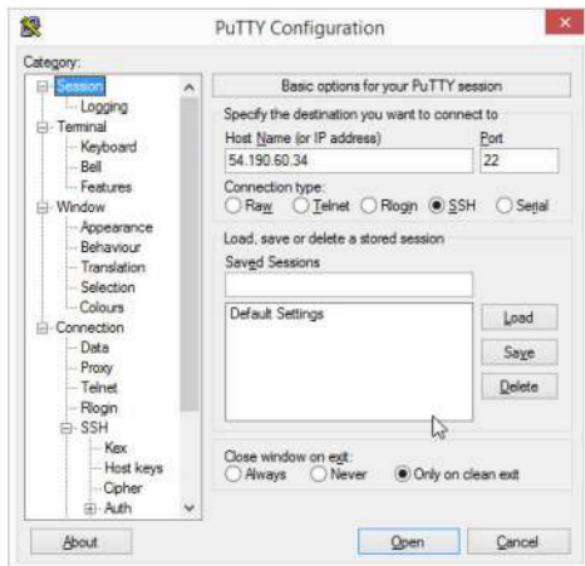
Click on Run



On Category page provide following values:

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

Port → 22

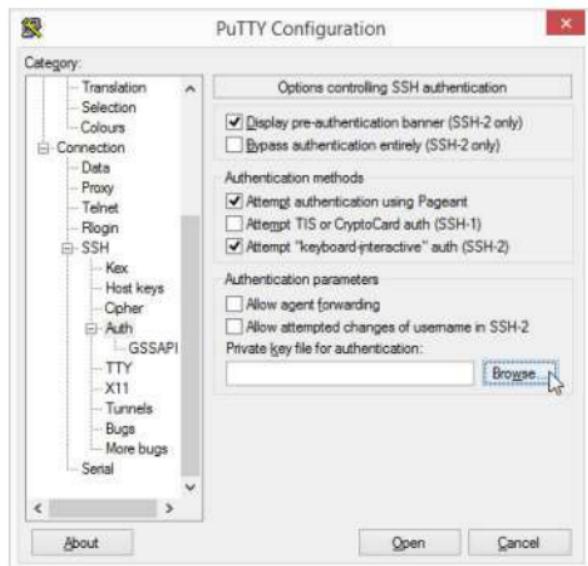


Under Connection expand

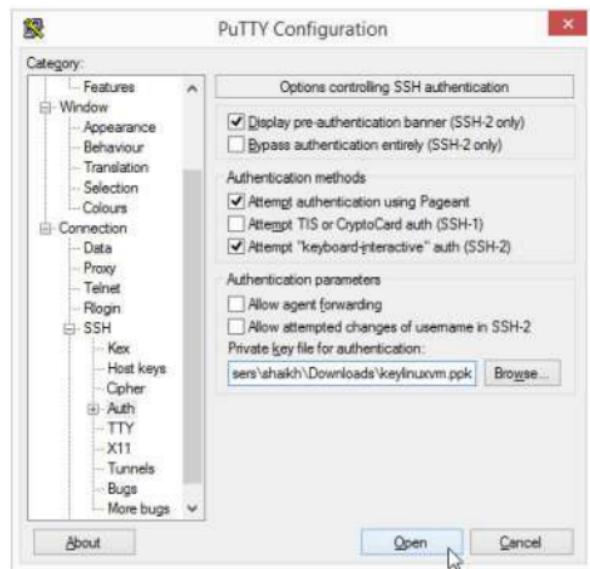
Click on SSH → Auth

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

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

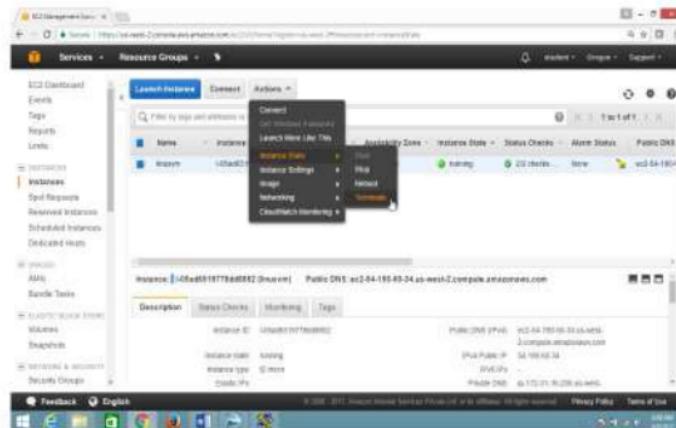
To start/stop/terminate instance

On Ec2 Dashboard

Select the Instance

Drop down on Action button

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



Note:

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

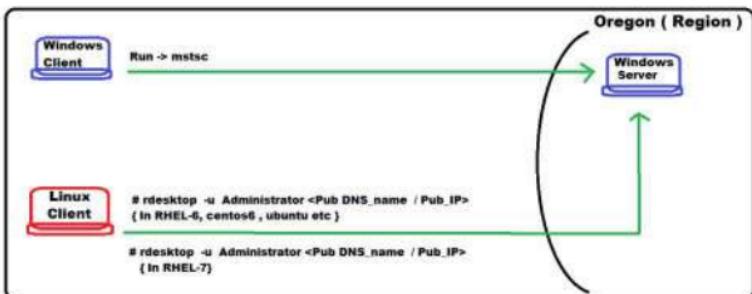
Otherwise it will be charged if the limit is over after free tier usage.

Lab 2: To Launch Windows EC2 instance in AWS

OBJECTIVE

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

TOPOLOGY



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

PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

TASK :

To Launch Windows instance

Select Region

Select Amazon Machine Image (AMI)

Create key pair

Connect from Windows operating system

Connect from Linux Operating system

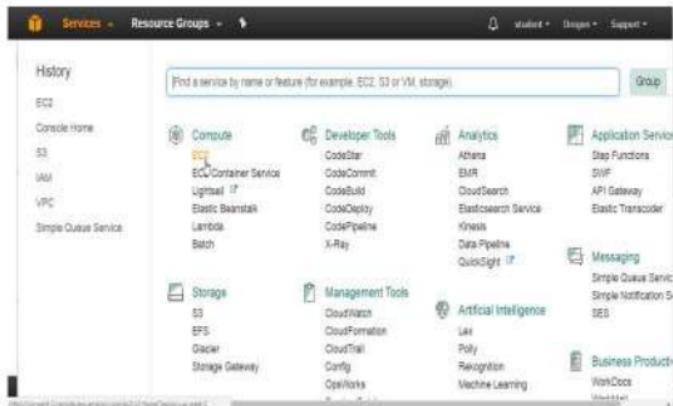
Start/stop/terminate instance

1. To Launch Windows instance in default VPC

Open the Amazon EC2 console.

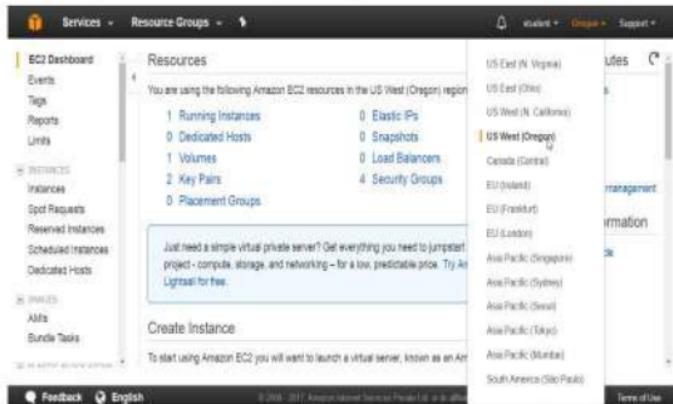
Select **Compute**

Click on **EC2 service**



Select the Region, "US West (Oregon)"

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



To check Service Health

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

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Units, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, and Bundle Tasks. The main area has two tabs: 'Service Health' and 'Scheduled Events'. Under 'Service Health', it says 'Service Status: US West (Oregon)' with a green status icon and the text 'This service is operating normally'. Under 'Availability Zone Status', it lists three zones: 'us-west-1a' (operating normally), 'us-west-2a' (operating normally), and 'us-west-2c' (operating normally). To the right, there's a sidebar for 'EC2 Launch Wizard... Only these popular AMIs:' which includes 'Barracuda NextGen Firewall F-Series - FNG' (provided by Barracuda Networks, Inc., rating 4.5/5, starting from \$0.60/hr or \$4,590/yr (12% savings) for software + AMI usage fees, view all Network Infrastructure), 'VM-Series Next-Generation Firewall Bundle 2' (provided by Palo Alto Networks, rating 4.5/5, \$1.25/hr or \$4,500/yr (60% off)), and 'AWS Lambda - Java 8' (provided by Amazon Web Services, Inc., rating 4.5/5, \$0.20/hr or \$4,500/yr (60% off)). At the bottom, there are 'Feedback', 'English', and other navigation links.

From the "EC2 Dashboard" panel

Select Instance

Click on "Launch Instance" button

The screenshot shows the AWS EC2 Dashboard. The left sidebar is identical to the previous one. The main area has a 'Launch Instance' button at the top. Below it is a search bar and a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm I. One row is visible: 'Instance: i-05ad9519779d8852 (imxnm)' with 'Public DNS: ec2-54-190-83-34.us-west-2.compute.amazonaws.com'. At the bottom, there are tabs for Description, Status Checks, Monitoring, and Tags. The Status Checks tab shows two entries: 'Instance ID: i-05ad9519779d8852' with 'Public IPv4: ec2-54-190-83-34.us-west-2.compute.amazonaws.com' and 'IPv6 Public IP: 54.190.63.34' (status 'running'), and 'Instance state: running' with 'IPv4 IP: -' (status 'running'). At the very bottom, there are 'Feedback', 'English', and other navigation links.

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 21 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)

Windows

Microsoft Windows Server 2012 with SQL Server Standard - ami-d5b1f4bd
Microsoft Windows Server 2012 Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Standard edition [English]
Root device type: msp - Virtualization type: HVM

Microsoft Windows Server 2008 R2 Base - ami-0381e483
Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture [English]
Root device type: msp - Virtualization type: HVM

Microsoft Windows Server 2008 R2 with SQL Server Express and IIS - ami-3483e654
Microsoft Windows Server 2008 R2 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 Express edition [English]
Root device type: msp - Virtualization type: HVM

Select

Select

Select

On "Choose an Instance Type" page

Select type "t2.micro", eligible for the free tier.

Click on "Next: Configure Instance Details" button

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

On "Configure Instance Details" page

Leave all values as default

Click on "Next : Add storage" button

Step 3: Configure Instance Details

Configure the instance to fit 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-0bc34f6e | 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) Create new directory

Domain join directory: None Create new directory

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 AMI, 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, a heading says "Step 4: Add Storage" with a sub-instruction: "Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2." A table lists a single volume entry:

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-09c0e0212374e6c8	30	General Purpose (SSD)	100 / 3000	N/A	No	Not Encrypted

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

On "Add Tags", page

Provide following values

Key → Name
Value → winserver

Click on "Next: Configure Security Group" 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	Value	Instances	Volumes
Name	winserver	1	0

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 LLC or its affiliates. All rights reserved. Privacy Policy Terms of Use

On “Configure Security Group” page

Select → Create a new security group

Leave all values as default.

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

Click "Review and Launch" button

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
RD ^P	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.

AMI Details

Microsoft Windows Server 2008 R2 Base - ami-0381e483

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

Free tier available for 1 year. View details

Launch

Verify the summary

Click on **Launch** button

Step 7: Review Instance Launch

Security group name: launch-wizard-4

Description: launch-wizard-4 created 2017-06-09T06:46:33.392+02:30

Type	Protocol	Port Range	Source
RDP	TCP	3389	0.0.0.0

Instance Details

Storage

Tags

Launch

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

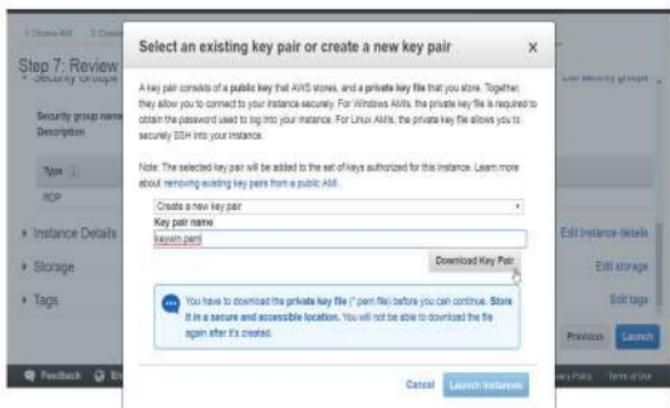
Select "Create a new key pair"

Enter Key pair name → keywin.pem

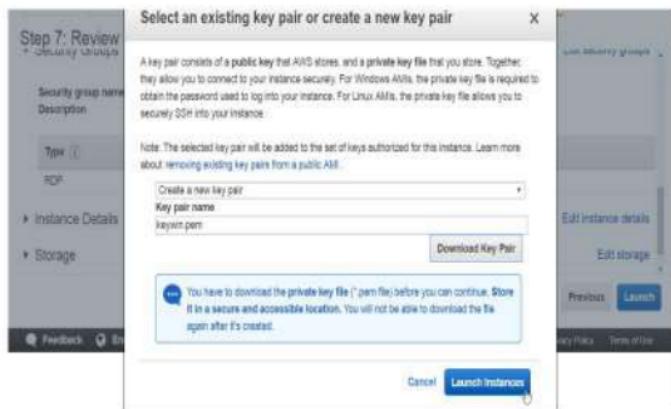
Click on "Download Key Pair"

Note: Store it in a secure and accessible location.

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

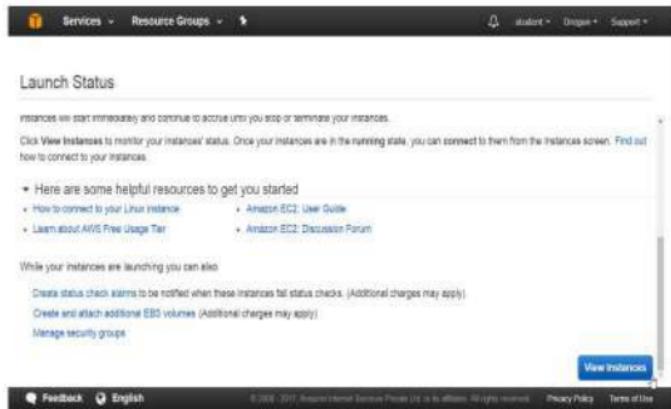


Click on "Launch an instance"



On Launch Status page, go to right bottom corner

Click "View instances" button



On EC2 Dashboard panel

Click on Instances

Select instances

Check instance state → pending

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links: Services (dropdown), Resource Groups (dropdown), Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, IAMs, and Elastic Block Store. At the top, there are buttons for Launch Instance, Create, Actions, and a search bar. Below the search bar is a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. There are two rows in the table:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
winserver	i-06e739863570803	t2.micro	us-west-2b	pending	2/2 checks ...	N/A
Inositi	i-0ed8519779a8802	t2.micro	us-west-2b	running	2/2 checks ...	N/A

A tooltip 'Select an instance above' is visible near the bottom of the table. At the bottom of the page, there are links for Feedback, English, and footer links: ©2017 Amazon Web Services, Inc. or its affiliates. All rights reserved., Privacy Policy, and Terms of Use.

Once instance starts state is →running

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'INSTANCES' section, 'Instances' is selected. The main content area displays a table of instances. The first instance, 'winserver', has an orange circle around its 'running' status in the 'Status Checks' column. The second instance, also 'winserver', also has an orange circle around its 'running' status in the same column. Both instances have a green circular icon next to their names.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
winserver	i-0fae73ff535793d	t2.micro	us-west-2b	running	2/2 checks	None
winserver	i-0fae73ff535793d	t2.micro	us-west-2b	running	2/2 checks	None

To check instance details like

Description, Status check, Monitoring, Tags

This screenshot shows the same AWS EC2 Instances page as the previous one, but it is focused on the details for the first 'winserver' instance. The 'Tags' tab in the navigation bar is highlighted with an orange circle. The instance details table shows the 'winserver' instance with its status as 'running' in the 'Status Checks' column, which is also circled in orange.

Description	Status Checks	Monitoring	Tags
Instance ID: i-0fae73ff535793d	Public DNS: ec2-54-214-137-73.us-west-2.compute.amazonaws.com	IPv4 Public IP: 54.214.137.73	

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

Open Ec2 Dashboard Console

Go to instance

Select the instance you want to connect

Click Connect button

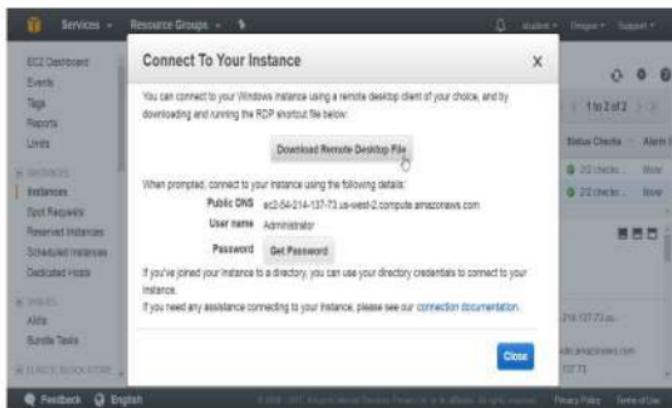
The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links: EC2 Dashboard, Events, Tags, Reports, Units, Instances (which is selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Photos, Alerts, and Elastic Block Store. The main content area has tabs: Launch Instance, Connect (which is highlighted), and Actions. A search bar at the top says "Filter by tags and attributes or search by keyword". Below it, a table lists two instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
winwin	i-05e651973a8a8852	t2.micro	us-west-2b	running	2/2 checks ...	N/A
winserver	i-06e073965570003	t2.micro	us-west-2b	running	2/2 checks ...	N/A

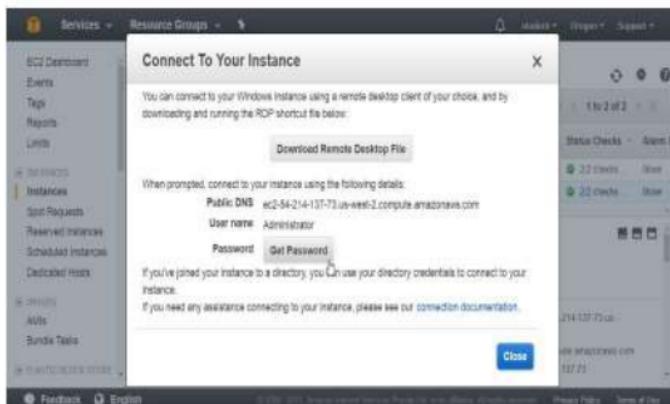
Below the table, there's a summary for the selected instance: Instance ID: i-06e073965570003, Public DNS: ec2-54-214-137-73.us-west-2.compute.amazonaws.com. It also shows the instance state as running and the IP/Public IP as 54.214.137.73.

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

Click on "Download Remote Desktop file" button



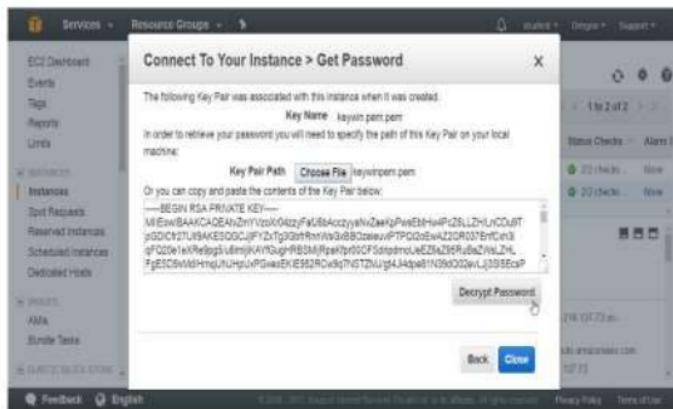
Click on "Get Password" button



Click on "Choose file" button

Provide the path of key file

Click on "Decrypt Password" button



Click on Close button



Copy your instance Detail in Notepad

Public DNS ec2-54-214-234-57.us-west-2.compute.amazonaws.com

User name Administrator

Password *****

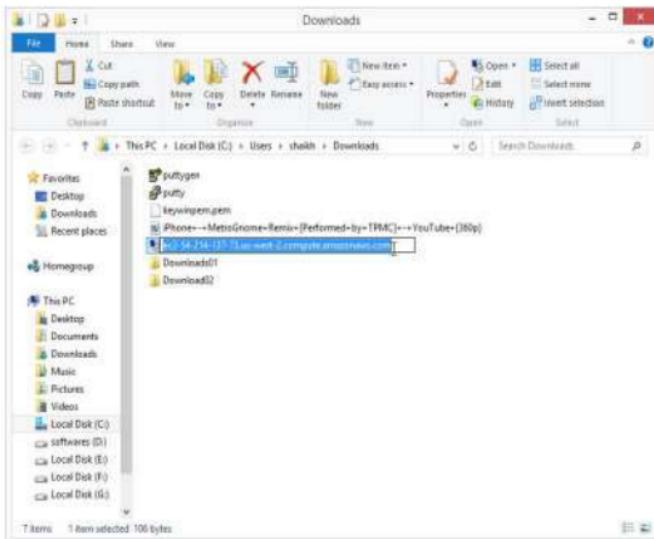
Click on **Close** button.



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

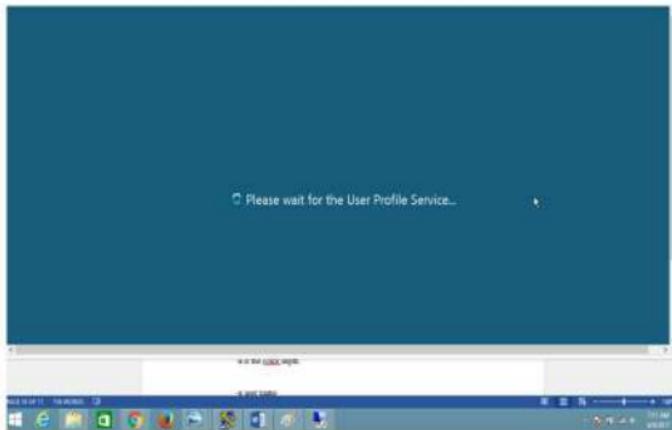
Click on OK



Click on Yes button



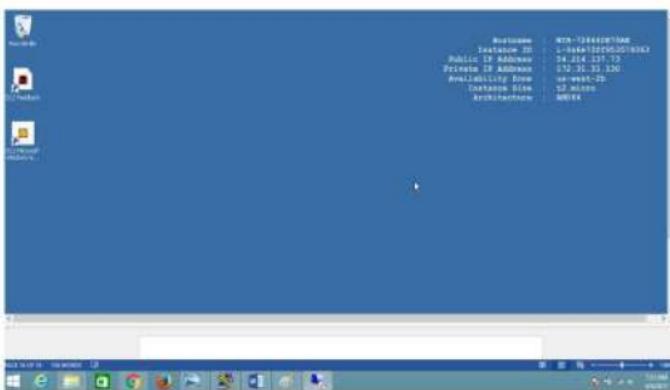
Wait for a movement



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

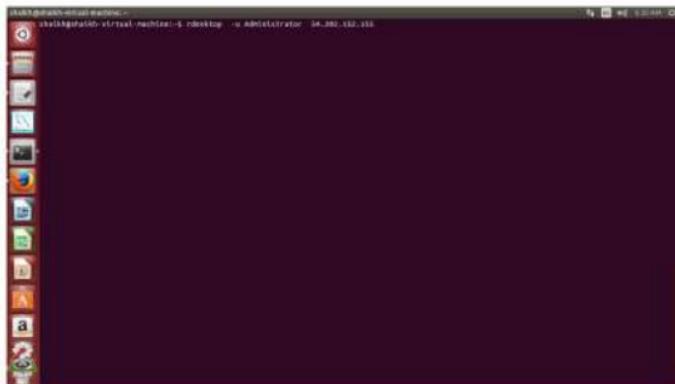
Note: rdesktop or xfreerdp { RHEL-6,7 } package should be installed

\$ rdesktop -u Administrator <Pub_DNS_name / Public_IP>

or

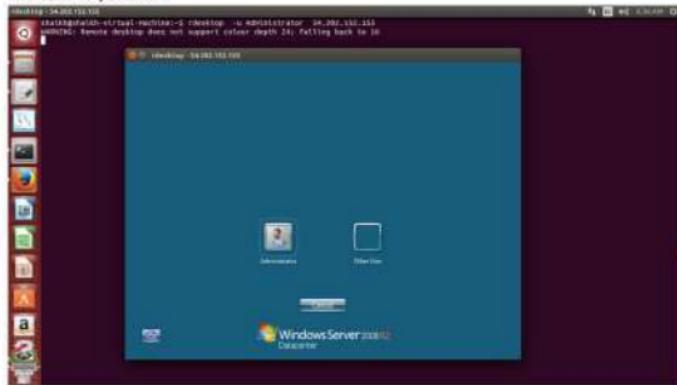
\$ xfreerdp -u Administrator <Pub_DNS_name / Public_IP> { in RHEL 6,7 }

-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

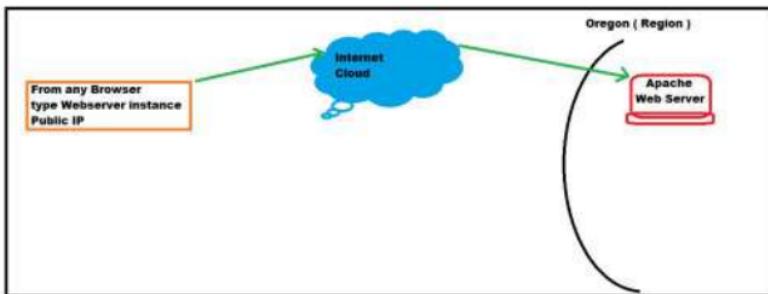
Otherwise it will be charged if the limit is over after free tier usage.

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

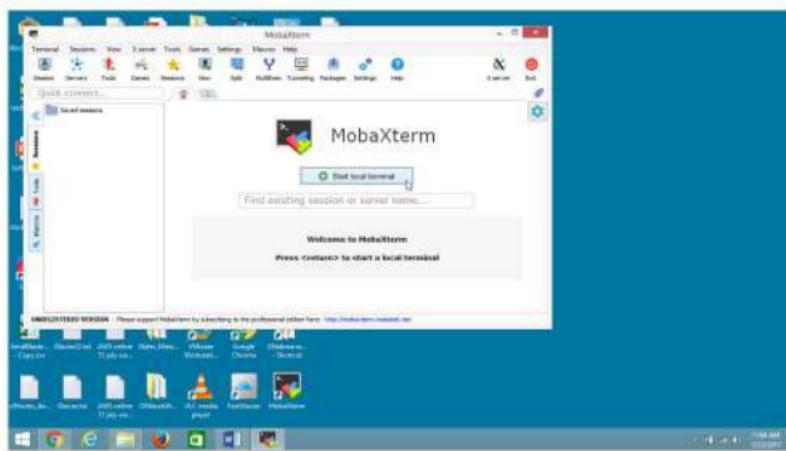
1) Launch Amazon linux instance and login to your instance

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

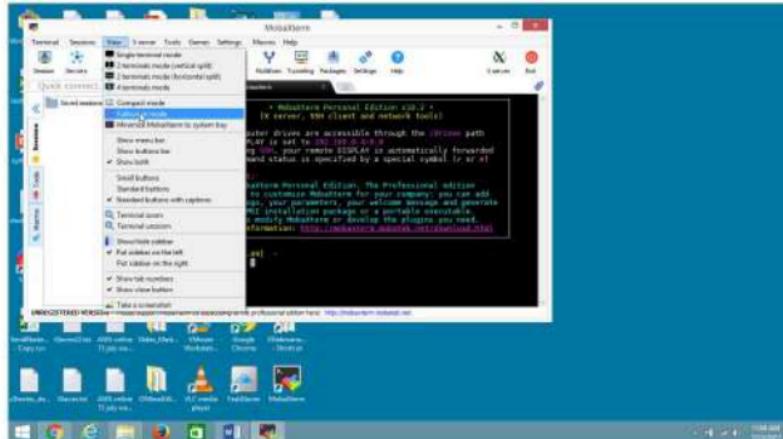
2) Connect to linux instance from windows using MobaXterm

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

```
~ MobaTerm Personal Edition v0.9.2 ~
[8 server, SSH client and network tools]
* local drives are accessible through the .drive path
* local FSCK'd
* when using .drive, your remote DISPLAY is automatically forwarded
* both command status is specified by a special symbol (< or >)

+ Important
The MobaTerm Personal Edition, the Professional edition
allows you to customize MobaTerm for your company, you can add
your own logo, your company's colors, your clients' names and
more. You can also add your own applications or additional executables
we can also modify MobaTerm or develop the plugins you need.
For more information: http://mobateam.com/moba-term/professional-edition.html

2017-01-21 11:04:09
root@ip-10-10-1-10 ~ % cd e:/awskeys
```

Login to linux instance by typing the following command

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

```
[2017-07-23 09:34:47] /drives/e/awskeys
[shaikh_pc_mas] > ssh -i "keyorg123.pem" ec2-user@ec2-54-186-150-140.us-west-2.compute.amazonaws.com
Warning: Permanently added 'ec2-54-186-150-140.us-west-2.compute.amazonaws.com' (RSA) to the list of known hosts.
X11 forwarding request failed on channel 0

[ ]( [ ] ) Amazon Linux AMI
[ ]\|_|_]

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

Switch to root user

Type "sudo su"

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

Configure Apache Webserver run following commands as shown in the screen

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

To use vi editor

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

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

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

Open the AWS console.

On the **EC2 Dashboard** panel

Select the linux instance

The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with navigation links: EC2 Dashboard, Events, Tags, Reports, Lists, Instances (selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Instances (under Instances), Alarms, Batch, Step Functions, and Elastic Block Store (EBSS). The main content area is titled "Instances" and shows a table with one row. The table columns are: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, and Public DNS. The single row contains: Name "Linuxwebserver", Instance ID "i-08e8a7e0ca8a3561", Instance Type "t2.micro", Availability Zone "us-west-2c", Instance State "running", Status Checks "2/2 checks", Alarm Status "None", and Public DNS "ec2-54-193-140.us-west-2.compute.amazonaws.com". Below the table, there's a detailed view for the instance: Description, Status Checks, Monitoring, Tags, and Metrics. It shows the instance ID, scheduled/unscheduled, Public DNS (IPv4), and IPv6 Public IP. The instance state is running, instance type is t2.micro, and flavor size is 1. At the bottom of the page, there are links for Feedback, English, and Terms of Use, along with a "Close all" button.

Go to the right end

Select **Security Groups**

Click on **Launch-wizard-1**

The screenshot shows the AWS Management Console with the EC2 Instances page open. On the left, there's a sidebar with navigation links like EC2 Dashboard, Events, Tags, Reports, Lists, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Metrics, Alarms, and CloudWatch Metrics. The main area shows a table of instances. One instance, 'Launch-wizard-1', is highlighted with a blue box. Its details are shown in a modal window below:

Description	Status Checks	Monitoring	Tags
Instance ID: i-06e8a71e0c0ca9561 (Linuxwebserver)	Public DNS (IPv4): ec2-54-185-182-142.us-west-2.compute.amazonaws.com	Public DNS (IPv6): ec2-54-185-182-142.us-west-2.compute.amazonaws.com	
Instance State: running	Private IP: 54.186.182.142	IPv6 IP: -	
Instance Type: t2.micro	Private DNS: ip-54-185-182-142.us-west-2.compute.amazonaws.com		

Click on **Inbound** button

The screenshot shows the AWS Management Console with the Create Security Group page open. The sidebar on the left is identical to the previous screenshot. The main area shows a table of security groups. One security group, 'Launch-wizard-1', is highlighted with a blue box. Its details are shown in a modal window below:

Description	Inbound	Outbound	Tags
Group name: Launch-wizard-1	Group ID: sg-04ab6510	VPC ID: vpc-0d8c86ee	Description: Launch-wizard-1 created 2017-07-22T06:37:33Z

The 'Inbound' tab is selected in the modal window. Below it, there's another table with columns: Group name, Group ID, and Group description.

Click on Edit button

The screenshot shows the AWS EC2 Management Console. In the center, there is a table titled "Security Group: sg-4ab05510". One of the rows in the table has an "Edit" button next to it. The table columns are "Type", "Protocol", "Port Range", and "Source". The first row's values are "SSH", "TCP", "22", and "0.0.0.0". Below the table, there are tabs for "Description", "Inbound", "Outbound", and "Tags". The "Inbound" tab is selected. At the bottom of the page, there is a large "Edit" button.

Click on Add Rule button

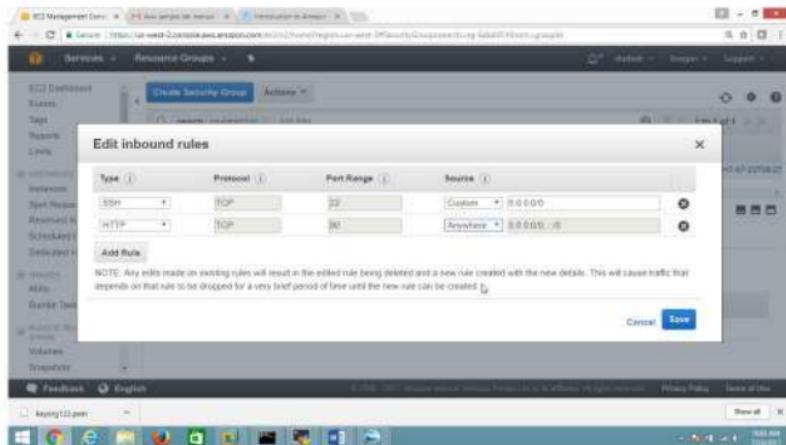
The screenshot shows the AWS EC2 Management Console with a modal dialog titled "Edit inbound rules". Inside the dialog, there is a form with fields for "Type" (set to "SSH"), "Protocol" (set to "TCP"), "Port Range" (set to "22"), and "Source" (set to "Custom 0.0.0.0"). Below the form is a note: "NOTE: 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 matching 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.

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 Management Console with the EC2 Services menu selected. On the left, the navigation pane is open, showing sections like Instances, AMIs, and EBS. The main area displays the 'Launch Instances' wizard. At the top, there are tabs for 'Launch Instances', 'Compute', and 'Actions'. A search bar is present above the table. The table lists two instances: 'Nurse' and 'Univerbank'. The 'Nurse' instance is highlighted. Below the table, a detailed view of the 'Nurse' instance is shown, including its description ('Ubuntu 14.04 LTS (64-bit)'), status check ('initial'), monitoring ('disabled'), and tags. It also shows its public DNS ('ec2-54-198-150-140.us-west-2.compute.amazonaws.com'), private IP ('54.198.150.140'), and IPv6 IP ('::'). The status bar at the bottom indicates the browser is running on Windows 7.

Verify

Website is running

The screenshot shows a web browser window with the URL 'http://54.198.150.140'. The page content is 'Welcome to Apache Webserver in AWS instance'. The browser interface includes a back button, forward button, and a search bar. The taskbar at the bottom shows icons for various applications, including a file explorer, a browser, and system tools. The status bar at the bottom right shows the date and time as 'Wednesday, April 22, 2015 10:30 AM'.

Lab 4: To Assign Elastic IP address

Elastic IP

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

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

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

To assigning Elastic IP to an instance

Open AWS console

On the **EC2 Dashboard** panel

Select "**Network Security**"

Click on **Elastic IP**

The screenshot shows the AWS EC2 Management Console interface. The left sidebar has a tree view with 'NETWORK & SECURITY' expanded, showing 'Security Groups', 'Elastic IPs' (which is selected and highlighted in blue), 'Placement Groups', 'Key Pairs', and 'Network Interfaces'. Below that is 'LOAD BALANCERS' with 'Load Balancers' and 'Target Groups'. Under 'AUTO SCALING' are 'Launch Configurations' and 'Auto Scaling Groups'. At the bottom of the sidebar is 'SYSTEM PAGER' with 'SERVICES'. The main content area has a header with 'Launch Instance', 'Connect', and 'Actions'. A search bar says 'Filter by tags and attributes or search by keyword'. A table lists one instance: 'Name: i-09e8a71e3ce8a8561 (Linuxwebserver)', 'Instance ID: i-09e8a71e3ce8a8561', 'Instance Type: t2.micro', 'Availability Zone: us-west-2c', 'Instance State: running', and 'Status Checks: 2/2 checks'. Below the table are tabs for 'Description', 'Status Checks', 'Monitoring', and 'Tags'. At the bottom of the page is a footer with links for 'AWS Support', 'AWS Marketplace', 'AWS Documentation', 'AWS Terms of Use', 'AWS Privacy Policy', and 'AWS Customer Agreement'. The status bar at the bottom right shows '100% 100% 100%'.

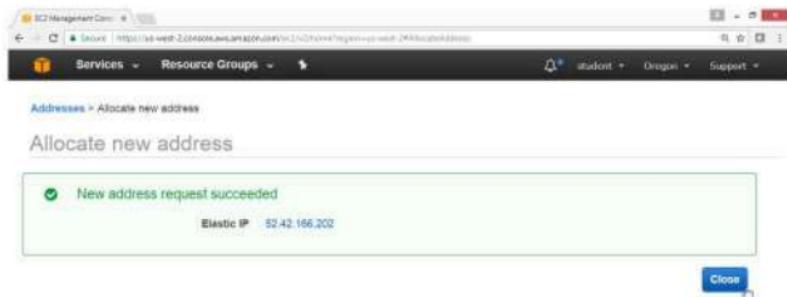
Click on Allocate new address button

The screenshot shows the AWS Management Console interface. The top navigation bar includes 'Services', 'Resource Groups', and 'Actions'. A sidebar on the left lists various services: 'Networking & Security' (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), 'Load Balancing' (Load Balancers, Target Groups), and 'Auto Scaling' (Launch Configurations, Auto Scaling Groups). The main content area has a heading 'Allocate new address' and a message 'You do not have any Addresses in this region'. Below this is a button labeled 'Allocate new address'. At the bottom of the page, there is footer information including 'Feedback', 'English', and copyright details.

Click **Allocate** button

The screenshot shows the 'Allocate new address' dialog box. It has a title 'Allocate new address' and a sub-instruction 'Allocate a new Elastic IP address by selecting the scope in which it will be used'. There is a required field indicator (* Required) and two buttons at the bottom: 'Cancel' and 'Allocate'. The background of the dialog is white, and it is centered over the previous screenshot's content.

Click on **Close** button



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

Verify website is running with elastic IP.



To releasing Elastic IP

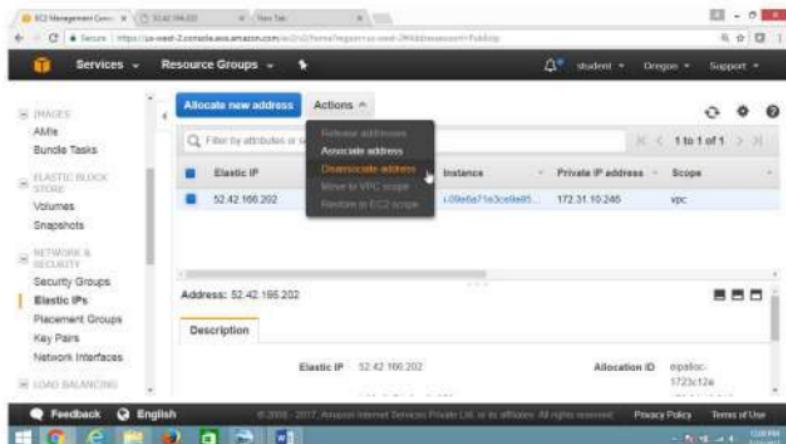
Open the console **EC2 Dashboard**

Expand "Network Security"

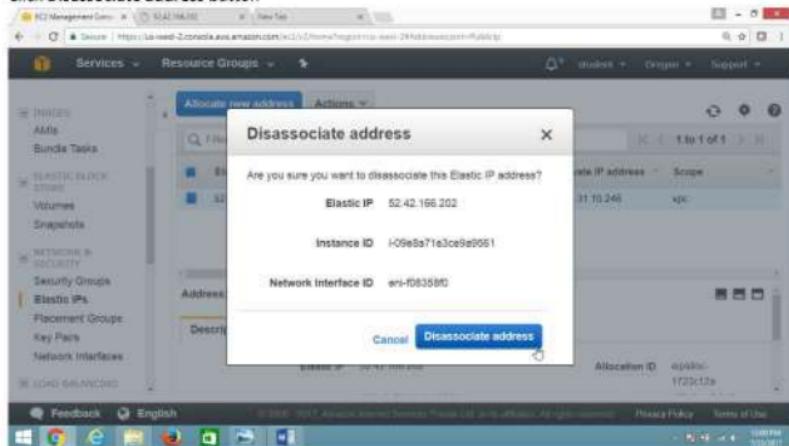
Select **Elastic IP**

Click **Action** button

Select **Disassociate Address**

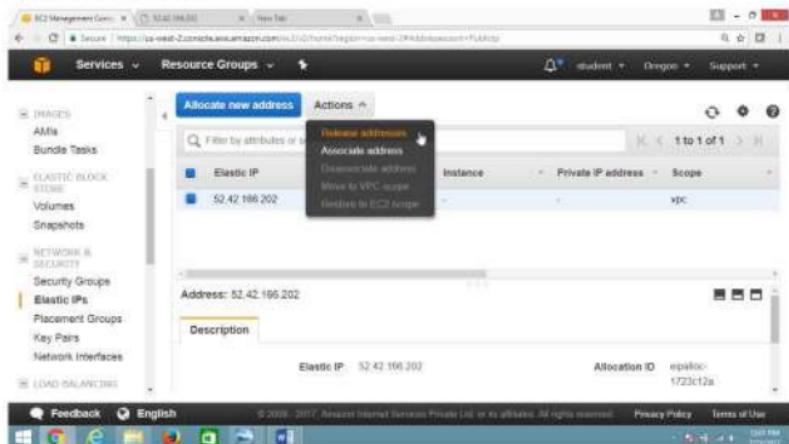


Click Disassociate address button

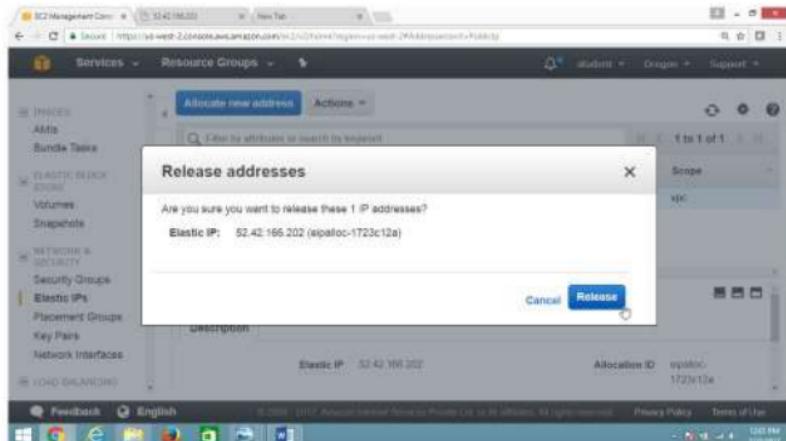


Click Action button

Select Release Addresses



Click Release button



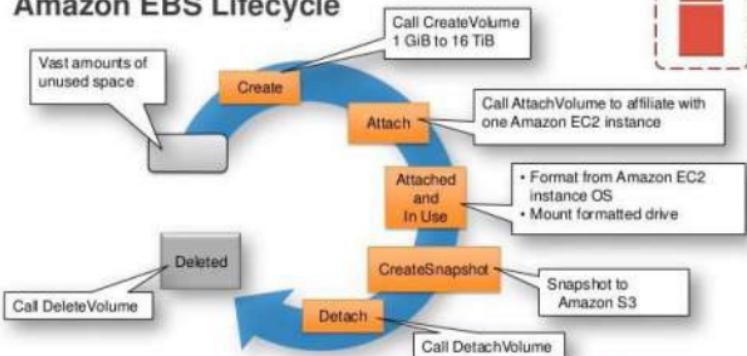
Lab 5: To Manage Elastic Block Store (EBS)

OBJECTIVE

To configure and use AWS EBS service

TOPOLOGY

Amazon EBS Lifecycle



©2014, Amazon Web Services, Inc., or its Affiliates. All rights reserved.



88

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.

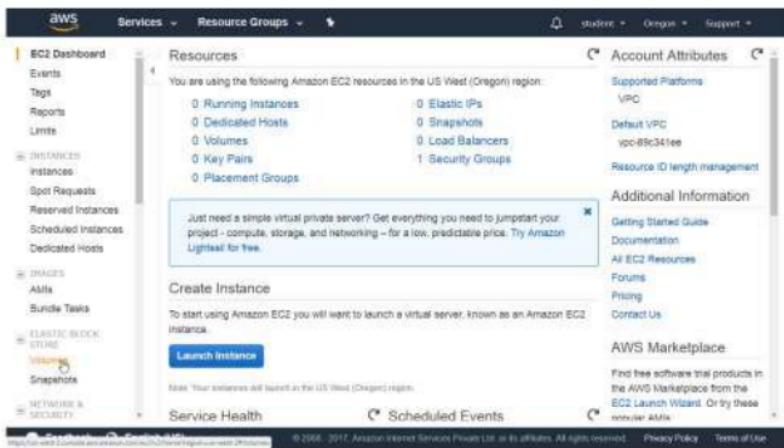
1. To create an EBS volume

Open the Amazon console

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

On the EC2 Dashboard panel

Choose "ELASTIC BLOCK STORE" click on Volumes



Click on Create Volumes button

The screenshot shows the AWS Management Console interface for creating EBS volumes. The left sidebar navigation includes 'Scheduled Instances', 'Dedicated Hosts', 'IMAGES', 'AMIs', 'Bundle Tasks', 'Elastic Block Store' (with 'Volumes' selected), 'Snapshots', 'NETWORK & SECURITY', 'Security Groups', 'Elastic IPs', 'Placement Groups', and 'Key Pairs'. The main content area has a heading 'Create Volume' and a message 'You do not have any EBS volumes in this region.' It also contains the instruction 'Click the Create Volume button to create your first volume.' and a prominent blue 'Create Volume' button. Below this button is a section titled 'Select a volume above' with three small icons.

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 100 / 3000, with a note: '(Baseline of 3 IOPS per GiB with a minimum of 100 IOPS. Available up to 3000 IOPS)'. The 'Availability Zone' is set to 'us-west-2a'. The 'Throughput (MB/s)' is listed as 'Not applicable'. The 'Snapshot ID' dropdown is set to 'Select a snapshot...'. The 'Encryption' checkbox is checked with the option 'Encrypt this volume'. Below the form, there is a 'Tags' section with a note '(Optional) Add tags to your volume.' At the bottom, there are 'Cancel' and 'Create Volume' buttons. A note '(Required)' is placed next to the 'Create Volume' button. The footer includes links for 'Feedback', 'English (US)', 'Privacy Policy', and 'Terms of Use'.

Verify Volume successfully created

Click Close button

The screenshot shows a browser window with the URL <https://us-west-2.console.aws.amazon.com/volumes?region=us-west-2&volumeId=vol-0004000000000000>. The AWS logo is at the top left, followed by 'Services' and 'Resource Groups'. The main content area has a green header bar with a green circular icon and the text 'Volume created successfully'. Below it, a message says 'Volume ID: vol-0004000000000000'. A blue 'Close' button is visible at the bottom right of the message box. At the very bottom of the page, there are links for 'Feedback', 'English (US)', and copyright information.

To Monitoring the State of Your Volumes

Select Volume check state → available

The screenshot shows a browser window with the same URL as the previous screenshot. The AWS logo is at the top left, followed by 'Services' and 'Resource Groups'. The main content area displays a table titled 'Volumes' with one row. The table columns are: Name, Volume ID, Size, Volume Type, IOPS, Snapshot ID, Created, Availability Zone, State, and Alarm Status. The single row shows: 'vol-0004000000000000', 'vol-0004000000000000', '2.0 GiB', 'gp2', '100 / 3000', 'November 10, 2017', 'us-west-2a', 'Available', and 'None'. The 'State' column for this volume is highlighted with a blue background. The bottom of the page shows a search bar with 'Volumes: vol-0004000000000000', navigation links for 'Previous', 'Next', 'Minimise', 'Maximise', and 'Time', and standard footer links for 'Feedback', 'English (US)', and copyright information.

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

The screenshot shows the AWS EC2 Management Console with the 'Create Volume' wizard open. The left sidebar lists services like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundled Tasks, Elastic Block Store, and Volumes. The main area has a title 'Create Volume' with a 'Actions' dropdown. A search bar says 'Filter by tags and/or filters or search by keyword'. Below is a table with columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, and Status. One row is selected: 'Name: vvol-0028894, Volume ID: vol-0028894, Size: 30 GiB, Volume Type: gp2, IOPS: 100 / 3000, Snapshot: MAD-0403.21, Created: November 10, 2017, Availability Zone: us-east-1a, Status: healthy'. At the bottom, there's a 'Volumes' dropdown set to 'vol-0028894' and tabs for Description, Related Changes, Associated, and Tags.

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 Management Console interface for the Elastic Block Store (EBS) service. On the left, there's a navigation sidebar with links like 'Spot Requests', 'Reserved Instances', 'Scheduled Instances', 'Dedicated Hosts', 'PHOTOS', 'AMIs', 'Bundle Tasks', 'ELASTIC BLOCK STORE' (which is currently selected), 'Snapshots', and 'SECURITY & CONNECTIVITY' (including 'Security Groups', 'Elastic IP's', 'Placement Groups', 'Key Pairs', and 'Network Interfaces').

The main content area displays a table of volumes. One volume, 'vol-00001559d0ff0abc' (size 30GB), is selected and highlighted with a blue border. A context menu is open over this volume, with the 'Actions' dropdown expanded. The 'Attach Volume' option is clearly visible and highlighted with a cursor icon.

Below the table, there's a summary bar showing 'Volumes: 3 vol-00001559d0ff0abc (3gb3a)' and tabs for 'Description', 'Status Overview', 'Monitors', and 'Tags'.

At the bottom of the page, there are standard footer links for 'Feedback', 'English (US)', and legal notices including '© 2011 Amazon Internet Services LLC or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Select instance → Winvm1

The screenshot shows the AWS Management Console with the 'Volumes' section selected. A modal dialog box titled 'Attach Volume' is open. Inside the dialog, a volume named 'vol-009a155a42ff3d8c (sgdh1)' is selected from a dropdown. Below it, an instance named 'i-0030c72f1003eab071' is selected. The 'Device' field contains '/dev/sdf'. At the bottom right of the dialog, the 'Attach' button is highlighted with a yellow box.

Click on Attach

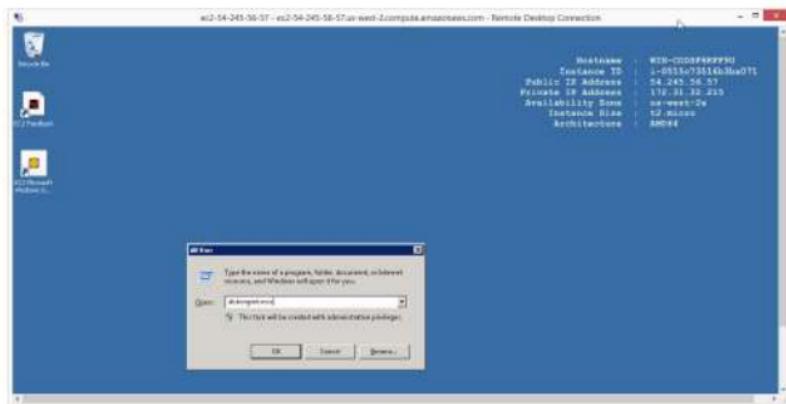
The screenshot shows the AWS Management Console with the 'Volumes' section selected. The 'Attached Volumes' tab is active, showing a list of volumes attached to instances. One volume, 'vol-009a155a42ff3d8c (sgdh1)', is listed, indicating it is now attached to the instance 'i-0030c72f1003eab071'.

Verify the Availability of new volume

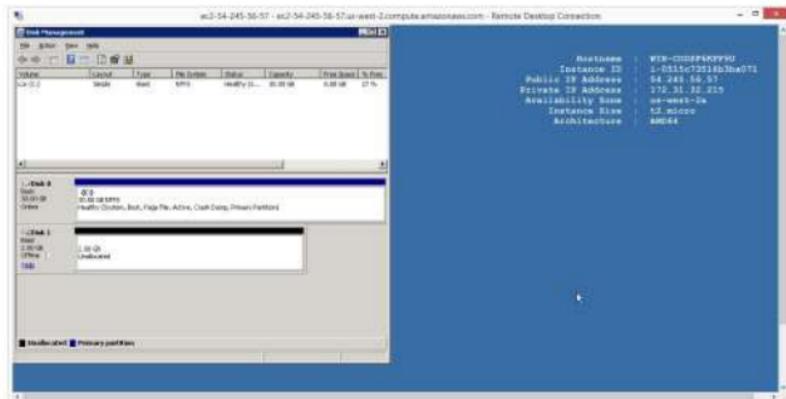
3. To check availability of new drive login to your Windows instance.

Login to windows instance

Run → diskmgmt.msc

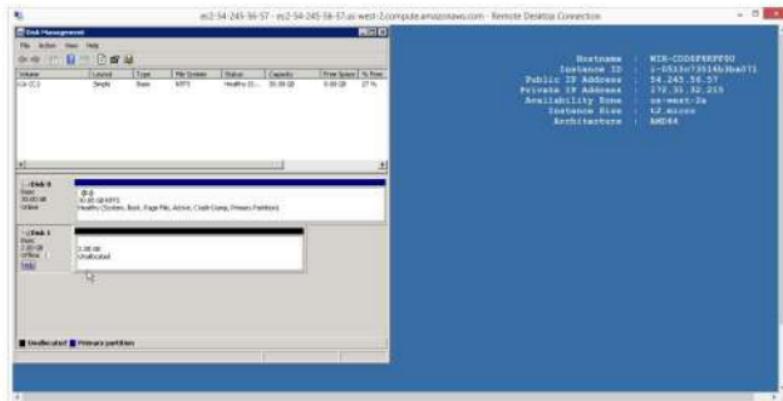


Verifies that 2 GB volume available as unallocated space

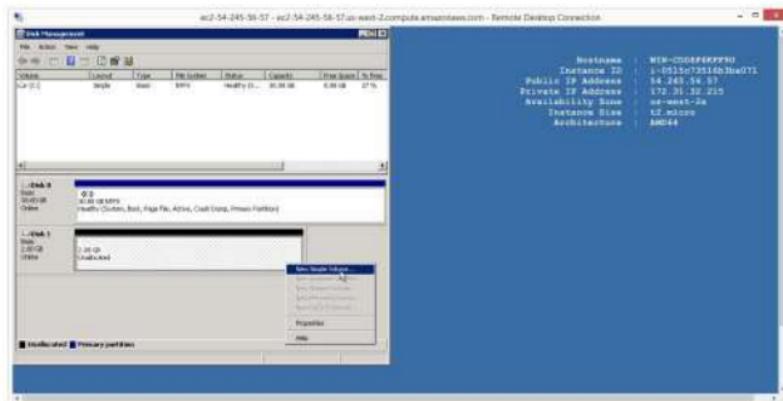


New disk is offline,

So turn it to online by right clicking and select online

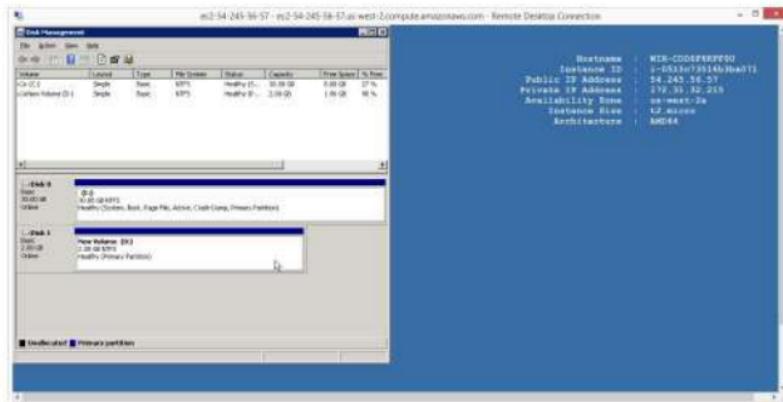


Format the unallocated disk



Verify

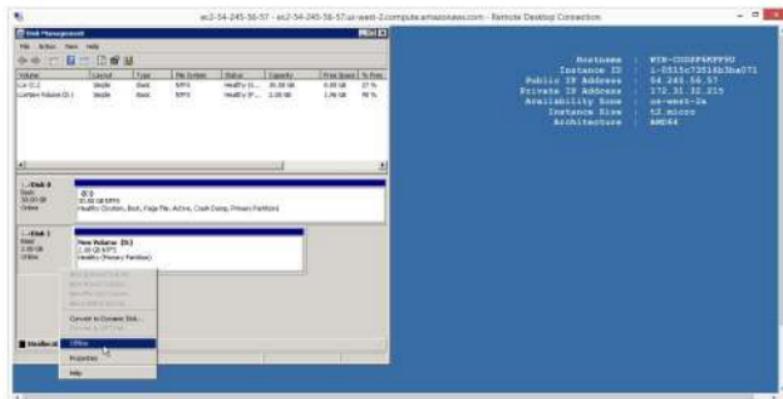
New Volume to 2GB is available to use



4. To Detach the volume

In Windows Select Disk 1

Right click select offline



On the EC2 Dashboard panel

Choose "ELASTIC BLOCK STORE" click on Volumes

Select volume to be detached under Name column.

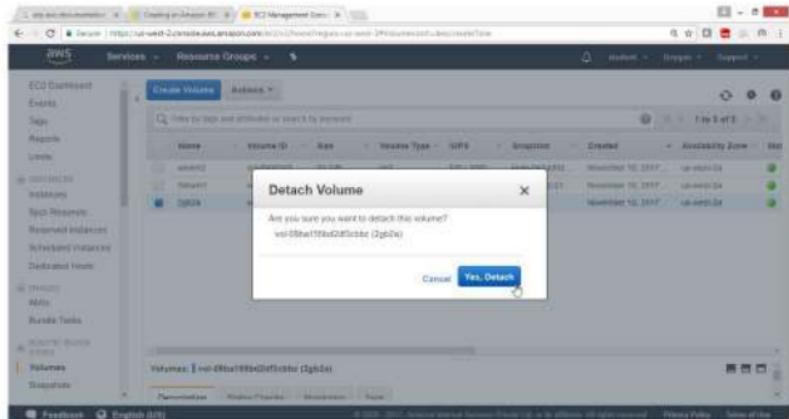
Drop Down Action button

Select "Detach Volume"

The screenshot shows the AWS EC2 Dashboard with the 'Elastic Block Store' section selected. On the left, there's a sidebar with various navigation links like EC2 Dashboard, Events, Tags, Reports, Logs, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Metrics, APIs, and Batch Tasks. The main area displays a table of volumes. One volume, 'vol-08ba195e0df0cbb0', has its 'Name' field selected. A context menu is open over this volume, with the 'Detach Volume' option highlighted. The table columns include Volume Type, IP-Address, Snapshot, Created, and Availability Zone. The volume listed is an 'SSD' type, IP-Address is '192.168.3.11', and it was created on November 10, 2017, in the 'us-west-2a' zone.

Volume Type	IP-Address	Snapshot	Created	Availability Zone
SSD	192.168.3.11	snap-04952f21	November 10, 2017	us-west-2a
SSD	192.168.3.10	None	November 10, 2017	us-west-2a

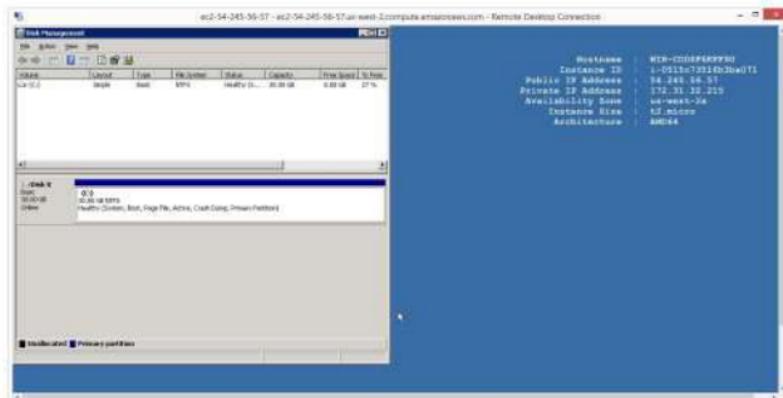
Click on "Yes, Detach" button



Verification

Login to windows instance

Check that D: drive is removed

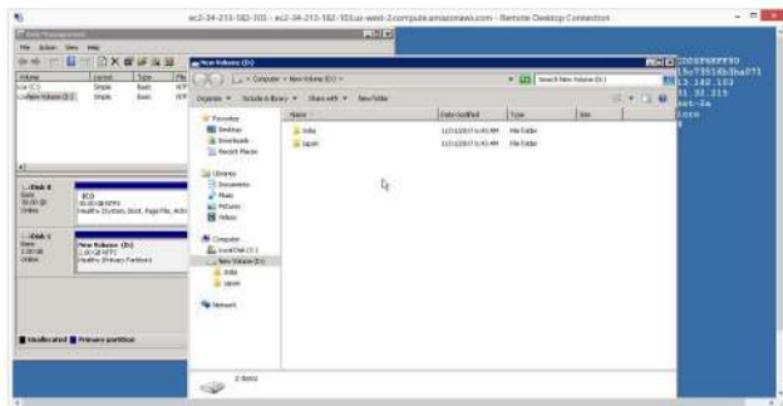


5. To Create Snapshot and Restore EBS volume.

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 Management Console with the EC2 service selected. On the left sidebar, under 'ELASTIC BLOCK STORE', 'Volumes' is selected. In the main content area, a volume named 'vol-08ba155bd2df3cbcc (2gb2a)' is listed. A context menu is open over this volume, with the 'Create Snapshot' option highlighted. The menu also includes options like 'Modify Volume', 'Detach Volume', 'Force Detach Volume', 'Change Auto-Enable IO Setting', and 'Add/Edit Tags'. Below the volume list, there is a 'Volumes' search bar and a table showing three existing snapshots with details like Volume Type, IOPS, Snapshot ID, and Creation Date.

Provide snapshot details

Click Create button

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

Verify that snapshot is created.

Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
KeyPairs
Network Interfaces

Create Snapshot Actions

Owned By Me Filter by tags and attributes or search by keyword

Name	Snapshot ID	Size	Description	Status
snapshot1	snap-0f04d25416	2 GB	snapshot1_des	cd

Snapshot: snap-0f04d25416 | snapshot1

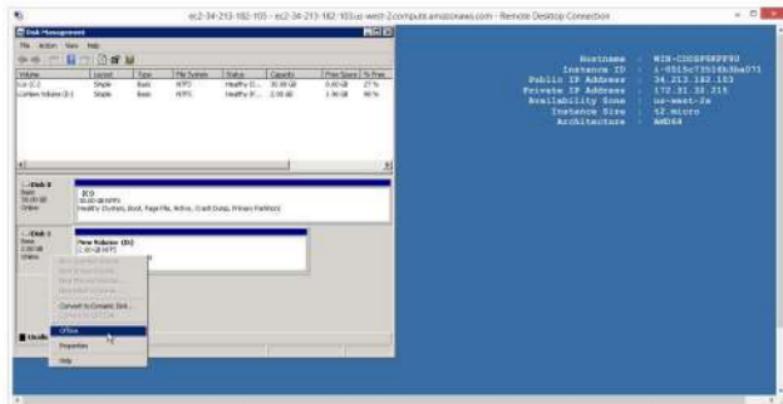
Description Permissions Tags

Documentation XML Terms of Use

6) To Delete the volume.

First select the disk 1 from Disk Management

Right click select offline



On the EC2 Dashboard panel

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

Select volume to be detached under the Name column.

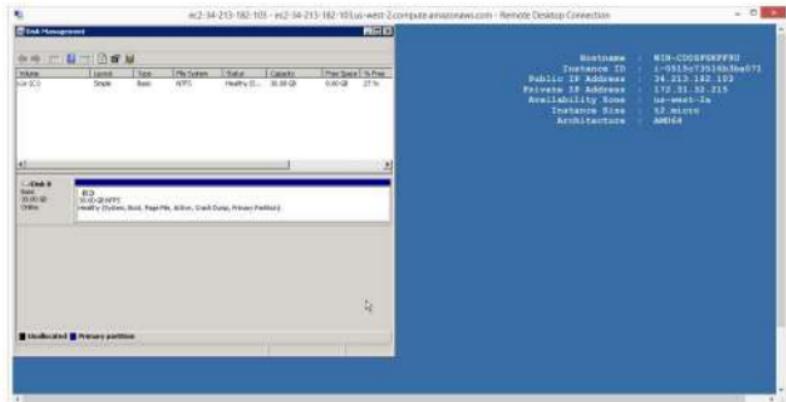
Drop Down Action button, Select “**Delete Volume**”

The screenshot shows the AWS EC2 Management Console. On the left, the navigation pane is visible with sections like Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, Elastic Block Store, Volumes (which is currently selected), and Snapshots. The main area displays a list of volumes. A context menu is open over the third volume in the list, showing options: Modify Volume, Attach Volume, Detach Volume (which is highlighted in red), Force Detach Volume, Create Snapshot, Change Auto-Enable IO Setting, and Add/Edit Tags. The volume list table has columns for Volume Type, IOPS, Snapshot, and Created. The third volume listed is a gp2 type with 100 IOPS, created on November 10, 2017, from a snapshot named snap.04e221...

Volume Type	IOPS	Snapshot	Created
gp2	100 / 3000	snap.04e221...	November 10, 2017
gp2	100 / 3000	snap.04e221...	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. The left sidebar shows 'AWS Services' like Scheduled Instances, Dedicated Hosts, AMIs, Bundl Tasks, Volumes, and Snapshots. Under 'VOLUME & SECURITY', it lists Security Groups, Elastic IPs, Placement Groups, Key Pairs, and Network Interfaces. The main area shows a table of volumes: 'vol-08ba155bd2d3cbcc' (2gb2a) with 100 / 3000 IOPS, 'snap-d4a2c004' (Created November 10, 2017); 'vol-08ba155bd2d3cbcc' (2gb2a) with 100 / 3000 IOPS, 'snap-d4a2c2f1' (Created November 10, 2017); and 'vol-08ba155bd2d3cbcc' (2gb2a) with 100 / 3000 IOPS, 'snap-d4a2c2f1' (Created November 10, 2017). A context menu is open over the first volume, with 'Delete Volume' highlighted. Other options in the menu include 'Attach Volume', 'Detach Volume', 'Create Snapshot', 'Change Auto-Enable IO Setting', and 'Add/Delete Tags'. The status bar at the bottom shows 'Feedback', 'English (US)', and copyright information: © 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

Verify volume is deleted.

EC2 Management Service

Scheduled Instances

Dedicated Hosts

Images

AMIs

Bundle Tasks

Elastic Block Store

Volumes

Snapshots

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Create Volume Actions

Filter by tags and attributes or search by keyword

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
wmin02	vols-0b0703d0	30 GB	gp2	100 / 3000	snap-0x2d004	November 10, 2017
Wmin01	vols-04b2950a	30 GB	gp2	100 / 3000	snap-04e2c21	November 10, 2017

Select a volume above

Feedback English (US) © 2006–2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy 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, there's a navigation sidebar with links like 'Scheduled Instances', 'Dedicated Hosts', 'IMAGES', 'AMIs', 'Bundle Tasks', 'ELASTIC BLOCK STORE' (which is expanded to show 'Volumes' and 'Snapshots'), 'NETWORK & SECURITY', 'Security Groups', 'Basic IPs', 'Placement Groups', 'Key Pairs', and 'Network Interfaces'. The 'Snapshots' link is highlighted with a yellow bar. In the main content area, a 'Create Snapshot' button is visible. A context menu is open over a specific snapshot entry, with 'Actions' expanded to show options: 'Delete', 'Create Volume' (which is highlighted with a yellow arrow), 'Create Image', 'Copy', 'Modify Permissions', and 'Add/Edit Tags'. Below the menu, the snapshot details are shown: 'Snapshot: snap-0ff148c354563cba6 (snapvoil)', 'Description: ', 'Permissions: ', and 'Tags: '. At the bottom of the page, there are footer links for 'Feedback', 'English (US)', and legal notices.

Accept the default 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-08f48c254953d0 (snapv01)
- 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, tunable to 3000 IOPS)
- Availability Zone:** us-west-2a
- Throughput (Mbps):** Not applicable
- Encryption:** Not Encrypted
- Tags:** Add tags to your volume

* Required

Create Volume

Verify Volume is created

The screenshot shows the 'Volumes' section in the AWS Management Console. The table lists three volumes:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
wlmv2	vol-0c350e0c...	20 GiB	gp2	100 / 3000	snap-08f48c03...	November 11, 2017
wlmv3	vol-06050d63...	30 GiB	gp2	100 / 3000	snap-0a2e0003...	November 10, 2017
wlmv1	vol-062080a0...	30 GiB	gp2	100 / 3000	snap-04e2c21...	November 10, 2017

Volumes: vol-0c350e0c73f0a3801

7) To expanding the size of EBS volume.

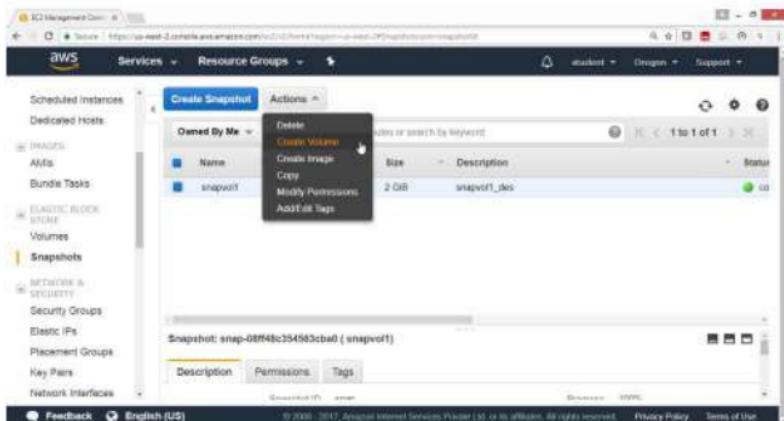
To expand EBS volume first take **snapshot**, now select the snapshot

On the **EC2 Dashboard** panel

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

Drop Down Action button

Select **Create Volume**



Give the required size → 4 GB

Check the right Availability Zone

click **Create Volume** button

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

- Snapshot ID:** snap-08f48c154663cba0 (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, tunable to 3000 IOPS)
- Availability Zone:** us-west-2a
- Throughput (MiB/s):** Not applicable
- Encryption:** Not Encrypted

At the bottom, there is a 'Tags' section with a link to 'Add tags to your volume'. The 'Create Volume' button is highlighted in blue.

Verify that 4 GB is created

The screenshot shows the 'Volumes' section in the AWS Management Console. A search bar at the top has 'vol-034d709' entered. The table lists three volumes:

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created
wst034d709	vol-034d709	4 GiB	gp2	100 / 2000	snap-08f48c154663cba0	November 11, 2017
wmt034d709	vol-034d709c	2 GiB	gp2	100 / 2000	snap-08f48c154663cba0	November 11, 2017
Wmt034d709	vol-034d709e	30 GiB	gp2	100 / 2000	snap-0a7600d4	November 10, 2017
Wmt034d709	vol-034d709f	30 GiB	gp2	100 / 2000	snap-0462c21...	November 10, 2017

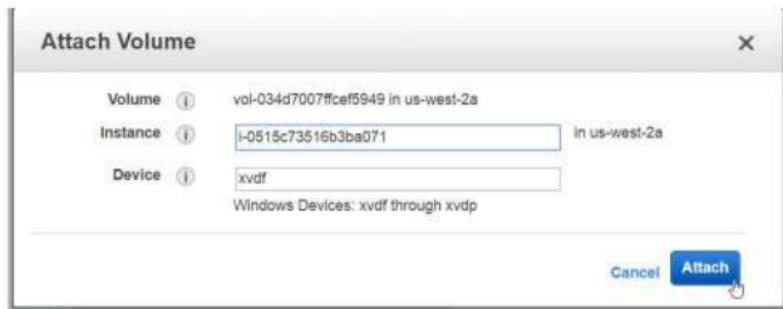
Now attach this expanded volume to your instance.

The screenshot shows the AWS Management Console with the EC2 service selected. On the left, there's a navigation pane with sections like Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, Elastic Block Store, Volumes (which is selected), and Snapshots. The main area shows a table of volumes. A context menu is open over a volume named 'winvm1'. The menu options are: Create Volume, Actions, Modify Volume, Delete Volume, Attach Volume (which is highlighted with a cursor), Detach Volume, Force Detach Volume, Create Snapshot, Change Auto-Enable IO Setting, and Add/Delete Tags. Below the table, there's a search bar with 'Volumes: vol-034d7007ffce5949' and tabs for Description, Status Checks, Monitoring, and Tests. At the bottom, there are links for Feedback, English (US), and a copyright notice from 2018.

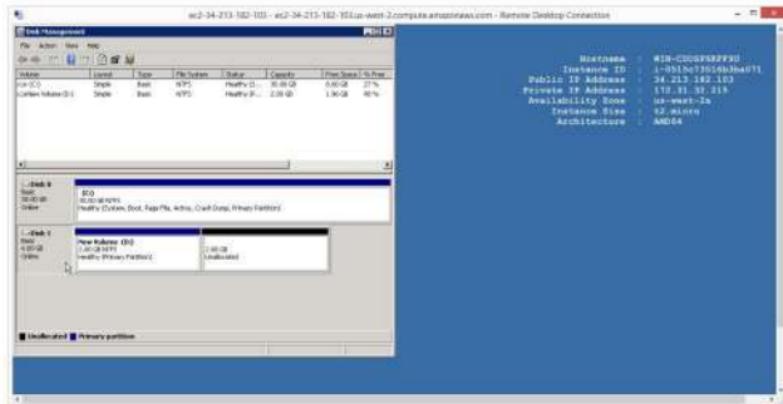
Select instance

The screenshot shows the 'Attach Volume' dialog box. It has fields for 'Volume' (set to 'vol-034d7007ffce5949 in us-west-2a'), 'Instance' (with a dropdown placeholder 'Search Instance ID or Name tag' and a filter 'in us-west-2a'), and 'Device' (listing two instances: 'i-0515c73516b3ba071 (Winvm1) (running)' and 'i-04bd24ef0affeed12 (winvm2) (running)'). The second instance is highlighted with a cursor. At the bottom right are 'Cancel' and 'Attach' buttons.

Click Attach button

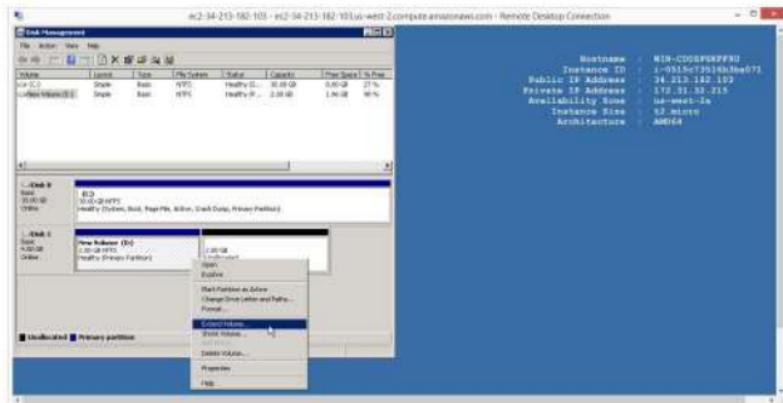


Verify 4 GB drive is available

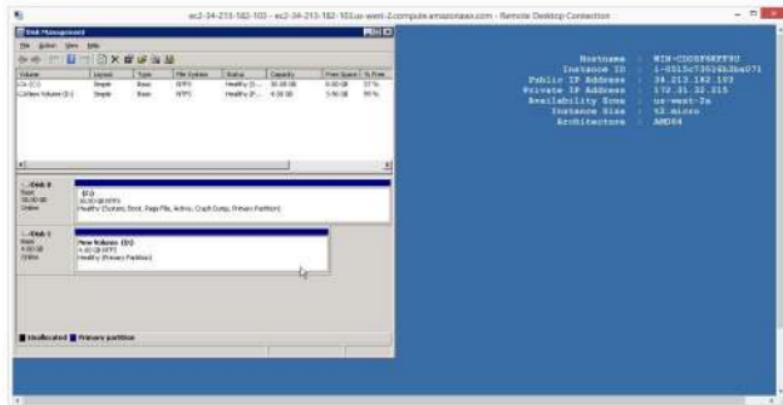


Now with respect to Windows operating system

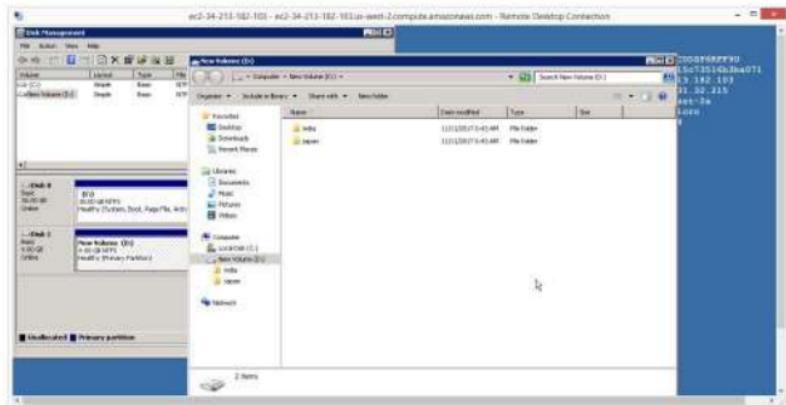
Right click on D drive extend your volume to your desired size



Verified that 4 GB volume available

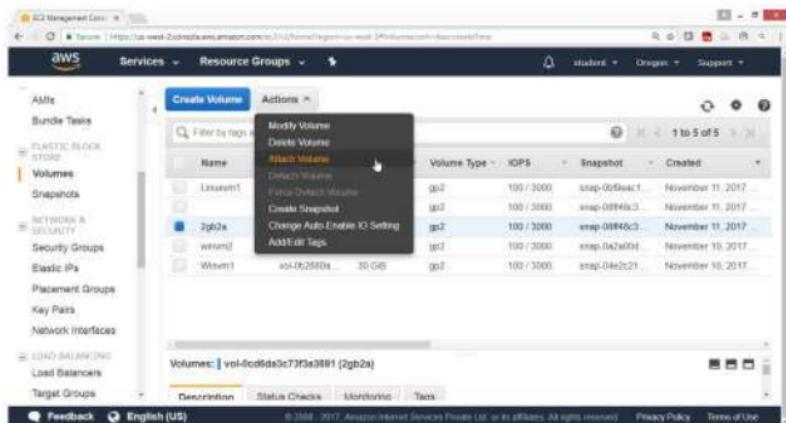


Verified that D drive contains two folders that was there in 2B drive earlier.

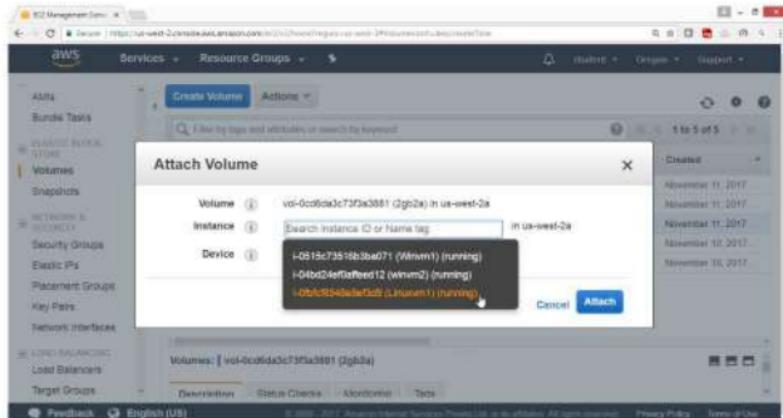


Similarly check volume in linux instance

From Action select **Attach volume**



Select Linux instance



Now connect to Linux instance

```
[2017-11-11 12:58:46] /drives/e/awskeys
[shaikh.pc_ms] > 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 49.206.283.114
```

Amazon Linux AMI

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

To verify

Switch to root user and run fdisk -l

```
$ sudo su
```

To check list of drives and partitions

```
# fdisk -l
```

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

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

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

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

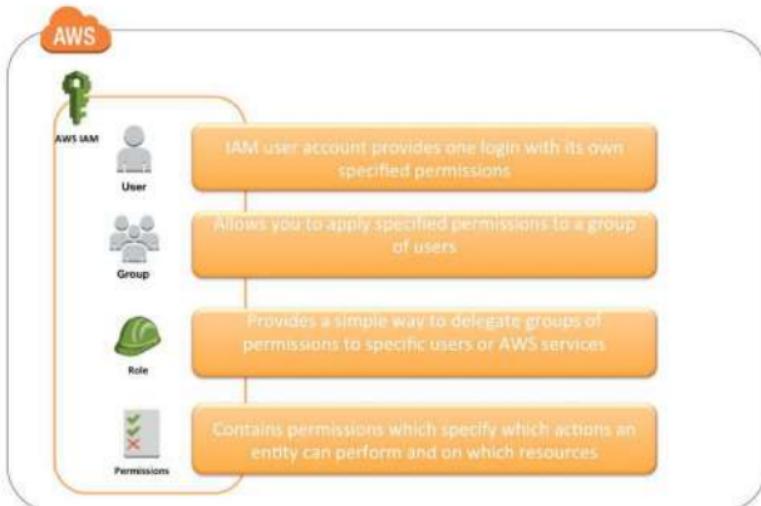
Lab 6: To Manage IAM Users, Groups and Policies

OBJECTIVE

To configure and use AWS IAM Service.

TOPOLOGY

AWS IAM Identities



PRE-REQUISITES

User should have AWS root account.

To configure IAM with following task.

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

Create IAM groups.

Add users to a group.

Add policies to Groups and Users.

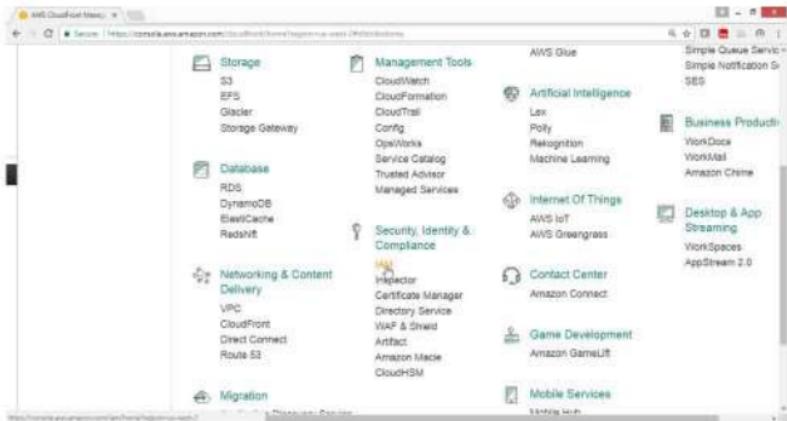
Create your own policies.

Users Login to sign-in page.

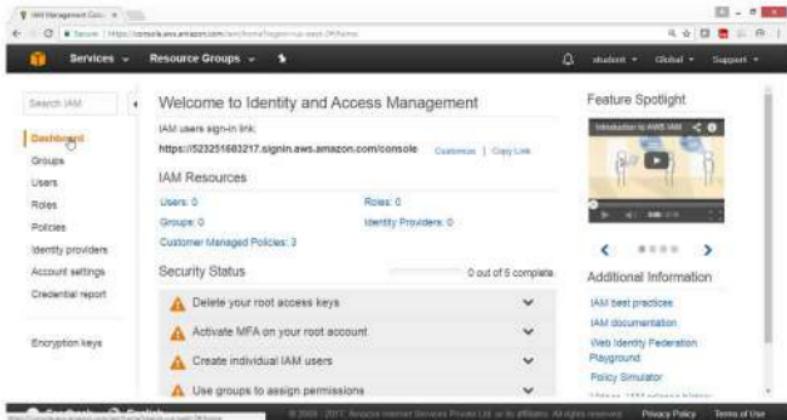
Deleting users and groups.

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

Click on IAM service



IAM Dashboard panel available



2) To Manage Groups and applying policies

From IAM dashboard, select **Groups**

Click on **Create New Group** button

The screenshot shows the AWS IAM Groups page. On the left, there's a sidebar with links like Dashboard, Groups (which is selected and highlighted in orange), Users, Roles, Policies, Identity providers, Account settings, and Credential report. Below that is an Encryption keys section. The main content area has a search bar and two buttons: 'Create New Group' (highlighted with a red circle) and 'Group Actions'. A table follows, with columns for Group Name, Users, Inline Policy, and Creation Time. A message at the bottom says 'No records found'. At the bottom of the page, there are links for Feedback, English, Privacy Policy, and Terms of Use.

Give Group Name → EC2admingroup

Click on **Next Step** button

The screenshot shows the AWS Management Console interface for creating a new IAM group. On the left, a sidebar displays the 'Create New Group Wizard' with three steps: Step 1 - Group Name, Step 2 - Attach Policy, and Step 3 - Review. The main area is titled 'Set Group Name' with the sub-instruction 'Specify a group name. Group names can be edited any time.' A text input field contains the value 'EC2admingroup'. Below the input field, a tooltip provides the definition: 'Control access to your Amazon S3 buckets and objects'. At the bottom right of the main form, there are 'Cancel' and 'Next Step' buttons, with 'Next Step' being highlighted.

In Filter type → EC2f

Select check box for **AmazonEC2FullAccess**

Click on **Next Step** button

The screenshot shows the 'Attach Policy' step of the 'Create New Group Wizard'. A filter has been applied to show only EC2 policies. One policy, 'AmazonEC2FullAccess', is selected and highlighted with a yellow icon. The table lists two policies:

Policy Name	Attached Entities	Creation Time	Edited Time
AmazonEC2FullAccess	0	2015-02-07 00:10 UTC...	2015-02-07 00:10 ...
AmazonEC2FullAccess...	0	2017-06-17 16:33 UTC...	2017-06-17 16:33 ...

At the bottom right, there are 'Cancel', 'Previous', and 'Next Step' buttons. The 'Next Step' button is highlighted with a blue border.

Click on **Create Group**

The screenshot shows the 'Review' step of the 'Create New Group Wizard'. It displays the information entered in the previous steps:

- Group Name:** EC2adminGroup
- Policies:** AmazonEC2FullAccess

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

Verify

Group EC2admingrp got created with AmazonEC2FullAccess policy

Creation Time: 2017-08-15 19:35 UTC+0530

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Policy Name Actions

AmazonEC2FullAccess Show Policy | Detach Policy | Simulate Policy

Now again create Another Group

Click on Create Group button

Group Name	Users	Inline Policy	Creation Time
EC2admingroup	0	AmazonEC2FullAccess	2017-08-15 18:35 UTC+0630

To create a group With S3FullAccess

The screenshot shows the 'Create New Group Wizard' in the AWS Management Console. The current step is 'Step 1 : Group Name'. The 'Group Name' field is filled with 's3admingrp1'. Below the field, there is a note: 'Specify a group name. Group names can be edited any time.' and examples: 'Example: Developers in Philadelphia' and 'Maximum: 128 characters'. At the bottom right, there are 'Cancel' and 'Next Step' buttons, with 'Next Step' being highlighted.

In Filter type → S3f

Select check box for **AmazonS3FullAccess**

Click on **Next Step** button

The screenshot shows the 'Attach Policy' step of the wizard. The 'Filter' dropdown is set to 'Policy Type: s3f'. There are two results listed: 'AmazonS3FullAccess' and 'AmazonS3FullAccess...'. The first row has a checked checkbox next to it. At the bottom right, there are 'Cancel', 'Previous', and 'Next Step' buttons, with 'Next Step' being highlighted.

Click on Create Group button

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	S3admingrp	Edit Group Name
Policies	arn:aws:iam::aws-policy:AmazonS3FullAccess	Edit Policies

Create Group

Verify EC2admingroup & S3admingrp groups got created

Search IAM

Groups

Users

Roles

Policy

Identity providers

Account settings

Credential report

Encryption keys

Create New Group **Group Actions**

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

Showing 2 results

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

Verify S3 policy is attached

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

- Creation Time:** 2017-08-15 15:42 UTC+0530
- Permissions Tab:** Shows 'Managed Policies' and 'Inline Policies' sections.
- Managed Policies:** A table lists the 'AmazonS3FullAccess' policy, which was attached via the 'Attach Policy' button.
- Actions:** For the policy, there are links to 'Show Policy', 'Detach Policy', and 'Simulate Policy'.

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 top navigation bar includes 'Services', 'Resource Groups', 'Actions', 'Regions', 'Global', and 'Support'. On the left, a sidebar menu lists 'Dashboard', 'Groups', 'Users' (which is selected and highlighted in yellow), 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Credential report'. Below the sidebar is an 'Encryption keys' section. The main content area has a header with 'Add user' and 'Delete user' buttons. A search bar at the top says 'Find users by username or access key'. Below it, there are two filter dropdowns: 'User name' and 'Groups'. A message states 'There are no IAM users.' with a 'Learn more' link. At the bottom of the page, there are links for 'AWS Support', 'AWS Marketplace', 'AWS Documentation', 'AWS Privacy Policy', and 'AWS Terms of Use'.

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. Step 1, 'Set user details', is active. A progress bar at the top indicates four steps: 1. Details (blue), 2. Permissions (grey), 3. Review (grey), and 4. Complete (grey). The 'User name*' field contains 'tom'. Below it is a radio button for 'Add another user'. The 'Select AWS access type' section follows, with a note about access keys and passwords. Under 'Access type*', two options are listed: 'Programmatic access' (unchecked) and 'AWS Management Console access' (checked). The checked option is described as enabling a password for sign-in to the AWS Management Console.

For Console password → *****

Click on Next Permissions button

The screenshot shows the 'AWS Management Console' interface for creating a new IAM user. The 'Services' and 'Resource Groups' tabs are visible at the top. Under 'User permissions details', the 'AWS Management Console access' checkbox is checked. Below it, the 'Console password' section is set to 'Custom password' with a visible password field. A 'Require password reset' checkbox is unchecked. At the bottom right, there are 'Cancel', 'Next: Permissions', and 'Create User' buttons. The status bar at the bottom includes 'Feedback', 'English', '© 2006 - 2011, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Under Group column

Select EC2adminingroup

Click on Next Review

The screenshot shows the 'AWS Management Console' interface for creating a new IAM user. The 'Services' and 'Resource Groups' tabs are visible at the top. Under 'Attached policies', the 'AmazonEC2ReadOnlyAccess' policy is selected. At the bottom right, there are 'Cancel', 'Previous', and 'Next: Review' buttons. The status bar at the bottom includes 'Feedback', 'English', '© 2006 - 2011, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Verify users detail

Click on **Create user** button

The screenshot shows the 'Create New User' step in the AWS Management Console. The 'User details' section includes fields for 'User name' (tirth), 'AWS access type' (AWS Management Console access - with a password), 'Console password type' (Custom), and 'Require password reset' (No). The 'Permissions summary' section shows the user will be added to the 'EC2Admins group'. At the bottom right are 'Cancel', 'Previous', and a blue 'Create user' button.

Down the .csv file

The screenshot shows 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, there's a 'Download CSV' button and a table showing the created user 'tirth'. The table has columns for 'User', 'Details', 'Permissions', 'Review', and 'Complete'. A 'Close' button is at the bottom right.

Click on close button

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with tabs like 'Services', 'Resource Groups', and 'AWS Lambda'. Below the navigation bar, there are four buttons: 'Details', 'Permissions', 'Review', and 'Complete'. A prominent green 'Success' message box is displayed, stating: 'You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.' It also mentions that 'Users with AWS Management Console access can sign-in at: https://[REDACTED].signin.aws.amazon.com/console'. Below this message, there's a 'Download.csv' button. The main content area is titled 'User' and shows a single entry: 'John'. To the right of this entry are two buttons: 'Email login instructions' and 'Send email'. At the bottom right of the user list area is a 'Close' button. At the very bottom of the page, there are links for 'Feedback', 'English', and other AWS policies.

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 shows a table with one row, where the 'User name' is 'john' and the 'Groups' assigned are 'S3admingroup'. A modal dialog box titled 'Add user' is open over the table, containing fields for 'User name' (set to 'john') and 'Groups' (set to 'S3admingroup'). Below the table, the URL in the browser bar is <https://console.aws.amazon.com/iam/home?region=us-east-1#users>.

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

Drag down

User name* john

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 Web Services, Inc. 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 Web Services, Inc. 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 left sidebar, under 'Resource Groups', the 'S3admingrp' group is selected. On the right, the 'Attached policies' section displays two policies: 'AmazonS3FullAccess' and 'AmazonS3FullAccess'. At the bottom of the page, there are 'Cancel', 'Previous', and 'Next: Review' buttons. 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. It includes a 'User details' section with fields for User Name (John), AWS access type (AWS Management Console access - with a password), Console password type (Custom), and Require password reset (No). Below this is a 'Permissions summary' section indicating the user will be added to the 'S3admingrp' group. At the bottom, there are 'Cancel', 'Previous', and 'Create user' buttons. The 'Create user' button is highlighted with a blue border.

Download .csv file

Click on **Close** button

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/console/home#/user-add-step-2?&userArn=arn:aws:iam::123456789012:root&groupArn=arn:aws:iam::123456789012:group/test>. The page title is "Add user". A progress bar at the top shows four steps: 1. Details (grey), 2. Permissions (grey), 3. Review (grey), and 4. Complete (blue). Step 4 is highlighted with a blue circle. Below the progress bar, a green success message box contains the text: "Success: You successfully created the user 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 "Users with AWS Management Console access can sign-in at: <https://12345678901217.signin.aws.amazon.com/console>". Below the message box, there is a "Download .csv" link, a "User" table with one row for "john", and a "Email login info" section. At the bottom right of the main content area is a "Close" button. The footer of the page includes links for "Feedback", "English", "© 2018 - 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved.", "Privacy Policy", and "Terms of Use".

Scenario 3)

Add a user individual user sai without joining to any group

Attach EC2FullAccess and S3FullAccess policy

Select User

Click on Add user button

The screenshot shows the AWS IAM Management Console. The left sidebar navigation bar includes 'Dashboard', 'Groups', 'Users' (which is selected), 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Credential report'. Below the sidebar is an 'Encryption keys' section. The main content area has a search bar at the top labeled 'Find users by username or access key'. Below the search bar is a table titled 'Showing 2 results'. The table has columns: 'User name', 'Groups', 'Access key age', 'Password age', 'Last activity', and 'MFA'. Two users are listed: 'sai' (Groups: EC2Testinggroup) and 'sai' (Groups: EC2Testinggroup). At the bottom of the page, there is a footer with links to 'AWS Terms of Use', 'AWS Privacy Policy', and 'AWS Customer Agreement'.

User name	Groups	Access key age	Password age	Last activity	MFA
sai	EC2Testinggroup	None	Today	None	Not enabled
sai	EC2Testinggroup	None	Today	None	Not enabled

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

Drag Down

User name* sal

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

Next Step

Click on Next permission button

AWS Management Console access

Custom 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**

Click on Attach existing policies directly box

The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iamv2/home?region=us-east-1#/users/sai/edit>. The page title is "Add user". The top navigation bar includes "Services", "Resource Groups", "Student", "Global", and "Support". Below the title, the steps are numbered 1 (Details), 2 (Permissions), 3 (Review), and 4 (Complete). The "Permissions" step is active. A sub-header says "Set permissions for sai". Three options are shown: "Add user to group" (with a people icon), "Copy permissions from existing user" (with a cloud and person icon), and "Attach existing policies directly" (with a document icon). A note below says: "Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more". At the bottom, there are "Feedback", "English", and links to "Privacy Policy" and "Terms of Use".

In Filter type search for ec2

Select AmazonEC2FullAccess check box

The screenshot shows the "Attach existing policies directly" interface. The URL is <https://console.aws.amazon.com/iamv2/home?region=us-east-1#/users/sai/policies/edit>. The top navigation bar and steps are identical to the previous screenshot. The main area has three tabs: "existing user", "Create policy", and "Refresh". A search bar contains "ec2". A note says: "Attach one or more existing policies directly to the user or create a new policy. Learn more". A "Create policy" button is available. A table lists policies: "AmazonEC2FullAccess" (AWS managed) and "AmazonEC2FullAccess" (Customer managed). Both rows have a checkbox next to them. The table has columns: Policy name, Type, Attachments, and Description. The "Showing 2 results" message is at the top right of the table. At the bottom, there are "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. In the top navigation bar, 'Services' and 'Resource Groups' are selected. Below the navigation, there's a table with columns: Policy name, Type, Attachments, and Description. One row is selected, showing 'AmazonS3FullAccess' (AWS managed) and 'AmazonS3FullAccess-20170119' (Customer managed). The 'Attachments' column shows a blue link labeled 'AmazonS3FullAccess-20170119'. The 'Description' column contains a brief explanation of the policy. At the bottom of the page, there are 'Cancel', 'Previous', and 'Next: Review' buttons. The 'Next: Review' button is highlighted with a blue border.

Verify users detail

Click on Create user button

The screenshot shows the 'Create user' step in the AWS IAM Management Console. It starts with a 'User details' section where 'User name' is set to 'val', 'AWS access type' is 'AWS Management Console account - with a password', 'Console password type' is 'Custom', and 'Require password reset' is 'No'. Below this is a 'Permissions summary' section which lists the policies attached to the user: 'AmazonEC2FullAccess' and 'AmazonS3FullAccess'. At the bottom of the page, there are 'Cancel', 'Previous', and 'Create user' buttons. The 'Create user' button is highlighted with a blue border.

Download .csv file

Click on **Close** button

The screenshot shows the AWS Management Console interface for creating a new user. At the top, there's a navigation bar with tabs like 'Services', 'Resource Groups', and 'AWS Lambda'. Below the navigation bar, a progress bar indicates four steps: 'Details' (step 1), 'Permissions' (step 2), 'Review' (step 3), and 'Complete' (step 4). Step 4 is highlighted with a blue circle. The main content area has a green success message box that says: 'Success: You successfully created the user 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 includes a link for users with AWS Management Console access. Below the message box, there's a table with one row showing a user named 'User'. The table columns are 'User' and 'Email (login info)'. There are download and delete icons next to the user name. At the bottom of the page, there are links for 'Feedback', 'English', and 'Close'.

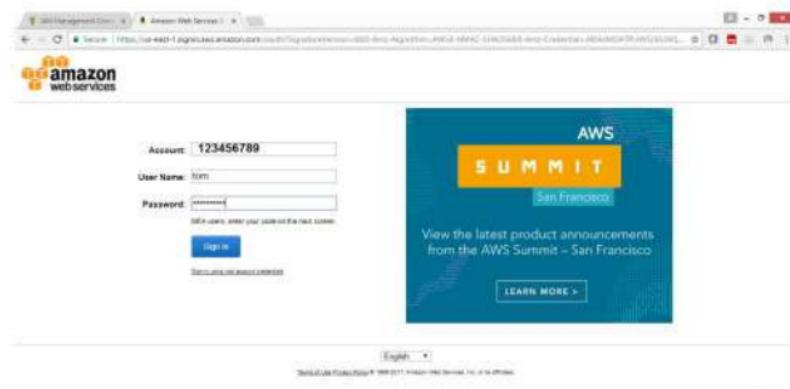
To verify whether users can access particular Service

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 menu open. The 'S3' icon is highlighted, indicating it is the selected service. Other services listed include IAM, CloudFront, VPC, EC2, Compute (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 allows users to find specific services or features.

Verification

Error Access Denied

The screenshot shows the AWS Management Console for the S3 service. The 'Create bucket' button is visible. Below it, an error message box displays the text 'Error' and 'Access Denied'. Navigation links for 'Discover new classes', 'Backups', and 'Regions' are also present.

Now select EC2 service

The screenshot shows the AWS Management Console homepage. On the left, there's a sidebar with links for S3, Console Home, IAM, CloudFront, VPC, and EC2. The main area is titled "Find a service by name or feature (for example: EC2, S3 or VM instances)" and lists several service categories with their respective icons and service names:

- Compute:** EC2 Container Service, 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.
- Business Products:** WorkDocs, WorkMail, Amazon Chime.
- Internet Of Things:** AWS IoT.
- Desktop & App:** (Icon shown).

Verification

User tom can access EC2 service.

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with links for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (with sub-links for Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), IMAGES (with sub-links for AMIs), and Feedback. The main area has tabs for Services and Resource Groups, with the Resource Groups tab selected. It displays the following information:

- Resources:** You are using the following Amazon EC2 resources in the US West (Oregon) region:
 - 1 Running Instances
 - 0 Dedicated Hosts
 - 1 Volumes
 - 3 Key Pairs
 - 0 Placement Groups
 - 0 Elastic IPs
 - 1 Snapshots
 - 0 Load Balancers
 - 6 Security Groups
- Account Attributes:**
 - Supported Platforms: VPC
 - Default VPC: vpc-8fc341ee
 - Resource ID length management: (link)
- Create Instance:** 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

Similarly check for user john

To Delete users and groups

From IAM dashboard, select **Users**

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

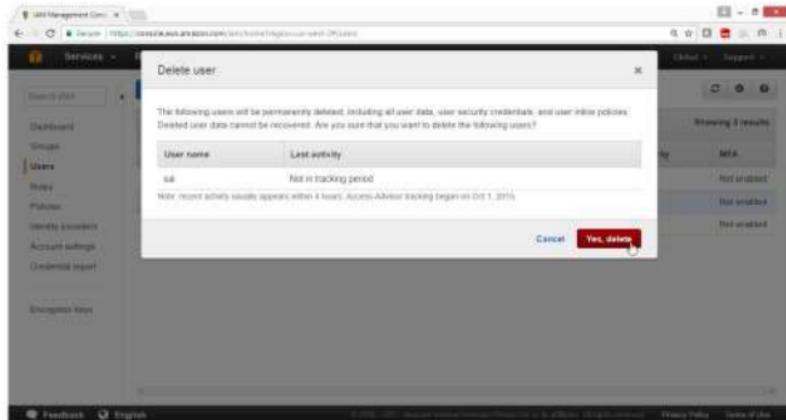
Click on **Delete Users** button

The screenshot shows the AWS IAM service's 'Users' page. On the left, there's a sidebar with navigation links: Dashboard, Groups, Users (which is selected and highlighted in yellow), Roles, Policies, Identity providers, Account settings, and Credential report. Below that is an 'Encryption keys' section. The main content area has a search bar at the top labeled 'Search User'. Underneath it, there are two buttons: 'Add user' (blue) and 'Delete user' (red). A search input field says 'Find users by username or access key'. Below that is a table with the following data:

User name	Groups	Access key age	Passwd age	Last activity	MFA
jdk	Ec2Testinggroup	None	Today	None	Not enabled
sri	None	None	Today	None	Not enabled
sru	EC2Testinggroup	None	Today	Today	Not enabled

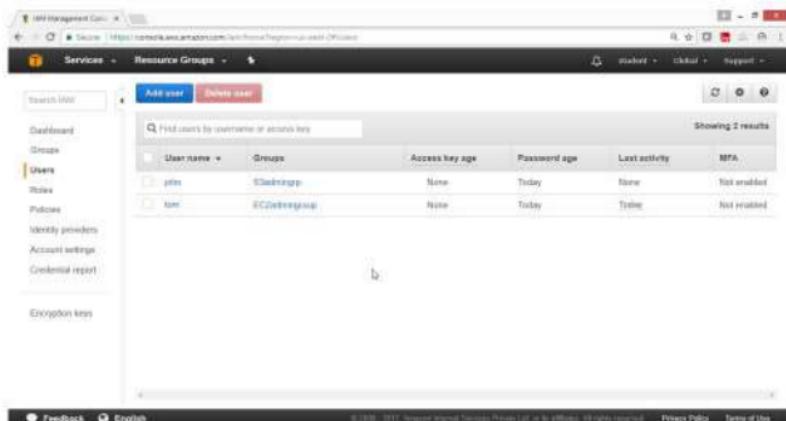
At the bottom of the page, there are links for Feedback, English, and footer text: © 2006–2017 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use.

Click on Yes, delete button



Verification

User sai is deleted



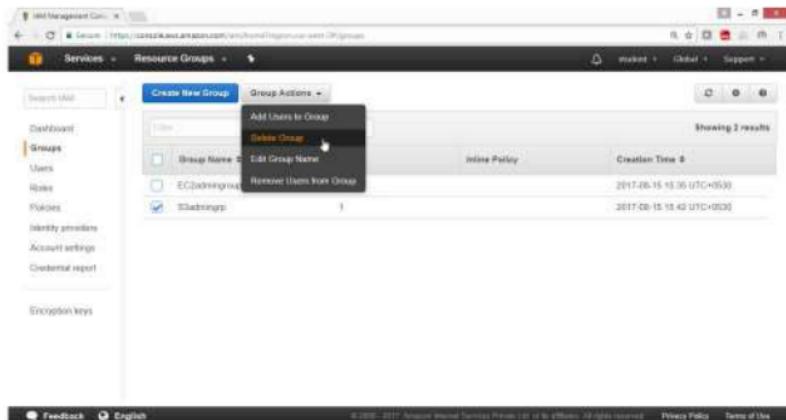
To Deleting Groups

From IAM Dashboard

Select the **Groups**

Drop down **Group Action** button

Select **Delete Group**



Click Yes, Delete button

The screenshot shows the AWS IAM Groups page. A modal dialog box is open, asking for confirmation to delete a group named 'S3SharingGroup'. The dialog states: '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?' It lists one group, 'S3SharingGroup'. At the bottom of the dialog are 'Cancel' and 'Yes, Delete' buttons.

Verification

Group is deleted

The screenshot shows the AWS IAM Groups page after the group 'S3SharingGroup' has been deleted. The table now displays only one group, 'EC2SharingGroup', which was previously listed as being deleted. The table columns are 'Group Name', 'Users', 'Inline Policy', and 'Creation Time'.

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 User Management console. On the left, there is a sidebar with navigation links: Dashboard, Groups, Users (which is selected and highlighted in orange), Roles, Policies, Identity providers, Account settings, and Credential report. The main area has tabs for 'Add user' (blue) and 'Delete user' (red). A search bar at the top says 'Find users by username or access key'. Below it is a table with columns: 'User name' (dropdown), 'Groups', 'Access key age', and 'Password age'. There are two entries: 'john' (S3admingrp, None, Today) and 'tom' (EC2admingroup, None, Today). The 'tom' row is currently selected, indicated by a blue background.

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

Click on Security credentials

Screenshot of the AWS IAM User Summary page for user 'tom'. The 'Security credentials' tab is selected. The page displays the following information:

Console password	Enabled	Manage password
Console login link	https://signin.aws.amazon.com/console	
Last login	2017-08-15 22:09 UTC+0530	
Assigned MFA device	No	
Signing certificates	None	

Click on pen sign for "Assigned MFS device"

Screenshot of the AWS IAM User Summary page for user 'tom'. The 'Security credentials' tab is selected. The page displays the following information:

Console password	Enabled	Manage password
Console login link	https://signin.aws.amazon.com/console	
Last login	2017-08-15 22:09 UTC+0530	
Assigned MFA device	No	
Signing certificates	None	

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

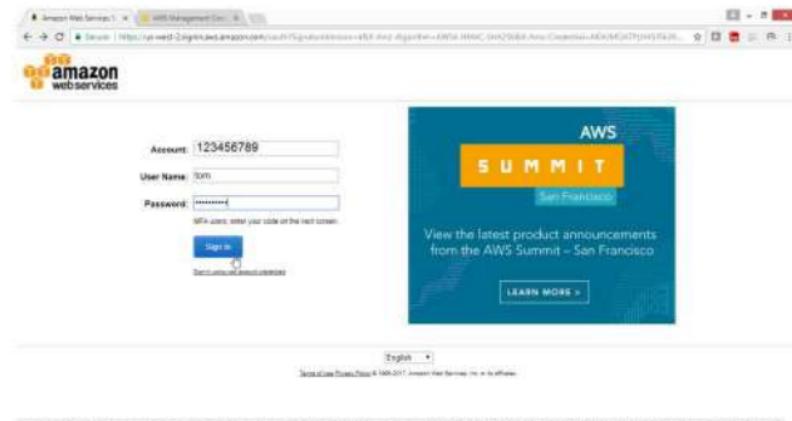
Retype 6 digit bar code in Authentication code 2



Click on Finish



Now login as tom user



Once the user types the MFA 6 digit code

Click on submit



Multi-factor Authentication

Philosophical topics 1982, volume 13, number 1, pp. 1-20

MFA Code: 133432

122

Downloaded from https://academic.oup.com/imrn/article/2020/10/3303/3277317 by guest on 10 August 2020

Verify user had successfully logged in.

The screenshot shows the AWS Management Console with the 'Services' navigation bar selected. The main content area displays several service categories:

- Compute**: Includes EC2 (Virtual Servers), EC2 Container Service (Run and Manage Docker Containers), Lightsail (Launch and Manage Virtual Private Servers), Elastic Beanstalk (Run and Manage Web Apps), Lambda (Serverless without Thinking about Servers), and Batch (Run batch Jobs at Any Scale).
- Developer Tools**: Includes CodeStar (Quickly develop, build, and deploy applications), CodeCommit (Store Code in Private Git Repositories), CodeBuild (Build and Test Code), CodeDeploy (Automate Code Deployments), CodePipeline (Build and Deliver Software using Continuous Delivery), and X-Ray (Monitor and Debug Your Applications).
- Internet of Things**: Includes AWS IoT (Connect Devices to the Cloud) and AWS Greengrass (Deploy and Run code on Your Devices).
- Contact Center**: Includes Amazon Connect (Amazon Connect is a contact center that enables engagement at any scale).
- Game Development**: Includes Amazon GameLift (Deploy and Run Sessions-Based Multiplayer Games).
- Storage**: Includes S3 (Scalable Storage in the Cloud).
- Management Tools**: Includes CloudWatch.
- Mobile Services**: Includes Mobile Hub.

On the right side, there is a sidebar titled "Resource Groups" with a sub-section "Learn more". It contains the following text: "A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account." Below this are two buttons: "Create a Group" and "Tag Editor".

Additional Resources

Getting Started
Read our documentation or view our training to learn more about AWS.

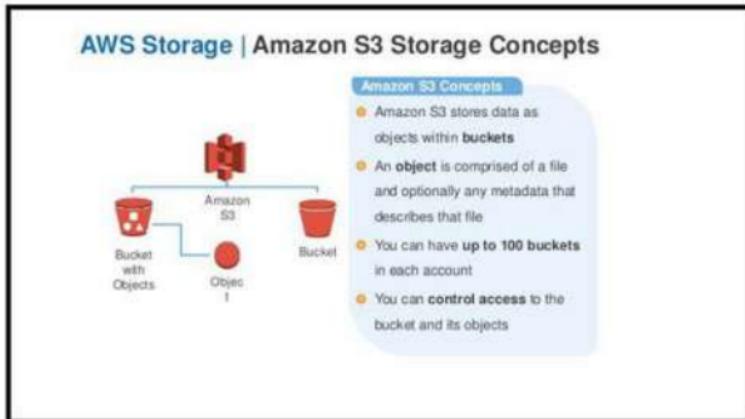
AWS Console Mobile App
View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or

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

OBJECTIVE

To configure and use AWS S3 service

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with AmazonS3FullAccess

To Configure S3 with following task:

Sign Up for Amazon S3

Create a Bucket

Add an Object to a Bucket

Add an folder to Bucket

View an Object

Move an Object

Delete an Object and Bucket

To empty a bucket

To delete a bucket

Hosting a Static Website on Amazon S3

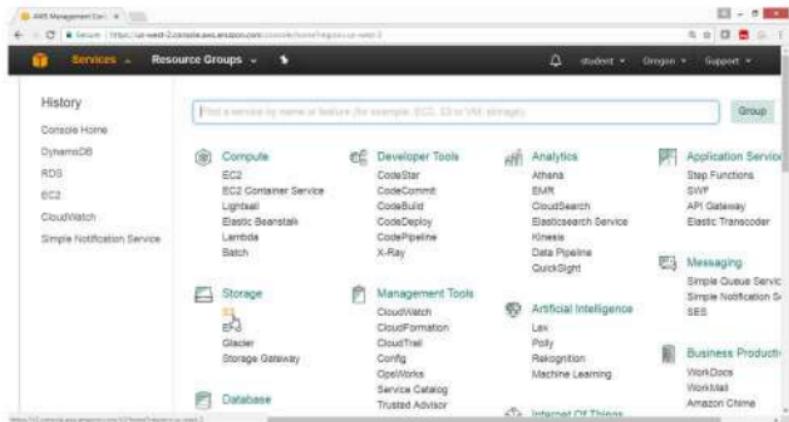
AWS user to control S3

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

Open AWS console

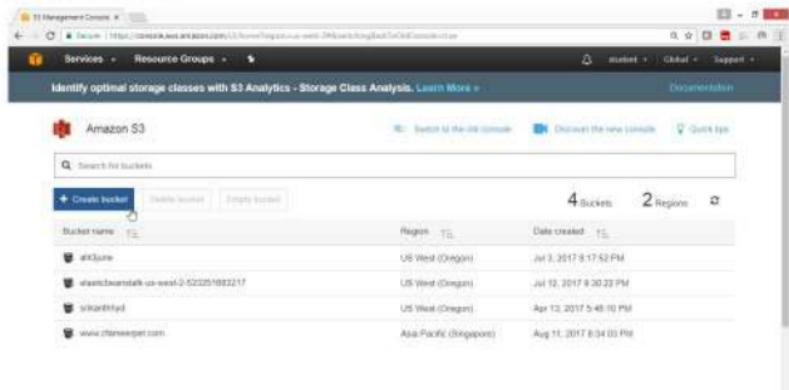
Select “Storage” service

Click on S3



On Amazon S3 page

Click on Create Bucket



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

Provide following values

Bucket Name → saleshydbucket

Region → Oregon

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

Create a Bucket - Select a Bucket Name and Region

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

Bucket Name:

Region:

Verify that bucket is created.

S3 Management Console | New Tab | Services | Resource Groups | student | Global | Sup

Create Bucket Actions Switch to new console None Properties Transfers

All Buckets (4)

Name
cloudmaran
creatic
saleshydbucket1
ekanthyd

Bucket: saleshydbucket1

Bucket: saleshydbucket1
Region: Oregon
Creation Date: Tue Aug 15 08:00:06 GMT+530 2017
Owner: sdmvad@99

+ Permissions
+ Static Website Hosting
+ Logging
+ Events
+ Versioning

To upload files of any type

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

Note: 5 GB can be uploaded

It will be charged if crossed free tier usage..

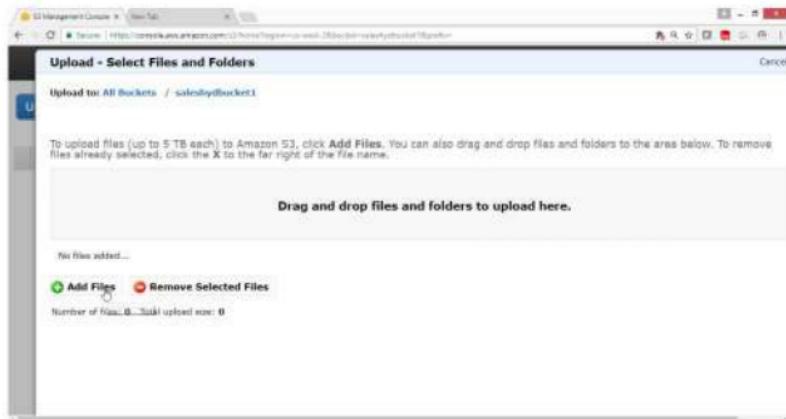
Click on Created bucket

Bucket: saleshydbucket1

Bucket: saleshydbucket1
Region: Oregon
Creation Date: Tue Aug 15 08:00:06 GMT+530 2017
Owner: slrma@999

Permissions
Static Website Hosting
Logging
Events
Versioning

Click on Add files.



In the upload Wizard

Click on **Add files**

Select some txt, pdf, video files

Click "start upload" button



Verify that the file got uploaded.

The screenshot shows the AWS Management Console interface. In the top navigation bar, 'Services' and 'Resource Groups' are selected. Below the navigation, there are three tabs: 'Upload', 'Create Folder', and 'Actions'. A search bar labeled 'Search by prefix' is present. On the left, a table lists a single file entry:

Name	Storage Class	Size	Last Modified
iPhone - MetroGnome Remix (Perf... Standard	Standard	91 MB	Tue Aug

To the right of the table, there is a 'Transfers' section with a checkbox for 'Automatically clear finished transfers'. At the bottom right of the main area, there is a large 'b' icon.

Select the file, Click on Properties on Right Panel,

Click on the link

The screenshot shows the AWS Management Console interface, similar to the previous one, but with the file 'iPhone - MetroGnome Remix (Perf... Standard' selected. The right panel displays detailed properties for this file:

Bucket:	signed-for-object
Name:	(iPhone - MetroGnome Remix [Performed by TPN]) - YouTube [DNG].mp4
Link:	https://s3-us-west-2.amazonaws.com/signed-for-object/1iPhone-MetroGnomeRemix[PerformedbyTPN]-YouTube[DNG].mp4
Size:	9030708
Last Modified:	Tue, 19 Dec 2017 04:00:00 GMT (+00:00)
Owner:	pkrnvel@299
ETag:	03330bae037942041f150e1291f02017ab
Expiration Date:	None
Expiration Rule:	N/A

Below the properties table, there are several expandable sections: 'Details', 'Permissions', 'Metadata', and 'Tags'. At the very bottom of the right panel, there is a URL: [http://127.0.0.1:8000/signed-for-object/1iPhone-MetroGnomeRemix\[PerformedbyTPN\]-YouTube\[DNG\].mp4](http://127.0.0.1:8000/signed-for-object/1iPhone-MetroGnomeRemix[PerformedbyTPN]-YouTube[DNG].mp4).

Verification : Cannot access due to lack of permission

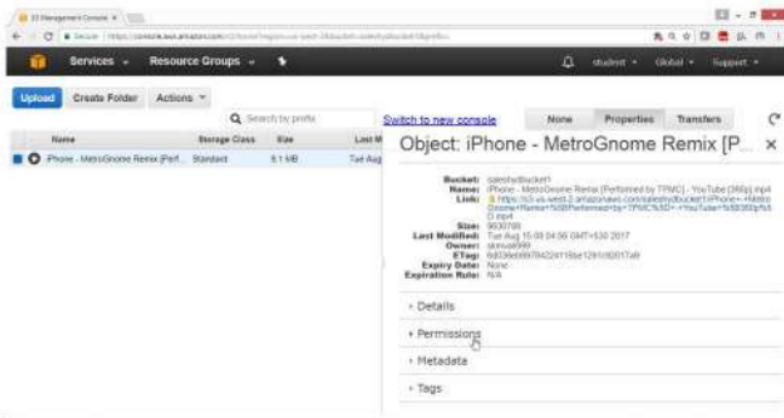


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Errors>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>5723AA1F3766B3B5</RequestId>
</RootId>
<RootId>57A8C9870918Wm4p8rj2pJz7zHwTQzR2Phjg_j7dHUT/t#RxR9VrUfD8qjyEbbQz
</RootId>
</RootId>
```

To allow users to Download, or view give permission

Select Permission tag



Click on Plus Radio button for Add more permissions

Drop down Grantee Button

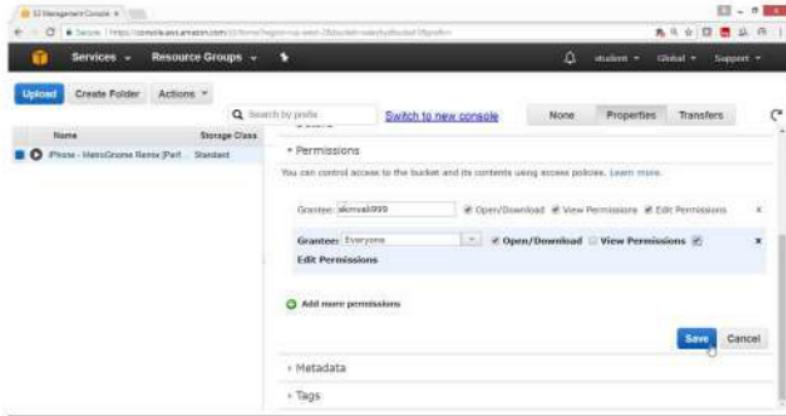
Select **Everyone** to make it public

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

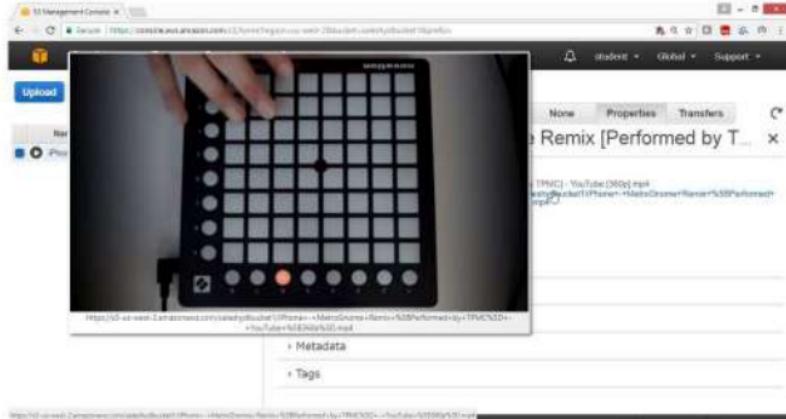
Enable the check box to **View Permission**

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

Click on **Save** button



Verify file is accessible.



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

Select the file from Bucket or Folder, right click,

now select copy/cut



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

Click on the Bucket → finshydbucket1

Click on Paste

The bucket 'finshydbucket1' is empty

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

The screenshot shows the AWS Management Console interface for the S3 service. A file named "iPhone - MacGraves Revis" is selected in the "finshydbucket1" bucket. A context menu is open over this file, displaying the following options: Open, Download, Make Public, Revert, Delete, Edit, Copy, and Properties. The "Delete" option is highlighted with a yellow arrow.

3) To delete a file from a bucket

Right click on it, select Delete

The screenshot shows the AWS Management Console interface for the S3 service. A file named "iPhone - MacGraves Revis" is selected in the "finshydbucket1" bucket. A context menu is open over this file, displaying the following options: Open, Download, Make Public, Revert, Delete, Edit, Copy, and Properties. The "Delete" option is highlighted with a yellow arrow.

To Delete a bucket

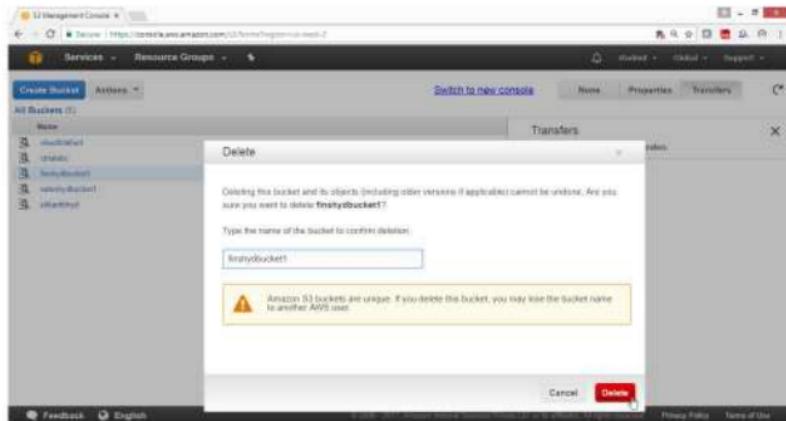
Select the bucket, right click select **Delete Bucket**

The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with tabs for 'Services' (selected), 'Resource Groups', and other account details. Below this is a search bar and a 'Create Bucket' button. The main area is titled 'All Buckets (5)' and lists five buckets: 'cloudthihari', 'ctrlab', 'firsthydbucket1', 'saleshydbucket1', and 'srikanthhyd'. To the right of the bucket list is a sidebar titled 'Transfers' with a checkbox for 'Automatically clear finished transfers'. A context menu is open over the 'firsthydbucket1' row, listing options: 'Create Bucket...', 'Delete Bucket...' (which is highlighted in orange), 'Empty Bucket', 'Paste Into...', and 'Properties'. The 'Delete Bucket...' option is clearly the target of the user's action.

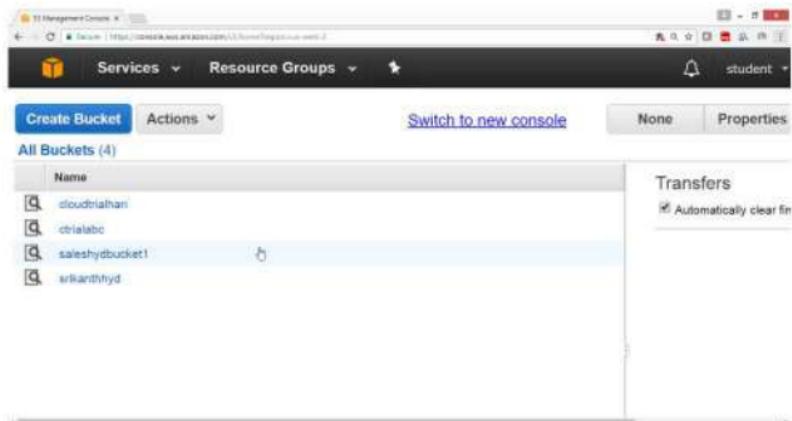
To Delete Bucket

Provide exact bucket name

Click on **Delete** button



Verify that the bucket **finshydbucket1** is deleted



4) To Host a Static Website using Amazon s3 Bucket

To Host a Static Website using Amazon s3 Bucket

Open AWS console

Select **Storage**

Click on **S3** service

Click on "Create Bucket"

The screenshot shows the AWS Management Console S3 service interface. At the top, there's a navigation bar with tabs for 'Services' and 'Resource Groups'. Below the navigation bar, there are buttons for 'Create Bucket' (highlighted in blue), 'Actions', 'Switch to new console', 'None', and 'Properties'. A sidebar on the right is titled 'Transfers' with an option to 'Automatically clear finished transfers'. The main area displays a table titled 'All Buckets (4)' with a column header 'Name'. The table lists four buckets: 'cloudtrilab1', 'cloudtrilab2', 'saleshydbucket1', and 'srikanthhyd'. Each bucket entry includes a small icon and a 'More' button.

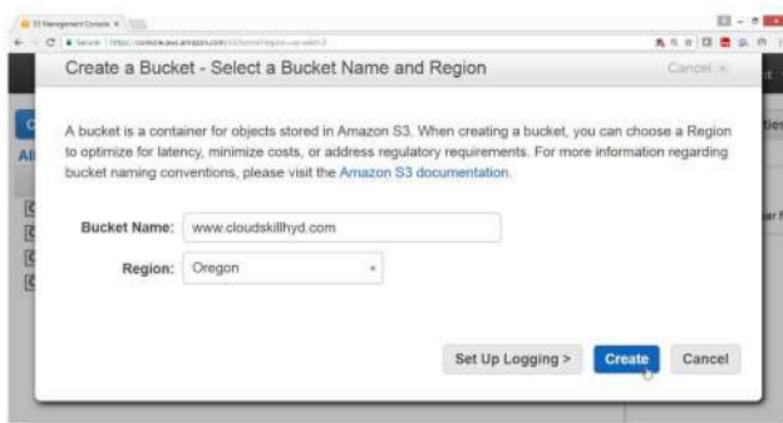
On "Create a Bucket - Select a Bucket Name and Region" page

Provide following values for

Bucket Name → www.cloudskillhyd.com

Region → Oregon

Click on **Create** button



Verify Bucket got created

The screenshot shows the AWS Management Console interface for the S3 service. At the top, there's a navigation bar with 'Services' and 'Resource Groups'. Below it, a sub-navigation bar has 'Create Bucket' highlighted in blue. To the right are 'Actions', 'Switch to new console', 'None', and 'Properties' buttons. A sidebar on the left lists 'All Buckets (4)'. The main content area displays a table with columns: 'Name', 'Last Modified', and 'Transfers'. The table lists four buckets: 'cloudtriahari', 'ctrialabc', 'saleshydbucket1', and 'www.cloudekillhyd.com'. The last bucket, 'www.cloudekillhyd.com', is currently selected, indicated by a blue highlight.

Upload all website contents in this bucket.

The screenshot shows the AWS Management Console interface for the S3 service, specifically viewing the contents of the 'www.cloudekillhyd.com' bucket. The top navigation bar includes 'Services', 'Resource Groups', and 'Actions'. Below it, there are buttons for 'Upload', 'Create Folder', and 'Actions'. To the right are 'Search by prefix', 'Switch to new console', 'None', 'Properties', and 'Transfers' buttons. A sidebar on the left shows the bucket structure with items like 'about.html', 'articles.html', 'contactus.html', 'css', 'images', 'index.html', 'js', and 'sitemap.html'. The main content area displays a table of files with columns: 'Name', 'Storage Class', 'Size', 'Last Modified', and 'Transfers'. The table lists ten files, all of which are 'Standard' storage class and were last modified on Tuesday, August 15, 2017, at various times between 0:00 and 0:37. The 'Transfers' section indicates that transfers are automatically cleared.

Select the bucket and click on properties button

The screenshot shows the AWS Management Console interface for the S3 service. At the top, there's a navigation bar with 'Services' and 'Resource Groups'. Below it, a sub-navigation bar has 'Create Bucket' and 'Actions' on the left, and 'None', 'Properties', and 'Transfers' on the right. The 'Properties' tab is currently selected. Underneath, a section titled 'All Buckets (4)' lists four buckets: 'cloudmohan', 'crislabz', 'saleshydbucket!', and 'www.cloudskilhyd.com'. The fourth bucket is highlighted with a blue selection bar. To the right of the bucket list is a 'Transfers' section with a checkbox for 'Automatically clear finished transfers'.

On the Properties panel

Click Static Website Hosting

Drag Down

This screenshot shows the 'Properties' panel for the 'www.cloudskilhyd.com' bucket. At the top, it displays basic bucket information: Bucket: www.cloudskilhyd.com, Region: Oregon, Creation Date: Tue Aug 15 08:44:43 GMT+530 2017, and Owner: srujan999. Below this, there are sections for 'Permissions' and 'Static Website Hosting'. The 'Static Website Hosting' section is expanded, showing a note that you can host your static website entirely on Amazon S3 once enabled. It also shows the 'Endpoint' as www.cloudskilhyd.com. A note below explains that each bucket serves a website namespace and can route requests to its contents. At the bottom, there's a link to 'AWS Lambda'.

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 Management Console interface for CloudFront. On the left, there's a sidebar with 'Services' and 'Resource Groups'. The main area shows a list of buckets: 'ame', 'soutrahari', 'trialabc', 'unashybucket1', 'unashyrd', and 'www.cloudseelhyd.com'. A modal window is open titled 'Enable website hosting'. It contains two input fields: 'Index Document' set to 'index.html' and 'Error Document' set to '404.html'. Below this, there's a section for 'Edit Redirection Rules' with a note about setting custom rules for redirects. At the bottom of the modal are 'Save' and 'Cancel' buttons, and a link to 'Logging'.

Note down the Endpoint.

The screenshot shows the AWS S3 console with the 'Properties' tab selected for a bucket named 'www.example.com'. The 'Endpoint' field is highlighted with a yellow box, displaying the URL 'www.example.com.v4.amazonaws.com'. A tooltip explains that this endpoint serves a website namespace and can be used for static websites. Below the endpoint, there are sections for 'Do not enable website hosting' (unchecked), 'Enable website hosting' (checked), and 'Edit Redirection Rules'. The 'Enable website hosting' section includes fields for 'Index Document' (set to 'index.html') and 'Error Document' (set to '404.html'). The 'Edit Redirection Rules' section allows for custom redirects. At the bottom right are 'Save' and 'Cancel' buttons. The left sidebar lists other buckets: 'codepipeline', 'CH180C', 'test123bucket', 'test123http', and 'www.example.com'. The bottom of the page includes a footer with links to '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. Below it, the 'Bucket Properties' section is open for the bucket 'www.cloudskillhyd.com'. On the left, a sidebar lists other buckets: 'cloudskillhyd', 'cloudskillhyd1', 'ealexhydtsucker1', 'erikarnhyd', and 'www.cloudskillhyd.com', with the last one currently selected. The main content area displays the bucket details: Bucket: www.cloudskillhyd.com, Region: Oregon, Creation Date: Tue Aug 15 08:44:43 GMT+930 2017, and Owner: skmail999. Below this, the 'Permissions' section is expanded, showing a grantee 'skmail999' with permissions for 'List' and 'Upload/Delete'. There are links to 'View Permissions' and 'Edit Permissions'. At the bottom of the page are buttons for 'Add more permissions', 'Add bucket policy' (which is highlighted in blue), and 'Add CORS Configuration'. A 'Save' button is also present.

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 Management Console with the 'Services' menu selected. In the left sidebar, under 'All Buckets (5)', the 'www.cloudskillhyd.com' bucket is selected. On the right, the 'Static Website Hosting' tab is active. The configuration pane shows the following settings:

- Do not enable website hosting** (radio button)
- Enable website hosting** (radio button)
- Index Document**: index.html
- Error Document**: 404.html

A note on the right explains that each bucket needs a website endpoint (e.g., "www.example.com") and that requests for your host name (e.g., "example.com" or "www.example.com") can be routed to the contents in your bucket. It also mentions how to set up an Amazon S3 static website with your host name.

Verify the website which is coming from S3 Bucket

The screenshot shows a web browser displaying the 'Car Club' website. The page features a purple sports car as the main visual. The navigation menu includes links for HOME, ABOUT, ARTICLES, CONTACTS, SITE MAP, Help, and FNG. Below the navigation, there's a search bar and a 'Latest News' section with two items:

- 10.09.2010** Ford Fiesta Clashes With Toyota Motor India's Corolla Altis
- 10.08.2010** Maruti Suzuki launches its first hybrid model

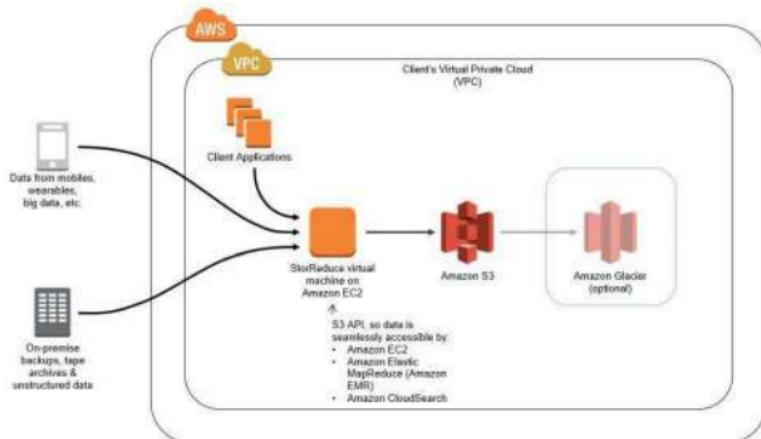
The 'Welcome to Our Club' section contains a brief introduction and links to 'About Us', 'Our Services', 'Contact Us', and 'FAQs'. A note at the bottom states that the website template is optimized for 1024x768 screen resolution.

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

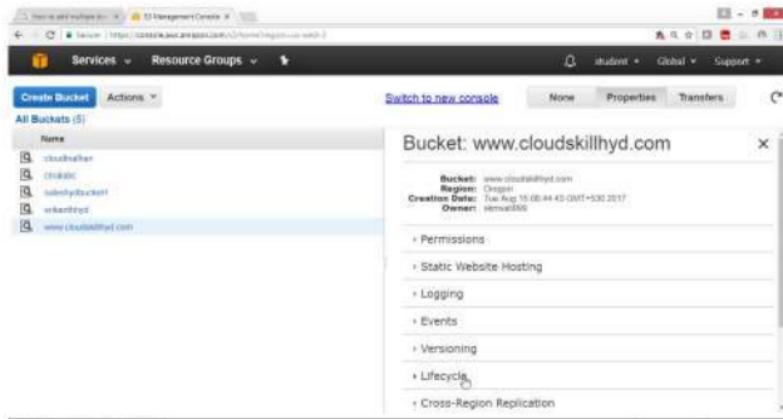
Select S3 bucket

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

Select the bucket,

Go to properties

Click on **Lifecycle**



Click on Add rule

The screenshot shows the AWS Management Console with the 'Services' menu open. Under 'Storage' > 'Buckets', a list of buckets is shown: 'cloud9bucket', 'ct9lab01', 's3nbyt3buck3t!', 'vikanthi', and 'www.cloud9byd.com'. A modal dialog box is open over the list, titled 'Add rule'. The dialog contains a note about enabling versioning and a section for defining rules. Below the note, there's a link to 'Add rule' and two buttons: 'Save' and 'Cancel'. On the right side of the dialog, there's a sidebar with links to 'Cross-Region Replication', 'Tags', 'Requester Pays', 'Transfer Acceleration', and 'Storage Management'.

Under Lifecycle Rules

select **Choose Rule Target**

Apply the Rule to → Whole Bucket

The screenshot shows the AWS Management Console with the 'Services' menu open. Under 'Storage' > 'Buckets', a list of buckets is shown: 'cloud9bucket', 'ct9lab01', 's3nbyt3buck3t!', 'vikanthi', and 'www.cloud9byd.com'. A modal dialog box is open, titled 'Lifecycle Rules'. It has three steps listed on the left: 'Step 1: Choose Rule Target', 'Step 2: Configure Rule', and 'Step 3: Review and Name'. The 'Step 1' panel is active, showing the 'Apply the Rule to:' section with a radio button selected for 'Whole Bucket: www.cloud9byd.com'. Below this are other options like 'A Prefix: e.g. MyFolder or MyFolder/MyObject'. At the bottom of the dialog are 'Cancel' and 'Configure Rule >' buttons.

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

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

click on **Review**

The screenshot shows the AWS Management Console for creating a new Lifecycle Rule. The rule consists of three actions:

- Transition to Standard - Infrequent Access Storage Class:** 7 days after the object's creation date. This rule applies to objects that are less than 30 days old.
- Archive to the Glacier Storage Class:** 7 days after the object's creation date. This rule could reduce your storage costs.
- Permanently Delete:** 372 days after the object's creation date. This rule will permanently delete the object with no recovery.

EXAMPLE: A timeline diagram shows the object's state over time:
Day 0: Object Uploaded → Day 7: Rule activates → Day 372: Rule Deletes → Day 372: Object Deleted.

Provide Rule Name → Testbackup

click on "Create and Activate Rule" button

The screenshot shows the AWS Management Console with the 'Testbackup' rule created and activated. The rule details are as follows:

- Rule Name:** Testbackup
- Rule Target:** This rule will apply to the whole bucket: www.cloudskilthyd.com
- Rule Configuration:** Action on Objects
- Archive to the Glacier Storage Class:** 7 days after the object's creation date.
- Permanently Delete:** 372 days after the object's creation date.

At the bottom, the 'Create and Activate Rule' button is highlighted in blue.

Click on Save button

The screenshot shows the AWS S3 Management Console with the 'Lifecycle' tab selected. A single lifecycle rule named 'TestBackup' is listed, which moves objects to the 'Standard - Infrequent Access' storage class after 30 days. The rule is set to target the 'Whole Bucket'. The 'Enabled' checkbox is unchecked. At the bottom right, there is a 'Save' button.

Verify Storage Class is Standard

The screenshot shows the AWS S3 Management Console listing files in the 'www.cloudifyit.com' bucket. The 'contact-us.html' file is selected. The table displays the following information:

Name	Storage Class	Size	Last Modified
404.html	Standard	6 KB	Tue Aug 15 08:46:32 GMT+01:00 2014
about-us.html	Standard	8.8 KB	Tue Aug 15 08:46:33 GMT+01:00 2014
article.html	Standard	5.3 KB	Tue Aug 15 08:46:34 GMT+01:00 2014
articles.html	Standard	4.8 KB	Tue Aug 15 08:46:34 GMT+01:00 2014
contact-us.html	Standard	4.7 KB	Tue Aug 15 08:46:35 GMT+01:00 2014
css	-	-	-
images	-	-	-
index.html	Standard	6 KB	Tue Aug 15 08:46:36 GMT+01:00 2014
js	-	-	-
sitemap.html	Standard	4.8 KB	Tue Aug 15 08:46:37 GMT+01:00 2014

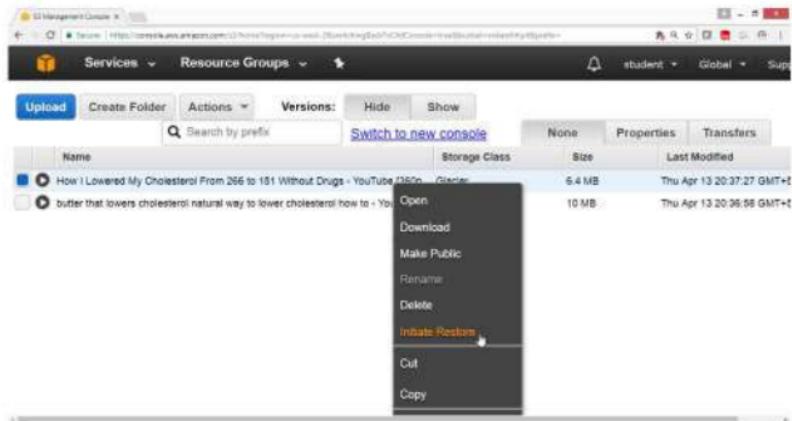
Verify Once the file goes to Glacier then Storage Class is Glacier

The screenshot shows the AWS Management Console interface for S3. At the top, there are navigation tabs for 'Services' (selected), 'Resource Groups', and other account information. Below the header is a toolbar with 'Upload', 'Create Folder', 'Actions', 'Versions', 'Hide', and 'Show' buttons. A search bar with the placeholder 'Search by prefix' is followed by a link to 'Switch to new console'. To the right of the search bar are buttons for 'None', 'Properties', and 'Transfers'. The main area displays a table of uploaded files:

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

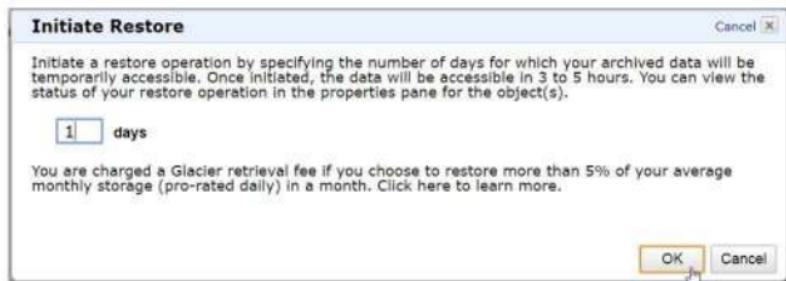
To Restore go to the bucket select the file

Right click and select **Initiate Restore**



Provide number of days → 1

Click on OK



Verify

File will get restored after 1 Day

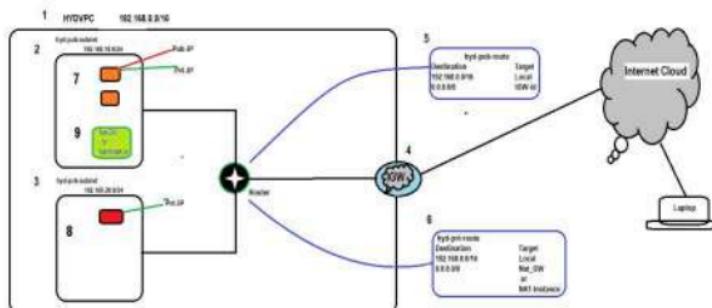
Storage class will become Standard.

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

OBJECTIVE

To configure Amazon Virtual Private Cloud with public and private subnet

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with VPCfullaccess

TASK

- Create your own VPC
- Create Public subnet
- Create Private subnet
- Create Internet Gateway
- Attach Internet Gateway to your VPC
- Create Public Routing Table, associate subnet and add routing rules
- Create Private Routing table, associate subnet and add routing rules
- Launch an instance in Public network
- Launch an instance in Private network
- Create Nat Gateway
- Connect to public instance and check internet connectivity
- Connect to private instance and check internet connectivity

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

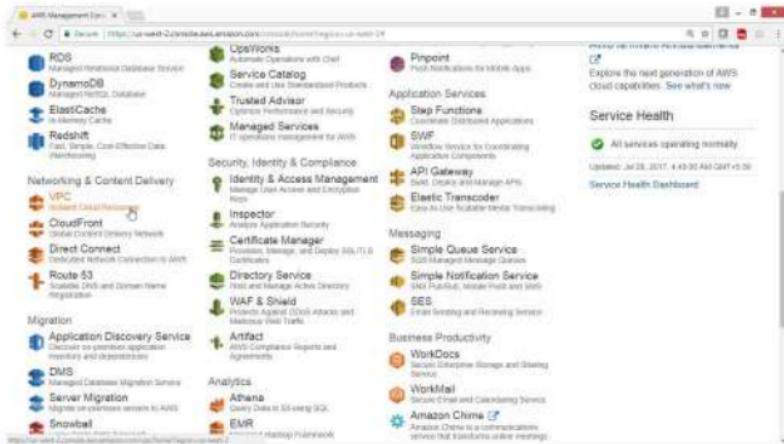
1) To create your own VPC

Open AWS console

Click on Services

Select Networking and Content Delivery

Click on VPC



On VPC Dashboard panel

Click on Your VPC

Click on Create VPC button

The screenshot shows the AWS VPC Management Dashboard. On the left, there's a sidebar with options like Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The 'Your VPC' option is highlighted with a yellow box and a cursor. The main area has a 'Create VPC' button at the top. Below it, there's a search bar and a table with one row of data:

Name	VPC ID	Status	IPv4 CIDR	IPv6 CIDR	DHCP options set
default-vpc-oregon	vpc-49c34f6e	available	172.31.0.0/16		dhcp-options-set100

On "Create VPC", page

For Name tag → HYDVPC

For IPv4 CIDR block → 192.168.0.0/16

Leave remaining field as default

Click on "Yes Create" button



Verify

HYDVPC is created

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

Services Resource Groups

Create VPC Actions

Search VPCs and their properties

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

vpc-7d934d1b | HYDVPC

Summary Flow Logs Tags

VPC ID: vpc-7d934d1b Network ACL: ad-hoc

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

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

Privacy Policy Terms of Use

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

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

On Create Subnet, page

For Name tag → hyd-pub-subnet

For VPC → HYDVPC

For IPv4 CIDR block → 192.168.10.0/24

Click on Yes Create button



Verify

hyd-pub-subnet got created

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with options like Services, Resource Groups, VPC Dashboard, and Subnets (which is currently selected). The main area is titled 'Create Subnet' and shows a table of subnets. One row is highlighted with a blue background, representing the newly created 'hyd-pub-subnet'. The table includes columns for Name, Subnet ID, State, VPC, IPv4 CIDR, and Available. Below the table, there's a detailed view of the selected subnet, showing its summary, route table, network ACL, flow logs, and tags. The subnet ID is listed as 'subnet-03db0fa' and the availability zone as 'us-west-2a'.

3) To create private subnet

Click on **Subnet**

Click on **Create Subnet** button

This screenshot is similar to the previous one, showing the AWS VPC Management Console. The 'Create Subnet' button is highlighted with a red box, drawing attention to it as the next action. The rest of the interface, including the subnet list and the detailed view below, remains the same.

On Create Subnet, page

- For Name tag → hyd-pvt-subnet
For VPC → HYDVPC
For IPv4 CIDR block → 192.168.20.0/24

Click on Yes Create button



Verify

hyd-pvt-subnet got created

The screenshot shows the AWS VPC Management Console. In the left sidebar, under the 'Subnets' section, there is a new entry: 'hyd-pvt-subnet'. The main table lists five subnets:

Name	Subnet ID	State	VPC	IPv4 CIDR	Available
hyd-pvt-subnet	subnet-6abc0f03	available	vpc-7b934df0 HYD-VPC	192.168.20.0/24	251
hyd-pub-subnet	subnet-63b3fe6e	available	vpc-7b934df0 HYD-VPC	192.168.10.0/24	251
subnet-18d31f41	available	vpc-8c341ee1 default-vpc-oregon	172.31.0.0/20	4091	
subnet-13f005fa	available	vpc-8c341ee1 default-vpc-oregon	172.31.32.0/20	4000	
subnet-620c10ec	available	vpc-8c341ee1 default-vpc-oregon	172.31.16.0/20	4091	

Below the table, a modal window titled 'subnet-6abc0f03 | hyd-pvt-subnet' is open, showing the 'Summary' tab. It displays the subnet ID as 'subnet-6abc0f03 | Hyd-pvt-' and the availability zone as 'us-west-2a'.

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

In VPC Dashboard panel

Click on Internet Gateway

The screenshot shows the AWS VPC Management Console. In the left sidebar, under the 'Internet Gateways' section, there is a new entry: 'hyd-pvt-subnet'. The main table lists five subnets:

Name	Subnet ID	State	VPC	IPv4 CIDR	Available
hyd-pvt-subnet	subnet-6abc0f03	available	vpc-7b934df0 HYD-VPC	192.168.20.0/24	251
hyd-pub-subnet	subnet-63b3fe6e	available	vpc-7b934df0 HYD-VPC	192.168.10.0/24	251
subnet-18d31f41	available	vpc-8c341ee1 default-vpc-oregon	172.31.0.0/20	4091	
subnet-13f005fa	available	vpc-8c341ee1 default-vpc-oregon	172.31.32.0/20	4000	
subnet-620c10ec	available	vpc-8c341ee1 default-vpc-oregon	172.31.16.0/20	4091	

Below the table, a modal window titled 'subnet-6abc0f03 | hyd-pvt-subnet' is open, showing the 'Summary' tab. It displays the subnet ID as 'subnet-6abc0f03 | Hyd-pvt-' and the availability zone as 'us-west-2a'.

Click on Create Internet Gateway button

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with navigation links like 'Virtual Private Cloud', 'Your VPCs', 'Subnets', 'Route Tables', 'Internet Gateways' (which is currently selected), 'Egress Only Internet Gateways', 'DHCP Options Sets', 'Elastic IPs', 'Endpoints', and 'NAT Gateways'. The main area has a title 'Create Internet Gateway' with a 'Delete' button and filters for 'Name', 'ID', 'State', and 'VPC'. A search bar says 'Search Internet Gateways ...'. Below it, a table shows one Internet Gateway: 'ipn-4eef7f1fa' (Status: attached) under 'vpc-48c34f6c | default vpc: us-west-2'. A note says 'Select an Internet gateway above' with three icons. At the bottom, there are 'Feedback', 'English', and links to 'Privacy Policy' and 'Terms of Use'.

In Create Internet Gateway, box

For Name tag → HYDIGW

Click on "Yes, Create" button

This screenshot shows the 'Create Internet Gateway' dialog box. It contains a description: 'An Internet gateway is a virtual router that connects a VPC to the Internet.' Below is a 'Name tag' input field with 'HYDIGW' typed in. At the bottom right are 'Cancel' and 'Yes, Create' buttons, with 'Yes, Create' being highlighted by a blue box.

Verify

Internet gateway is created

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

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 Internet Gateway Delete Attach to VPC Details (View VPC)

Search Internet Gateways and X

Name ID State VPC

HYDIGW igw-be27ef09 detached

igw-be27ef09 igw-be27ef09 attached vpc-09c341ee | default-vpc-oregon

igw-be27ef09 | HYDIGW

Summary Tags

ID: igw-be27ef09 | HYDIGW Attached VPC ID:

Feedback English

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

Select HYDIGW

Click "Attach to VPC"

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

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 Internet Gateway Delete Attach to VPC Details (View VPC)

Search Internet Gateways and X

Name ID State VPC

HYDIGW igw-be27ef09 detached

igw-be27ef09 igw-be27ef09 attached vpc-09c341ee | default-vpc-oregon

igw-be27ef09 | HYDIGW

Summary Tags

ID: igw-be27ef09 | HYDIGW Attached VPC ID:

Feedback English

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

In "Attach to VPC" box

For VPC → HYDVPC

click on "Yes, Attach" button



Verify

Internet gateway is connected to your VPC

Name	ID	State	VPC
HYDOW	igw-be027af9	attached	vpc-7d934d1b HYDVPC
	igw-be027af9a	attached	vpc-40c34fca default-vpc-oregon

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

On VPC Dashboard panel

Click on Route Table

Name	ID	State	VPC
HYDVGW	igw-0e27abdb	attached	vpc-7d934d7b HYDVPC
igw-0e27abdb	igw-0e27abdb	attached	vpc-7d934d7b default vpc-oregon

Click on "Create Route table" button

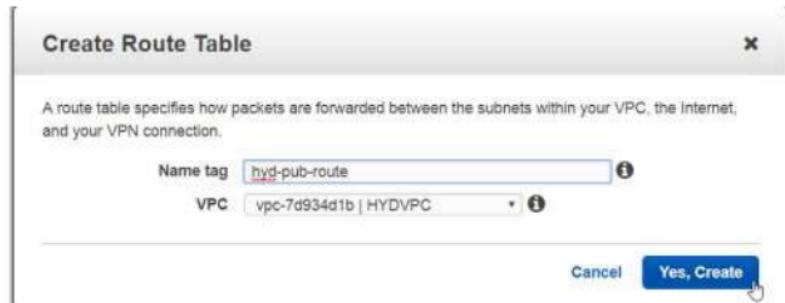
Select a route table above.

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. A table lists three route tables:

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	0 Subnets	No	vpc-7d934d1b HYDVPC
	rtb-199c27e	0 Subnets	Yes	vpc-ff934fe1 default-vpc-oregon
	rtb-8476526	0 Subnets	Yes	vpc-7d934d1b HYDVPC

Below the table, a detailed view of the 'hyd-pub-route' route table is shown, including tabs for Summary, Routes, Subnet Associations, Route Propagation, and Tags. The 'Summary' tab is selected.

Click on "Subnet Association" button

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	0 Subnets	No	vpc-78934810 HYD-VPC
	rtb-199b27e	0 Subnets	Yes	vpc-85c341ee default-vpc-oregon
	rtb-647-6524	0 Subnets	Yes	vpc-78934810 HYD-VPC

Click on Edit button

rtb-234b6445 | hyd-pub-route

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pub-route	rtb-234b6445	0 Subnets	No	vpc-78934810 HYD-VPC

Edit

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:

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

The screenshot shows the AWS VPC Management Console interface. On the left sidebar, under 'Route Tables', the 'Subnets' section is selected. In the main area, a 'Create Route Table' button is visible. A route table named 'rtb-234b6445 | hyd-pub-route' is listed. The 'Associate' tab is selected, showing two subnets associated with the route table:

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
✓	subnet-0303b4f9 hyd-pub-subnet	192.168.10.0/24	-	Main
✓	subnet-040c0223 hyd-pv1-subnet	192.168.20.0/24	-	Main

Verify

hyd-pub-subnet is associated with routing table

The screenshot shows the AWS VPC Management Console interface. On the left sidebar, under 'Route Tables', the 'Subnets' section is selected. In the main area, a route table named 'rtb-234b6445 | hyd-pub-route' is listed. The 'Associate' tab is selected, and a note at the bottom states: "The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table."

Click on **Route** button

Click on **Edit** button

The screenshot shows the AWS VPC Management Console. On the left sidebar, under the 'Route Tables' section, the 'rtb-234b6445 | hyd-pub-route' table is selected. In the main content area, there is a table listing route tables. The 'rtb-234b6445 | hyd-pub-route' table is highlighted. Below the table, there are tabs for 'Summary', 'Routes', 'Subnet Associations', 'Route Propagation', and 'Tags'. The 'Routes' tab is active. A blue 'Edit' button is located above the route table details. The details pane shows the route table ID as 'rtb-234b6445', associated with 'subnet-034f816e | hyd-pub-subnet' (IP range 10.10.0.0/16), and a note stating that some subnets have not been explicitly associated with any route tables and are therefore associated with the main route table.

Click on "Add another route" button

This screenshot shows the 'Routes' tab for the 'rtb-234b6445 | hyd-pub-route' route table. The table lists one existing route: '10.10.0.0/16' pointing to 'local' with an 'Active' status and 'No' propagation. Below the table, there is a blue 'Save' button. At the bottom of the route list, there is a button labeled 'Add another route' with a small arrow icon pointing to it. The rest of the interface is identical to the previous screenshot, including the sidebar and other tabs.

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 'Route Tables' section selected. A new route table has been created and is being configured. The 'Routes' tab is active, showing a single route entry:

Destination	Target	Status	Propagated	Remove
192.168.0.0/16	xgw	Active	No	(Remove)
0.0.0.0/0	igw-0e27a5d9 HYDIGW		No	(Remove)

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

Verification

Public route is added through internet gateway

The screenshot shows the same AWS VPC Management Console interface after saving the route table. The route table now contains two entries, confirming the addition of the public route via the internet gateway.

Destination	Target	Status	Propagated	Remove
192.168.0.0/16	xgw	Active	No	(Remove)
0.0.0.0/0	igw-0e27a5d9		No	(Remove)

Verify

Status column show Active

The screenshot shows the AWS VPC Management Console interface. On the left, a sidebar lists various VPC components: Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, and NAT Gateways. The 'Route Tables' section is currently selected. The main content area displays a list of route tables under the heading '1 to 3 of 3 Route Tables'. One route table is selected, showing its details. The 'Routes' tab is active, and the table below lists the routes:

Destination	Target	Status	Propagated
192.168.0.0/16	igw-12345678	Active	No
0.0.0.0	gw-12345678	Active	No

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

On VPC Dashboard panel

Select Route Tables

Click on "Create Route Table"

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with navigation links like Services, Resource Groups, and various VPC components. The main area is titled 'VPC Dashboard' and shows a table of existing route tables. One row is selected, 'rtb-234b6445 | hyd-pvt-route'. Below the table, there are tabs for Summary, Routes, Subnet Associations, Route Propagation, and Tags. Under the 'Routes' tab, there's a 'View' dropdown set to 'All routes'. At the bottom of the page, there are links for Feedback, English, and legal notices.

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' and a descriptive text about route tables. It contains two input fields: 'Name tag' with the value 'hyd-pvt-route' and 'VPC' with the value 'vpc-7d934d1b | HYDVPC'. At the bottom right, there are 'Cancel' and 'Yes, Create' buttons, with 'Yes, Create' being highlighted.

Verify

hyd-pvt-route table is created

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	rtb-ac446bca	0 Subnets	No	vpc-7d934d1b HYD VPC
hyd-pvt-route	rtb-234b6445	1 Subnet	No	vpc-7d934d1b HYD VPC
	rts-1993c2fe	0 Subnets	Yes	vpc-803341ee default vpc-arnogen
	rts-847452e2	0 Subnets	Yes	vpc-7d934d1b HYD VPC

Click on Subnet Association button

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	rtb-ac446bca	0 Subnets	No	vpc-7d934d1b HYD VPC
hyd-pvt-route	rtb-234b6445	1 Subnet	No	vpc-7d934d1b HYD VPC
	rts-1993c2fe	0 Subnets	Yes	vpc-803341ee default vpc-arnogen
	rts-847452e2	0 Subnets	Yes	vpc-7d934d1b HYD VPC

Click on Edit button

VPC Dashboard
Filter by VPC:
None

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

Services Resource Groups

Create Route Table Delete Route Table Set As Main Table

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

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	rtb-ac44fbca	0 Subnets	No	vpc-74934d1b HYDVPC
hyd-pub-route	rtb-234b6445	1 Subnet	No	vpc-74934d1b HYDVPC
	rtb-199b27e	0 Subnets	Yes	vpc-09c34f6e default-vpc-oregon
	rtb-647b52e2	0 Subnets	Yes	vpc-09c34f6e HYDVPC

rtb-ac44fbca | hyd-pvt-route

Summary Routes Subnet Associations Route Propagation Tags

Edit Subnet IPv4 CDR IPv6 CDR

* You can now associate a subnet association.

Feedback English © 2018 - 2019 Amazon Web Services, Inc. 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

Services Resource Groups

Create Route Table Delete Route Table Set As Main Table

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

Name	Route Table ID	Explicitly Associated	Main	VPC
hyd-pvt-route	rtb-ac44fbca	0 Subnets	No	vpc-74934d1b HYDVPC
hyd-pub-route	rtb-234b6445	1 Subnet	No	vpc-74934d1b HYDVPC
	rtb-199b27e	0 Subnets	Yes	vpc-09c34f6e default-vpc-oregon
	rtb-647b52e2	0 Subnets	Yes	vpc-09c34f6e HYDVPC

rtb-ac44fbca | hyd-pvt-route

Summary Routes Subnet Associations Route Propagation Tags

Associate Subnet IPv4 CDR IPv6 CDR Current Route Table

Cancel Save

Associate	Subnet	IPv4 CDR	IPv6 CDR	Current Route Table
<input type="checkbox"/>	subnet-b20d0bfa hyd-pvt-subnet	192.168.20.0/24	-	rtb-234b6445 hyd-pub-route
<input checked="" type="checkbox"/>	subnet-0ebcb3d5 hyd-pvt-subnet	192.168.20.0/24	-	Main

Feedback English © 2018 - 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click on Save button

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with navigation links like Services, Resource Groups, VPC Dashboard, and various subnets and route tables. The main area is titled "Create Route Table". A search bar at the top says "Search Route Tables and their X". Below it is a table with columns: Name, Route Table ID, Explicitly Associated, Main, and VPC. There are two entries: one for a standard route table and another for "hyd-pvt-route". The "hyd-pvt-route" entry has a "Save Successful" message below it. At the bottom of the table, it says "The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table." The URL in the browser is <https://us-west-2.console.aws.amazon.com/vpc/routes?region=us-west-2&tab=routeTables>.

Verify

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

This screenshot is identical to the previous one, showing the "Create Route Table" screen. The "hyd-pvt-route" table now has "1 Subnet" listed under the "Explicitly Associated" column. The "Save Successful" message is still present. The URL in the browser is <https://us-west-2.console.aws.amazon.com/vpc/routes?region=us-west-2&tab=routeTables>.

Click on Route button

The screenshot shows the AWS VPC Management Console. On the left sidebar, under 'Route Tables', 'hyd-pvt-route' is selected. In the main content area, the 'Routes' tab is active for the route table 'rtb-ac446bca | hyd-pvt-route'. The table lists one 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 AWS VPC Management Console. On the left sidebar, under 'Route Tables', 'hyd-pvt-route' is selected. In the main content area, the 'Routes' tab is active for the route table 'rtb-ac446bca | hyd-pvt-route'. The table lists one route entry:

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No

7) To launch Windows instance in Public subnet

Open the AWS console.

Click on Services

Click on Ec2 services

The screenshot shows the AWS Management Console with the Services menu selected. The main area displays various AWS services categorized into groups:

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

The screenshot shows the AWS Management Console EC2 Dashboard. On the left, there's a sidebar with navigation links: 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 content area has three tabs: Resources, Account Attributes, and Additional Information. The Resources tab shows usage statistics for the US West (Oregon) region:

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

A callout box highlights the "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." link. Below this, there's a "Create Instance" section with a "Launch Instance" button. The Additional Information tab contains 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 for 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 content area has a title bar "Launch Instance" with tabs for "Compute" and "Actions". Below it is a search bar with placeholder text "Filter by tags and attributes or search by keyword". A table lists three instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
vmt1	i-0105a6e0204e919fc	t2-small	us-west-2c	terminated	None	
nodejs_server	i-0d48e700188c4472	t2-micro	us-west-2c	terminated	None	
wmt1	i-0f1a44f9f18100325	t2-micro	us-west-2a	terminated	None	

A message "Select an Instance above" is displayed below the table. At the bottom, there are "Feedback" and "English" buttons, along with copyright information: "© 2006-2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy | Terms of Use".

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

Free tier eligible

Step 1: Choose an Amazon Machine Image (AMI)

Root device type: ebs Virtualization type: hvm

Windows

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

Windows

Microsoft Windows Server 2012 with SQL Server Express - ami-7ac8de03
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

Windows

Microsoft Windows Server 2012 with SQL Server Web - ami-f2cf6dbb

Select

Cancel and Exit

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 ShowHide Columns

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

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

Review and Launch

Cancel Previous Next: Configure Instance Details

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

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 Management Console interface for launching an Amazon Machine Image (AMI). The top navigation bar includes 'Services', 'Resource Groups', and tabs for 'Configure Instance', 'Add Storage', 'Add Tags', 'Configure Security Group', and 'Review'. The main content area is titled 'Step 3: Configure Instance Details' with the 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.' Below this, there are several configuration fields:

- Number of Instances:** Set to 1, with a link to 'Launch Into Auto Scaling Group'.
- Purchasing option:** Set to 'Request Spot Instances'.
- Network:** Set to 'vpc-7e934a15 | HYDVPC'.
- Subnet:** Set to 'subnet-b3tobaf0 | hyd-pub-subnet | us-west-2a'.
- Auto-assign Public IP:** Set to 'Enable'.
- Domain join directory:** Set to 'None'.

At the bottom of the form are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is 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 (GB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-01e5ba77f81e7258	30	General Purpose (SSD)	100 / 3000	N/A		Not Encrypted

Add New Volume

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

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 = Webscraper.

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	(256 characters maximum)	Instances	Volumes
Key	Value	Instances	Volumes		

This resource currently has no tags.

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

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

For "Key" → Name

For Value → Winpubvm

Click on "Next: Configure Security Group"

The screenshot shows the AWS EC2 Management Console with the title 'EC2 Management Console'. The navigation bar includes 'Services', 'Resource Groups', 'Student', 'Groups', and 'Support'. Below the navigation, a progress bar indicates steps 1 through 7, with '6. Add Tags' currently selected. A note explains that a tag consists of a key-value pair, such as 'Name=Winserver'. It also states that a tag can be applied to volumes, instances, or both, and that tags will be applied to all instances and volumes. A 'Feedback' link is at the bottom left, and a footer links to 'AWS Privacy', 'AWS Terms of Use', and 'AWS Customer Agreement'.

Key	Value	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 - 2014 Amazon Web Services, Inc. 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 <input style="width: 100px; height: 15px;" type="button" value="..."/>

Add Rule

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

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
Microsoft Windows 2012 Standard edition with 64-bit architecture. (English)
Free tier eligible
View Recent Activity

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

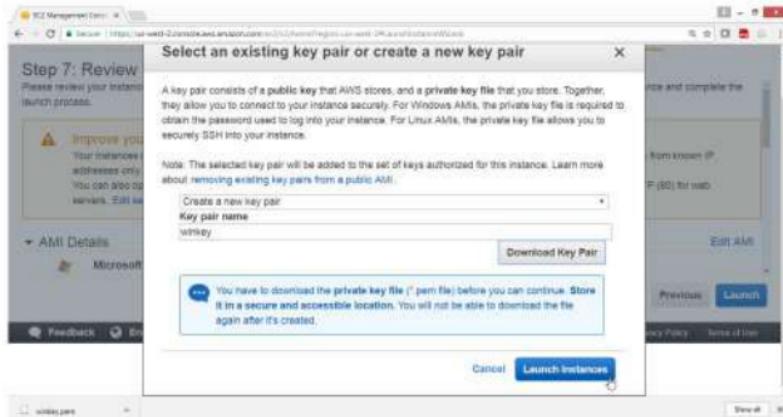
Select "Create a new key pair"

For "Key pair name" → winkey

Click on "Download Key Pair" button



Click on "Launch Instance" button



Check summary, Drag down

Click on "View Instance" button

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2&tab=instances>. The page title is "Launch Status". A sub-header says "Click View Instances to monitor your instances' status. Once your instances are in the running state, you can connect to them from the Instances screen. Find out how to connect to your instances." Below this, a section titled "Here are some helpful resources to get you started" lists links to the Amazon EC2 User Guide, Amazon EC2: Microsoft Windows Guide, and the Amazon EC2 Discussion Forum. Further down, it says "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 is a blue "View Instances" button.

Verify that instance is Running

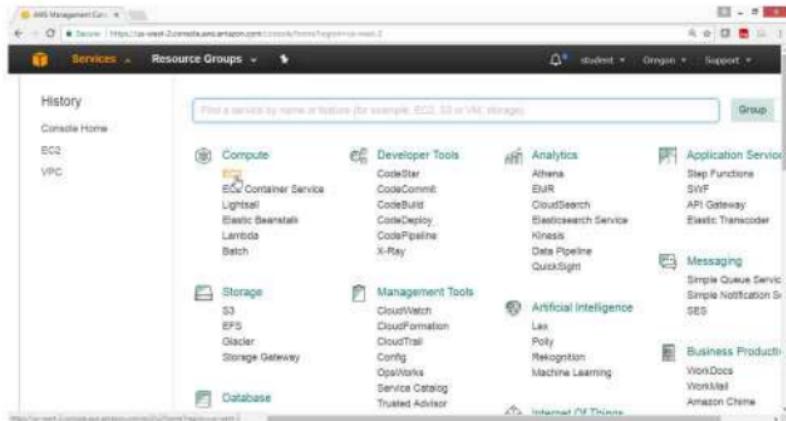
The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2&tab=instances>. The left sidebar shows navigation options like EC2 Dashboard, Events, Tags, Reports, Limits, Instances (which is selected), Instances Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, and Elastic Block Store. The main content area has tabs for "Launch Instance", "Connect", and "Actions". It includes a search bar and filters for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. A table lists one instance: "Winputvm" (Instance ID: i-0cb28994e13174e05, Instance Type: t2.micro, Availability Zone: us-west-2a, Instance State: running). Below the table are tabs for Description, Status Checks, Monitoring, and Tags. At the bottom right are "Feedback" and "English" buttons, and a footer with copyright information and links to 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. The left sidebar has 'Instances' selected under 'EC2 Dashboard'. The main area displays 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, details for the instance are shown: Instance ID i-0cb26994e13174e85 (Winpubvm), Public IP 54.202.132.130. A tab bar at the bottom includes 'Description', 'Status Checks', 'Monitoring', and 'Tags'. The 'Status Checks' tab is active.

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

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

Free tier eligible

The screenshot shows the AWS Management Console interface for creating a new instance. The top navigation bar includes 'Services', 'Resource Groups', and a user dropdown. Below the navigation is a step-by-step wizard:

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

The main content area is titled "Step 1: Choose an Amazon Machine Image (AMI)". It lists several AMI options under the "Windows" category:

AMI Name	Description	Action
Microsoft Windows Server 2016 with SQL Server Standard - ami-39fae540	Microsoft Windows 2016 Datacenter 64bit, 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, Microsoft SQL Server 2012 Express, (English)	Select

At the bottom of the page, there are links for "Feedback", "English", "© 2008 - 2017 Amazon Web Services, Inc. or its affiliates. All rights reserved.", "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 Management Console interface for choosing an instance type. The top navigation bar includes 'Services', 'Resource Groups', and several user account details. Below the navigation is a breadcrumb trail: '1. Choose AMI' (disabled), '2. Choose Instance Type' (highlighted in yellow), '3. Configure Instance', '4. Add Storage', '5. Add Tags', '6. Configure Security Group', and '7. Review'. A 'Step 2: Choose an Instance Type' header is present. A filter bar allows filtering by 'All instance types' or 'Current generation' and provides 'Show/Hide Columns' options. A note at the top states: 'Currently selected: t2.micro (Variable ECUs, 1 vCPU, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)'. The main table lists various instance types with columns for Family, Type, vCPUs, Memory (GiB), Instance Storage (GiB), EBS-Optimized Available, Network Performance, and IPv6 Support. The 't2.micro' row is selected, highlighted with a green background and a blue border around the 'Type' column. Other visible rows include t2.nano, t2.small, t2.medium, and t2.xlarge. At the bottom of the table are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is highlighted in blue), and 'Next: Configure Instance Details'.

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
<input checked="" type="checkbox"/> General purpose	t2.micro <small>(Variable ECUs, 1 vCPU, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)</small>	1	1	EBS only	+	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

On 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 AWS EC2 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 from a dropdown, with 'Create new VPC' as an option. In the 'Subnet' section, 'subnet-6abcf033 | hyd-pvt-subnet | us-west-2a' is selected, with 'Create new subnet' and '251 IP Addresses available' options. Under 'Auto-assign Public IP', 'Disable' is selected. A 'Domain join directory' field is set to 'None'. At the bottom, there are 'Cancel', 'Previous', 'Review and Launch', 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 AWS EC2 wizard. It displays a table for adding storage volumes. A single row is present for the 'Root' volume, which is mounted at '/dev/sda1'. The 'Size (GiB)' is set to 30, and the 'Volume Type' is 'General Purpose (SSD)'. The 'Throughput (Mbps)' is 100 / 3000, and 'Delete on Termination' is checked. The 'Encrypted' column shows 'Not Encrypted'. Below the table, there is a note about free tier usage and a 'Add New Volume' button. At the bottom, there are 'Cancel', 'Previous', 'Review and Launch', and 'Next: Add Tags' buttons.

Click on “Add tag” button

The screenshot shows the 'Add Tag' step of the EC2 instance creation wizard. At the top, there are tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (which is highlighted), 6. Configure Security Group, and 7. Review. Below the tabs, there are fields for 'Key' (Name) and 'Value' (Winpvttvm). A note says 'This resource currently has no tags.' Below the fields, it 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 highlighted in blue), and 'Next: Configure Security Group'. There are also 'Feedback' and 'English' links at the bottom.

For “Key” → Name

For Value → Winpvttvm

Click on “Next: Configure Security Group” button

The screenshot shows the 'Configure Security Group' step of the EC2 instance creation wizard. 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 (which is highlighted), and 7. Review. Below the tabs, there are fields for 'Key' (Name) and 'Value' (Winpvttvm). A note says 'This resource currently has no tags.' Below the fields, it 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 highlighted in blue), and 'Next: Configure Security Group'. There are also 'Feedback' and 'English' links at the bottom.

Take Default Values

Click on "Review and Launch" button

The screenshot shows the AWS EC2 Management Console with the 'Configure Security Group' step selected. A new security group named 'Launch-wizard-2' is being created. It contains one rule: Type: RDP, Protocol: TCP, Port Range: 3389, Source: 0.0.0.0/0. At the bottom right, the 'Review and Launch' button is highlighted.

Drag down

Click on "Launch" button

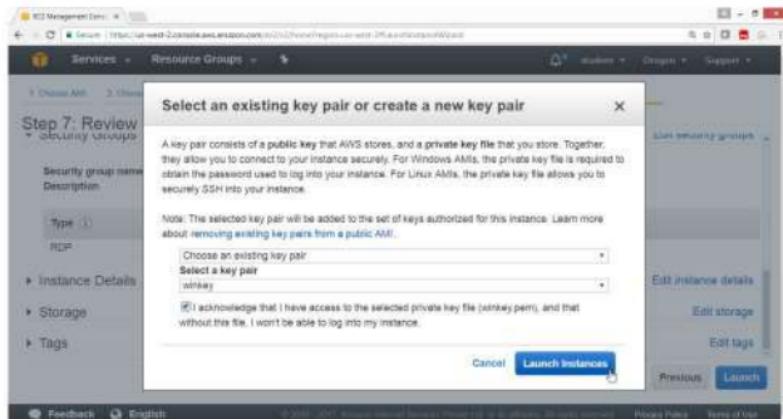
The screenshot shows the AWS EC2 Management Console with the 'Review Instance Launch' step selected. A warning message states: 'Improve your instances' security. Your security group, launch-wizard-1, is open to the world.' It advises updating security group rules to allow access from known IP addresses only. Below this, the 'Launch' button is prominently displayed.

Select "Choose an existing key pair"

For "Key pair name" → winkey

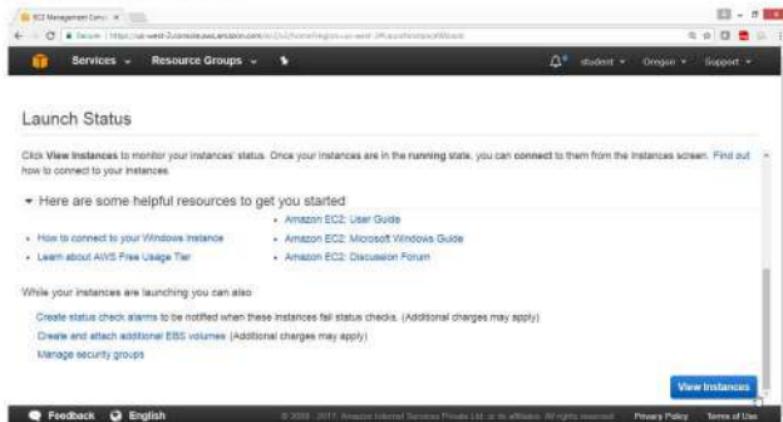
Select I acknowledge check box

Click on "Launch Instance" button



Check summary, Drag down

Click on "View Instance" button



Verify that instance is Running

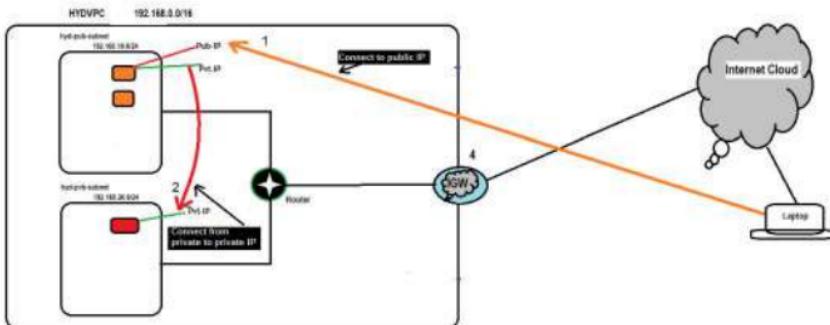
The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with navigation links: Services, Resource Groups, EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, Bundl Tasks, and Elastic Block Store. Under Instances, 'Instances' is selected. In the main pane, there's a search bar at the top followed by a table. The table has columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, and Alarm. There are two rows: one for 'Wingutvm' (Instance ID: i-0c20994e13174e85, Type: t2.micro, Zone: us-west-2a, State: running, 2/2 checks) and one for 'Wingvifm' (Instance ID: i-0e2251b25ee0894e, Type: t2.micro, Zone: us-west-2a, State: running, 2/2 checks). Below the table, a message says 'Instances: [i-0c20994e13174e85 (Wingutvm), i-0e2251b25ee0894e (Wingvifm)]'. At the bottom, there are tabs for Description, Status Checks, Monitoring, and Tags.

Verification

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

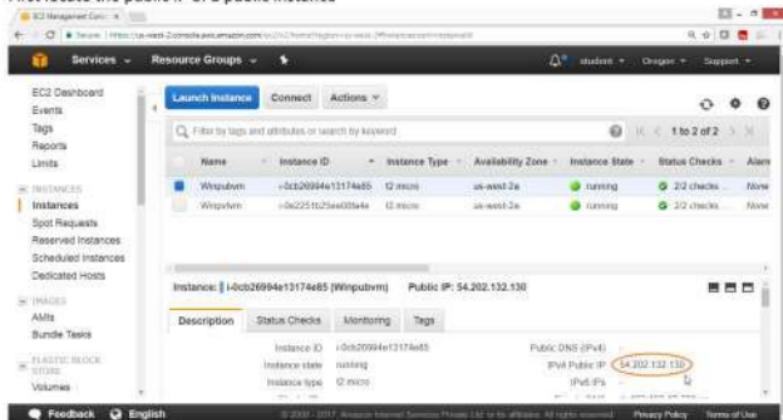
This screenshot is identical to the one above, showing the AWS EC2 Management Console with two instances running: 'Wingutvm' and 'Wingvifm'. The interface includes the sidebar with 'Instances' selected, the search bar, the table with instance details, and the message at the bottom indicating the instances are running.

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



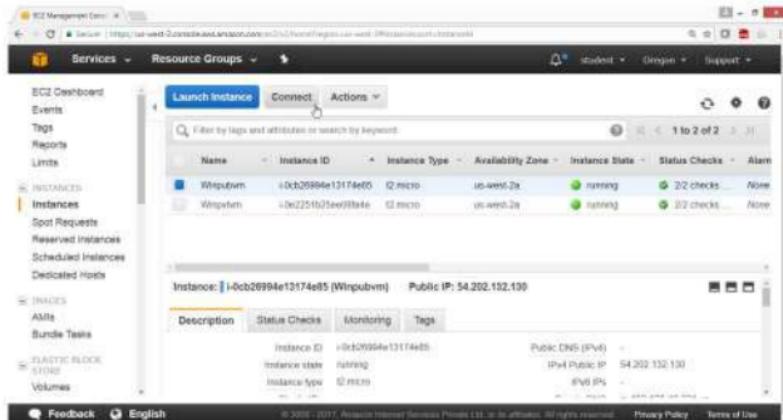
9) To Connect to Public subnet instance

First locate the public IP of a public instance



The screenshot shows the AWS EC2 Management Console. 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 (AMIs), Bundle Tasks, and Elastic Block Store (Volumes). The main content area displays a table of instances. One instance, 'Winpubvm', is highlighted with a blue selection bar. Below the table, there's a detailed view of 'Winpubvm' with tabs for Description, Status Checks, Monitoring, and Tags. Under the 'Description' tab, it shows Instance ID: i-0cb26994e13174e65, Instance state: running, and Instance type: t2.micro. In the 'Tags' section, there's a single tag: Name: Winpubvm. At the bottom of the instance card, it lists Public DNS (IPv4): 54.202.132.130 and IPv4 Public IP: 54.202.132.130. A mouse cursor is positioned over the 'Connect' button at the top of the instance card.

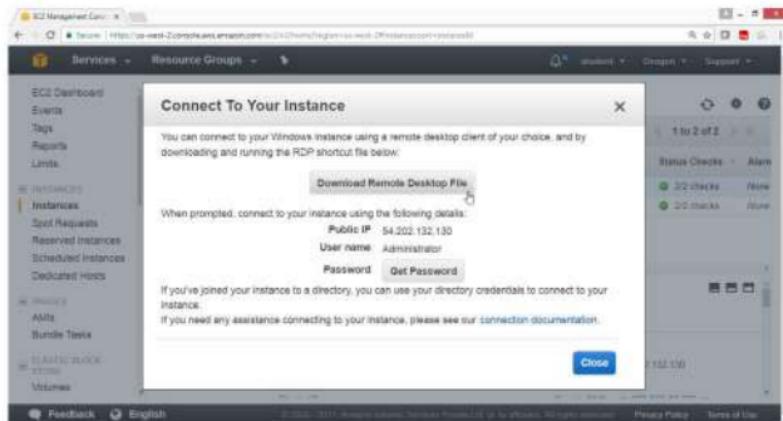
Click on "Connect" button



This screenshot is identical to the one above, showing the AWS EC2 Management Console with the 'Instances' page selected. The instance 'Winpubvm' is highlighted. The detailed view for 'Winpubvm' shows the same information: Instance ID: i-0cb26994e13174e65, Instance state: running, Instance type: t2.micro. The 'Tags' section is empty. The 'Description' tab shows Public DNS (IPv4): 54.202.132.130 and IPv4 Public IP: 54.202.132.130. A mouse cursor is hovering over the 'Connect' button.

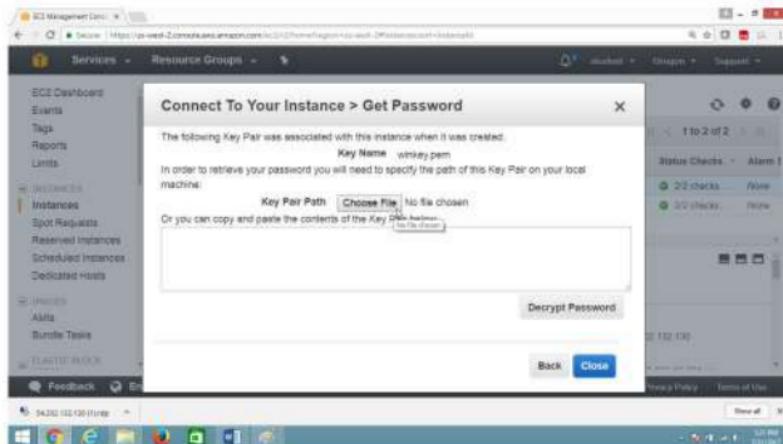
Click on "Download Remote Desktop file"

Click on "Get Password"



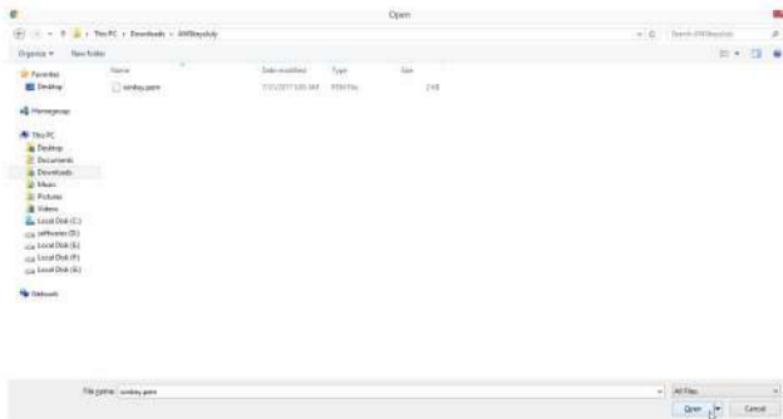
Provide the path of key file

Click on Choose file button



Select the key file

Click on **Open** button



Now click on "Decrypt Password" button:

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: Choose File winkey.pem

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

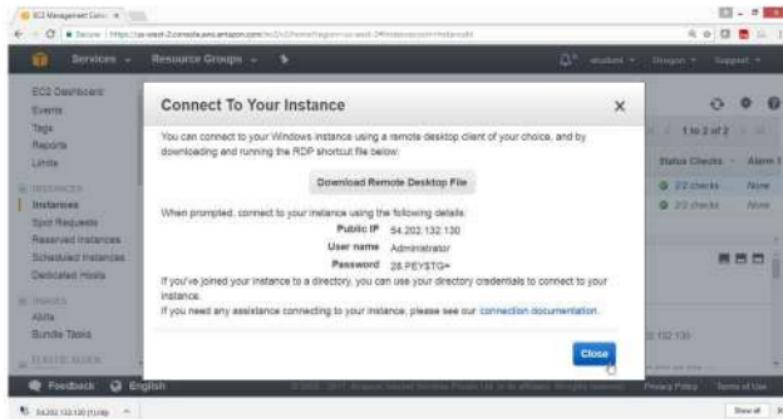
```
Q3XYW4UwptpHlTgk+ZEt9jZSxJjGZ5f9xpuLjrhTw9t1vSeNv54mM435UH+gM7bG9nAgCj5
f5597TvWwuhzDkG2OCo/mV+q1D/Prs9mnzWVApJQK9GjQxUvKvQq4Y73HJy72RqgwV
KwAjAcKoBjVjaD3OjAqKgmb2j7OryFnBun1MDW9hrImP+7fHkaQgDrWqjQ2jeA2
T89R6Ks100PjuzYe4BZevXK9p2j3jHu/ZBR88jRNcBCTjPeEcIeYYiQswnZjX
---END RSA PRIVATE KEY---
```

Decrypt Password

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 Management Console interface for the EC2 service. On the left, there's a sidebar with navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, and Elastic Block. The main area is titled 'Launch Instance' and shows a list of instances. There are two instances listed: 'Winpubvm' and 'Winpubsh'. Both instances are in the 'running' state with 2/2 checks green. Below the list, a specific instance is selected: 'Winpubvm' (i-0cb26994e13174685). Its details are displayed: Public IP: 54.202.132.130, Instance ID: i-0cb26994e13174685, Instance state: running, Instance type: t2.micro, Public DNS (IPv4): 54.202.132.130, IPv4 Public IP: 54.202.132.130, and PVIP: -.

Click on "Connect" button

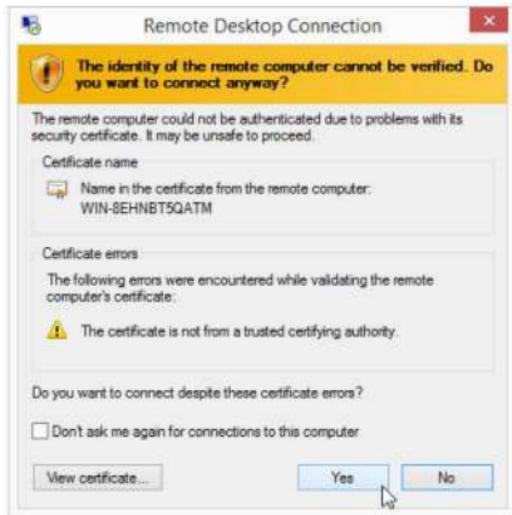


Paste the password

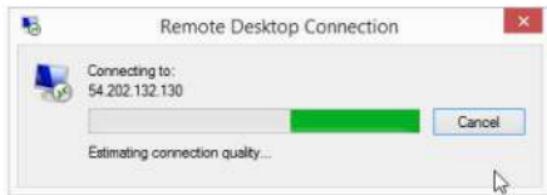
Click on **OK** button



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

The screenshot shows the AWS EC2 Management Console. On the left sidebar, under the 'INSTANCES' section, 'Instances' is selected. In the main content area, a table lists two instances: 'Winpvtm' and 'Winpvtm'. The 'Winpvtm' row is highlighted with a blue box. Next to the instance name is a 'Connect' button. The instance details pane shows 'Elastic IP' and 'Private DNS' (ip-192-168-20-87.us-west-2.compute.internal). Below that, it shows 'Private IPs' (192.168.20.87, 192.168.20.84). Other details like security groups, availability zone, and VPC ID are also listed.

Click on Connect button

This screenshot is identical to the one above, showing the AWS EC2 Management Console. The 'Winpvtm' instance is selected, and its details are shown in the pane. The 'Connect' button is now highlighted with a blue box, indicating it has been clicked. The rest of the interface remains the same, showing the sidebar and other instance details.

To get the password

Click on "Get Password" button



Click on "Decrypt Password"



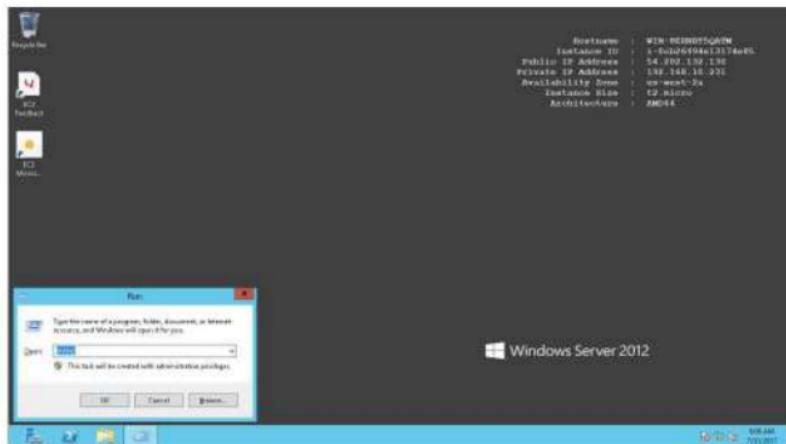
Verify

IP and password of private subnet instance is provided



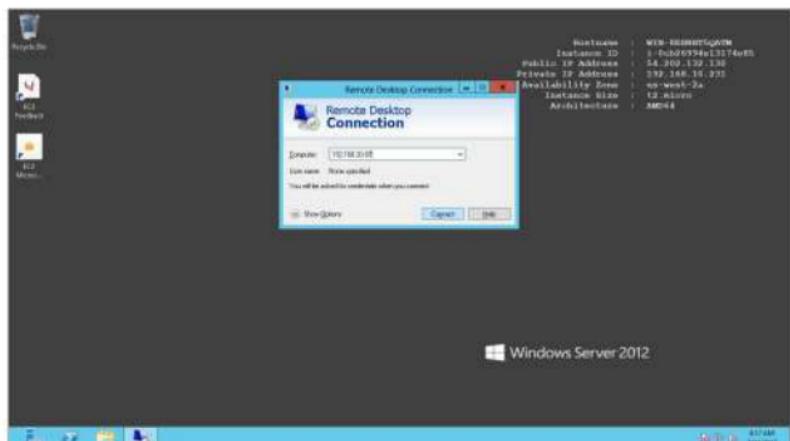
Now logging to public instance

Open Run and type mstsc to connect to window private instance

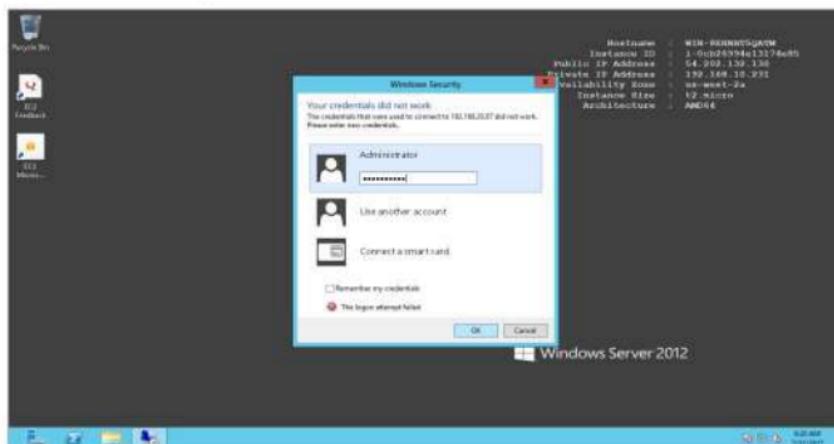


Provide private instance

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



Now Provide Username & password



Verification

Check private IP at Right top corner

Now you are connected to windows private instance.



11) To connect to linux instance in private subnet

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

Open the AWS console

Click on Services

Click on Instance

Click on "Launch Instance" button

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
Insider1	i-00115e0bd2b24f4	t2.micro	us-west-2c	terminated	None	None
win2008rm1	i-0a105aa100223084	t2.micro	us-west-2c	terminated	None	None
Wnpalben	i-0dc29944c1217a65	t2.micro	us-west-2a	running	2/2 checks	None
Wnpalvnm	i-0dc251927ae33fe0e	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

The screenshot shows the AWS Management Console interface for creating a new instance. The top navigation bar includes 'Services', 'Resource Groups', and several tabs like 'Configure Instance Type', 'Add Storage', 'Add Tags', 'Configure Security Groups', and 'Review'. Below the tabs, there's a 'Quick Start' section with links for 'My AMIs', 'AWS Marketplace', and 'Community AMIs'. The main content area displays a list of AMIs. One item, 'Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-6df1e514', is highlighted with a red box. To its right is a 'Select' button. Other items listed include 'SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami-e4d30984' and 'Ubuntu Server 17.04 (HVM), PVH (General Purpose) (x86_64)'. At the bottom of the page, there are links for 'Feedback', 'English', and various AWS policies.

On the "Choose an Instance Type" page

Select "General purpose"

Type → t2.micro

Click on "Next: Configure Instance Details"

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateNewInstanceStep2:t2.micro>. The page title is "Step 2: Choose an Instance Type". The "t2.micro" instance type is selected, highlighted with a green border. The table below lists various instance types with their details:

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>(Selected)</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
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
General purpose	t2.xlarge	4	16	EBS only	-	Medium	Yes

At the bottom, there are buttons for "Cancel", "Previous", "Review and Launch", and "Next: Configure Instance Details".

On the "Configure Instance Details" page

Number of instance → 1
Network → HYDVPC
Subnet → hyd-pub-subnet
Auto-assign Public IP → Enable

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/home?region=us-east-1#LaunchNewInstancesWizard>. The navigation bar includes Services, Resource Groups, student, Original, Support, and a search bar. Below the navigation, a progress bar shows Step 3: Configure Instance Details.

Step 3: Configure Instance Details

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

Form fields:

- Number of Instances: 1
- Purchasing option: Request Spot Instances
- Network: vpc-7d934d1b | HYDVPC (dropdown menu with Create new VPC option)
- Subnet: subnet-b33dbafe | hyd-pub-subnet | us-west-2a (dropdown menu with Create new subnet, 250 IP Addresses available option)
- Auto-assign Public IP: Enable
- IAM role: None (dropdown menu with Create new IAM role option)

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

On the "Add Storage" page

Leave the values as default

Click on "Next: Add Tags" button

Step 4: Add Storage

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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	SNAP-095e196a82ed7efc3	8	General Purpose SSD	100 / 3000	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New Volume

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

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

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

On the "Add Tags" page

Key → Name

Value → Linuxpubvbm

Click on "Next: Configure Security Group" button

The screenshot shows the AWS EC2 Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateNewInstances:step=5>. The top navigation bar includes 'Services', 'Resource Groups', 'Student', 'Groups', and 'Support'. Below the navigation, a progress bar shows steps 1 through 7, with step 5 highlighted. The main content area is titled 'Step 5: Add Tags'. It contains instructions: 'A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.' Below this, it says 'A copy of a tag can be applied to volumes, instances or both.' and 'Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.' There is a table with two rows:

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

Below the table is a button labeled 'Add another tag' with '(Up to 50 tags maximum)' next to it. At the bottom of the page are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is highlighted in blue), and 'Next: Configure Security Group'. The footer includes links for 'Feedback', 'English', '© 2006 - 2014 Amazon Internet Services LLC 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

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateLaunchWizard:6>. The navigation bar at the top has tabs: Services, Resource Groups, Configure Instance, Add Storage, Add Tags, Configure Security Group, and Review. Below the tabs, there's a sub-navigation: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. The main content area is titled "Step 6: Configure Security Group". A sub-instruction says: "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." There are two radio buttons: "Create a new security group" (selected) and "Select an existing security group". A dropdown menu for "Security group name" shows "launch-wizard-5". A text input field for "Description" contains "launch-wizard-5 created 2017-06-01T13:31:54.220+00:00". Below this, there's a table for defining a rule: "Type" (SSH), "Protocol" (TCP), "Port Range" (22), and "Source" (Anywhere). The "Source" dropdown shows "0.0.0.0/0". At the bottom right are "Cancel", "Previous", "Review and Launch" (highlighted in blue), and "Feedback" and "English" buttons.

On the "Review Instance Launch" page

Click on Launch button

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateLaunchWizard:7>. The navigation bar at the top has tabs: Services, Resource Groups, Configure Instance, Add Storage, Add Tags, Configure Security Group, and Review (selected). Below the tabs, there's a sub-navigation: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. The main content area is titled "Step 7: Review Instance Launch". A sub-instruction 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 yellow warning box contains: "⚠ 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." Below this, there's a section titled "AMI Details": "Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-6ddfe514". A "Launch" button is visible. At the bottom right are "Cancel", "Previous", "Launch" (highlighted in blue), and "Feedback" and "English" buttons.

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 AWS EC2 Management Console with the URL https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2&tab=instances#. The page displays the 'Launch Status' section, which includes instructions on how to connect to instances, helpful resources like the User Guide and Discussion Forum, and links for creating status check alarms, EBS volumes, and security groups. A prominent blue 'View Instances' button is located on the right side of the main content area.

Verification

Linux instance in public subnet is launched

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/instances?region=us-west-2>. The 'Instances' section is selected in the sidebar. The main pane displays a table of instances, with one row highlighted for 'Linuxputvm'. The details for this instance are shown in a modal dialog at the bottom:

Instance ID	Public DNS (IPv4)	IPv4 Public IP	IPv6 Public IP
i-0c5f560c48fb5f00	ec2-52-35-63-48.us-west-2.compute.amazonaws.com	54.202.241.190	-
Instance state	running	-	-
Instance type	t2.micro	-	-

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

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarms
Linuxpubvm	i-0c53f560c48ff3f80	t2.micro	us-west-2a	running	1/2 checks	None
Ubuntu1	i-08115409cd5247a	t2.micro	us-west-2c	terminated	0/2 checks	None
Windows	i-0cb9544e15174e60	t2.micro	us-west-2a	running	0/2 checks	None

Instance: i-0c53f560c48ff3f80 [Linuxpubvm] Public IP: 54.202.241.190

Description	Instance ID	Public DNS (IPv4)	Public IP (IPv4)
Instance ID	i-0c53f560c48ff3f80	54.202.241.190	54.202.241.190
Instance state	running	(PvB IP)	-
Instance type	t2.micro	(PvB IP)	-

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

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

Click on **Select** button

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

Cancel and Exit

My AMIs: My AMIs

AWS Marketplace: Amazon Linux

Community AMIs: Free tier only

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

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: /dev/sda1 Infrastructure type: t2.micro

Select

SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami-0a2f333c

Select

Feedback English

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

Show off X

On the "Choose an Instance Type" page

Select "General purpose"

Type → t2.micro

Click on "Next: Configure Security Group" button

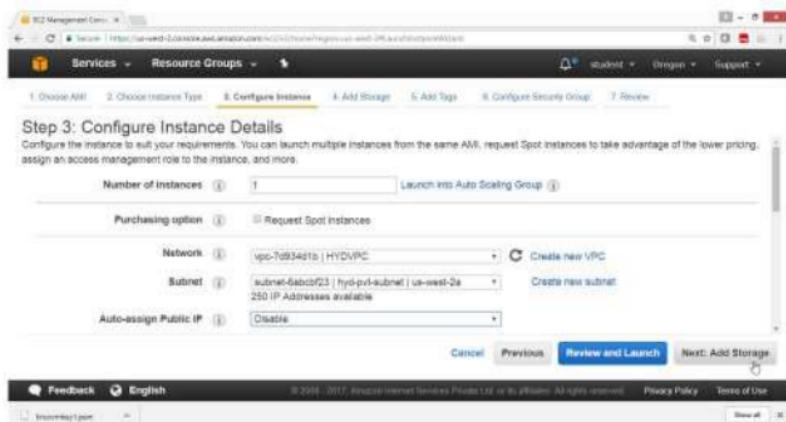
Step 2: Choose an Instance Type

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>(Cross-region replicated)</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
General purpose	t2.large	7	8	EBS only	-	Low to Moderate	Yes

Cancel Previous Review and Launch Next: Configure Security Group

On the "Configure Instance Details" page

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



On the "Add Storage" page

Leave the values as default

Click on "Next: Add Tags" button

Step 4: Add Storage

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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (Mbps)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-0de1b56a02ed7efc3	8	General Purpose	100 / 3000	N/A	Selected	Not Encrypted

Add New Volume

Cancel Previous Review and Launch Next: Add Tags

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

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 (1)	Volumes (1)
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 © 2006 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use Show off X

On the "Add Tags" page

Key → Name

Value → Linuxpvvm

Click on "Next: Configure Security Group" button

The screenshot shows the AWS EC2 Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateNewInstance:step=5>. The top navigation bar includes 'Services', 'Resource Groups', 'Student', 'Groups', 'Support', and tabs for '1. Choose AMI', '2. Choose Instance Type', '3. Configure Instance', '4. Add Storage', '5. Add Tags' (which is highlighted in yellow), '6. Configure Security Group', and '7. Review'. The main content area is titled 'Step 5: Add Tags'. It contains instructions: 'A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.' Below this, it says 'A copy of a tag can be applied to volumes, instances or both.' and 'Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.' There is a table with two rows:

Key	(127 characters maximum)	Value	(255 characters maximum)	Instances	Volumes
Name	Linuxpvvm				

Below the table is a button labeled 'Add another tag' with the note '(Up to 50 tags maximum)'. At the bottom of the page are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is blue), and 'Next: Configure Security Group'. The footer includes links for 'Feedback', 'English', '© 2006 - 2014 Amazon Internet Services LLC 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: launch-wizard-6

Description: launch-wizard-6 created 2017-08-01T13:51:38.871+05:30

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

Add Rule Cancel Previous Review and Launch

On the "Review Instance Launch" page

Click on Launch button

Step 7: Review Instance Launch

Security group name: launch-wizard-6

Description: launch-wizard-6 created 2017-08-01T13:51:38.871+05:30

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

Instance Details Edit instance details
Storage Edit storage
Tags Edit tags

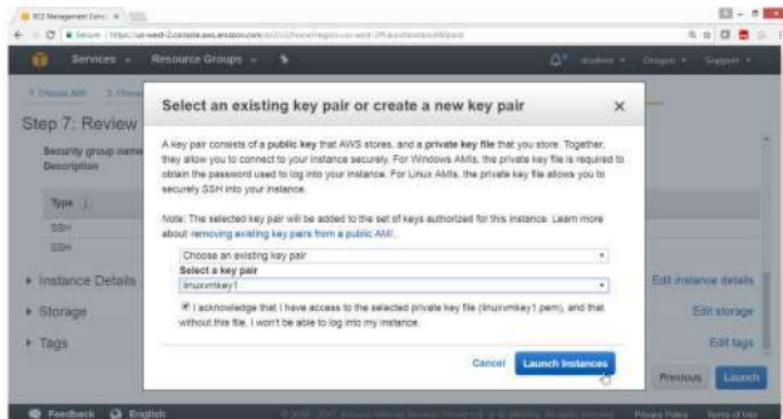
Cancel Previous Launch

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

Select **Create a new key pair**

Key pair name → linuxvmlinkey1

Click on "Launch Instance" button



Check the summary

Click on View Instance button

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchStatus>. The page title is "Launch Status". It displays a summary of instance creation status: "Your instances are launching" with 4 instances in progress. Below this, there's 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", and "Amazon EC2 Discussion Forum". A note says "Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)." Another note says "Create and attach additional EBS volumes. (Additional charges may apply)." There's also a link to "Manage security groups". At the bottom right is a blue "View Instances" button.

Verification

Linux instance in public subnet is launched

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances>. The page title is "Instances". On the left sidebar, under "INSTANCES", the "Launch Instance" button is highlighted. The main table lists five instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
Vm1pvtvm	i-00251025e00f9fa4e	t2.micro	us-west-2a	running	2/2 checks
Vm2pvtvm	i-03d2094e13f14465	t2.micro	us-west-2a	running	2/2 checks
Linuxpvtvm	i-0da6594c71079c242	t2.micro	us-west-2a	running	2/2 checks
Umsazpvtvm	i-0cd3f560c40d8fb0	t2.micro	us-west-2a	running	2/2 checks

The instance **Linuxpvtvm** is selected. The details panel at the bottom shows:

Description	Status Checks	Monitoring	Tags
Instance ID: i-0da6594c71079c242	Public DNS (IPv4):		
Instance state: running	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
Linuxpriv	i-0aa8504c71678c242	t2.micro	us-west-2a	running	2/2 checks	None
Winpubvm	i-0d20094e13174e6b	t2.micro	us-west-2a	running	2/2 checks	None
Winprivvm	i-0e226fb25ew03t6fe	t2.micro	us-west-2a	running	2/2 checks	None

View the guide lines

The screenshot shows the AWS Management Console with the EC2 Management Service selected. A modal window titled "Connect To Your Instance" is open. It asks if you want to connect with a "standalone SSH client" or a "Java SSH Client directly from my browser (Java required)". Below this, instructions for connecting via PuTTY are provided, including steps to locate the private key file ("linuxvmkey1.pem") and its location ("54.202.243.196"). An example command is shown: "ssh -i \"linuxvmkey1.pem\" ec2-user@54.202.243.196". A note at the bottom states: "Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage-instructions to ensure that the AMI owner has not changed the default AMI username." On the right side of the screen, there is a sidebar with "Status Checks" and "Alarms" sections.

Use the above public ip of linux instance in mobaxterm

Copy *.pem file to puun 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@54.202.243.196:/home/ec2-user
linuxvmkey1.pem                                         100% 1692     1.7KB/s  00:00

[2017-08-01 14:21:50] /drives/e/awskeys
[shaikh.pc_Mas] *
```

Verify

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

```
[2017-08-01 14:22:27] /drives/e/mwskeys
[shaikh.pc_Mas] ~ pwd
/drives/e/mwskeys

[2017-08-01 14:22:29] /drives/e/mwskeys
[shaikh.pc_Mas] ~ ls
dmc.mp3      linuxvmkey1.pem  putty.exe      puttygen.exe  winkey.pem

[2017-08-01 14:22:30] /drives/e/mwskeys
[shaikh.pc_Mas] ~ [ ]
```

Now connect to public instance using ssh command

```
[2017-08-01 14:22:43] /drives/e/mwskeys
[shaikh.pc_Mas] ~ ssh -i "linuxvmkey1.pem" ec2-user@54.202.241.190
X11 forwarding request failed on channel 0
Last login: Tue Aug  1 08:50:19 2017 from 183.62.211.216
[ec2-user@ip-192-168-10-197 ~]$
```

Select private instance and get private ip

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Linuxptm	i-0c30502c48026f50	t2.micro	us-west-2a	running	2/2 checks	None
Linuxptvm	i-0de8594c71079c242	t2.micro	us-west-2a	running	2/2 checks	None
Wingptm	i-0d03094a13174e65	t2.micro	us-west-2a	running	2/2 checks	None
Wingptvm	i-0225fb2525e00fe4e	t2.micro	us-west-2a	running	2/2 checks	None

Instance: i-0de8594c71079c242 (Linuxptvm) Private IP: 192.168.20.101

Description Status Checks Monitoring Tags

Instance ID: i-0de8594c71079c242 Public DNS (IPv4):
Instance state: running IPv4 Public IP:
Instance type: t2.micro IPv6 IPs:

View the details of private instance

To access your instance:

1. Open an SSH client. (Find out how to connect using PUTTY)
2. Locate your private key file (LinuxKey1.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 LinuxKey1.pem`
4. Connect to your instance using its Private IP:
`192.168.20.101`

Example:

```
ssh -i "LinuxKey1.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.

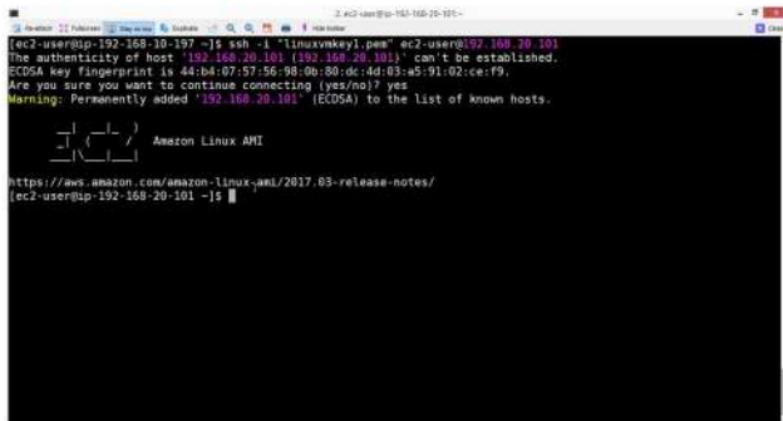
If you need any assistance connecting to your instance, please see our connection documentation.

Close

Verification

Run ssh command to login to private instance

Now you are connected to private instance in private subnet



The screenshot shows an SSH terminal window titled "Terminal" with the command "ssh -i "linuxvmkey1.pem" ec2-user@192.168.20.101". The output shows a warning about host key fingerprint and a prompt to continue connecting. The user types "yes" and the connection is established. The banner "Amazon Linux AMI" is visible at the bottom of the terminal.

```
[ec2-user@ip-192-168-10-197 ~]$ ssh -i "linuxvmkey1.pem" ec2-user@192.168.20.101
The authenticity of host '192.168.20.101 (192.168.20.101)' can't be established.
ECDSA key fingerprint is 44:b4:07:57:56:98:06:80:dc:d4:03: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.

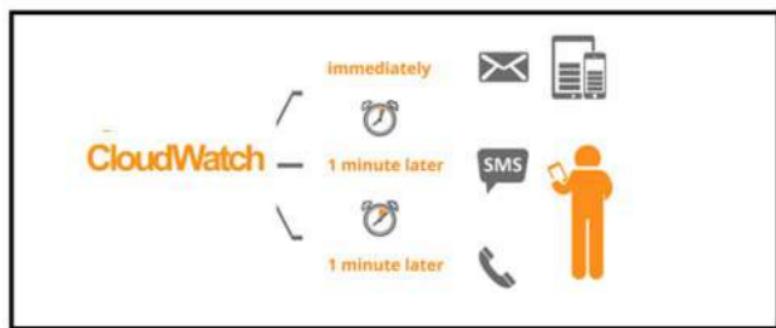
[ec2-user@ip-192-168-20-101 ~]$ 
```

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

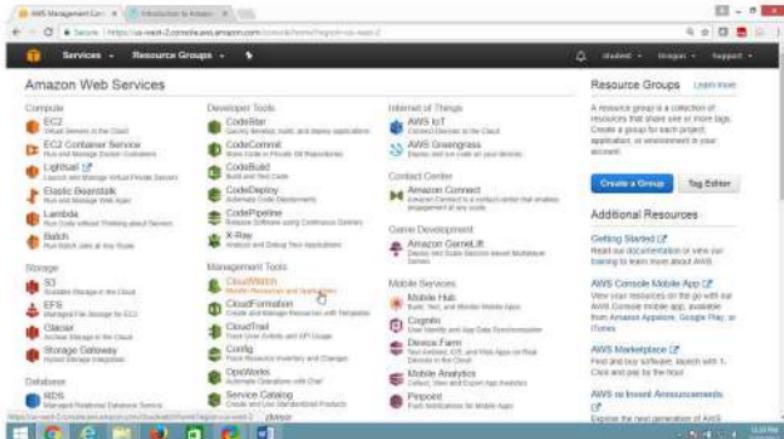
Launch a Amazon linux instance, then

[Open AWS Console](#)

Click on Services

In the Management Tools section

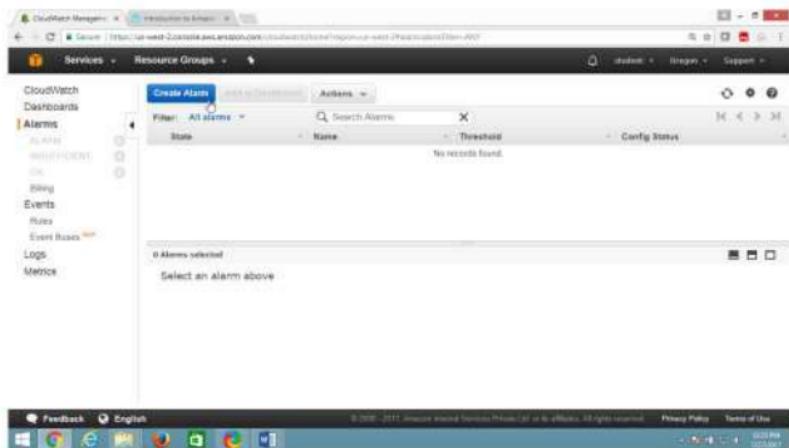
Click on CloudWatch



On "CloudWatch", panel

Select **Alarms**.

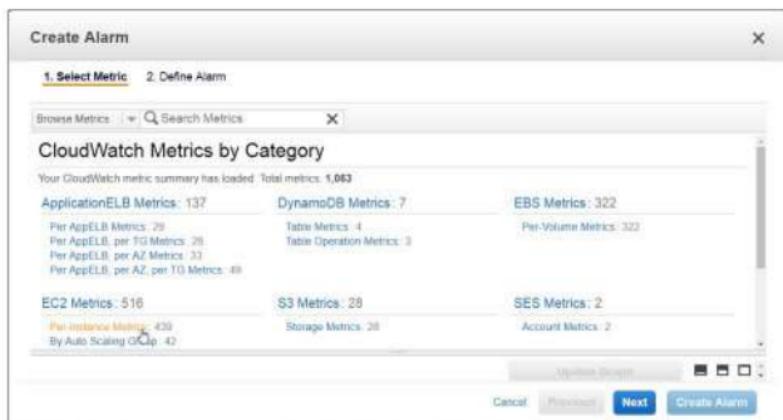
Click on "Create Alaram" button



In "Create Alarm" page

Select "EC2 Metrics"

Click on "Per-instance Metrics"



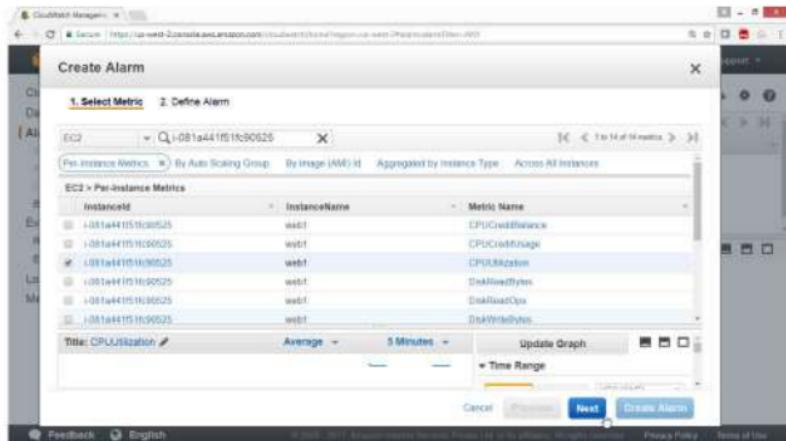
From "Create Alarm" page

Select "1. Select Metric"

In search box provide instance ID or Name

Under Metric Name, select **CPUUtilization** checkbox

Click on **Next** button



On **Create Alarm** page

Select “**2. Define Alarm**”

Under **Alarm Threshold**

Name → testcpuutilization

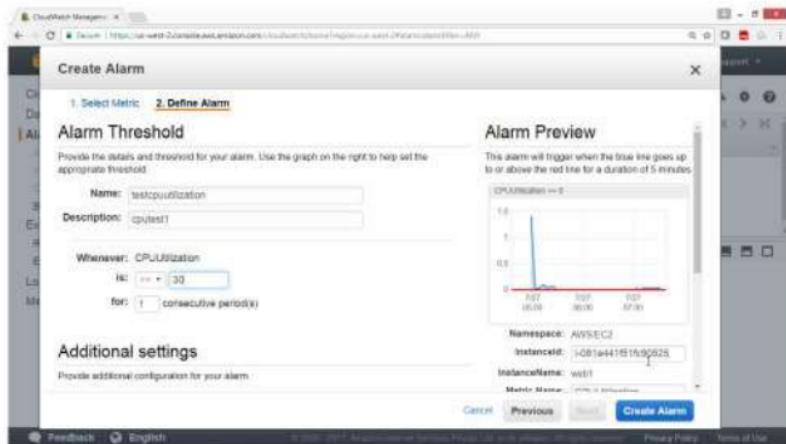
Description → cputest

Under Whenever CPUUtilization

is \geq **30**

for **1** consecutive periods

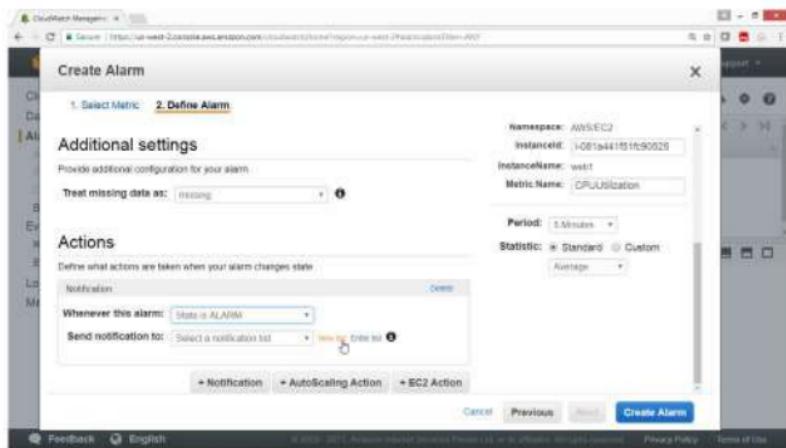
Drag Down



Under Actions

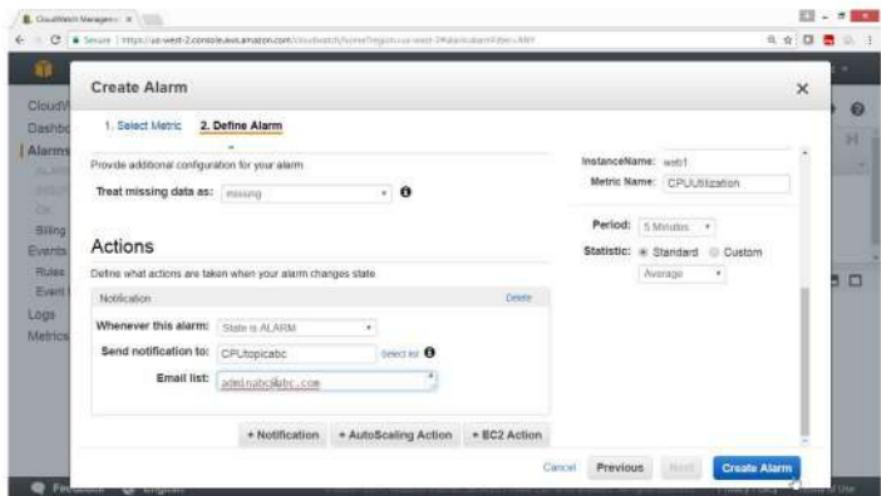
Whenever this alarm → State is Alaram

Send notification to → Click on New list

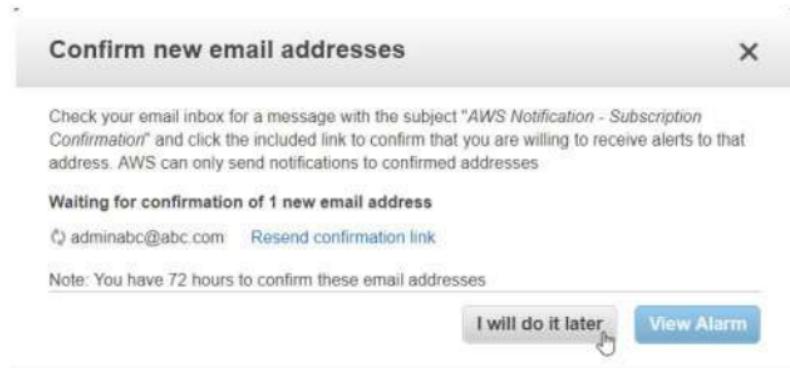


Send notification to → CPUtopicabc
Email → adminabc@abc.com

Click on "Create Alaram" button



Click on "I will do it Later" button.



Go to your Email account and check the Mail

Once mail is been checked

Config status → Pending confirmation

Verify the link from your Email

The screenshot shows the AWS CloudWatch Metrics Metrics Explorer. On the left sidebar, under 'Alarms', there is a single entry: 'testcpuutilization'. The main pane displays a success message: 'Your alarm testcpuutilization has been saved.' Below this, there is a table with one row:

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

At the bottom of the main pane, it says 'Select an alarm above'.

Open your email

The screenshot shows a Gmail inbox with 166 messages. The top navigation bar includes a search bar, a notifications icon, and a user profile icon. The inbox header shows tabs for Primary, Social, Promotions, and Subscriptions. The 'Inbox (113)' tab is selected. A prominent yellow banner at the top of the inbox area reads: 'Click here to enable desktop notifications for Gmail. Learn more Hide'. Below the banner, the inbox lists several emails, with the first one being an 'AWS Notification' from 'AWS Notification - Subscript' at '1:26 pm'.

Click on "Confirm subscription"

=====

AWS Notification - Subscription Confirmation Inbox x

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

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

=====

The screenshot shows an email from Amazon Web Services. The subject is "Simple Notification Service". The body of the email contains the following text:

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

The screenshot shows the AWS CloudWatch Metrics Metrics Explorer interface. On the left, there is a sidebar with navigation links: CloudWatch, Dashboards, Alarms, Metrics, Logs, Event Buses, Metrics (selected). The main area displays a success message: "Your alarm testcpuutilization has been saved." Below this, there is a "Create Alarms" button and a search bar. A table lists the alarm configuration:

Filter	Status	Name	Threshold	Config Status
All alarms	OK	testcpuutilization	CPUUtilization >= 20	for 5 minutes

At the bottom, there is a note: "0 Alarms selected" and a placeholder text: "Select an alarm above".

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 user, 0.0 nice, 0.0 sys, 100.0 idl, 0.0 iow, 0.0 hi, 0.0 si, 0.0 st
Mem: 1817372k total, 166080k used, 151292k free, 9224k buffers
Swap: 0k total, 0k used, 0k free, 98380k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S %CPU	WCHAN	TIME+ COMMAND
1	root	20	0	19628	2420	2100	5	0.0	0:00.00 init
2	root	20	0	0	0	0	5	0.0	0:00.00 kthreadd
3	root	20	0	0	0	0	5	0.0	0:00.00 ksoftirqd/0
4	root	20	0	8	0	0	5	0.0	0:00.00 kworker/0:0
5	root	0	-20	0	0	0	5	0.0	0:00.00 kworker/0:0H
6	root	20	0	0	0	0	5	0.0	0:00.00 kworker/u30:0
7	root	20	0	0	0	0	5	0.0	0:00.00 rCU sched
8	root	20	0	0	0	0	5	0.0	0:00.00 rCU_bh
9	root	RT	0	0	0	0	5	0.0	0:00.00 migration/0
10	root	0	-20	0	0	0	5	0.0	0:00.00 lru-add-drain
11	root	20	0	0	0	0	5	0.0	0:00.00 cpuhp/0
12	root	20	0	0	0	0	5	0.0	0:00.00 kdevtmpfs
13	root	0	-20	0	0	0	5	0.0	0:00.00 netns
16	root	20	0	0	0	0	5	0.0	0:00.01 xenwatch
17	root	20	0	0	0	0	5	0.0	0:00.02 kworker/u30:2
21	root	20	0	0	0	0	5	0.0	0:00.00 xenbus
139	root	20	0	0	0	0	5	0.0	0:00.00 khungtaskd
140	root	20	0	0	0	0	5	0.0	0:00.00 oom_reaper
141	root	0	-20	0	0	0	5	0.0	0:00.00 writeback
143	root	20	0	0	0	0	5	0.0	0:00.00 kcompactd0
144	root	25	5	0	0	0	5	0.0	0:00.00 ksm
145	root	39	19	0	0	0	5	0.0	0:00.00 khugepaged
146	root	0	-20	0	0	0	5	0.0	0:00.00 crypto
147	root	0	-20	0	0	0	5	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: 344 total, 41 running, 103 sleeping, 0 stopped, 0 zombie										
Cpu(s): 100.0%us, 0.0sy, 0.0ni, 0.0id, 0.0wa, 0.0hi, 0.0si, 0.0st										
Mem: 191x/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	0:00.73 stress
3147	root	20	0	7260	96	0	R	2.7	0.0	0:00.73 stress
3179	root	20	0	7260	96	0	R	2.7	0.0	0:00.73 stress
3141	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3142	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3144	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3145	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3146	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3148	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3149	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3150	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3151	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3152	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3153	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3154	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3155	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3156	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3157	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3158	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3159	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3160	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3161	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3162	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress
3163	root	20	0	7260	96	0	R	2.3	0.0	0:00.72 stress

Go to CloudWatch service

Check the status

The screenshot shows the AWS CloudWatch Metrics Dashboard. 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 'Temperature' with a red line graph showing values from 0 to 40 over time from 07:00 to 09:00. The chart shows a sharp spike from approximately 35 to 40 at 08:00. Below the chart, it says 'All your alarms are in OK state in US West (Oregon) region.' and there is a 'Create Alarm' button. The 'Service Health' section shows a green status icon for 'Amazon CloudWatch Metrics Service' with the message 'Service is operating normally'. 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, showing the CloudWatch Metrics Dashboard. The only difference is the status of the 'Amazon CloudWatch Metrics Service' in the 'Service Health' section, which has turned red and now says 'Service is temporarily unavailable'. This indicates that an alarm was triggered and the service became unhealthy due to the metric threshold being crossed.

Go to email and check mail

The screenshot shows a Gmail inbox with 113 messages. The interface includes a search bar at the top with a notification icon and a link to enable desktop notifications. Below the search bar are buttons forCompose, More, and settings. The inbox list shows two messages from "AWS Notifications": one titled "ALARM: 'testcpuutilization' in US West - Oregon" and another titled "AWS Notification - Subscription Confirmation". Both messages were sent at 2:39 pm.

Click on mail

Verify output

=====

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

You are receiving this email because your Amazon CloudWatch Alarm "testcpuutilization" 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=testcpuutilization>

Alarm Details:

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

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

Threshold:

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

Monitored Metric:

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

State Change Actions:

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

↳ State Change Actions:

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

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

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

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

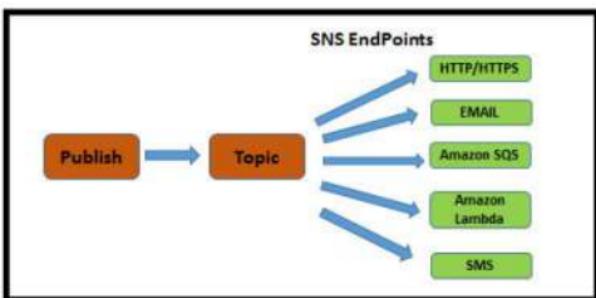
===== END OF OUTPUT =====

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

OBJECTIVE

To configure Amazon Simple Service (SNS)

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with AmazonSNSFullAccess

TASK :

Create a Topic

Subscribe your topic

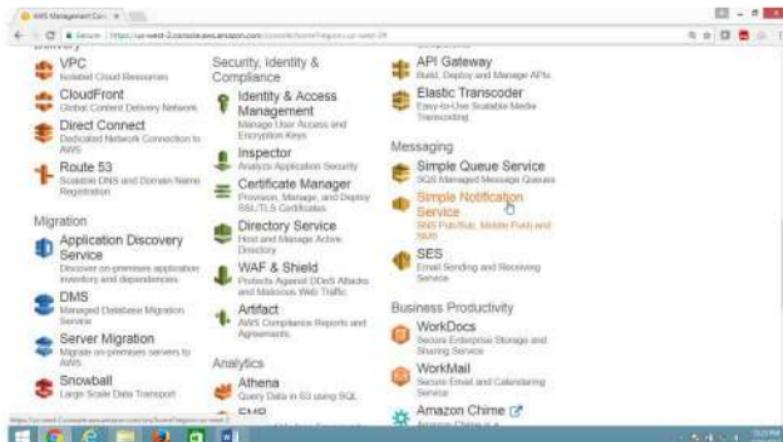
Verify in your mail account

1) To configure Amazon Simple Notification Service (SNS)

Open AWS console

Select "Messaging" service

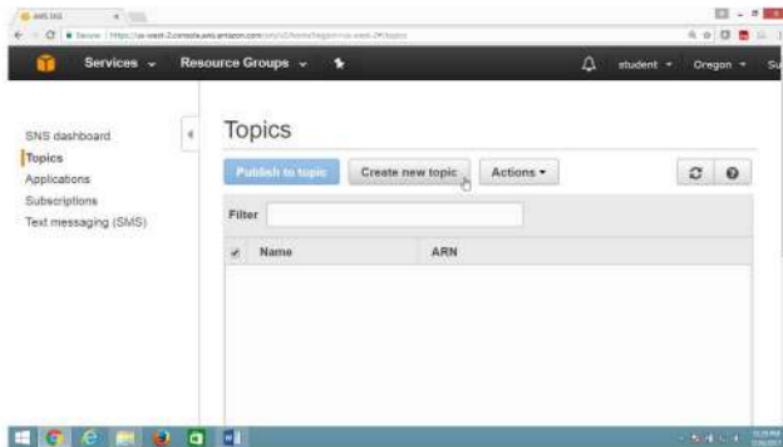
Click on "Simple Notification service"



From "SNS Dashboard" panel

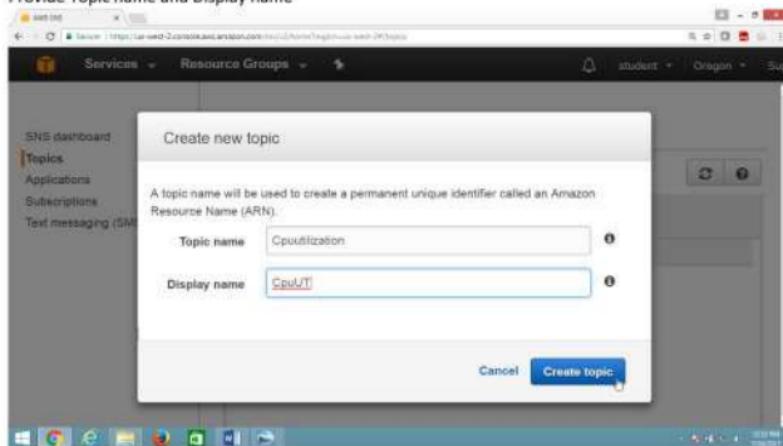
Select Topic

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 of the 'Cpuutilization' topic, which is `arn:aws:sns:us-west-2:523251680217:Cpuutilization`. The ARN is also copied to the clipboard.

2) To create Subscription

Click on "Createsubscription" button

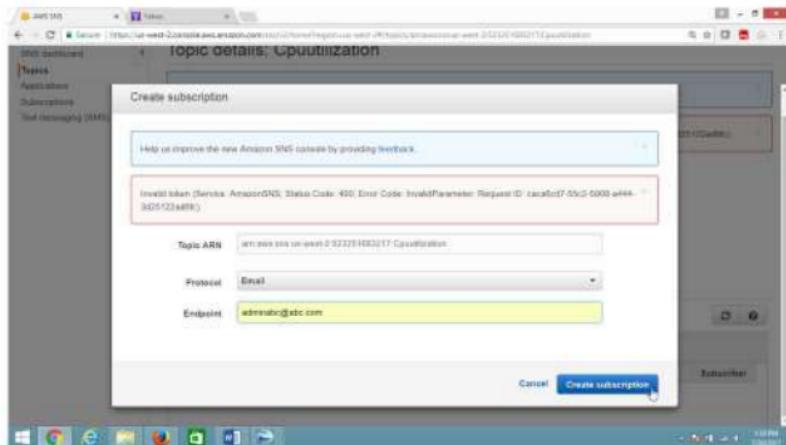
The screenshot shows the AWS SNS Topic details page for the 'Cpuutilization' topic. A red box highlights the 'Create subscription' button. Below it, the topic's ARN is listed as `arn:aws:sns:us-west-2:523251680217:Cpuutilization`.

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 Lambda console with the URL <https://us-west-2.console.aws.amazon.com/lambda/functions/us-west-2%3A2916822117%3Aoptimization>. The region is set to us-west-2 and the display name is 'CPU/IT'. The 'Subscriptions' tab is selected, showing a single entry: 'PendingConfirmation' with a status of 'Pending'. The protocol is 'email' and the endpoint is 'alarm@zoomgroup.com'. There are tabs for 'Create subscription', 'Request confirmation', 'Confirm subscription', and 'Other subscription actions'.

Go to your mail account

Click on the mail

The screenshot shows a Gmail inbox with 1 unread message. The subject of the message is 'AWS Notification - Subscription Confirmation'. The message body contains a confirmation link: <http://cavut.us-west-2.2916822117.optimization>. The message was sent at 10:54 AM (1 minute ago).

Click on "Confirm message"

The screenshot shows an email message from 'aws-lambda@amazonaws.com' to 'alarm@zoomgroup.com'. The subject is 'AWS Notification - Subscription Confirmation'. The message body contains the same confirmation link: <http://cavut.us-west-2.2916822117.optimization>. Below the link, there is a note: 'You have chosen to subscribe to the topic us-west-2.2916822117.optimization'. It also says 'To confirm this subscription, click or visit the link above (if this link is broken no action is necessary)' and 'Confirm subscription'. At the bottom, it says 'Please do not reply directly to this email. If you wish to remove yourself from receiving all future AWS subscription confirmation requests please send an email to aws-lambda@amazonaws.com'.

Now subscription is verified

The screenshot shows the AWS Lambda console interface. At the top, there's a navigation bar with tabs like 'Lambda functions', 'Topics', 'Logs', etc. Below the navigation, there's a search bar and a 'Create new' button. The main area has two sections: 'Topic configuration' and 'Subscriptions'.

Topic configuration:

- Publish to topic** (button)
- Other topic actions** (dropdown menu)
- Topic ARN:** arn:aws:sns:us-west-2:523251683217:CpuUtilization
- Topic owner:** 023291683217
- Region:** us-west-2
- Display name:** CpuUtil

Subscriptions:

- Create subscription** (button)
- Request confirmations** (button)
- Confirm subscription** (button)
- Other subscription actions** (dropdown menu)

A 'Filter' input field is present above the subscription list. The subscription list table has columns: **Subscription ID**, **Protocol**, **Endpoint**, and **Status**. One row is visible in the table:

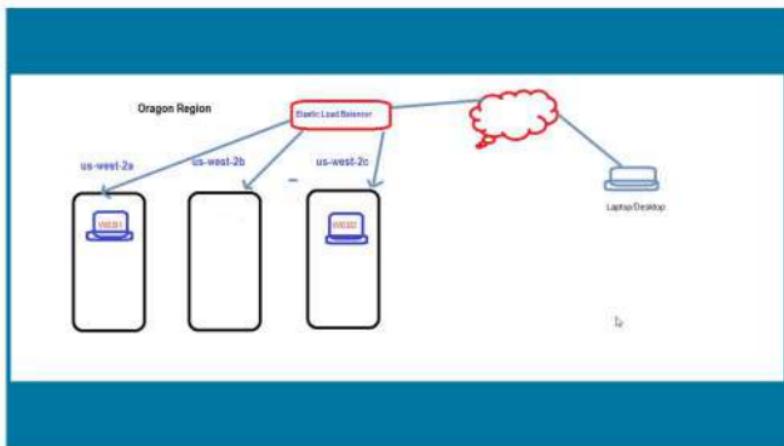
Subscription ID	Protocol	Endpoint	Status
arn:aws:sns:us-west-2:523251683217:CpuUtilization b5ff80a3-4831-405e-b5e1-a37209c3...	email	skr:52...	Subscribed

Lab 12: To Configure Amazon Elastic Load Balancer

OBJECTIVE

To configure Elastic load balancer in AWS

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

TASK :

Launch two instance in two separate Availability Zone.

Configure httpd (Apache) webserver in each instances.

Verify Webserver from browser.

Configure Elastic Load Balancer.

Verify Webserver through ELB

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

Note

[To configure webserver refer lab – webserver configuration]

- 2) Check websites are running**

Open the browser

Provide public ip of both instances

Verify both website are running.

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

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

Description	Status Checks	Monitoring	Tags
i-081a441f51fc90525 ec2-54-218-192-19.us-west-2.compute.amazonaws.com			
i-090dfbcc632605047: ec2-54-203-189-110.us-west-2.compute.amazonaws.com			

Verify Public IP of both instance

The screenshot shows the AWS EC2 Management Console. The left sidebar has sections for Services, Resource Groups, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Travis CI, and Elastic Block Store. Under Instances, it lists two instances: i-081a441f1fc90525 (web1) and i-090dfbcc8320805047 (web2). Both instances are running, with 2/2 checks and no alarms. Their public DNS and IPv4 addresses are listed: web1 has ec2-54-218-150-19.us-west-2.compute.amazonaws.com and 54.218.182.19; web2 has ec2-54-203-189-115.us-east-2.compute.amazonaws.com and 54.203.189.115. The bottom of the screen shows the AWS navigation bar with Feedback, English, and links to Support, Privacy Policy, and Terms of Use.

Verify

Output of Webserver one



Verify

Output of Webserver two



3) To Configure Elastic Load Balancer.

Open the AWS console.

On **EC2 Dashboard** panel

Expanding “**LOAD BALANCING**”

Select **Load Balancer**,

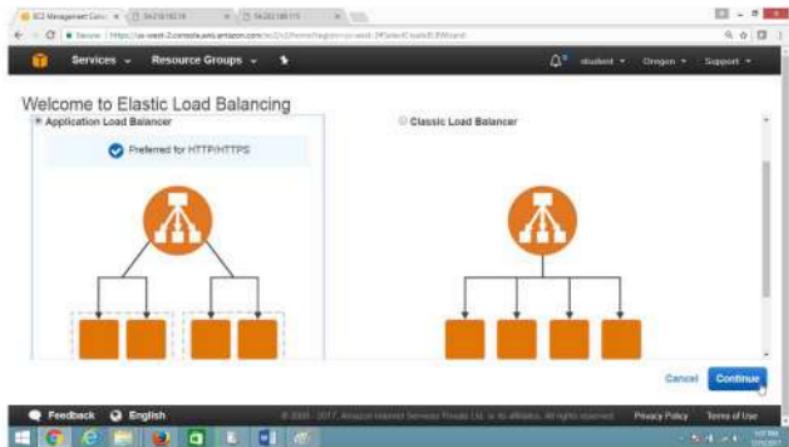
Click on “**Create Load Balancer**” button



On "Welcome to Elastic Load Balancing" page

Select "Application Load Balancer",

Click Continue button



On "Configure Load Balancer" page:

Provide

Name → ELBsales

Schema → Internet-facing

Drag down

The screenshot shows the AWS Lambda console with the URL <https://lambda.console.aws.amazon.com/functions/configureLoadBalancer?functionName=ELBsales&stageName=prod>. The page is titled "Configure Load Balancer" and is part of a multi-step wizard. Step 1: Configure Load Balancer is currently selected. The configuration section includes fields for Name (ELBsales), Scheme (Internet-facing), and IP address type (IPv4). Below this, a "Listeners" section is visible, though it appears empty. At the bottom right, there 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: HTTP Load Balancer Port: 80

Add listener

Availability Zones

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

Cancel Next: Configure Security Settings

Under Availability Zones

Select all zones

Click on "Next:Configure Security Settings" button

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

Availability Zone	Subnet ID	Subnet IPv4 CIDR	Name
us-west-2a	subnet-1390e5a	172.31.32.0/20	
us-west-2b	subnet-5b9e30ec	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 for the AWS Management Console. The URL is https://us-west-2.console.aws.amazon.com/elbv2/CreateLoadBalancer?wizard=2#ConfigureSecurityGroups. The page title is "Step 2: Configure Security Settings". There are several tabs at the top: 1. Configure Load Balancer, 2. Configure Security Groups (which is active), 3. Configure Security Groups, 4. Configure Routing, 5. Register Targets, and 6. Review. Below the tabs, there is a warning message: "⚠ Improve your load balancer's security. Your load balancer is not using any secure listener. 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 main content area, there are "Cancel", "Previous", and "Next: Configure Security Groups" buttons. The status bar at the bottom of the browser window shows "Feedback English © 2018 Amazon Internet Services Private Limited. All rights reserved Privacy Policy Terms of Use".

On "Configure Security Groups" page.

Under Assign a security group

Select "Create a new security group"

click on Configure Routing button

The screenshot shows the AWS Management Console interface for configuring a security group. The top navigation bar includes 'Services', 'Resource Groups', and tabs for 'Configure Load Balancer', 'Configure Security Settings', 'Configure Security Groups' (which is the active tab), 'Configure Routing', 'Register Targets', and 'Review'. Below the tabs, the title 'Step 3: Configure Security Groups' is displayed, followed by a sub-instruction: 'A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.' Under 'Assign a security group:', the radio button for 'Create a new security group' is selected. The 'Security group name:' field contains 'load-balancer-wizard-2'. The 'Description:' field shows 'load-balancer-wizard-2 created on 2017-07-28T12:35:42.009+00:00'. A table lists a single rule: 'Type: Custom TCP Rule', 'Protocol: TCP', 'Port Range: 80', and 'Source: Custom 0.0.0.0/0'. At the bottom right, there are 'Cancel', 'Previous', and 'Next: Configure Routing' buttons. The bottom of the screen shows the Windows taskbar with various icons and the system tray.

ON "Configure Routing" page give following values

Name → Websales

Leave remaining values as default

click "Next: Register Targets" button

Step 4: Configure Routing

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

Target group

Target group	New target group...
Name	WebSales
Protocol	HTTP
Port	80

Health checks

Protocol	HTTP
Path	

Cancel Previous Next: Register Targets

On Register Targets page, Drag down

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

Click on “Add to register” button, Drag down

Instance	Name	State	Security group	Zone	Subnet ID	Subnet CIDR
10819a441515... +090d9cc532695047	web1 web2	running running	launch-wizard-5 launch-wizard-6	us-west-2a us-west-2c	subnet-1380e6fa subnet-1960f141	172.31.32.0/20 172.31.0.0/20

Verify that running instances are registered.

Click on “Next: Review” button

Instance	Name	Port	State	Security group	Zone
10819a441515... +090d9cc532695047	web1 web2	80	running running	launch-wizard-5 launch-wizard-6	us-west-2a us-west-2c

Verify

Check the summary

Drag Down

Step 6: Review

Please review the load balancer details before continuing.

Load balancer

Name: ELSales
Scheme: internet-facing
Listeners: Port 80 - Protocol: HTTP
IP address type: IPv4
VPC: ip-10-20-241-102 (default-vpc-oregon)
Subnets: subnet-123e01fa, subnet-98be36ec, subnet-19d0f141
Tags

Security settings

Certificate name
Security policy name

Create

Click on "Create" button

Step 6: Review

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

Targets

Instances: i-031a441fb9b90525 (web1):80, i-090dfbcc63280047 (web2):80

Create

Verify

Load balancer successfully created.

The screenshot shows a browser window with the AWS CloudFront Management Console URL: https://us-west-2.console.aws.amazon.com/cloudfront/home?region=us-west-2&id=ZGZlLwDQJw&tab=overview. The page displays a success message: "Successfully created load balancer". It states that the load balancer "ElBlaies" was successfully created and provides a note: "Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks." A "Close" button is visible at the bottom right of the message box.

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
ELBsample	ELBs-sample-123441202.us-west-2.elasticloadbalancing.amazonaws.com (A Record)	provisioning	vpc-89c341ee

ARN: arn:aws:elasticloadbalancing:us-west-2:523261683217:loadbalancer/app/ELBs-sample-123441202
Hosted zone: Z1H1FLSHABSP5
DNS name: ELBs-sample-123441202.us-west-2.elasticloadbalancing.amazonaws.com (A Record)
VPC: vpc-89c341ee
Scheme: internet-facing
IP address type: ipv4
Type: application
AWS WAF Web ACL:
Availability: subnet-1230feta - us-west-2a

In browser type load balancer DNS name

Verify website by frequently refreshing browser (press F5)



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



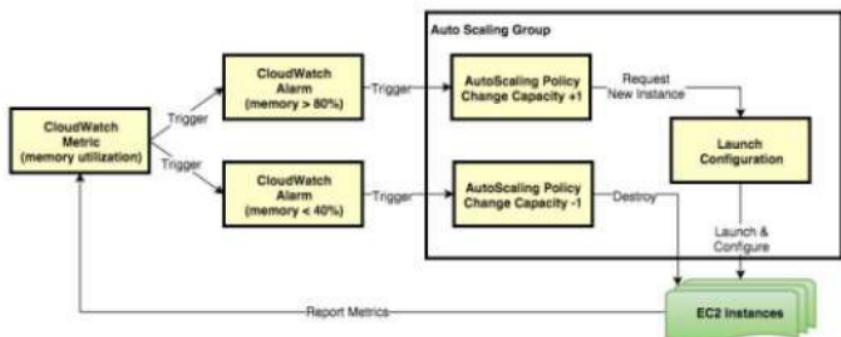
If you get this output, Congratulation your ELB configuration is successful.

Lab 13: To Configure Auto Scaling With Load Balancer

OBJECTIVE

To configure Auto Scaling in AWS

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with EC2fullaccess

TASK

Launch Amazon linux instance

Configure web server

Stop the instance

Create AMI image of above instance

Configure Autoscaling launch configuration and autoscaling group

Configure Load balancer with Autoscaling

Practical Steps

1) First launch Amazon linux Instance and configure webserver

2) Create AMI image

To create AMI from this instance

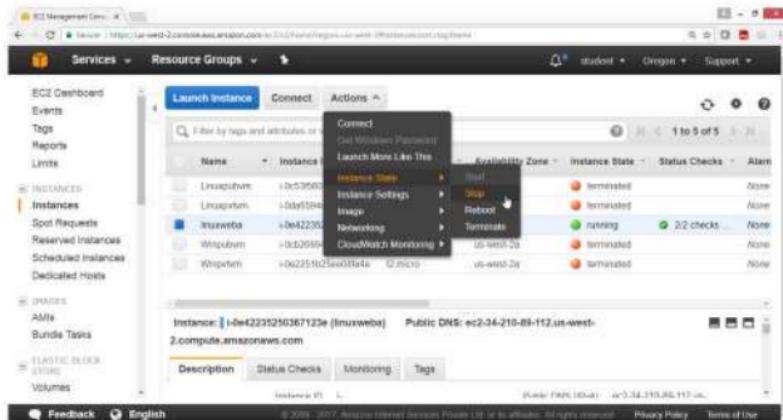
On "EC2 Dashboard" panel

Select the instance

Click on Action button

Select Instance state

Click stop



Click on **Yes Stop** button



Select the stopped instance

Click on **Action** button

Select **Image**

Click on **Create image** button

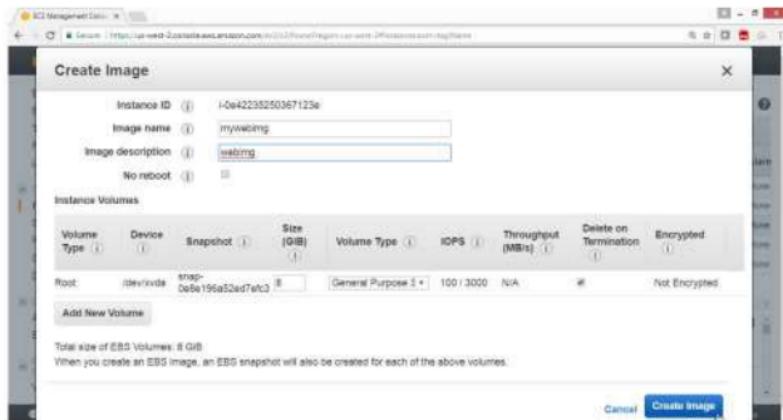
The screenshot shows the AWS EC2 Management Console interface. On the left, there's a sidebar with navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images, Abilities, Bundle Tasks, and Elastic Block Store. The main area displays a list of instances. One instance, named 'Imuzweb1' with Instance ID i-0e42235250367123e, is selected and highlighted with a blue border. A context menu is open over this instance, with the 'Actions' option expanded. Under the 'Image' section of the Actions menu, the 'Create Image' option is highlighted with a mouse cursor. Below the instance list, there's a detailed view for the selected instance, showing its description as 'Imuzweb1', private IP as 172.31.19.173, instance ID as i-0e42235250367123e, and public DNS (IPv4) as 'ip-172-31-19-173'. At the bottom of the page, there are links for Feedback, English, and other AWS services.

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 has 'Services' expanded, with 'EC2 Dashboard' selected. Under 'IMAGES', 'AMIs' is selected. The main content area shows a table titled 'AMIs' with one item listed:

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

Below the table, there is a detailed view for the selected AMI, showing tabs for 'Details', 'Permissions', and 'Tags'. The 'Edit' button is visible at the bottom right of this view.

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 several sections: LOAD BALANCING (Load Balancers, Target Groups), AUTO SCALING (Launch Configurations, Auto Scaling Groups), SYSTEMS MANAGER (Run Command, State Manager, Automations, Patch Compliance, Patch Baselines), and SYSTEMS MANAGER SHARED RESOURCES (Managed Instances, Activations). The 'AUTO SCALING' section is currently selected, indicated by a blue border around its items. The main content area has a title 'Resources' and a message: 'You are using the following Amazon EC2 resources in the US West (Oregon) region:'. Below this, there's a table with the following data:

Value	Description
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

On the right side of the main content area, there's a sidebar titled 'Account Attributes' with the following information:

- Supported Platforms: VPC
- Default VPC: vpc-89c34f1e
- Resource ID length management: 128

Below the account attributes, there's a section titled 'Additional Information' with links to 'Getting Started Guide', 'Documentation', 'All EC2 Resources', 'Forums', 'Pricing', and 'Contact Us'. At the bottom of the main content area, there's a button labeled 'Launch Instance'.

Click on "Launch Configuration"

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#AutoScaling:LaunchConfigurations>. The left navigation bar has 'Launch Configurations' selected under the 'Auto Scaling' category. The main content area is titled 'Welcome to Auto Scaling' and discusses Auto Scaling's benefits like reusable instance templates, automated provisioning, and adjustable capacity. A prominent blue button labeled 'Create Auto Scaling group' is visible.

Click on "Create Auto Scaling Group" button

This screenshot shows the 'Create Auto Scaling group' wizard step 1. It displays the same 'Welcome to Auto Scaling' information and features as the previous screenshot, but the 'Create Auto Scaling group' button is highlighted with a red box. The URL in the address bar is <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#AutoScaling:LaunchConfigurations>CreateAutoScalingGroupStep1>.

Click on "Create launch configuration" button

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/autoscaling/home?region=us-east-1#/launching/choose-launch-configuration?wizardId=createAutoScalingGroup>. The page title is "Create Auto Scaling Group". A large orange callout box highlights the "Create launch configuration" button at the bottom right of the main content area.

Create Auto Scaling Group

To create an Auto Scaling group, you will need to choose a template that your Auto Scaling group will use when it launches instances for you, called a launch configuration. Choose a launch configuration or create a new one, and then apply it to your group.

Later, if you want to use a different template, you can create another launch configuration and apply it to this group, even if you already have instances running in it. Using this method, you can update the software that your group uses when it launches new instances.

Step 1: Create launch configuration

First, define a template that your Auto Scaling group will use to launch instances. You can change your template.

Create launch configuration

Click on "My AMI"

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/autoscaling/home?region=us-east-1#/launching/choose-launch-configuration?wizardId=createAutoScalingGroup&step=1>. The page title is "Create Launch Configuration". A callout box highlights the "Select" button next to the "Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-8dfe514" option.

Create Launch Configuration

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

Quick Start

My AMIs **Select** **64-bit**

Amazon Linux **Select** **64-bit**

Community AMIs

Press F1 for help

Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-8dfe514
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: /dev/sda
Virtualization type: hvm

Red Hat Enterprise Linux 7.3 (HVM), SSD Volume Type - ami-b55a51cc
Red Hat Enterprise Linux version 7.3 (HVM, EBS General Purpose (SSD) Volume Type)
Root device type: /dev/sda
Virtualization type: hvm

Feedback **English** © 2006–2017, Amazon Web Services Privacy Notice | Terms of Use | Privacy Policy | Terms of Use

Select the AMI which was created with Webserver.

Click on Select button

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Ownership

Owned by me

Shared with me

mywebimg - ami-3fe6947

ami-3fe6947
mywebimg
64-bit
64-bit
t2.micro
Virtually Private Server
Owner: 822911683217

Select

Choose instance Type,

General purpose, t2.micro free tier

Click on Next : Configuration Details

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

Family	Type	vCPUs	Memory (GB)	Instance Storage	EBS-Optimized Available	Network Performance
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
General purpose	t2.micro <small>(Variable ECUs, 1 vCPU, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS-only)</small>	1	1	EBS only	-	Low to Moderate
General purpose	t2.small	1	2	EBS only	-	Low to Moderate
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate

Cancel Previous Next: Configure details

On Create launch Configuration page:

Name → mylaunchconf

Monitoring → Enable check box

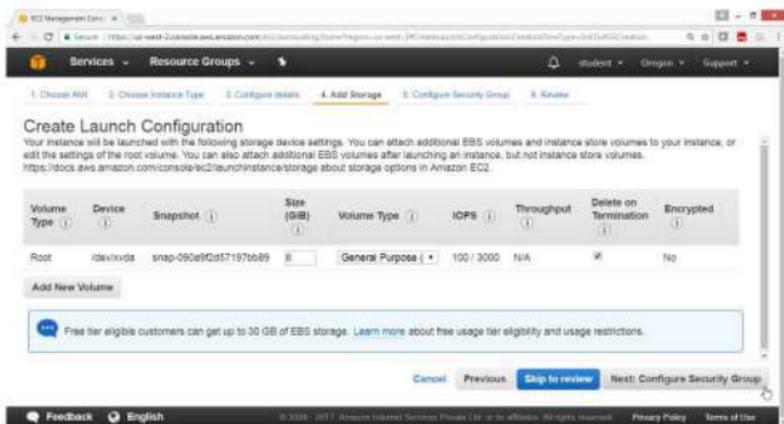
Click on **Next : Add storage** button

The screenshot shows the 'Create Launch Configuration' wizard on the 'Configure details' step. The 'Name' field is set to 'mylaunchconf'. Under 'Purchasing option', there is a checkbox for 'Request Spot Instances' which is unchecked. The 'IAM role' dropdown is set to 'None'. In the 'Monitoring' section, there is a checked checkbox for 'Enable CloudWatch detailed monitoring' with a link to 'Learn more'. Below this, there is a note: '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.' At the bottom right of the form, there are 'Cancel', 'Previous', 'Skip to review', and 'Next: Add Storage' buttons.

By default linux takes 8 GB EBS volume

Leave all values as default

Click on " Next: Configure Security Group" button



On Create Launch Configuration page

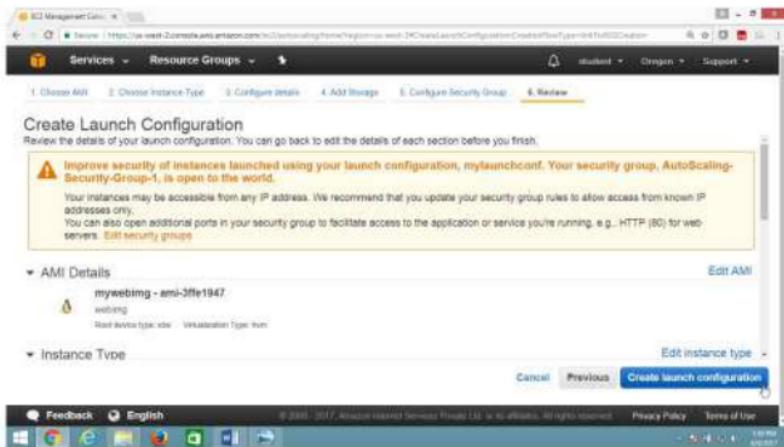
Select “Create a new security Group”

Click on Review

The screenshot shows the AWS EC2 Management Console interface. The top navigation bar includes 'Services', 'Resource Groups', and 'Review'. Below the navigation, a progress bar indicates steps 1 through 8, with step 8, 'Configure Security Group', highlighted. A sub-header 'Create Launch Configuration' is present. The main content area is titled 'Assign a security group' and contains two options: 'Create a new security group' (selected) and 'Select an existing security group'. Underneath, there are fields for 'Security group name' (set to 'AutoScaling-Security-Group-1') and 'Description' (set to 'AutoScaling-Security-Group-1 (2017-08-09 13:47:40 +05:30)'). Below these fields is a table with columns 'Type', 'Protocol', 'Port Range', and 'Source'. A single row is shown with 'SSH' in 'Type', 'TCP' in 'Protocol', '22' in 'Port Range', and 'Anywhere' in 'Source'. At the bottom of the form are 'Add Rule' and 'Review' buttons. The footer of the page includes links for 'Feedback', 'English', and legal notices.

Check the summary

Click on “Create launch configuration” button



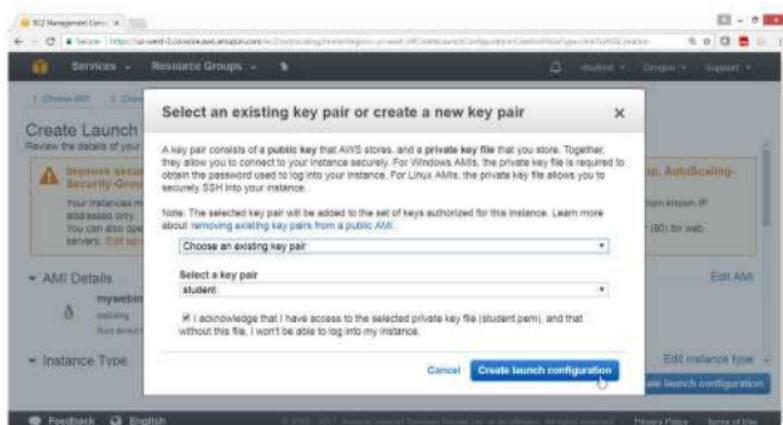
On "Select an existing key pair or create a new key pair" page

Select "Choose an existing key pair"

Select a key pair → student

Select Acknowledge check box

Click on "Create launch Configuration" button



On "Create Auto Scaling Group" page, give values as

Launch Configuration → mylaunchconf

Group name → myautoscalegrp

For Network → select default

Create Auto Scaling Group

Launch Configuration: mylaunchconf

Group name: myautoscalegrp

Group size: Start with 1 instances

Network: us-west-2

Subnet: subnets-1940f141 (172.31.0.0/20) | Default in us-west-2a
subnets-1360e5ef (172.31.32.0/20) | Default in us-west-2b
subnets-66e30ec (172.31.36.0/20) | Default in us-west-2b

Cancel Next: Configure scaling policies

Select ALL subnet one by one

Click on "Next Configure scaling policies" button

The screenshot shows the AWS Management Console interface for creating an Auto Scaling group. The top navigation bar includes 'Services', 'Resource Groups', 'student', 'Dragon', 'Support', and 'Cancel and Exit'. Below the navigation is a progress bar with four steps: 1. Configure Auto Scaling group details (selected), 2. Configure scaling policies, 3. Configure Notifications, 4. Configure Tags, and 5. Review. The main form is titled 'Create Auto Scaling Group' and contains the following fields:

- Launch Configuration:** mylaunchconf
- Group name:** myautosclegrp
- Group size:** Start with 1 instances
- Network:** vpc://ic34tne (172.31.0.0/16) | Default in us-west-2a
- Subnet:** (checkboxes selected for all three subnets)
 - subnet-19d0f041 (172.31.0.0/20) | Default in us-west-2a
 - subnet-1390e5ac (172.31.32.0/20) | Default in us-west-2a
 - subnet-fb010bac (172.31.16.0/20) | Default in us-west-2b

At the bottom right of the form are 'Cancel' and 'Next: Configure scaling policies' buttons.

On "Create Auto Scaling Group" page

Select "Use scaling policies to adjust the capacity of this group"

Scale between [] and [] instances.

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: seconds to warm up after scaling

Cancel Previous Review Next: Configure Notifications

Drag Down

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

Create Auto Scaling Group

Scale Group Size

Name: Scale Group Size
Metric type: Average CPU Utilization
Target value:
Target value must be specified

Instances need: seconds to warm up after scaling
Disable scale-in:

Scale the Auto Scaling group using step or simple scaling policies (1)

Cancel Previous Review Next: Configure Notifications

Select Increase Group Size

Click on "Add new alarm"

Name: Increase Group Size
Execute policy when: No alarm selected [Add new alarm](#)
Take the action: Add • 0 instances
Add step [\(i\)](#)
Instances need: [redacted] seconds to warm up after each step.
[Create a simple scaling policy \(i\)](#)

Decrease Group Size

Name: Decrease Group Size

Cancel Previous Review Next: Configure Notifications

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 notifications should be sent.

Send a notification to: No SNS topics found... [create topic](#)

Whenever: Average of CPU Utilization
List: >= 90 Percent

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

Name of alarm: awssec2-myautoscalegrp-High-CPU-Utilization

CPU Utilization Percent

04:00 08:00

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: powers2-mysqlscalegrp-High-CPU-Utilization

CPU Utilization Percent

Cancel **Create Alarm**

For Take the action → Add 1

Drag down and give Decrease policy parameters

The screenshot shows the 'Create Auto Scaling Group' wizard at step 2, 'Configure scaling policies'. A modal window titled 'Increase Group Size' is open. It contains the following fields:

- Name:** Increase Group Size
- Execute policy when:** asic2-myautoscalegrp-High-CPU-Utilization Edit Remove (This row has a tooltip: 'triggers the alarm threshold: CPUUtilization >= 30 for 300 seconds for the metric dimensions: AutoScalingGroupName = myautoscalegrp')
- Take the action:** Add + 1 instances When 30 <= CPUUtilization < +Infinity
- Add step (1)**
- Instances need:** 0 seconds to warm up after each step

At the bottom of the modal are 'Cancel', 'Previous', 'Review' (highlighted in blue), and 'Next: Configure Notifications'.

In Decrease Group wizard

Click on "Add new alarm"

The screenshot shows the 'Create Auto Scaling Group' wizard at step 2, 'Configure scaling policies'. A modal window titled 'Decrease Group Size' is open. It contains the following fields:

- Name:** Decrease Group Size
- Execute policy when:** No alarm selected (with a 'Add new alarm' button)
- Take the action:** Remove - 0 instances
- Add step (1)**
- Create a simple scaling policy (i)**

At the bottom of the modal are 'Cancel', 'Previous', 'Review' (highlighted in blue), and '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 • create topic)

Whenever: Average of CPU Utilization

Is: <= 20 Percent

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

Name of alarm: asecd2-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 • create topic)

Whenever: Average of CPU Utilization

Is: <= 20 Percent

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

Name of alarm: asecd2-myautoscalegrp-High-CPU-Utilization

CPU Utilization Percent

Cancel Create Alarm

Check the summary

Click on "Next: Configure Notificaion"

Name: Decrease Group Size
Execute policy when: swsc2-myautoscalegrp-High-CPU-Utilization Edit Remove
Creates the alarm threshold: CPUUtilization >= 20 for 300 seconds for the metric dimensions AutoScalingGroupName = myautoscalegrp
Take the action: Remove 1 Instances When: 100 >= CPUUtilization > -infinity
Add step

Create a simple scaling policy

Cancel Previous Review Next: Configure Notifications

Click on "Add notification" button

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 AWS Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2&CreateAutoScalingGroup=&wizard=ConfigurationStep1InMyLaunch...>. The page title is "EC2 Management Console - Services - Resource Groups". The navigation bar includes "student", "Dragon", and "Support". The main content area has tabs: 1. Configure Auto Scaling group details, 2. Configure scaling policies, 3. Configure Notifications (which is selected), 4. Configure Tags, and 5. Review. The "Configure Auto Scaling Group" section is titled "Create Auto Scaling Group". It says "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." A note below states: "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." A "Send a notification to:" field contains "CpuUtilizationabc (kimerhearn09@gmail.com) - create topic". Below it, "Whenever Instances:" has four radio buttons: "launch" (unchecked), "terminate" (checked), "fail to launch" (unchecked), and "fail to terminate" (unchecked). A "Add notification" button is present. At the bottom are "Cancel", "Previous", "Review" (highlighted in blue), and "Next: Configure Tags". The footer includes "Feedback", "English", and links to "© 2006-2017 Amazon Internet Services LLC or its affiliates. All rights reserved.", "Privacy Policy", and "Terms of Use".

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	myautoscaleapp	Edit details
Group size	1	
Minimum Group Size	1	
Maximum Group Size	3	
Subnet(s)	subnet-13d0f141, subnet-13d0e5a, subnet-13d0e5b	
Health Check Grace Period	300	
Detailed Monitoring	No	
Instance Protection	None	

Scaling Policies

Edit scaling policies

Cancel Previous Create Auto Scaling group

Drag down

Click on "Create Auto Scaling group" button

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

Create Auto Scaling Group

Detailed Monitoring **N/A**
Instance Protection **None**

Scaling Policies [Edit scaling policies](#)

Increase Group Size: With alarm: `aws@2 myautoscalegrp High CPU Utilization: Add 1 instances and 300 seconds for instances to warm up`
Decrease Group Size: With alarm: `aws@2 myautoscalegrp High CPU Utilization: Remove 1 instances`

Notifications [Edit notifications](#)

Coupling notifications: `skmarfan99@gmail.com` launch, terminate, fail to launch, fail to terminate

Tags [Edit tags](#)

Name: `WebAutoscale` My new instances

[Cancel](#) [Previous](#) **Create Auto Scaling group**

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

Successfully created

Click on Close button

Auto Scaling group creation status

✓ Successfully created Auto Scaling group [View creation log](#)

View

View your Auto Scaling groups
View your launch configurations

Here are some helpful resources to get you started

Close

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

Verification

Now go to EC2 Dash Board

Click on Instances

Observer that WebAutoscale instance got launched

The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with navigation links for Services (EC2 Dashboard, Events, Tags, Reports, Limits), Instances (Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), Images (AMIs, Bundle Tasks), and Elastic Block Store (Volumes). The main area is titled 'Launch Instance' and has a search bar. A table lists two instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Instance	i-042235250367123e	t2.micro	us-west-2a	stopped	None	None
WebAutoscale	i-0a7aaafe07044125e	t2.micro	us-west-2c	running	2/2 checks	None

Select an Instance above:

Now login to Web Autoscale instance

This screenshot is similar to the previous one, showing the EC2 Management Console Instances page. The 'WebAutoscale' instance is now selected, indicated by a blue selection bar. The Public DNS is displayed as 'ec2-54-244-159-247.us-west-2.compute.amazonaws.com'. The bottom of the screen shows the AWS footer with links for Feedback, English, Privacy Policy, and Terms of Use.

Run the following command to increase the load

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

Verification

After 15 minutes 3 instance got loaded automatically

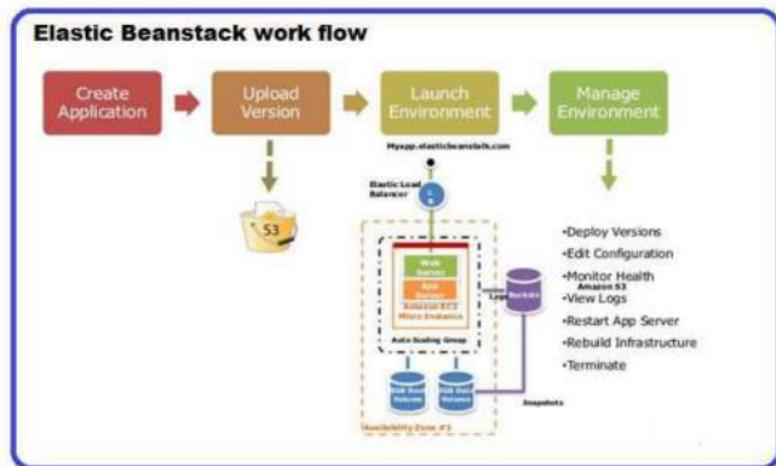
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
Stressweb	i-0a422d5250967123e	t2.micro	us-west-2a	stopped	0/2 checks	None
Vm1Autoscale	i-045629a50663ba75	t2.micro	us-west-2a	running	2/2 checks	None
Vm2Autoscale	i-07aef0f7044123e	t2.micro	us-west-2c	running	2/2 checks	None
Vm3Autoscale	i-0fb79030d04edc7c	t2.micro	us-west-2b	running	2/2 checks	None

Lab 14: To Configure an Elastic Beanstalk with Tomcat Application

OBJECTIVE

To configure Elastic Beanstalk in AWS

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user with AWSElasticBeanstalkFullAccess

TASK :

Create Elastic Beanstalk Tomcat Application

Deploy java war files

Open Browser and check your web application

Practical Steps

1) To create Elastic Beanstalk Application

Open AWS Console

Select Compute service

Click on "Elastic BeanStalk"

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/compute/home?region=us-east-1>. The top navigation bar includes 'Services' (selected), 'Resource Groups', and links for 'student', 'Original', and 'Support'. Below the navigation is a search bar and a 'Create New' button. The main content area is titled 'Amazon Web Services' and lists various services under 'Compute' and 'Storage'. Under 'Compute', 'Elastic Beanstalk' is highlighted with a yellow box. Other services listed include EC2, Lambda, and Batch. Under 'Storage', S3, EFS, and Glacier are listed. 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 links for 'Getting Started', 'AWS Console Mobile App', and 'AWS Marketplace'.

"Welcome to Amazon Elastic Beanstalk" page opens

Click on "Get started" button

The screenshot shows the AWS Elastic Beanstalk 'Welcome' page. At the top, there's a navigation bar with tabs for 'Services', 'Resource Groups', 'Create New Application', and a user icon. Below the navigation is a search bar with the placeholder 'Elastic Beanstalk'. The main content area features a large title 'Welcome to AWS Elastic Beanstalk' and a sub-section titled '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.' It includes two small line graphs showing metrics over time. Below this, there's a section for deploying a sample application with a 'Get started' button. At the bottom, a footer bar says 'Get Started in Three Easy Steps'.

On "Create a Web app", page, provide values

Application Name → Tomcatapp

Environment Name → Tomcatenv

Drag down

The screenshot shows the 'Create a web app' wizard in the AWS Elastic Beanstalk console. The top navigation bar includes 'Services', 'Resource Groups', 'Student', 'Orgs', and 'Support'. A 'Create New Application' button is visible on the right. The main section is titled 'Create a web app' with a sub-section 'Application information'. It shows an application name 'Tomcatapp' and a note about character limits. Below this is 'Environment information' with an environment name 'tomcatevn' and a domain 'us-east-2.elasticbeanstalk.com'.

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

Environment name: tomcatevn

Domain: us-east-2.elasticbeanstalk.com

In Platform box select **Tomcat**

Drag down

Base configuration

Platform

- Choose a platform —
- Choose a platform —
- Preconfigured:
 - Node.js
 - PHP
 - Python
 - Ruby
 - Tomcat**
 - .NET (Windows/IIS)
 - Java
 - Go
 - Packer
- Preconfigured – Docker
 - GlassFish
 - Go
 - Python
 - Generic
 - Docker
 - Multi-container Docker

Options 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.

Feedback English

© 2008–2015 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy Terms of Use

Select **Upload your code**

Base configuration

Platform Tomcat

Configure more options for more platform configuration options.

Application code Sample application
(Get started right away with sample code.)

Upload your code
Upload a source bundle from your computer or copy and paste from Amazon S3.

ZIP or tar.gz

Cancel Configure more options 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.

Feedback English

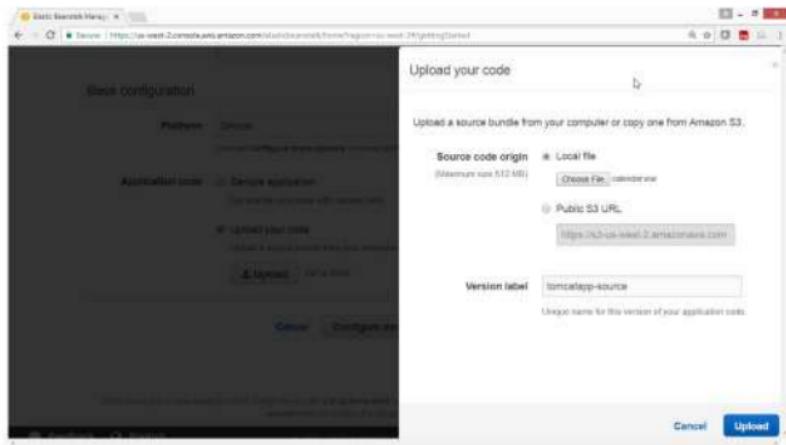
© 2008–2015 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy 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

Application code: Sample application

Upload your code

Cancel Configure more options 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 change.

Feedback English

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

Privacy Policy Terms of Use

Verification :

Tomcat application at background is getting created,

Progress on screen are displayed

Creating tomcatenv

This will take a few minutes.

4:20pm Using s3://elasticbeanstalk-us-west-2-52351953211 as Amazon S3 storage bucket for environment data.

4:20pm createEnvironment is starting

Actions

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

Feedback English

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

Privacy Policy Terms of Use

Verify

Creating tomcatenv
This will take a few minutes..

4:28pm 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-yygorzbowiec-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

All Applications > Tomcatapp > tomcatenv (Environment ID: a-yygorzbowiec, URL: tomcatenv.s3-website-us-west-2.amazonaws.com) Actions

Dashboard Overview Refresh

Configuration

Logs Health Monitoring Alarms

Health: Ok Causes

Running Version: tomcatapp-source Upload and Deploy

Configuration: 64bit Amazon Linux 2017.03 v2.6.2 running Tomcat 8 Java 8

Verification

Open any Browser

Click on URL link

Website is open

The screenshot shows a web browser window with the title "Welcome Calendar Dev". The address bar contains the URL "turconsoftguru.net/LambdaWebSite.com". The main content area displays a calendar application with the following sections:

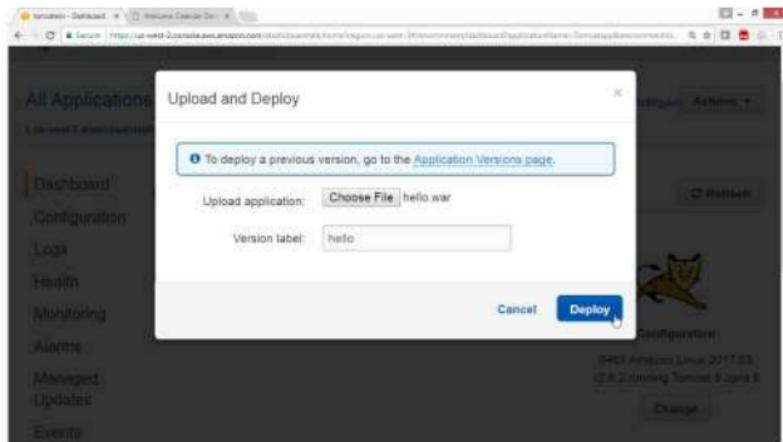
- Simple Calendar:** A birth date input field set to "10/7/1975" with a calendar icon.
- Supports Multiple Calendars:** Two date input fields, "StartDate: 10/7/1975" and "EndDate: 10/07/2000", each with a calendar icon.
- Supports indexed properties:** Five sets of date input fields, each consisting of "StartDate: 10/7/1975" and "EndDate: 10/07/2000", followed by a small calendar icon.

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 CloudWatch Metrics Dashboard. In the top navigation bar, the path is "All Applications > Tomcatapp > tomcatenv". Below this, the URL is listed as "https://us-west-2.elasticbeanstalk.com". The main interface has a sidebar with links like Dashboard, Configuration, Logs, Health, Monitoring, Alarms, Managed Updates, and Events. The "Overview" tab is selected. On the right, there's a large green circle with a white checkmark, labeled "Health" and "Ok". Below it is a "Causes" button. To the right is a section titled "Running Version" showing "hello" and a "Upload and Deploy" button. A cartoon cat icon is next to the version information. Below this is a "Configuration" section with "64bit Amazon Linux 2017.03 v2.6.2 running Tomcat 8 Java 8" and a "Change" button. At the bottom left, there's a link to "Event Log".

Verify the website



Hello Index

Try the [servlet](#).

4) To Remove Elastic Bean stack

Select Action button

Click Delete application button

The screenshot shows the AWS Elastic Beanstalk console with the URL <https://us-west-2.console.aws.amazon.com/elasticbeanstalk/home?region=us-west-2#applications>. The main area displays a list of applications under 'All Applications'. One application, 'Tomcatapp', is highlighted with a green background. A context menu is open over this application, with the 'Actions' dropdown expanded. The 'Delete application' option is highlighted with a blue background and a white border. Other options in the menu include 'Create environment', 'View application versions', 'View saved configurations', and 'Restore terminated environment'. On the left sidebar, there are sections for 'Learn More' (with links to 'Get started using Elastic Beanstalk', 'Modify the code', 'Create and connect to a database', and 'Add a custom domain') and 'Featured' (with a link to 'Create your own custom platform'). At the bottom left, there's a link to 'Command Line Interface (v3)'. The top navigation bar includes 'Services', 'Resource Groups', and user information ('student', 'Oregon', 'Su...').

This screenshot shows a confirmation dialog box titled 'Delete Application' with the message 'Are you sure you want to delete the application: Tomcatapp?'. Below the message are two buttons: 'Cancel' on the left and 'Delete' on the right, both with a red background. In the background, the 'Tomcatapp' application card is visible, showing its configuration details: Environment tier: Web Server; Platform: 64bit Amazon Linux 2017.03 v2.6.2 running Tomcat 8 Java 8; Running versions: hello; Last modified: 2017-07-27 16:40:51 UTC+0630; URL: tomcatapp.sfc55gpvrr.us-west-2.elasticbean...'. The rest of the interface is identical to the previous screenshot, including the sidebar with 'Learn More' and 'Featured' sections, and the top navigation bar.

Application will now get terminated

The screenshot shows the AWS Elastic Beanstalk console. In the top navigation bar, 'Services' and 'Resource Groups' are selected. Below the navigation, there's a search bar and a 'Create New Application' button. A dropdown menu for 'Tomcatapp' is open. On the left, there's a sidebar with 'Learn More' sections for getting started with Elastic Beanstalk, modifying code, connecting to databases, and adding custom domains. Under 'Featured', there's a link to 'Create your own custom platform'. At the bottom of the sidebar is a link to 'Command Line Interface (v3)'. The main content area is titled 'All Applications' and shows a single entry: 'Tomcatapp'. This entry includes a status box for 'tomcatenv (Terminated)', details about the environment tier (Web Server), platform (64-bit Amazon Linux 2017.03 v2.8.2 running Tomcat 8 Java 8), running versions (helio), last modified date (2017-07-27 16:48:14 UTC+0530), and URL (tomcatenv.s0b05gprk.us-east-2.elasticbeanstalk.com). There's also an 'Actions' button.

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 screenshot. The main content area features a large 'Welcome to AWS Elastic Beanstalk' heading. Below it is a brief description: '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.' To the left of the text is a dashboard box displaying metrics: 53.6 (available instances), 148K (current requests), 65% (utilization), 354KB (new requests), and 12KB (new errors). Below the dashboard are two line graphs showing trends over time. To the right of the text, there's a section with instructions: 'To deploy your existing web application, create an application source bundle and then create a new application. If you're using GitHub and would prefer to use it with our command line tool, please see Getting Started with the EB CLI.' At the bottom, there's a call-to-action: 'To deploy a sample application, click Get started, choose a name, select a platform and'.

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 Management Console interface for the S3 service. At the top, there's a navigation bar with links for 'Services', 'Resource Groups', and dropdowns for 'Region' (set to 'Global'), 'Filter' (set to 'All'), and 'Logins'. Below the navigation is a banner for 'Amazon QuickSight' with a 'Get started today' button. The main area is titled 'Amazon S3' and features a search bar with placeholder 'Search for buckets'. There are three buttons at the top of the list: 'Create Bucket', 'Create Vault', and 'Create Folder'. The list itself has two columns: 'Bucket Name' and 'Region'. The buckets listed are:

Bucket Name	Region	Date Created
antigone	US West (Oregon)	Jul 1, 2017 8:47:53 PM
anuradha94	US West (Oregon)	Jan 22, 2017 10:17:16 AM
elast-beanstalk-ap-south-1-02233163217	US West (Oregon)	Jul 2, 2017 9:06:36 AM
elast-beanstalk-us-west-2-02307148217	Korea Pacific (Seoul)	Jan 27, 2017 9:40:24 AM
elast-beanstalk-us-west-2-02307148217	US West (Oregon)	Jul 1, 2017 9:02:22 PM
hydrangeaplates0072101	US West (Oregon)	Jul 7, 2017 8:43:19 PM
hydrangeatmpimg	US West (Oregon)	Jul 10, 2017 8:22:19 PM
instacartorderhistory	US West (Oregon)	Jul 1, 2017 9:26:13 PM
instacartreceipts	US West (Oregon)	Jan 16, 2017 7:32:46 PM
zoomgroup	US West (Oregon)	Jul 25, 2017 9:27:53 AM

AWS Services	
EC2	 Compute EC2 EC2 Container Service Lightsail Elastic Beanstalk Lambda Batch
CloudWatch	 Developer Tools CodeStar CodeCommit CodeBuild CodeDeploy CodePipeline X-Ray
Simple Notification Service	 Analytics Athena EMR CloudSearch Elasticsearch Service Kinesis Data Pipeline QuickSight
VPC	 Storage EFS Glacier Storage Gateway
	 Management Tools CloudWatch CloudFormation CloudTrail Config OpsWorks Service Catalog Trusted Advisor Managed Services
	 Artificial Intelligence Lex Poly Rekognition Machine Learning
	 Internet Of Things AWS IoT AWS Greengrass

Select elastic Beanstalk Bucket, Click Properties

Select Permissions

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/s3/home?region=us-west-2&tab=switchToCloudWatchLogs>. The top navigation bar includes 'Services', 'Resource Groups', 'Marketplace', 'CloudWatch Logs', and 'Support'. Below the navigation is a search bar and a 'Create Bucket' button. The main content area displays a list of buckets under 'All Buckets (1)'. One bucket, 'www.mackfilips.com', is selected, indicated by a blue background. The right side of the screen features tabs for 'None', 'Properties', and 'Transfers', with 'Properties' currently selected.

Click "Edit bucket policy"

The screenshot shows the AWS Management Console with the 'Bucket Properties' page open. The bucket name is 'elasticbeanstalk-us-west-2-52325168...'. The 'Permissions' section is visible, showing a single policy named 'elasticbeanstalk-us-west-2-5232516817'. Below it, there are buttons for 'Add more permissions', 'Edit bucket policy', and 'Add CORS Configuration'. At the bottom, there are 'Save' and 'Cancel' buttons.

In Bucket Policy Editor wizard,

Click Delete to remove policy, click OK

The screenshot shows the 'Bucket Policy Editor' dialog box for the same bucket. It displays a JSON policy document with one statement. The 'Delete' button is highlighted, indicating it's being clicked to remove the policy. The dialog has 'Save', 'Delete', and 'Close' buttons at the bottom.

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:DeleteObject",
            "Resource": "arn:aws:s3:::elasticbeanstalk-us-west-2-5232516817/*"
        }
    ]
}
```

Click on Save button

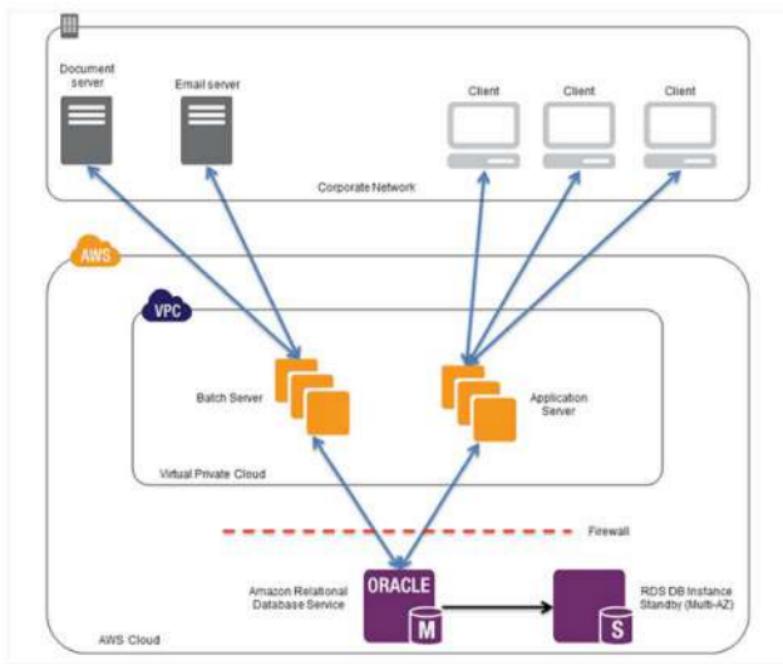
The screenshot shows the AWS Management Console interface for the S3 service. On the left, there's a sidebar with 'Create Bucket' and 'Actions' dropdowns, and a list of 'All Buckets (14)' containing items like 'all-time', 'awscloudwatch', etc. The main right panel is titled 'Bucket: elasticbeanstalk-us-west-2-52325168...' and shows the 'Properties' tab. Under the 'Permissions' section, it says 'You can control access to the bucket and its contents using access policies. Learn more.' Below this are fields for 'Access key' (set to 'arn:aws:s3:::elasticbeanstalk-us-west-2-52325168*'), checkboxes for 'List', 'GetObject', 'View Permissions', and 'Edit Permissions', and three buttons: 'Add more permissions', 'Add bucket policy', and 'Add CORS Configuration'. At the bottom of the 'Permissions' section is a large blue 'Save' button with a white arrow icon, and a 'Cancel' button next to it. The status bar at the bottom includes links for 'Feedback', 'English', and legal notices.

Lab 15: To Configure an Amazon Relational Database Service

OBJECTIVE

To configure Amazon Relation Database service

TOPOLOGY



PRE-REQUISITES

User should have AWS account, or IAM user withAmazonRDSFullAccess

Task

Create Amazon Relational Database Service

Verify connection from mysql client command line tool

Verify Connection using MySQL Workbench client application

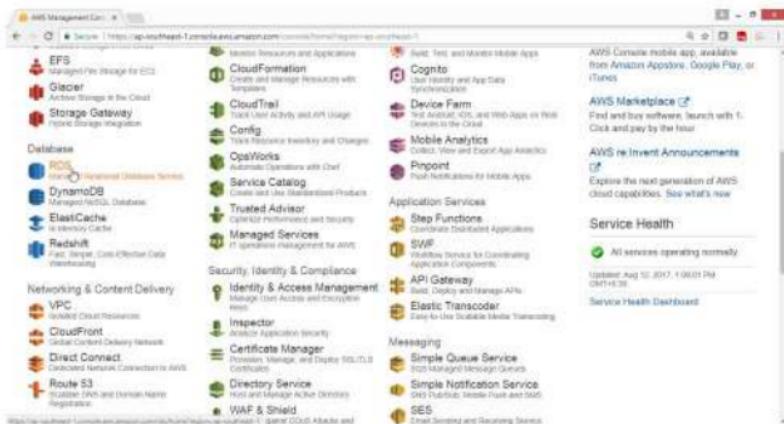
Practical Steps

To create Amazon Relational Database Service

From the AWS console

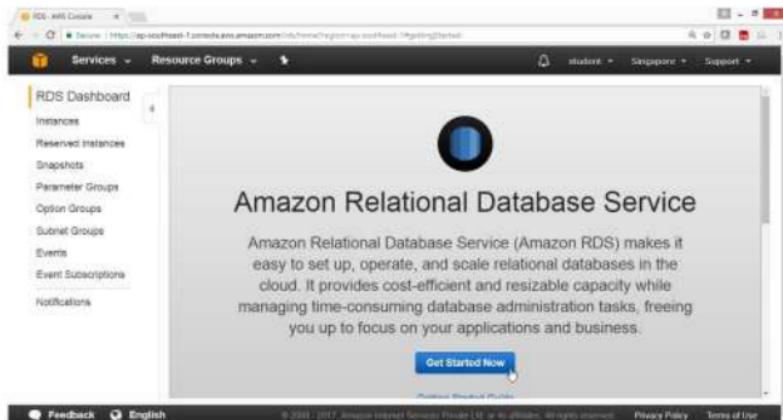
Select Database

Click on BDS service



In "RDS Dashboard", wizard

Click "Get Started Now", button



In Select Engine, wizard

Click on MySQL

Click on Select button

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

MySQL
MySQL Community Edition

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

- Supports database sizes up to 5 TB
- Instances offer up to 22 vCPUs and 244 GB Memory
- Supports automated backup and point-in-time recovery
- Supports cross-region read replicas
- Free tier eligible

MariaDB

PostgreSQL

Oracle

SQL Server

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

In Production wizard

select Dev/Test, Choose MySQL

Do you plan to use this database for production purposes?

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

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

Billing is based on RDS pricing.

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

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

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: Selected 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 explains that the Free Tier provides a single db.t2.micro instance up to 20 GB of storage. There's a checkbox to 'Only show options that are eligible for RDS Free Tier'. Under 'Instance Specifications', the DB Engine is set to 'mysql', License Model to 'general-public-license', and DB Engine Version to 'MySQL 5.6.35'. A callout box points to the version dropdown with the text 'Review the Known Issues/Limitations to learn about potential compatibility issues with specific database versions.' At the bottom, there's a dropdown for 'DB Instance Class - Select One -'.

Amazon RDS Console

Services Resource Groups

Amazon RDS DB - db-simpler

DB Instance Storage Total 19.67 USD

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 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 GB RAM

Multi-AZ Deployment No

Storage Type General Purpose (SSD)

Allocated Storage* 5 GB

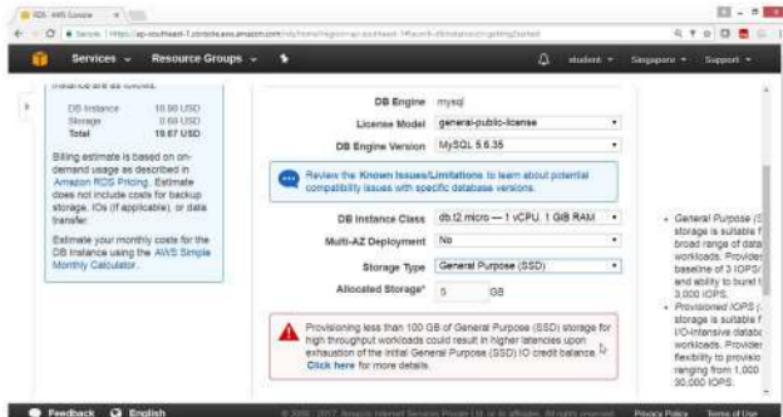
⚠ Provisioning less than 100 GB of General Purpose (SSD) storage for high-throughput workloads could result in higher latencies upon exhaustion of the initial General Purpose (SSD) I/O credit balance. Click Here for more details.

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

+ Provisioned IOPS (SSD) storage is suitable for IO-intensive data workloads. Provides flexibility to provision ranging from 1,000 to 30,000 IOPS.

Feedback English

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



Under Settings

For Allocated Storage* → 5 GB

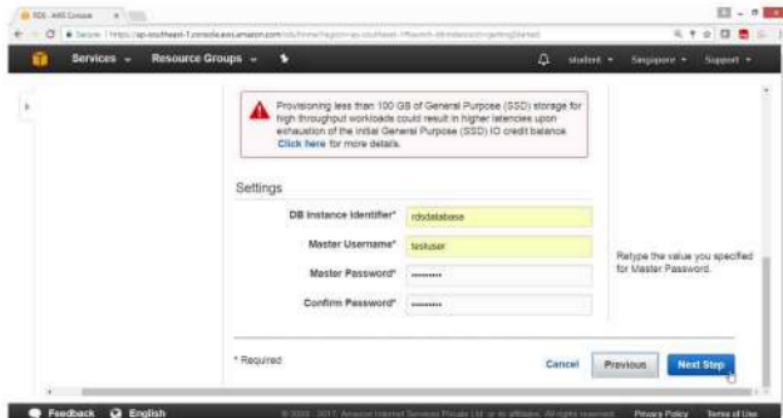
For DB Instance Identifier → rdsdatabase

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 'Configure Advanced Settings' wizard at Step 4: Configure Advanced Settings. The 'Network & Security' section is selected. The 'VPC Security Group(s)' dropdown is open, showing four options: 'Create new Security Group', 'default (VPC)', 'launch-lizard-1 (VPC)', and 'rds-launch-lizard (VPC)'. A tooltip provides instructions for selecting security groups. Other settings shown include VPC: Default VPC (vpc-ec2fe388), Subnet Group: default, Publicly Accessible: Yes, and Availability Zone: No Preference.

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 for a new MySQL database. The 'Database Name' is set to 'salesdba'. The 'Database Port' is set to '3306'. The 'DB Parameter Group' is 'default.mysql5.6' and the 'Option Group' is 'default.mysql-5.6'. The 'Copy Tags To Snapshots' checkbox is unchecked. Under 'IAM DB Authentication', 'No Preference' is selected. Under 'Encryption', 'No' is selected. A note at the bottom states that automated backups are currently supported for Innodb storage engine only. At the bottom of the page, there are links for 'Feedback', 'English', 'Privacy Policy', and 'Terms of Use'.

Provider Following Values

Under Backup

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

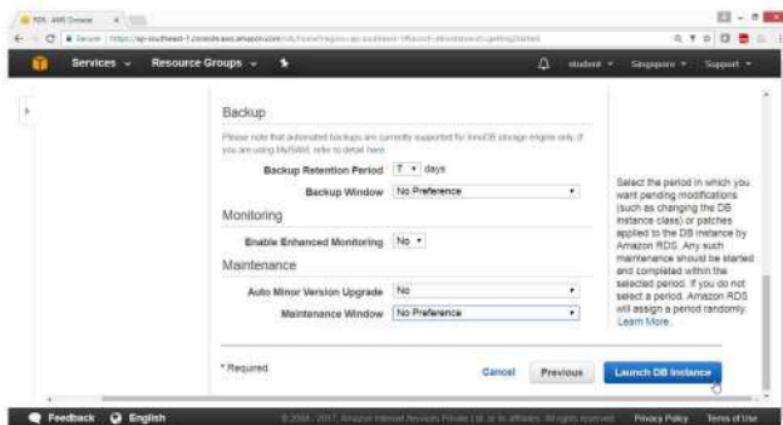
Under Monitoring

- Enable Enhanced Monitoring → No

Under Maintenance

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

Click on **Launch DB Instance**



Your DB Instance is being created.

Click on View Your DB Instances button

Step 1: Select Engine:
Step 2: Production?
Step 3: Specify DB Details
Step 4: Configure Advanced Settings

Your DB Instance is being created.
Note: Your instance may take a few minutes to launch.

Connecting to your DB Instance
Once Amazon RDS finishes provisioning your DB instance, you can use a SQL client application or utility to connect to the instance.
Learn about connecting to your DB instance

View Your DB Instances

Under status column

Verify creating

Launch DB Instance Show Monitoring Instance Actions

Filter: All Instances Search DB Instances... X

Viewing 1 of 1 DB Instances

Engine	DB Instance	Status	CPU	Current Activity	Maintenance	Class	VPC
MySQL	rdsdatabase	creating				None	db.t2.micro ipo-ed2f6

Feedback English © 2006–2017, Amazon Internet Services Private Limited. All rights reserved. Privacy Policy Terms of Use

Select MySQL Engine

The screenshot shows the AWS RDS Dashboard. On the left sidebar, under the 'Instances' section, there is a list of items: Reserved Instances, Snapshots, Parameter Groups, Option Groups, Subnet Groups, Events, Event Subscriptions, and Notifications. At the top, there are buttons for 'Launch DB Instance', 'Show Monitoring', and 'Instance Actions'. A search bar is present above the main content area. The main area displays a table with one row for a MySQL DB instance named 'rdsdatabase'. The status column shows 'creating'. Below the table, there is a section titled 'Alarms and Recent Events' and a 'Monitoring' section.

Under status column

Verify backing-up

The screenshot shows the AWS RDS Dashboard. The left sidebar and top navigation are identical to the previous screenshot. The main area now shows a MySQL DB instance named 'rdsdatabase' with the status 'backing-up'. The endpoint is listed as 'rdsdatabase.cdtjyq1sl4-sp.us-east-west-1.rds.amazonaws.com:1433 (authorized)'. The 'Monitoring' section shows 'No Data' for both CPU and Memory metrics over the last hour.

Under status column

Verify available

The screenshot shows the AWS RDS Dashboard. On the left, there's a sidebar with links for Instances, Reserved Instances, Snapshots, Parameter Groups, Option Groups, Subnet Groups, Events, Event Subscriptions, and Notifications. The main area has tabs for Launch DB Instance, Show Monitoring, and Instance Actions. A search bar and filter dropdown (set to All Instances) are at the top. Below is a table with columns: Engine, DB Instance, Status, CPU, Current Activity, Maintenance, and Class. One row is shown: MySQL, rdsdatabase, available, 1.33%, 0 Connections, None, db.t2.micro. An endpoint URL is also displayed. At the bottom, there are sections for Alarms and Recent Events (listing backup and creation events) and Monitoring (CPU and Memory metrics).

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

Endpoint: rdsdatabase.us-east-1.rds.amazonaws.com:3306 (authorized)

Event Type	Event Description
Event	
Aug 12 1:49 PM	Finished DB instance backup
Aug 12 1:45 PM	Backing up DB instance
Aug 12 1:44 PM	DB instance created

Monitoring	
CPU	1.42%
Memory	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 VARCHAR(100) NOT NULL,tutorial_author VARCHAR(40) NOT NULL,submission_date DATE,PRIMARY KEY (tutorial_id));
Query OK, 0 rows affected (0.04 sec) : 

mysql>
mysql> INSERT INTO tutorials_tbl(tutorial_title, tutorial_author, submission_date) VALUES('Learn PHP', 'John Paul', 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;

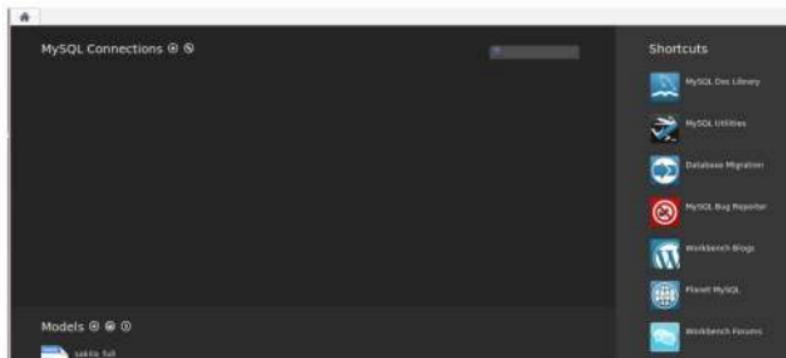
```
mysql> select * from tutorials_tbl;
+-----+-----+-----+-----+
| tutorial_id | tutorial_title | tutorial_author | submission_date |
+-----+-----+-----+-----+
| 1 | Learn PHP | John Poul | 2017-08-12 |
| 2 | Learn MySQL | Abdul S | 2017-08-12 |
| 3 | JAVA Tutorial | Sanjay | 2007-05-06 |
+-----+-----+-----+-----+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

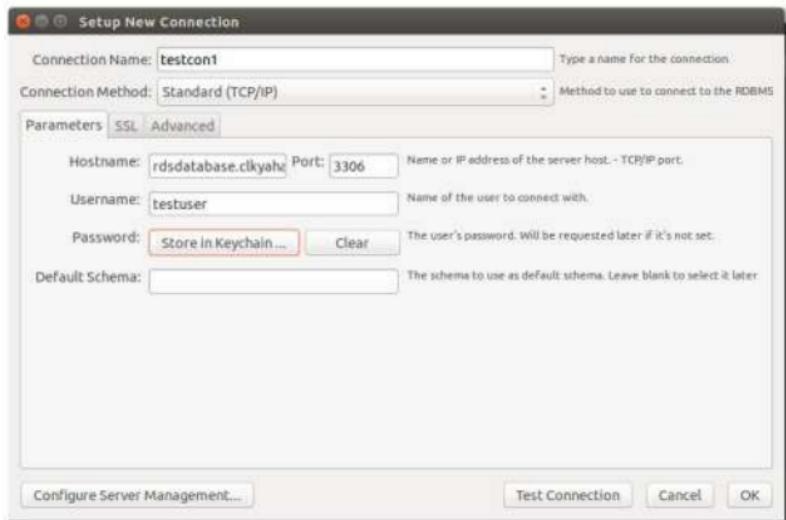
Hostname → copy RDS url

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

Port → 3306

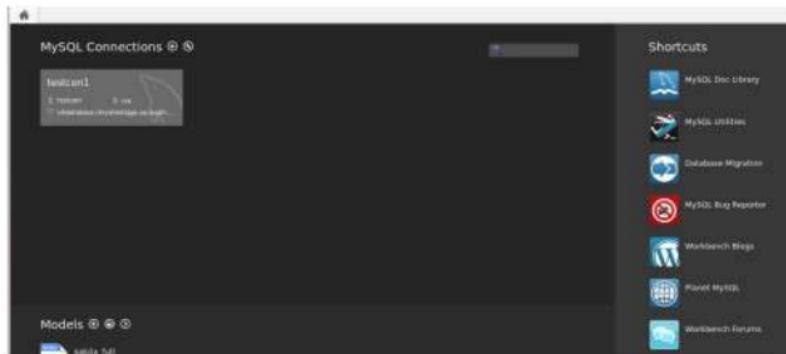
Username → testuser

Password → *****

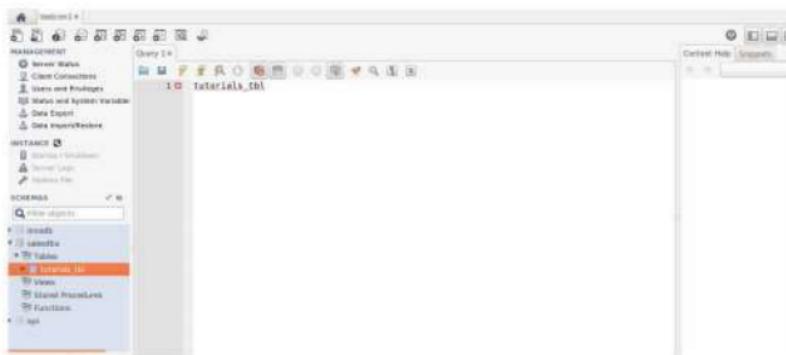


Verify

Connection is getting established.



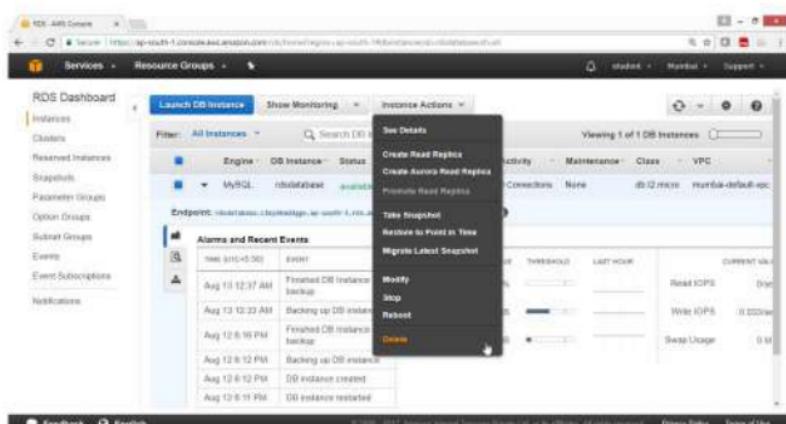
So we can see that tables are listed in Mysql clients.



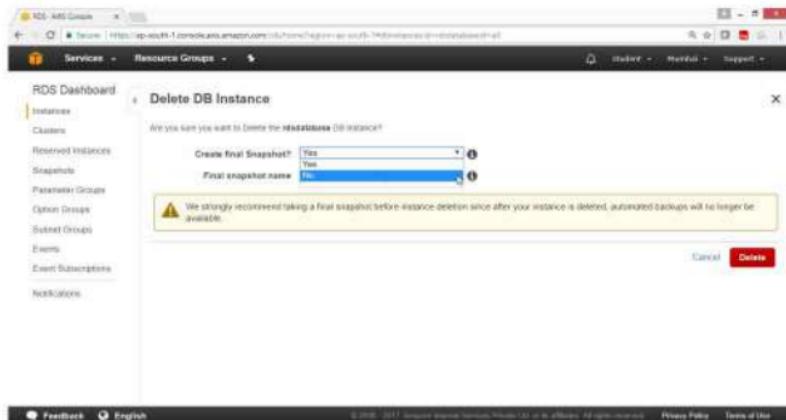
3. To Delete the RDS instance

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 options like Instances, Clusters, Reserved Instances, Snapshots, Parameter Groups, Option Groups, Subnet Groups, Events, Event Subscriptions, and Notifications. The main area has tabs for Launch DB Instance, Show Monitoring, and Instance Actions. A search bar says "Search DB Instances...". Below it, a table lists one instance: "Engine: MySQL" and "DB Instance: rdsdb00565". The "Status" column shows "deleting". Other columns include CPU (7.00%), Current Activity (0 connections), Maintenance (None), Class (db.t2.micro), VPC (rdsdb00565.vpc), and Multi-AZ (No). Below the table, there are two sections: "Alarms and Recent Events" and "Monitoring". The "Alarms and Recent Events" section lists several events with timestamps from Aug 13 at 12:37 AM to Aug 13 at 0:11 PM. The "Monitoring" section shows CPU usage at 0.91%, Memory usage at 536 MB, Storage usage at 4,532 GB, and Swap usage at 0 MB.

Delete Confirmed

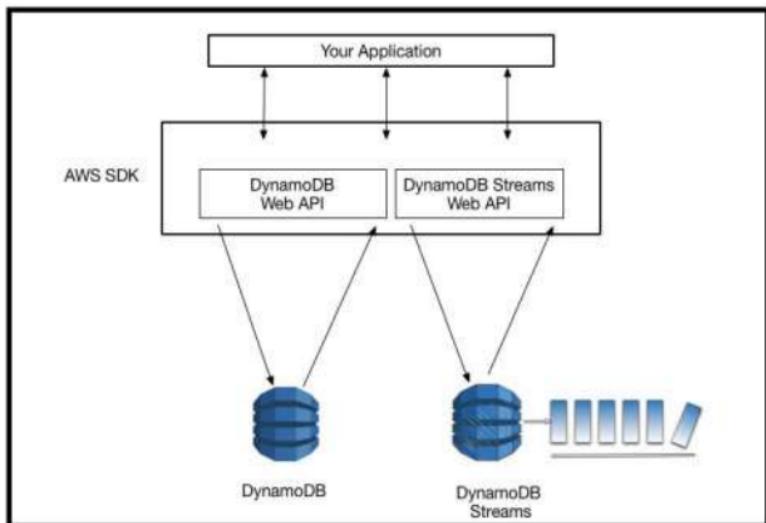
This screenshot is from the same RDS Dashboard as the previous one, but the MySQL instance is now listed as "deleted" in the status column. The rest of the interface remains the same, including the sidebar, the table with the deleted instance, and the "Alarms and Recent Events" and "Monitoring" sections.

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

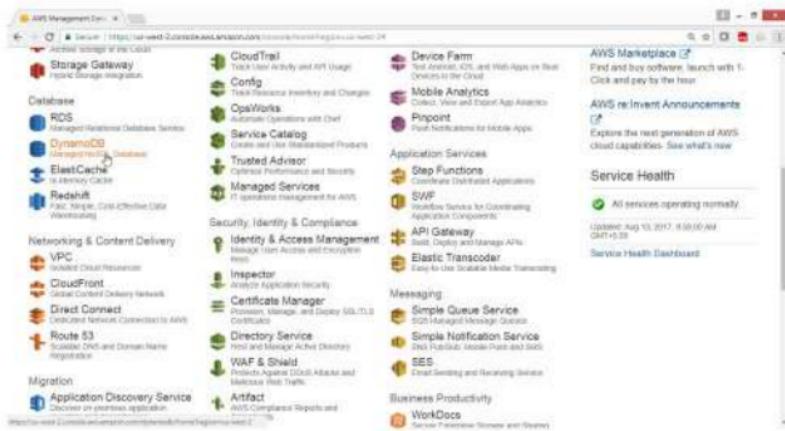
1) To Create an Amazon DynamoDB table

To Create Table

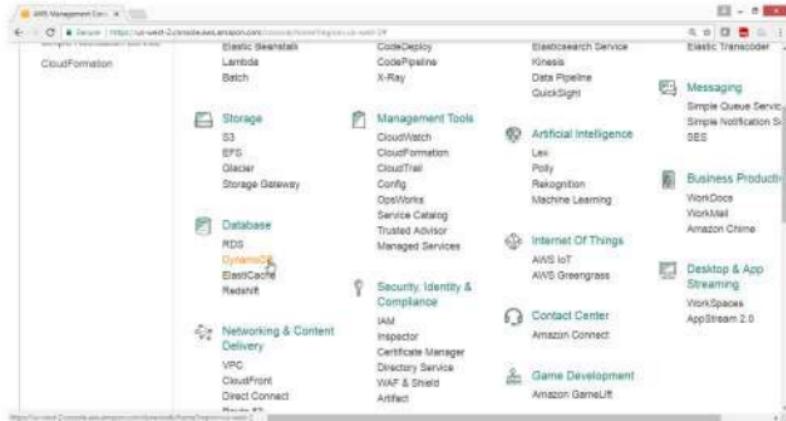
[Open AWS console](#)

Select services Database

[Click on DynamoDB](#)

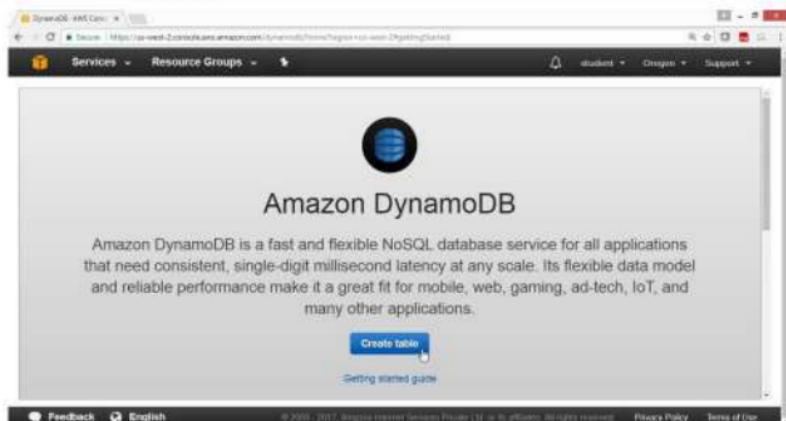


OR



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 navigation bar with links like 'Services', 'Resource Groups', 'Tutorial', 'Student', 'Groups', and 'Support'. Below the title 'Create DynamoDB table', a note states: 'DynamoDB is a schema-less database that only requires a table name and primary key. The table's primary key is made up of one or two attributes that uniquely identify items, partition the data, and sort items within each partition.' The main configuration area has two fields: 'Table name*' containing 'Salestable' and 'Primary key*' containing 'itemno' with a dropdown menu showing 'String'. There's also a checkbox 'Add sort key' which is unchecked. Under 'Table settings', there's a note: '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.' Below this, there are two radio button options: 'Use default settings' (selected) and '+ No secondary indexes.'

Under Table settings

Select "Use default settings" check box

click on **Create** button

The screenshot shows the 'Table settings' step of the 'Create Table' wizard. It includes the following elements:

- Table settings**: A section describing default settings and how to modify them.
- Use default settings**: A checked checkbox.
- Additional charges may apply if you exceed the AWS Free Tier limits for CloudWatch or Simple Notification Service.**: A note about additional charges.
- You do not have the required role to enable Auto Scaling by default.**: A message indicating a missing role.
- Create**: A blue 'Create' button at the bottom right.

Creating

The screenshot shows the 'Saleable' step of the 'Create Table' wizard. It includes the following elements:

- Saleable**: A tab selected in the top navigation bar.
- Overview**: A sub-tab under 'Saleable'.
- Table is being created**: A message in a box.
- Recent alerts**: A section stating "No CloudWatch alarms have been triggered for this table."
- Stream details**: A section with "Stream enabled: No", "View type: -", and "Latest stream ARN: -".
- Manage Stream**: A button for managing streams.
- Table details**: A section for viewing table details.

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, with 'Tables' selected. A search bar at the top right contains the filter 'Salestable'. The main panel displays the 'Salestable' table details under the 'Overview' tab. It shows 'Stream enabled: No', 'View type: -', and 'Latest stream ARN: -'. Below this, the 'Table details' section shows the 'Table name: Salestable'. At the bottom of the page, there are links for 'Feedback', 'English', and copyright information.

Select Capacity

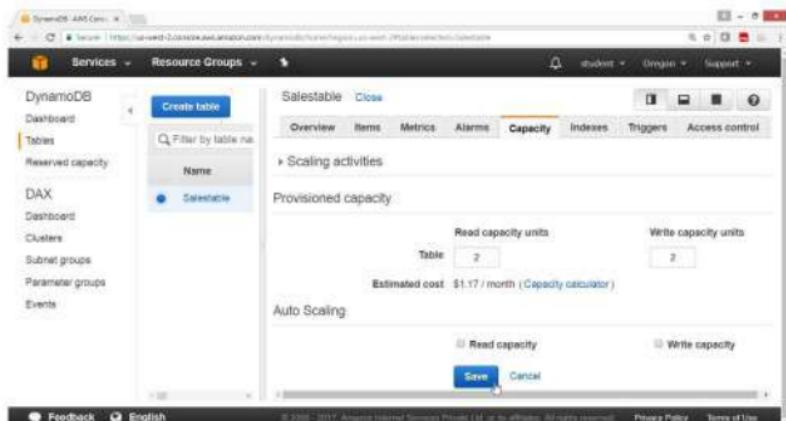
Under "Provisioned capacity"

Provide the following values

Read Capacity → 2

Write Capacity units → 2

Click on Save button



Select item

Click on **Create item**

The screenshot shows the AWS DynamoDB console. 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 says 'Scan: [Table] Salestable: Itemno <'. A note below the search bar states: '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 of the interface, there are links for 'Feedback', 'English', and legal notices.

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

The screenshot shows a 'Create item' dialog box. At the top, there is a toolbar with icons for back, forward, and search, followed by a close button (X). Below the toolbar is a tree view titled 'Tree'. The tree has a single node labeled 'Item {1}' which contains a single item named 'itemno String 1' (value: 1). This item is highlighted with a yellow background. At the bottom right of the dialog are two buttons: 'Cancel' and 'Save'.

Select insert, select string

ItemName String fruits



Verify output

The screenshot shows the AWS Lambda function editor with the 'Create item' step. The code pane contains the following JSON object:

```
{ "Item": { "fruits": "String", "itemno": "String" } }
```

A context menu is open over the 'itemno' field, with the 'Insert' option selected. The 'Insert' option is highlighted in blue, while 'Append' and 'Remove' are grayed out. The 'Save' button is visible at the bottom right of the code area.

The screenshot also shows the AWS DynamoDB 'Create item' results page. It displays the same JSON object:

```
{ "Item": { "fruits": "String", "itemno": "String" } }
```

The 'Save' button is visible at the bottom right of the results area. The left sidebar shows the AWS navigation menu.

Click on plus radio button

select insert, select number

Ph → 123456789

click on **Save**



To View all entered data

select Scan , click start search

The screenshot shows the AWS DynamoDB console. On the left, there's a sidebar with options like 'Create table', 'Tables', 'Reserved capacity', 'DAX', 'Clusters', 'Subnet groups', 'Parameter groups', and 'Events'. The 'Tables' section is selected. In the main area, a table named 'Salestable' is shown. The 'Items' tab is selected. A search bar at the top says 'Scan: [Table] Salestable: itemno'. Below it, a dropdown menu shows 'Scan' is selected. A button labeled 'Start search' is visible. The results table has columns 'Itemno', 'Ph', and 'fruits'. One row is listed: Itemno 1, Ph 1234567890, fruits fruits.

To add values in the created fields

Select the Table row, click Action button

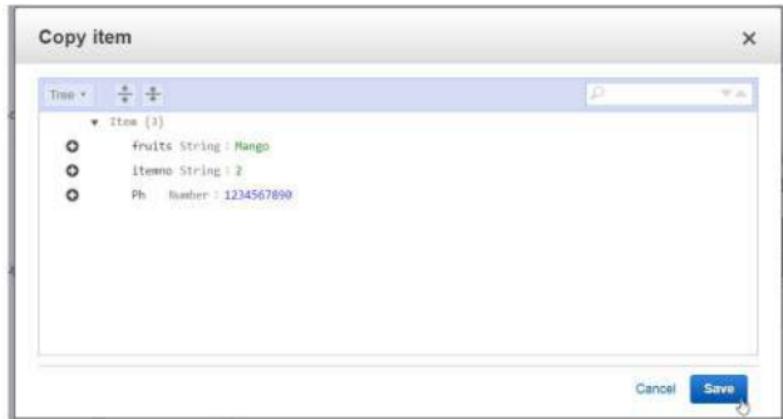
select Duplicate

This screenshot is similar to the previous one, showing the AWS DynamoDB console with the 'Salestable' table. The 'Actions' dropdown menu is open over the first table row. The 'Duplicate' option is highlighted with a red box. Other options in the menu include 'Edit', 'Delete', 'Export to .csv', and 'Manage TTL'. The table below shows the same data as before: Itemno 1, Ph 1234567890, fruits fruits.

Now modify the values of the field

New row will be created

Click on save



Verify

The screenshot shows the AWS DynamoDB 'Items' page for a table named 'Salestable'. The table contains two items:

Itemno	Ph	fruits
2	1234567890	Mango
1	1234567890	truts

On the left, the navigation pane shows 'Tables' selected. On the right, the 'Items' tab is active. A 'Scan' filter dropdown is open at the top, with 'Scan' and 'Add filter' options. The status bar at the bottom indicates 'Viewing 1 to 2 items'.

To Delete the table permanently for DymonaDb

From the AWS console

Select services Database

Choose DynamoDB

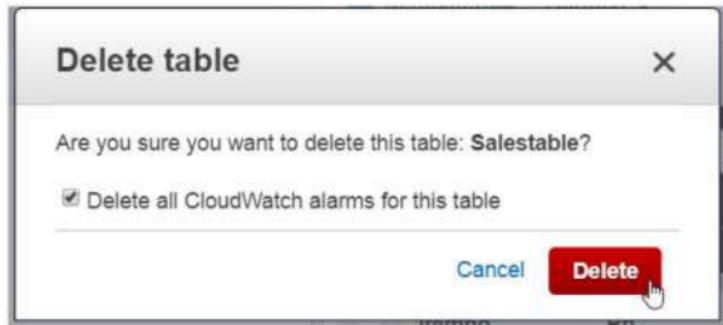
Under **Tables**, select the table for the list

click on Action button

Select "Delete Table"

The screenshot shows the AWS DynamoDB console interface. On the left, the navigation pane is visible with options like 'DynamoDB', 'Dashboard', 'Tables' (which is selected), 'Reserved capacity', 'DAX', 'Clusters', 'Subnet groups', 'Parameter groups', and 'Events'. In the center, there's a table named 'Salestable'. A context menu is open over the table, with the 'Actions' dropdown expanded. The 'Delete table' option is highlighted with a yellow background and a black border. To the right of the table, the main content area shows the table's details: Overview, Items, Metrics, Alarms, Capacity, and More. Below these tabs, there's a 'Create Item' button and another 'Actions' dropdown. The 'Items' tab is active, displaying a list of items with attributes 'Iidemo', 'Ph', and 'Fruits'. Two items are listed: one with Iidemo 2, Ph 1234567890, and Fruits Mango; and another with Iidemo 1, Ph 1234567890, and Fruits Tutta. At the bottom of the page, there are links for 'Feedback', 'English', '© 2008–2017, Amazon Internet Services Private Ltd. All Rights Reserved.', 'Privacy Policy', and 'Terms of Use'.

Click on Delete button



Verify Table is deleted.

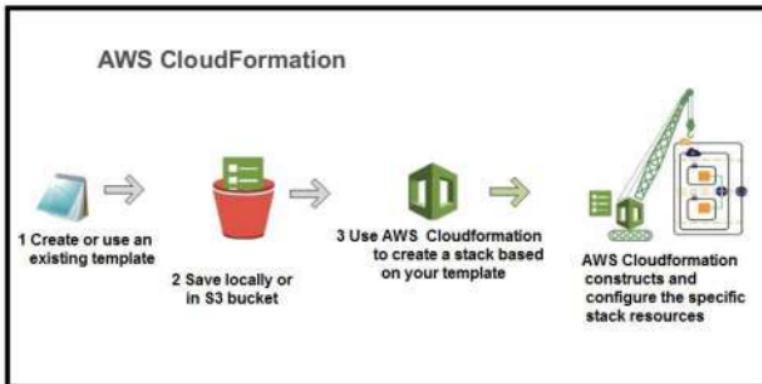
A screenshot of the AWS DynamoDB service dashboard. The left sidebar shows 'Tables' selected. In the main area, there is a table with one row. The table has columns for 'Name', 'Status', 'Item Count', and 'Last Scan Time'. The single row is for the 'Salestable' table, which is now listed as 'Deleted'. A tooltip for the 'Salestable' row provides information about the service and links to 'More Info'.

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

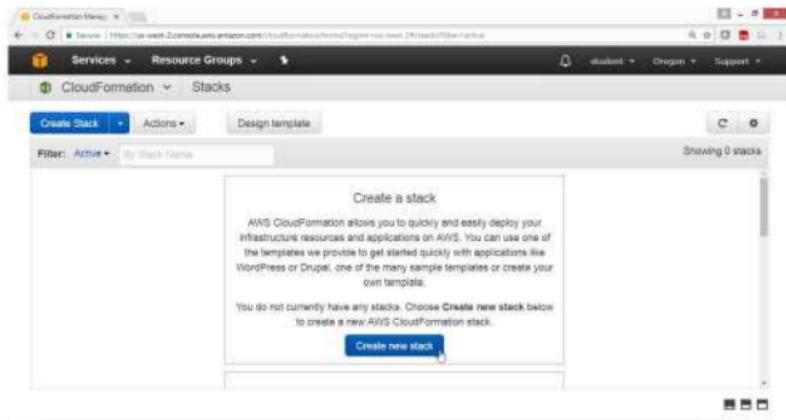
Click on CloudFormation service.

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/cloudformation/home?region=us-east-1>. The page displays the CloudFormation service under the 'Management Tools' category. On the left, there's a sidebar with various AWS services like Compute, Storage, and Management Tools. The main content area shows the CloudFormation interface, which includes sections for 'CloudFormation Stacks' (with a 'Create New Stack' button), 'CloudWatch Metrics' (with a 'View Metrics' button), and 'AWS Lambda Functions' (with a 'View Functions' button). On the right, there's a 'Resource Groups' section with a 'Create a Group' button and a 'Tag Editor' button. Below that is an 'Additional Resources' section with links to 'Getting Started', 'AWS Console Mobile App', and 'AWS Marketplace'. The top navigation bar includes 'Services', 'Resource Groups', and user account information.

2) To create a new stack

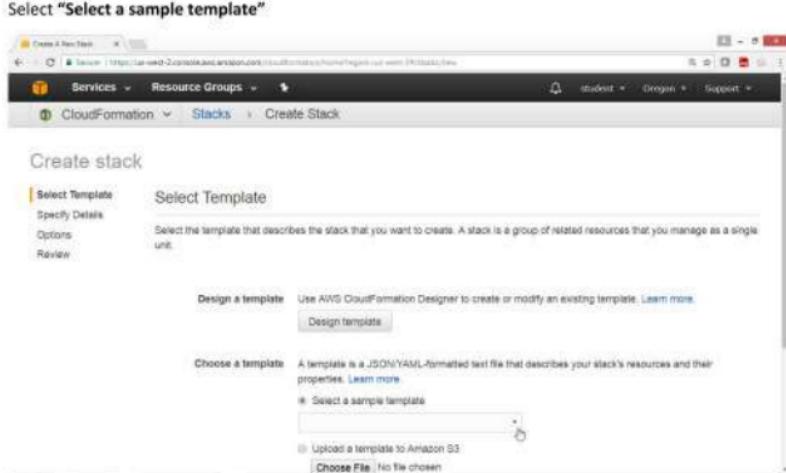
On “Create Stack”, page

Click on “Create New Stack” button



Under “Choose a template”

Select “Select a sample template”

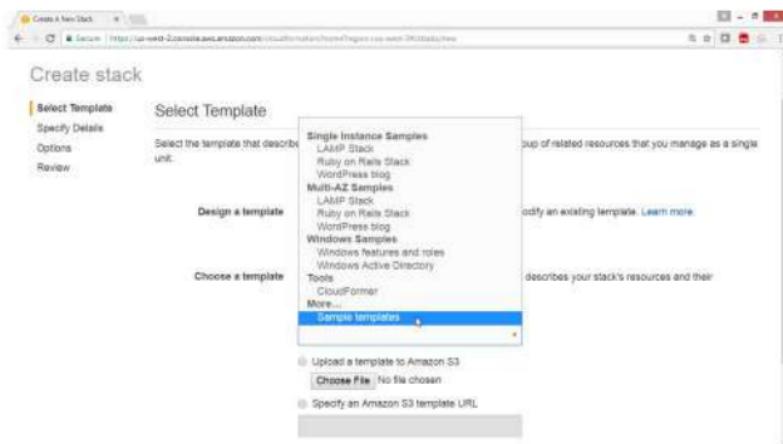


On **Create stack** page

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', 'Services', 'Products', 'More', 'English', 'My Account', and 'Sign In to the Console'. Below the navigation is the AWS logo and a search bar. The main title is 'AWS CloudFormation Templates'. A sub-section title 'Templates & Snippets by AWS Service' follows, with links to 'Browse sample templates by AWS service', 'Browse template snippets by AWS service', and 'Refer to our developer documentation for more examples and references'. Another section, 'Application Frameworks', has a link to 'Application framework templates demonstrate how to use AWS CloudFormation to provision popular frameworks such as LAMP and Ruby on Rails.'. To the right, there's a 'Reference Implementations' section with 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 that is a 'Sample Solutions' section with a link to 'Visit AWS Test Drive to try popular IT solutions from vendors such as Oracle and Microsoft, provisioned using AWS CloudFormation in a private sandbox environment.' At the bottom of the page, there's a footer with links to 'Documentation - This Guide', 'Search', 'What is AWS CloudFormation?', 'Setting Up', 'Getting Started', 'Best Practices', 'Continuous Delivery', 'Working with Stacks', 'Working with Templates', 'Working with AWS CloudFormation stacks', and 'Terms of Use | © 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.' There are also 'Did this page help you?' buttons for 'Yes' and 'No'.

Under Topics

Select Amazon EC2

The screenshot shows the AWS CloudFormation page under the 'Amazon EC2' topic. The left sidebar has a 'Topics' section with a tree view: 'Amazon EC2' is expanded, showing 'Auto Scaling', 'AWS Config', 'Amazon DynamoDB', 'Amazon Fargate', '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'. The main content area displays the text: 'The service sample templates show you how you can use AWS CloudFormation with other AWS services.' Below this is a 'Topics' section with the same list of services as the sidebar. At the bottom, there are links for 'Documentation - This Guide', 'Search', 'What is AWS CloudFormation?', 'Setting Up', 'Getting Started', 'Best Practices', 'Continuous Delivery', 'Working with Stacks', 'Working with Templates', 'Working with AWS CloudFormation stacks', and 'Terms of Use | © 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.' There are also 'Did this page help you?' buttons for 'Yes' and 'No'.

Select "Amazon EC2 instance in a security group",

Click on "Launch stack"

The screenshot shows the AWS CloudFormation console with the URL <https://console.aws.amazon.com/cloudformation/home#/stacks?region=us-east-1>. The page displays a table of AWS CloudFormation templates under the heading "Amazon EC2".

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 similar template list:

Template Name	Description	View	View in Designer	Launch
ElastiCache	Create 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" and "Feedback", along with a "Did this page help you?" poll with "Yes" and "No" options.

In option "Specify an Amazon S3 template URL"

Verify template is loaded in S3

Click on **Next** button

The screenshot shows the AWS CloudFormation Designer interface. At the top, there are tabs for 'Create A New Stack', 'AWS CloudFormation', 'Services', 'AWS CloudWatch Metrics', and 'Create A New Stack'. Below the tabs, there's a 'Review' section with a progress bar. The main area is titled 'Design a template' with a sub-instruction: 'Use AWS CloudFormation Designer to create or modify an existing template. Learn more.' There are three options: 'Design template' (button), 'Choose a template' (radio button selected), and 'Upload a template to Amazon S3' (radio button). Under 'Choose a template', there are two sub-options: 'Select a sample template' (radio button selected) which shows a dropdown menu with 'aws-s3-bucket', 'aws-vpc', and 'aws-lambda'; and 'Specify an Amazon S3 template URL' (radio button selected) which has a text input field containing the URL <https://s3-us-west-2.amazonaws.com/cloudform/>. Below the URL is a link 'View/Edit template in Designer'. At the bottom right of the main area are 'Cancel' and 'Next' buttons. The footer of the page includes links for 'Feedback', 'English', '© 2008–2011 Amazon Web Services, Inc. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

On Specific Details page

Key Name → "key*.pem"

Click on Next button



Under Options Tag, provide values for

Key → Nameweb

Value → Web

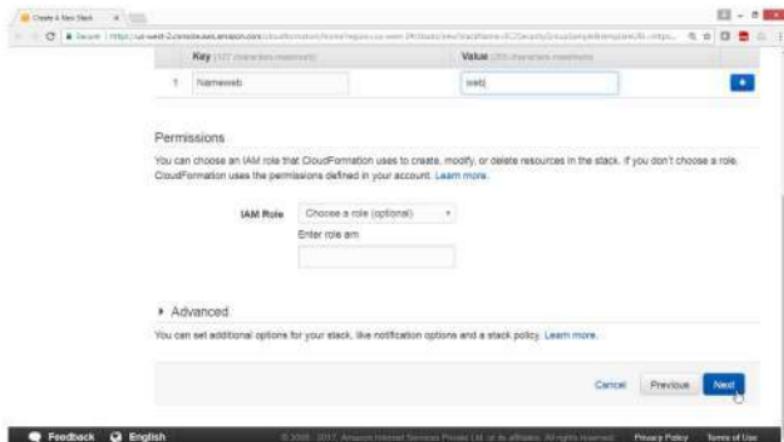
Drag Down

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 highlighted in yellow), and 'Review'. The main area is titled 'Options' and contains a section for 'Tags'. A note states: '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 is a table with two rows:

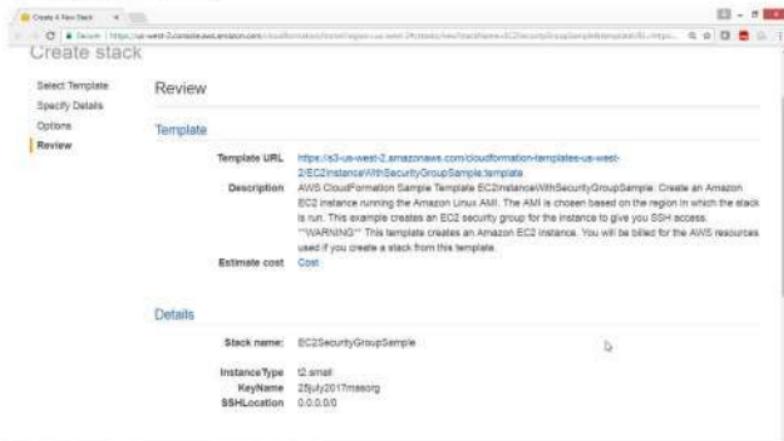
Key	Value
1 Nameweb	web

At the bottom of the 'Tags' section is a blue '+' button. Below the table is a section for 'Permissions' with the note: '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 fields for 'IAM Role' (with a dropdown menu showing 'Choose a role (optional)') and 'Enter role arn' (with a text input field).

Click on Next



Review , check the summary



Click Create button

The screenshot shows the 'Create A New Stack' wizard in the AWS CloudFormation console. The stack name is set to 'EC2SecurityGroupSample'. Configuration details include:

- InstanceType: t2.small
- KeyName: 25July2017mesorg
- SSHLocation: 0.0.0.0

Under the 'Options' tab, there are sections for 'Tags' (with 'Name' and 'web' listed) and 'Advanced' (with 'Notification' (Timeout: none), 'Rollback on failure' (Yes), and other parameters). At the bottom right of the wizard are 'Cancel', 'Previous', and 'Create' buttons.

Check the status

Cloudformation is in progress state.

The screenshot shows the 'Stacks' page in the AWS CloudFormation console. The stack 'EC2SecurityGroupSample' is listed with the following details:

Stack Name	Created Time	Status	Description
EC2SecurityGroupSample	2017-07-27 19:10:47 UTC+0650	CREATE_IN_PROGRESS	AWS CloudFormation Sample Template EC2Instan...

Verify

Status is Create_Complete

The screenshot shows the AWS CloudFormation console interface. At the top, there's a banner stating "AWS StackSets is a container for a set of AWS CloudFormation stacks and allows you to create stacks across multiple AWS Accounts and AWS Regions. Open the StackSets console to get started." Below the banner, there are three tabs: "Create Stack", "Actions", and "Design template". The "Actions" tab is currently selected. A filter bar below the tabs shows "Filter: Active" and "My Stack Name". The main area displays a table with one row of data:

Stack Name	Created Time	Status	Description
EC2SecurityGroupSample	2017-07-27 19:10:47 UTC-HC650	CREATE_COMPLETE	AWS CloudFormation Sample Template: EC2 instance security group

At the bottom of the page, there are links for "Feedback", "English", "© 2008 - 2017 Amazon Web Services, Inc. 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 Services, Resource Groups, Launch Instance, Connect, Actions, Instances, Images, and Elastic Block Store. The Instances section is currently selected, showing two instances: 'web' and 'web1'. The 'web' instance is highlighted with a blue selection bar. The details for the 'web' instance are shown in a modal window at the bottom right.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
web	i-0668c180a0f3da41	t2.small	us-west-2c	running	2/2 checks	None
web1	i-081e44151fc50525	t2.micro	us-west-2a	stopped	0/0 checks	OK

Modal window for Instance i-0668c180a0f3da41 (web):

Description	Status Checks	Monitoring	Tags
Instance ID: i-0668c180a0f3da41	Public DNS (IPv4): ec2-34-212-227-98.us-west-2.compute.amazonaws.com	Public DNS (IPv6): ec2-34-212-227-98.us-west-2.compute.amazonaws.com	
InstanceState: running	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 console interface. At the top, there's a navigation bar with 'Services', 'Resource Groups', and 'CloudFormation' selected. Below it, a sub-navigation bar has 'Stacks' selected. A modal window titled 'Introducing StackSets' is open, explaining what a StackSet is. The main content area shows a table of stacks. The table has columns: 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 EC2 instan...' as the description. Below the table, there are tabs for Overview, Outputs, Resources, Events, Template, Parameters, Tags, Stack Policy, and Change Sets. The 'Overview' tab is selected. At the bottom of the page, it says 'Stack name: EC2SecurityGroupSample'.

Stack Name	Created Time	Status	Description
EC2SecurityGroupSample	2017-07-27 19:10:47 UTC+0550	CREATE_COMPLETE	AWS CloudFormation Sample Template EC2 instan...

Click on Actions button

Select "Delete stack"

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.

Create Stack Actions Design template

Filter: Active ▾

Stack Name	Status	Description
EC2SecurityGroupSample	CREATE_COMPLETE	AWS CloudFormation Sample Template EC2Instan...

Showing 1 stack

Actions ▾

Create Change Set For Current Stack
Update Stack
Delete Stack (Currently selected)
View/Edit template in Designer

Overview Outputs Resources Events Template Parameters Tags Stack Policy Change Sets

Stack name: EC2SecurityGroupSample
Stack ID: arn:aws:cloudformation:us-west-2:623201683217:stack/EC2SecurityGroupSample/31f376a0-72d1-11e7a2e9-503f202ad1e
Status: CREATE_COMPLETE
Status reason:

© 2006-2015, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click on "Yes, Delete"

Are you sure you want to delete this stack?
EC2SecurityGroupSample
Deleting a stack deletes all stack resources.

Cancel Yes, Delete

Overview Outputs Resources Events Template Parameters Tags Stack Policy Change Sets

Stack name: EC2SecurityGroupSample
Stack ID: arn:aws:cloudformation:us-west-2:623201683217:stack/EC2SecurityGroupSample/31f376a0-72d1-11e7-a2e9-503f202ad1e
Status: CREATE_COMPLETE

Feedback Report

Verify

Deletion is in progress

The screenshot shows the AWS CloudFormation console with the URL <https://us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks>. The page displays a table of stacks. One stack, 'EC2SecurityGroupSample', is listed with the status 'DELETE_IN_PROGRESS'. The table columns include Stack Name, Created Time, Status, and Description. Below the table, there are tabs for Overview, Outputs, Resources, Events, Template, Parameters, Tags, Stack Policy, and Change Sets. The 'Overview' tab is selected.

Stack Name	Created Time	Status	Description
EC2SecurityGroupSample	2017-07-27 19:10:47 UTC+0650	DELETE_IN_PROGRESS	AWS CloudFormation Sample Template EC2 instan...

Verification

After deletion again starting screen of CloudFormation is displayed

The screenshot shows the AWS CloudFormation console with the URL <https://us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks>. The page displays a 'Create a stack' wizard. It includes a descriptive text about CloudFormation, a note that no stacks are currently present, and a 'Create new stack' button. Below the button, there are tabs for Feedback, English, Copyright notice, Privacy Policy, and Terms of Use.

Create a stack

AWS CloudFormation allows you to quickly and easily deploy your infrastructure resources and applications on AWS. You can use one of the templates we provide to get started quickly with applications like WordPress or Drupal, one of the many sample templates or create your own template.

You do not currently have any stacks. Choose **Create new stack** below to create a new AWS CloudFormation stack.

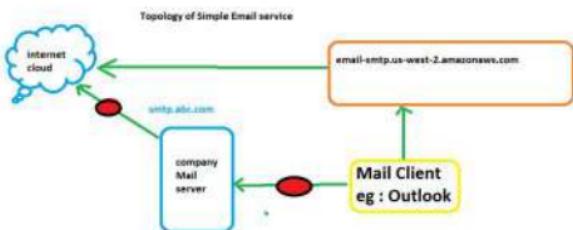
Create new stack

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

Objective

TO configure and use Simple Email Service (SES)

Topology



PRE-REQUISITES

User should have AWS account, or IAM user with AmazonSESFullAccess

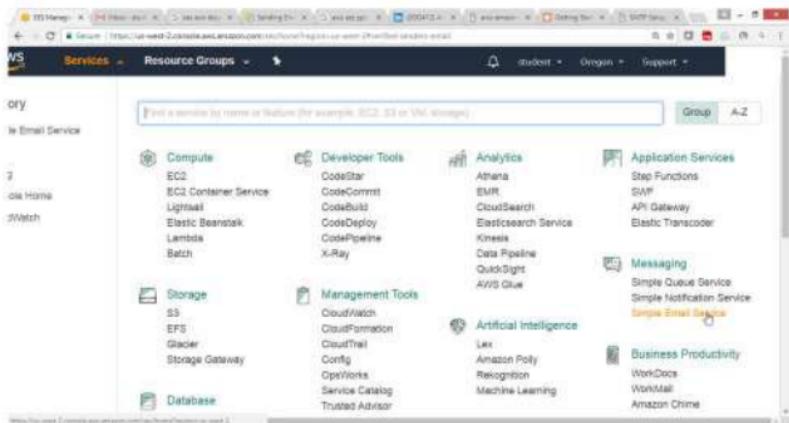
To Configure SES with following task:

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

To use Amazon Simple E-Mail Service SES

1. Create SES account

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



From SES Home, panel

select "Email Addresses"

The screenshot shows the AWS Simple Email Service (SES) home page. On the left, a sidebar menu lists various options: Identity Management, Domains, Email Addresses (which is highlighted in blue), Email Sending, Sending Statistics, Reputation Dashboard, Dedicated IPs, Configuration Sets, SMTP Settings, Suppression List Removal, Cross-Account Notifications, Feedback, and English (US). The main content area features the Amazon SES logo and the text: "Amazon Simple Email Service enables you to send and receive email using a reliable and scalable email platform." It also includes three icons: two people with a plus sign, a computer monitor with a graph and an envelope, and two interlocking gears.

Select "Verify a New Email Address" button

The screenshot shows the "Verify a New Email Address" page. At the top, there is a search bar labeled "Search email addresses" and a dropdown menu set to "All identities". Below this, a section titled "Email Address Identities" displays a message: "You have not verified any email addresses. To verify a new email address, click the Verify a New Email Address button above." The left sidebar contains the same navigation options as the previous screenshot. The bottom of the page includes standard AWS footer links: Feedback, English (US), © 2006 - 2017, Privacy Policy, and Terms of Use.

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



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

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

Go back to your Amazon Console, select SES service

Under SES home dashboard select "Email Address"

Check your email is **verified**

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

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

3. To configure SMTP settings

From SES Home panel

Select "SMTP Setting"

Click on "Create My SMTP Credentials" button

SES Management Console

aws Services Resource Groups student Orange 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) © 2008–2012 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 screenshot shows the 'Create User for SMTP' page in the AWS IAM Management Console. The URL in the browser is <https://console.aws.amazon.com/iamv2/home#/createUserForSmtp>. The page title is 'Create User for SMTP'. It contains a form with a single input field labeled 'IAM User Name:' containing the value 'ses-smtp-user.20171111-13'. Below the input field is a link 'Show More Information'. At the bottom right are two buttons: 'Cancel' and 'Create'.

User SMTP Security Credentials will be displayed

click "Download Credentials" keep at safe place

This screenshot shows the 'User SMTP Security Credentials' page in the AWS IAM Management Console. The URL in the browser is <https://console.aws.amazon.com/iamv2/home#/choosePki/20171111-13>. The page title is 'User SMTP Security Credentials'. It displays a message 'Your 1 User(s) have been created successfully.' and a note that the credentials are only available during the creation process. Below this is a section titled 'Hide User SMTP Security Credentials' which contains the user's details: 'ses-smtp-user.20171111-135833', 'SMTP Username: AKIAJXWQLY0S74PRQWQ', and 'SMTP Password: AmnF45T0H2G9z4Dk3nBHOH4+st7gMbznaKbVJZ1'. At the bottom right are 'Close' and 'Download Credentials' buttons.

Verify credentials

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/home?region=us-east-1#>. The Services menu is open, and the Resource Groups option is selected. A modal window titled "Create User for SMTP" is displayed, stating "Your 1 User(s) have been created successfully." It includes a note: "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 this is a link "Hide User SMTP Security Credentials". A yellow callout box highlights the download link: "aws-smtp-user.20171111-135833". The modal also shows the SMTP Username "AMAZON" and SMTP Password "AdminSP4".

Open Outlook

The screenshot shows the Microsoft Outlook 2016 application window. The ribbon tabs include FILE, HOME, MAIL, REACTIONS, FINDER, and NEW. The main view displays the inbox with one unread email from "AWS Support" with the subject "AWS Lambda function test succeeded". The calendar view shows Saturday, November 11, 2017, with no scheduled events. The tasks and messages sections are also visible.

Click Add Account



Outlook Today - Outlook

?

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

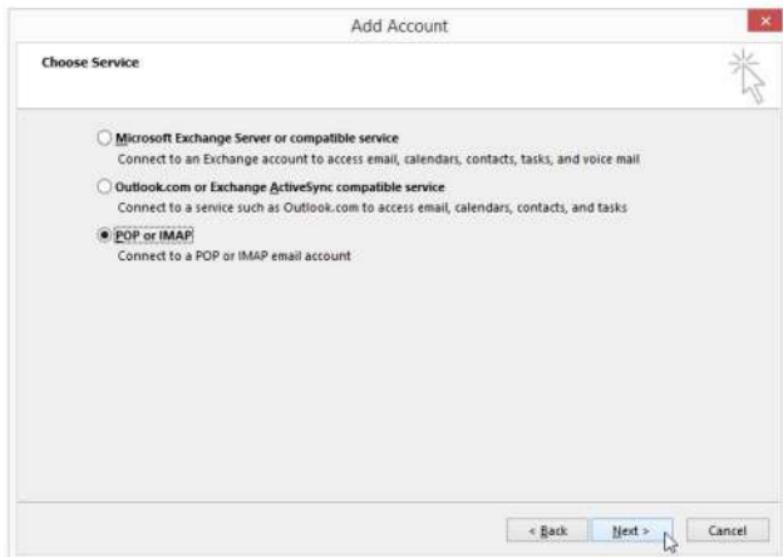
Password:

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 ...

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

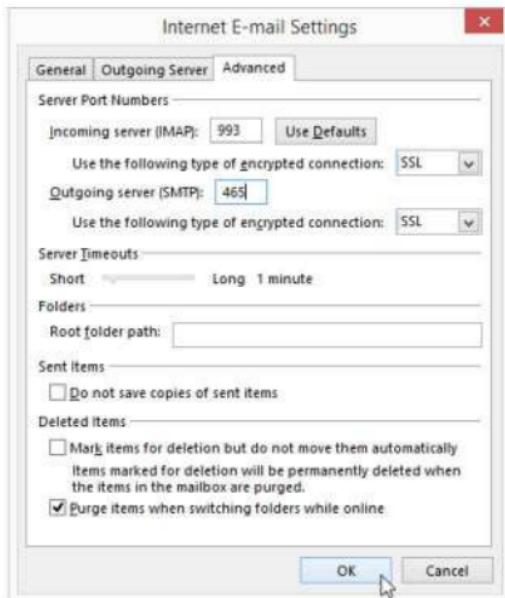
Require logon using Secure Password Authentication (SPA) More Settings ...

< Back Next > Cancel

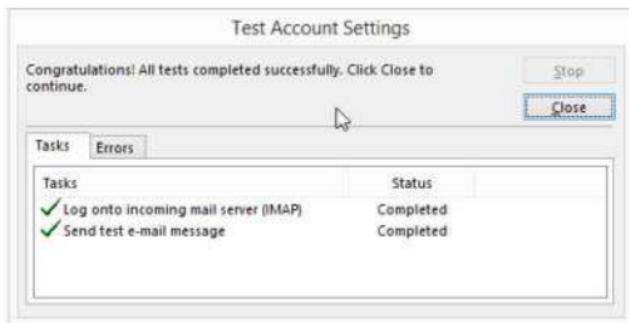
Provide following details in Outgoing Server



Provide following details in Advance



Verify successfully connected

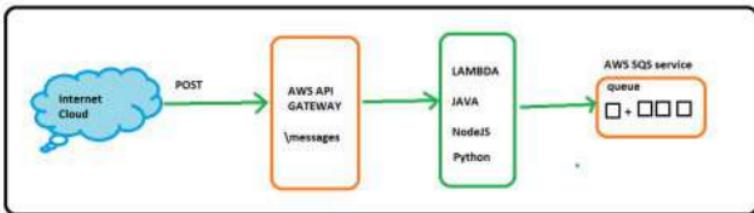


Lab 19: To Configure Amazon Simple QUEUE Service SQS

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 with the 'Services' tab selected. The 'Messaging' category is highlighted with a yellow circle. Other categories like Compute, Storage, Database, Developer Tools, Management Tools, Analytics, Artificial Intelligence, Application Services, Business Productivity, and Notifications are also visible.

Click on **Get started on**

The screenshot shows the Simple Queue Service landing page. It features a large yellow 3D cube icon, the text "Simple Queue Service", and a brief description: "Amazon Simple Queue Service (SQS) is a reliable, scalable, fully-managed message queuing service." Below the description are two buttons: "Get Started Now" and "Learn more about AWS SQS".

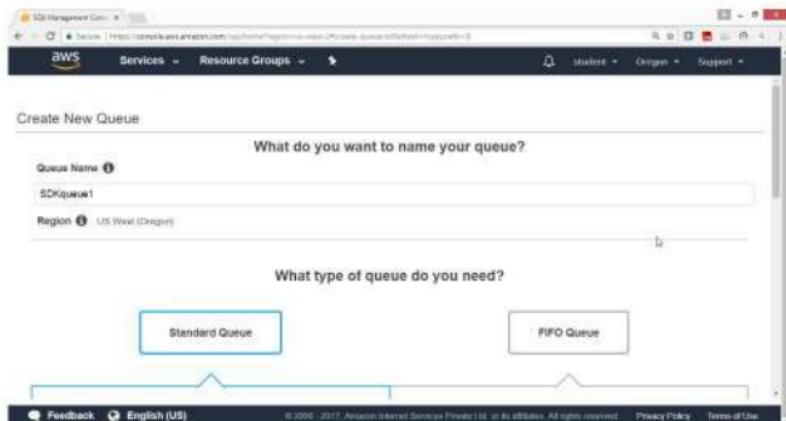


In "Create New Queue" wizard

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. At the top, there's a navigation bar with 'Services' and 'Resource Groups'. Below it, a search bar contains 'student'. On the right, there are 'Support', 'student', 'Oregon', and 'Sign Out' buttons.

The main area has two 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 rendering 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's a note: "For more information, see the Amazon SQS FAQs and the Amazon SQS Developer Guide". Below that, a message 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 a blue "Quick-Create Queue" button.

At the very bottom, there are links for "Feedback", "English (US)", and legal notices: "© 2006-2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.", "Privacy Policy", and "Terms of Use".

Verify Queue is Created

The screenshot shows the AWS SQS Management Console with a single queue listed under "Create New Queue" and "Queue Actions".

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

Below the table, the "1 SQS Queue selected" section shows the queue details:

Details	Permissions	Redrive Policy	Monitoring	Tags	Encryption
Name: SDKqueue1 URL: https://sqs.us-east-2.amazonaws.com/522251632217/SQSqueue1 ARN: arn:aws:sqs:us-east-2:522251632217:SQSqueue1 Created: 2017-11-12 18:42:48 GMT+05:30 Last Updated: 2017-11-12 18:42:48 GMT+05:30	Placeholder Placeholder				

On the right, there are configuration settings:

- 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 (Visible): 0

At the bottom, there are links for "Feedback", "English (US)", and legal notices: "© 2006-2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.", "Privacy Policy", and "Terms of Use".

Select the Queue

Drop down “Queue Action” button

select “Send message”

The screenshot shows the AWS Management Console interface for the Simple Queue Service (SQS). At the top, there's a navigation bar with 'Services' and 'Resource Groups'. Below it, a search bar and user information ('student' from 'Oregon'). The main area displays a table of queues, with one queue named 'SDKqueue1' selected. A context menu is open over this queue, with the 'Send a Message' option highlighted. The menu also includes 'View/Delete Message', 'Configure Queue', 'Add a Permission', 'Delete Queue', and 'Subscribe Queue to SNS Topic'. The table below shows details for the selected queue, including its name, URL, ARN, creation and update times, and visibility timeout settings.

Name	URL	ARN	Created	Default Visibility Timeout	Message Retention Period	Maximum Message Size	Receive Message Wait Time	Messages Available (Visible)	Messages In Flight	Created
SDKqueue1	https://sqs.us-west-2.amazonaws.com/523251683217/SDKqueue1	arn:aws:sqs:us-west-2:523251683217:SDKqueue1	2017-11-12 18:42:48 GMT+05:30	30 seconds	4 days	256 KB	0 seconds	0	0	2017-11-12 18:42:48 GMT+05:30

Feedback English (US) © 2006–2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

From "Send a Message to SDKqueue" Wizard

In Message Body type the Message

Note: Message size should not be more than 64K

click on "Send Message" then elect close

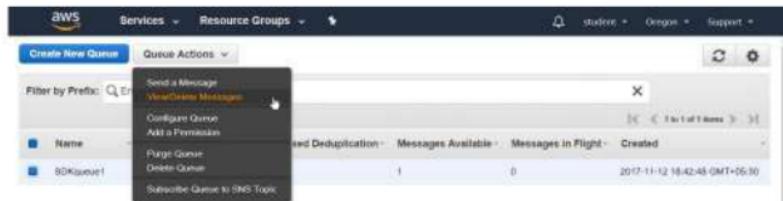


2) To View the message

Select the Queue

Drop down Queue Action button

Select the option "View/Delete Message"



The screenshot shows the AWS SQS Queue Actions dropdown menu. The 'View/Delete Message' option is highlighted with a mouse cursor. The menu also includes options like 'Send a Message', 'Configure Queue', 'Add a Permission', 'Purge Queue', and 'Delete Queue'. Below the menu, the SQS queue details are visible, including the queue name '80Kqueue1', a single message entry with the URL 'https://sns.us-west-2.amazonaws.com/523251633217/SDResponse1', and other queue metadata.

1 SQS Queue selected:

Details	Permissions	Redrive Policy	Monitoring	Tags	Encryption
Name: SDResponse1 URL: https://sns.us-west-2.amazonaws.com/523251633217/SDResponse1 ARN: arn:aws:sns:us-west-2:523251633217:SDResponse1 Created: 2017-11-12 18:42:48 GMT+05:30 Last Updated: 2017-11-12 18:42:48 GMT+05:30 Published Policies: None					

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
More... in Right-Click Methods

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

Click "Start Polling for Message"

The screenshot shows the AWS SQS 'View/Delete Messages' interface for a queue named 'SDKqueue1'. At the top, it says 'View up to: 10 messages' and 'Poll queue for: 30 seconds'. A blue button labeled 'Polling for Messages...' is visible. Below this is a table with columns: Delete, Body, Size, Sent, and Receive Count. There is one message listed: 'test msg 1' (11 bytes, 2017-11-12 18:47:34 GMT+02:30, 2, More Detail). A progress bar at the bottom indicates 'Polling the queue at 0.0 items/second. Stopping in 19.8 seconds. Messages shown above are currently hidden from other consumers.' The progress bar is at 0%. A red 'Delete Message' button is located at the bottom right.

Verify message is in the queue

This screenshot shows the same AWS SQS interface after polling has begun. The progress bar at the bottom now shows '34%' completion. The message 'test msg 1' remains in the list. The red 'Delete Message' button is still present.

3) To delete the message

Select the Queue

Drop Down Queue Action

Select "Delete Message"

The screenshot shows the AWS Management Console with the AWS Services navigation bar at the top. A dropdown menu titled "Queue Actions" is open, listing options: "Send a Message", "View/Delete Messages", "Configure Queue", "Add a Permission", "Delete Queue", and "Subscribe Queue to SNS Topic". Below the menu, a table displays information for a queue named "SDKqueue1". The table columns include Name, URL, ARN, Created, Last Updated, Default Visibility Timeout, Message Retention Period, Maximum Message Size, Receive Message Wait Time, and Messages Available (Visible). The "Delete Queue" option is highlighted with a cursor.

Confirm

The screenshot shows a modal dialog box titled "Delete Queues". The message inside asks if the user is sure they want to delete the following queue, and any messages left in it. It lists "SDKqueue1 - contains 1 message." At the bottom right of the dialog are two buttons: "Cancel" and a red "Yes, Delete Queue" button with a checkmark icon. The footer of the dialog includes standard links: Feedback, English (US), © 2006–2011, Amazon Internet Services Inc. All rights reserved., Privacy Policy, and Terms of Use.

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

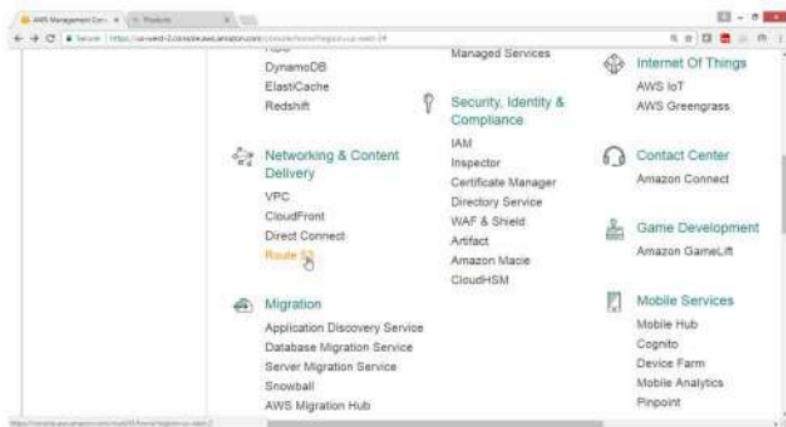
Creating CNAME record set

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 dashboard. At the top, it says "Amazon Route 53" and describes its purpose: "You can use Amazon Route 53 to register new domains, transfer existing domains, route traffic for your domains to your AWS and external resources, and monitor the health of your resources." Below this, there are four main service sections:

- DNS management**: Describes how Route 53 can help manage domain names. It includes a "Get started now" button.
- Traffic management**: Describes how Route 53 can help route traffic between multiple endpoints. It includes a "Get started now" button.
- Availability monitoring**: Describes how Route 53 can monitor the health and performance of applications. It includes a "Get started now" button.
- Domain registration**: Describes how Route 53 can help register domains. It includes a "Get started now" button.

At the bottom of the page, there are links for "Feedback", "English", "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 'Create Hosted Zone' button at the top. Below it is a description of Route 53 as an authoritative DNS service. At the bottom is a 'Create Hosted Zone' button.

Again Click on Create Hosted Zone button

The screenshot shows the AWS Route 53 Management console. The left sidebar has 'Hosted zones' selected. The main area displays a message 'You have no hosted zones.' and features a 'Create Hosted Zone' button.

Under "Created Hosted Zone", wizard

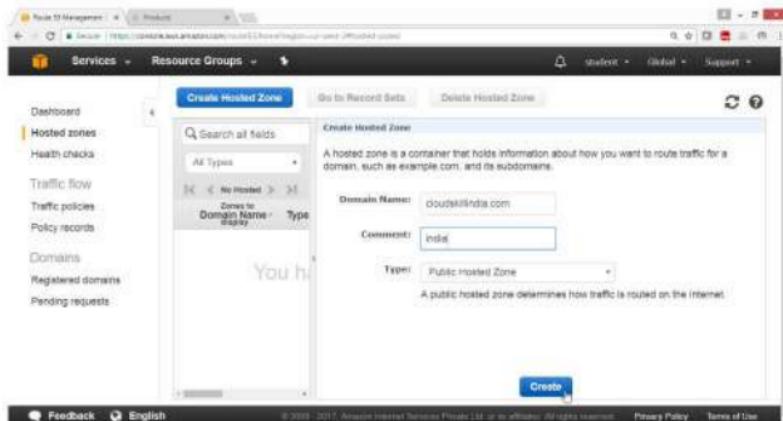
On right side panel provide following values

For Domain Name: → cloudskillindia.com

For Comment → india

For Type → Public Hosted Zone

Click on **Create** button



Now the list of AWS NS records will appear

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

The screenshot shows the AWS Route 53 Management console. In the top navigation bar, 'Services' is selected under 'Resource Groups'. The main area displays a 'Record Set Name' search bar and two filter buttons: 'Aliases Only' and 'Weighted Only'. Below this, a table lists two entries:

Name	Type	Value
cloudskillindia.com	NS	ns-140.awsdns-17.com. ns-165.awsdns-03.co.uk. ns-726.awsdns-26.net. ns-1256.awsdns-32.org.
cloudskillindia.com	SOA	ns-140.awsdns-17.com. awsoa

To the right of the table, a modal window titled 'Edit Record Set' is open. It contains fields for 'Name' (set to 'cloudskillindia.com'), 'Type' (set to 'NS - Name server'), and an 'Aliases' section. The 'Aliases' section includes a 'TTL (Seconds)' dropdown set to '1m', a 'Values' input field containing 'ns-140.awsdns-17.com.', and a note explaining how to enter multiple name servers on separate lines. A 'Save Record Set' button is at the bottom of the modal.

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

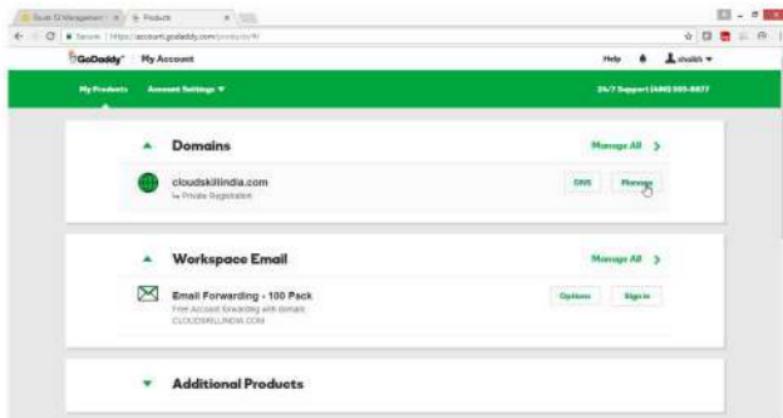
ns-140.awsdns-17.com
ns-1565.awsdns-03.co.uk
ns-726.awsdns-26.net
ns-1286.awsdns-32.org

Open the browser

Go to godaddy.com site

Login and select your domain name

Click on Manage



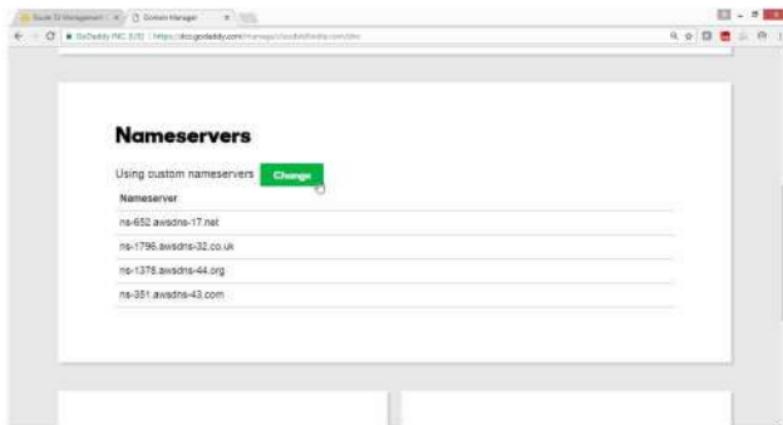
Drag Down

Click on Manage DNS

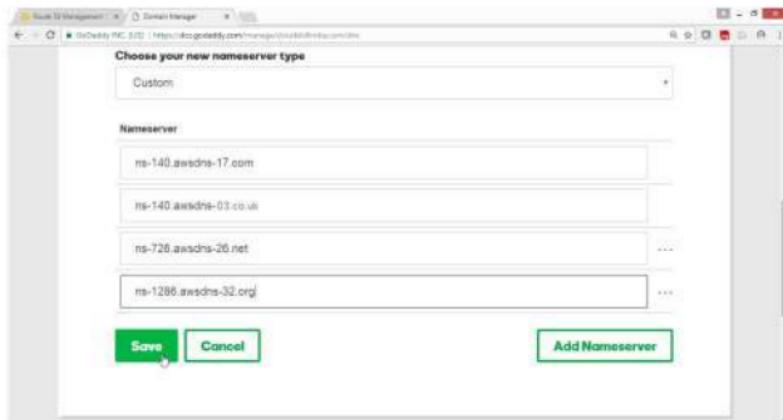
The screenshot shows a web browser window for GoDaddy Domain Management. The main content area is titled "Additional Settings". It includes a note about automatic removal if no payment is made by November 29, 2017, and a "Transfer Domain to Another GoDaddy Account" link. A "Locking" section indicates the domain is locked (OFF ESE). The right sidebar lists "Manage DNS", "Transfer domain to another GoDaddy account", "Delete domain from GoDaddy", "Get authorization code", and "Delete domain". At the bottom, there's a copyright notice and a link to "Privacy Policy".

Click on change

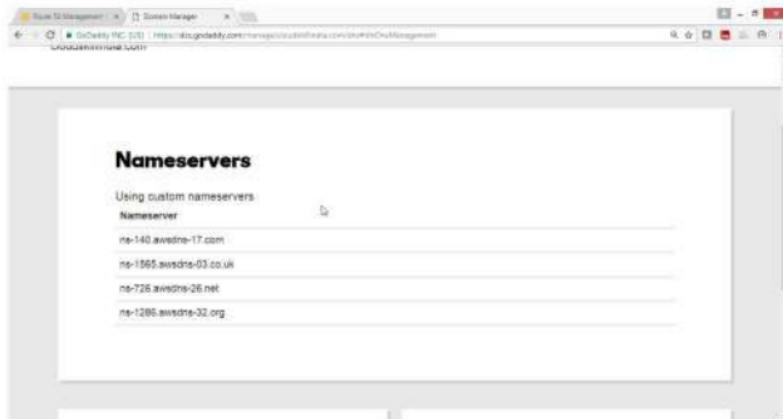
Add latest entries provided by Route53 NS records



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

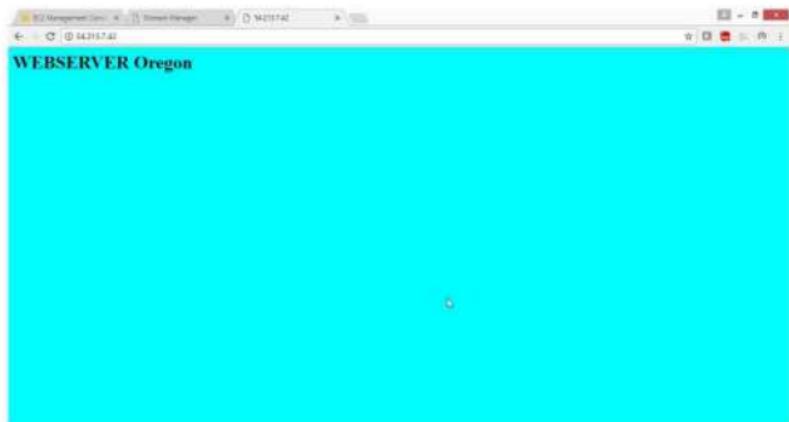
Configure it as a Web Server

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, Instances, Trades, 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, a table lists instances. One instance is selected, showing its details: Name (i-0988888cc1426206), Instance ID (i-0988888cc1426206), Instance Type (t2.micro), Availability Zone (us-east-2a), Instance State (running), Status Checks (2/2 checks), and Alarm (None). 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 Status Checks tab, it shows Instance ID (i-0988888cc1426206), Instance state (running), Instance type (t2.micro), and Elastic IPs. The Public DNS is also listed here. At the bottom of the page, there are links for Feedback, English, 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 management console. On the left, there's a sidebar with navigation links like Dashboard, Hosted zones, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The 'Hosted zones' link is highlighted. In the main content area, there's a search bar at the top labeled 'Search all fields' and a dropdown menu for 'All Types'. Below it, a table lists one hosted zone: 'Domain Name: cloudskillindia.com' (Type: Public, Record Set Count: 2). The table has columns for 'Domain Name', 'Type', and 'Record Set Count'. The 'cloudskillindia.com' row is selected. To the right of the table, there's a 'Hosted Zone Details' panel. It shows the domain name as 'cloudskillindia.com', the type as 'Public Hosted Zone', and the Hosted Zone ID as 'Z3JBZ3DEZMRNPV'. It also displays the 'Record Set Count: 2' and a 'Comments: India' field with a pencil icon. Under 'Name Servers', it lists four servers: 'ns-144.awsdns-17.org', 'ns-1555.awsdns-20.co.uk', 'ns-728.awsdns-26.net', and 'ns-1298.awsdns-32.org'. At the bottom of the details panel, there's a note: '* Before the domain name system can start to route queries for this domain to Route 53 name servers, you must update the name server records either with the current DNS service or with the registrar for the domain as applicable. For more information, click the ? icon below.' At the very bottom of the page, there are footer links for 'AWS Lab Manual', 'Page | 429', and 'www.zoomgroup.com'.

Click on Create Record set button

The screenshot shows the AWS Route 53 Management Console. In the top navigation bar, 'Services' is selected under 'AWS Cloud Services'. Below it, 'Resource Groups' is also visible. On the left sidebar, 'Hosted zones' is highlighted. The main content area displays a 'Create Record Set' dialog. At the top right of this dialog is a blue 'Create Record Set' button. To its left are 'Back to Hosted Zones' and 'Import Zone File' buttons. Below these are 'Delete Record Set' and a help link. The central part of the dialog has a search bar labeled 'Record Set Name' and a dropdown menu for 'Type'. Underneath, there are two tabs: 'Aliases Only' and 'Weighted Only'. A note below the tabs says 'Displaying 1 to 2 out of 2 Record Sets'. Two record sets are listed: one for 'cloudkafkaindex.com' of type 'NS' and another for 'cloudkafka.com' of type 'SOA'. A note at the bottom right of the dialog says 'To get started, click Create Record Set button or click an existing record set.'

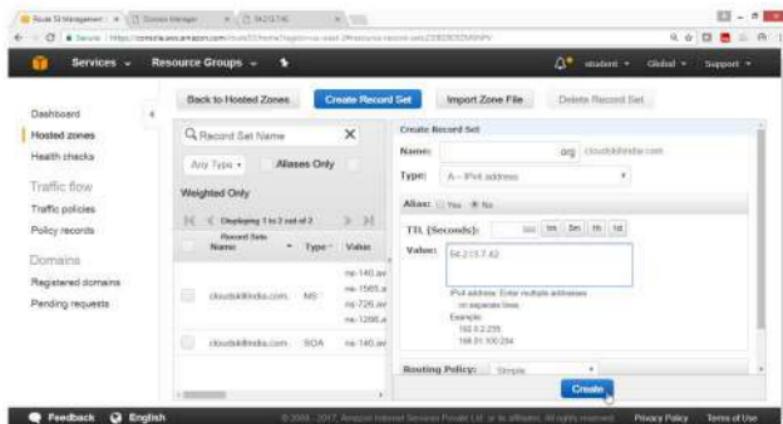
To add A record

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



Verify the A record got created

The screenshot shows the AWS Route 53 service dashboard. In the left sidebar, 'Hosted zones' is selected. The main area displays a table of existing record sets. On the right, a modal window titled 'Edit Record Set' is open for the record set 'org.cloudkillindia.com'. The 'Type' is set to 'A - IPv4 address'. The 'Value' field contains '54.213.7.42'. Below the table, a note says 'The IP address must resolve to one or more static IP addresses.' and provides examples: '98.10.2.255' and '198.51.100.234'. At the bottom of the modal is a 'Save Record Set' button.

Create Alias record

The screenshot shows the AWS Route 53 service dashboard. In the left sidebar, 'Hosted zones' is selected. The main area displays a table of existing record sets. On the right, a modal window titled 'Create Record Set' is open for a new record set. The 'Name' field is filled with 'www.cloudkillindia.com'. The 'Type' is set to 'CNAME - Canonical name'. The 'Value' field contains 'org.cloudkillindia.com'. Below the table, a note says 'The domain name that you want to resolve to instead of the value in the Name field.' and provides an example: 'www.example.com'. At the bottom of the modal is a 'Create' button.

Verify the CNAME record got created

The screenshot shows the AWS Route 53 service console. The left sidebar has 'Hosted zones' selected. The main area shows a table of records under a 'Record Set Name' search bar. The table has columns 'Name', 'Type', and 'Value'. The records listed are:

Name	Type	Value
cloudskillindia.com.	NS	ns-140.awsdns-17.co... ns-100.awsdns-03.co... ns-720.awsdns-20.co... ns-1286.awsdns-12.co...
cloudskillindia.com.	SOA	ns-140.awsdns-17.co...
org.cloudskillindia.com.	A	54.235.7.42
www.cloudskillindia.com.	CNAME	org.cloudskillindia.com

Verification

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

The screenshot shows a web browser window with the URL 'org.cloudskillindia.com' in the address bar. The main content area of the browser is filled with a solid cyan color, suggesting either a loading state or a failure to load the intended website.

Verification

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

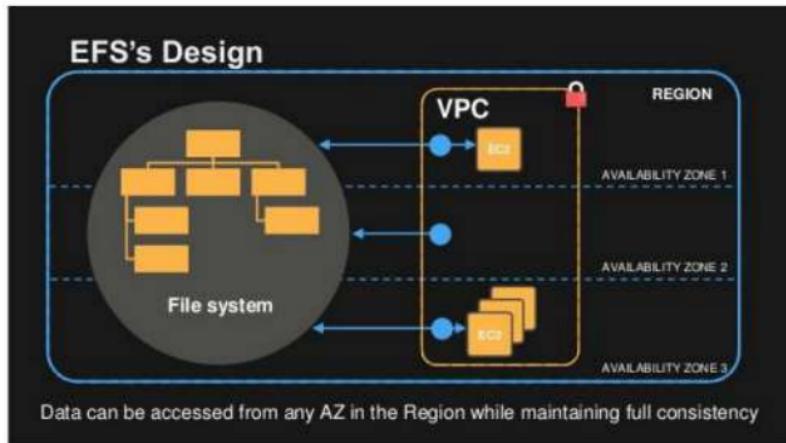


Lab 21: To configure Amazon EFS Service

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 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2&stackId=1>. The top navigation bar includes 'AWS Lab Manual', 'Getting Started with AWS', 'Services', 'Resource Groups', 'student', 'Oregon', and 'Support'. The left sidebar lists services: History, S3, Glacier, IAM, and EC2. The main content area is titled 'Find a service by name or feature (for example: EC2, S3 or VM, storage)' and displays several service categories: Compute (EC2 Container Service, Lambda, Batch), Developer Tools (CodeStar, CodeCommit, CodeBuild, CodeDeploy, CodePipeline, X-Ray), Analytics (Athens, EMR, CloudSearch, Elasticsearch Service, Kinesis, Data Pipeline, Quicksight, AWS Glue), Application Service (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), and Business Productivity (WorkDocs, WorkMail, Amazon Chime). A 'Group' button is located in the top right corner.

Under EC2 Dashboard go for Network & Security

Select Security Groups

Click on Create Security Group

The screenshot shows the AWS EC2 Management Console with the 'Create Security Group' wizard open. On the left, there's a sidebar with 'Bundle Tasks' and several service links: ELASTIC BLOCK STORE, Volumes, Snapshots, NETWORK & SECURITY (Security Groups is selected), Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, LOAD BALANCING (Load Balancer, Target Groups), and AUTO SCALING (Launch Configurations). The main area has tabs for 'Create Security Group' (selected) 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, Group ID, Group Name, VPC ID, and Description. There are four rows in the table:

Name	Group ID	Group Name	VPC ID	Description
	sg-275b2f64	launch-wizard-1	vpc-09c341ee	launch-wizard-
	sg-38295442	launch-wizard-2	vpc-09c341ee	launch-wizard-
	sg-42344bb8	launch-wizard-3	vpc-09c341ee	launch-wizard-
	sg-53577195	default	vpc-09c341ee	default VPC

Below the table, a section titled 'Select a security group above' shows icons for creating a new security group, viewing existing ones, and deleting them.

Under "Create Security Group" wizard

Give Following values

Security group name → NFSsecurity2

Description → NFSrule2

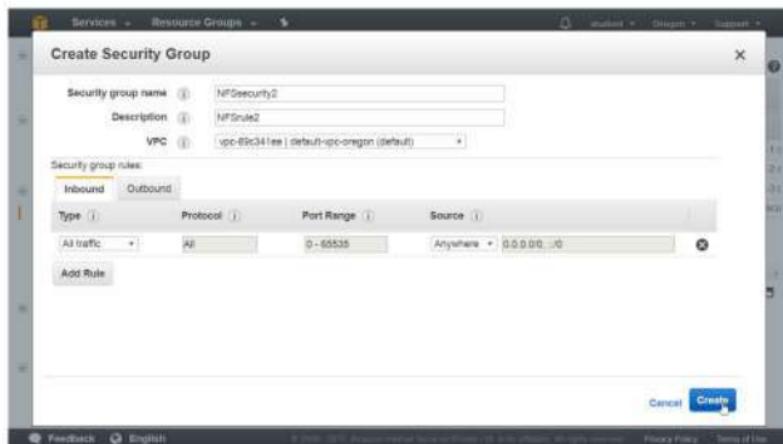
VPC → take default

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 selected. The page lists numerous AWS services categorized into groups:

- Compute:** EC2, EC2 Container Service, Lambda, Elastic Beanstalk, 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, FSx, Glacier, Storage Gateway.
- Management Tools:** CloudWatch, CloudFormation, CloudTrail, Config, OpenShift, Service Catalog, Trusted Advisor, Managed Services.
- Artificial Intelligence:** Lex, Polly, Rekognition, Machine Learning.
- Messaging:** Simple Queue Service, Simple Notification Service, SES.
- Business Productivity:** WorkDocs, WorkMail, Amazon Chime.

Click on "Create file system" button

The screenshot shows the 'Amazon Elastic File System (EFS)' landing page. The page has a clean, modern design with a central circular icon containing a stylized red and orange block. Below the icon, the title 'Amazon Elastic File System (EFS)' is displayed in a large, bold, black font. A short description follows: 'Amazon EFS provides file storage for use with your EC2 instances.' At the bottom of the main content area is a large blue button with white text that reads 'Create file system'. Below this button is a smaller link labeled 'Getting started guide'. The page also includes three smaller icons at the bottom: one showing a stack of files, another showing a cloud with a dollar sign, and a third showing a person's head profile with a gear icon.

Select Default VPC

The screenshot shows the 'Create file system' wizard. Step 1: Configure file system access is selected. A dropdown menu shows 'VPC: vpc-89c34f1ee - default'. Below it, 'Create mount targets' is listed. A note says: '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.' A table lists three mount targets:

Availability Zone	Subnet	IP address	Security groups
us-west-2a	subnet-12b0e5a (default)	Automatic IP	tg-3241edb - default
us-west-2b	subnet-039e38ec (default)	Automatic IP	tg-3241edb - default
us-west-2c	subnet-19d0f141 (default)	Automatic IP	tg-3241edb - default

Remove all Security Groups

The screenshot shows the 'Create mount targets' section. It lists three mount targets in the us-west-2 region, each associated with a different subnet and security group. The security groups are all named 'tg-3241edb - default'.

Availability Zone	Subnet	IP address	Security groups
us-west-2a	subnet-12b0e5a (default)	Automatic IP	tg-3241edb - default
us-west-2b	subnet-039e38ec (default)	Automatic IP	tg-3241edb - default
us-west-2c	subnet-19d0f141 (default)	Automatic IP	tg-3241edb - default

Verify that all security groups go deleted

VPC vpc-85c341es - default... i

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 i
<input checked="" type="checkbox"/> us-west-2a	subnet-13f50e5a (default)	Automatic i	Select Security
<input checked="" type="checkbox"/> us-west-2b	subnet-809e38ec (default)	Automatic i	Select Security
<input checked="" type="checkbox"/> us-west-2c	subnet-19d0f141 (default)	Automatic i	Select Security

i Next Step

Feedback English © 2016 - 2017, Amazon Internet Services Private Ltd. All rights reserved. Privacy Policy Terms of Use

Now add NFSsecurity2 group in all A.Z

VPC vpc-85c341es - default... i

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 i
<input checked="" type="checkbox"/> us-west-2a	subnet-13f50e5a (default)	Automatic i	NFSsecurity2
<input checked="" type="checkbox"/> us-west-2b	subnet-809e38ec (default)	Automatic i	NFSsecurity2
<input checked="" type="checkbox"/> us-west-2c	subnet-19d0f141 (default)	Automatic i	NFSsecurity2

i Cancel

Feedback English © 2016 - 2017, Amazon Internet Services Private Ltd. 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-1380e5a (default)	Automatic	sg-23652152 NFSsecurity2
us-west-2b	subnet-38de38ec (default)	Automatic	sg-23652152 NFSsecurity2
us-west-2c	subnet-19d0f141 (default)	Automatic	sg-23652152 NFSsecurity2

[Cancel](#)

[Next Step](#)

Provide tags

Key → Name

Value → NFShyd1

Drag Down

The screenshot shows the AWS Step Functions Create State Machine wizard at Step 2: Review and create. In the 'Add tags' section, there is one tag named 'Name' with the value 'NFShyd1'. In the 'Choose performance mode' section, 'General Purpose (default)' is selected. The browser address bar shows the URL for creating a state machine.

Step 2: 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=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-89c541ee - default-vpc-oregon (default)	us-west-2a	subnet-129c0fca (default)	Automatic	sg-23652152 - NFSsecurity2
vpc-89c541ee - default-vpc-oregon (default)	us-west-2b	subnet-5bd9e38ec (default)	Automatic	sg-23652152 - NFSsecurity2
vpc-89c541ee - default-vpc-oregon (default)	us-west-2c	subnet-19c0f141 (default)	Automatic	sg-23652152 - NFSsecurity2

Optional settings

Tags: Name:NFShyd1

Performance mode: General Purpose (default)

Encrypted: No

Cancel Previous Create File System

Verify

The screenshot shows the AWS Lambda console under the 'File systems' section. A success message states: "You have created a file system. You can mount your file system from an EC2 instance with an NFSv4.1 client installed. You can also mount your file system from an on-premises server over an AWS Direct Connect connection. Click here for EC2 mount instructions, and here for on-premises mount instructions." Below this, a table lists the newly created file system: Name: NFSdryd1, File system ID: fs-53f822fa, Mounted size: 6.0 KB, Number of mount targets: 3, Creation date: 2017-08-15T06:16:05Z. Under 'Other details', Owner ID is listed as 523291683217 and Life cycle state is Available.

Drag Down

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

The screenshot shows the AWS Lambda console under the 'Mount targets' section. It displays three entries for VPCs: us-west-2a, us-west-2a, and us-west-2b. Each entry shows an availability zone, subnet, IP address, mount target ID, network interface ID, security group, and life cycle state. All three entries show a life cycle state of 'Creating'. The table has columns: VPC, Availability Zone, Subnet, IP address, Mount target ID, Network interface ID, Security groups, and Life cycle state.

VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Life cycle state
vpc-8c341ee - default-vpc-oregon (default)	us-west-2a	subnet-19a0141 (default)	172.31.7.82	fmr-8ea0072f	eni-7adcc27a		Creating
vpc-8c341ee - default-vpc-oregon (default)	us-west-2a	subnet-1360a5a (default)	172.31.40.86	fmr-87a0072a	eni-e80b8406		Creating
vpc-8c341ee - default-vpc-oregon (default)	us-west-2b	subnet-80e18ec (default)	172.31.27.220	fmr-99a0073f	eni-ee053c1		Creating

Verify that Life cycle state is Available

The screenshot shows the AWS EBS File System Manager interface. At the top, there's a navigation bar with tabs like 'File Systems', 'Mount Targets', and 'Attachments'. Below the navigation is a search bar and a 'Getting Started with Amazon FSx' button. The main content area has a heading 'Amazon FSx for Lustre' and a sub-section 'Amazon EC2 mount instructions'. A table titled 'Mount targets' is displayed, showing the following data:

VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Life cycle state
vpc-89c341ea - default-vpc-oregon (default)	us-west-2c	subnet-19e0f141 (default)	172.31.7.82	fsm-8fa0072f	eni-7aefc27a	sg-28602152	Available
	us-west-2a	subnet-1360e9a (default)	172.31.40.88	fsm-87a0072a	eni-8bd88406	sg-28602152	Available
	us-west-2b	subnet-80e3ec (default)	172.31.27.220	fsm-98a00731	eni-ecc533c1	sg-28602152	Available

At the bottom of the page, there are links for 'Feedback', 'English', and legal notices: '© 2006–2017, Amazon Internet Services Private LLC or its affiliates. All rights reserved.', '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/n/mkeys
[shaikh_pc_nas] > ssh -i "studentorg.pem" ec2-user@ec2-54-213-7-42.us-west-2.compute.amazonaws.com
```

Run the following commands

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

Verify is it mounted

Check the last line

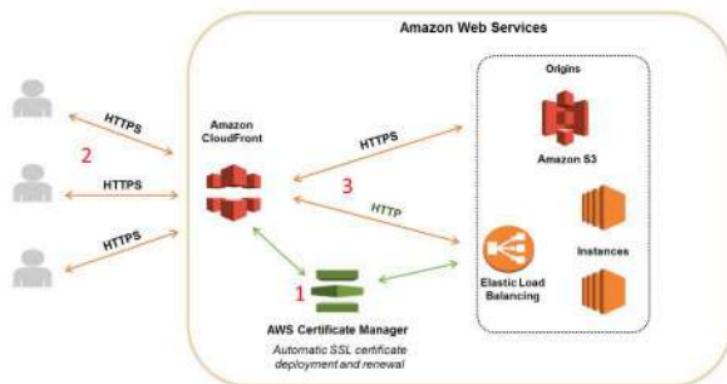
```
proc on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
devtmpfs on /dev type devtmpfs (rw,relatime,size=499756k,nr_inodes=124939,mode=755)
devpts on /dev/pts type devpts (rw,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /dev/shm type tmpfs (rw,relatime)
/dev/xvda1 on / type ext4 (rw,noatime,data=ordered)
devpts on /dev/pts type devpts (rw,relatime,gid=5,mode=620,ptmxmode=000)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
fs-53f822fa.efs.us-west-2.amazonaws.com:/ /opt/oracledata type nfs4 (rw,relatime,vers=4.0,rsize=1048576,wsize=1048576,namlen=255,hard,proto=tcp,timeo=600,retrans=2,secdelay,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

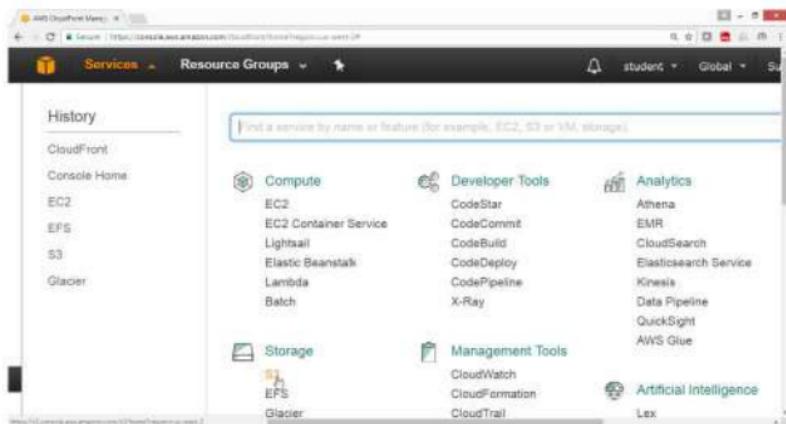
Create a CloudFront Web Distribution

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



Check the S3 bucket content

The screenshot shows the AWS Management Console interface for the S3 service. The top navigation bar includes 'Services' (selected), 'Resource Groups', and 'Actions'. Below the navigation is a search bar labeled 'Search by prefix' and a link 'Switch to new console'. On the right, there are buttons for 'None', 'Properties', and 'Transfers'. The main area displays a table of objects in the 'Bucket: www.cloudskillhyd.com'.

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, detailed information about the bucket is provided:

- Bucket:** www.cloudskillhyd.com
- Region:** Oregon
- Creation Date:** Tue Aug 15 08:44:43 GMT+530 2017
- Owner:** srimuvi989

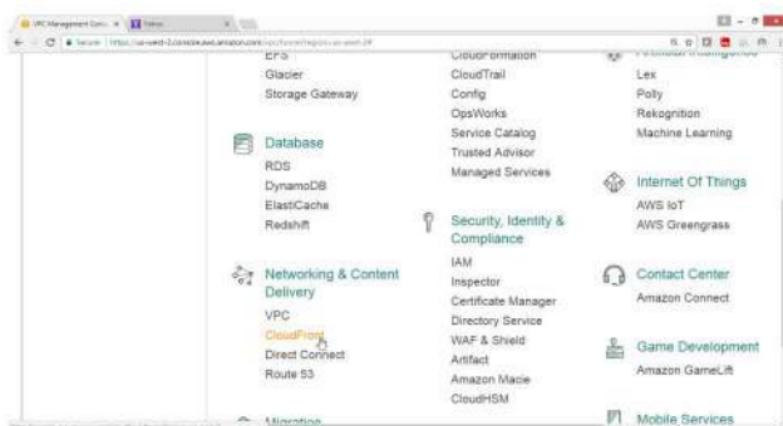
Below this, under 'Permissions', there is a section for 'Static Website Hosting' with the note: 'You can host your static website entirely on Amazon S3. Once you set your bucket for static website hosting, all your content is accessible to web browsers via the Amazon S3 website endpoint for your bucket.' The 'Endpoint' is listed as 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 Distributions page. On the left sidebar, under 'Distributions', there is a 'Create Distribution' button. The main area displays a table with one row, showing a distribution with the ID 'CMB2ACTOR0000000000000000', a domain name 'www.cloudfront.net', and an origin 'www.cloudflare.com'. The table has columns for 'Delivery Method', 'ID', 'Domain Name', 'Comment', and 'Origin'.

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. It highlights the 'Web' option. Below it, there is a note about creating a web distribution if you want to speed up distribution of static and dynamic content. A 'Get Started' button is visible at the bottom of this section.

Web

Create a web distribution if you want to:

- Speed up distribution of static and dynamic content, for example, HTML, CSS, JS, and graphics files.
- Distribute media files using HTTP or HTTPS.
- Cache, compress, and transform data from web forms.
- Use live streaming to stream an event in real time.

You also have the option to create a distribution for an origin - either an Amazon S3 bucket or a web server. After you create the distribution, you can add more origins to the distribution.

Get Started

RTMP

Create an RTMP distribution to speed up distribution of your streaming media files using Adobe Flash Media Server's RTMP protocol. An RTMP distribution allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location. Note the following:

- To create an RTMP distribution, you must store the media files in an Amazon S3 bucket.
- To use CloudFront live streaming, create a web distribution.

Get Started

Under Create Distribution

For Origin Domain Name → Drop down → www.cloudskill.com.s3.amazonaws.com

The screenshot shows the 'Create Distribution' wizard on the 'Step 2: Create distribution' page. In the 'Origin Settings' section, the 'Origin Domain Name' dropdown is expanded, displaying several options including 'www.cloudskill.com.s3.amazonaws.com'. This indicates that the user has selected the correct origin domain name.

Verify Origin Domain Name got selected

The screenshot shows the 'Create Distribution' wizard on the 'Step 2: Create distribution' page. In the 'Origin Settings' section, the 'Origin Domain Name' field is populated with 'www.cloudskill.com.s3.amazonaws.com'. This confirms that the previously selected origin domain name has been successfully applied.

Drag Down

Go for **Distribution Settings**

For Price Class

Select Edge location

The screenshot shows the AWS CloudFront Distribution Settings page. At the top, there are two tabs: 'Step 1: Select delivery method' and 'Step 2: Create distribution'. The second tab is selected. Below the tabs, the page title is 'Distribution Settings'. There are three main configuration sections:

- Price Class:** A dropdown menu set to 'Use All Edge Locations (Best Performance)'.
- AWS WAF Web ACL:** A dropdown menu set to 'None'.
- Alternate Domain Names (CNAMEs):** An input field containing 'cloudfront.net'.

Below these sections is a 'SSL Certificate' section. It contains a radio button for 'Default CloudFront Certificate (*.cloudfront.net)' (selected) and another for 'Custom SSL Certificate (example.com)'. A note explains that the custom certificate option allows users to access content via HTTPS or HTTP, with examples like `https://ET11111111111111.cloudfront.net/logo.jpg`. It also notes that CloudFront requires that browsers on devices support TLS 1.2 or later to access your content.

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

Price Class → Use only Canada and Europe

The screenshot shows the 'Distribution Settings' page for a CloudFront 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 (*.cloudfront.net)). A note about SSL certificates is present, mentioning the option to use an alternate domain name or a custom SSL certificate from ACM.

Drag Down

Click on Create Distribution

The screenshot shows the 'Step 2: Create distribution' configuration page. It includes fields for 'Default Root Object', 'Logging' (Off), 'Bucket for Logs', 'Log Prefix', 'Cookie Logging' (Off), 'Enable IPv6' (On), 'Comments' (empty), and 'Distribution State' (Enabled). At the bottom are 'Cancel', 'Back', and 'Create Distribution' buttons.

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 References, Usage, Viewers, Private Content, How-to Guide, and Origin Access Identity. The main area is titled "CloudFront Distributions" and has tabs for Create Distribution, Distribution Settings, Delete, Enable, and Disable. It shows two distributions:

Delivery Method	ID	Domain Name	Comment	Origin
Web	E3M8ZACTGBBNK	d2vegpb2u0z2.cloudfront.net		www.clarenejeet.com.s3.amazonaws.com
Web	E3T2G9HJL11V7Q	d2mufvqjwvry.cloudfront.net		www.cloudskillsby.com.s3.amazonaws.com

Check column Status

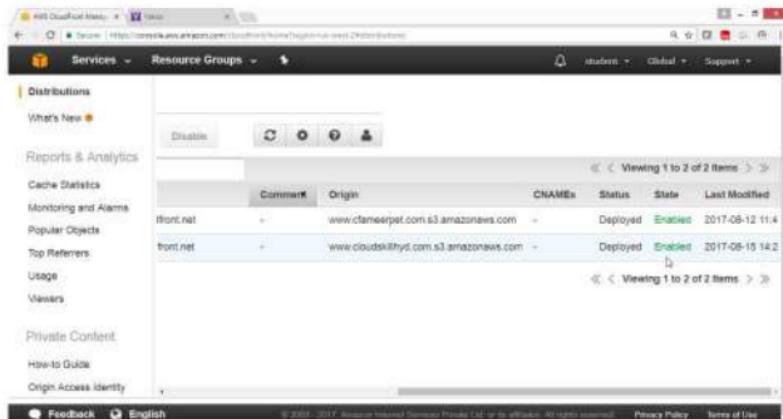
Shows → In Progress

The screenshot shows the AWS CloudFront Origins page. The sidebar is identical to the previous one. The main area is titled "CloudFront Origins" and has tabs for Delete, Enable, and Disable. It shows two origins:

Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
d2wsfkl20rnx2.cloudfront.net		www.clarenejeet.com.s3.amazonaws.com		Deployed	Enabled	2017-08-12 11:4
d2hvbs1gptvq.cloudfront.net		www.cloudskillsby.com.s3.amazonaws.com		In Progress	Enabled	2017-08-15 14:2

Wait for status to gen **Enable**

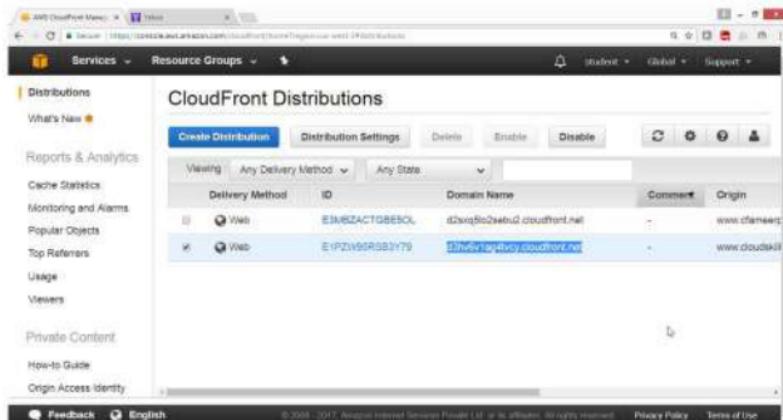
Note : It takes around 15 minutes



The screenshot shows the AWS CloudFront Metrics interface. On the left, there's a sidebar with links like '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 'Services' (selected), 'Resource Groups', and 'CloudFront'. Below these are buttons for 'Disable', 'Edit', 'Delete', and 'Create'. A table lists two distributions:

Comment	Origin	CNAMEs	Status	State	Last Modified
front.net	www.cloudflare.com s3.amazonaws.com	-	Deployed	Enabled	2017-08-12 11:42
front.net	www.cloudskilhyd.com s3.amazonaws.com	-	Deployed	Enabled	2017-08-15 14:22

Verify the Site with DNS name "d3hv6v1ag4tvcy.cloudfront.net"



The screenshot shows the AWS CloudFront Distributions interface. The left sidebar is identical to the previous screenshot. The main area has tabs for 'Services' (selected), 'Resource Groups', and 'CloudFront'. Below these are buttons for 'Create Distribution', 'Distribution Settings', 'Delete', 'Enable', and 'Disable'. A table lists two distributions:

Delivery Method	ID	Domain Name	Comment	Origin
Web	E3NBZACTQBS0L	d3hv6v1ag4tvcy.cloudfront.net	-	www.cloudflare.com
Web	E1PZV95RSB3Y79	d3hv6v1ag4tvcy.cloudfront.net	-	www.cloudskilhyd.com

Verify

Now Open the Browser and type

<http://d3hv6v1ag4tvcy.cloudfront.net/index.html>

The screenshot shows the AWS CloudFront console with the distribution configuration for the domain name `d3hv6v1ag4tvcy.cloudfront.net`. The distribution ID is `E1PZWH99SB3Y79`. Key settings include:

- ARN:** `arn:aws:cloudfront:us-east-1:522511603217:distribution/E1PZWH99SB3Y79`
- Log Prefix:** -
- Delivery Method:** Web
- Cookie Logging:** Off
- Distribution Status:** InProgress
- Comment:** -
- Price Class:** Use Only US, Canada and Europe
- AWS WAF Web ACL:** -
- Alternate Domain Names (CNAMEs):** -
- SSL Certificate:** Default CloudFront Certificate (`*.cloudfront.net`)
- Domain Name:** `d3hv6v1ag4tvcy.cloudfront.net`
- Custom SSL Client Support:** Enabled
- Supported HTTP Versions:** HTTP/2, HTTP/1.1, HTTP/1.0
- HTTP:** Enabled
- Default Root Object:** -
- Last Modified:** 2017-08-15 14:29 UTC+5:30
- Log Bucket:** -

This Website is coming from CloudFront Service

The screenshot shows the `Car Club` website, which is served via CloudFront. The homepage features a purple sports car and navigation links for **HOME**, **ABOUT**, **ARTICLES**, **CONTACTS**, and **SITE MAP**. The **Latest News** section includes two items:

- 10.09.2018** [New car models added to our site](#)
- 10.09.2018** [New car models added to our site](#)

The **Welcome to Our Club** section includes a welcome message and a note about the website's compatibility:

Car Club Site is a free web template created by [TemplateMonster.com](#) team. This website template is optimized for 1024x768 screen resolution.

Access and account of users:
Only administrators have access to administrative functions.

Content areas and pages:
Dashboard, news, portfolio, contact, about us, and a few other pages.

Our website template can be delivered in two packages: with PSD source files included.

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

Practical 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: CCNA / MCSE / LINUX)

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 7.30 or Evening: 7.30

CCNP R&S

CISCO CERTIFIED NETWORK PROFESSIONAL

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 • Afternoon: 2.00 • Evening: 7.00

• Labs on latest routers with IOS version 15.X

Monitoring, Diagnostics & Troubleshooting Tools

• PRTG • Wireshark • SolarWinds, etc.

Exam Practice Challenge Labs

CCIE R&S

CISCO CERTIFIED INTERNETWORK EXPERT

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 • Evening: 6.00

• Individual Rack For Every Student

• Real time scenarios by 20+ years experienced CCIE certified industry expert who has worked on critical projects worldwide.

Written + Lab Exam Focus

FREE Full Scale 8 Hours Exam Lab Included

Unlimited Lab Access For 1 Year

**Complete Package
for Only**

Fees: ₹ 5,900/-

+ 18% GST

**Duration: 3 Months
4 Hrs Per Day**

**100%
GUARANTEED
JOB
ASSISTANCE**

**Fees: ₹ 9,500/-
+ 18% GST**

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 eSECURITY 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.