



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML  
Academic Year: 2022-23**

<b>NAME</b>	<b>PRATHAMESH CHIKANKAR</b>
<b>BRANCH</b>	<b>CSE-(AI&amp;ML)</b>
<b>ROLL NO.</b>	<b>11</b>
<b>SUBJECT</b>	<b>CLOUD COMPUTING LAB</b>
<b>COURSE CODE</b>	<b>CSL605</b>
<b>PRACTICAL NO.</b>	<b>01</b>
<b>DOP</b>	<b>02/02/2023</b>
<b>DOS</b>	



## AWS (EC2) Installation steps for Linux instance

Please find the AWS account creation steps in the link.

- <https://aws.amazon.com/premiumsupport/knowledge-center/create-and-activate-aws-account/>
- [https://signin.aws.amazon.com/signin?redirect\\_uri=https%3A%2F%2Fconsole.aws.amazon.com%2Fsupport%2Fhome%2F%3Fnc2%3Dh\\_qI\\_cu%26state%3DhashArgs%2523%26isauthcode%3Dtrue&client\\_id=arn%3Aaws%3Aiam%3A015428540659%3Auser%2Fsupportcenter&forceMobileApp=0](https://signin.aws.amazon.com/signin?redirect_uri=https%3A%2F%2Fconsole.aws.amazon.com%2Fsupport%2Fhome%2F%3Fnc2%3Dh_qI_cu%26state%3DhashArgs%2523%26isauthcode%3Dtrue&client_id=arn%3Aaws%3Aiam%3A015428540659%3Auser%2Fsupportcenter&forceMobileApp=0)

Requirement – Amazon web service account

The screenshot shows two side-by-side browser windows. On the left, the AWS sign-in page is displayed, allowing the user to choose between 'Root user' or 'IAM user'. It also shows the 'Root user email address' as 'prathameshchikankar\_aiml\_2020@ltce.in' and a 'Next' button. Below the sign-in form, there is a note about agreeing to the AWS Customer Agreement and Privacy Notice. At the bottom, there are links for 'New to AWS?' and 'Create a new AWS account'. On the right, the AWS Management Console home page is shown, with the URL 'ap-northeast-1.console.aws.amazon.com/console/home?nc2=h\_ct&src=header-signin&region=ap-northeast-1'. The console interface includes a sidebar with 'Recently visited' and 'Favorites' sections, and a main area titled 'Console Home' with a highlighted 'EC2' service card.

### Step 0 : Login

### Step 1 : Open AWS services and select EC2

The screenshot shows the AWS EC2 Manager home page for the 'ap-northeast-1' region. The left sidebar contains navigation links for EC2 Dashboard, Instances, Images, Elastic Block Store, Network & Security, and more. The main content area is divided into several sections: 'Resources' (listing Instances (running), Dedicated Hosts, Elastic IPs, Key pairs, Placement groups, Security groups, and Volumes), 'Launch instance' (with 'Launch Instance' and 'Migrate a server' buttons), 'Scheduled events' (showing 'No scheduled events' for the Asia Pacific (Tokyo) region), 'Service health' (showing 'This service is operating normally'), 'Zones' (listing Zone names and Zone IDs for ap-northeast-1a, ap-northeast-1c, and ap-northeast-1d), and 'Explore AWS' (sections for Get Up to 40% Better Price Performance, Enable Best Price-Performance with AWS Graviton2, Amazon GuardDuty Malware Protection, and Additional information). The bottom of the page shows the URL 'https://ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#insta...' and a footer with copyright information.



## Step 2 : CLICK ON instance (running) in above screen

The screenshot shows the AWS EC2 Instances page. The left sidebar includes sections for EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs), and Feedback. The main content area has a search bar and a table with the following columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4, and Elastic IP. A message at the top of the table says "No matching instances found". Below the table, a modal window titled "Select an instance" is open.

## Step 3 : On above screen click on launch Instances

The screenshot shows the AWS Launch an instance page. The left sidebar shows the navigation path: EC2 > Instances > Launch an instance. The main content area includes sections for Name and tags, Application and OS Images (Amazon Machine Image), and a summary. The summary section contains fields for Number of instances (set to 1), Software Image (AMI) (Amazon Linux 2 Kernel 5.10 AMI), Virtual server type (instance type) (t2.micro), Firewall (security group) (New security group), and Storage (volumes) (1 volume(s) - 8 GiB). A callout box provides information about the Free tier. At the bottom right is a "Launch instance" button.



- Step 4 :** Select **Ubuntu server 22.04** and Select **free tier eligible** and click on button – **Next:configure instance details**
- Step 5 :** Don't change any setting directly click on button – **Next: Add storage**
- Step 6 :** Check Volume type: **General purpose SSD (gp 2)** and then click on button – **next: Add Tags**
- Step 7 :** Need to add key so click on **Add Tag**, In key tab give **any name**, value – **database**
- Step 8 :** Click on **Create a new key pair**, Insert key pair name anything like – test

EC2 > Instances > Launch an instance

### Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

**Name and tags Info**

Key <small>Info</small>	Value <small>Info</small>	Resource types <small>Info</small>
<input type="text" value="prathamesh"/> X	<input type="text" value="database"/> X	<input type="button" value="Select resource type..."/>
<input type="button" value="Instances"/> X		
<input type="button" value="Volumes"/> X		

**Add tag**

49 remaining (Up to 50 tags maximum)

**Instance type Info**

Instance type	Free tier eligible
<input type="text" value="t2.micro"/>	<input type="button" value="Compare instance types"/>
Family: t2 1 vCPU 1 GiB Memory On-Demand Windows pricing: 0.0198 USD per Hour On-Demand SUSE pricing: 0.0152 USD per Hour On-Demand RHEL pricing: 0.0752 USD per Hour On-Demand Linux pricing: 0.0152 USD per Hour	

**Key pair (login) Info**

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - **required**

**Network settings Info**

Network Info  
vpc-077ade6090977a400

Subnet Info  
No preference (Default subnet in any availability zone)

Auto-assign public IP Info  
Enable

**Firewall (security groups) Info**  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group     Select existing security group

We'll create a new security group called **'launch-wizard-1'** with the following rules:

- Allow SSH traffic from Helps you connect to your instance  
 0.0.0.0/0
- Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server
- Allow HTTP traffic from the Internet To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

**Application and OS Images (Amazon Machine Image) Info**

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

**Quick Start**

<input type="button" value="Amazon Linux"/>	<input type="button" value="macOS"/>	<input type="button" value="Ubuntu"/>	<input type="button" value="Windows"/>	<input type="button" value="Red Hat"/>

**Amazon Machine Image (AMI)**

<input type="button" value="Ubuntu Server 22.04 LTS (HVM, SSD Volume Type)&lt;br/&gt;ami-0cd7ad8676931d727 (64-bit (x86)) / ami-0a09e744e6643e376 (64-bit (Arm))&lt;br/&gt;Virtualization: hvm ENA enabled: true Root device type: ebs"/>	Free tier eligible
---	--------------------

**Description**  
Canonical, Ubuntu, 22.04 LTS, amd64 Jammy Image build on 2023-01-15

**Architecture** 64-bit (x86)    **AMI ID** ami-0cd7ad8676931d727    **Verified provider**

**Create key pair**

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

**Key pair name**

  
⚠ Key pair already exists.  

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

**Key pair type**

RSA RSA encrypted private and public key pair

ED25519 ED25519 encrypted private and public key pair (Not supported for Windows instances)

**Private key file format**

.pem For use with OpenSSH

.ppk For use with PuTTY

**Create key pair**

**Configure storage Info**

Tx:  GiB:  Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

**Add new volume**

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

O File systems

**Advanced details Info**

AIML11\_PRATHAMESH



## Step 9 : Click on Launch Instances

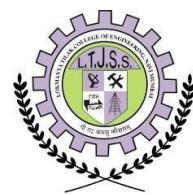
The screenshot shows the AWS EC2 Launch Instance wizard. On the left, a sidebar lists navigation options like Summary, Software Image (AMI), Virtual server type (instance type), Firewall (security group), Storage (volumes), and a detailed Free tier summary. The main area displays a success message: "Successfully initiated launch of instance (i-0c8581dba021071c6)". Below this, a "Next Steps" section offers options to Create billing and free tier usage alerts, Connect to your instance, and Connect an RDS database. At the bottom, there are "Cancel" and "Launch instance" buttons.

## Step 10 : You get the mgs in green color – click on View Instances

Step 11 : Click on refresh button because we need Status check tab – 2/2 check pass

Step 12 : Select check box which is present at before name DATABASE and click on connect Button

The screenshot shows the AWS EC2 Instances page. It displays a single instance named "prathamesh" with the ID "i-0c8581dba021071c6". The instance is listed as "Running" with a status check of "2/2 checks passed". The page includes tabs for Details, Security, Networking, Storage, Status checks, Monitoring, and Tags. The "Status checks" tab is currently selected. At the bottom, there are "Launch instances" and "View all instances" buttons.



## Step 13 : Here you can change the user name if you want – like db\_sg1, Step- click on Connect

EC2 > Instances > i-0c8581dba021071c6 > Connect to instance

### Connect to instance info

Connect to your instance i-0c8581dba021071c6 (prathamesh) using any of these options

EC2 Instance Connect Session Manager SSH client EC2 serial console

Instance ID [i-0c8581dba021071c6](#) (prathamesh)

Public IP address [13.115.66.152](#)

User name  Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ubuntu.

**Note:** In most cases, the default user name, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel **Connect**

## Step 14 : Next step perform some **command** on your Ubuntu server-

\$ sudo -i (root login)

# apt update (update your system)

```
11_CCL_EXP1 - Google Doc | Instances | EC2 Management | Connect to instance | EC2 Instance Connect | New Tab | +  
← → C ap-northeast-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-northeast-1&connType=standard&instanceId=i-0c8581dba021071c6&osUser=ubuntu&sshPort=22#/  
aws Services Search [Alt+S] Tokyo prathameshpc77  
  
System information as of Thu Feb 2 05:03:26 UTC 2023  
  
System load: 0.080078125 Processes: 97  
Usage of /: 19.9% of 7.57GB Users logged in: 1  
Memory usage: 21% IPv4 address for eth0: 172.31.7.160  
Swap usage: 0%  
  
0 updates can be applied immediately.  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Thu Feb 2 04:58:01 2023 from 3.112.23.5  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-172-31-7-160:~$ sudo -i  
root@ip-172-31-7-160:# sudo apt update  
Hit:1 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease  
Get:2 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]  
Get:3 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [104 kB]  
Get:4 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]  
Get:5 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]  
Get:6 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]  
Get:7 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]  
Get:8 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]  
Get:9 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]  
Get:10 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [852 kB]  
  
i-0c8581dba021071c6 (prathamesh)  
PublicIPs: 13.115.66.152 PrivateIPs: 172.31.7.160  
  
Feedback Looking for language selection? Find it in the new Unified Settings © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences
```



# top (table of processes, which are the running processes in our system and also check usage management)

Press Ctrl+c or press q for the end top command.

```
11_CCL_EXP1 - Google Doc | Instances | EC2 Management | Connect to instance | EC2 | EC2 Instance Connect
ubuntu@ip-172-31-7-160:~$ sudo -i
root@ip-172-31-7-160:~# sudo apt update
Hit http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 https://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Get:3 https://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [104 kB]
Get:4 https://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-security InRelease [104 kB]
Get:5 https://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [562 kB]
Get:6 https://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c=src-f Metadata [286 kB]
Get:7 https://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:8 https://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:9 https://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c=n-f Metadata [8372 B]
Get:10 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [852 kB]
Get:11 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c=n-f Metadata [188 kB]
Get:12 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c=n-f Translation-en [13.2 kB]
Get:13 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [566 kB]
Get:14 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [87.1 kB]
Get:15 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c=n-f Metadata [556 B]
Get:16 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [79 kB]
Get:17 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [42 kB]
Get:18 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c=n-f Metadata [15.0 kB]
Get:19 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [7988 B]
Get:20 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [2448 B]
Get:21 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c=n-f Metadata [432 B]
Get:22 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [40.7 kB]
Get:23 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [9800 B]
Get:24 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c=n-f Metadata [392 B]
Get:25 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c=n-f Metadata [116 B]
Get:26 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [19.5 kB]
Get:27 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [13.8 kB]
Get:28 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [110 kB]
Get:29 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-security Translation-en [116 B]
Get:30 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c=src-f Metadata [392 B]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [127 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c=n-f Metadata [8064 B]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [528 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [81.2 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c=n-f Metadata [556 B]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [637 kB]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [67.3 kB]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c=n-f Metadata [11.3 kB]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [4268 B]
Get:41 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [972 B]
Get:42 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c=n-f Metadata [228 B]
Fetched 25.5 MB in 4s (6244 kB/s)
Reading package lists... Done
Building dependency tree... Done
```

i-0c8581dba021071c6 (prathamesh )

PublicIPs: 13.115.66.152 PrivateIPs: 172.31.7.160

```
11_CCL_EXP1 - Google Doc | Instances | EC2 Management | Connect to instance | EC2 | EC2 Instance Connect
ubuntu@ip-172-31-7-160:~# top
top - 05:09:50 up 21 min, 2 users, load average: 0.00, 0.02, 0.01
Tasks: 98 total, 1 running, 97 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
Mem: 966.2 total, 157.2 free, 212.8 used, 596.2 buff/cache
Swap: 0.0 total, 0.0 free, 0.0 used, 610.0 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1 root 20 0 101920 12756 S 0.0 1.3 0:05.36 systemd
2 root 20 0 0 0 S 0.0 0.0 0.0 0:00.00 kthreadd
3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
5 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 slub flushhwq
6 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu_wq
8 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker/0:0H-events_highpri
10 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_tasks_rude_
11 root 20 0 0 0 S 0.0 0.0 0:00.00 rcu_tasks_trace
12 root 20 0 0 0 S 0.0 0.0 0:00.00 ksoftirqd/0
13 root 20 0 0 0 S 0.0 0.0 0:00.00 ksoftirqd/1
14 root 20 0 0 0 I 0.0 0.0 0:00.41 migration/0
15 root rt 0 0 0 S 0.0 0.0 0:00.00 migration/0
16 root -51 0 0 0 S 0.0 0.0 0:00.00 idle_inject/0
17 root 20 0 0 0 I 0.0 0.0 0:00.11 kworker/0:1-cgroup_destroy
18 root 20 0 0 0 S 0.0 0.0 0:00.00 cpuhp/0
19 root 20 0 0 0 S 0.0 0.0 0:00.00 kdevtmpfs
20 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 inet_frag_wq
21 root 20 0 0 0 S 0.0 0.0 0:00.00 kauditd
22 root 20 0 0 0 S 0.0 0.0 0:00.00 khungtaskd
23 root 20 0 0 0 S 0.0 0.0 0:00.00 com_reaper
24 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 writeback
top - 05:09:53 up 21 min, 2 users, load average: 0.00, 0.02, 0.01
Tasks: 98 total, 1 running, 97 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
Mem: 966.2 total, 157.2 free, 212.8 used, 596.2 buff/cache
Swap: 0.0 total, 0.0 free, 0.0 used, 610.0 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
27 root 39 19 0 0 0 S 0.0 0.0 0:00.00 khugepaged
73 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kintegrityd
74 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kblockd
75 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 blkcg_punt_bio
76 root 20 0 0 0 S 0.0 0.0 0:00.00 xen-balloon
top - 05:09:56 up 22 min, 2 users, load average: 0.00, 0.02, 0.01
Tasks: 98 total, 1 running, 97 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
79 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 md
80 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 edac-poller
81 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 devfreq_wq
82 root -51 0 0 0 S 0.0 0.0 0:00.00 watchdogd
85 root 0 -20 0 0 0 I 0.0 0.0 0:00.04 kworker/0:1H-kblockd
top - 05:09:59 up 22 min, 2 users, load average: 0.00, 0.02, 0.01
```

i-0c8581dba021071c6 (prathamesh )

PublicIPs: 13.115.66.152 PrivateIPs: 172.31.7.160

Feedback Looking for language selection? Find it in the new Unified Settings

# history

# vmstat (virtual memory static ,how much memory in the buffer,in the cache, what is in the input,output,systems and the cpu)

# df (disk file system)

#df -kh (k-kilobyte h-human readable)

#whatis df (using whatis command take help from system)

```
11_CCL_EXP1 - Google Doc | Instances | EC2 Management | Connect to instance | EC2 | EC2 Instance Connect
ubuntu@ip-172-31-7-160:~# history
1 sudo apt update
2 top
3 history
root@ip-172-31-7-160:~# vmsat
Command 'vmsat' not found, did you mean:
  Command 'vmstat' from 'deb procs (2:3.3.17-6ubuntu2)'
Try: apt install <deb name>
root@ip-172-31-7-160:~# vmstat
procs --memory-- --swap-- --io-- --system-- --cpu--
r b swpd free buff cache si so bi bo in cs us sy id wa st
0 0 0 160984 18416 592376 0 0 177 368 41 91 2 1 97 0 1
root@ip-172-31-7-160:~# history
1 sudo apt update
2 top
3 history
4 vmsat
5 vmstat
6 history
root@ip-172-31-7-160:~# df -kh
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/root 7941576 1753764 6171428 23% /
tmpfs 494692 0 494692 0 /dev/shm
tmpfs 197880 832 197048 1% /run
tmpfs 5120 0 5120 0 /run/lock
/dev/xvda15 106858 5329 101529 5% /boot/efi
tmpfs 98936 4 98932 1% /run/user/1000
root@ip-172-31-7-160:~# df -kh
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/root 7.6G 1.7G 5.9G 23% /
tmpfs 484M 0 484M 0 /dev/shm
tmpfs 194M 832K 193M 1% /run
tmpfs 5.0M 0 5.0M 0 /run/lock
/dev/xvda15 105M 5.3M 100M 5% /boot/efi
tmpfs 97M 4.0K 97M 1% /run/user/1000
root@ip-172-31-7-160:~# whatis df
df - something appropriate
root@ip-172-31-7-160:~# df --help
Usage: df [OPTION]... [FILE]...
Show information about the file system on which each FILE resides,
or all file systems by default.

Mandatory arguments to long options are mandatory for short options too.
-a, --all           include pseudo, duplicate, inaccessible file systems
```

i-0c8581dba021071c6 (prathamesh )

PublicIPs: 13.115.66.152 PrivateIPs: 172.31.7.160

Feedback Looking for language selection? Find it in the new Unified Settings

AIML11\_PRATHAMESH



```
#df --help (help command)
```

```
# ctrl + I (clear the screen)
```

```
#uname -a (information related to ip, kernel version)
```

```
All are Validation steps for checking your EC2 instance working properly or not(check system performance).
```

```
11_CCL_EXP1-Google Do Instances | EC2 Manager Connect to instance | EC2
aws Services Search [Alt+S]
Show information about the file system on which each FILE resides,
or all file systems by default.

Mandatory arguments to long options are mandatory for short options too.
-a, --all           include pseudo, duplicate, inaccessible file systems
-B, --block-size=SIZE scale sizes by SIZE before printing them; e.g.,
                     '-BM' prints sizes in units of 1,048,576 bytes;
                     see SIZE format below
-h, --human-readable print sizes in powers of 1024 (e.g., 1023M)
-H, --si            print sizes in powers of 1000 (e.g., 1.1G)
-i, --inodes        list inode information instead of block usage
-k                 like --block-size=1K
-l, --local         limit listing to local file systems
--no-sync          do not invoke sync before getting usage info (default)
--output[=FIELD_LIST] use the output format defined by FIELD_LIST,
                      or print all fields if FIELD_LIST is omitted.
-P, --portability   use the POSIX output format
--sync             invoke sync before getting usage info
--total            elide all entries insignificant to available space,
                  and produce a grand total
-t, --type=TYPE     limit listing to file systems of type TYPE
-T, --print-type    print file system type
--exclude-type=TYPE limit listing to file systems not of type TYPE
-v                 (ignored)
--help              display this help and exit
--version           output version information and exit

Display values are in units of the first available SIZE from --block-size,
and the DF_BLOCK_SIZE, BLOCK_SIZE and BLOCSIZE environment variables.
Otherwise, units default to 1024 bytes (or 512 if POSIXLY_CORRECT is set).

The SIZE argument is an integer and optional unit (example: 10K is 10*1024).
Units are K,M,G,T,P,E,Z,Y (powers of 1024) or KB,MB,... (powers of 1000).
Binary prefixes can be used, too: KiB=K, MiB=M, and so on.

FIELD_LIST is a comma-separated list of columns to be included. Valid
field names are: 'source', 'fstype', 'itotal', 'iused', 'iavail', 'ipcent',
'size', 'used', 'avail', 'pcent', 'file' and 'target' (see info page).

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Report any translation bugs to <https://translationproject.org/team/>
Full documentation <https://www.gnu.org/software/coreutils/df>
or available locally via: info '(coreutils) df invocation'
root@ip-172-31-7-160:~#
```

i-0c8581dba021071c6 (prathamesh )  
PublicIPs: 13.115.66.152 PrivateIPs: 172.31.7.160

Feedback Looking for language selection? Find it in the new Unified Settings

```
# mkdir test
# ls
# cd test
test# touch file1 (create file)
# ls
# touch file2 file3
# ls
# rm file1 (remove file)
# ls
# rm file* (remove all files)
# ls
# cd ..
# ls
# rmdir test
# ls
# mkdir test1 test2 test3
#ls
# rmdir test*
# ls
```

```
11_CCL_EXP1-Google Do Instances | EC2 Manager Connect to instance | EC2 EC2 Instance Connect
aws Services Search [Alt+S]
df: nothing appropriate.
root@ip-172-31-7-160:~# df --help
Usage: df [OPTION]... [FILE]...
root@ip-172-31-7-160:~# uname -a
Linux ip-172-31-7-160 5.15.0-1028-aws #32-Ubuntu SMP Mon Jan 9 12:28:07 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
root@ip-172-31-7-160:~# mkdir test
root@ip-172-31-7-160:~# ls
snap test
root@ip-172-31-7-160:~# cd test
root@ip-172-31-7-160:~/test# touch file1
root@ip-172-31-7-160:~/test# ls
file1
root@ip-172-31-7-160:~/test# touch file2 file3
root@ip-172-31-7-160:~/test# ls
file1 file2 file3
root@ip-172-31-7-160:~/test# rm file*
root@ip-172-31-7-160:~/test# ls
root@ip-172-31-7-160:~/test# cd ..
root@ip-172-31-7-160:~# ls
snap test
root@ip-172-31-7-160:~# rmdir test
root@ip-172-31-7-160:~# ls
snap
root@ip-172-31-7-160:~# mkdir test1 test2 test3
root@ip-172-31-7-160:~# ls
snap test1 test2 test3
root@ip-172-31-7-160:~# rmdir test*
root@ip-172-31-7-160:~# ls
snap
root@ip-172-31-7-160:~#
```

i-0c8581dba021071c6 (prathamesh )  
PublicIPs: 13.115.66.152 PrivateIPs: 172.31.7.160

Feedback Looking for language selection? Find it in the new Unified Settings



## Step 15 : To terminate the instance -

Select the checkbox which is available at the start of your name of instant , then click on **Instant State** Button on the top and select **Terminal Instance**

The screenshot shows the AWS EC2 Instances page. A single instance named "prathamesh" is listed as "Running". In the "Actions" dropdown menu, the "Terminate instance" option is highlighted. The instance details page is also visible, showing security group information and inbound rules.

## Step 16 : If you want to terminate then this will, and if not the following instance will show as it is !

The screenshot shows the AWS EC2 Instances page again. The same instance "prathamesh" is now listed as "terminated". In the "Actions" dropdown menu, the "Terminate instance" option is highlighted. The instance details page is visible, showing terminated status and other instance metadata.



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML**  
**Academic Year: 2022-23**

<b>NAME</b>	<b>PRATHAMESH CHIKANKAR</b>
<b>BRANCH</b>	<b>CSE-(AI&amp;ML)</b>
<b>ROLL NO.</b>	<b>11</b>
<b>SUBJECT</b>	<b>CLOUD COMPUTING LAB</b>
<b>COURSE CODE</b>	<b>CSL605</b>
<b>PRACTICAL NO.</b>	<b>02</b>
<b>DOP</b>	<b>09/02/2023</b>
<b>DOS</b>	



## Step1 : Login to AWS console and go to **Elastic Beanstalk**

The screenshot shows the AWS Management Console with the search bar at the top containing 'elastic Beanstalk'. The left sidebar is collapsed. The main search results page displays 'Services (12)' and 'Features (26)'. Under 'Services', 'Elastic Beanstalk' is listed under 'Top features' with the subtext 'Run and Manage Web Apps'. Other services like 'Elastic Transcoder', 'Elastic Container Service', and 'Elastic Container Registry' are also listed. Under 'Features', categories include 'Applications', 'Environments', 'Elastic IPs', and 'Volumes', each with a single item listed.

## Step 2 : Click on **Create Application**

The screenshot shows the Amazon Elastic Beanstalk landing page. The header reads 'Amazon Elastic Beanstalk End-to-end web application management.' Below the header, there's a 'Get started' section with a 'Create Application' button. To the right, there's a 'Pricing' section stating 'There's no additional charge for Elastic Beanstalk. You pay for Amazon Web Services resources that we create to store and run your web application, like Amazon S3 buckets and Amazon EC2 instances.' Further down, sections include 'How it works', 'Benefits and features' (with sub-sections 'Easy to get started', 'Complete resource control', 'Fully managed', and 'Automatic application health'), 'Getting Started' (with a 'Launch a web application' link), and 'More resources' (with links to 'Documentation', 'FAQ', and 'Forum'). The bottom of the page shows the footer with copyright information and links.



**Step 3 :** Write Application information : **Name, Tag,Platform** etc.

**Step 4 :** In Application Code: select sample application and then Click on button Create Application

AWS Services Search [Alt+S]

Elastic Beanstalk X

Elastic Beanstalk > Getting started

## Create a web app

Create a new application and environment with a sample application or your own code. By creating an environment, you allow Amazon Elastic Beanstalk to manage Amazon Web Services resources and permissions on your behalf. [Learn more](#)

### Application information

Application name  
prathameshpc777

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

### Application tags

Apply up to 50 tags. You can use tags to group and filter your resources. A tag is a key-value pair. The key must be unique within the resource and is case-sensitive. [Learn more](#)

Key	Value	Remove tag
name	selfWebSite	

Add tag  
49 remaining

### Platform

Platform  
PHP

Platform branch  
PHP 8.1 running on 64bit Amazon Linux 2

Platform version  
3.5.4 (Recommended)

### Application code

Sample application  
Get started right away with sample code.

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

Cancel Configure more options Create application

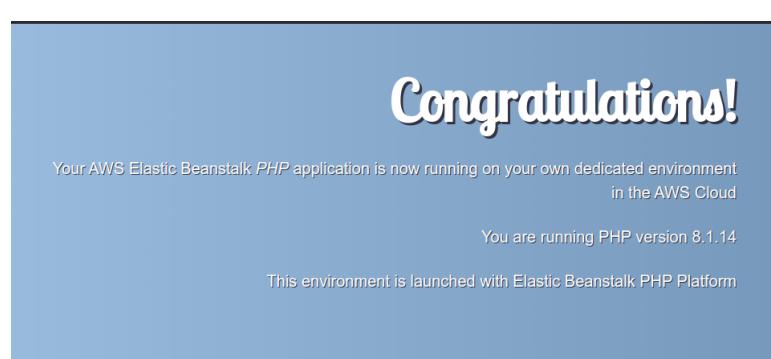


## Step 5 : Click on Environments -> Check the health of Environment wait till it becomes 'OK'

The screenshot shows the AWS Elastic Beanstalk console. On the left, there's a sidebar for 'Elastic Beanstalk' with sections like 'Environments', 'Applications', 'Change history', and a expanded section for 'Prathameshpc777-env' which includes 'Go to environment', 'Configuration', 'Logs', 'Health', 'Monitoring', 'Alarms', 'Managed updates', 'Events', and 'Tags'. The main content area shows the 'Prathameshpc777-env' environment details. It has tabs for 'Health' (which shows 'Ok'), 'Running version' (set to 'Sample Application' with a 'Upload and deploy' button), and 'Platform' (PHP 8.1 running on 64bit Amazon Linux 2/3.5.4 with a 'Change' button). Below these is a 'Recent events' table with several log entries from February 9, 2023, detailing the launch and deployment process.

## Step 6 : Click the URL

The screenshot shows the 'All environments' page in the AWS Elastic Beanstalk console. It lists one environment: 'Prathameshpc777-env' with a green 'Ok' status icon. The table columns include 'Environment name', 'Health', 'Application name', 'Date created', 'Last modified', 'URL', 'Running versions', 'Platform', 'Platform state', and 'Tier name'. The 'Prathameshpc777-env' row shows it was created on 2023-02-09 at 10:13:33 UTC+0530, last modified on 2023-02-09 at 10:16:27 UTC+0530, and is running on PHP 8.1. A large blue banner at the bottom congratulates the user on successful deployment.



### What's Next?

- AWS Elastic Beanstalk overview
- Deploying AWS Elastic Beanstalk Applications in PHP Using Eb and Git
- Using Amazon RDS with PHP
- Customizing the Software on EC2 Instances
- Customizing Environment Resources

### AWS SDK for PHP

- AWS SDK for PHP home
- PHP developer center
- AWS SDK for PHP on GitHub

To **Delete** the application and Environment (Select it and in Action -Delete/Terminate : give conformation)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML  
Academic Year: 2022-23**

<b>NAME</b>	<b>PRATHAMESH CHIKANKAR</b>
<b>BRANCH</b>	<b>CSE-(AI&amp;ML)</b>
<b>ROLL NO.</b>	<b>11</b>
<b>SUBJECT</b>	<b>CLOUD COMPUTING LAB</b>
<b>COURSE CODE</b>	<b>CSL605</b>
<b>PRACTICAL NO.</b>	<b>03</b>
<b>DOP</b>	
<b>DOS</b>	



## Open AWS account and search & select s3

Search results for 'amazon s3'

**Services (142)**

- Features (285)
- Resources New
- Blogs (21,390)
- Documentation (97,804)
- Knowledge Articles (30)
- Tutorials (229)
- Events (839)
- Marketplace (411)

**Services**

- AWS Transfer Family ☆  
Fully managed support for SFTP, FTPS and FTP
- S3 ☆  
Scalable Storage in the Cloud
- S3 Glacier ☆  
Archive Storage in the Cloud
- Top features**
- Create Vault
- AWS Private Certificate Authority ☆  
Managed private certificate authority service

**Features**

- Amazon S3 File Gateway  
Storage Gateway feature
- SQL queries  
Athena feature
- Logging configuration  
Amazon Interactive Video Service feature
- Create Macie sensitive data discovery job  
Amazon Macie feature

## Step-1 : Click on create bucket

s3.console.aws.amazon.com/s3/buckets?region=ap-south-1

**Amazon S3**

**Buckets**

- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

**Storage Lens**

- Dashboards
- AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3

**Amazon S3 > Buckets**

**Account snapshot**  
Storage lens provides visibility into storage usage and activity trends. Learn more

**Buckets (1) Info**  
Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date
elasticbeanstalk-ap-south-1-404055596869	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 9, 2023, 10:13:26 (UTC+05:30)



**Step-2** : Give Bucket name & select region for storage

**Step-3** : Keep object ownership setting as ACLs Disabled as by-default

**Step-4** : Disable block all public access checkbox

Screenshot of the AWS S3 'Create bucket' configuration page.

**General configuration**

Bucket name: prathameshpc77  
Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region: Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - optional  
Only the bucket settings in the following configuration are copied.  
[Choose bucket](#)

**Object Ownership**

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

**ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

**ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership: Bucket owner enforced

**Upcoming permission changes to disable ACLs**  
Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you will no longer need the s3:PutBucketOwnershipControls permission. [Learn more](#)

**Block Public Access settings for this bucket**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

**Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

**Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.

**Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

**Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



**Step-5 : Select the checkbox for Turning off block all public access might result in this bucket and the objects within becoming public**

**Step-6 : Keep bucket versioning as disabled and add tags if required**

**Step-7 : Keep default encryption disabled and click on create bucket button**

You can now see the successful creation of your bucket

**policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**Turning off block all public access might result in this bucket and the objects within becoming public**  
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

**Upcoming permission changes to disable any Block Public Access setting**  
Starting in April 2023, to disable any Block Public Access setting when creating buckets by using the S3 console, you must have the s3:PutBucketPublicAccessBlock permission. [Learn more](#)

**Bucket Versioning**  
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

**Bucket Versioning**  
 Disable  
 Enable

**Tags (0) - optional**  
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.  
[Add tag](#)

**Default encryption** [Info](#)  
Server-side encryption is automatically applied to new objects stored in this bucket.

**Encryption key type** [Info](#)  
 Amazon S3-managed keys (SSE-S3)  
 AWS Key Management Service key (SSE-KMS)

**Bucket Key**  
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)  
 Disable  
 Enable

**Advanced settings**

[Info](#) After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)



## Step-8 : Now click on the bucket that you have created

s3.console.aws.amazon.com/s3/buckets?region=ap-south-1

Guest Update

Amazon S3 Services Search [Alt+S]

Successfully created bucket "prathameshpc77". To upload files and folders, or to configure additional bucket settings choose View details.

Amazon S3 > Buckets

▶ Account snapshot Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (2) Info Buckets are containers for data stored in S3. Learn more

Find buckets by name

Name AWS Region Access Creation date

Name	AWS Region	Access	Creation date
elasticbeanstalk-ap-south-1-404055596869	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 9, 2023, 10:13:26 (UTC+05:30)
prathameshpc77	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 23, 2023, 10:15:48 (UTC+05:30)

View Storage Lens dashboard

C Copy ARN Empty Delete Create bucket

Block Public Access settings for this account

Storage Lens Dashboards AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3

Step-9 : You can either create a folder here or upload an existing file in the bucket

Step-10 : now click on upload button and click on add files button browse your local machine and select which file you need to upload on S3 next click on upload button at bottom right end

s3.console.aws.amazon.com/s3/upload/prathameshpc77?region=ap-south-1

aws Services Search [Alt+S]

Amazon S3 > Buckets > prathameshpc77 > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.

Files and folders (1 Total, 20.0 B) All files and folders in this table will be uploaded.

Name	Folder	Type	Size
text_file.txt	-	text/plain	20.0 B

Remove Add files Add folder

Destination

Destination s3://prathameshpc77

▶ Destination details Bucket settings that impact new objects stored in the specified destination.

▶ Permissions Grant public access and access to other AWS accounts.

▶ Properties Specify storage class, encryption settings, tags, and more.

Cancel Upload



## Now you can check the upload status screen

s3.console.aws.amazon.com/s3/upload/prathameshpc77?region=ap-south-1

aws Services Search [Alt+S]

Upload succeeded

View details below.

### Upload: status

The information below will no longer be available after you navigate away from this page.

#### Summary

Destination	Succeeded	Failed
s3://prathameshpc77	1 file, 20.0 B (100.00%)	0 files, 0 B (0%)

**Files and folders** (1 Total, 20.0 B)

Name	Folder	Type	Size	Status	Error
text_file.txt	-	text/plain	20.0 B	Succeeded	-

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Now click on close button, The screen will appear as below

s3.console.aws.amazon.com/s3/buckets/prathameshpc77?region=ap-south-1&tab=objects

aws Services Search [Alt+S]

Amazon S3 > Buckets > prathameshpc77

### prathameshpc77 Info

Objects Properties Permissions Metrics Management Access Points

#### Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI  Copy URL  Download  Open  Delete  Actions  Create folder  Upload

Find objects by prefix

Name	Type	Last modified	Size	Storage class
text_file.txt	txt	February 23, 2023, 10:23:00 (UTC+05:30)	20.0 B	Standard

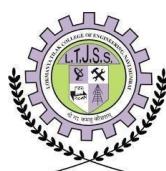


**Step-11 :** Select properties and scroll down to Static website hosting option which is disabled now click on Edit option on right side

The screenshot shows the AWS S3 console for a bucket named 'prathameshpc77'. The 'Properties' tab is selected. Under 'Transfer acceleration', 'Disabled' is selected. Under 'Object Lock', it says 'Amazon S3 currently does not support enabling Object Lock after a bucket has been created. To enable Object Lock for this bucket, contact Customer Support'. Under 'Requester pays', 'Disabled' is selected. Under 'Static website hosting', it says 'Use this bucket to host a website or redirect requests.' Both 'Static website hosting' and 'Index document' dropdowns are set to 'Disabled'. There are 'Edit' buttons for each section.

**Step-12 :** Enable the radio button and specify the file name in **Index document** which you have added in S3

The screenshot shows the 'Edit static website hosting' page for the 'prathameshpc77' bucket. Under 'Static website hosting', the 'Enable' radio button is selected. Under 'Hosting type', the 'Host a static website' radio button is selected. A note at the bottom states: 'For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access'.



#### Index document

Specify the home or default page of the website.

#### Error document - optional

This is returned when an error occurs.

#### Redirection rules – optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

```
1
```

[Cancel](#)[Save changes](#)

Scroll down and save the changes at bottom right, following screen will appear

(2) WhatsApp x | 11\_CCL\_EXP3 - Google Doc x | prathameshpc77-S3 buck x | Exp No-6 S3.pdf x | owncloudfinal\_Expt6(1).x | +

s3.console.aws.amazon.com/s3/buckets/prathameshpc77?region=ap-south-1&tab=properties

Guest Update

aws Services Search [Alt+S]

Successfully edited static website hosting.

Amazon S3 > Buckets > prathameshpc77

**prathameshpc77** [Info](#)

Objects Properties Permissions Metrics Management Access Points

**Bucket overview**

AWS Region	Amazon Resource Name (ARN)	Creation date
Asia Pacific (Mumbai) ap-south-1	arn:aws:s3:::prathameshpc77	February 23, 2023, 10:15:48 (UTC+05:30)

**Bucket Versioning**

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

[Edit](#)

Bucket Versioning  
Disabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

**Tags (0)**

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

[Edit](#)

Key	Value
No tags associated with this resource.	



## Step-13 : Click on Permissions Tab

The screenshot shows the AWS S3 Bucket Permissions Overview page for the bucket 'prathameshpc77'. The 'Permissions' tab is selected. The 'Access' section indicates that objects can be public. The 'Block public access (bucket settings)' section is off. The 'Bucket policy' section shows no policy displayed, with edit and delete buttons available.

## Step-14 : In bucket policy click on Edit option

### Step 15 : After clicking on edit button paste the following code in bucket policy

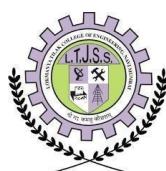
```
{ "Version": "2012-10-17", "Statement": [ { "Sid": "PublicReadGetObject", "Effect": "Allow", "Principal": "*", "Action": [ "s3:GetObject" ], "Resource": [ "arn:aws:s3:::Bucket-Name/*" ] } ] }
```

Note - Make sure that you add your bucket name in the code above Scroll down and click on Save Changes button

The screenshot shows the AWS S3 Bucket Policy Editor for the 'prathameshpc77' bucket. The policy JSON code is pasted into the 'Policy' field:

```
1: {  
2: "Version": "2012-10-17",  
3: "Statement": [  
4: {  
5: "Sid": "PublicReadGetObject",  
6: "Effect": "Allow",  
7: "Principal": "*",  
8: "Action": [  
9: "s3:GetObject"  
10: ],  
11: "Resource": [  
12: "arn:aws:s3:::prathameshpc77/*"  
13: ]  
14: },  
15: ]  
16: }
```

The 'Edit statement' and 'Select a statement' sections are visible on the right. At the bottom, there are buttons for '+ Add new statement', 'Save changes', and 'Cancel'.



Screenshot of the AWS S3 console showing the bucket policy editing interface for the 'prathameshpc77' bucket.

The browser tab bar shows multiple tabs including WhatsApp, 11\_CCL\_EXP3 - Google Doc, prathameshpc77-S3 buck, Exp No-6 S3.pdf, owncloudfinal\_Expt6(1).pdf, and a guest tab.

The AWS navigation bar includes Services, Search, and Global dropdown.

A green success message at the top states: "Successfully edited bucket policy."

The main content area shows the bucket details for 'prathameshpc77'. The 'Permissions' tab is selected. A 'Publicly accessible' button is present.

**Permissions overview**

Access: Public

**Block public access (bucket settings)**

Block all public access: Off

**Bucket policy**

The bucket policy is defined as follows:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddPerm",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::prathameshpc77/*"
    }
  ]
}
```

Copy button available for the policy.

Feedback, Language, and cookie preferences buttons are at the bottom.

## Step-16 : Open your text/html file and click on Object URL

Screenshot of the AWS S3 object details page for 'text\_file.txt' in the 'prathameshpc77' bucket.

The browser tab bar shows multiple tabs including WhatsApp, 11\_CCL\_EXP3 - Google Doc, prathameshpc77-S3 buck, Exp No-6 S3.pdf, owncloudfinal\_Expt6(1).pdf, and a guest tab.

The AWS navigation bar includes Services, Search, and Global dropdown.

The object details page for 'text\_file.txt' shows the following information:

**Properties**

- Owner: 19a975106c9c82e4b2484e8a771ae58705467f27ae426fd645951c9457c0c036
- AWS Region: Asia Pacific (Mumbai) ap-south-1
- Last modified: February 23, 2023, 10:23:00 (UTC+05:30)
- Size: 20.0 B
- Type: txt
- Key: text\_file.txt

**Object overview**

- S3 URI: s3://prathameshpc77/text\_file.txt
- Amazon Resource Name (ARN): arn:aws:s3:::prathameshpc77/text\_file.txt
- Entity tag (Etag): 6ddd8c65ec3ad17e121fc383db95bcd7
- Object URL: [https://prathameshpc77.s3.ap-south-1.amazonaws.com/text\\_file.txt](https://prathameshpc77.s3.ap-south-1.amazonaws.com/text_file.txt)

**Object management overview**

The following bucket properties and object management configurations impact the behavior of this object.

**Bucket properties**

Bucket Versioning: Disabled

**Management configurations**

Replication status: When a replication rule is applied to an object the replication status indicates the progress of the operation.

Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences



2 (2) WhatsApp x | 11\_CCL\_EXP3 - Google Doc x https://prathameshpc77.s3.ap-south-1.amazonaws.com/text\_file.txt Exp No-6

← → C 🔒 prathameshpc77.s3.ap-south-1.amazonaws.com/text\_file.txt

hello prathamesh !!

**Step-17 :** Now for delete files click on checkbox of your file and then click on **Delete Button**

Amazon S3 > Buckets > prathameshpc77

**prathameshpc77** [Info](#)

Publicly accessible

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

**Objects (1)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	<a href="#">text_file.txt</a>	txt	February 23, 2023, 10:23:00 (UTC+05:30)	20.0 B	Standard

Write permanently delete and click on delete object button

aws Services Search [Alt+S]

Amazon S3 > Buckets > prathameshpc77 > Delete objects

**Delete objects** [Info](#)

**Warning:**

- If a folder is selected for deletion, all objects in the folder will be deleted, and any new objects added while the delete action is in progress might also be deleted. If an object is selected for deletion, any new objects with the same name that are uploaded before the delete action is completed will also be deleted.
- Deleting the specified objects can't be undone.

[Learn more](#)

**Specified objects**

Find objects by name

Name	Type	Last modified	Size
<a href="#">text_file.txt</a>	txt	February 23, 2023, 10:23:00 (UTC+05:30)	20.0 B

**Permanently delete objects?**

To confirm deletion, type *permanently delete* in the text input field.

permanently delete

[Cancel](#) [Delete objects](#)

AIML11\_PRATHAMESH



(2) WhatsApp | 11\_CCL\_EXP3 - Google Doc | prathameshpc77-S3 buck | Exp No-6 S3.pdf | owncloudfinal\_Expt6(1). | +

s3.console.aws.amazon.com/s3/buckets/prathameshpc77/object/delete?region=ap-south-1&showversions=false

AWS Services Search [Alt+S]

Successfully deleted objects

Delete objects: status

The information below will no longer be available after you navigate away from this page.

**Summary**

Source	Successfully deleted	Failed to delete
s3://prathameshpc77	1 object, 20.0 B	0 objects

**Failed to delete** Configuration

**Failed to delete (0)**

Name	Folder	Type	Last modified	Size	Error
No objects failed to delete.					

Now click on close button

**Step-18 :** Now come to Amazon S3 tab and select your bucket and then click on delete button

(2) WhatsApp | 11\_CCL\_EXP3 - Google Doc | S3 Management Console | Exp No-6 S3.pdf | owncloudfinal\_Expt6(1). | +

s3.console.aws.amazon.com/s3/buckets?region=ap-south-1

AWS Services Search [Alt+S]

**Amazon S3**

**Buckets**

- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

**Storage Lens**

- Dashboards
- AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

**Amazon S3 > Buckets**

**Account snapshot**

Storage lens provides visibility into storage usage and activity trends. Learn more

**Buckets (2) Info**

Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date
elasticbeanstalk-ap-south-1-404055596869	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 9, 2023, 10:13:26 (UTC+05:30)
prathameshpc77	Asia Pacific (Mumbai) ap-south-1	Public	February 23, 2023, 10:15:48 (UTC+05:30)

**Actions:** Copy ARN, Empty, Delete, Create bucket



Write down your bucket name in delete bucket tab and click on delete button at bottom right

The screenshot shows the 'Delete bucket' confirmation dialog in the AWS S3 console. At the top, the path is shown as Amazon S3 > Buckets > prathameshpc77 > Delete bucket. Below this, the title 'Delete bucket' has an 'Info' link. A warning icon with three bullet points is displayed:

- Deleting a bucket cannot be undone.
- Bucket names are unique. If you delete a bucket, another AWS user can use the name.
- This bucket is configured to host a static website. We recommend that you clean up the Route 53 hosted zone settings that are related to the bucket.

A 'Learn more' link is also present. The main section asks 'Delete bucket "prathameshpc77"?'. It contains a text input field with the value 'prathameshpc77'. At the bottom, there are 'Cancel' and 'Delete bucket' buttons.

You can see that the bucket is deleted

The screenshot shows the 'Amazon S3' service page. The left sidebar includes 'Buckets', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Block Public Access settings for this account', 'Storage Lens' (with 'Dashboards' and 'AWS Organizations settings'), 'Feature spotlight', and 'AWS Marketplace for S3'. The main content area displays a success message: 'Successfully deleted bucket "prathameshpc77"'. Below this, the 'Buckets' section shows one item:

Name	AWS Region	Access	Creation date
elasticbeanstalk-ap-south-1-404055596869	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 9, 2023, 10:13:26 (UTC+05:30)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML**  
**Academic Year: 2022-23**

<b>NAME</b>	<b>PRATHAMESH CHIKANKAR</b>
<b>BRANCH</b>	<b>CSE-(AI&amp;ML)</b>
<b>ROLL NO.</b>	<b>11</b>
<b>SUBJECT</b>	<b>CLOUD COMPUTING LAB</b>
<b>COURSE CODE</b>	<b>CSL605</b>
<b>PRACTICAL NO.</b>	<b>04</b>
<b>DOP</b>	<b>02/03/2023</b>
<b>DOS</b>	



## AMAZON RDS

### STEP 1 : Login to AWS console and search RDS.

Search results for 'RDS'

Services (14)

- Features (28)
- Resources **New**
- Blogs (1,739)
- Documentation (62,581)
- Knowledge Articles (50)
- Tutorials (16)
- Events (58)
- Marketplace (420)

Services

- RDS **Managed Relational Database Service**
- AWS FIS **Improve resiliency and performance with controlled experiments.**
- AWS Glue DataBrew **Visual data preparation tool to clean and normalize data for analytics and machine le...**
- Database Migration Service **Managed Database Migration Service**

See all 14 results ▶

Features

- Reserved Instances **RDS feature**
- Proxies **RDS feature**
- Databases **RDS feature**
- Query Editor **RDS feature**

See all 28 results ▶

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

### STEP 2 - Click on to RDS and Create database.

Try the new Amazon RDS Multi-AZ deployment option for MySQL and PostgreSQL.  
For your Amazon RDS for MySQL and PostgreSQL workloads, improve transactional commit latencies by 2x, experience faster failover typically less than 35 seconds and, get read scalability with two readable standby DB instances by deploying the Multi-AZ DB cluster. [Learn more](#)

**Create database**

Or, [Restore Multi-AZ DB Cluster from Snapshot](#)

**Amazon RDS**

**Dashboard**

Databases  
Query Editor  
Performance insights  
Snapshots  
Exports in Amazon S3  
Automated backups  
Reserved instances  
Proxies

Subnet groups  
Parameter groups  
Option groups  
Custom engine versions

Events  
Event subscriptions

Recommendations (0)  
Certificate update

**Resources**

You are using the following Amazon RDS resources in the Asia Pacific (Mumbai) region (used/quota)

DB Instances (0/20)	Parameter groups (0)
Allocated storage (0 TB/100 TB)	Default (0)
Increase DB Instances limit <a href="#">[?]</a>	Custom (0/40)
DB Clusters (0/40)	Option groups (0)
Reserved Instances (0/20)	Default (0)
Snapshots (0)	Custom (0/20)
Manual	Subnet groups (0/20)
DB Cluster (0/100)	Supported platforms <a href="#">[?]</a> VPC
DB Instance (0/100)	Default network vpc-0449edc9aa9d9291
Automated	
DB Cluster (0)	
DB Instance (0)	

Recent events (0)  
Event subscriptions (0/20)

**Create database**

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale a relational database in the cloud.

**Recommended for you**

**Test Your DR Strategy in Minutes**  
Amazon Aurora Global Database now supports planned managed failover, making disaster recovery drills a breeze. [Learn more](#)

**Implementing Cross-Region DR**  
Learn how to set up Cross-Region disaster recovery (DR) for Aurora PostgreSQL, using an Aurora global database spanning multiple Regions. [Learn more](#)

**Migrate SSRS to RDS for SQL Server**  
Learn how you can migrate existing SSRS content to an Amazon RDS for SQL Server instance using a PowerShell module. [Learn more](#)

**Time-Series Tables in PostgreSQL**  
Step-by-step guide to design high-performance time series data tables on Amazon RDS for PostgreSQL. [Learn more](#)

**Additional information**

[Getting started with RDS](#) [\[?\]](#)  
[Overview and features](#) [\[?\]](#)

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

### STEP 3 - Select standard database.

### STEP 4 - Select MySQL and MySQL Community edition.

### STEP 5 - In Templates select Free tier.

### STEP 6 - Mention database name (default is database1) and username and password



## STEP 7 - Instance is db.t2.micro . Rest of things keep default

## STEP 8 - Select Public Access -Yes

We listened to your feedback! Now, create a database with a single click using our pre-built configurations! Or choose your own configurations.

**Create database**

**Choose a database creation method**

- Standard create You set all of the configuration options, including ones for availability, security, backups, and maintenance.
- Easy create Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

**Engine options**

Engine type: MySQL

- Aurora (MySQL Compatible)
- Aurora (PostgreSQL Compatible)
- MySQL
- MariaDB
- PostgreSQL
- Oracle
- Microsoft SQL Server
- SQL Server

Edition: MySQL Community

**Known issues/limitations**  
Review the Known issues/limitations [link](#) to learn about potential compatibility issues with specific database versions.

Show filters

Engine Version: MySQL 8.0.28

**Templates**  
Choose a sample template to meet your use case.

- Production Use defaults for high availability and fast, consistent performance.
- Dev/Test This instance is intended for development use outside of a production environment.
- Free tier Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.

**Availability and durability**

Deployment options

The deployment options below are limited to those supported by the engine you selected above.

- Multi-AZ DB Cluster - new Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy, and increases capacity to serve read workloads.
- Multi-AZ DB instance (not supported for Multi-AZ DB cluster snapshot) Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
- Single DB instance (not supported for Multi-AZ DB cluster snapshot) Creates a single DB instance with no standby DB instances.

**Settings**

**DB instance identifier** databasePrathamesh

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

**Credentials Settings**

**Master username** admin

1 to 10 alphanumeric characters. First character must be a letter.

Manage master credentials in AWS Secrets Manager Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

If you manage the master user credentials in Secrets Manager, some RDS features aren't supported. [Learn more](#)

Auto generate a password Amazon RDS can generate a password for you, or you can specify your own password.

**Master password** [Info](#)  
\*\*\*\*\*  
Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

**Confirm master password** [Info](#)  
\*\*\*\*\*

**Instance configuration**  
The DB instance configuration options below are limited to those supported by the engine that you selected above.

**DB instance class** [Info](#)  
 Standard classes (includes m classes)  
 Memory optimized classes (includes r and x classes)  
 Burstable classes (includes t classes)

db.t2.micro  
1 vCPU 1 GiB RAM Not EBS Optimized

Include previous generation classes

**Storage**

**Storage type** [Info](#)  
General Purpose SSD (gp2)  
Baseline performance determined by volume size

**Allocated storage** [Info](#)  
200 GiB  
The minimum value is 20 GiB and the maximum value is 6,144 GiB

**Storage autoscaling** [Info](#)  
Provides dynamic scaling support for your database's storage based on your application's needs.

Enable storage autoscaling Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

**Maximum storage threshold** [Info](#)  
Charges will apply when your database autoscales to the specified threshold  
1000 GiB  
The minimum value is 220 GiB and the maximum value is 6,144 GiB

**Connectivity** [Info](#)

**Compute resource**  
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Don't connect to an EC2 compute resource Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

Connect to an EC2 compute resource Set up a connection to an EC2 compute resource for this database.

**Virtual private cloud (VPC)** [Info](#)  
Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Default VPC (vpc-0449edc9aa9d9291)  
Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

**DB subnet group** [Info](#)  
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

default

**Public access** [Info](#)

Yes RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

No RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

**VPC security group (firewall)** [Info](#)  
Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

Choose existing Choose existing VPC security groups

Create new Create new VPC security group

**Existing VPC security groups**  
Choose one or more options  
default X

**Availability Zone** [Info](#)  
No preference

**RDS Proxy**  
RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

Create an RDS Proxy [Info](#)  
RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see [Amazon RDS Proxy pricing](#).

**Certificate authority - optional** [Info](#)  
Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-2019 (default)

If you don't select a certificate authority, RDS chooses one for you.



## STEP 9 - Click on to Create Database.

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-2019 (default)

If you don't select a certificate authority, RDS chooses one for you.

► Additional configuration

**Database authentication**

Database authentication options [Info](#)

Password authentication  
Authenticates using database passwords.

Password and IAM database authentication  
Authenticates using the database password and user credentials through AWS IAM users and roles.

Password and Kerberos authentication  
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

**Monitoring**

Monitoring

Enable Enhanced monitoring  
Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU.

► Additional configuration

Database options, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

**Estimated monthly costs**

The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free:

- 750 hrs of Amazon RDS in a Single-AZ db.t2.micro, db.t3.micro or db.t4g.micro Instance.
- 20 GB of General Purpose Storage (SSD).
- 20 GB for automated backup storage and any user-initiated DB Snapshots.

[Learn more about AWS Free Tier](#)

When your free usage expires or if your application use exceeds the free usage tiers, you simply pay standard, pay-as-you-go service rates as described in the [Amazon RDS Pricing page](#).

**Important** You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

[Cancel](#) [Create database](#)

## STEP 10 - It will take some time.

## STEP 11 - Click on to view credentials.

(2) WhatsApp | ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#databases: MySQL :: Begin Your Down [Alt+S] Guest (Update)

aws Services Search [Alt+S]

Amazon RDS

Databases

Successfully created database databaseprathamesh How was your experience creating an Amazon RDS database? [Provide feedback](#)

RDS > Databases

Consider creating a Blue/Green Deployment to minimize downtime during upgrades You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

Databases

Filter by databases

DB identifier	Role	Engine	Region & AZ	Size	Status	Actions	CPU	Current activity	Maintenance
databaseprathamesh	Instance	MySQL Community	ap-south-1b	db.t2.micro	Available	-	-	none	

[View connection details](#) [Create database](#)

## STEP 12 - Go to google type mysql workbench.

Google mysql workbench

About 1,31,00,000 results (0.26 seconds)

MySQL https://www.mysql.com › products › workbench

**MySQL Workbench**

MySQL Workbench is a unified visual tool for database architects, developers, and DBAs. MySQL Workbench provides data modeling, SQL development, ...

**MySQL Workbench 8.0.32**

The following LGPL libraries are used by MySQL Workbench and ...

**SQL Development**

MySQL Workbench gives developers a complete set of ...

**Visual Database Design**

MySQL Workbench is a visual database design tool that integrates SQL development, administration, database design, creation and maintenance into a single integrated development environment for the MySQL database system. [Wikipedia](#)

AIML11\_PRATHAMESH



## STEP 13 - Click on to download.

The screenshot shows the MySQL website with the URL [mysql.com/products/workbench/](https://www.mysql.com/products/workbench/). The main navigation bar includes links for MySQL.COM, DOWNLOADS, DOCUMENTATION, and DEVELOPER ZONE. Below the navigation, there's a sub-navigation for Products, Cloud, Services, Partners, Customers, Why MySQL?, News & Events, and How to Buy. A sidebar on the left lists MySQL HeatWave, MySQL Enterprise Edition (which is selected), Datasheet (PDF), Technical Specification, MySQL Database, MySQL Document Store, Oracle Enterprise Manager, and Enterprise Monitor. The central content area features a section for MySQL Workbench with a sub-section for Enhanced Data Migration. It includes a 'Download Now' button and a screenshot of the software interface. A descriptive text below the screenshot states: 'MySQL Workbench is a unified visual tool for database architects, developers, and DBAs. MySQL Workbench provides data modeling, SQL development, and comprehensive administration tools for server configuration, user administration, backup, and much more. MySQL Workbench is available on Windows, Linux and Mac OS X.'

## STEP 14 - MySQL community download – Microsoft Windows.

### STEP 15 - Click on to – No thanks, just download.

The screenshot shows the MySQL Community Downloads page for MySQL Workbench. The URL is [dev.mysql.com/downloads/workbench/](https://dev.mysql.com/downloads/workbench/). The page has tabs for General Availability (GA) Releases and Archives. The GA tab is selected, showing MySQL Workbench 8.0.32. A dropdown menu for 'Select Operating System' is set to 'Microsoft Windows'. Below this, a 'Recommended Download' section shows the MySQL Installer for Windows, which includes icons for MySQL Workbench, MySQL Server, and MySQL Community Server. A link 'Go to Download Page >' is present. Other download options include Windows (x86, 32 & 64-bit), MySQL Installer MSI, and Windows (x86, 64-bit), MSI Installer. A note at the bottom suggests using MD5 checksums and GnuPG signatures for package verification.

**No thanks, just start my download.**

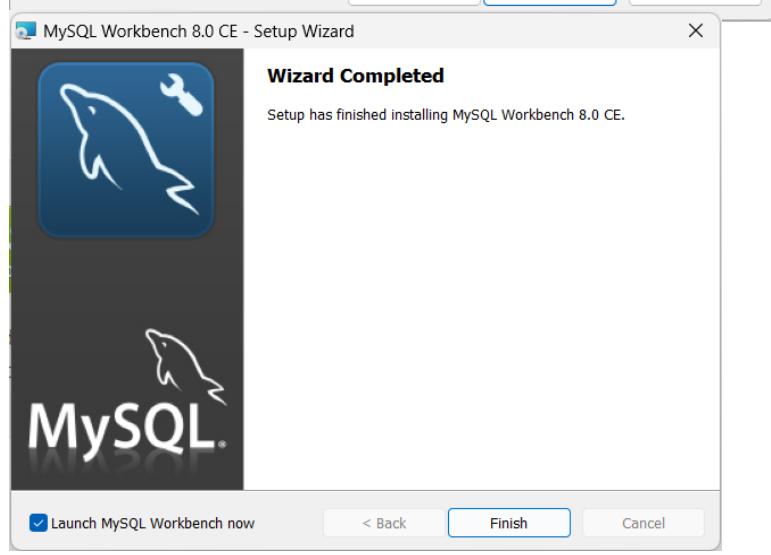
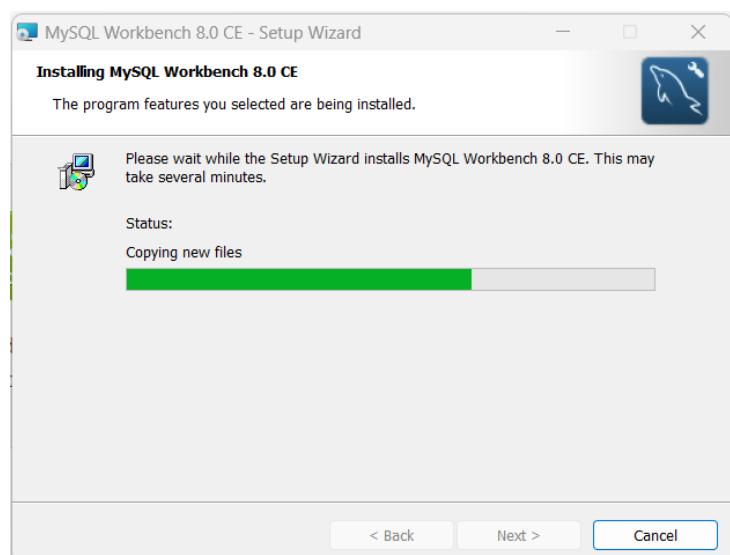
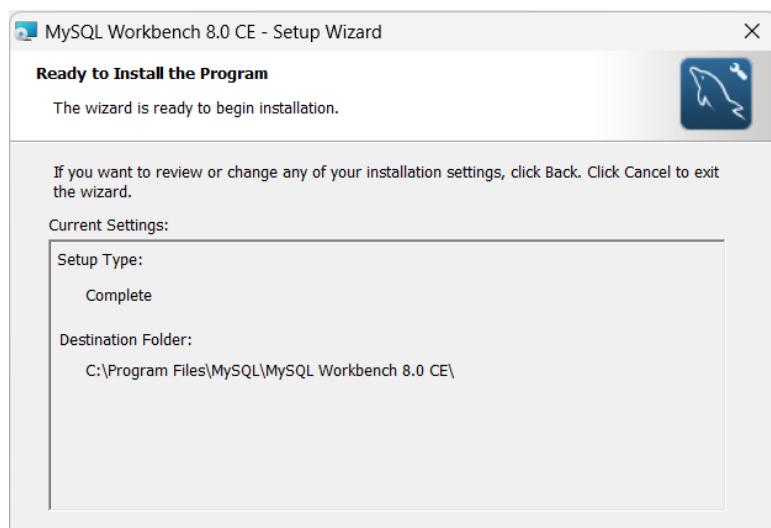
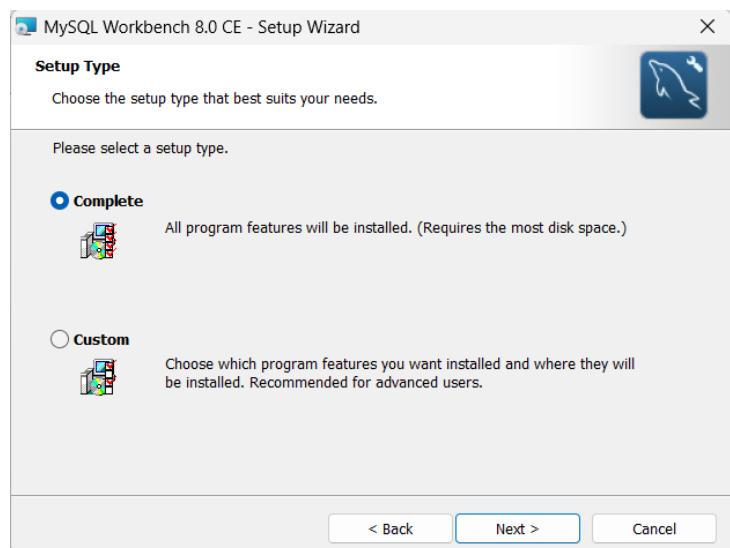
This screenshot shows the same MySQL Community Downloads page, but the 'No thanks, just start my download.' button is highlighted, indicating it has been clicked. The page also includes sections for Login and Sign Up.

## STEP 16 - Go to downloads of your machine and install it with default settings

The screenshot shows the MySQL Workbench 8.0 CE - Setup Wizard. The title bar says 'MySQL Workbench 8.0 CE - Setup Wizard'. The main window displays the 'Welcome to the Setup Wizard for MySQL Workbench 8.0 CE' screen. It features a large MySQL logo icon on the left and a welcome message: 'The Setup Wizard will install version 8.0.32 on your computer. To continue, click Next.' Below this is a 'WARNING' message: 'WARNING: This program is protected by copyright law and international treaties.' At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

The screenshot shows the 'Destination Folder' screen of the MySQL Workbench 8.0 CE - Setup Wizard. The title bar says 'MySQL Workbench 8.0 CE - Setup Wizard'. The main content area asks 'Click Next to install to this folder, or click Change to install to a different folder.' It shows the current destination folder as 'C:\Program Files\MySQL\MySQL Workbench 8.0 CE\' and a 'Change...' button. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

AIML11\_PRATHAMESH



Check your database is created and status is available.

Amazon RDS

Databases

databaseprathamesh

Summary

DB Identifier databaseprathamesh	CPU 5.17%	Status Available	Class db.t2.micro
Role Instance	Current activity 0 Connections	Engine MySQL Community	Region & AZ ap-south-1b

Connectivity & security

Endpoint databaseprathamesh.csvvk8v18qu.ap-south-1.rds.amazonaws.com	Networking Availability Zone ap-south-1b VPC vpc-0449edc9aaf9d9291 Subnet group default-vpc-0449edc9aaf9d9291 Subnets subnet-00aea300ab46c7aab subnet-02be2f55336da33d subnet-0e745ac9657b00c4b Network type IPv4	Security VPC security groups default (sg-06e78ec6298178a32) Active Publicly accessible Yes Certificate authority rds-ca-2019 Certificate authority date August 22, 2024, 22:38 (UTC+05:30) DB instance certificate expiration date August 22, 2024, 22:38 (UTC+05:30)
---	---	--



## STEP 17 - Click on the databases and select yours

(2) WhatsApp    11\_CCL\_EXP4 - Google Docs    RDS Management Console    MySQL :: Begin Your Download

Amazon RDS Services Search [Alt+S]

Databases

RDS Databases

Successfully created database databaseprathamesh

How was your experience creating an Amazon RDS database? Provide feedback

Consider creating a Blue/Green Deployment to minimize downtime during upgrades

You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

Databases

DB identifier: databaseprathamesh

DB identifier	Role	Engine	Region & AZ	Size	Status	Actions	CPU	Current activity	Maintenance
databaseprathamesh	Instance	MySQL Community	ap-south-1b	db.t2.micro	Available	-	-	none	

## STEP 18 - Copy Endpoint

(1) WhatsApp    11\_CCL\_EXP4 - Google Docs    RDS Management Console    MySQL :: Begin Your Download

Amazon RDS Services Search [Alt+S]

Dashboard Databases

Query Editor Performance insights Snapshots Exports in Amazon S3 Automated backups Reserved instances Proxies

Subnet groups Parameter groups Option groups Custom engine versions

Connectivity & security

Endpoint & port	Networking	Security
Endpoint: databaseprathamesh.csxvk8v18qku.ap-south-1.rds.amazonaws.com	Availability Zone: ap-south-1b VPC: vpc-0449edc9aaf9d9291 Subnet group: default-vpc-0449edc9aaf9d9291 Subnets: subnet-00aea300ab46c7aab, subnet-02fbe2f55336da33d, subnet-0e745ac9657b00c4b Network type: IPv4	VPC security groups: default (sg-06e78ec6298178a32) Active Publicly accessible: Yes Certificate authority: rds-ca-2019 Certificate authority date: August 22, 2024, 22:38 (UTC+05:30) DB instance certificate expiration date: August 22, 2024, 22:38 (UTC+05:30)

## STEP 19 - Go back to the workbench.

## STEP 20 - Click on to mysql connection

MySQL Workbench

Welcome to MySQL Workbench

MySQL Workbench is the official graphical user interface (GUI) tool for MySQL. It allows you to design, create and browse your database schemas, work with database objects and insert data as well as design and run SQL queries to work with stored data. You can also migrate schemas and data from other database vendors to your MySQL database.

Browse Documentation >    Read the Blog >    Discuss on the Forums >

MySQL Connections    Rescan servers

MySQL Workbench could not detect any MySQL server running.  
This means that MySQL is not installed or is not running.  
Rescan servers

## STEP 21 - Paste copied endpoint in Hostname, Connection Name: databaseprathamesh Username: admin, Enter admin password and then Click on to Test Connection



Setup New Connection

Connection Name: databaseprathamesh

Connection Method: Standard (TCP/IP)

Parameters SSL Advanced

Hostname: 3v18qxu.ap-south-1.rds.amazonaws.com Port: 3306

Name or IP address of the server host - and TCP/IP port.

Username: admin

Name of the user to connect with.

Password:  Store in Vault ... Clear

The user's password. Will be requested later if it's not set.

Default Schema:

The schema to use as default schema. Leave blank to select it later.

Configure Server Management... Test Connection Cancel OK

## STEP 22 - Go to VPC security group

WhatsApp 11\_CCL\_EXP4 - Google Docs RDS Management Console MySQL :: Begin Your Download

ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#database:id=databaseprathamesh;is-cluster=false

AWS Services Search [Alt+S]

Mumbai prathameshpc77

Amazon RDS

Dashboard Databases Query Editor Performance insights Snapshots Exports in Amazon S3 Automated backups Reserved instances Proxies Subnet groups Parameter groups Option groups Custom engine versions

Connectivity & security

Endpoint & port	Networking	Security
Endpoint databaseprathamesh.csxvk8v18qxu.ap-south-1.rds.amazonaws.com	Availability Zone ap-south-1b	VPC security groups default (sg-06e78ec6298178a32) Active
Port 3306	VPC vpc-0449edc9aaf9d9291	Publicly accessible Yes
	Subnet group default-vpc-0449edc9aaf9d9291	Certificate authority Info rds-ca-2019
	Subnets subnet-00aea300ab46c7aab subnet-02fbe2f55336da33d subnet-0e745ac9657b00c4b	Certificate authority date August 22, 2024, 22:38 (UTC+05:30)
	Network type IPv4	DB instance certificate expiration date August 22, 2024, 22:38 (UTC+05:30)

## STEP 23 - Click on to Inbound rules

Security Groups (1/1) Actions Export security groups to CSV Create security group

search: sg-06e78ec6298178a32

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
-	sg-06e78ec6298178a32	default	vpc-0449edc9aaf9d9291	default VPC security gr...	404055596869	2 Permission entries	1 Permission entry

sg-06e78ec6298178a32 - default

Inbound rules Outbound rules Tags

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-0093059cc0d7462c7	-	All traffic	All	All	sg-06e78ec6298178a...	-
-	sgr-01e27290577c499...	IPv4	Custom TCP	TCP	0	0.0.0.0/0	-



**STEP 24 - First select Click on to Edit inbound rule  
add rule select ipv4 --all traffic (add 0.0.0.0/0) and  
save Rules (Important step to add inbound rule)**

Inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
sgr-0093059cc0d7462c7	All traffic	All	All	Custom	sg-06e78ec6298178a32
sgr-0d0c7aeee9cb618c1	All traffic	All	All	Custom	0.0.0.0/0

[Add rule](#)

Cancel [Preview changes](#) [Save rules](#)

New EC2 Experience [Tell us what you think](#)

EC2 Dashboard [Services](#) [Search](#) [Alt+S]

[Inbound security group rules successfully modified on security group \(sg-06e78ec6298178a32 | default\)](#)

Details

Security Groups (1/1) [Info](#)

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-06e78ec6298178a32	default	vpc-0449edc9af9d9291	default VPC security gr...	404055596869

**STEP 25 - Go to workbench (after giving details click on to Test Connection)**

Setup New Connection

Connection Name: **databaseprathamesh**

Connection Method: **Standard (TCP/IP)**

Parameters **SSL** Advanced

Hostname: **3v18qxu.ap-south-1.rds.amazonaws.com**

Username: **admin**

Password: **Store in Vault ...** Clear

Default Schema:

MySQL Workbench

**Successfully made the MySQL connection**

Information related to this connection:

Host: **databaseprathamesh.csxvk8v18qxu.ap-south-1.rds.amazonaws.com**  
Port: **3306**  
User: **admin**  
SSL: **enabled with TLS\_AES\_256\_GCM\_SHA384**

A successful MySQL connection was made with the parameters defined for this connection.

OK

Configure Server Management... [Test Connection](#) Cancel OK

Click on **Ok** button twice

Go to workbench double click on connection (databaseprathamesh)



MySQL Workbench

File Edit View Database Tools Scripting Help

# Welcome to MySQL Workbench

MySQL Workbench is the official graphical user interface (GUI) tool for MySQL. It allows you to design, create and browse your database schemas, work with database objects and insert data as well as design and run SQL queries to work with stored data. You can also migrate schemas and data from other database vendors to your MySQL database.

Browse Documentation >    Read the Blog >    Discuss on the Forums >

MySQL Connections ⊕ ↻

databaseprathamesh

admin  
databaseprathamesh.csvvkv8v18qxu....

It will get opened.

MySQL Workbench

File Edit View Query Database Server Tools Scripting Help

Navigator

MANAGEMENT

- Server Status
- Client Connections
- Users and Privileges
- Status and System Variables
- Data Export
- Data Import/Restore

INSTANCE

- Startup / Shutdown
- Server Logs
- Options File

PERFORMANCE

- Dashboard
- Performance Reports
- Performance Schema Setup

Query 1

Automatic context help is disabled. Use the toolbar to manually get help for the current caret position or to toggle automatic help.

## STEP 26 - Write query and execute

Create database tsec;

Use tsec; Show tables;

create table student( roll int, name varchar(10), city varchar(10));

Desc student; insert into student values(11,'prathamesh','mumbai');

Select \* from student;

MySQL Workbench

File Edit View Query Database Server Tools Scripting Help

Navigator

MANAGEMENT

- Server Status
- Client Connections
- Users and Privileges
- Status and System Variables
- Data Export
- Data Import/Restore

INSTANCE

- Startup / Shutdown
- Server Logs
- Options File

PERFORMANCE

- Dashboard
- Performance Reports
- Performance Schema Setup

Query 1

Automatic context help is disabled. Use the toolbar to manually get help for the current caret position or to toggle automatic help.

```
1 • Create database tsec;
2 • use tsec;
3 • Show tables;
4 • create table student( roll int, name varchar(10), city varchar(10));
5 • Desc student;
6 • insert into student values(11,'prathamesh','mumbai');
7 • select * from student;
```

Result Grid | Filter Rows: Export: Wrap Cell Content: □

roll	name	city
11	prathamesh	mumbai

Output

Action Output

#	Time	Action	Message	Duration / Fetch
1	10:43:57	Create database tsec	1 row(s) affected	0.031 sec
2	10:44:10	use tsec	0 row(s) affected	0.000 sec
3	10:44:52	Show tables	0 row(s) returned	0.000 sec / 0.000 sec
4	10:45:15	create table student(roll int, name varchar(10), city varchar(10))	0 row(s) affected	0.078 sec
5	10:45:35	Desc student	3 row(s) returned	0.000 sec / 0.000 sec
6	10:46:09	insert into student values(11,'prathamesh','mumbai')	1 row(s) affected	0.016 sec
7	10:46:34	select * from student LIMIT 0, 1000	1 row(s) returned	0.000 sec / 0.000 sec



## STEP 27 - Now delete the instance (once you have done with it)

Select databases, go to action **stop instance** and then **delete instance**.

The screenshot shows the AWS RDS console. On the left, the navigation pane includes options like Dashboard, Databases (which is selected), Query Editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups, Stop DB instance temporarily, and a Snapshot - optional section. The main area displays a 'Databases' table with one entry: 'databaseprathamesh' (Instance: MySQL Community). A context menu is open over this entry, showing actions: Quick Actions - New, Convert to Multi-AZ deployment, Stop temporarily, Reboot, and Delete. The 'Delete' option is highlighted. A separate window titled 'Stop DB instance temporarily' is also visible, containing instructions and checkboxes for stopping the instance.

### Delete databaseprathamesh instance?

Are you sure you want to Delete the databaseprathamesh DB Instance?

- Create final snapshot  
Determines whether a final DB Snapshot is created before the DB instance is deleted.
- Retain automated backups  
Determines whether retaining automated backups for 7 days after deletion
- I acknowledge that upon instance deletion, automated backups, including system snapshots and point-in-time recovery, will no longer be available.

To confirm deletion, type *delete me* into the field

delete me

⚠ We strongly recommend taking a final snapshot before instance deletion since after your instance is deleted, automated backups will no longer be available.

Cancel

Delete

The screenshot shows the AWS RDS console. The left navigation pane is identical to the previous screenshot. The main area shows the 'Databases' table with the 'databaseprathamesh' entry. A context menu is open over the database row, with 'Delete' highlighted. A blue header bar at the top of the main content area displays the message 'Stopping database databaseprathamesh is in progress'. The rest of the interface is similar to the previous screenshot, showing the 'Delete' confirmation dialog.

Uncheck the final snapshot., As you can see that DB instance is deleted successfully

The screenshot shows the AWS RDS console. The left navigation pane is identical. The main area shows the 'Databases' table, which is now empty, displaying the message 'No instances found'. The context menu from the previous screenshots is no longer present.



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML**  
**Academic Year: 2022-23**

<b>NAME</b>	<b>PRATHAMESH CHIKANKAR</b>
<b>BRANCH</b>	<b>CSE-(AI&amp;ML)</b>
<b>ROLL NO.</b>	<b>11</b>
<b>SUBJECT</b>	<b>CLOUD COMPUTING LAB</b>
<b>COURSE CODE</b>	<b>CSL605</b>
<b>PRACTICAL NO.</b>	<b>05</b>
<b>DOP</b>	<b>09/03/2023</b>
<b>DOS</b>	



## SECURITY AS A SERVICE ON AWS

**Aim : To study Security as a Service on AWS Security**

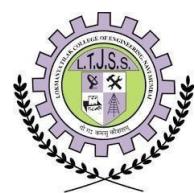
### **Theory :**

Cloud security at AWS is the highest priority. As organizations embrace the scalability and flexibility of the cloud, AWS is helping them evolve security, identity, and compliance into key business enablers. AWS builds security into the core of our cloud infrastructure, and offers foundational services to help organizations meet their unique security requirements in the cloud.

- As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations. Security in the cloud is much like security in your on-premises data centers—only without the costs of maintaining facilities and hardware. In the cloud, you don't have to manage physical servers or storage devices. Instead, you use software-based security tools to monitor and protect the flow of information into and out of your cloud resources.
- An advantage of the AWS Cloud is that it allows you to scale and innovate, while maintaining a secure environment and paying only for the services you use. This means that you can have the security you need at a lower cost than in an on-premises environment.
- As an AWS customer you inherit all the best practices of AWS policies, architecture, and operational processes built to satisfy the requirements of our most security-sensitive customers. Get the flexibility and agility you need in security controls.
- The AWS Cloud enables a shared responsibility model. While AWS manages security of the cloud, you are responsible for security in the cloud. This means that you retain control of the security you choose to implement to protect your own content, platform, applications, systems, and networks no differently than you would in an on-site data center.
- AWS provides you with guidance and expertise through online resources, personnel, and partners. AWS provides you with advisories for current issues, plus you have the opportunity to work with AWS when you encounter security issues.
- You get access to hundreds of tools and features to help you to meet your security objectives. AWS provides security-specific tools and features across network security, configuration management, access control, and data encryption.
- Finally, AWS environments are continuously audited, with certifications from accreditation bodies across geographies and verticals. In the AWS environment, you can take advantage of automated tools for asset inventory and privileged access reporting.

### **Benefits of AWS security**

- **Keep Your data safe —** The AWS infrastructure puts strong safeguards in place to help protect your privacy. All data is stored in highly secure AWS data centers.
- **Meet compliance requirements —** AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed.
- **Save money —**Cut costs by using AWS data centers. Maintain the highest standard of security without having to manage your own facility
- **Scale quickly —** Security scales with your AWS Cloud usage. No matter the size of your business, the AWS infrastructure is designed to keep your data safe.



Security as a Service on AWS refers to a set of cloud-based security services that are provided by Amazon Web Services (AWS) to help customers secure their applications and data in the cloud.

The screenshot shows the AWS Management Console with the sidebar open, displaying a list of services. The 'Services' button is highlighted. The search bar contains 'Search'. The keyboard shortcut '[Alt+S]' is shown in the top right. The main content area is titled 'Security, Identity, & Compliance' and lists various services:

- AWS Artifact
- AWS Audit Manager
- Certificate Manager
- CloudHSM
- Cognito
- Detective
- Directory Service
- AWS Firewall Manager
- GuardDuty
- IAM
- IAM Identity Center (successor to AWS Single Sign-On)

## Amazon Inspector

Continual vulnerability management at scale

## Key Management Service

Securely Generate and Manage AWS Encryption Keys

## Amazon Macie

Amazon Macie classifies and secures your business-critical content.

## AWS Private Certificate Authority

Managed private certificate authority service

## Resource Access Manager

Share AWS resources with other accounts or AWS Organizations

## Secrets Manager

Easily rotate, manage, and retrieve secrets throughout their lifecycle

## Security Hub

AWS Security Hub is AWS's security and compliance center

## Security Lake

Automatically centralize all your security data with a few clicks

## AWS Signer

Ensuring trust and integrity of your code

## Amazon Verified Permissions

Manage, analyze and enforce permissions across your applications

## WAF & Shield

Protects Against DDoS Attacks and Malicious Web Traffic



To study Security as a Service on AWS, you can follow the following steps:

- **Learn about the AWS Shared Responsibility Model:** The AWS Shared Responsibility Model is a critical concept to understand when it comes to security on AWS. AWS is responsible for securing the infrastructure that runs the cloud, while the customer is responsible for securing their data and applications in the cloud. Understanding the shared responsibility model is critical to ensuring that you are securing your applications and data appropriately on AWS.
- **Understand the various AWS Security Services:** AWS offers a wide range of security services that can help you secure your applications and data. These services include:
  1. Identity and Access Management (IAM): IAM allows you to manage access to AWS resources securely. You can create users and groups, assign permissions, and use IAM roles to grant temporary access to users or services.
  2. Amazon Inspector: Inspector is an automated security assessment service that helps you test the security of your applications and infrastructure.
  3. Amazon GuardDuty: GuardDuty is a threat detection service that continuously monitors for malicious activity in your AWS account.
  4. AWS WAF: The AWS Web Application Firewall (WAF) helps you protect your web applications from common web exploits and attacks.
  5. Amazon Macie: Macie is a fully managed data security and privacy service that uses machine learning and pattern matching to discover and protect sensitive data.
  6. AWS Certificate Manager: Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.
- **Study AWS Security Best Practices:** AWS publishes a set of security best practices for all of its services. These best practices include detailed guidance on how to secure your applications and data, and they cover topics such as access management, network security, data encryption, and logging.
- **Review AWS Compliance and Security Reports:** AWS regularly publishes compliance and security reports, such as SOC 2, ISO 27001, and PCI DSS reports. These reports provide independent verification of AWS's compliance with industry-standard security and compliance frameworks.
- **Practice with AWS Security Services:** AWS provides a free tier that allows you to experiment with many of its security services without incurring any costs. Use this opportunity to practice and experiment with AWS security services.
- **Get Certified:** AWS offers several security-related certifications, such as AWS Certified Security – Specialty. These certifications demonstrate your knowledge and expertise in securing applications and data on AWS. Consider getting certified to validate your skills.
- **Stay up-to-date:** AWS is constantly updating and adding new security features and services. Stay up-to-date with these changes by reading AWS blogs, attending webinars, and participating in AWS events.

By following these steps, you can gain a comprehensive understanding of Security as a Service on AWS and become proficient in securing applications and data in the cloud.



## **8 Securities Case Study**

8 Securities uses the following products from AWS as part of its infrastructure:

- **Amazon EC2 Windows instances**— To run the portal, main website, and business intelligence tools
- **Elastic IP Addresses for Amazon EC2**—To bind to domain names, and start and stop instances on demand
- **Amazon EBS**— Used for data storage, for starting and stopping instances, and for having data always available
- **Amazon VPC**— Used for a production network. Roll notes, “As some of our applications are bound to the machine Media Access Control [MAC] address, the key benefit for us is to have static MAC addresses when instances are restarted.”
- **Elastic Load Balancing**— Used for the main website, to load balance across multiple instances

### **Top 6 AWS Account Security Tools**

#### **1. AWS Identity and Access Management (IAM)**

AWS IAM is essential for controlling access to your AWS resources. It enables you to create users and roles with permissions to specific resources in your AWS environment. Always assigning least-privilege permissions to these users and roles minimizes the impact of a breach where an attacker has gained access. AWS IAM also has multi-factor authentication and supports single sign-on (SSO) access to further secure and centralize user access.

#### **2. Amazon GuardDuty**

Amazon GuardDuty uses machine learning to look for malicious activity in your AWS environments. It combines your CloudTrail event logs, VPC Flow Logs, S3 event logs, and DNS logs to continuously monitor and analyze all activity. GuardDuty identifies issues such as privilege escalation, exposed credentials, and communication with malicious IP addresses and domains. It can also detect when your EC2 instances are serving malware or mining bitcoin.

#### **3. Amazon Macie**

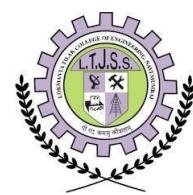
Amazon Macie discovers and protects your sensitive data stored in AWS S3 buckets. It first identifies sensitive data in your buckets, such as personally-identifiable information or personal health information, through discovery jobs. You can schedule these jobs to monitor new data added to your buckets. After it finds sensitive data, Macie continuously evaluates your buckets and alerts you when a bucket is unencrypted, is publicly accessible, or is shared with AWS accounts outside of your organization.

#### **4. AWS Config**

AWS Config records and continuously evaluates your AWS resource configuration. This includes keeping a historical record of all changes to your resources, which is useful for compliance with legal requirements and your organization's policies. AWS Config evaluates new and existing resources against rules that validate certain configurations. For example, if all EC2 volumes must be encrypted, AWS Config can detect non-encrypted volumes and send a notification. In addition, it can also execute remediation actions such as encrypting the volume or deleting it.

#### **5. AWS CloudTrail**

AWS CloudTrail tracks all activity in your AWS environment. It records all actions a user executes in the AWS console and all API calls as events. You can view and search these events to identify unexpected or unusual requests in your AWS environment.



## 6. Security Hub

AWS Security Hub combines information from all the above services in a central, unified view. It collects data from all security services from multiple AWS accounts and regions, making it easier to get a complete view of your AWS security posture. In addition, Security Hub supports collecting data from third-party security products. Security Hub is essential to providing your security team with all the information they may need.

### Top 4 AWS Application Security Tools

#### 1. Amazon Inspector

Amazon Inspector is a security assessment service for applications deployed on EC2. These assessments include network access, common vulnerabilities and exposures (CVEs), Center for Internet Security (CIS) benchmarks, and common best practices such as disabling root login for SSH and validating system directory permissions on your EC2 instances.

#### 2. AWS Shield

AWS Shield is a fully-managed distributed denial-of-service (DDoS) protection service. Shield is enabled by default as a free standard service with protection against common DDoS attacks against your AWS environment.

#### 3. AWS Web Application Firewall

AWS Web Application Firewall (WAF) monitors and protects applications and APIs built on services such as CloudFront, API Gateway, and AppSync. You can block access to your endpoints based on different criteria such as the source IP address, the request's origin country, values in headers and bodies, and more (i.e, you can enable rate limiting, only allowing a certain number of requests per IP)

#### 4. AWS Secrets Manager

AWS Secrets Manager is a managed service where you can store and retrieve sensitive information such as database credentials, certificates, and tokens. Use fine-grained permissions to specify exact actions an entity can perform on the secrets, such as creating, updating, deleting, or retrieving secrets.

**Conclusion : We had successfully studied Security as a Service on AWS Security.**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML  
Academic Year: 2022-23**

<b>NAME</b>	<b>PRATHAMESH CHIKANKAR</b>
<b>BRANCH</b>	<b>CSE-(AI&amp;ML)</b>
<b>ROLL NO.</b>	<b>11</b>
<b>SUBJECT</b>	<b>CLOUD COMPUTING LAB</b>
<b>COURSE CODE</b>	<b>CSL605</b>
<b>PRACTICAL NO.</b>	<b>06</b>
<b>DOP</b>	<b>16/03/2023</b>
<b>DOS</b>	



## IAM - (IDENTITY & ACCESS MANAGEMENT)

**Step 1 - Sign in.** Sign in as a root user. Provide username and password when prompted. Open the console and search for **IAM** and click on it.

The screenshot shows the AWS Services search results for 'iam'. The 'Services' section on the left lists various services like Features, Resources (New), Blogs, Documentation, Knowledge Articles, Tutorials, Events, and Marketplace. The main search results page shows 'Search results for 'iam'' at the top. It lists three services: 'IAM' (Manage access to AWS resources), 'IAM Identity Center (successor to AWS Single Sign-On)' (Manage workforce user access to multiple AWS accounts and cloud applications), and 'Resource Access Manager' (Share AWS resources with other accounts or AWS Organizations). A link to 'See all 8 results' is also present.

**Step 2 - Select the Users menu.** Navigate to the Users screen. You'll find it in the IAM dashboard, under **Identity and Access Management (IAM)** drop-down menu on the left side of the screen. Click on **Users**.

The screenshot shows the IAM Management Console dashboard. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'Users' is listed. The main dashboard has sections for 'Security recommendations' (with items like 'Add MFA for root user', 'Root user has no active access keys', and 'Update your access permissions for AWS Billing, Cost Management, and Account consoles'), 'IAM resources' (showing 0 User groups, 0 Users, 8 Roles, 0 Policies, and 0 Identity providers), and 'What's new' (listing recent updates like 'Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023.', 'AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs.', 'AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions.', and 'Amazon ElastiCache simplifies password rotations with Secrets Manager.'). On the right, there are sections for 'AWS Account' (Account ID: 404055596869, Account Alias: 404055596869 Create), 'Quick Links' (My security credentials, Tools), 'Policy simulator', 'Web identity federation playground', and 'Additional information' (Best practices for Identity and Access Management, IAM documentation, Videos, IAM release history, and additional resources).

**Step 3 - Add a user.** Click on **Add User** to navigate to a user detail form. Provide all details, such as the username and access type. We use the name **cli-user**, and check the **Programmatic access** box under **Access type**. This option gives the user access to AWS development tools, such as the command line interface used later. Click on **Next: Permissions** to continue.



Screenshot of the AWS IAM Management Console showing the 'Users' page and the 'Create user' wizard.

The 'Users' page shows a table with columns: User name, Groups, Last activity, MFA, Password age, and Active key age. A message indicates "No resources to display".

The 'Create user' wizard is at Step 1: Specify user details. It includes fields for User name (prathameshpc77), a checkbox for "Provide user access to the AWS Management Console - optional", and sections for "Console password" (Custom password selected) and "Permissions options".

**Step 4 - Set the user permissions.** Click **Attach existing policies directly** and then filter the policies by keyword: IAM. For this user, select IAMFullAccess from the list of available policies.

The IAMFullAccess policy enables this user to create and manage user permissions in AWS. Later, this user will perform AWS IAM operations.

Screenshot of the 'Set permissions' step in the 'Create user' wizard.

The 'Permissions options' section shows two choices: "Add user to group" and "Attach policies directly". The "Attach policies directly" option is selected.

The "Permissions policies" section shows a table with a single row for "iamfullaccess". The table has columns: Policy name, Type, Attached entities, and Attached groups.



**Step 5 - Finish the user setup.** We will skip the tags section of user creation and go to the review page. Check details of the username, AWS access type & permissions. Then, click **Create user**.

The screenshot shows the 'Review and create' step of the user creation process. On the left, a sidebar lists steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main area displays 'User details' and 'Permissions summary'. Under 'User details', the 'User name' is 'prathameshpc77', 'Console password type' is 'Custom password', and 'Require password reset' is set to 'Yes'. The 'Permissions summary' table shows two policies: 'IAMFullAccess' (AWS managed, Permissions policy) and 'IAMUserChangePassword' (AWS managed, Permissions policy). Below this, a 'Tags - optional' section indicates 'No tags associated with the resource' and provides an 'Add new tag' button. At the bottom right are 'Cancel', 'Previous', and 'Create user' buttons.

**Step 6** - At this point, the user cli-user exists, with the chosen policies applied to the account. AWS provides this user an access key ID and secret access key. Download or copy these keys to a secure place to use later.

The screenshot shows the 'Retrieve password' step. A green success message at the top states 'User created successfully'. The main area displays 'Console sign-in details' for the user 'prathameshpc77', including the sign-in URL 'https://404055596869.siginin.aws.amazon.com/console' and a redacted console password. Buttons for 'Download .csv file' and 'Return to users list' are at the bottom right.

The screenshot shows the 'Users' page. A green success message at the top states 'User created successfully'. The main area displays a table of users with one entry: 'prathameshpc77'. The table includes columns for User name, Groups, Last activity, MFA, Password age, and Active key age. Buttons for 'View user', 'Delete', and 'Add users' are at the top right.



## Set up AWS user credentials in the CLI

With minimal setup, AWS CLI enables an admin to use their favorite shell or CLI to interact with AWS services. You can choose any Linux distribution or shell. This demonstrates a Bash shell running on an Ubuntu Linux distribution.

**1. Install the command line tool.** First, install AWS CLI on your system using the following command in Bash terminal : **sudo apt install awscli**

```
Activities Terminal Mar 16 10:54 AM computer@computer-ThinkCentre:~
```

```
[base] computer@computer-ThinkCentre:~$ sudo apt install awscli
[sudo] password for computer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libevent-core-2.1-7
  libevent-pthreads-2.1-7 libflashrom1 libfdt1-2
  libgstreamer-plugins-bad1.0-0 libjs-highlight.js libl LLVM13 libl LLVM13:i386
  libmecab2 mecab-ipadic mecab-ipadic-utf8 mecab-utils
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  docutils-common groff gsfonts imagemagick imagemagick-6-common
  imagemagick-6.q16 libjxr-tools libjxr0 liblqr-1-0 libmagickcore-6.q16-6
  libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libnetpbm10 netpbm psutils
  python3-botocore python3-docutils python3-jmespath python3-pyasn1
  python3-pygments python3-roman python3-rsa python3-s3transfer
Suggested packages:
  imagemagick-doc autotrace curl enscript ffmpeg gnuplot grads hp2xx html2ps
  libwmf-bin mplayer povray radiance transfig ufraw-batch inkscape
  docutils-doc fonts-linuxlibertine | ttf-linux-libertine texlive-lang-french
  python-pygments-doc ttf-bitstream-vera
The following NEW packages will be installed:
  awscli docutils-common groff gsfonts imagemagick imagemagick-6-common
  imagemagick-6.q16 libjxr-tools libjxr0 liblqr-1-0 libmagickcore-6.q16-6
  libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libnetpbm10 netpbm psutils
  python3-botocore python3-docutils python3-jmespath python3-pyasn1
  python3-pygments python3-roman python3-rsa python3-s3transfer
0 upgraded, 24 newly installed, 0 to remove and 8 not upgraded.
Need to get 18.1 MB of archives.
After this operation, 114 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 liblqr-1-0 amd64 0.4.2-2.1 [27.7 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 imagemagick-6-common all 8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1 [64.5 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libmagickcore-6.q16-6 amd64 8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1 [1,789 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libmagickwand-6.q16-6 amd64 8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1 [328 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy/universe amd64 groff amd64 1.22.4-8build1 [4,104 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy/main amd64 python3-jmespath all 0.10.0-1 [21.7 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy/universe amd64 python3-botocore all 1.23.34+repack-1 [4,508 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy/main amd64 python3-pyasn1 all 0.4.8-1 [50.9 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy/main amd64 docutils-common all 0.17.1+dfsg-2 [117 kB]

Setting up libmagickcore-6.q16-6-extra:amd64 (8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1) ...
Setting up imagemagick-6.q16 (8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1) ...
update-alternatives: using /usr/bin/compare-im6.q16 to provide /usr/bin/compare (compare) in auto mode
update-alternatives: using /usr/bin/compare-im6.q16 to provide /usr/bin/compare-im6 (compare-im6) in auto mode
update-alternatives: using /usr/bin/animate-im6.q16 to provide /usr/bin/animate (animate) in auto mode
update-alternatives: using /usr/bin/animate-im6.q16 to provide /usr/bin/animate-im6 (animate-im6) in auto mode
update-alternatives: using /usr/bin/convert-im6.q16 to provide /usr/bin/convert (convert) in auto mode
update-alternatives: using /usr/bin/convert-im6.q16 to provide /usr/bin/convert-im6 (convert-im6) in auto mode
update-alternatives: using /usr/bin/composite-im6.q16 to provide /usr/bin/composite (composite) in auto mode
update-alternatives: using /usr/bin/composite-im6.q16 to provide /usr/bin/composite-im6 (composite-im6) in auto mode
update-alternatives: using /usr/bin/conjure-im6.q16 to provide /usr/bin/conjure (conjure) in auto mode
update-alternatives: using /usr/bin/conjure-im6.q16 to provide /usr/bin/conjure-im6 (conjure-im6) in auto mode
update-alternatives: using /usr/bin/import-im6.q16 to provide /usr/bin/import (import) in auto mode
update-alternatives: using /usr/bin/import-im6.q16 to provide /usr/bin/import-im6 (import-im6) in auto mode
update-alternatives: using /usr/bin/identify-im6.q16 to provide /usr/bin/identify (identify) in auto mode
update-alternatives: using /usr/bin/identify-im6.q16 to provide /usr/bin/identify-im6 (identify-im6) in auto mode
update-alternatives: using /usr/bin/stream-im6.q16 to provide /usr/bin/stream (stream) in auto mode
update-alternatives: using /usr/bin/stream-im6.q16 to provide /usr/bin/stream-im6 (stream-im6) in auto mode
update-alternatives: using /usr/bin/display-im6.q16 to provide /usr/bin/display (display) in auto mode
update-alternatives: using /usr/bin/display-im6.q16 to provide /usr/bin/display-im6 (display-im6) in auto mode
update-alternatives: using /usr/bin/montage-im6.q16 to provide /usr/bin/montage (montage) in auto mode
update-alternatives: using /usr/bin/montage-im6.q16 to provide /usr/bin/montage-im6 (montage-im6) in auto mode
update-alternatives: using /usr/bin/mogrify-im6.q16 to provide /usr/bin/mogrify (mogrify) in auto mode
update-alternatives: using /usr/bin/mogrify-im6.q16 to provide /usr/bin/mogrify-im6 (mogrify-im6) in auto mode
Setting up imagemagick (8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for shared-mime-info (2.1-2) ...
Processing triggers for sgml-base (1.30) ...
Setting up python3-docutils (0.17.1+dfsg-2) ...
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
Processing triggers for fontconfig (2.13.1-4.2ubuntu5) ...
Processing triggers for desktop-file-utils (0.26-1ubuntu3) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu3) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Setting up awscli (1.22.34-1) ...
```



Once the setup runs, verify the installation by checking the version : **aws –version**

```
(base) computer@computer-ThinkCentre:~$ aws --version
aws-cli/1.22.34 Python/3.10.6 Linux/5.19.0-35-generic botocore/1.23.34
(base) computer@computer-ThinkCentre:~$
```

**2. Configure the user with the keys.** Run the **aws configure** command in the shell to quickly set up the access key ID & secret access key obtained from AWS when you created a new user in IAM console.

```
(base) computer@computer-ThinkCentre:~$ 
(base) computer@computer-ThinkCentre:~$ aws configure
AWS Access Key ID [None]: AKIAJAXWRV!
AWS Secret Access Key [None]: prathameshpc77
Default region name [ap-south-1]:
Default output format [json]: json
(base) computer@computer-ThinkCentre:~$ 
This step saves your credentials in a local file at path: ~/.aws/credentials and region and output format
configs at path: ~/.aws/config file.

Now that cli-user with programmatic access is set up, we can use that account to create other users and
give them policy-based access through AWS CLI. The next two sections walk through these steps.
```

#### Create a user and assign permissions

To create a user using IAM, run the **aws iam create-user** command in AWS CLI with a username:

```
aws iam create-user --user-name prathameshpc77
```

It creates a new user and shows the user details in the bash console.

```
(base) computer@computer-ThinkCentre:~$ aws iam create-user --user-name prathameshpc77
{
  "User": {
    "Path": "/",
    "UserName": "prathameshpc77",
    "UserId": "AIDAXWRVBDHII7PCK47BG",
    "Arn": "arn:aws:iam::529465940434:user/prathameshpc77",
    "CreateDate": "2021-06-21T16:33:28Z"
  }
}
(base) computer@computer-ThinkCentre:~$
```

Suppose this user needs to manage EC2 services. To grant this new user EC2 admin rights, start by listing which EC2 policies we can grant. Use the command:

```
aws iam list-policies | grep EC2FullAccess
```

Identify the appropriate policy for the user's access level. In this case, it is **AmazonEC2FullAccess**. Pass the Amazon Resource Name (ARN) to the following command in **--policy-arn** parameter:

```
aws iam attach-user-policy --user-name prathameshpc77 --policy-arn
"arn:aws:iam::aws:policy/AmazonEC2FullAccess"
```

```
(base) computer@computer-ThinkCentre:~$ 
(base) computer@computer-ThinkCentre:~$ aws iam list-policies | grep EC2FullAccess
{
  "PolicyName": "Amazon EC2FullAccess",
  "Arn": "arn:aws:iam::aws:policy/Amazon EC2FullAccess"
}
(base) computer@computer-ThinkCentre:~$ 
(base) computer@computer-ThinkCentre:~$ aws iam attach-user-policy --user-name prathameshpc77 --policy-arn
"arn:aws:iam::aws:policy/Amazon EC2FullAccess"
(base) computer@computer-ThinkCentre:~$
```

#### Check user details and list user permissions

Once you create the user and attach the appropriate user policy to them, verify that AWS assigned the appropriate policy by checking the user details.

To check the list of IAM users, run: **aws iam list-users**

The following command tells AWS to list all attached policies for a user account:

```
aws iam list-attached-user-policies --user-name prathameshpc77
```



```
(base) computer@computer-ThinkCentre:~$ ~
(base) computer@computer-ThinkCentre:~$ 
(base) computer@computer-ThinkCentre:~$ aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "cli-user",
      "UserId": "AIDAXWRVBDHJDOWXYJSI3",
      "Arn": "arn:aws:iam::529465940434:user/cli-user",
      "CreateDate": "2021-06-21T15:48:20Z"
    },
    {
      "Path": "/",
      "UserName": "prathameshpc77",
      "UserId": "AIDAXWRVBDHJ17PCK47BG",
      "Arn": "arn:aws:iam::529465940434:user/prathameshpc77", "CreateDate": "2021-06-21T16:33:28Z"
    }
  ]
}
(base) computer@computer-ThinkCentre:~$ aws iam list-attached-user-policies
--user-name prathameshpc77
"AttachedPolicies": [
{
  "PolicyName": "Amazon EC2FullAccess",
  "PolicyArn": "arn:aws:iam::aws:policy/Amazon EC2FullAccess"
}
]
(base) computer@computer-ThinkCentre:~$
```

- Now you can **delete** your users from **IAM - Access Management > Users** > select your username > click on **Delete**

The screenshot shows the AWS IAM service interface. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'Users' is also selected. The main content area is titled 'Users (Selected 1/1) Info'. It shows a table with one row for 'prathameshpc77'. The table columns include 'User name' (with a checkbox checked), 'Groups' (empty), 'Last activity' (Never), 'MFA' (None), 'Password age' (43 minutes ago), and 'Active key age' (empty). At the top right of the table are buttons for 'Delete' and 'Add users'.

- You can see the users you created deleted successfully.

This screenshot shows the same AWS IAM interface after the user 'prathameshpc77' has been deleted. The 'Users (0) Info' section now displays 'No resources to display'. The rest of the interface remains the same, with the 'Users' option still selected in the sidebar.



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML  
Academic Year: 2022-23**

<b>NAME</b>	<b>PRATHAMESH CHIKANKAR</b>
<b>BRANCH</b>	<b>CSE-(AI&amp;ML)</b>
<b>ROLL NO.</b>	<b>11</b>
<b>SUBJECT</b>	<b>CLOUD COMPUTING LAB</b>
<b>COURSE CODE</b>	<b>CSL605</b>
<b>PRACTICAL NO.</b>	<b>07</b>
<b>DOP</b>	<b>23/03/2023</b>
<b>DOS</b>	



## DOCKER

**Step 1 - Go to official website of docker : <https://hub.docker.com/>**

The screenshot shows the Docker Hub homepage. At the top, there's a navigation bar with links for Products, Developers, Pricing, Blog, About Us, and Partners. On the right, there are 'Sign In' and 'Get Started' buttons. The main header features the Docker+WASM logo and the text 'Play with Docker' followed by 'Hands-on Docker Tutorials for Developers'. To the right is a cartoon illustration of a blue whale-like character interacting with a computer monitor displaying a binary whale. Below this, a large call-to-action button says 'Don't let app complexity get in the way of opportunity'. Underneath it, a sub-headline reads 'Learn Docker today and join the millions of developers who use Docker Desktop and Docker Hub to simplify building and sharing world-changing apps'. At the bottom of the page, there's a cookie consent banner and a notification bar about Docker Desktop.

**Step 2 - Create your docker account**

**Step 3 - Choose for personal use with \$0 and click on Continue with Free**

This screenshot shows two side-by-side pages. On the left is the 'Create a Docker Account' form, which includes fields for Username (prathameshpc77), Email (prathu332@gmail.com), Password, and a reCAPTCHA checkbox. It also has terms and conditions checkboxes for product updates and the Subscription Service Agreement. On the right is the 'Choose a Plan' page, which displays four pricing options: Personal (\$0), Pro (\$5/month), Team (\$9/month), and Business (\$24/month). The Personal plan is described as ideal for individual developers and small businesses, while the Pro plan adds Docker Engine + Kubernetes. The Team plan adds unlimited teams and concurrent builds, and the Business plan adds centralized management and security features like audit logs. Each plan has a 'Buy Now' button.

**Step 4 - You have to verify your account from your added gmail account through mail**

This screenshot shows a browser window with multiple tabs open. The active tab is 'hub.docker.com/verify-email'. The Docker Hub navigation bar is visible at the top. The main content area shows a success message: 'Your email has been verified!'. This indicates that the account verification process has been completed.



## Step 5 - Creating first repository

Click on **Create a Repository**

Welcome to Docker  
Download the desktop application  
Download for Windows  
Also available for Mac and Linux

**Create a Repository**  
Push container images to a repository on Docker Hub.

**Docker Hub Basics**  
Watch the guide on how to create and push your first image into a Docker Hub repository.

**Language-Specific Guides**  
Learn how to containerize language-specific applications using Docker.

Access the world's largest library of container images

nginx, mongoDB, alpine, node, redis, busybox, ubuntu, python, postgres, httpd

Name it <your-username>/prathamesh  
Set the visibility to private

Wasm is a fast, light alternative to Linux containers – try it out today with the Docker+Wasm Beta.

**Create repository**

prathameshpc77 prathamesh

**Visibility**

Using 0 of 1 private repositories. [Get more](#)

Public Appears in Docker Hub search results

Private Only visible to you

**Pro tip**  
You can push a new image to this repository using the CLI  
`docker tag local-image:tagname new-repo:tagname  
docker push new-repo:tagname`

Make sure to change `tagname` with your desired image repository tag.

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

Click on **Create**

prathameshpc77 / prathamesh

Description

Last pushed: 23 minutes ago



Now next,

## Step 6 - Click on Explore tab to see official and publisher images

The screenshot shows the Docker Explore tab with a list of 10,000 available results. The results are displayed in a grid format, each row containing an image icon, the image name, its status (e.g., DOCKER OFFICIAL IMAGE), size, rating, and last update. To the right of each row is a pull count chart for the previous week and a 'Learn more' link.

Image Name	Status	Last Update	Size	Rating	Pulls (Last Week)
alpine	DOCKER OFFICIAL IMAGE	Updated 10 days ago	1B+	9.8K	9,268,526
nginx	DOCKER OFFICIAL IMAGE	Updated 9 days ago	1B+	10K+	32,868,043
busybox	DOCKER OFFICIAL IMAGE	Updated 6 days ago	1B+	2.9K	12,698,125
ubuntu	DOCKER OFFICIAL IMAGE	Updated 7 days ago	1B+	10K+	25,915,974

Here you can click on the docker tab

The screenshot shows the Docker tab with a list of various Docker images from publishers. Each row contains the publisher logo, image name, status, last update, size, rating, and a brief description. To the right of each row is a pull count chart for the previous week and a 'Learn more' link.

Publisher	Image Name	Status	Last Update	Size	Rating	Pulls (Last Week)
traefik	traefik	DOCKER OFFICIAL IMAGE	Updated 5 hours ago	1B+	5.3K	1,222,191
mariadb	mariadb	DOCKER OFFICIAL IMAGE	Updated 6 days ago	1B+	5.3K	5,158,020
rabbitmq	rabbitmq	DOCKER OFFICIAL IMAGE	Updated a day ago	1B+	4.7K	4,007,808
hello-world	hello-world	DOCKER OFFICIAL IMAGE	Updated 7 days ago	1B+	2.0K	1,607,377
OpenJDK	openjdk	DOCKER OFFICIAL IMAGE	Updated 5 hours ago	1B+	3.6K	5,005,679

You can explore that tab in which various versions of docker's downloads are given.

You can select various platforms, architecture and operating systems



## Installing using apt repository on ubuntu

Before you install Docker Engine for the first time on a new host machine, you need to set up the Docker repository. Afterward, you can install and update Docker from the repository.

### **Set up the repository**

**Step 1** - Update the apt package index and install packages to allow apt to use a repository over HTTPS:

```
sudo apt-get update  
sudo apt-get install \  
    ca-certificates \  
    curl \  
    gnupg
```

**Step 2** - Add Docker's official GPG key:

```
sudo mkdir -m 0755 -p /etc/apt/keyrings  
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o  
/etc/apt/keyrings/docker.gpg
```

**Step 3** - Use the following command to set up the repository:

```
echo \  
"deb [arch="$(dpkg --print-architecture)" signed-by=/etc/apt/keyrings/docker.gpg]  
https://download.docker.com/linux/ubuntu \  
"$(. /etc/os-release && echo "$VERSION_CODENAME")" stable" | \  
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Use 'sudo apt autoremove' to remove them.



## Installing Docker Engine

### **Step 1 - Update the apt package index : `sudo apt-get update`**

Receiving a GPG error when running apt-get update?

Your default umask may be incorrectly configured, preventing detection of the repository public key file. Try granting read permission for the Docker public key file before updating the package index : `sudo chmod a+r /etc/apt/keyrings/docker.gpg`

`sudo apt-get update`

### **Step 2 - Install Docker Engine, containerd, and Docker Compose.**

`sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin`

```
(base) computer@computer-ThinkCentre:~$ sudo apt-get update
Get:1 https://download.docker.com/linux/ubuntu jammy InRelease [48.9 kB]
Get:2 https://download.docker.com/linux/ubuntu jammy/stable amd64 Packages [13.6 kB]
Hit:3 https://deb.nodesource.com/node_16.x jammy InRelease
Hit:4 https://dl.google.com/linux/chrome/deb stable InRelease
Hit:5 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:7 https://ppa.launchpadcontent.net/gns3/ppa/ubuntu jammy InRelease
Get:8 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 398 kB in 4s (106 kB/s)
Reading package lists... Done
(base) computer@computer-ThinkCentre:~$ sudo chmod a+r /etc/apt/keyrings/docker.gpg
sudo apt-get update
Hit:1 https://download.docker.com/linux/ubuntu jammy InRelease
Hit:2 https://deb.nodesource.com/node_16.x jammy InRelease
Hit:3 https://dl.google.com/linux/chrome/deb stable InRelease
Hit:4 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:5 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:6 https://ppa.launchpadcontent.net/gns3/ppa/ubuntu jammy InRelease
Get:7 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 336 kB in 2s (217 kB/s)
Reading package lists... Done
(base) computer@computer-ThinkCentre:~$ sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
```

### **Step 3 - Verify that the Docker Engine installation is successful by running the hello-world image : `sudo docker run hello-world`**

### **Step 4 - Check docker version to ensure that its installed successfully : `docker -v`**

```
(base) computer@computer-ThinkCentre:~$ sudo docker run hello-world
Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/

(base) computer@computer-ThinkCentre:~$ docker -v
Docker version 23.0.1, build a5ee5b1
(base) computer@computer-ThinkCentre:~$
```



## Creating containerised docker

**Step 1 - Cloning : `git clone https://github.com/docker/Cloning` into 'getting-started'...**

**Step 2 - Open code : `code ./getting-started/app/`**

```
(base) computer@computer-ThinkCentre:~/Documents/AIML/CCL$ git clone https://github.com/docker/getting-started.git
Cloning into 'getting-started'...
remote: Enumerating objects: 957, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 957 (delta 0), reused 1 (delta 0), pack-reused 952
Receiving objects: 100% (957/957), 5.24 MiB | 21.05 MiB/s, done.
Resolving deltas: 100% (541/541), done.
(base) computer@computer-ThinkCentre:~/Documents/AIML/CCL$ code ./getting-started/app/
(base) computer@computer-ThinkCentre:~/Documents/AIML/CCL$
```

**Step 3 - Create file : Dockerfile and locate localhost, then enter :**

**`sudo docker build -t getting-started .`**

Type required password of your system

The screenshot shows the Visual Studio Code interface. In the Explorer sidebar, there is a project named 'APP' containing 'spec', 'src', 'Dockerfile', 'package.json', and 'yarn.lock'. The 'Dockerfile' tab is selected, displaying the following content:

```
1 # syntax=docker/dockerfile:1
2
3 FROM node:18-alpine
4 WORKDIR /app
5 COPY .
6 RUN yarn install --production
7 CMD ["node", "src/index.js"]
8 EXPOSE 3000
```

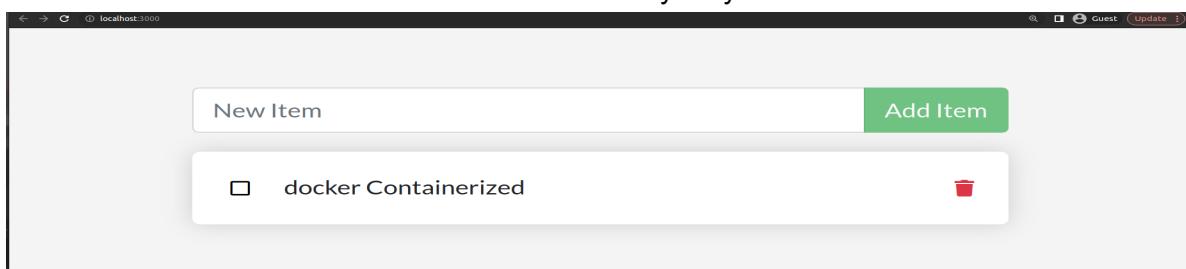
In the Terminal tab, the command `sudo docker build -t getting-started .` is being run. The terminal output shows:

```
● computer@computer-ThinkCentre:~/Documents/AIML/CCL/getting-started/app$ touch Dockerfile
● computer@computer-ThinkCentre:~/Documents/AIML/CCL/getting-started/app$ docker build -t getting-started .
ERROR: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/_ping": dial unix /var/run/docker.sock: connect: permission denied
● computer@computer-ThinkCentre:~/Documents/AIML/CCL/getting-started/app$ sudo docker build -t getting-started .
[sudo] password for computer:
Sorry, try again.
[sudo] password for computer:
[+] Building 19.5s (11/11) FINISHED
= [internal] load build definition from Dockerfile
= => transferring dockerfile: 184B
0.0s
```

**Step 4 - Getting-started : `sudo docker run -dp 3000:3000 getting-started`**

```
● computer@computer-ThinkCentre:~/Documents/AIML/CCL/getting-started/app$ sudo docker run -dp 3000:3000
00 ge+-----+
33762
● computer@computer-ThinkCentre:~/Documents/AIML/CCL/getting-started/app$
```

You can see that containerized docker created successfully on your localhost

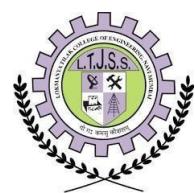




**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML  
Academic Year: 2022-23**

<b>NAME</b>	<b>PRATHAMESH CHIKANKAR</b>
<b>BRANCH</b>	<b>CSE-(AI&amp;ML)</b>
<b>ROLL NO.</b>	<b>11</b>
<b>SUBJECT</b>	<b>CLOUD COMPUTING LAB</b>
<b>COURSE CODE</b>	<b>CSL605</b>
<b>PRACTICAL NO.</b>	<b>08</b>
<b>DOP</b>	<b>06/04/2023</b>
<b>DOS</b>	



## KUBERNETES

**Aim : To study container orchestration using Kubernetes**

### Theory :

Kubernetes (also known as "K8s") is an open-source container orchestration tool that helps manage and automate the deployment, scaling, and management of containerized applications. Kubernetes was originally developed by Google, and is now maintained by the Cloud Native Computing Foundation (CNCF).

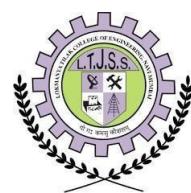
At a high level, Kubernetes works by managing a cluster of nodes (physical or virtual machines) that run containerized applications. A Kubernetes cluster consists of one or more master nodes, which control the cluster and make decisions about scheduling and scaling containers, and one or more worker nodes, which actually run the containers.

### **Benefits of Kubernetes**

Kubernetes is a powerful container orchestration tool that offers a number of benefits to organizations deploying containerized applications:

- Scalability: Kubernetes enables automatic scaling of containers to meet the changing demands of an application. It can automatically add or remove containers based on metrics like CPU and memory utilization.
- High availability: Kubernetes provides a highly available infrastructure for containerized applications by automatically restarting containers that fail, and distributing containers across multiple nodes in a cluster.
- Portability: Kubernetes enables easy deployment of containerized applications across different environments, including on-premises data centers, public clouds, and hybrid environments.
- Resource efficiency: Kubernetes helps optimize the use of computing resources by packing containers efficiently onto nodes in the cluster, and dynamically allocating resources as needed.
- Simplified management: Kubernetes provides a declarative API for defining the desired state of an application, and automatically reconciles the actual state of the application with the desired state. This simplifies management and reduces the risk of configuration errors.
- Ecosystem support: Kubernetes has a large and growing ecosystem of tools and add-ons, such as Helm charts and Operators, which help automate the deployment and management of complex applications on Kubernetes.

Overall, Kubernetes provides a powerful platform for managing containerized applications, with features that help simplify management, improve scalability and availability, and optimize resource utilization.



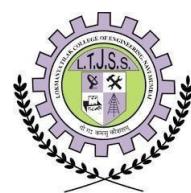
Kubernetes is a powerful tool for managing containerized applications, with a rich set of features that help automate the deployment, scaling, and management of applications at scale. While Kubernetes can be complex to set up and manage, it has become a de facto standard for container orchestration in the cloud-native ecosystem, and is widely used by organizations of all sizes.

Official website : <https://kubernetes.io/>

The screenshot shows a browser window with multiple tabs open, including "11\_CCL\_EXP8 - Google Docs", "11\_CCL\_EXP8-kubernetes", "What Is Kubernetes? | Go", "kubernetes documentation", "Learn Kubernetes with M", and "Kubernetes". The main content area is a red banner with the Kubernetes logo and the text: "Legacy k8s.gcr.io container image registry is being redirected to registry.k8s.io. k8s.gcr.io image registry is gradually being redirected to registry.k8s.io (since Monday March 20th). All images available in k8s.gcr.io are available at registry.k8s.io. Please read our announcement for more details." Below the banner, there is a section about Kubernetes, a diagram showing containers grouped into pods which are managed by a controller and run on a node, and sections for "Planet Scale" and "Never Outgrow" with their respective icons and descriptions.

For installation in ubuntu visit : <https://ubuntu.com/kubernetes/install#download>

The screenshot shows the Ubuntu website's "Download" section. It features four main categories: "Ubuntu Desktop", "Ubuntu Server", "Ubuntu for IoT", and "Ubuntu Cloud". Under "Ubuntu Server", there is a "Get Ubuntu Server" button and links for "Mac and Windows", "ARM", "IBM Power", and "s390x". Under "Ubuntu for IoT", there are links for "Raspberry Pi", "Intel IoT platforms", "Intel NUC", "KVM", "Qualcomm Dragonboard 410c", "Intel IEI TANK 870", "AMD-Xilinx Evaluation kits & SOMs", and "RISC-V platforms". The "Ubuntu Cloud" section links to "Get started on Amazon AWS, Microsoft Azure, Google Cloud Platform and more..." and "Download cloud images for local development and testing".



Here are some steps you can take to get started:

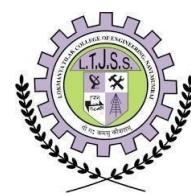
- Learn the basics of containers: Before diving into Kubernetes, it's important to understand the basics of containers. You can start by reading about Docker, which is one of the most popular containerization tools.
- Set up a Kubernetes cluster: You can set up a Kubernetes cluster locally using tools like Minikube or Kind, or you can use a cloud provider like Google Cloud, Amazon Web Services, or Microsoft Azure to create a Kubernetes cluster.
- Learn the Kubernetes architecture: Kubernetes has a complex architecture, so it's important to understand how all the components fit together. The Kubernetes documentation is a good place to start.
- Practice deploying applications: Once you have a Kubernetes cluster set up, you can practice deploying applications using Kubernetes. Start with a simple application and gradually work your way up to more complex deployments.
- Learn about Kubernetes networking: Kubernetes has its own networking model, so it's important to understand how it works. You can start by reading about Kubernetes Services and Ingress.
- Learn about Kubernetes storage: Kubernetes also has its own storage model, so it's important to understand how to manage storage for your applications. You can start by reading about Kubernetes Volumes.
- Explore Kubernetes ecosystem: Kubernetes has a large ecosystem of tools and add-ons that can help you manage and extend your cluster. Some popular tools include Helm, Prometheus, and Istio.

Overall, learning Kubernetes takes time and practice, but it can be a very rewarding skill to have in today's world of cloud-native applications.

Container orchestration using Kubernetes involves managing a cluster of nodes (physical or virtual machines) that run containerized applications using Kubernetes.

Kubernetes is a popular open-source container orchestration tool that has become a de facto standard for managing containerized applications in cloud computing environments. Kubernetes provides a powerful platform for automating the deployment, scaling, and management of containerized applications, and can be used with a wide range of cloud computing services and platforms.

In cloud computing environments, Kubernetes can be used to manage containerized applications deployed on a range of cloud platforms, including public clouds like Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure, as well as private clouds and hybrid clouds. Kubernetes can also be used to manage containers on on-premises data centers.



## **Applications**

Kubernetes provides a number of key features that help automate the management of containerized applications:

- Container orchestration: Kubernetes can manage containers at scale, orchestrating the deployment, scaling, and management of containerized applications across multiple nodes in a cluster.
- Service discovery and load balancing: Kubernetes provides a built-in service discovery and load balancing mechanism, enabling containers to find and communicate with other containers in the same application.
- Automatic scaling: Kubernetes can automatically scale containers based on metrics like CPU and memory usage, enabling applications to handle traffic spikes and sudden increases in demand.
- Self-healing: Kubernetes can automatically restart containers that fail, and can detect and replace nodes that become unavailable.
- Rollouts and rollbacks: Kubernetes enables controlled rollouts and rollbacks of containerized applications, allowing organizations to test new versions of applications before deploying them to production.
- Configuration management: Kubernetes provides a declarative API for defining the desired state of an application, and can automatically reconcile the actual state of the application with the desired state. This helps simplify configuration management and reduces the risk of configuration errors.

**Conclusion : We had successfully studied container orchestration using Kubernetes**



Name :- Prathamesh J. Charkar

Roll No. :- AIML11 Branch :- CSE - (AIML)

Year :- TE Subject :- Cloud Computing Lab  
(CCL)

Topic :- Assignment No. 01

Sign :- Prathmesh Date :- February '23



Q.1. What is the difference between hosted and Bare metal Hypervisors with suitable parameters along with their use in public / private cloud platform.

Ans:- A hypervisor, also known as virtual machine monitor, is a software program that allows multiple virtual machines (VMs) to run on a single physical machine. There are two main types of hypervisors: hosted hypervisors and bare metal hypervisors.

- Hosted Hypervisor: Also known as Type 2 hypervisors, are installed on top of a host operating system. They rely on the host OS to access hardware.
- Bare metal hypervisor: Also known as Type 1 hypervisors, run directly on the host machine's hardware. Not require underlying OS.

<u>Hosted Hypervisor</u>	<u>Bare metal Hypervisors</u>
- Also known as Type 2 Hypervisors	Also known as Type 1 hypervisors
- Installed on top of host OS operating system	Installed directly on host machine's hardware.
- Rely on the Host OS to access the underlying hardware & to manage hardware resources	Don't require any underlying operating system and have direct access to the hardware.
- Hosted Hypervisors are commonly used for desktop virtualization, testing and development.	Bare metal Hypervisors provide higher performance & security than hosted hypervisors.
- Examples of hosted hypervisor are, VMware Workstation, VirtualBox & parallels Desktop.	Examples of Bare metal Hypervisors are VMWare, ESXi, MS Hyper-V, and Citrix Hypervisor.

- Suitable parameters for Hosted Hypervisors:
- Resource overhead: Rely on the host OS to access hardware resources. This can reduce the performance of both host OS & virtual machines.

- Isolation: Hosted hypervisors provide control of isolation b/w the host OS and virtual machines, but not strong as Bare metal hypervisors.
- Security: Hosted hypervisors may be less secure than bare metal, as they share resources with host OS, which may increase attack surface for Bare metal Hypervisors!
- Resource Allocation: more granular control over hardware resources & offer better performance than hosted hypervisors.
- Isolation: stronger isolation b/w virtual machine and underlying HW, improving security of virtual environments.
- Security: provide higher level of security, as they have a smaller attack surface & can be hardened more easily than hosted one.

### ⇒ Use in public / private cloud platform:

Hypervisors: Hosted hypervisors can be used in private cloud environments, where they are typically used for small-scale app dev or for development and testing. In public cloud environments, hosted hypervisors may be used for virtual desktops or other similar use cases.

Bare metal Hypervisors: commonly used in public and private cloud environments for running multiple virtual machines on a single physical server. They offer higher performance & security making them suitable for running mission-critical workloads in cloud environment.

2. explore and compare the similar types of services provided by AWS and Azure [Any ten services]

AWS (Amazon Web Services) and Azure (Microsoft Azure) are two of the most popular cloud computing platforms. They both offer

a wide range of services that enables customers to build and run applications in the cloud. Here are ten services that are provided by both AWS and Azure:

- **① Compute Services:** Both AWS and Azure offer compute services that enable customers to provision and manage virtual machines (VMs) in the cloud. AWS provides EC2, while Azure offers VMs.
- **② Storage Services:** Both AWS and Azure provide a variety of storage services, including object storage, block storage & file storage. AWS offers S3 and EBS while Azure provides Blob storage & managed disk.
- **③ Database Services:** AWS and Azure both offer a range of database services, including relational and non-relational databases. AWS provides services such as RDS and DynamoDB, while Azure offers SQL DB.
- **④ Networking Services:** Both AWS and Azure provide networking services that enables customers to connect and manage virtual networks, load balancers and firewalls. AWS provides services such as VPC & ELB, while Azure offers like services virtually NVA & Load Balancer.
- **⑤ Content Delivery Network (CDN):** Both AWS and Azure offer a CDN service that helps customers deliver their content to end-users faster. AWS provides Amazon CloudFront, while Azure offers Azure CDN.
- **⑥ Identity and Access Management (IAM):** Both AWS and Azure offer IAM services that enable customers to manage user access & permissions to their resources. AWS provides services such as IAM & Cognito, while Azure offers Azure Directory & Role-Based Access Control.
- **⑦ Container Services:** Both AWS and Azure offer container services that enable customers to deploy & manage containerized applications. AWS provides ECS and EKS, while Azure offers Azure Container Instances and the AKS (Azure Kubernetes Service). container services.
- **⑧ Serverless Computing:** Both AWS and Azure offer container services serverless computing services that allow customers to run application



without managing servers. AWS provides Lambda while Azure Functions.

- **④ Analytics services:** Both AWS and Azure offer a range of analytics services including data warehousing, big data processing, and business intelligence. AWS provides services such as Redshift & EMR, while Azure offers services like Azure SQL Data warehouse & HDInsight.
- **⑤ Internet of things (IoT):** Services both AWS & Azure provide IoT services that enable customers to connect and manage IoT devices & data. AWS provides IoT Core, while Azure offers IoT Hub.  
⇒ In summary, while AWS and Azure offer similar types of services, there may be differences in their implementation, pricing, and features. Customers should evaluate their specific requirements and compare the offerings of each provider before choosing a cloud platform.

3. Explain in detail different service models in cloud computing :-
- Cloud computing is a model for developing on-demand computing services over the internet. There are three main service models in cloud computing : Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each of these models provides different levels of abstraction and flexibility for the customers.
  - **Infrastructure as a Service (IaaS) :** IaaS provides customers with access to virtualized computing resources, including servers, storage and networking. Customers can use these resources to build, deploy and manage their own applications & infrastructure. With IaaS, customers have full control over the underlying infrastructure, and they are responsible for managing and maintaining the OS, application & data. Some examples of IaaS providers include AWS EC2, Microsoft Azure VM and Google Compute Engine.



- platform as a service (PaaS): PaaS provides a higher level of abstraction than IaaS by providing customers with a pre-configured platform on which they can build and deploy their web applications. PaaS providers handle the underlying infrastructure, including the OS, runtime environment and middleware, while customers are responsible for managing their application and data. PaaS can be more cost-effective & faster to deploy than IaaS, but it may have less flexibility in terms of customization. Examples of PaaS providers include AWS Elastic Beanstalk, Amazon App Services & Google App Engine.

- software as a service (SaaS): SaaS provides customers with access to a complete software application that is hosted in the cloud & delivered over the internet. Customers can use the application without having to manage the underlying infrastructure, SW or data. SaaS providers handle all aspects of the SW, including maintenance, upgrade and security. SaaS can be more convenient & cost-effective than on-premises SW, but it may have less flexibility in terms of customization. Examples of SaaS providers include Salesforce, Microsoft Office 365, and Google Workspace.

\* In addition to these main service models, there are also hybrid & multi-cloud models, which combine different cloud service models or multiple cloud providers. A hybrid cloud model may combine private and public cloud resources, while a multi-cloud model may use different cloud providers for different applications or services.

⇒ In summary, each cloud service model provides a different level of abstraction & flexibility for customers, and customers should choose the model that best meets their specific requirements for managing their application, infrastructure and the data.



Name :- Prathamesh S. Chikankar

ROLL NO. :- AIML11 BRANCH:- ESE - (AI & ML)

YEAR:- T.E. Subject:- cloud computing lab  
(CCL)

TOPIC:- Assignment No. 02

SIGN :- Prathy Date:- March' 23



- Q.1. Distinguish between the different computing technologies (parallel, distributed, clusty; Grid, Quantum)

Ans:- parallel computing: parallel computing involves the use of multiple processors or cores to execute tasks simultaneously, thereby reducing the time required to complete a task. It is a form of computation in which multiple calculations or the execution of multiple instructions occur simultaneously.

- Distributed computing: Distributed computing involves the use of n/w of computers to work together to solve a complex problem. The workload is divided into smaller pieces, and each computer on the n/w works on a different piece of the problem. The results are then combined to produce the final output.
- Clusty computing: Clusty computing involves the use of multiple computers (called nodes) that are connected together to act as a single system. The nodes in a cluster are typically located in close proximity to each other and connected by a high-speed local area network (LAN). Clusty computing commonly used in scientific research and data analysis.
- Grid computing: Grid computing involves the use of multiple computers and resources, typically located in different geographic locations, to work together to solve a complex problem. Grid computing allows organizations to share computing resources and collaborate on large-scale projects that require significant computational power.
- Quantum computing: Quantum computing involves the use of quantum-mechanical phenomena to perform calculations. Unlike classical computers which use bits to store and process information, quantum computers use qubits.



which can exist in multiple states simultaneously. Quantum computing has the potential to solve complex problems that are beyond the capabilities of classical computers, such as cryptography and optimization.

Q. 2. What are the recent trends in cloud computing?

Explain in detail.

Ans:- Cloud computing has become an essential technology for modern business and organization due to its flexibility, scalability, cost-effectiveness.

Here are some recent trends in cloud computing:

- 1. Multi-cloud strategy: Businesses are increasingly adopting a multi-cloud strategy, which involves using multiple cloud providers for different services or workloads. This strategy enables organizations to avoid vendor lock-in and leverage the unique strengths of each cloud provider.
- 2. Hybrid cloud: Hybrid cloud is a mix of on-premises and cloud services, which allows businesses to store sensitive data on premises while leveraging the scalability and flexibility of the cloud. With the adoption of hybrid cloud, organizations can have the best of both worlds - the control and security of on-premises infrastructure and the scalability & flexibility of cloud services.
- 3. Serverless computing: Serverless computing is a cloud computing model where the cloud provider manages the infrastructure & automatically allocates resources to run the application code. This eliminates the need for businesses to manage servers and enables them to focus on developing & deploying code.
- 4. Edge computing: Edge computing is a distributed computing model that brings data storage and computation closer to source data, reducing latency and improving application performance. With the adoption of edge computing, businesses can process data in real-time, enabling them to react to user decisions.
- 5. Artificial Intelligence (AI) and machine learning (ML): Cloud providers are investing heavily in AI and ML services, making it easier for businesses to

integrate AI and ML capability into their applets, with the adoption of AI and ML, businesses can gain insights from their data, automate routine tasks and improve decision-making.

- **6. Cloud Security:** Cloud security continues to be a top concern for businesses. Cloud providers are investing in advanced security measures, such as encryption, firewalls, and identity and access management, to ensure the security & privacy of data stored in the cloud.

In summary, the recent trends in cloud computing reflects a continued focus on flexibility, scalability, and security, as well as the adoption of new technology such as AI & edge computing, to derive value & improve business outcomes.

**Q.3. How is the selection of suitable cloud platform solutions done?**

Based on requirement analysis of given problem statement.

**Ans:-** The selection of a suitable cloud platform solution is a critical decision that can have a significant impact on the success of a project. Here are some steps to follow for selecting a suitable cloud platform solution based on the requirement analysis of a given problem statement.

# **1. Identify the requirements:** The first step is to identify the specific requirements of the project. This includes determining the type of workload, data storage and processing needs, security and compliance requirements, performance requirements, and budget constraints.

# **2. Evaluate cloud platforms:** Once the requirements are identified, it is important to evaluate the various cloud platforms available in the market. This involves researching & comparing the features, pricing & performance of different cloud platforms such as Anaranda, Amazon Web Services (AWS), Microsoft Azure, and cloud platform (GCP).

# **3. Determine the fit:** Next, the cloud platforms should be assessed against the identified requirements to determine the fit. This involves evaluating the platform based on the following criteria:



- compatibility with the existing IT infrastructure.
- support for the required programming languages & frameworks.
- availability of the required services & features.
- security and compliance certifications.
- performance & security, with scalability.
- cost-effectiveness.

- # 4. Consider the support: The support offered by the cloud platform provider is an important factor to consider. The provider should have a reliable support team and offer tools for monitoring and troubleshooting issues.
- # 5. Test the platform: Before finalizing the selection, it is recommended to try the cloud platform by setting up a small-scale deployment of the application. This can help identify any compatibility or performance issues that may arise during the deployment process.
- # 6. Finalize the selection: Once the testing is complete, a final decision can be made based on the results of the evaluation. The selected cloud platform should meet the requirements of the project while also being cost-effective, reliable, and scalable.

Q.4. Is the cloud secure? How can you be sure?  
What are the top security risks of the cloud?

- Ans:- The cloud is generally secure, but as with any technology, there are risks that must be managed. It is important to understand that the cloud is not inherently more or less secure than traditional IT infrastructures.
- The security of the cloud largely depends on the specific cloud service provider and the security measures they have in place.
  - To ensure that the cloud is secure, cloud service providers typically implement a range of security measures, such as encryption, firewall, intrusion detection and prevention, identity and access management, and



Security monitoring. They also undergo regular security audits and certifications to ensure that they comply with industry security standards and regulations.

→ However, there are still security risks associated with the cloud that need to be managed, including:

- 1. Data breaches: The theft or unauthorized access to sensitive data stored in the cloud can have significant consequences for business.
- 2. Insider threats: Malicious or unintentional actions by employees or contractors with the access to cloud resources can compromise security.
- 3. Lack of control: Outsourcing IT infrastructure to the cloud can result in a loss of control over security measures, which can make it more difficult to detect and respond to security incidents.
- 4. Cloud service provider vulnerabilities: Cloud service providers can also be subject to security breaches, which can impact their customers.
- 5. Compliance: Compliance with regulatory requirements can be more challenging when using cloud services due to concerns about data protection and privacy.

→ To mitigate these risks, businesses must have a robust cloud security strategy in place, which includes implementing appropriate security measures, performing regular security assessments, and ensuring compliance with regulatory requirements. It is also essential to carefully select a cloud service provider with a proven track record to security and to regularly review and update security measures to ensure they remain effective.