

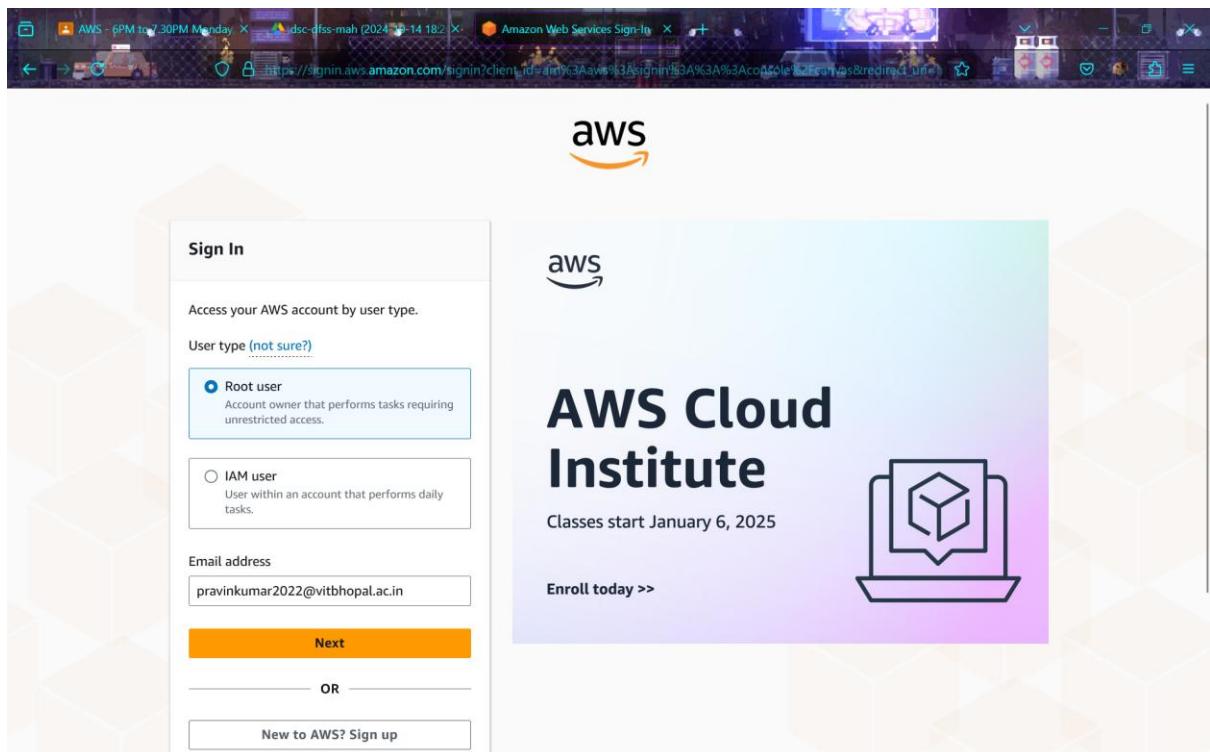
Date: 20-10-2024	Course Code: CSE3015	Reg No: 22BET10027
Day: Wednesday	Course Name: AWS Cloud Practitioner	Name: Pravin Kumar GS

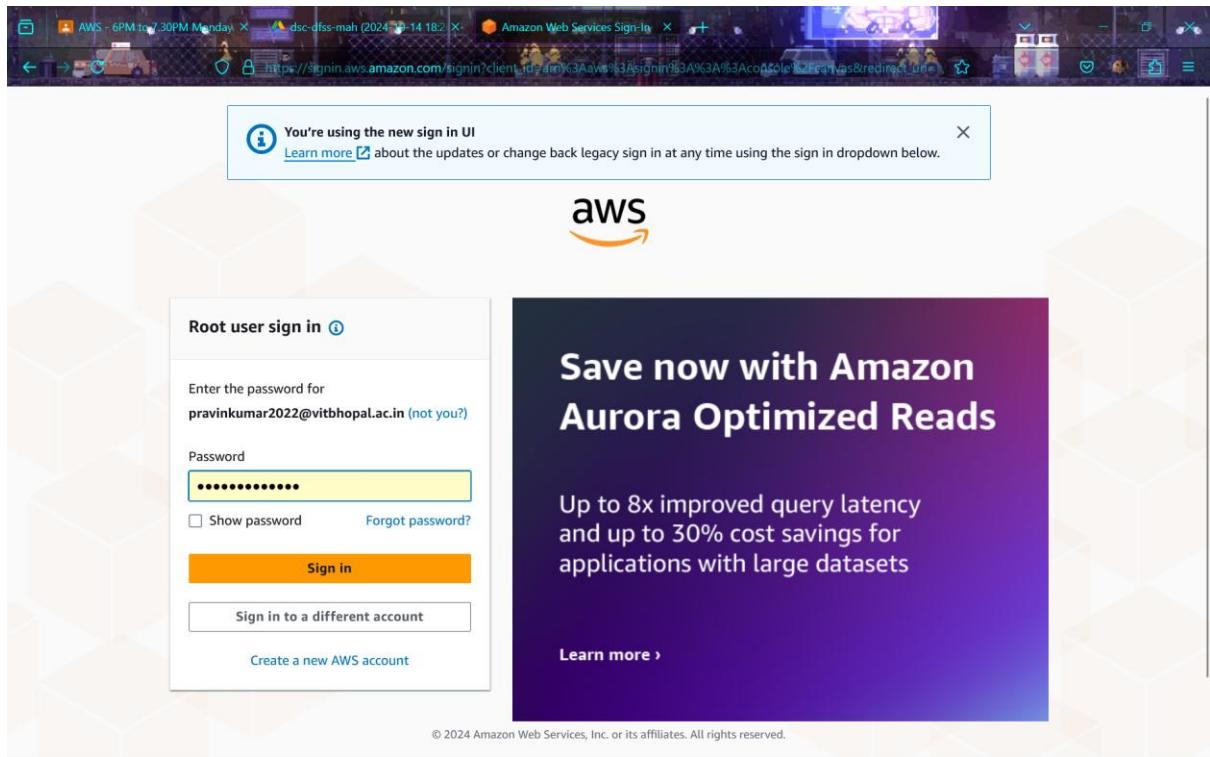
LAB EXPERIMENT – 2

AIM:

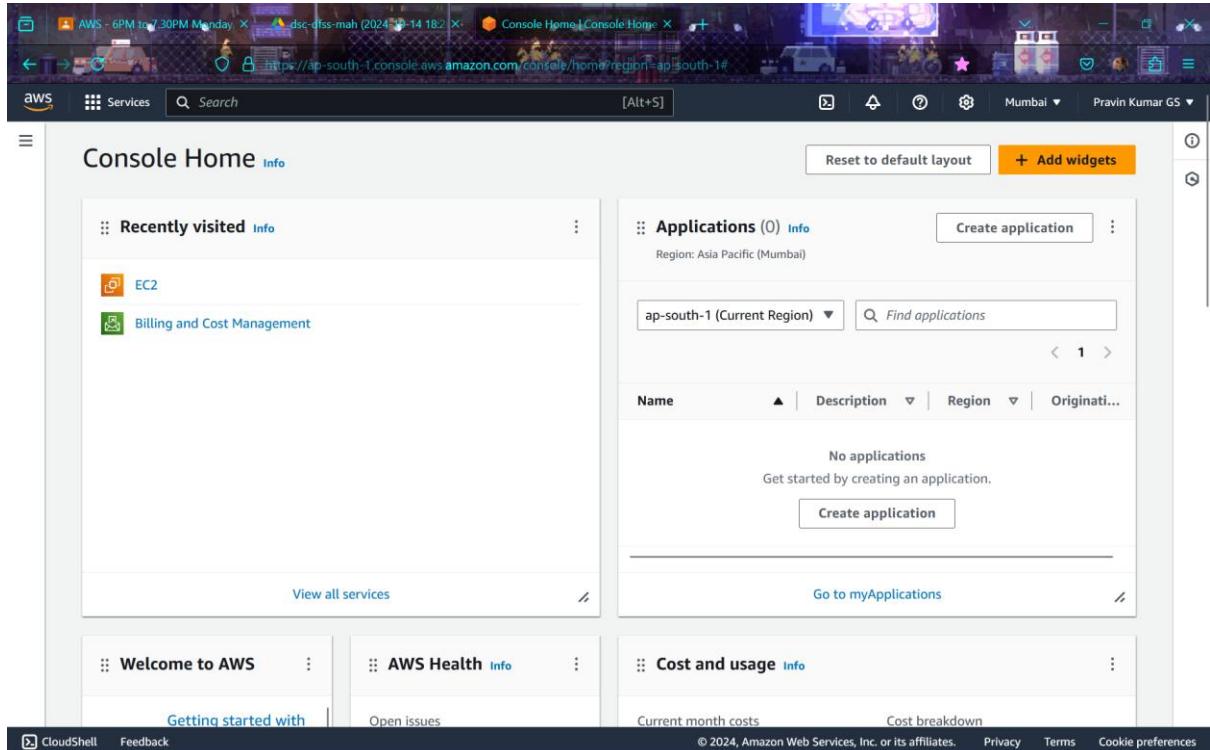
To explore the process of creating an EC2 instance in AWS, attaching and managing storage volumes, and understanding how to create, utilize, and delete both the EC2 instance and its associated storage volume.

STEP 1: Login to your account on AWS Console by adding root user email address and an account name follow the necessary instructions on screen and fill in your account details for billing information. After filling in the details, proceed to the login page and sign in using ‘root user email address’





STEP 2: After clicking 'EC2' you will be redirected to the 'EC2 dashboard', to launch the instance, click on the option 'Instances running'



The screenshot shows the AWS EC2 Dashboard for the Asia Pacific (Mumbai) Region. On the left, a sidebar lists various EC2 management options like Instances, Images, and Block Store. The main panel displays a summary of resources: 0 running instances, 0 auto scaling groups, 0 capacity reservations, etc. It also features a 'Launch instance' button and a 'Service health' section with the AWS Health Dashboard. A sidebar on the right provides information about the EC2 Free Tier, mentioning 2 offers in use and exceeding the free tier limit.

STEP 3: Now we need to name the instance in here. I will name the instance as '22BET10027'.

The screenshot shows the AWS EC2 Instances page. The sidebar is identical to the previous dashboard. The main area is titled 'Instances Info' and shows a search bar and filter options (Name, Instance ID, Instance state, Instance type, Status check, Alarm status). Below this, a message states 'No instances' and 'You do not have any instances in this region'. A prominent 'Launch instances' button is located at the bottom of this section. A modal window titled 'Select an instance' is partially visible at the bottom.

The screenshot shows the AWS EC2 'Launch an instance' wizard. The top navigation bar includes tabs for 'AWS - 6PM to 7:30PM Monday' and 'dsc-dfss-mah (2024-10-14 18:21)'. The main title is 'Launch an instance | EC2 | aws.amazon.com'. The left sidebar has 'Services' selected under 'aws' and shows 'EC2 > ... > Launch an instance'. The right sidebar shows 'Mumbai' and 'Pravin Kumar GS'. The main content area has a 'Summary' section with 'Number of instances' set to 1. It also includes sections for 'Software Image (AMI)', 'Virtual server type (instance type)', 'Firewall (security group)', and 'Storage (volumes)'. A note about the free tier is displayed. At the bottom are 'Cancel' and 'Launch instance' buttons.

AWS - 6PM to 7:30PM Monday dsc-dfss-mah (2024-09-14 18:25) Launch an instance | EC2 | apps Mumbai Pravin Kumar GS

CloudShell Feedback

https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstance

Search our full catalog including 1000s of application and OS images [Alt+S]

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat S...

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible

ami-04a37924ffe27da53 (64-bit (x86), uefi-preferred) / ami-0846b753e2af0da6e (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Architecture: 64-bit (x86) Boot mode: uefi-preferred AMI ID: ami-04a37924 Username: ec2-user

Verified provider

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...read more
ami-04a37924fe27da53

Virtual server type (instance type): t2.micro

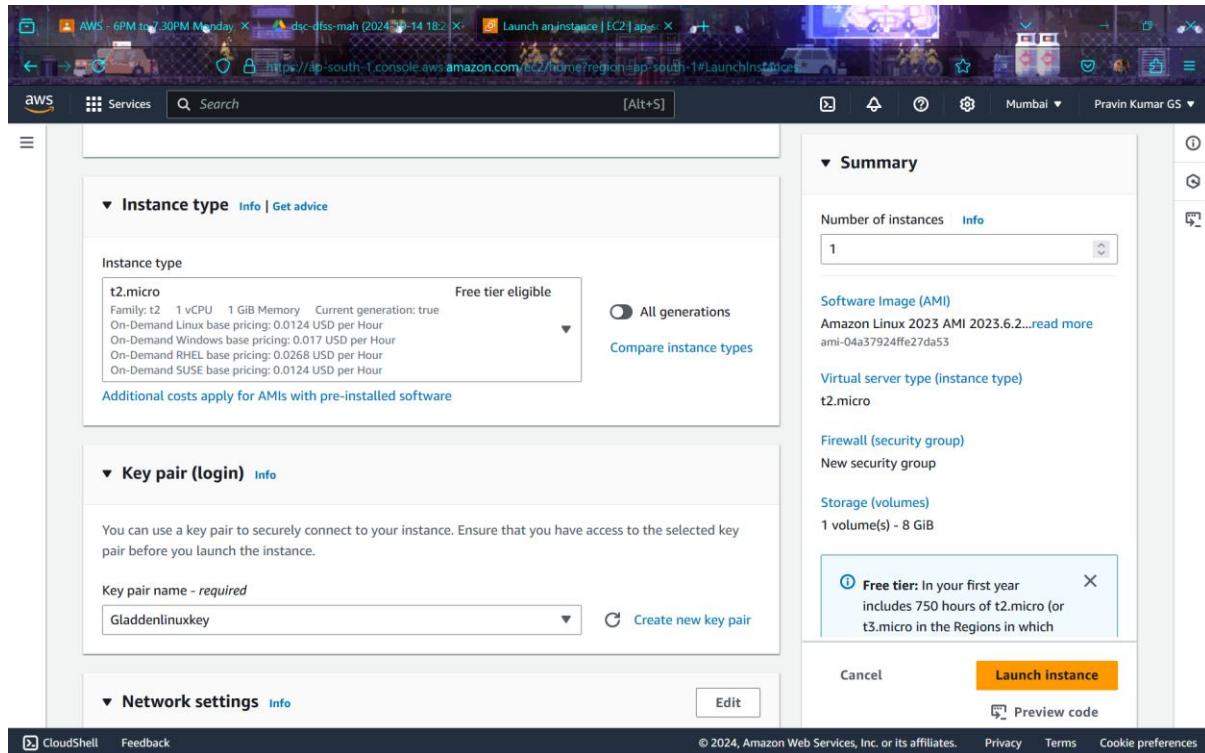
Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

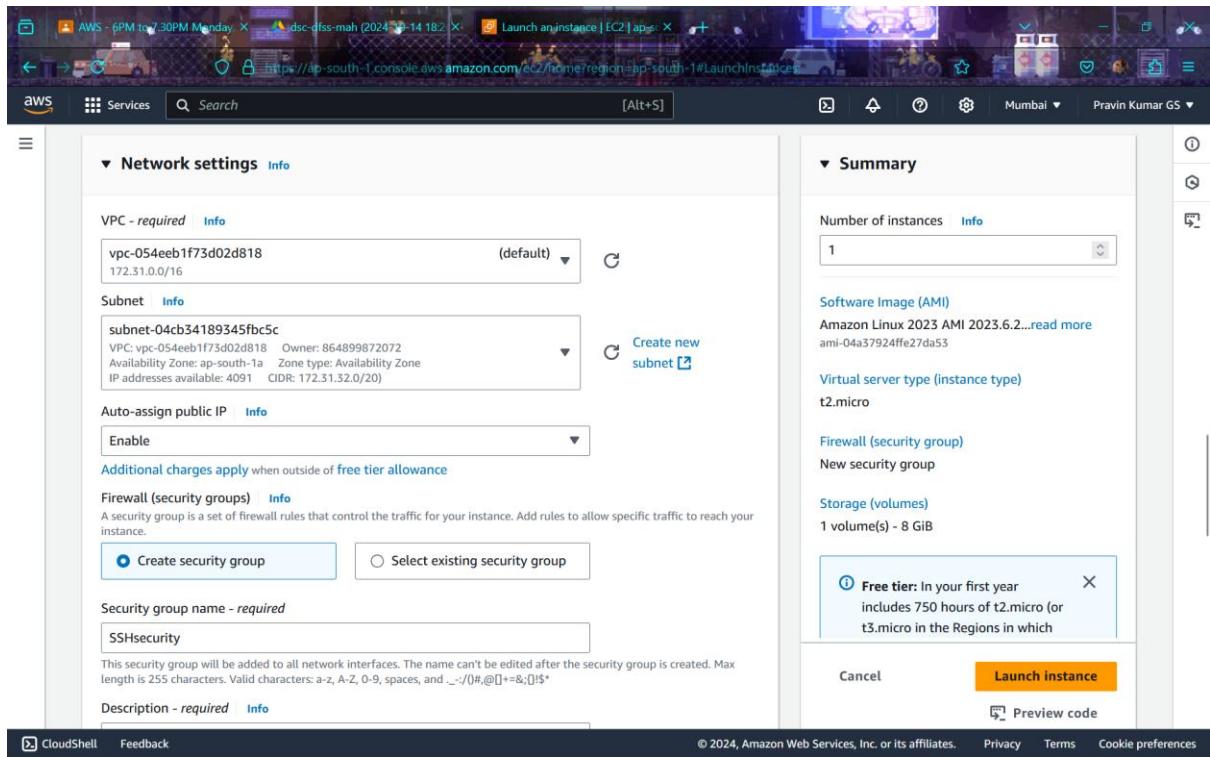
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro) in the Regions in which you launch instances

Cancel Launch Instance Preview code

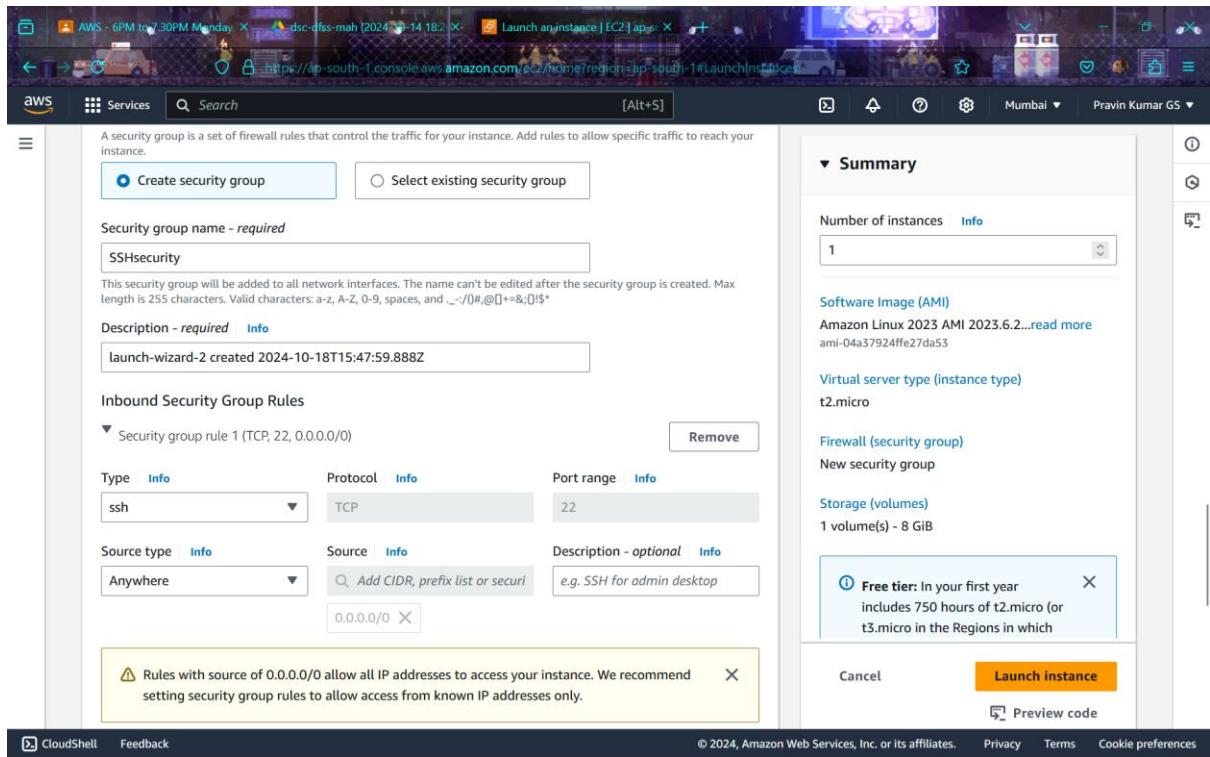
STEP 4: After selecting the necessary ‘AMI’ the next step is to select the instance type, where “t” means family, “2” is the generation and micro meaning the size of the instance. Here we will choose “t2 micro”. In the drop-down menu we will get to see several instance types, but as we are working with free tier we choose ‘t2 micro’.



STEP 5: Now we need to create a new key pair for accessing the instance, the following step creates two types of keys a “Private key” and “Public key”. The public key will be sent to AWS and the private key will be with the user. So in order to login to the instance you need to use the private key.

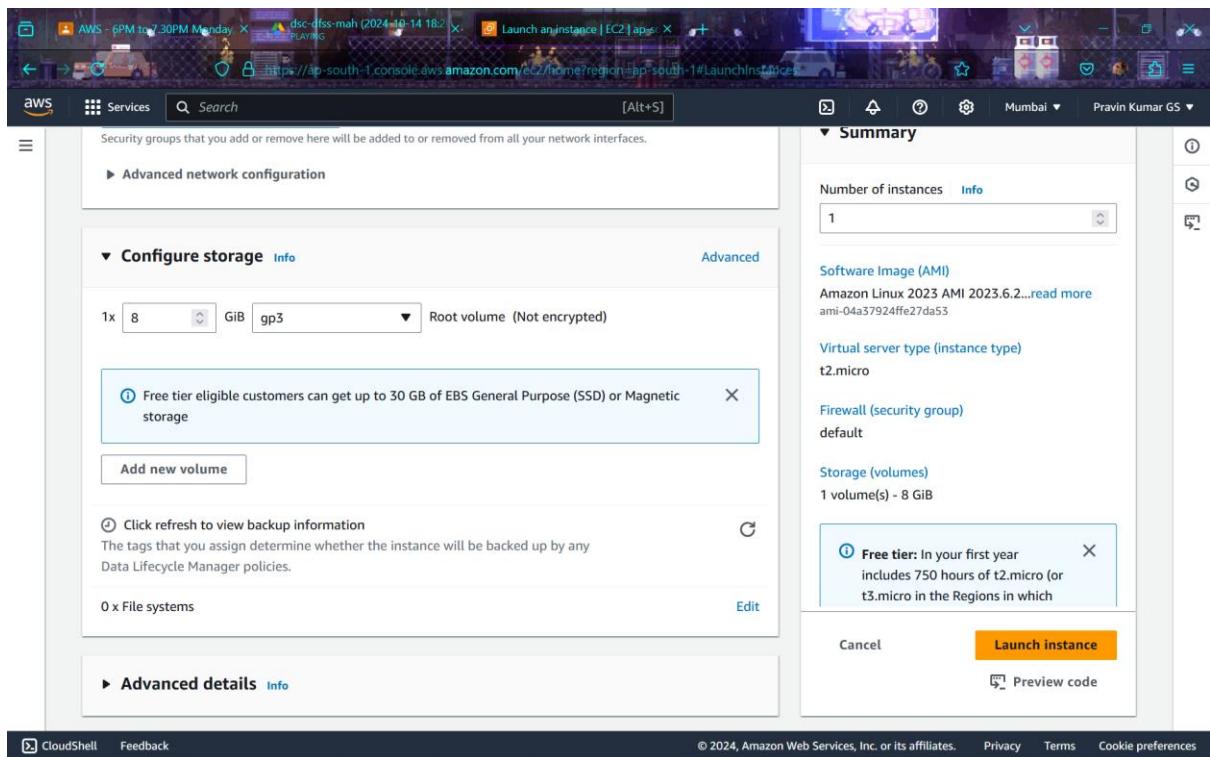


STEP 6: After clicking on “create new key pair”, we first have to give a name for the key pair, here I am going to name my key pair as “Gladdenlinuxkey” Its important to note that the name must not contain any spaces. Here we are going to select “RSA” as the key pair type. There are two file formats which are offered, “. pem” and “. ppk”. Pem is used to log in to the Linux system using CLI (Command line interface) and the ppk format is used to log in through PuTTY. Here we are going to use the “. Pem is essential for securely accessing EC2 instances via SSH or other services requiring authentication.

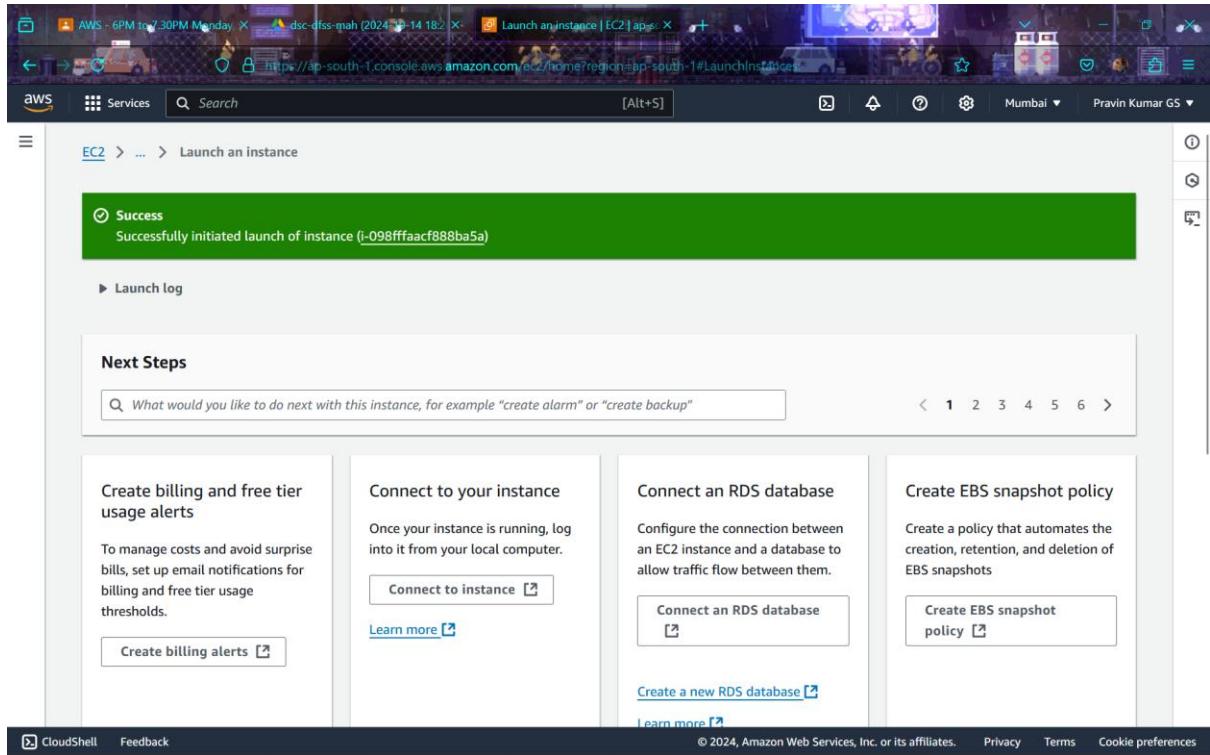


STEP :7 Now we must configure the storage, which is nothing but a hard drive. You can choose either an HDD or SSD. We will now increase the size to 15GB.

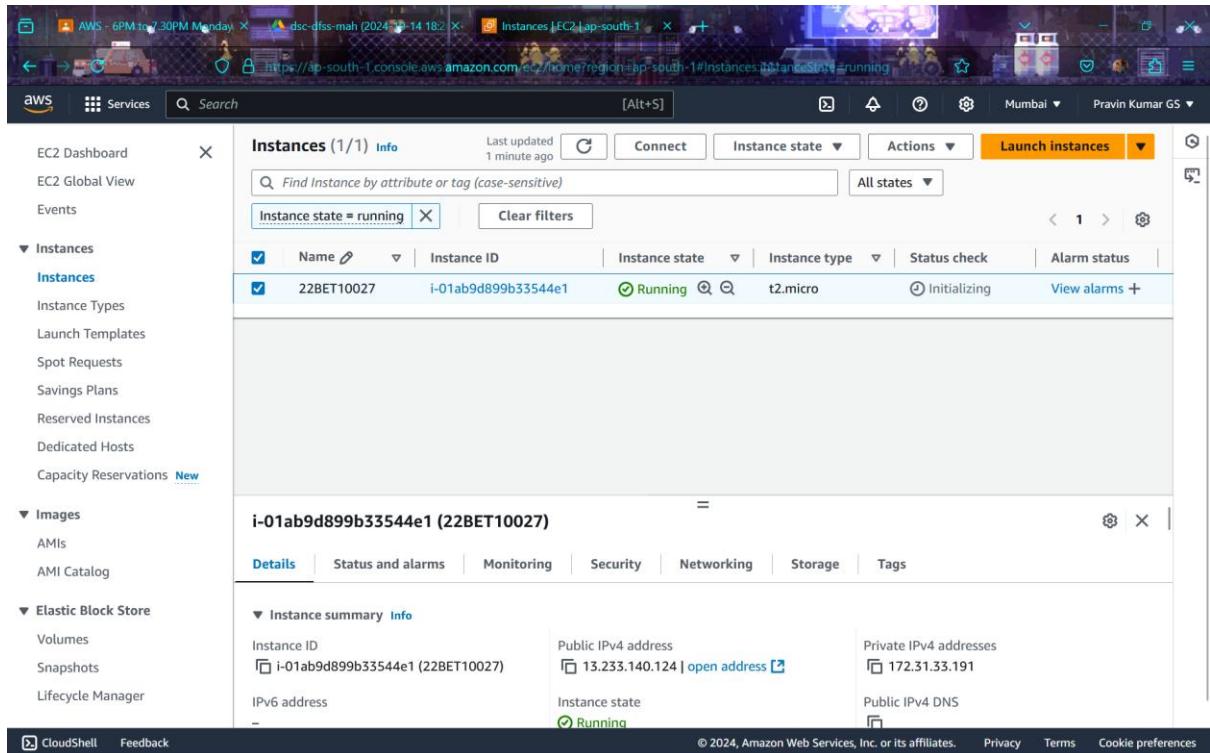
STEP 8: On the right side of the screen, you get to see the summary, an option “number of instances” will specify how many instances you will create, let’s leave it at 1. Confirm all the settings in the above screenshot, ‘t2.micro’ enabled, this is because a subnet has been selected where t2 wasn’t available. Therefore, this shows that before launching an instance its important to check the summary and now press the Launch Instance option.



STEP 9: Finally you have launched the instance.



STEP 10: Click on the reload option if the instance is not visible, after that you can check the “Status field” where its showing “2/2 checks passed” which means that your EC2 instance is running fine.



STEP 11: Now go to Volumes, which is under EBS section and press the create volume option.

STEP 12: Now under volume settings, select the General Purpose SSD (gp3) which is also a default setup, give 10GiB under size section, IOPS (Input/Output Operations Per Second) which has the minimum of 3000 and throughput has the minimum of 125 (MiB/s) and the availability zone is ap-south-1a as am in South Zone, snapshot ID is optional so make it as don't create volume from a snapshot which is the default option.

STEP 13: Now under volume settings, select the General Purpose SSD (gp3) which is also a default setup, give 10GiB under size section, IOPS (Input/Output Operations Per Second) which has the minimum of 3000 and throughput has the minimum of 125 (MiB/s) and the

availability zone is ap-south-1a as am in South Zone, snapshot ID is optional so make it as don't create volume from a snapshot which is the default option.

The screenshot shows the AWS CloudWatch Metrics console with a success message: "Successfully attached volume vol-0d5f93b38e873d54c to instance i-0b510ee593aca4999." Below this, the "Volumes" section lists two volumes: "vol-0bcbf8dfb98a3bd33" (gp3, 8 GiB, 3000 IOPS, Throughput 125, Snapshot ID snap-0875c14...) and "vol-0d5f93b38e873d54c" (gp3, 10 GiB, 3000 IOPS, Throughput 125, Snapshot ID -). A modal window titled "Fault tolerance for all volumes in this Region" displays a "Snapshot summary" showing 0 / 1 recently backed up volumes. The left sidebar includes sections for 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, Network Interfaces), Load Balancing (Load Balancers, Target Groups), and CloudShell/Feedback.

STEP 14: Now under Actions option, you can see Attach Volume, click on it.

The screenshot shows the AWS EBS Volumes page with a success message: "Successfully attached volume vol-0d5f93b38e873d54c to instance i-0b510ee593aca4999." The "Actions" dropdown menu is open, and the "Attach volume" option is highlighted. The main table lists two volumes: "vol-0bcbf8dfb98a3bd33" and "vol-0d5f93b38e873d54c". Below the table, a detailed view for "Volume ID: vol-0d5f93b38e873d54c" shows various metrics like Type (gp3), Size (10 GiB), IOPS (3000), Throughput (125), and creation date (Fri Oct 18 2024 21:04:10 GMT+0530 (India Standard Time)). The left sidebar includes sections for 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, Network Interfaces), Load Balancing (Load Balancers, Target Groups), and CloudShell/Feedback.

STEP 15: Select the shown instance which you have created it before.

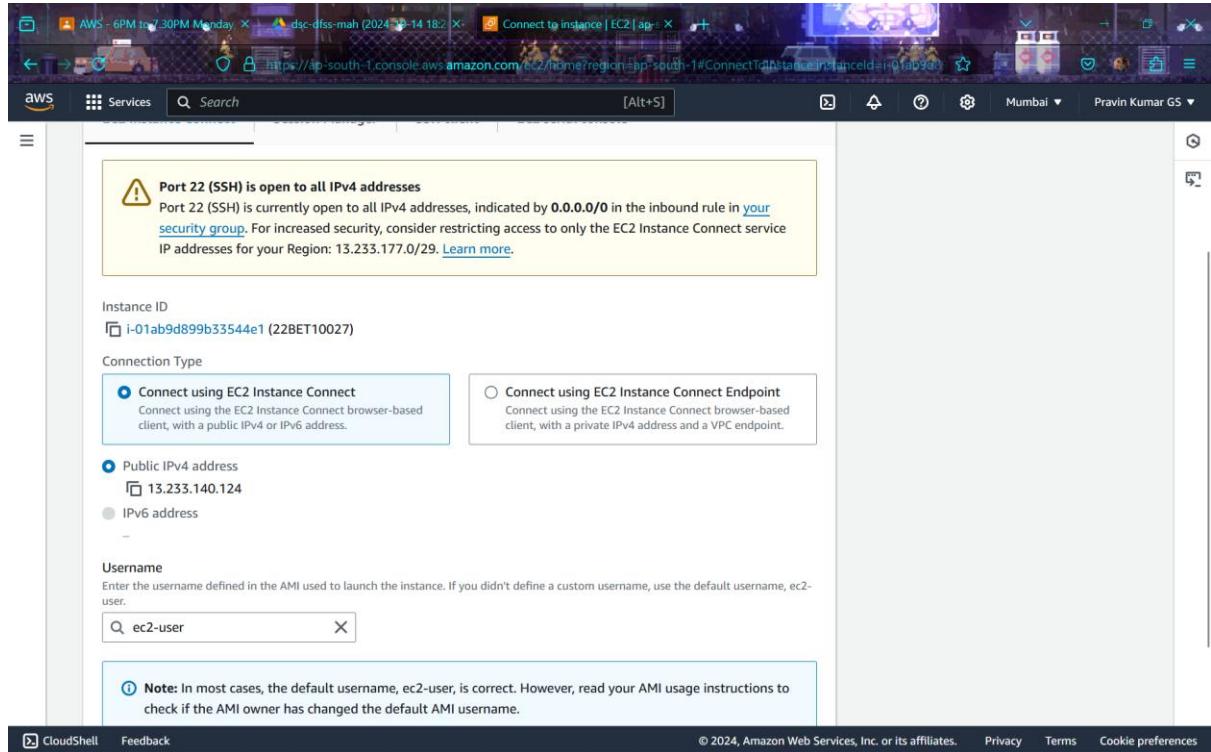
The screenshot shows the 'Attach volume' page in the AWS EC2 console. In the 'Basic details' section, the Volume ID is 'vol-0d5f93b38e873d54c' and the Availability Zone is 'ap-south-1a'. Under 'Instance', the instance 'i-01ab9d899b33544e1' is selected. Under 'Device name', the device name '/dev/xvdf' is entered. A note indicates that newer Linux kernels may rename devices to /dev/xvdf through /dev/xvdp internally. At the bottom, there are links for CloudShell, Feedback, and cookie preferences.

STEP 16: Under device name select a custom device name and attach to the volume.

The screenshot shows the 'Volumes' page in the AWS EC2 console. A green success message at the top states 'Successfully attached volume vol-0d5f93b38e873d54c to instance i-01ab9d899b33544e1'. Below this, the 'Volumes' table lists two volumes: 'snap-0875c14...' and another unnamed volume. Both are in the 'In-use' state and are attached to the instance 'i-01ab9d899b33544e1'. The sidebar on the left shows the navigation menu for EC2, including 'Instances', 'Images', and 'Elastic Block Store'.

STEP 17: Give the device name as /dev/xvdf and save the information.

STEP 18: Now go to instance which is under instances in the dashboard and connect the instance.



STEP 19: The page is redirected to Linux based system.c

Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together.

Close permanently

```
'~\ #####  
~~~ \#####  
~~~ \###  
~~~ \#/ https://aws.amazon.com/linux/amazon-linux-2023  
~~~ \~/  
~~~ /  
[ec2-user@ip-172-31-33-191 ~]$
```

i-01ab9d899b33544e1 (22BET10027)
Public IPs: 13.233.140.124 Private IPs: 172.31.33.191

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type the following commands as listed below,

1. `sudo su -` [to get root access]
2. `lsblk` [list blocks]
3. `file -s /dev/xvda` [checking the file]
4. `mkfs -t xfs /dev/xvdf` [for creating file system]
5. `mkdir -p /app/volume` [for creating folder]
6. `mount /dev/xvdf /app/volume` [mounting EBS on our instance]
7. `file -s /dev/xvdf` [to check the changes we made]
8. `df -h` [for adding extra storage]

STEP 19: Type the following command on the terminal “sudo su –“ this is to use as root user.

The screenshot shows a terminal window in the AWS CloudShell interface. The title bar indicates the session is titled "dsc-dfss-mah (2024-10-14 18:21 PLAYING)". The URL in the address bar is "https://ap-south-1.console.aws.amazon.com/ec2/instance-connect/shell?region=ap-south-1&connType=standardeline". The terminal content includes a keyboard shortcut message, a snippet of Amazon Linux 2023 configuration, and a command prompt. A floating modal box provides information about the keyboard shortcut for navigating between button elements.

① Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together.

```
~\_\_ ##### Amazon Linux 2023
~~ \####\_
~~ \###\_
~~ \###\_
~~ \###\_
~~ \###\_
~~ \###\_
[ec2-user@ip-172-31-33-191 ~]$ sudo su -
```

i-01ab9d899b33544e1 (22BET10027)
PublicIPs: 13.233.140.124 PrivateIPs: 172.31.33.191

The screenshot shows a CloudShell terminal window with the following content:

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-33-191 ~]$ sudo su -
[root@ip-172-31-33-191 ~]#
```

A tooltip at the top left of the terminal area provides a keyboard shortcut: "To tab out of the terminal window and select the next button element, press the left and right Shift keys together." A "Close permanently" button is also visible in the top right corner of the terminal window.

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-172-31-33-191 ~]$ sudo su -
[root@ip-172-31-33-191 ~]# pwd
/root
[root@ip-172-31-33-191 ~]# df -h
```

i-01ab9d899b33544e1 (22BET10027)
PublicIPs: 13.233.140.124 PrivateIPs: 172.31.33.191

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-172-31-33-191 ~]$ sudo su -
[root@ip-172-31-33-191 ~]# df -h
```

i-01ab9d899b33544e1 (22BET10027)
PublicIPs: 13.233.140.124 PrivateIPs: 172.31.33.191

STEP 19: Type the following command on the terminal “df -h” this is to use to display the disk space usage of file systems in a human-readable format. The -h option stands for "human-

"readable," which means it shows the sizes in easy-to-read units such as MB, GB, or TB instead of blocks.

The screenshot shows a CloudShell terminal window with the following content:

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-172-31-33-191 ~]$ sudo su -
[root@ip-172-31-33-191 ~]# pwd
/root
[root@ip-172-31-33-191 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0    4.0M  0% /dev
tmpfs          475M   0   475M  0% /dev/shm
tmpfs          190M  452K  190M  1% /run
/dev/xvda1       8.0G  1.6G  6.4G 20% /
tmpfs          475M   0   475M  0% /tmp
/dev/xvda128     10M  1.3M  8.7M 13% /boot/efi
tmpfs          95M   0   95M  0% /run/user/1000
[root@ip-172-31-33-191 ~]#
```

At the bottom of the terminal, the CloudShell interface displays the session ID (i-01ab9d899b33544e1), the public IP (13.233.140.124), and the private IP (172.31.33.191).

STEP 20: Type the following command on the terminal “lsblk“ is used to list information about all available or specified block devices. It provides a detailed tree structure of block devices such as hard drives, SSDs, and their partitions.

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-172-31-33-191 ~]$ sudo su -
[root@ip-172-31-33-191 ~]# pwd
/root
[root@ip-172-31-33-191 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0  4.0M  0% /dev
tmpfs          475M   0  475M  0% /dev/shm
tmpfs          190M  452K 190M  1% /run
/dev/xvda1      8.0G  1.6G  6.4G  20% /
tmpfs          475M   0  475M  0% /tmp
/dev/xvda128    10M  1.3M  8.7M  13% /boot/efi
tmpfs          95M   0  95M  0% /run/user/1000
[root@ip-172-31-33-191 ~]# lsblk
```

i-01ab9d899b33544e1 (22BET10027)
Public IPs: 13.233.140.124 Private IPs: 172.31.33.191

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-172-31-33-191 ~]$ sudo su -
[root@ip-172-31-33-191 ~]# pwd
/root
[root@ip-172-31-33-191 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0  4.0M  0% /dev
tmpfs          475M   0  475M  0% /dev/shm
tmpfs          190M  452K 190M  1% /run
/dev/xvda1      8.0G  1.6G  6.4G  20% /
tmpfs          475M   0  475M  0% /tmp
/dev/xvda128    10M  1.3M  8.7M  13% /boot/efi
tmpfs          95M   0  95M  0% /run/user/1000
[root@ip-172-31-33-191 ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
xvda   202:0    0   8G  0 disk 
└─xvda1 202:1    0   8G  0 part /
  └─xvda127 259:0  0   1M  0 part 
  └─xvda128 259:1  0  10M 0 part /boot/efi
xvdf   202:80   0   10G 0 disk
```

i-01ab9d899b33544e1 (22BET10027)
Public IPs: 13.233.140.124 Private IPs: 172.31.33.191

STEP 21: Type the following command on the terminal “file -s /dev/xvdf “ is used to list information about all available or specified block devices. It provides a detailed tree structure of block devices such as hard drives, SSDs, and their partitions.

STEP 22: Type the following command on the terminal “`mkfs -t xfs /dev/xvdf`“ is used to format the `/dev/xvdf` block device with the **XFS** file system.

```

AWS - 6PM to 7:30PM Monday AWS - dsc-dfss-mah (2024-09-14 18:21) Volumes | EC2 Instance Connect
https://ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-south-1&connType=standard&id=
Services Search [Alt+S] Close permanently
① Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together.

~~ \#/ https://aws.amazon.com/linux/amazon-linux-2023
~~ ~~~ / 
~~ .- / 
~/ /m/
[ec2-user@ip-172-31-33-191 ~]$ sudo su -
[root@ip-172-31-33-191 ~]# pwd
/root
[root@ip-172-31-33-191 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0M  4.0M  0% /dev
tmpfs          475M   0M  475M  0% /dev/shm
tmpfs          190M  452K 190M  1% /run
/dev/xvda1      8.0G  1.6G  6.4G  20% /
tmpfs          475M   0M  475M  0% /tmp
/dev/xvda128    10M  1.3M  8.7M  13% /boot/efi
tmpfs          95M   0M  95M  0% /run/user/1000
[root@ip-172-31-33-191 ~]# lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
xvda   202:0    0  8G  0 disk
└─xvda1  202:1    0  8G  0 part /
xvda127 259:0    0  1M  0 part
xvda128 259:1    0 10M  0 part /boot/efi
xvdf   202:80   0 10G  0 disk
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf
/dev/xvdf: data
[root@ip-172-31-33-191 ~]# mkfs -t xfs /dev/xvdf

i-01ab9d899b33544e1 (22BET10027)
PublicIPs: 13.233.140.124 PrivateIPs: 172.31.33.191

```

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

```

AWS - 6PM to 7:30PM Monday AWS - dsc-dfss-mah (2024-09-14 18:21) Volumes | EC2 Instance Connect
https://ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-south-1&connType=standard&id=
Services Search [Alt+S] Close permanently
① Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together.

devtmpfs        4.0M   0  4.0M  0% /dev
tmpfs          475M   0  475M  0% /dev/shm
tmpfs          190M  452K 190M  1% /run
/dev/xvda1      8.0G  1.6G  6.4G  20% /
tmpfs          475M   0  475M  0% /tmp
/dev/xvda128    10M  1.3M  8.7M  13% /boot/efi
tmpfs          95M   0  95M  0% /run/user/1000
[root@ip-172-31-33-191 ~]# lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
xvda   202:0    0  8G  0 disk
└─xvda1  202:1    0  8G  0 part /
xvda127 259:0    0  1M  0 part
xvda128 259:1    0 10M  0 part /boot/efi
xvdf   202:80   0 10G  0 disk
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf
/dev/xvdf: data
[root@ip-172-31-33-191 ~]# mkfs -t xfs /dev/xvdf
meta-data=/dev/xvdf      isize=512   agcount=4, agsize=655360 blks
                          sectsz=512   attr=2, projid32bit=1
                          crc=1     finobt=1, sparse=1, rmapbt=0
                          reflink=1   bigtime=1 inobtcount=1
data          =           bsize=4096   blocks=2621440, imaxpct=25
                     sunit=0     swidth=0 blks
naming        =version 2   bsize=4096   ascii-ci=0, ftype=1
log           =internal log  bsize=4096   blocks=16384, version=2
                     sectsz=512   sunit=0 blks, lazy_count=1
realtime      =none       extsz=4096   blocks=0, rtextents=0
[root@ip-172-31-33-191 ~]# 

i-01ab9d899b33544e1 (22BET10027)
PublicIPs: 13.233.140.124 PrivateIPs: 172.31.33.191

```

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

STEP 23: Type the following command on the terminal “file -s /dev/xvdf“ is used to check the type of the /dev/xvdf block device. The -s option ensures that the contents of the special file.

The screenshot shows a CloudShell terminal window with the following content:

```

① Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together.

devtmpfs      4.0M    0  4.0M  0% /dev
tmpfs        475M    0  475M  0% /dev/shm
tmpfs       190M  452K 190M  1% /run
/dev/xvda1    8.0G  1.6G  6.4G  20% /
tmpfs        475M    0  475M  0% /tmp
/dev/xvda128   10M  1.3M  8.7M  13% /boot/efi
tmpfs        95M    0  95M  0% /run/user/1000
[root@ip-172-31-33-191 ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
xvda    202:0    0   8G  0 disk
└─xvda1  202:1    0   8G  0 part /
  ├─xvda127 259:0    0   1M  0 part
  ├─xvda128 259:1    0   10M 0 part /boot/efi
  └─xvdf   202:80   0  10G  0 disk
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf
/dev/xvdf: data
[root@ip-172-31-33-191 ~]# mkfs -t xfs /dev/xvdf
meta-data=/dev/xvdf isize=512 agcount=4, agsize=655360 blks
      =           sectsz=512 attr=2, projid32bit=1
      =           crc=1   finobt=1, sparse=1, rmapbt=0
      =           reflink=1 bigtime=1 inobtcount=1
data     =           bsize=4096 blocks=2621440, imaxpct=25
      =           sunit=0 swidth=0 blks
naming   =version 2 bsize=4096 ascii-ci=0, ftype=1
log      =internal log bsize=4096 blocks=16384, version=2
      =           sectsz=512 sunit=0 blks, lazy-count=1
realtime =none      extsz=4096 blocks=0, rtextents=0
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf

```

Below the terminal output, there is a message box with the following content:

i-01ab9d899b33544e1 (22BET10027)
Public IPs: 13.233.140.124 Private IP: 172.31.33.191

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

STEP 24: Type the following commands on the terminal

- “mkdir -p /app/volume” is used to creates the directory /app/volume (and any necessary parent directories) where the volume will be mounted.
- mount /dev/xvdf /app/volume, this mounts the block device /dev/xvdf to the directory /app/volume, making it accessible at that location.
- df -h, this displays the disk space usage of mounted filesystems in a human-readable format (MB, GB, etc.). It helps confirm that the device has been successfully mounted and is using the correct space.

```
[root@ip-172-31-33-191 ~]# df -h
Filesystem      Size  Used Avail Capacity  Mounted on
tmpfs           475M   475M     0% /tmp
/dev/xvda128    10M   1.3M   8.7M  13% /boot/efi
tmpfs           95M    0     95M  0% /run/user/1000
[root@ip-172-31-33-191 ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
xvda    202:0    0   8G  0 disk
└─xvda1  202:1    0   8G  0 part /
  └─xvda127 259:0    0   1M  0 part
    └─xvda128 259:1    0  10M 0 part /boot/efi
xvdf    202:80   0  10G  0 disk
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf
/dev/xvdf: data
[root@ip-172-31-33-191 ~]# mkfs -t xfs /dev/xvdf
meta-data=/dev/xvdf      isize=512   agcount=4, agsize=655360 blks
                      =       sectsz=512  attr=2, projid32bit=1
                      =       crc=1    finobt=1, sparse=1, rmapbt=0
                      =       reflink=1 bigtime=1 inobtcount=1
data     =       bsize=4096   blocks=2621440, imaxpct=25
          =       sunit=0    swidth=0 blks
naming  =version 2      bsize=4096   ascii-ci=0, ftype=1
log     =internal log    bsize=4096   blocks=16384, version=2
          =       sectsz=512  sunit=0 blks, lazy-count=1
realtime =none          extsz=4096   blocks=0, rtextents=0
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf
/dev/xvdf: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
[root@ip-172-31-33-191 ~]# mkdir -p /app/volume
[root@ip-172-31-33-191 ~]# mount /dev/xvdf /app/volume
```

i-01ab9d899b33544e1 (22BET10027)

Public IPs: 13.233.140.124 Private IPs: 172.31.33.191

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

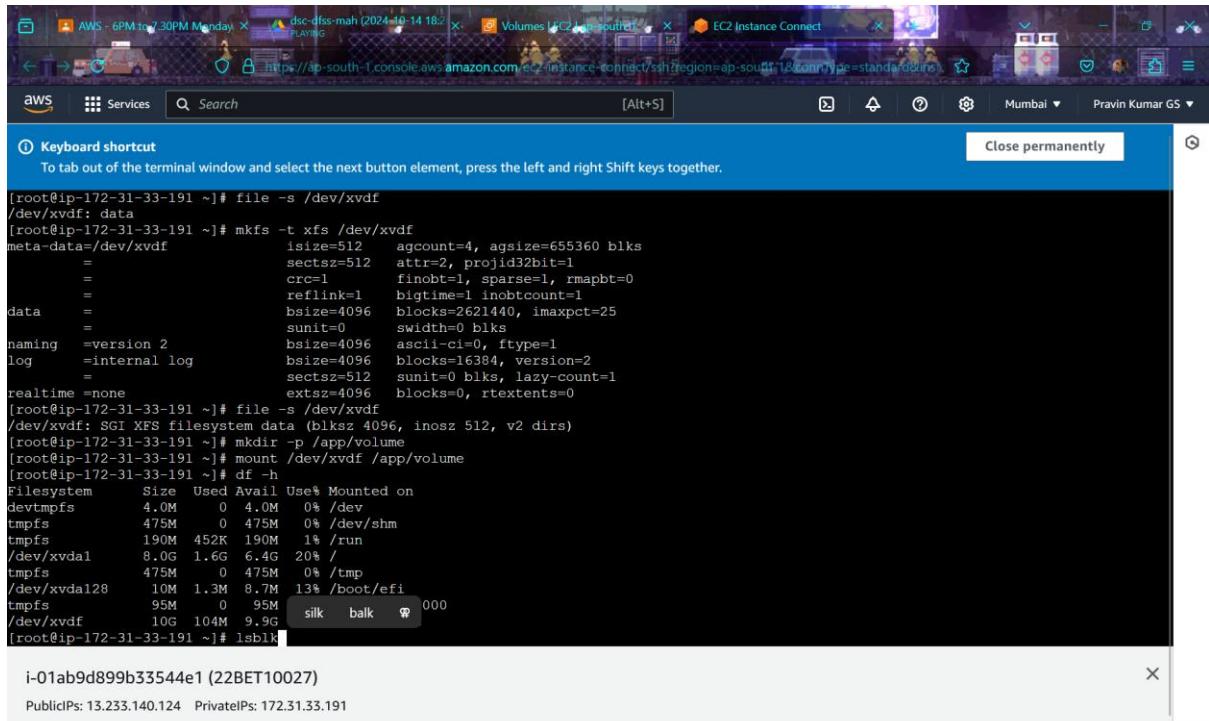
```
[root@ip-172-31-33-191 ~]# df -h
Filesystem      Size  Used Avail Capacity  Mounted on
tmpfs           475M   475M     0% /tmp
/dev/xvda128    10M   1.3M   8.7M  13% /boot/efi
tmpfs           95M    0     95M  0% /run/user/1000
[root@ip-172-31-33-191 ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
xvda    202:0    0   8G  0 disk
└─xvda1  202:1    0   8G  0 part /
  └─xvda127 259:0    0   1M  0 part
    └─xvda128 259:1    0  10M 0 part /boot/efi
xvdf    202:80   0  10G  0 disk
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf
/dev/xvdf: data
[root@ip-172-31-33-191 ~]# mkfs -t xfs /dev/xvdf
meta-data=/dev/xvdf      isize=512   agcount=4, agsize=655360 blks
                      =       sectsz=512  attr=2, projid32bit=1
                      =       crc=1    finobt=1, sparse=1, rmapbt=0
                      =       reflink=1 bigtime=1 inobtcount=1
data     =       bsize=4096   blocks=2621440, imaxpct=25
          =       sunit=0    swidth=0 blks
naming  =version 2      bsize=4096   ascii-ci=0, ftype=1
log     =internal log    bsize=4096   blocks=16384, version=2
          =       sectsz=512  sunit=0 blks, lazy-count=1
realtime =none          extsz=4096   blocks=0, rtextents=0
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf
/dev/xvdf: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
[root@ip-172-31-33-191 ~]# mkdir -p /app/volume
[root@ip-172-31-33-191 ~]# mount /dev/xvdf /app/volume
[root@ip-172-31-33-191 ~]# df -h
```

i-01ab9d899b33544e1 (22BET10027)

Public IPs: 13.233.140.124 Private IPs: 172.31.33.191

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

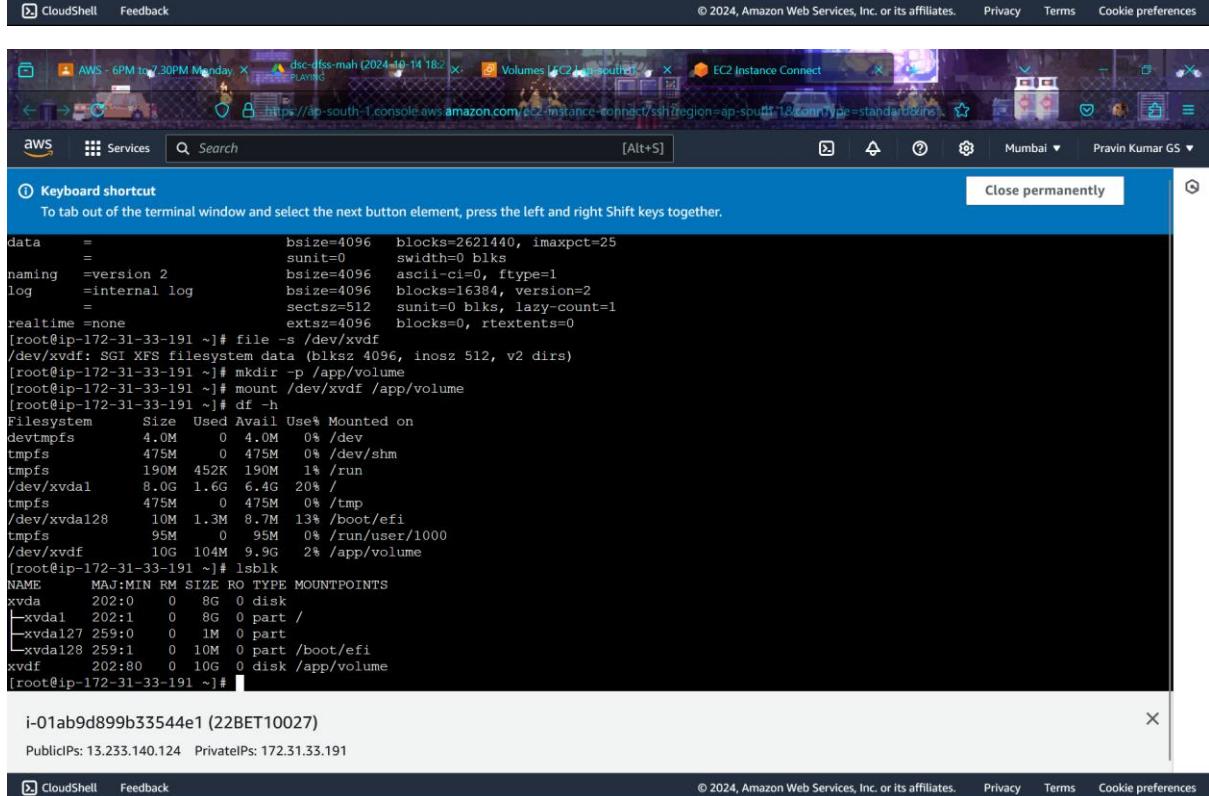
STEP 25: Type the following command on the terminal “lsblk“ is used to list information about all available or specified block devices. It provides a detailed tree structure of block devices such as hard drives, SSDs, and their partitions.



```
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf
/dev/xvdf: data
[root@ip-172-31-33-191 ~]# mkfs -t xfs /dev/xvdf
meta-data=/dev/xvdf      isize=512   agcount=4, agsize=655360 blks
=                      sectsz=512   attr=2, projid32bit=1
=                      crc=1     finobt=1, sparse=1, rmapbt=0
data        =             reflink=1   bigtime=1, inobtcount=1
bsize=4096   blocks=2621440, imaxpct=25
=             sunit=0    swidth=0 blks
naming      =version 2   bsize=4096  ascii-ci=0, ftype=1
log         =internal log bsize=4096  blocks=16384, version=2
=             sectsz=512  sunit=0 blks, lazy-count=1
realtime    =none        extsz=4096  blocks=0, rtextents=0
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf
/dev/xvdf: SG1 XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
[root@ip-172-31-33-191 ~]# mkdir -p /app/volume
[root@ip-172-31-33-191 ~]# mount /dev/xvdf /app/volume
[root@ip-172-31-33-191 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0    4.0M  0% /dev
tmpfs          475M   0   475M  0% /dev/shm
tmpfs          190M  452K 190M  1% /run
/dev/xvda1      8.0G  1.6G  6.4G  20% /
tmpfs          475M   0   475M  0% /tmp
/dev/xvda128    10M  1.3M  8.7M  13% /boot/efi
tmpfs          95M   0   95M  0% /run/user/1000
/dev/xvdf       10G 104M  9.9G  2% /app/volume
[root@ip-172-31-33-191 ~]# lsblk
```

i-01ab9d899b33544e1 (22BET10027)

PublicIPs: 13.233.140.124 PrivateIPs: 172.31.33.191



```
[root@ip-172-31-33-191 ~]# file -s /dev/xvdf
/dev/xvdf: SG1 XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
[root@ip-172-31-33-191 ~]# mkdir -p /app/volume
[root@ip-172-31-33-191 ~]# mount /dev/xvdf /app/volume
[root@ip-172-31-33-191 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0    4.0M  0% /dev
tmpfs          475M   0   475M  0% /dev/shm
tmpfs          190M  452K 190M  1% /run
/dev/xvda1      8.0G  1.6G  6.4G  20% /
tmpfs          475M   0   475M  0% /tmp
/dev/xvda128    10M  1.3M  8.7M  13% /boot/efi
tmpfs          95M   0   95M  0% /run/user/1000
/dev/xvdf       10G 104M  9.9G  2% /app/volume
[root@ip-172-31-33-191 ~]# lsblk
```

i-01ab9d899b33544e1 (22BET10027)

PublicIPs: 13.233.140.124 PrivateIPs: 172.31.33.191

STEP 26: Type the following command on the terminal “lsblk“ is used to list information about all available or specified block devices. It provides a detailed tree structure of block devices such as hard drives, SSDs, and their partitions.

The screenshot shows the AWS CloudShell interface with the EC2 Volumes page open. The left sidebar shows various EC2 services like Instances, Images, and Elastic Block Store. The main table lists two volumes: one with ID vol-0bcbf8dfb98a3bd33 (8 GiB gp3) and another with ID vol-0d5f93b38e873d54c (10 GiB gp3). A context menu is open over the second volume, with 'Create snapshot' highlighted. The details panel for the selected volume shows its configuration, including AWS Compute Optimizer finding, volume state (In-use), and creation date (Fri Oct 18 2024 21:04:10 GMT+0530).

STEP 27: You can see varies details to create a snapshot, just follow the instructions, under description box type this, ebs snapshot-1 or you can change name as per your wish, then click create snapshot.

The screenshot shows the AWS EC2 console with the 'Create snapshot' wizard open. The 'Source volume' section displays a volume with ID `vol-0d5f93b38e873d54c` and availability zone `ap-south-1a`. The 'Snapshot details' section includes a description field containing `ebs snapshot-1`. The 'Tags' section shows no tags associated with the resource. The status bar at the bottom indicates the snapshot was successfully created.

The screenshot shows the AWS EC2 console with the 'Volumes' page open. A success message at the top states 'Successfully created snapshot snap-0fbcd1862094651e1 from volume vol-0d5f93b38e873d54c.' The 'Volumes' table lists two volumes: `vol-0bcbf8dfb98a3bd33` (gp3, 8 GiB, 3000 IOPS, 125 Throughput, Snapshot ID snap-0875c14...) and `vol-0d5f93b38e873d54c` (gp3, 10 GiB, 3000 IOPS, 125 Throughput, Snapshot ID -). The detailed view for volume `vol-0d5f93b38e873d54c` shows it was created on Fri Oct 18 2024 21:04:10 GMT+0530 (India Standard Time) and is attached to instance `i-01ab9d899b3544e1` with device `(22BET10027): /dev/xvdf`.

STEP 28: Yaay! You have created the snapshot for volume.

The screenshot shows the AWS EC2 Snapshots page. The left sidebar is collapsed. The main content area displays a table titled "Snapshots (1/1) info". The table has columns: Name, Snapshot ID, Volume size, Description, Storage tier, and Snapshot status. One row is listed: Name is "-", Snapshot ID is "snap-0fbcd1862094651e1", Volume size is "10 GiB", Description is "ebs snapshot-1", Storage tier is "Standard", and Snapshot status is "Completed". Below the table, a detailed view for "Snapshot ID: snap-0fbcd1862094651e1" is shown. It includes tabs for Details, Snapshot settings, Storage tier, and Tags. Under Details, it shows: Snapshot ID (snap-0fbcd1862094651e1), Progress (Available (100%)), Snapshot status (Completed), Owner (864899872072). It also shows: Started (Fri Oct 18 2024 21:49:33 GMT+0530 (India Standard Time)), Product codes (-), Fast snapshot restore (-), and Description (ebs snapshot-1). Under Source volume, it shows Volume ID (vol-0d5f93b38e873d54c) and Volume size (10 GiB).

STEP 29: Try to refresh, it will be automatically gets updated and the Snapshot status will be updated to Completed status.

STEP 30: Now, go under actions bar and click the copy Snapshot.

The screenshot shows the AWS EC2 Snapshots page. On the left, there's a sidebar with navigation links like EC2 Dashboard, EC2 Global View, Events, Instances, Images, and Elastic Block Store. The main area displays a table titled 'Snapshots (1/1) info' with one item: 'Name: snap-0fbcd1862094651e1', 'Snapshot ID: snap-0fbcd1862094651e1', 'Volume size: 10 GiB', and 'Description: ebs snapshot-1'. A context menu is open over this item, showing options like 'Create volume from snapshot', 'Create image from snapshot', 'Copy snapshot', 'Delete snapshot', 'Manage tags', 'Snapshot settings', and 'Archiving'. Below the table, a detailed view for 'Snapshot ID: snap-0fbcd1862094651e1' is shown with tabs for Details, Snapshot settings, Storage tier, and Tags. The 'Details' tab shows information such as Progress (Available 100%), Snapshot status (Completed), Owner (864899872072), Started (Fri Oct 18 2024 21:49:33 GMT+0530 (India Standard Time)), Product codes (-), Fast snapshot restore (-), Description (ebs snapshot-1), Source volume (Volume ID: vol-0df5f93b38e873d54c, Volume size: 10 GiB), and Volume type (-).

STEP 31: The description part is automatically filled and the destination part select the ap-south-1 zone as we are in South Zone and then click the copy snapshot.

The screenshot shows the 'Copy snapshot' page. At the top, it says 'Copy snapshot info' and 'Copy a snapshot from one AWS Region to another, or within the same Region.' Below this, the 'Source snapshot' section shows the 'Snapshot ID' as 'snap-0fbcd1862094651e1' and the 'Region' as 'ap-south-1'. The 'Snapshot copy details' section contains a 'Description' field with the value '[Copied snap-0fbcd1862094651e1 from ap-south-1] ebs snapshot-1' and a 'Destination Region' dropdown set to 'ap-south-1'. At the bottom, there's an 'Encryption' section with a 'Info' link. The footer includes standard AWS links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

STEP 31: Now under the Actions bar select delete snapshot for deleting the snapshot.

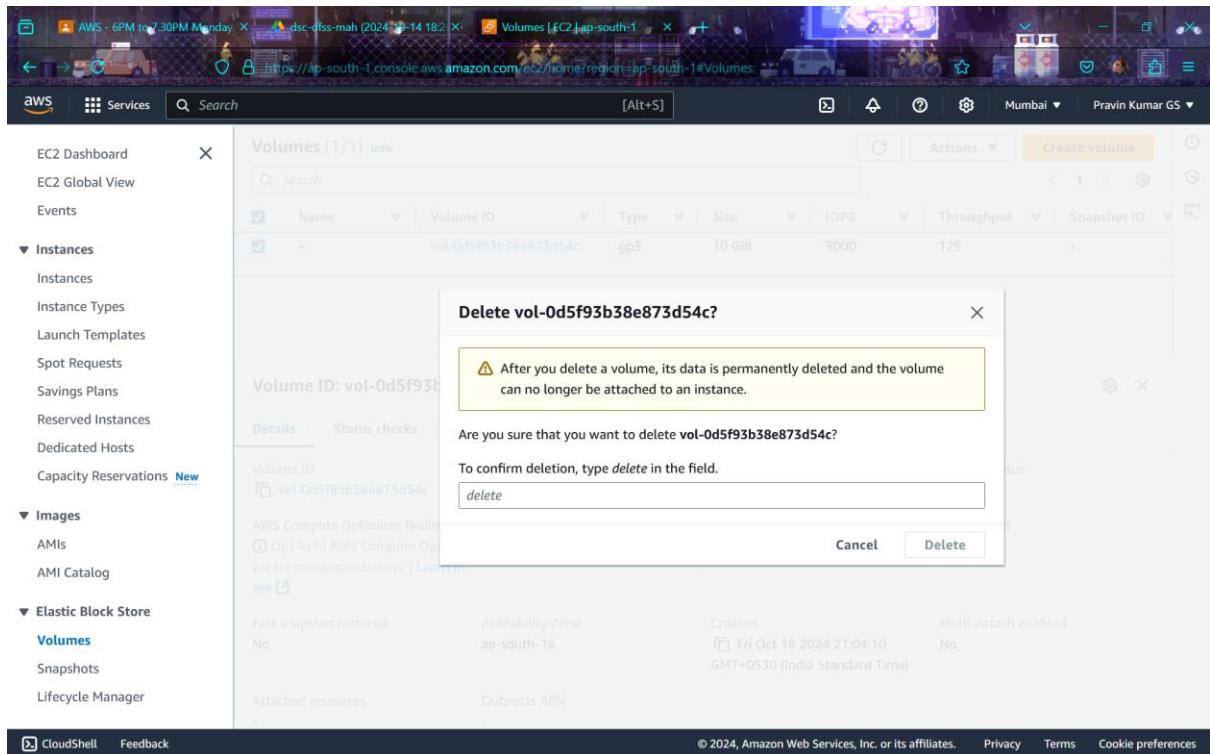
STEP 32: Confirming before deleting the snapshot for integrity purpose.

The screenshot shows the AWS EC2 Volumes page. A modal dialog box is open, asking for confirmation to delete a volume. The dialog contains the following text:
Delete vol-0d5f93b38e873d54c?
⚠ After you delete a volume, its data is permanently deleted and the volume can no longer be attached to an instance.
Are you sure that you want to delete vol-0d5f93b38e873d54c?
To confirm deletion, type *delete* in the field.
A text input field contains the word "delete".
Buttons at the bottom right of the dialog are "Cancel" and "Delete".

STEP 33: Yaay! You have deleted the snapshot.

The screenshot shows the AWS EC2 Instances page. A green success message banner at the top reads: "Successfully initiated termination (deletion) of i-01ab9d899b33544e1". The main table lists two terminated instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
22BET10027	i-01ab9d899b33544e1	Terminated	t2.micro	-	View alarms +
22BET10027	i-0b510ee593aca4999	Terminated	t2.micro	-	View alarms +



STEP 34: We will now stop the ‘EC2 Instance’. Go to the instance’s dashboard on the top a “instance state” option will be present. You get three options: stop, reboot instance and delete the instance. Here we will stop our instance.

The screenshot shows the AWS CloudShell interface. On the left, there is a sidebar with navigation links for EC2 Dashboard, EC2 Global View, Events, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots, Lifecycle Manager). The main content area has a green header bar indicating "Successfully deleted volume vol-0d5f93b38e873d54c." Below this is a table titled "Volumes" with columns for Name, Volume ID, Type, Size, IOPS, Throughput, and Snapshot ID. A message states "You currently have no volumes in this region." At the bottom of the main content area, there is a section titled "Fault tolerance for all volumes in this Region" and a "Snapshot summary" table showing "Recently backed up volumes / Total # volumes" as 0 / 1. The status is "Data Lifecycle Manager default policy for EBS Snapshots status" with a note "No default policy set up | Create policy". The footer of the CloudShell window includes links for CloudShell, Feedback, and various AWS terms like Privacy, Terms, and Cookie preferences.

CONCLUSION:

In this lab, we successfully created and managed an EBS volume in AWS. We attached the volume to an EC2 instance, formatted it, and mounted it to make it available for use. The experiment demonstrated how to handle persistent block storage using EBS, allowing us to store and retrieve data even after an instance is stopped or terminated.

We also explored fundamental operations such as creating a directory, mounting the volume, and verifying the available storage.

LAB EXPERIMENT – 3

AIM:

To explore the process of creating an EC2 instance in AWS, attaching and managing storage volumes, and understanding how to create and utilize both the EC2 instance and its associated storage volume.

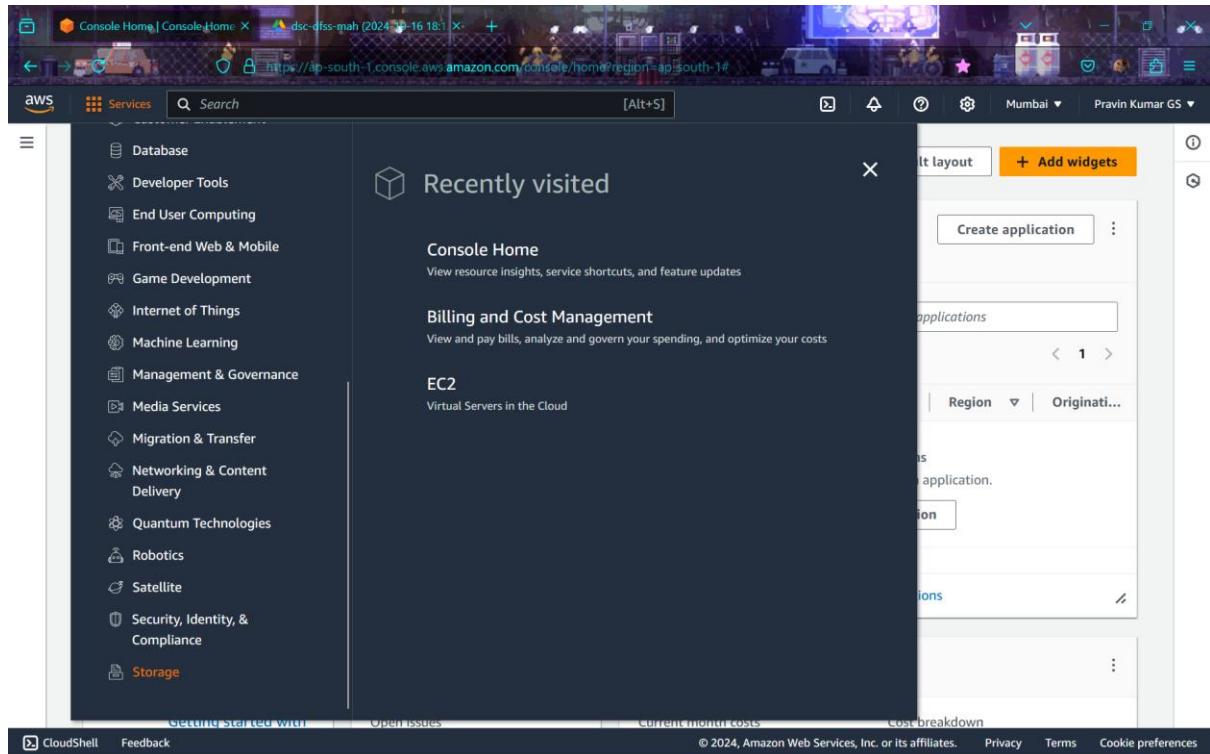
STEP 1: Login to your account on AWS Console; by adding root user email address and an account name follow the necessary instructions on screen and fill in your account details for billing information. After filling in the details, proceed to the login page and sign in using ‘root user email address’.

STEP 2:

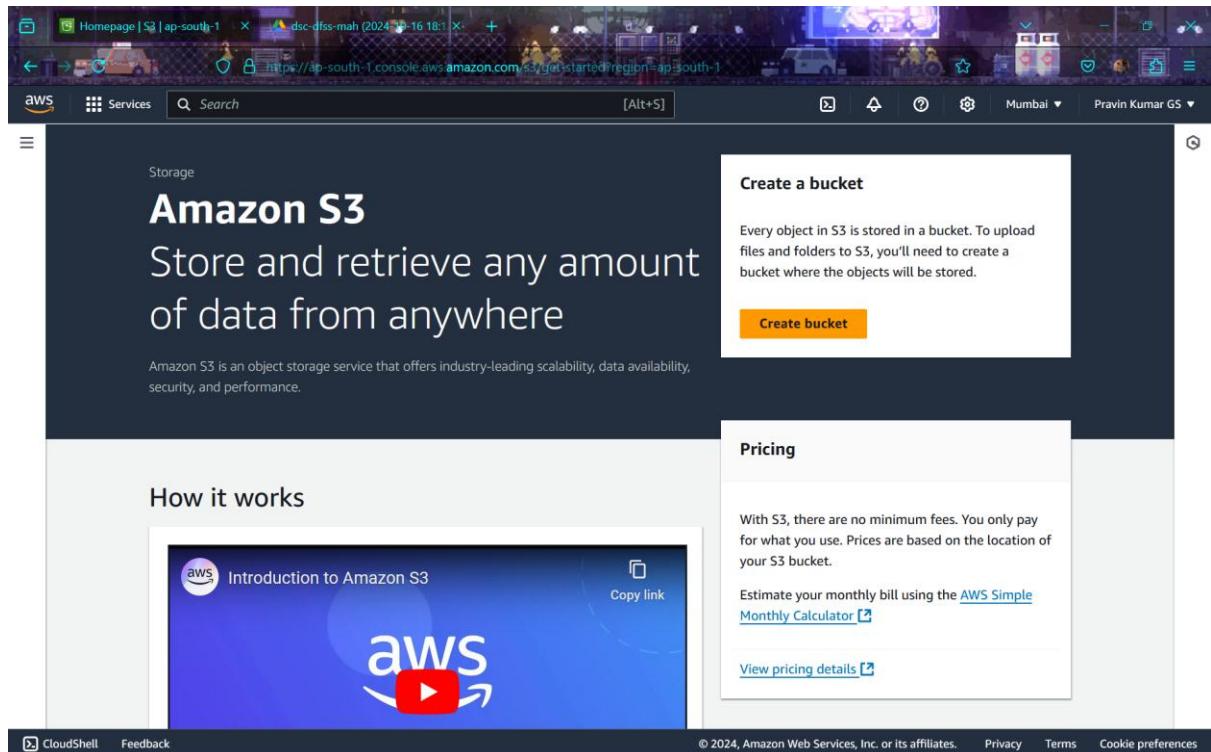
After logging-in you will be redirected to Console page, where you see the services option in the left corner, click on it.

STEP 3: Select storage in the shown list.

STEP 4: Under storage, you can see the S3 feature, click on it.

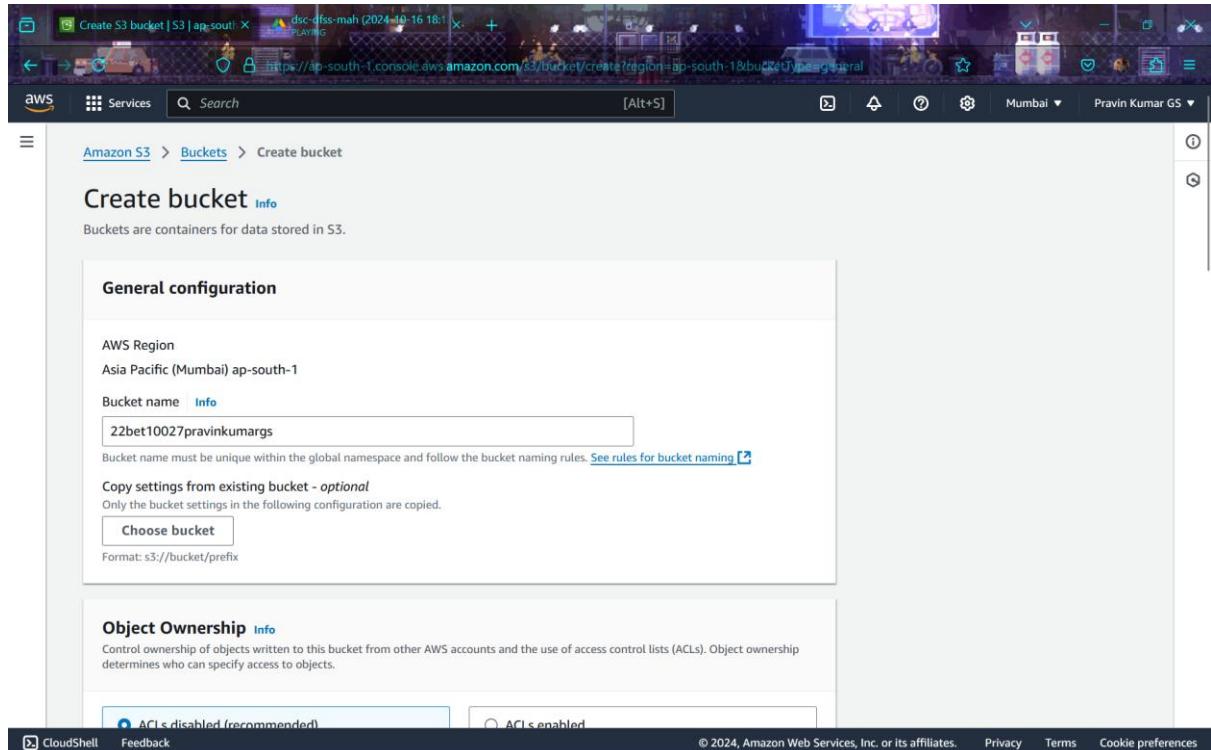


STEP 5: Now, you will be directed to creating a bucket page, press on the create bucket option.



The screenshot shows the Amazon S3 landing page. At the top right, there is a prominent orange "Create bucket" button. To its left, a text box explains that every object in S3 is stored in a bucket and provides instructions for uploading files and folders. Below this, there's a section titled "How it works" featuring a video thumbnail for "Introduction to Amazon S3". To the right of the video, there's a "Pricing" section stating that there are no minimum fees and providing links to the AWS Simple Monthly Calculator and pricing details. The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

STEP 6: You will be directed to creating bucket page fill the details.



The screenshot shows the "Create bucket" configuration page. The top navigation bar indicates the user is in the "Buckets" section. The main form is titled "General configuration". It includes fields for "Bucket name" (set to "22bet10027pravinkumargang"), "AWS Region" (set to "Asia Pacific (Mumbai) ap-south-1"), and a "Copy settings from existing bucket - optional" section. Below this is the "Object Ownership" section, which notes that ownership is disabled (recommended). At the bottom, there are two radio buttons for "ACLs": one selected for "ACLs disabled (recommended)" and one for "ACLs enabled". The footer contains standard AWS links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

STEP 7: Now, click the feature of block the public access.

The screenshot shows the AWS S3 console interface for creating a new bucket. The URL in the address bar is <https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general>. The main content area is titled "Object Ownership" with a sub-section "Block Public Access settings for this bucket". Under "Block all public access", several checkboxes are listed:

- 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.

STEP 8: Click create bucket for creating the bucket.

The screenshot continues from the previous step, showing the "Block Public Access settings for this bucket" section with the "Block all public access" checkbox checked. Below it, the "Bucket Versioning" section is partially visible. At the bottom of the page, there is a footer with links: CloudShell, Feedback, © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

STEP 9: Yaay!! You have successfully created the bucket.

The screenshot shows the AWS S3 Bucket Creation Wizard Step 3: Set Bucket Settings. The page title is "Create S3 bucket | S3 | ap-south-1". The URL is <https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general>. The top navigation bar includes "Services", "Search", "[Alt+S]", and user information "Mumbai" and "Pravin Kumar GS".

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

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

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

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS S3 Bucket Creation Wizard Step 4: Set Bucket Encryption. The page title is "Create S3 bucket | S3 | ap-south-1". The URL is <https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general>. The top navigation bar includes "Services", "Search", "[Alt+S]", and user information "Mumbai" and "Pravin Kumar GS".

Default encryption:
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type:
 Server-side encryption with Amazon S3 managed keys (SSE-S3)
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key:
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#).
 Disable
 Enable

Advanced settings

Note: After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel [Create bucket](#)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS S3 buckets page. At the top, a green banner displays the message: "Successfully created bucket '22bet10027pravinkumargs'". Below this, the "General purpose buckets" tab is selected, showing one bucket named "22bet10027pravinkumargs". The bucket details are listed as follows:

Name	AWS Region	IAM Access Analyzer	Creation date
22bet10027pravinkumargs	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	October 27, 2024, 17:25:51 (UTC+05:30)

At the bottom of the page, there are links for CloudShell, Feedback, and cookie preferences.

STEP 10: Now press the created bucket which is 22BET10027pravinkumargs and press upload button for uploading the file.

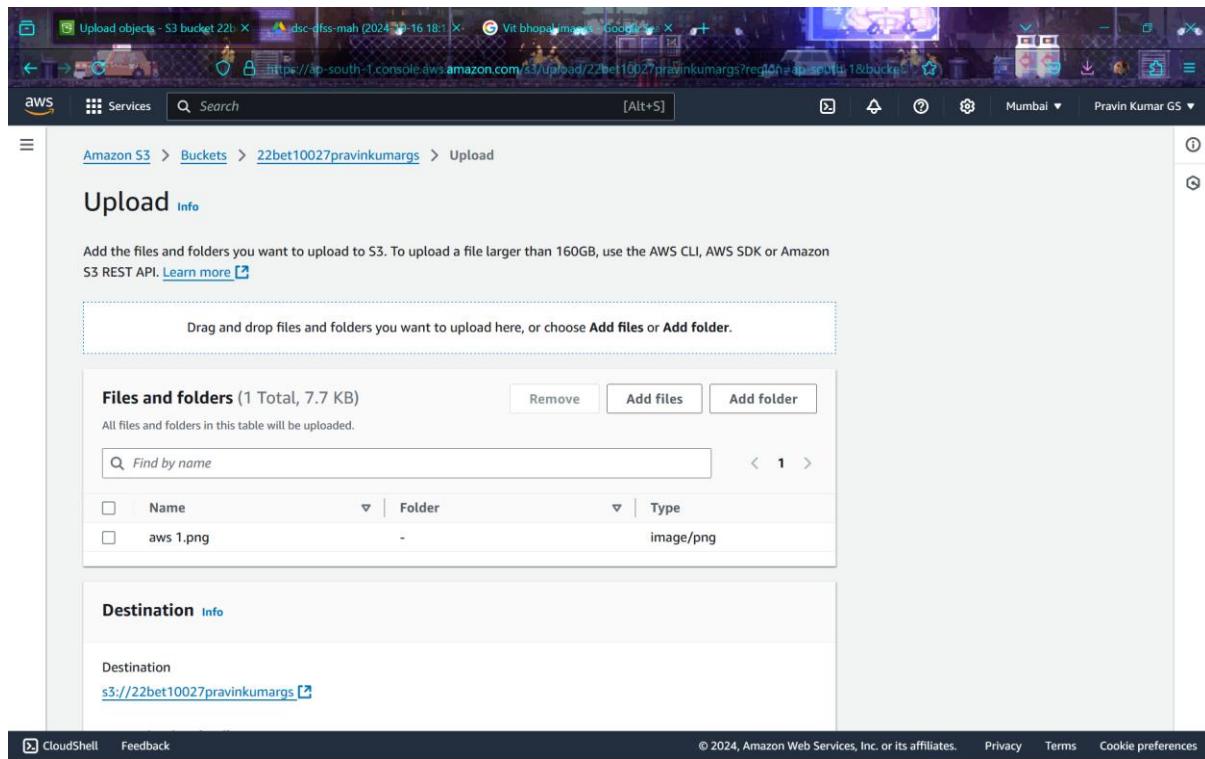
STEP 11: Press add files for inserting new files.

The screenshot shows the "Objects" tab of the "22bet10027pravinkumargs" bucket. The "Upload" button is highlighted. The "Actions" dropdown menu is open, showing options like Copy S3 URI, Copy URL, Download, Open, Delete, Create folder, and Upload.

Below the actions, a search bar and a "Show versions" checkbox are visible. A table lists objects, with the first column being "Name" and the second being "Type". The table header includes "Last modified", "Size", and "Storage class". A message at the bottom states: "No objects You don't have any objects in this bucket." There is also a "Upload" button at the bottom of the table.

At the bottom of the page, there are links for CloudShell, Feedback, and cookie preferences.

STEP 12: It will be redirecting you to File Explorer, where all your files will be stored in different locations, you can select your file. Here, I have uploaded a file name in the name of **aws 1.png**.



The screenshot shows the AWS S3 'Upload' interface. At the top, there's a breadcrumb navigation: Amazon S3 > Buckets > 22bet10027pravinkumargs > Upload. Below this, a large central area is titled 'Upload' with a 'Info' link. A placeholder text 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' is present. Below this is a table titled 'Files and folders (1 Total, 7.7 KB)'. The table has three columns: Name, Folder, and Type. One item is listed: 'aws 1.png' (Type: image/png). There are 'Remove', 'Add files', and 'Add folder' buttons above the table. To the right of the table is a search bar labeled 'Find by name' and navigation arrows. Below the table is a section titled 'Destination' with an 'Info' link. The destination URL is listed as 's3://22bet10027pravinkumargs'. At the bottom of the page are links for CloudShell, Feedback, and various legal and preference links.

STEP 14: Once you upload the file, then scroll down for storage class and select standard option.

The screenshot shows the AWS S3 console interface for creating a new bucket. The top navigation bar includes tabs for 'Upload objects - S3 bucket 22' and 'dsc-dfss-mah (2024-10-16 18:11)'. The main content area is titled 'Create bucket' with the URL <https://ap-south-1.console.aws.amazon.com/s3/upload/22bet002/pravinkumars?region=ap-south-1&bucket=dsc-dfss-mah>. The 'Storage class' section is open, showing a table with five rows:

Storage class	Designed for	Bucket type	Availability Zones	M
S3 Express One Zone	Single-digit millisecond response times for the most frequently accessed data.	Directory	1	-
Standard	Frequently accessed data (more than once a month) with milliseconds access	General purpose	≥ 3	-
Intelligent-Tiering	Data with changing or unknown access patterns	General purpose	≥ 3	-
Standard-IA	Infrequently accessed data (once a month) with milliseconds access	General purpose	≥ 3	31

At the bottom of the storage class table, there is a note: 'Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)'.

STEP 15: Scroll down and go for Server-side encryption and opt for Don't specify an encryption key, and follow the image instructions and customize the bucket.

STEP 16: After customizing the bucket, click on the upload button for uploading the bucket.

STEP 17: Yaay!! Successfully you have created a bucket.

The screenshot shows the AWS S3 console interface. At the top, there's a green success message: "Upload succeeded" with a link to "View details below." Below this, the title "Upload: status" is displayed with a "Close" button. A note says, "The information below will no longer be available after you navigate away from this page." The main section is titled "Summary" and shows the destination "s3://22bet10027pravinkumargs" with one succeeded file: "aws bucket pic" (7.7 KB, 100.00%). There are tabs for "Files and folders" (selected) and "Configuration". Under "Files and folders", there's a table with one item: "aws bucket pic" (image/png, 7.7 KB, Succeeded). The bottom of the screen includes standard AWS links like CloudShell, Feedback, and copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates." and links for Privacy, Terms, and Cookie preferences.

STEP 18: Now you see a file under Files and Folders option, a file named as aws bucket pic, which we have uploaded it in the Step 12.

STEP 19: After clicking on the file, it be directed to its properties.

STEP 20: Click on the open function, which will be opening in a new tab.

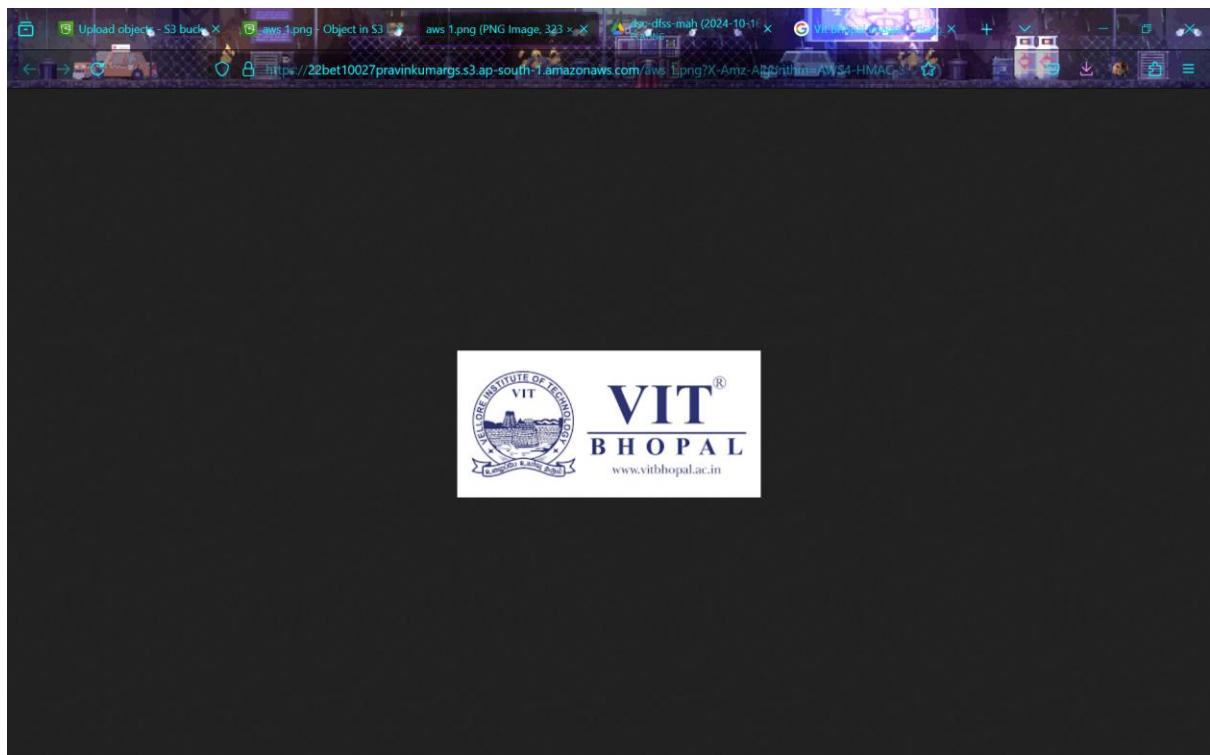
The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with various options like Buckets, Storage Lens, and Feature spotlight. The main area displays the properties of an object named 'aws 1.png'. The object overview section shows the following details:

Object overview	
Owner 7c85c7b49a676b428ecc03127d4d5139268e99699de75eedfe95e5f21b365744	S3 URI s3://22bet10027pravinkumargs/aws 1.png
AWS Region Asia Pacific (Mumbai) ap-south-1	Amazon Resource Name (ARN) arn:aws:s3:::22bet10027pravinkumargs/aws 1.png
Last modified October 27, 2024, 17:35:32 (UTC+05:30)	Entity tag (Etag) 77b5ba38b4eb7e70dfe3496e4ef983b8
Size 7.7 KB	Object URL https://22bet10027pravinkumargs.s3.ap-south-1.amazonaws.com/aws+1.png
Type png	

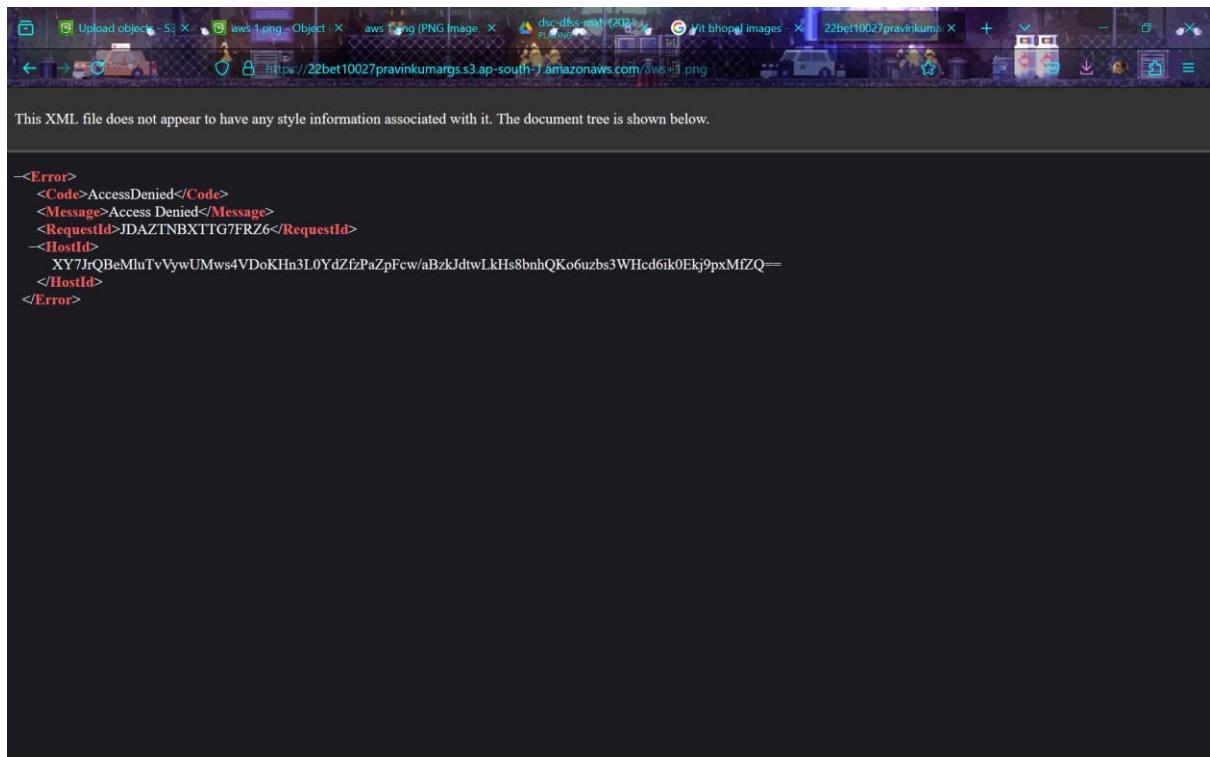
At the bottom of the page, there are links for AWS Marketplace for S3, CloudShell, and Feedback, along with copyright information: © 2024, Amazon Web Services, Inc. or its affiliates.

STEP 21: The uploaded file is opened in a new tab and this is the picture.

STEP 22: Now again go to properties section and copy the url for sharing with someone.



STEP 23: It wont open as we didn't give access to public, the bucket was created as private.



STEP 24: Now go to buckets, and change the settings from private to public.

STEP 25: Click on the bucket which was created in the name of 22bet10027pravinkumargs.

A screenshot of the AWS S3 console. The left sidebar shows navigation options like 'Upload objects', 'Access Grants', 'Access Points', etc. The main area shows the '22bet10027pravinkumargs' bucket details. The 'Objects' tab is selected, showing one object named 'aws 1.png'. The object details are: Name: aws 1.png, Type: png, Last modified: October 27, 2024, 17:35:32 (UTC+05:30), Size: 7.7 KB, Storage class: Standard.

STEP 26: You will be directed to this page and select the permissions for giving access to public.

STEP 27: Go to edit feature where the Block public access is in On.

The screenshot shows the AWS S3 console with the 'Permissions' tab selected. In the 'Block public access (bucket settings)' section, the 'On' checkbox is checked. Below it, there is a link to 'Individual Block Public Access settings for this bucket'. At the bottom of the page, there is a 'Bucket policy' section with an 'Edit' button.

STEP 28: Deselect all the ticks in this step for giving access to public and press save changes option.

Edit Block public access (bucket settings)

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets 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 29: After saving the changes, type delete for confirming the changes.

Edit Block public access (bucket settings)

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets 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.

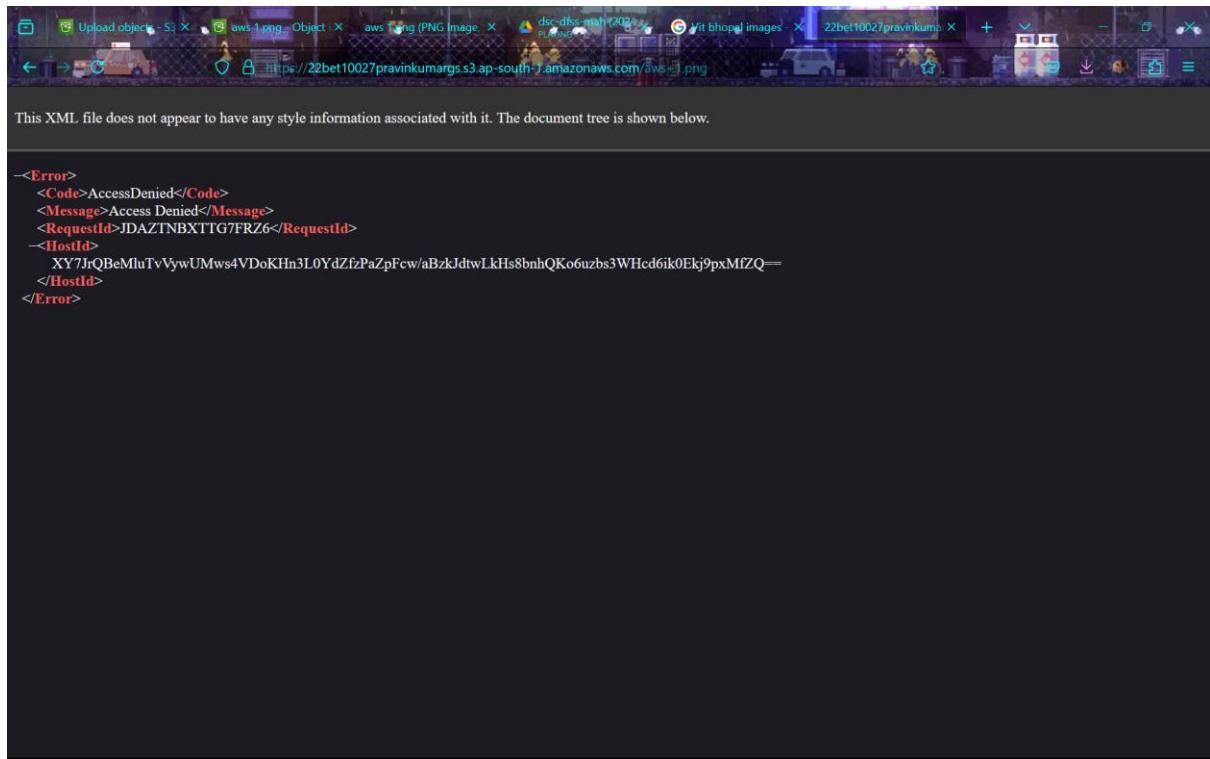
Block public and cross-account access to buckets and objects through any public bucket or access point policies

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

STEP 30: Yaay!! Successfully completed the change of the access to the public access from private access.

STEP 31: Go to bucket policy and select edit option.

The screenshot shows the AWS S3 console interface. The left sidebar has sections like Buckets, Storage Lens, and Feature spotlight. The main content area shows the bucket '22bet10027pravinkumargs' under 'Amazon S3 > Buckets'. The 'Permissions' tab is selected. A green success message at the top says 'Successfully edited Block Public Access settings for this bucket.' Below it, the 'Permissions overview' section includes an 'Access finding' section with a link to 'How IAM analyzer findings work' and a 'View analyzer for ap-south-1' button. The 'Block public access (bucket settings)' section contains a toggle switch labeled 'Block all public access' which is set to 'Off'. An 'Edit' button is located in the top right corner of this section. At the bottom, there are links for 'AWS Marketplace for S3', 'CloudShell', and 'Feedback', along with copyright information and links for 'Privacy', 'Terms', and 'Cookie preferences'.



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

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>JDAZTNBXTT7FRZ6</RequestId>
<HostId>
XY7JrQBeMluTvVywUMws4VDoKHn3L0YdZfzPaZpFew/aBzkJdtwLkHs8bnhQKo6uzbs3WHcd6ik0Ekj9pxMfZQ==
</HostId>
</Error>
```

STEP 32: Now got to Add new statement.

STEP 33: This is the default code.

STEP 34: Edit the statement as below.

The screenshot shows the AWS S3 Bucket Policy editor. On the left, there's a sidebar with 'Buckets' selected, showing options like Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. Below that is a section for Block Public Access settings for this account. Under 'Storage Lens', there are links for Dashboards, Storage Lens groups, and AWS Organizations settings. At the bottom of the sidebar is a 'Feature spotlight' section with a link to 'AWS Marketplace for S3'. The main area is titled 'Bucket policy' and contains a JSON code editor. The code is as follows:

```
1▼ {
2    "Version": "2012-10-17",
3    "Statement": [
4        {
5            "Sid": "Statement1",
6            "Principal": "*",
7            "Effect": "Allow",
8            "Action": []
9        }
10   ]
11 }
```

To the right of the code editor is a panel for editing statements. It shows 'Statement1' with a 'Remove' button. Below it is a 'Add actions' section with a 'Choose a service' dropdown containing 'Filter services', 'Available' (AMP, API Gateway, API Gateway V2, ASC), and 'Included' (S3). The status bar at the bottom indicates '© 2024, Amazon Web Services, Inc. or its affiliates.' and includes links for Privacy, Terms, and Cookie preferences.

STEP 35: Copy the bucket arn and paste it in the resource row.

STEP 36: Type the following code and save the changes

This screenshot is identical to the previous one, but the JSON code in the editor has been modified. The 'Action' array now contains the 's3:GetObject' action, indicating that the policy now allows getting objects from the bucket. The rest of the policy remains the same.

```
1▼ {
2    "Version": "2012-10-17",
3    "Statement": [
4        {
5            "Sid": "Statement1",
6            "Principal": "*",
7            "Effect": "Allow",
8            "Action": "s3:GetObject"
9        }
10   ]
11 }
```

The screenshot shows the AWS S3 Bucket Policy editor. On the left, there's a sidebar with navigation links like 'Buckets', 'Storage Lens', and 'Feature spotlight'. The main area is titled 'Bucket policy' and contains a JSON code editor. The JSON code is as follows:

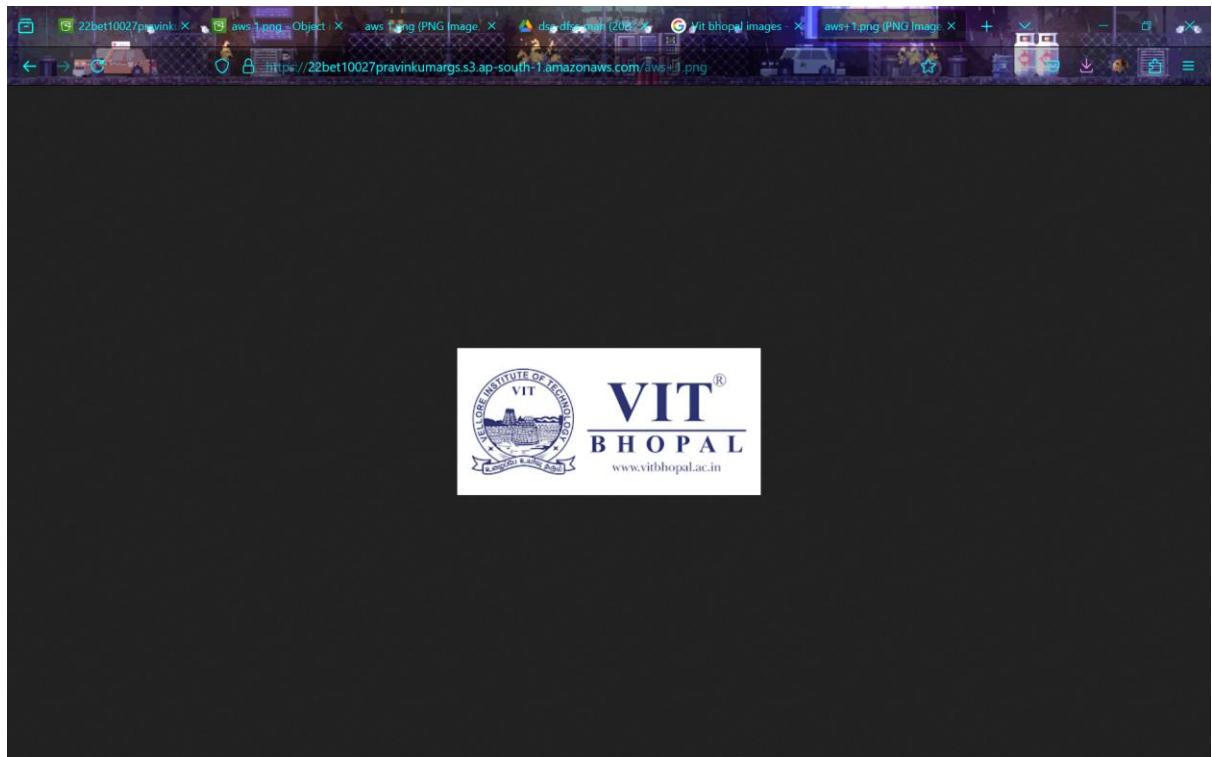
```
1  {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "Statement1",
6             "Principal": "*",
7             "Effect": "Allow",
8             "Action": "S3:GetObject",
9             "Resource": "arn:aws:s3:::22bet10027pravinkumargs/*"
10        }
11    ]
12 }
```

To the right of the code editor, there are sections for 'Edit statement Statement1', 'Remove', 'Add actions', 'Choose a service', 'Included S3', and 'Available AMP API Gateway'. At the bottom, there are links for 'AWS Marketplace for S3', 'CloudShell', and 'Feedback'.

STEP 37: Yaay!! Successfully completed the changes and you can see the Block all the public access as turned off.

The screenshot shows the AWS S3 Bucket Permissions overview page for the bucket '22bet10027pravinkumargs'. The top navigation bar includes 'Amazon S3', 'Services', 'Search', and 'Mumbai'. The main content area has tabs for 'Objects', 'Properties', 'Permissions' (which is selected), 'Metrics', 'Management', and 'Access Points'. A green success message at the top says 'Successfully edited bucket policy.' Below the tabs is a 'Permissions overview' section with 'Access finding' information. Under the 'Permissions' tab, there's a 'Block public access (bucket settings)' section with an 'Edit' button. It explains that public access is granted through ACLs, bucket policies, or access point policies. It also notes that turning on 'Block all public access' will block access to all objects in the bucket. There's a link to 'Learn more' about this setting. At the bottom, there's a 'Block all public access' toggle switch set to 'Off'. The footer includes links for 'AWS Marketplace for S3', 'CloudShell', 'Feedback', and standard AWS footer links.

STEP 38: Now with the copied url, refresh the page you can see the image, as it is changed to public access you have access to use it.



STEP 39: Now again press the bucket which is 22BET10027 and press upload button for uploading the file.

STEP 40: Click on the upload option and upload the file from your device.

STEP 41: Already we have stored one file, now after changing the file name with the same pic and the format click upload.

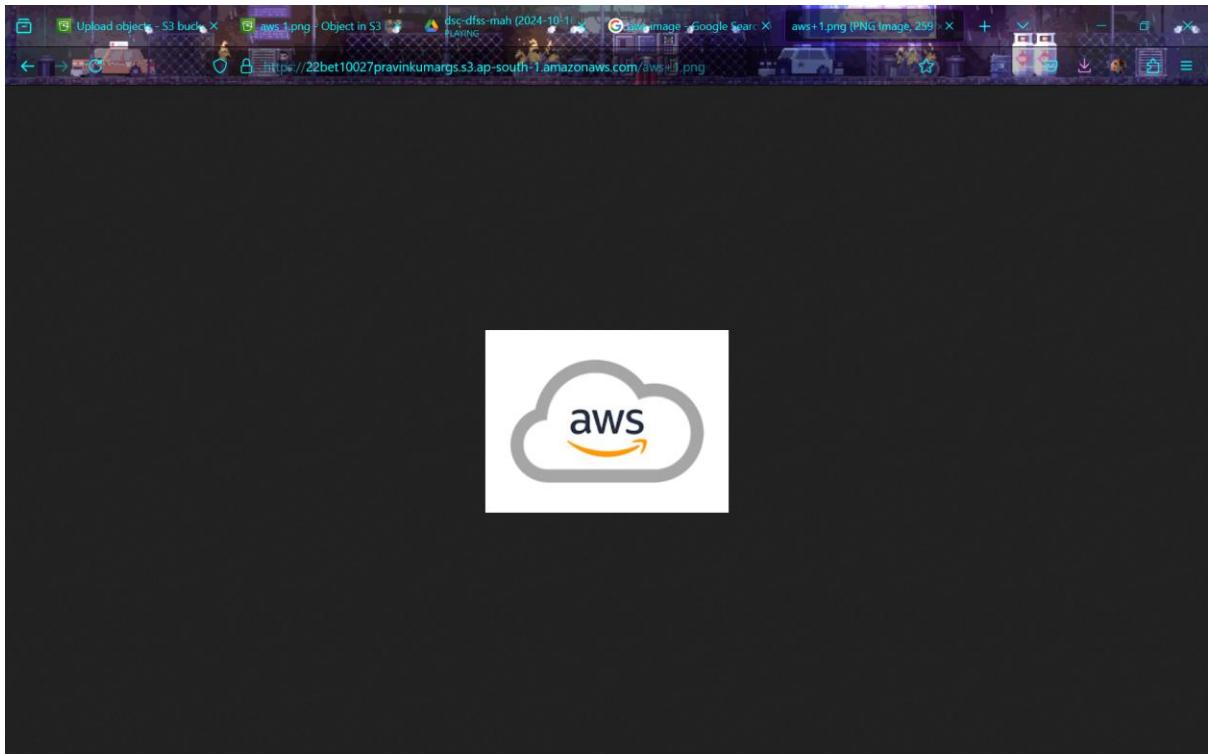
STEP 42: Select the file aws bucket pic which in the png format.

STEP 43: Once you upload the file, click on the upload option.

The screenshot shows the AWS S3 'Upload objects - S3' interface. The user is uploading a file named 'aws 1.png' to the bucket '22bet10027pravinkumargs'. The 'Upload' step is active, showing a drag-and-drop area and a file list table. The table contains one item: 'aws 1.png' (Type: image/png). Below the table is a 'Destination' section with the URL 's3://22bet10027pravinkumargs'. The bottom navigation bar includes CloudShell, Feedback, and links to AWS terms and privacy.

STEP 44: Yaay!! Successfully you have uploaded the file.

The screenshot shows the AWS S3 'Upload: status' interface after the upload was completed. A green success message at the top states 'Upload succeeded' and 'View details below.' The 'Summary' section shows the destination 's3://22bet10027pravinkumargs' and upload results: 'Succeeded' (1 file, 3.7 KB (100.00%)) and 'Failed' (0 files, 0 B (0%)). The 'Files and folders' section lists the uploaded file 'aws 1.png' (image/png, 3.7 KB, Status: Succeeded). The bottom navigation bar includes CloudShell, Feedback, and links to AWS terms and privacy.



STEP 45: Click on the bucket which is saved as 22bet10027pravinkumargs.

STEP 46: Go into the object which is saved as aws 1.png.

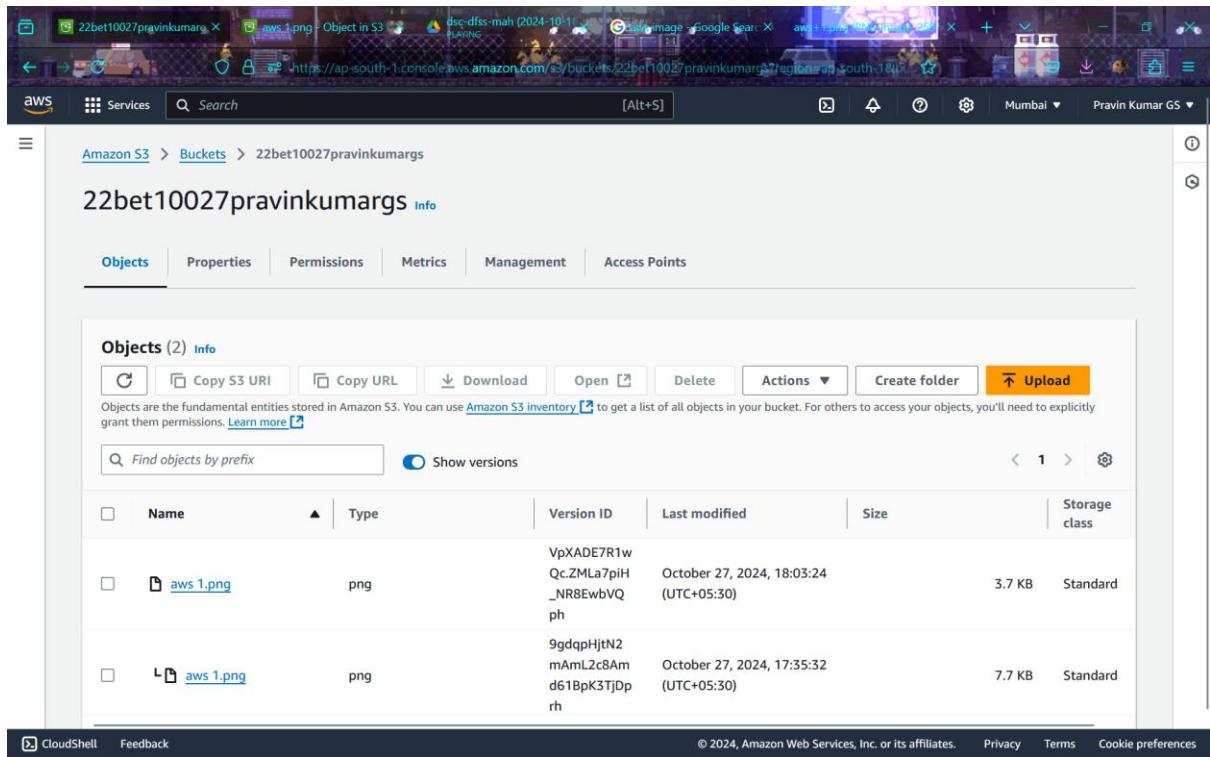
STEP 47: It will be redirected to properties page, go to versions.

STEP 48: Two versions are there of the same file name and same file format and click on the open which will be opening in new tab.

STEP 49: If you have noticed it, the picture has been changed once you reload the page though it's in the same file name and file format.

STEP 50: Click on the versions, so you can see the multiple versions of the file.

You can identify with version ids. If you upload the same file with different name, it will consider as a different file, it won't be coming under version



STEP 51: Now again press the bucket which is 22bet10027pravinkumargs and press upload button for uploading the file.

STEP 52: Click on the upload option for uploading a new file.

STEP 53: Upload a new file from your device.

STEP 54: Click on the file what you are going to upload, here we are going to upload this aws logo file.

STEP 55: After uploading your file, click on the upload button.

STEP 56: you have uploaded the file.

STEP 57: Select the file which as uploaded here, aws logo pic.png.

And open the picture, which will be opened in new tab. If you notice the picture is same though the file name is different.

STEP 58: Go to versions page and you can't see any versions as we have changed the file name with the same picture

STEP 59: Click on the management and see the different versions.

The screenshot shows the AWS S3 console interface. At the top, there are several tabs and a search bar. Below the navigation bar, the path 'Amazon S3 > Buckets > 22bet10027pravinkumargs' is displayed. The main content area is titled 'Objects (2)'. It lists two objects: 'aws_1.png' and 'aws.png'. Both are of type 'png' and have a storage class of 'Standard'. The 'aws_1.png' object was last modified on October 27, 2024, at 18:03:24 (UTC+05:30), while 'aws.png' was last modified on October 27, 2024, at 18:06:11 (UTC+05:30). The 'Actions' dropdown menu is highlighted with a yellow box. The bottom of the screen includes standard AWS footer links like CloudShell, Feedback, and Copyright information.

Name	Type	Last modified	Size	Storage class
aws_1.png	png	October 27, 2024, 18:03:24 (UTC+05:30)	3.7 KB	Standard
aws.png	png	October 27, 2024, 18:06:11 (UTC+05:30)	3.7 KB	Standard

Objects (3) [Info](#)

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

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](#)

Name	Type	Version ID	Last modified	Size	Storage class
aws 1.png	png	VpXADE7R1wQc.ZMLa7piH_NR8EwbVQph	October 27, 2024, 18:03:24 (UTC+05:30)	3.7 KB	Standard
aws 1.png	png	9gdqphijtN2mAmL2c8Amd61BpK3TjDprh	October 27, 2024, 17:35:32 (UTC+05:30)	7.7 KB	Standard
aws.png	png	yERDKqPO9qYBeOBuo1Yh_rHdR2Gj3xX	October 27, 2024, 18:06:11 (UTC+05:30)	3.7 KB	Standard

STEP 60: As you will be redirected to management page and press on the create life cycle.

STEP 61: Follow the instructions and finish the creating life cycle rule.

Lifecycle rules

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

Lifecycle rule n...	Status	Scope	Current version ...	Noncurrent vers...	Expired object ...	Incomplete mu...
No lifecycle rules						

Create lifecycle rule

Replication rules (0)

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. [Learn more](#)

Replication	Destination	Destination	...	Replica	Replication

STEP 62: Now click on the create rule.

The screenshot shows the 'Create lifecycle rule' configuration page in the AWS S3 console. The 'Lifecycle rule configuration' section is active. A 'Lifecycle rule name' input field contains 'pravinkumargs'. Under 'Choose a rule scope', the radio button for 'Limit the scope of this rule using one or more filters' is selected. The 'Filter type' section includes a 'Prefix' input field with 'Enter prefix' placeholder text and a note about avoiding certain characters in key names. The 'Object tags' section notes that key/value pairs can be added below. At the bottom, there are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

STEP 63: Now we are going to delete the objects which are inside in the bucket.

The screenshot shows the 'Lifecycle rule actions' configuration page. It lists several actions: 'Transition current versions of objects between storage classes', 'Transition noncurrent versions of objects between storage classes', 'Expire current versions of objects', 'Permanently delete noncurrent versions of objects', and 'Delete expired object delete markers or incomplete multipart uploads'. Below this is a 'Review transition and expiration actions' section showing 'Current version actions' and 'Noncurrent versions actions', both of which show 'Day 0' and 'No actions defined.' At the bottom right are 'Cancel' and 'Create rule' buttons.

The screenshot shows the AWS S3 console interface. At the top, there are several tabs and a search bar. Below the navigation bar, the path 'Amazon S3 > Buckets > 22bet10027pravinkumargs' is visible. The main area is titled 'Objects (2)'. A table lists two objects:

Name	Type	Last modified	Size	Storage class
aws 1.png	png	October 27, 2024, 18:03:24 (UTC+05:30)	3.7 KB	Standard
aws.png	png	October 27, 2024, 18:06:11 (UTC+05:30)	3.7 KB	Standard

At the bottom of the page, there are links for CloudShell, Feedback, and a copyright notice: © 2024, Amazon Web Services, Inc. or its affiliates.

STEP 64: Type delete word on the dialogue box for the confirmation before deleting the objects.

The screenshot shows the 'Delete objects' dialog box. It contains a warning message: "⚠ 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." Below this is a note: " ⓘ Deleting the specified objects adds delete markers to them. If you need to undo the delete action, you can delete the delete markers." The 'Specified objects' section shows the same two objects listed earlier. At the bottom, there is a 'Delete objects?' confirmation button.

The screenshot shows the AWS S3 console interface. At the top, there are several tabs and a search bar. Below the tabs, a message states: "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." A link to "Learn more" is provided. A note below says: "Deleting the specified objects adds delete markers to them. If you need to undo the delete action, you can delete the delete markers." Another link to "Learn more" is shown. The main section is titled "Specified objects" and contains a table with two rows:

Name	Type	Last modified	Size
aws 1.png	png	October 27, 2024, 18:03:24 (UTC+05:30)	3.7 KB
aws.png	png	October 27, 2024, 18:06:11 (UTC+05:30)	3.7 KB

Below this is a "Delete objects?" dialog box. It contains a text input field with the value "delete". At the bottom right are "Cancel" and "Delete objects" buttons.

STEP 65: Yaay!! You have successfully deleted the objects.

The screenshot shows the AWS S3 console after the deletion process. A green header bar indicates "Successfully deleted objects". Below it, a message says: "The information below will no longer be available after you navigate away from this page." The "Summary" section shows the following data:

Source	Successfully deleted	Failed to delete
s3://22bet10027pravinkumargs	2 objects, 7.3 KB	0 objects

Below the summary is a "Failed to delete" tab, which is currently active. It displays a message: "Failed to delete (0)". A table below shows the failed deletion details:

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

At the bottom, there are standard navigation links: CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

The screenshot shows the AWS S3 Buckets page. At the top, there's an account snapshot section with a link to 'View Storage Lens dashboard'. Below it, there are tabs for 'General purpose buckets' and 'Directory buckets', with 'General purpose buckets' selected. A search bar allows you to 'Find buckets by name'. A table lists the bucket details:

Name	AWS Region	IAM Access Analyzer	Creation date
22bet10027pravinkumargs	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	October 27, 2024, 17:25:51 (UTC+05:30)

At the bottom right of the table are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'. The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

STEP 67: Before deleting the bucket, type the bucket name for the confirmation.

The screenshot shows the 'Delete bucket' confirmation dialog. It displays a message: 'This bucket is not empty. Buckets must be empty before they can be deleted.' There is a 'Empty bucket' button. Below this, a question asks 'Delete bucket "22bet10027pravinkumargs"?'. A text input field contains the bucket name '22bet10027pravinkumargs'. At the bottom are 'Cancel' and 'Delete bucket' buttons.

STEP 68: Now we are going to empty the bucket, its important we have to empty the bucket, before deleting the bucket. Here we have to type permanently delete for emptying the bucket.

The screenshot shows the 'Empty bucket' dialog box for the S3 bucket '22bet10027pravinkumargs'. It includes a warning about deleting all objects, a lifecycle rule configuration link, and a text input field for confirming deletion with the text 'permanently delete'. A large orange 'Empty' button is at the bottom right.

STEP 69: Yaay!! You have successfully emptied the bucket.

The screenshot shows the 'Empty bucket: status' page after the deletion. It displays a summary table with successful and failed deletions and a 'Failed to delete (0)' section showing no results.

Source	Successfully deleted	Failed to delete
s3://22bet10027pravinkumargs	5 objects, 15.0 KB	0 objects

STEP 70: Now we are going to delete the bucket.

The screenshot shows the AWS S3 Buckets page. At the top, there is an account snapshot and a 'View Storage Lens dashboard' button. Below that, there are tabs for 'General purpose buckets' and 'Directory buckets', with 'General purpose buckets' selected. A table lists one bucket: '22bet10027pravinkumargs'. The table has columns for Name, AWS Region, IAM Access Analyzer, and Creation date. The bucket details are: Name - 22bet10027pravinkumargs, AWS Region - Asia Pacific (Mumbai) ap-south-1, IAM Access Analyzer - View analyzer for ap-south-1, and Creation date - October 27, 2024, 17:25:51 (UTC+05:30). Action buttons for the row include 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

STEP 71: Before deleting the bucket, type the bucket name for the confirmation.

The screenshot shows the 'Delete bucket' confirmation dialog. It includes a warning message about the不可逆性 of deleting a bucket and a text input field where the bucket name '22bet10027pravinkumargs' is typed. There are 'Cancel' and 'Delete bucket' buttons at the bottom.

Step 72: Yaay!! You have successfully deleted the bucket.

The screenshot shows the AWS S3 service page. At the top, there is a green banner with the message "Successfully deleted bucket '22bet10027pravinkumargs'". Below this, the main heading is "Amazon S3" with the subtext "Store and retrieve any amount of data from anywhere". A descriptive paragraph explains that Amazon S3 is an object storage service. To the right, there is a "Create a bucket" section with a button and a brief explanation. Further down, there is a "How it works" section featuring a video thumbnail titled "Introduction to Amazon S3" and a "Pricing" section with a link to the monthly calculator. The bottom navigation bar includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.