

Index

No	Title	Page No.
1	Study and implementation of Infrastructure as a Service	3
2	Study and implementation of Platform as a Service	29
3	Study and implementation of Software as a Service	35
4	Study and implementation of Storage as a Service	53
5	User Management in Cloud	59
6	Study and implementation of Identity and Access Management	65
7	Study and implementation of MFA in the environment of Popular Cloud service provider	79
8	Write a Program for Web Feed	86
9	Study and implementation of Single-sign-on (SSO)	95
10	Case Study on Google Cloud	f

Practical No. 1

Aim: Study and implementation of Infrastructure as a Service

Theory: IaaS is also known as **Hardware as a Service (HaaS)**. It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per use model.

In traditional hosting services, IT infrastructure was rented out for a specific period of time, with pre-determined hardware configuration. The client paid for the configuration and time, regardless of the actual use. With the help of the IaaS cloud computing platform layer, clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used.

IaaS provider provides the following services -

1. **Compute:** Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end-users.
2. **Storage:** IaaS provider provides back-end storage for storing files.
3. **Network:** Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
4. **Load balancers:** It provides load balancing capability at the infrastructure layer.

There are the following advantages of IaaS computing layer -

1. Shared infrastructure

IaaS allows multiple users to share the same physical infrastructure.

2. Web access to the resources

IaaS allows IT users to access resources over the internet.

3. Pay-as-per-use model

IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.

4. Focus on the core business

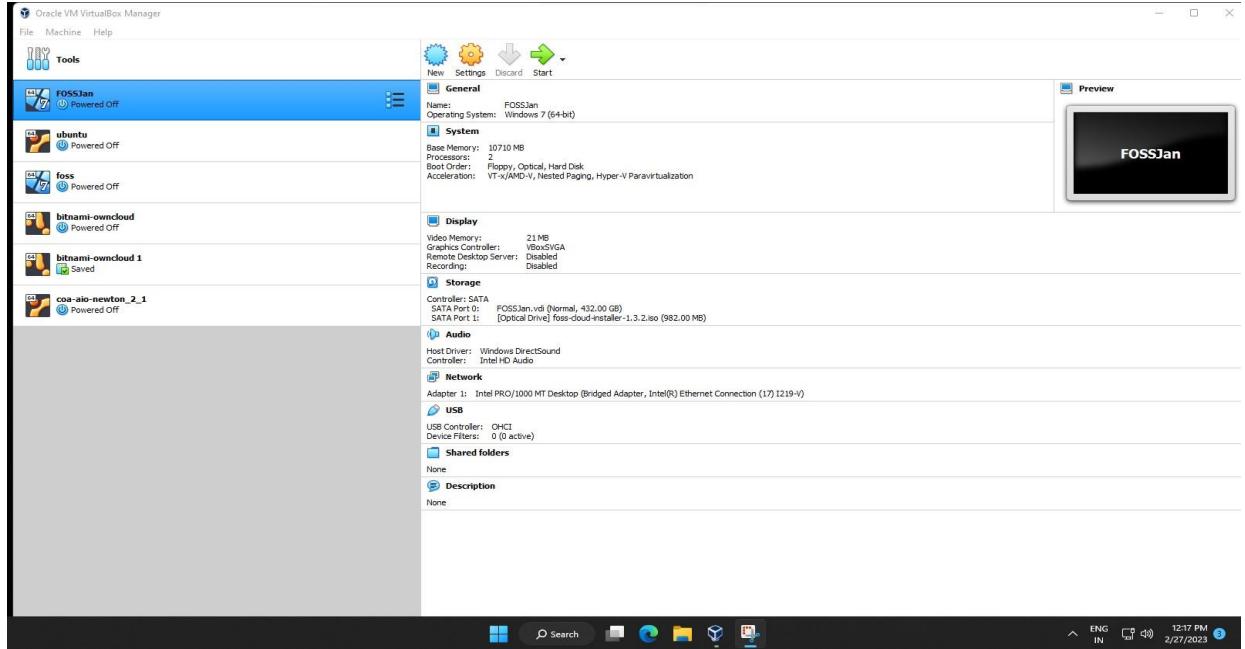
IaaS providers focus on the organization's core business rather than on IT infrastructure.

5. On-demand scalability

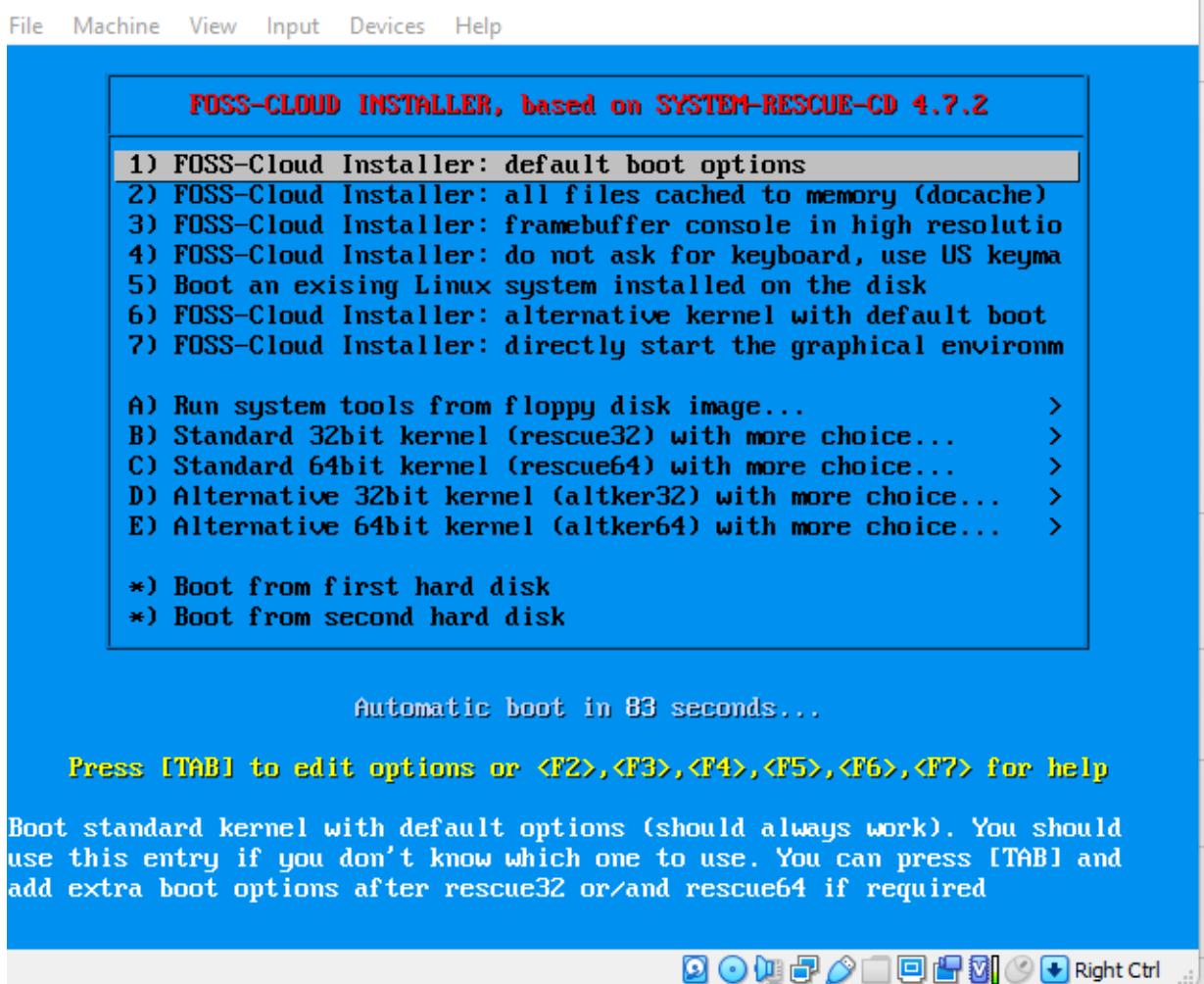
On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

Methods and Steps:

A. Using FOSS Demo / FOSS Server. INSTALLATION:



File Machine View Input Devices Help



Boot standard kernel with default options (should always work). You should use this entry if you don't know which one to use. You can press [TAB] and add extra boot options after rescue32 or/and rescue64 if required

```
FOSSJan [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

installer v1.3.2

Copyright (C) 2010 – 2023 FOSS-Group
http://www.foss-group.de

+---+
|   Welcome to the FOSS-Cloud-Installer
+---+
The installer comes WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND,
either expressed or implied.

Do you want to start the installation?
yes or no?: yes
```

```
FOSSJan [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

+---+
|   Node Type Selection
+---+
The Installer supports four different types of servers:
- The Demo-System which lets you quickly install and test the
FOSS-Cloud on a single machine without any further network
requirements.
- The Single-Server which runs the whole FOSS-Cloud on
a single physical server, without any high availability.
- The VM-Node which hosts the virtual machines in a multi node setup
(requires at least four physical servers).
- The Storage-Node which serves the images of the virtual machines
in a multi node setup (requires at least four physical servers).

Please enter the number of the server type you would like to install
1) Demo-System
2) Single-Server
3) VM-Node (multi node setup)
4) Storage-Node (multi node setup)
Node type: 1_
```

```

+-----+
| Installation Device Selection |
+-----+
A dedicated SCSI, SATA or PATA disk is required for the installation
The disk has to be at least 130 GB in size

Found sda (432 GB). Size is OK

Below you will find a list of all detected and supported disks
sda (432 GB)

Please enter the device name on which you would like to install
Device: sda

```

[Icons: Volume, File, Print, Copy, Paste, Find, Replace, Undo, Redo, Right Ctrl, etc.]


```

+-----+
| Logical Volume Cleanup and Preparation |
+-----+
Checking for existing volume groups and physical volumes

Found existing FOSS-Cloud related physical volumes for
volume group local0:
/dev/sda5

Those are most likely leftovers from a previous installation
In order to continue those volume groups and physical volumes
have to be removed
THIS MEANS THAT ALL LVM META DATA WILL BE LOST
Do you want to continue?
yes or no?: yes_

```

[Icons: Volume, File, Print, Copy, Paste, Find, Replace, Undo, Redo, Right Ctrl, etc.]

FOSSJan [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help


```

+-----+
| Installation Device Partitioning |
+-----+
Below is the existing partition layout of your selected device

Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sda: 464GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start    End     Size   Type      File system    Flags
 1       1049kB  67.1MB  66.1MB primary    ext4          boot
 2       67.1MB   4362MB  4295MB primary    linux-swap(v1)
 3       4362MB   8657MB  4295MB primary    xfs
 4       8657MB   464GB   455GB  extended
                                         lba
 5       8658MB   464GB   455GB  logical
                                         lvm

All existing partitions have to be deleted in order to continue
THIS MEANS THAT ALL DATA ON THIS DISK WILL BE LOST
Do you want to continue?
yes or no?: yes_

```

[Icons: Volume, File, Print, Copy, Paste, Find, Replace, Undo, Redo, Right Ctrl, etc.]

FOSSJan [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse.

Stage4 Installation

Unpacking stage4 tarball
This will take a while - please be patient

Unpacking of stage4 tarball was successful

Network Device Selection

Please enter the device which you would like to use

Available ethernet devices: enp0s3
Device #0: enp0s3

Network Configuration

Do you want to use automatic network configuration (via DHCP)?
yes or no?: no

```
+--+
|   Installation Complete
+--+
Congratulation! You have finished the installation of FOSS-Cloud
Now all you need to do is reboot the system and remove the CD-ROM

Do you want to reboot your system?
yes or no?: no
```

FOSSJan [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse. Device #0: enp0s3

+-----+
| Network Configuration |
+-----+
Do you want to use automatic network configuration (via DHCP)?
yes or no?: no
OK, you will have to configure your network manually

+-----+
| Network Host Name Configuration |
+-----+
Please enter the host name for your node (without the domain)
Host name: ashutosh478

+-----+
| Network Configuration for the 'pub' Network |
+-----+
Please enter the domain name for the 'pub' interface
Domain name: ashutosh.com_
```

FOSSJan [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
Please enter the IP address of your local DNS resolver #1
IP address: 8.8.8.8

Would you like to configure an additional DNS resolver?
yes or no?: no

Below you see the overall network configuration:
<< Host Name >>
Host name: ashutosh478

<< 'pub' Network >>
Domain name: ashutosh.com
IP address/mask: 172.30.1.56/16
Broadcast: 172.30.255.255

<< DNS Resolvers >>
DNS Resolver: 8.8.8.8

<< Default Gateway >>
Default Gateway: 172.30.1.1

Is the above configuration correct?
yes or no?: yes
```

FOSSJan [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
+-----+
| Network Configuration for the 'pub' Network
+-----+
Please enter the domain name for the 'pub' interface
Domain name: ashutosh.com
Please enter the IP address which should be assigned to the 'pub' interface
IP address: 172.30.1.56

Please enter the corresponding network mask in the CIDR format
For example you have to enter 24 for 255.255.255.0
Netmask: 16

Please enter the broadcast IP address
(usually the last IP address in your network block)
Broadcast IP address: 172.30.255.255

Below you see the current configuration for the 'pub' network:
<< 'pub' Network >>
Domain name: ashutosh.com
IP address/mask: 172.30.1.56/16
Broadcast: 172.30.255.255

Is the above configuration correct?
yes or no?: yes
```

Right Ctrl

```
+-----+
| Installation Complete
+-----+
Congratulation! You have finished the installation of FOSS-Cloud
Now all you need to do is reboot the system and remove the CD-ROM

Do you want to reboot your system?
yes or no?: yes
```

Right Ctrl

Step 1: After installation, it will show you an IP Address. Put it in your browser to access your administrator page. The default user credentials are user: admin and password: admin. For root login – username- root and password – password.

192.168.75.129/vm-manager/

The screenshot shows a web browser window with the URL '192.168.75.129/vm-manager/'. The page has a header with the 'FOSS Cloud' logo and navigation links for 'Home', 'About', and 'Contact'. Below this is a 'Login' section with a form. The form includes fields for 'Username *' (with 'admin' entered), 'Password *' (with 'admin' entered), and a note 'Password cannot be blank.' There is also a checkbox for 'Remember me next time' and a 'Login' button.

CLOUD COMPUTING JOURNAL

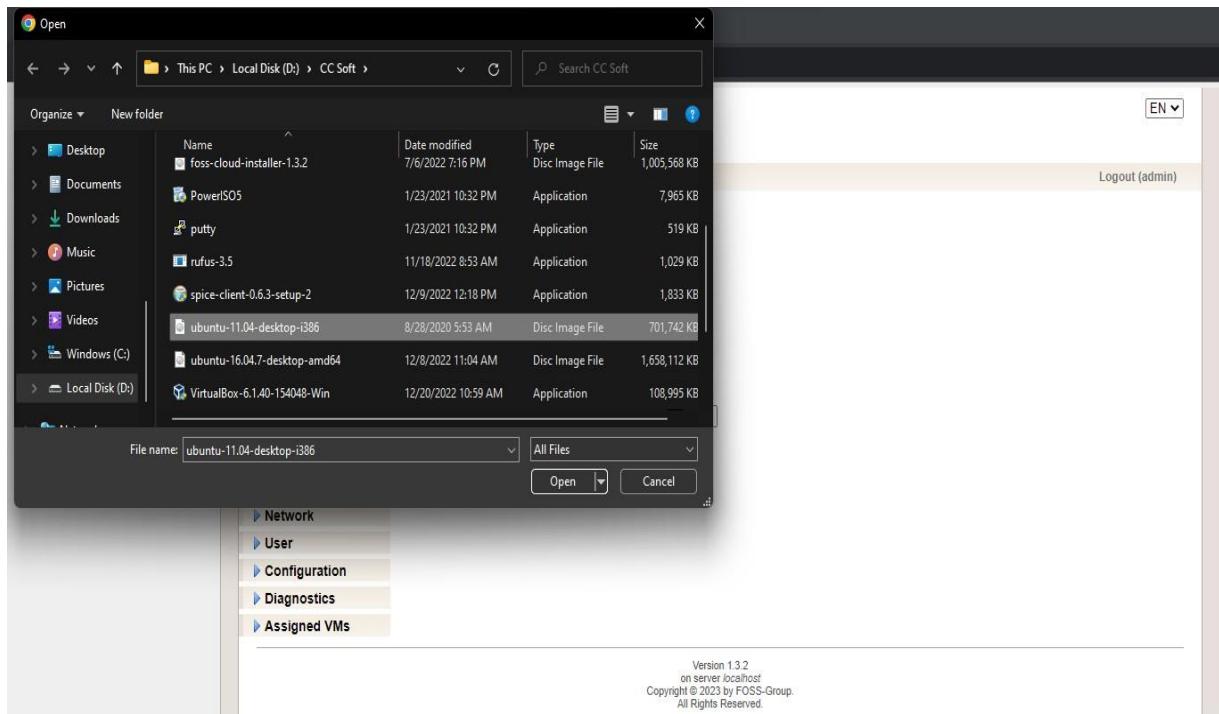
Step 2: The first screen after login shows many options to install and deploy any virtual machine. To install a virtual machine click on Virtual Machine-> Upload ISO File option and upload the bootable ISO file. Here, we are going to upload Linux Elementary OS ISO.

The screenshot shows the FOSS Cloud VM Manager interface at the URL 192.168.75.129/vm-manager/vmProfile/uploadIso.html. The left sidebar has a 'Virtual Machine' section with 'Upload ISO File' selected. The main area is titled 'Upload ISO File' with a note that fields with * are required. It includes an 'Iso File' input field ('Choose File') which shows 'No file chosen', a 'File Name' input field, and an 'Upload' button. The bottom right of the page displays the version information: Version 1.3.2 on server localhost, Copyright © 2023 by FOSS-Group, All Rights Reserved.

Step 3: Once you uploaded the file, create VmTemplate. In this option you are basically configuring your virtual machine's storage location, CPU, Memory, Node etc. Here, you will find single nodes and VM pool in respective options because everything was installed at the single server.

The screenshot shows the FOSS Cloud VM Manager interface at the URL 172.30.1.222/vm-manager/vmTemplate/create.html. The left sidebar has a 'Virtual Machine' section with 'Create' selected. The main area is titled 'Create VmTemplate' with notes for Step I (select a profile) and Step II (choose a node). It includes a 'Profile' dropdown set to 'Vmpool' with 'Vm-template-virtual-machine-pool-01' selected, a 'Node' dropdown set to 'tsc.tsc.org', a 'Name' input field ('Basant'), a 'Description' input field ('Hellooooooook'), a 'Memory' slider set to 128 MB, a 'Volume Capacity' slider set to 10 GB, a 'CPU' dropdown set to '1', a 'Clock Offset' dropdown set to 'utc', and a 'Number of displays' dropdown set to '1'.

CLOUD COMPUTING JOURNAL



Step 4: Now, click on VM Templates and you will see a template which you have created in step 4. To start your machine go to Run action Tab and click on the green arrow. Under status tab, it shows the running text with the green circle which shows that your machine is running without any errors. To view your virtual machine click on a blue square box under Action Tab.

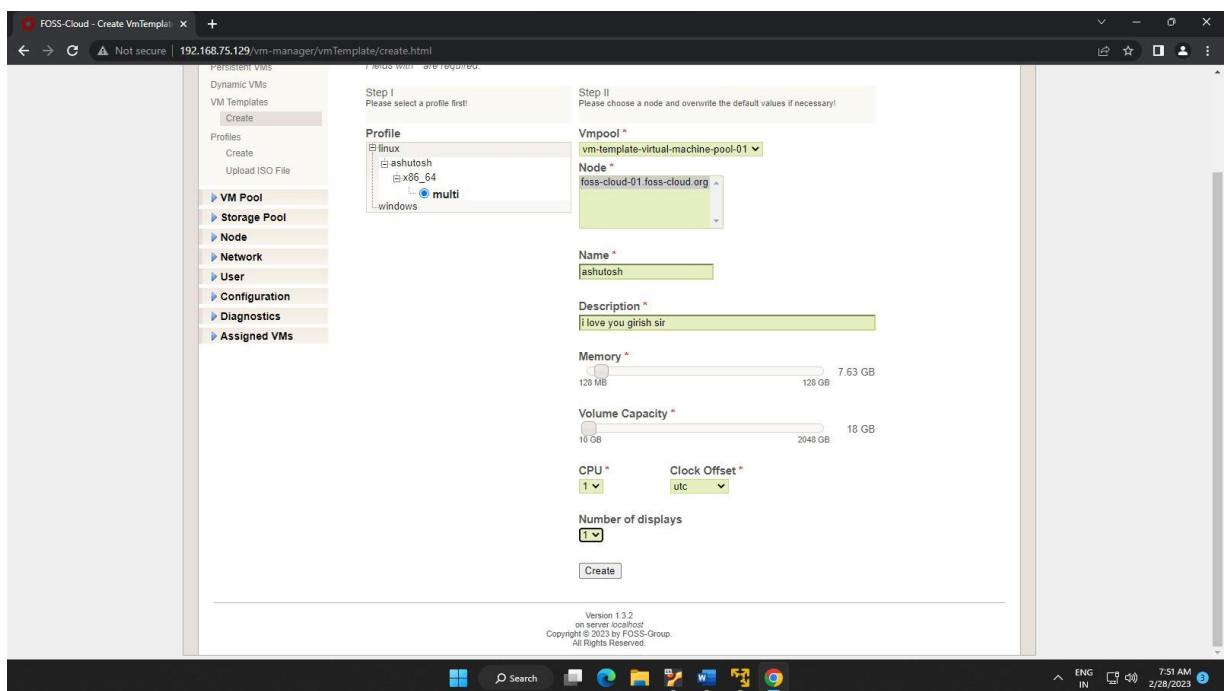
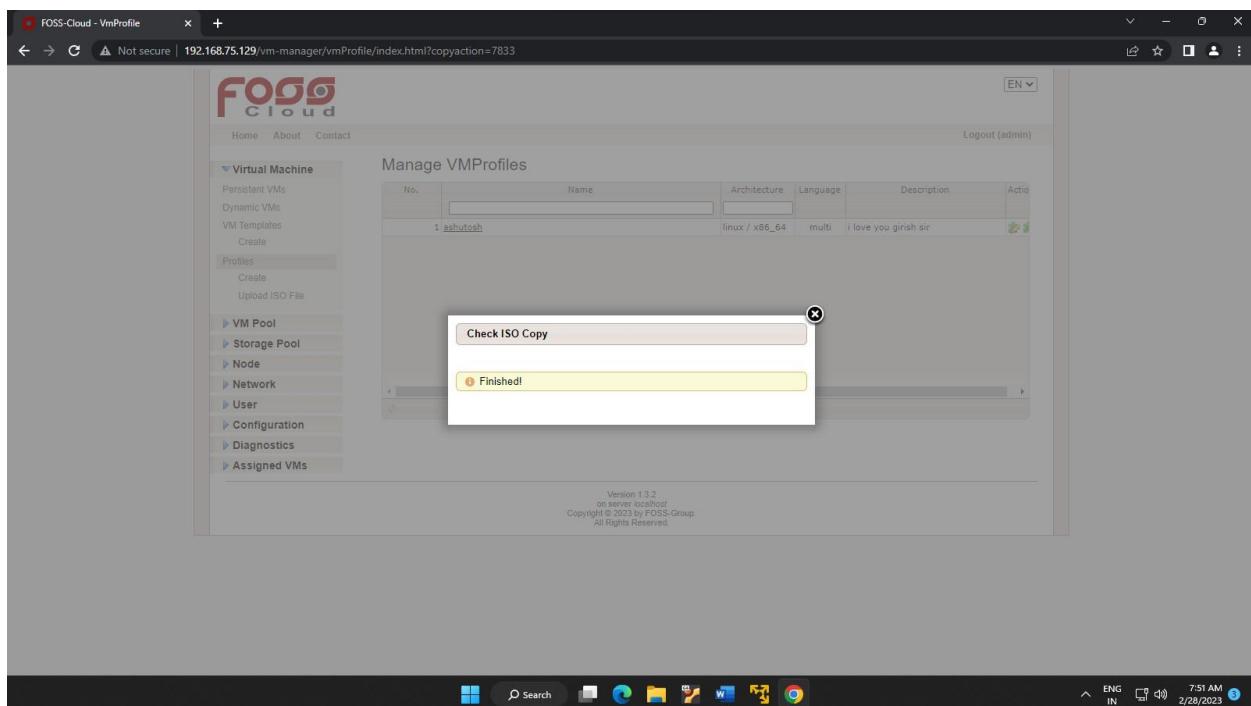
192.168.75.129/vm-manager/vmProfile/uploadIso.html

CLOUD COMPUTING JOURNAL

The screenshot shows the FOSS Cloud web interface. On the left, there is a sidebar with various navigation options under 'Virtual Machine' such as Persistent VMs, Dynamic VMs, VM Templates, Profiles, and VM Pools. The 'Upload ISO File' option is selected. In the main area, there is a form titled 'Upload ISO File' with a note that fields with * are required. A section for 'Alternative upload method' is present. Below it, there is an 'Iso File' section with a 'Choose File' button set to 'ubuntu-11.0...ktop-i386.iso'. A progress bar shows '100%' and 'Upload finished (685.29 MB)'. To the right, a message box says 'File Name' with 'ashu' entered, 'Finished', and 'Upload finished!'. Below the progress bar, it says 'took 8 seconds'. At the bottom, there is a copyright notice: 'Version 1.3.2 on server localhost Copyright © 2023 by FOSS-Group. All Rights Reserved.'

The screenshot shows the 'Create VM Profile' page in the FOSS Cloud interface. The URL is 192.168.75.129/vm-manager/vmProfile/create.html. The sidebar on the left is identical to the previous screenshot. The main form has two steps: Step I (Please select a profile first!) and Step II (Override the default values if necessary!). Under Step II, there are sections for 'BaseProfile' (set to 'linux' with 'x86_64' selected), 'Isofile' (with a dropdown showing 'user.iso', 'abiiso', 'tcs.iso', and 'ashu.iso'), 'Name' (set to 'ashutosh'), 'Description' (set to 'I love you girish sir'), 'Memory' (set to 7.63 GB), 'Volume Capacity' (set to 18 GB), 'CPU' (set to 1), and 'Clock Offset' (set to 'utc'). A 'Create' button is at the bottom. The bottom of the screen shows a Windows taskbar with various icons.

CLOUD COMPUTING JOURNAL



CLOUD COMPUTING JOURNAL

secure | 192.168.75.129/vm-manager/vmTemplate/index.html

Manage VMTemplates

Vm Pool **vm-template-virtual-machine-pool-01**

No.	DisplayName	Status	Run Action	Memory	Node	Action
1	ashutosh	running	Stop	7.63 GB / 7.63 GB	foss-cloud-01.foss-cloud.org	

Page 1 of 1 Refresh 10

Links
Download Spice Client

Version 1.3.2
on server localhost
Copyright © 2023 by FOSS-Group.
All Rights Reserved.

192.168.75.129/vm-manager/diagnostics/vmtemplateinfos.html?dn=sstVirtualMachine=196d41db-1907-4372-9211-5e097d4338dc,ou=virtual%20machines,ou=virtualization,ou=services,

VM Template Infos

- ashutosh
- Libvirt URI
qemu+tcp://127.0.0.1/system
- SPICE URI
<spice://192.168.75.129?port=5900&password=JCjHL507w94D>
- Start XML

```
<domain type="kvm">
    <name>196d41db-1907-4372-9211-5e097d4338dc</name>
    <uuid>196d41db-1907-4372-9211-5e097d4338dc</uuid>
    <memory>7995392</memory>
    <vcpu>1</vcpu>
    <os>
        <type arch="x86_64" machine="pc">hvm</type>
        <boot dev="cdrom"/>
        <smbios mode="sysinfo"/>
    </os>
    <sysinfo type="smbios">
        <bios>
            <entry name="vendor">FOSS-Group</entry>
        </bios>
        <system>
            <entry name="manufacturer">FOSS-Group</entry>
            <entry name="vendor">FOSS-Group</entry>
            <entry name="serial">196d41db-1907-4372-9211-5e097d4338dc</entry>
        </system>
    </sysinfo>

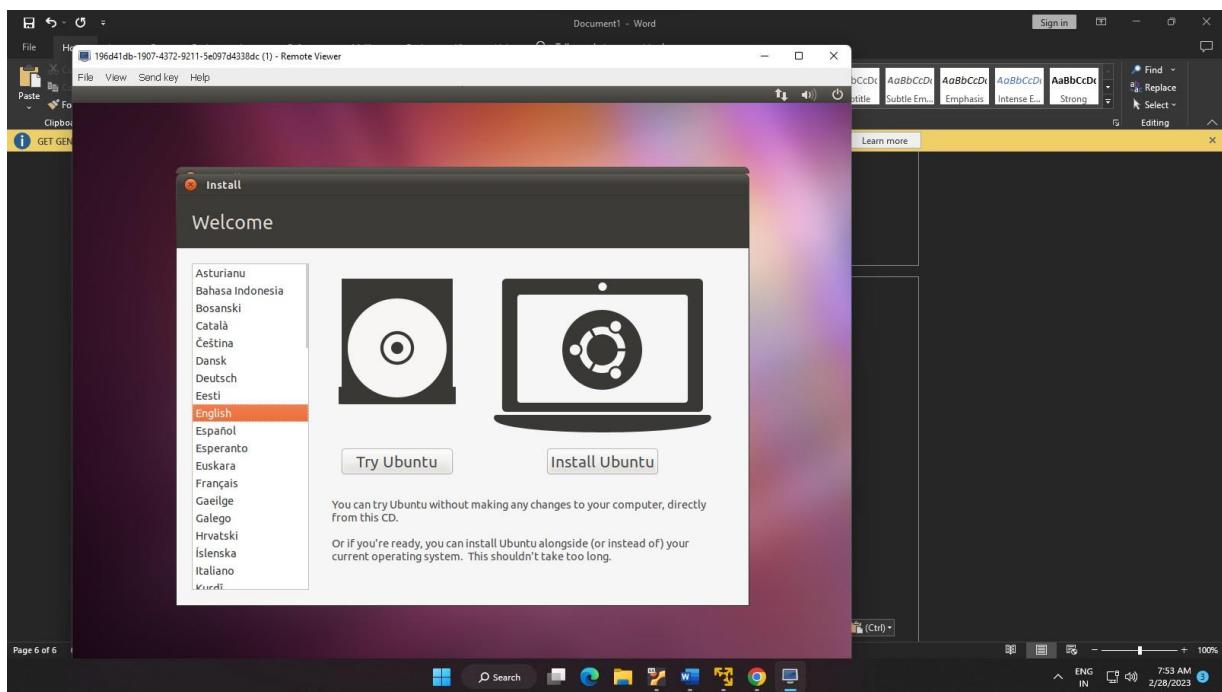
```

CLOUD COMPUTING JOURNAL

```

<domain type="kvm">
    <name>196d41db-1907-4372-9211-5e097d4338dc</name>
    <uuid>196d41db-1907-4372-9211-5e097d4338dc</uuid>
    <memory>7995392</memory>
    <vcpu>1</vcpu>
    <os>
        <type arch="x86_64" machine="pc">hvm</type>
        <boot dev="cdrom"/>
        <smbios mode="sysinfo"/>
    </os>
    <sysinfo type="smbios">
        <bios>
            <entry name="vendor">FOSS-Group</entry>
        </bios>
        <system>
            <entry name="manufacturer">FOSS-Group</entry>
            <entry name="vendor">FOSS-Group</entry>
            <entry name="serial">196d41db-1907-4372-9211-5e097d4338dc</entry>
        </system>
    </sysinfo>
</domain>

```



CLOUD COMPUTING JOURNAL

B. USING Ubuntu and KVM

```

dscstcsc@tcsc:~/Desktop$ sudo adduser ashus
[sudo] password for dcstcsc:
Sorry, try again.
[sudo] password for dcstcsc:
Adding user 'ashus' ...
Adding new group 'ashus' (1042) ...
Adding new user 'ashus' (1042) with group 'ashus' ...
Creating home directory '/home/ashus' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ashus
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
dscstcsc@tcsc:~/Desktop$ sudo usermod -aG sudo ashus
dscstcsc@tcsc:~/Desktop$ su ashus
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ashus@tcsc:~/home/dcstcsc/Desktop$ sudo kvm-ok
[sudo] password for ashus:
INFO: /dev/kvm exists
KVM acceleration can be used
ashus@tcsc:~/home/dcstcsc/Desktop$ sudo apt install cpu-checker
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
cpu-checker is already the newest version (0.7-1.3build1).
0 upgraded, 0 newly installed, 0 to remove and 112 not upgraded.
ashus@tcsc:~/home/dcstcsc/Desktop$ sudo apt update
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 https://ppa.launchpadcontent.net/ondrej/php/ubuntu jammy InRelease
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [601 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease [104 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [247 kB]

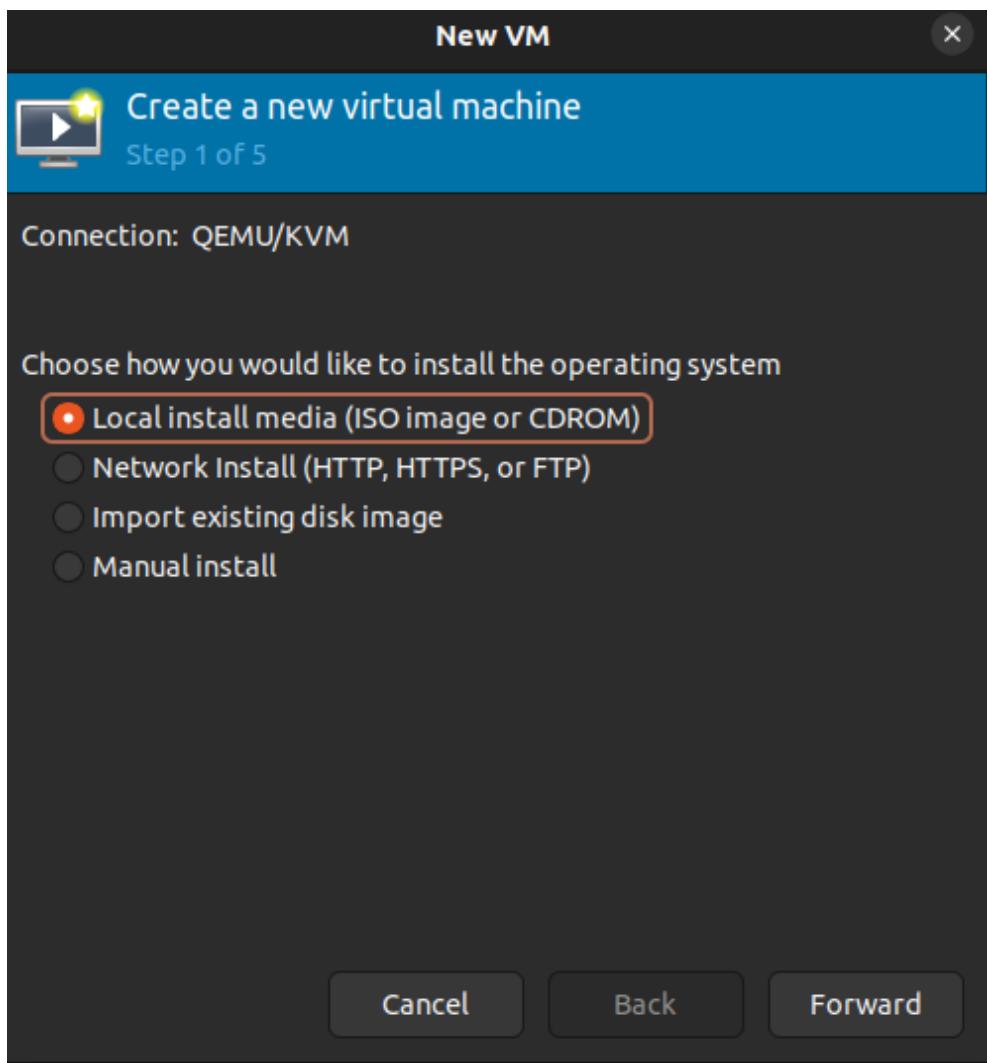
```

```

ashus@tcsc:~/home/dcstcsc/Desktop$ sudo adduser ashus libvirt
Adding user 'ashus' to group 'libvirt' ...
Adding user ashus to group libvirt
Done.
ashus@tcsc:~/home/dcstcsc/Desktop$ sudo adduser ashus kvm
Adding user 'ashus' to group 'kvm' ...
Adding user ashus to group kvm
Done.
ashus@tcsc:~/home/dcstcsc/Desktop$ sudo systemctl status libvirtd
● libvirtd.service - Virtualization daemon
   Loaded: loaded (/lib/systemd/system/libvirtd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-02-02 10:18:00 IST; 1min ago
     TriggeredBy: ● libvirtd-ro.socket
                  ● libvirtd-admin.socket
                  ● libvirtd.socket
   Docs: man:libvirtd(8)
         https://libvirt.org
 Main PID: 1139 (libvirtd)
   Tasks: 21 (limit: 32768)
  Memory: 42.2M
    CPU: 524ms
   CGroup: /system.slice/libvirtd.service
           ├─1139 /usr/sbin/libvirtd
           ├─1691 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/lib/libvirt/libvirt-dnsmasq
           └─1692 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/lib/libvirt/libvirt-dnsmasq

Feb 02 10:18:00 tcsc.org systemd[1]: Started Virtualization daemon.
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: started, version 2.86 cachesize 150
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua TFTP conntrack ipset a
Feb 02 10:18:03 tcsc.org dnsmasq-dhcp[1691]: DHCP, IP range 192.168.122.2 -- 192.168.122.254, lease time 1h
Feb 02 10:18:03 tcsc.org dnsmasq-dhcp[1691]: DHCP, sockets bound exclusively to interface virbr0
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: reading /etc/resolv.conf
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: using nameserver 127.0.0.53#53
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: using docnames file, read /etc/hosts 7 addresses
ashus@tcsc:~/home/dcstcsc/Desktop$ sudo virt-manager
ashus@tcsc:~/home/dcstcsc/Desktop$ 
```

CLOUD COMPUTING JOURNAL



CLOUD COMPUTING JOURNAL

Create a new virtual machine
Step 2 of 5

Choose ISO or CDROM install media:

/Downloads/ubuntu-18.04.6-desktop-amd64.iso

Choose the operating system you are installing:

Q Ubuntu 18.04 LTS

Automatically detect from the installation media / source

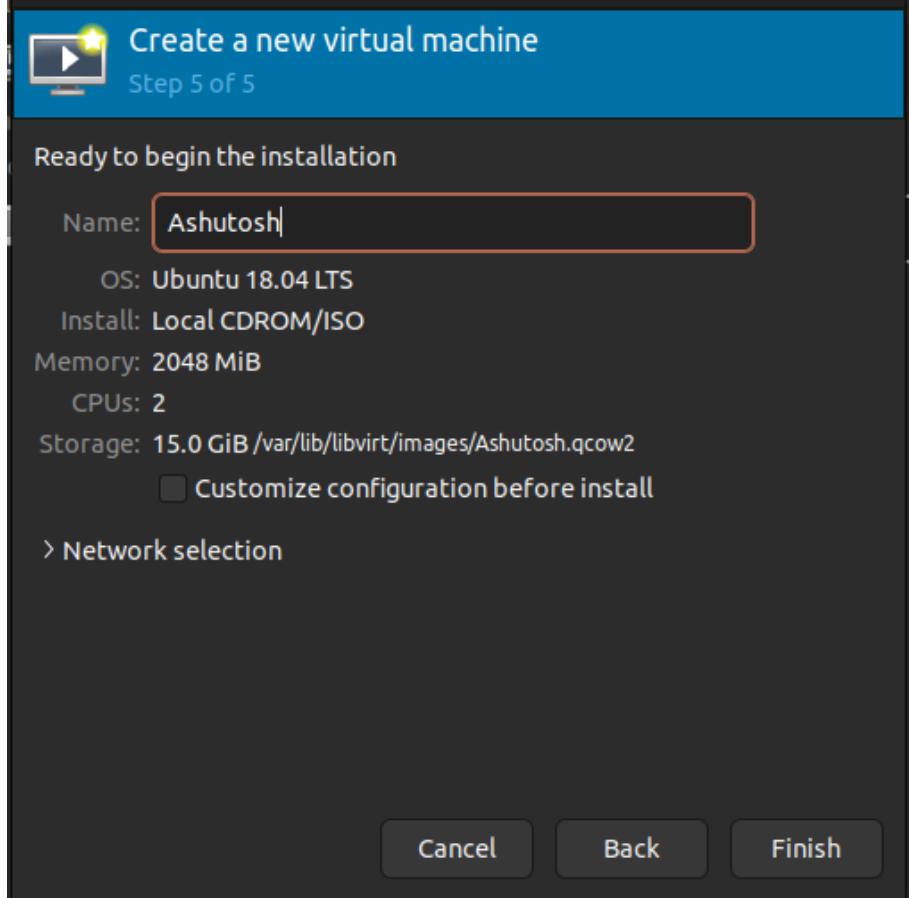
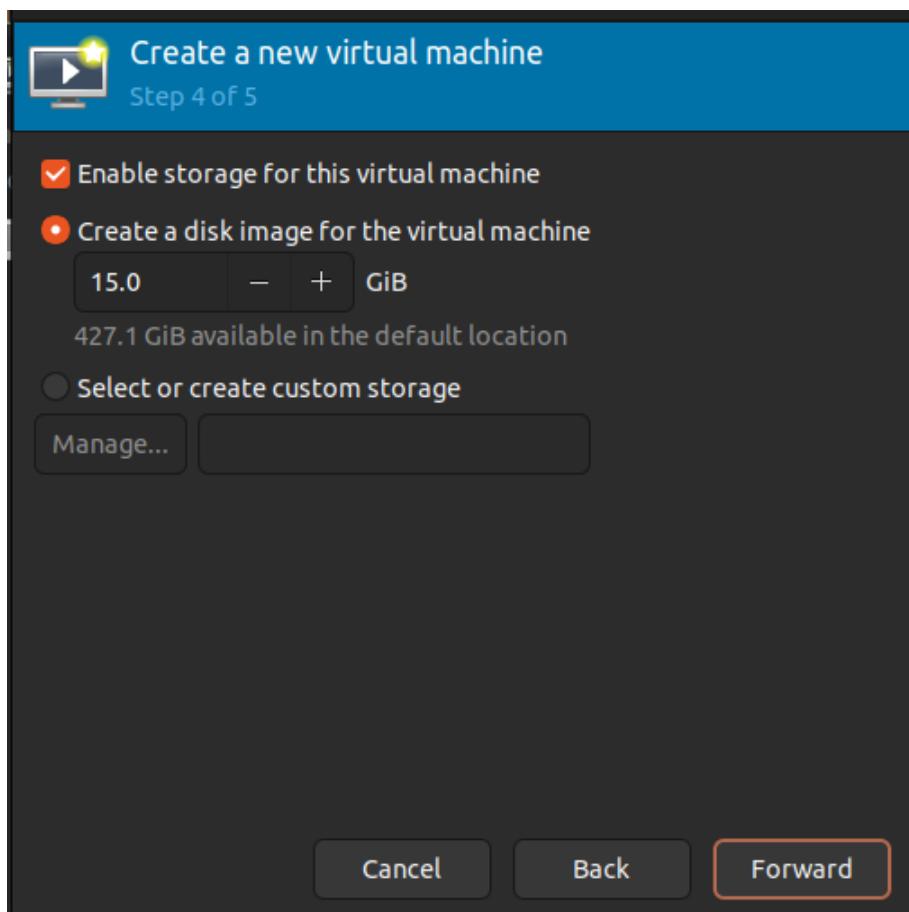
Create a new virtual machine
Step 3 of 5

Choose Memory and CPU settings:

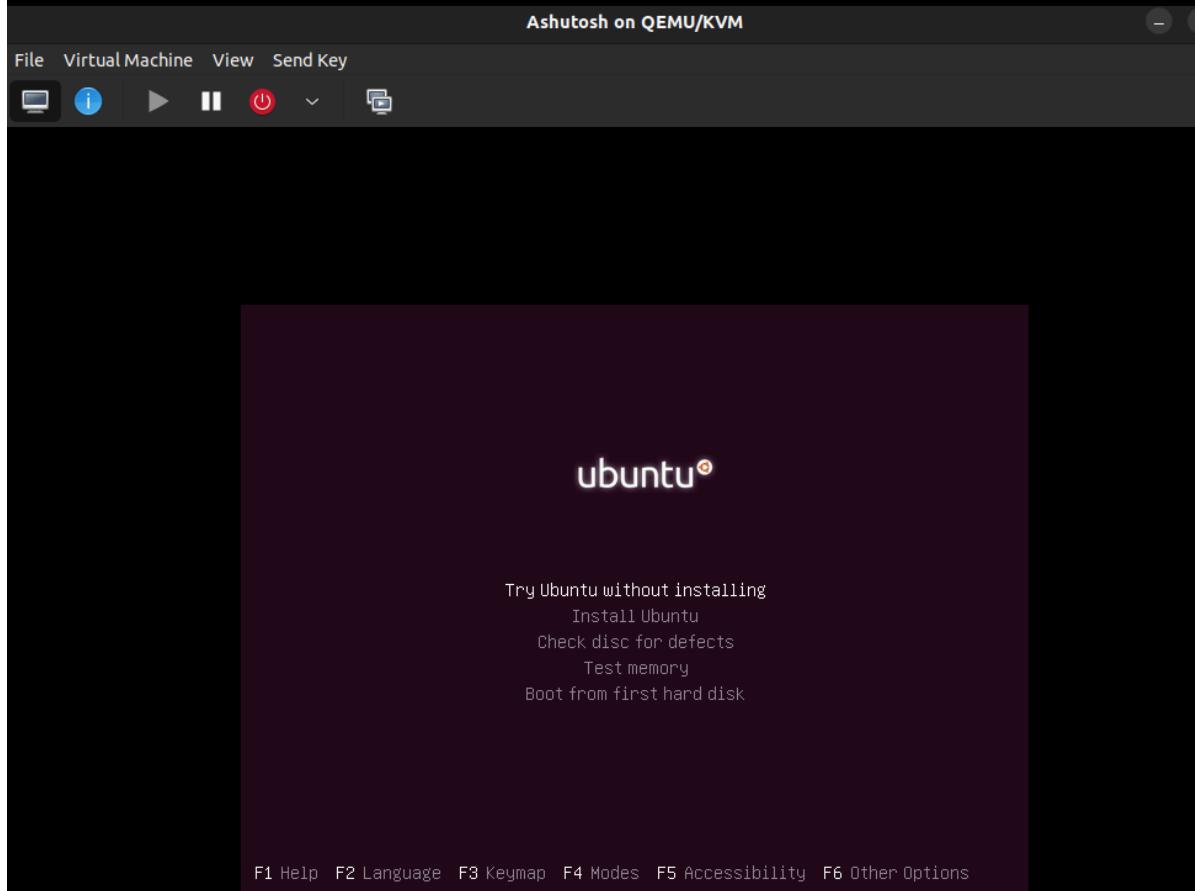
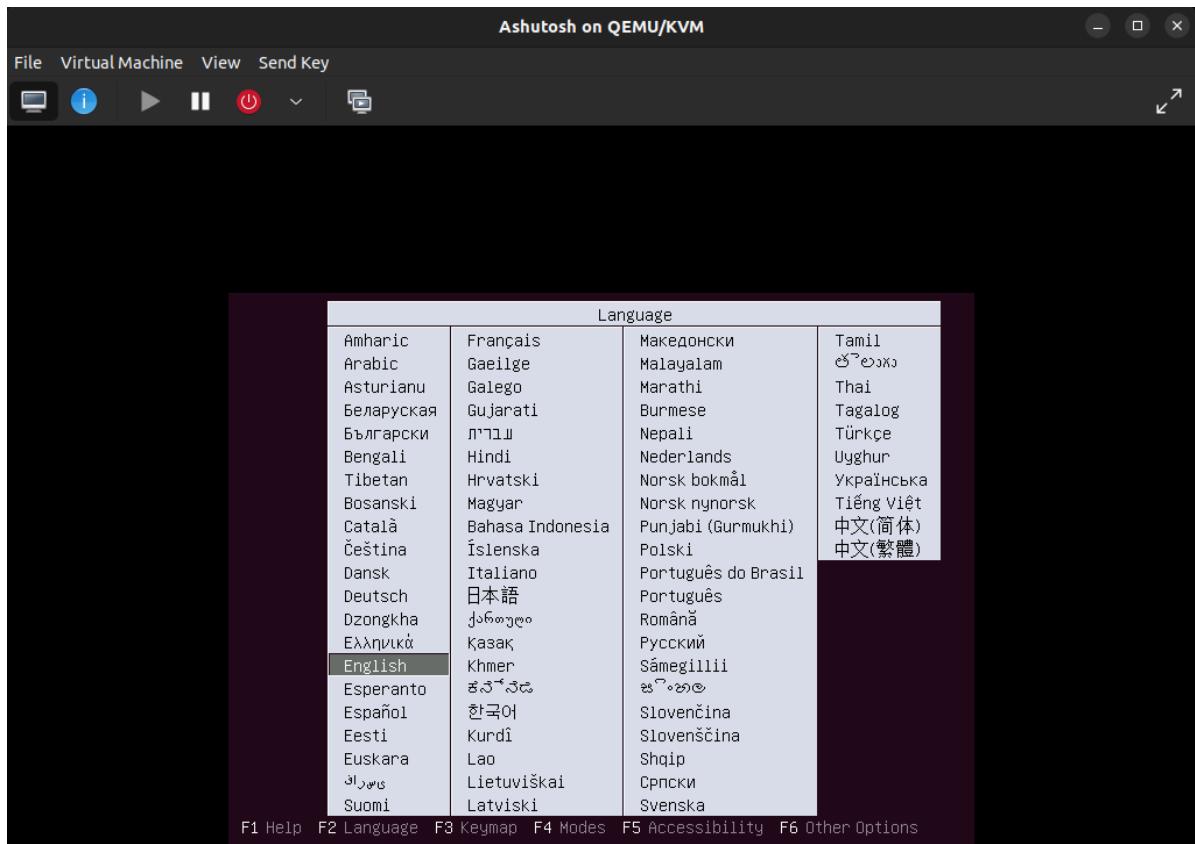
Memory: 2048
Up to 15675 MiB available on the host

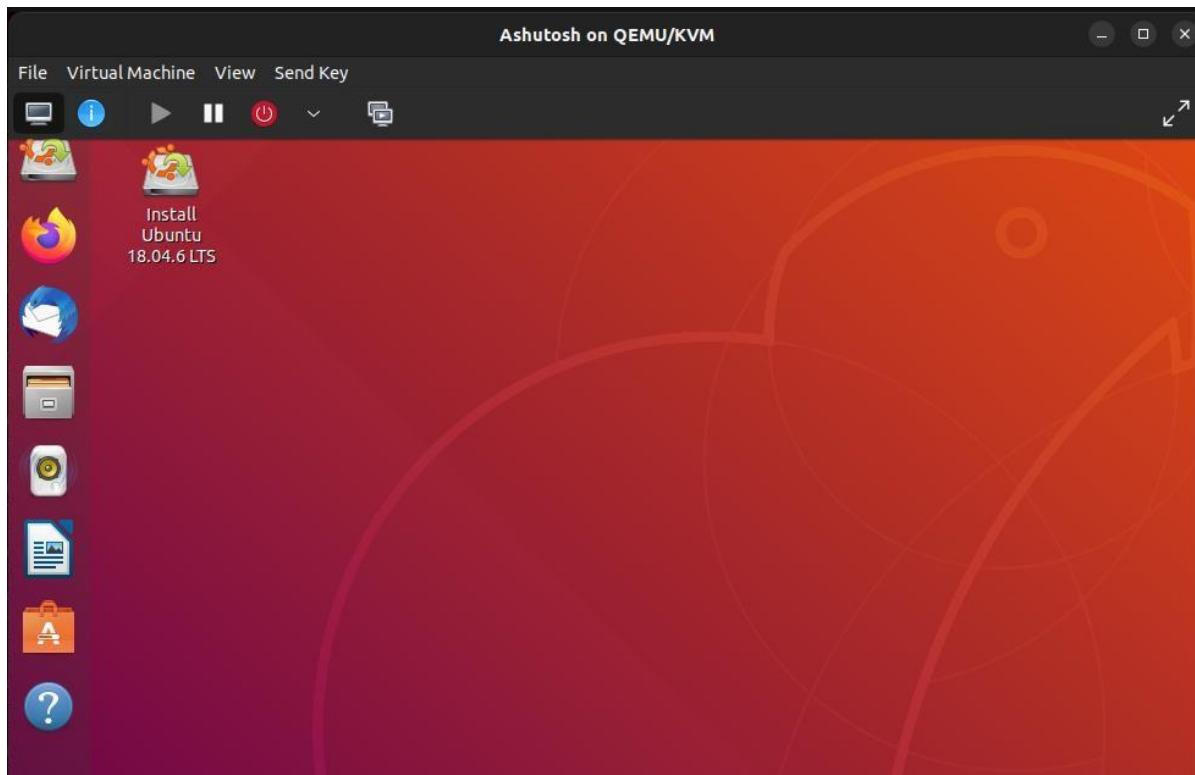
CPUs: 2
Up to 12 available

CLOUD COMPUTING JOURNAL



CLOUD COMPUTING JOURNAL





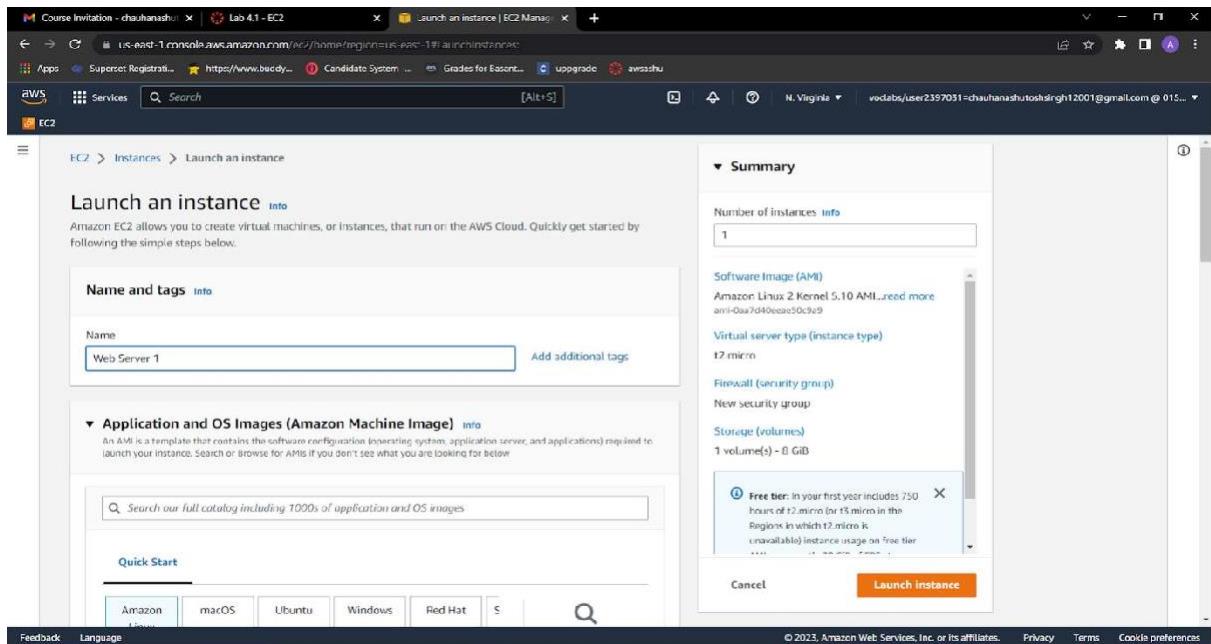
D. GCP/AWS/IBM/Azure/...

1. Choose the **Services** menu, locate the **Compute** services, and select **EC2**.

A screenshot of the AWS Academy interface showing a lab titled "Lab 4.1 - EC2". The left sidebar contains links for Account, Dashboard, Courses, Calendar, Inbox, History, and Help. The main content area displays the lab title "Module 4 Lab 1: Launching an EC2 Instance" and a "Lab overview" section stating, "In this lab, you create an Amazon Elastic Compute Cloud (Amazon EC2) instance that hosts a simple website." Below this is a "Duration" section indicating it requires approximately 30 minutes. Navigation buttons for "Previous" and "Next" are at the bottom.

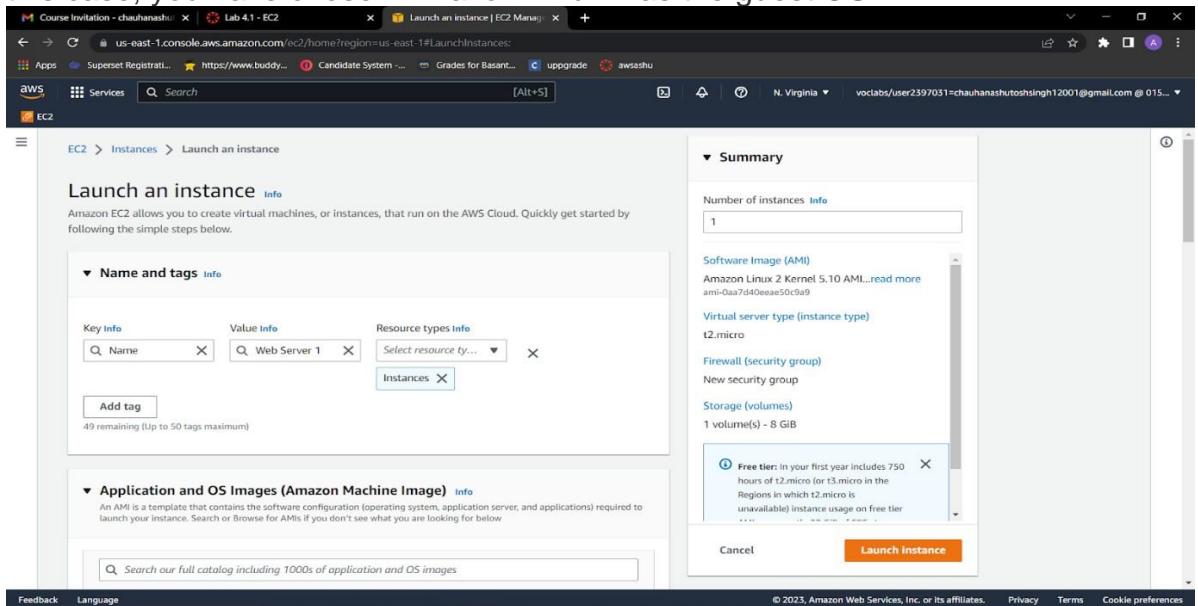
2. Choose the **Launch instance** button in the middle of the page, and then select **Launch instance** from the dropdown menu.

3. Give it the name **Web Server 1**



4. Choose an AMI from which to create the instance:

- In the list of available *Quick Start* AMIs, keep the default **Amazon Linux AMI** selected.
 - Also keep the default **Amazon Linux 2 AMI (HVM)** selected.
- The type of *Amazon Machine Image (AMI)* you choose determines the Operating System (OS) that will run on the EC2 instance that you launch. In this case, you have chosen Amazon Linux 2 as the guest OS.



The screenshot shows the AWS EC2 'Launch an instance' page. In the 'Application and OS Images (Amazon Machine Image)' section, an Amazon Linux 2 AMI (ami-0aa7d40eeae50c9a9) is selected. In the 'Summary' section, the 'Virtual server type (instance type)' is set to 't2.micro'. A tooltip for the 'Free tier' indicates it covers 750 hours of t2.micro usage in the N. Virginia region. The 'Launch instance' button is visible at the bottom right.

5. In the *Instance type* panel, keep the default t2.micro selected.
6. Select the key pair to associate with the instance From the Key pair name menu, select vockey.

The screenshot shows the 'Instance type' configuration page. The 't2.micro' instance type is selected. In the 'Key pair (login)' section, 'vockey' is chosen from the dropdown menu. A tooltip for the 'Free tier' indicates it covers 750 hours of t2.micro usage in the N. Virginia region. The 'Launch instance' button is visible at the bottom right.

7. Next to Network settings, choose **Edit**.
8. Keep the default VPC and *subnet* settings. Also keep the **Auto-assign public IP** setting set to **Enable**.
9. Under *Firewall (security groups)*, keep the default **Create security group** option chosen.

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
vockey

Network settings Info
Edit

Network Info
vpc-0a9a15224d9d5acde

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

Summary

Number of instances Info
1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0aa7d40eeae50c9a9

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

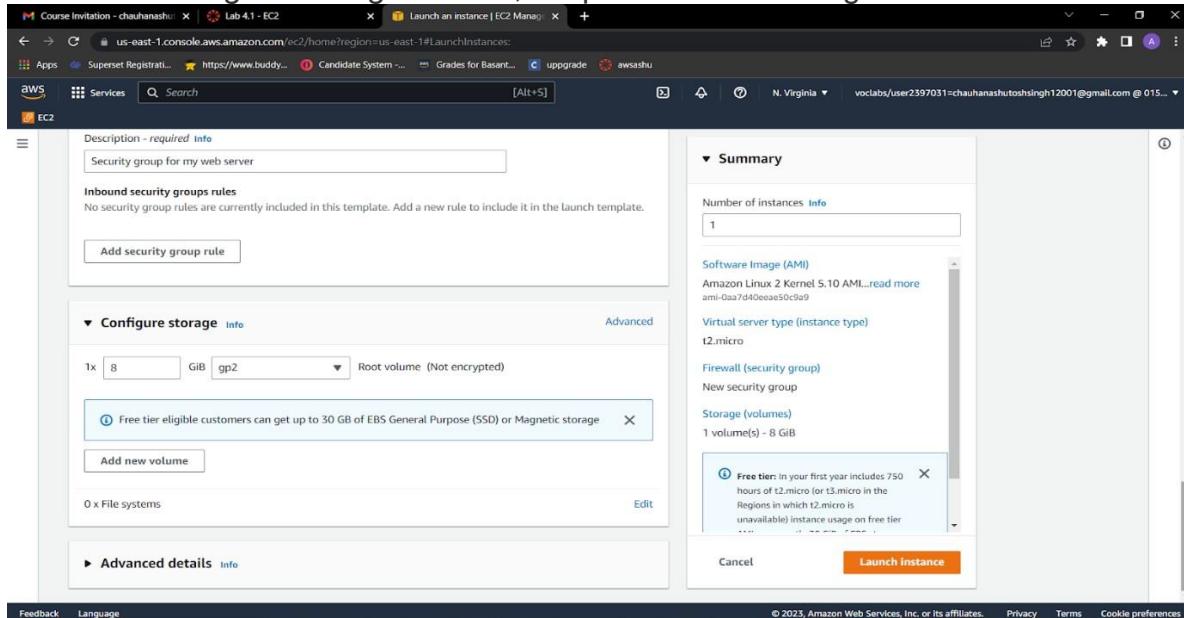
Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier

10. Configure a new security group:

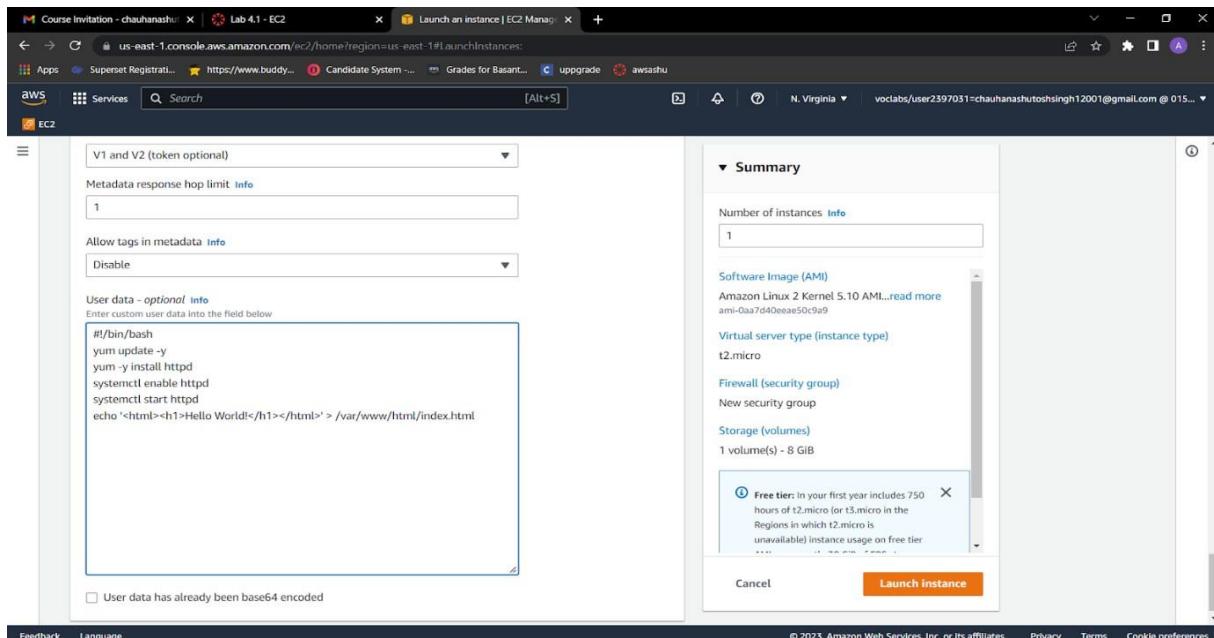
- o Keep the default selection **Create a new security group.**
- o **Security group name:** Clear the text and enter **Web Server**
- o **Description:** Clear the text and enter **Security group for my web server**
- o Choose **Remove** to remove the default SSH inbound rule.

11. In the *Configure storage* section, keep the default settings.



12. Configure a script to run on the instance when it launches:

- Expand the **Advanced details** panel.
- Scroll to the bottom of the page and then copy and paste the code shown below into the **User data** box:



13. At the bottom of the **Summary** panel on the right side of the screen choose **Launch instance** You will see a Success message.

14. Go to **View all instances**

15. Before you continue, wait for your instance to display the following:

- **Instance state: Running**
- **Status check: 2/2 checks passed**

The image consists of three vertically stacked screenshots of the AWS EC2 Management Console.

Screenshot 1: Launch an instance - Step 4

This screenshot shows the "Launch an instance" step of the wizard. It displays a success message: "Successfully initiated launch of instance (i-01d223b60e88dbc20)". Below this, there is a link to "Launch log". The "Next Steps - preview" section contains five items:

- Create billing and free tier usage alerts**: To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds. Includes a "Create billing alerts" button.
- Connect to your instance**: Once your instance is running, log into it from your local computer. Includes a "Connect to instance" button and a "Learn more" link.
- Connect an RDS database**: Configure the connection between an EC2 instance and a database to allow traffic flow between them. Includes a "Connect an RDS database" button and a "Learn more" link.
- Create EBS snapshot policy**: Create a policy that automates the creation, retention, and deletion of EBS snapshots. Includes a "Create EBS snapshot policy" button.

Screenshot 2: Instances (1/1) - Details

This screenshot shows the "Instances (1/1) Info" page. It lists one instance named "Web Server 1" with the following details:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server 1	i-01d223b60e88dbc20	Running	t2.micro	-	No alarms	us-east-1e	ec2-54-89-134-4

Screenshot 3: Instances (1) - Details

This screenshot shows the "Instances (1) Info" page. It lists the same instance "Web Server 1" with the following details:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server 1	i-01d223b60e88dbc20	Running	t2.micro	2/2 checks passed	No alarms	us-east-1e	ec2-54-89-134-40.c

14. From the **Details** tab, copy the **Public IPv4 address** value of your instance to your clipboard.

Open a new tab in your web browser, paste the public IP address you just copied, and press **Enter**. The webpage does not load. You must update the security group to be able to access the page.



15. Return to the **EC2 Management Console** browser tab.
16. In the left navigation pane, under **Network & Security**, choose **Security Groups**.
17. Select the **Web Server** security group, which you created when launching your EC2 instance.
18. In the lower pane, choose the **Inbound rules** tab.

Name	Security group ID	Security group name	VPC ID	Description	Owner
sg-09b5d6d3574a6d52e	Web Server	vpc-0a9a15224d9d5acde	Security group for my ...	015608633545	
sg-0668948f4977346ec	default	vpc-0a9a15224d9d5acde	default VPC security gr...	015608633545	

Inbound rules

No security group rules found.

19. Choose **Edit inbound rules**, and then choose **Add rule**. Configure the following:
 - **Type:** HTTP, **Source:** Anywhere-IPv4, Choose **Save rules**

The new inbound HTTP rule creates an entry for IPv4 IP (0.0.0.0/0) and IPv6 IP addresses (::/0).

20. Return to the tab that you used to try to connect to the web server. Refresh the page. The page should display the message *Hello World!*

Conclusion: Successfully performed IaaS ,The IaaS cloud computing platform vendor can get access to your sensitive data.

Practical No.02

Aim: Study and implementation of Platform as a Service

Theory: Platform as a Service (PaaS) provides a runtime environment. It allows programmers to easily create, test, run, and deploy web applications. You can purchase these applications from a cloud service provider on a pay-as-per use basis and access them using the Internet connection. In PaaS, back end scalability is managed by the cloud service provider, so end- users do not need to worry about managing the infrastructure.

PaaS includes infrastructure (servers, storage, and networking) and platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle.

Example: Google App Engine, Force.com, Joyent, Azure.

PaaS providers provide the Programming languages, Application frameworks, Databases, and Other tools:

1. Programming languages

PaaS providers provide various programming languages for the developers to develop the applications. Some popular programming languages provided by PaaS providers are Java, PHP, Ruby, Perl, and Go.

2. Application frameworks

PaaS providers provide application frameworks to easily understand the application development. Some popular application frameworks provided by PaaS providers are Node.js, Drupal, Joomla, WordPress, Spring, Play, Rack, and Zend.

3. Databases

PaaS providers provide various databases such as ClearDB, PostgreSQL, MongoDB, and Redis to communicate with the applications.

4. Other tools

PaaS providers provide various other tools that are required to develop, test, and deploy the applications.

Method and Steps:

A. Using KVM.

The terminal window shows the following commands and output:

```
ashus@tcsc: /home/dcstcsc/Desktop$ sudo adduser ashus libvirt
Adding user 'ashus' to group 'libvirt'
Adding user ashus to group libvirt
Done.
ashus@tcsc: /home/dcstcsc/Desktop$ sudo adduser ashus kvm
Adding user 'ashus' to group 'kvm' ...
Adding user ashus to group kvm
Done.
ashus@tcsc: /home/dcstcsc/Desktop$ sudo systemctl status libvirtd
● libvirtd.service - Virtualization daemon
   Loaded: loaded (/lib/systemd/system/libvirtd.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-02-02 10:18:00 IST; 11min ago
TriggeredBy: ● libvirtd-ro.socket
              ● libvirtd-admin.socket
              ● libvirtd.socket
    Docs: man:libvirtd(8)
          https://libvirt.org
   Main PID: 1139 (libvirtd)
      Tasks: 21 (limit: 32768)
     Memory: 42.2M
        CPU: 524ms
       CGroup: /system.slice/libvirtd.service
               ├─1139 /usr/sbin/libvirtd
               ├─1691 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/lib/libvirt/libvirt-dnsmasq
               └─1692 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/lib/libvirt/libvirt-dnsmasq
Feb 02 10:18:00 tcsc.org systemd[1]: Started Virtualization daemon.
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: started, version 2.86 cachesize 150
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: compile time options: IPv6 GNU-getopt DBus no-UBus l18n IDN2 DHCP DHCPv6 no-Lua TFTP conntrack ipset a...
Feb 02 10:18:03 tcsc.org dnsmasq-dhcp[1691]: DHCP, IP range 192.168.122.2 -- 192.168.122.254, lease time 1h
Feb 02 10:18:03 tcsc.org dnsmasq-dhcp[1691]: DHCP, sockets bound exclusively to interface virbr0
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: reading /etc/resolv.conf
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: using nameserver 127.0.0.53#53
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: read /etc/hosts - 7 addresses
ashus@tcsc: /home/dcstcsc/Desktop$ sudo virt-manager
ashus@tcsc: /home/dcstcsc/Desktop$
```

The virt-manager 'Create a new virtual machine' wizard is shown. Step 1 of 5. Connection: QEMU/KVM. Choose how you would like to install the operating system. Local install media (ISO image or CDROM) is selected. Other options include Network Install (HTTP, HTTPS, or FTP), Import existing disk image, and Manual install. Buttons at the bottom are Cancel, Back, and Forward.

[Type here]

The screenshot shows two sequential steps in the Oracle VM VirtualBox Manager for creating a new virtual machine.

Step 2 of 5: Choose ISO or CDROM install media

Choose ISO or CDROM install media:
:/Downloads/ubuntu-18.04.6-desktop-amd64.iso

Choose the operating system you are installing:

Q Ubuntu 18.04 LTS Automatically detect from the installation media / source

Cancel Back Forward

Step 3 of 5: Choose Memory and CPU settings

Choose Memory and CPU settings:

Memory: 2048
Up to 15675 MiB available on the host

CPUs: 2
Up to 12 available

Cancel Back Forward

[Type here]

Create a new virtual machine
Step 4 of 5

Enable storage for this virtual machine

Create a disk image for the virtual machine
15.0 GiB

427.1 GiB available in the default location

Select or create custom storage
Manage...

Cancel Back Forward

Create a new virtual machine
Step 5 of 5

Ready to begin the installation

Name: Ashutosh

OS: Ubuntu 18.04 LTS

Install: Local CDROM/ISO

Memory: 2048 MiB

CPUs: 2

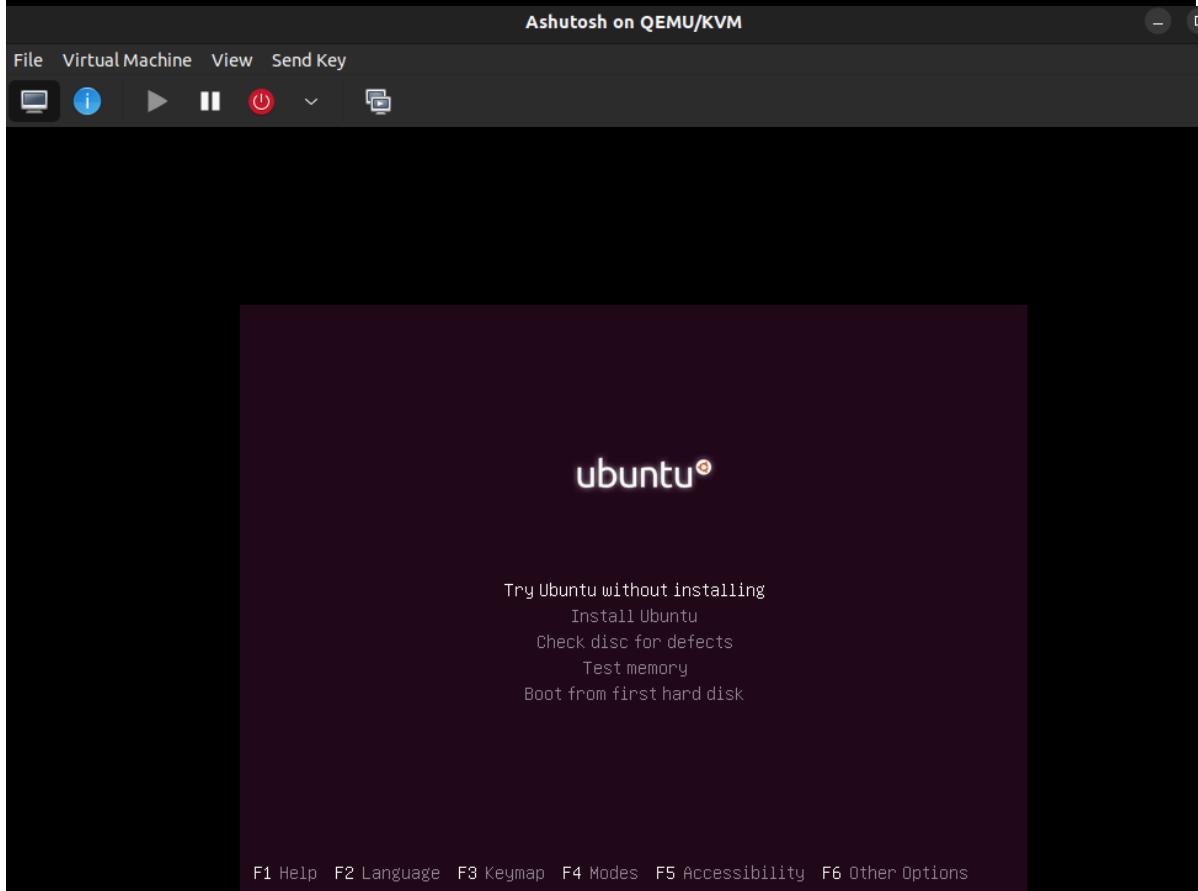
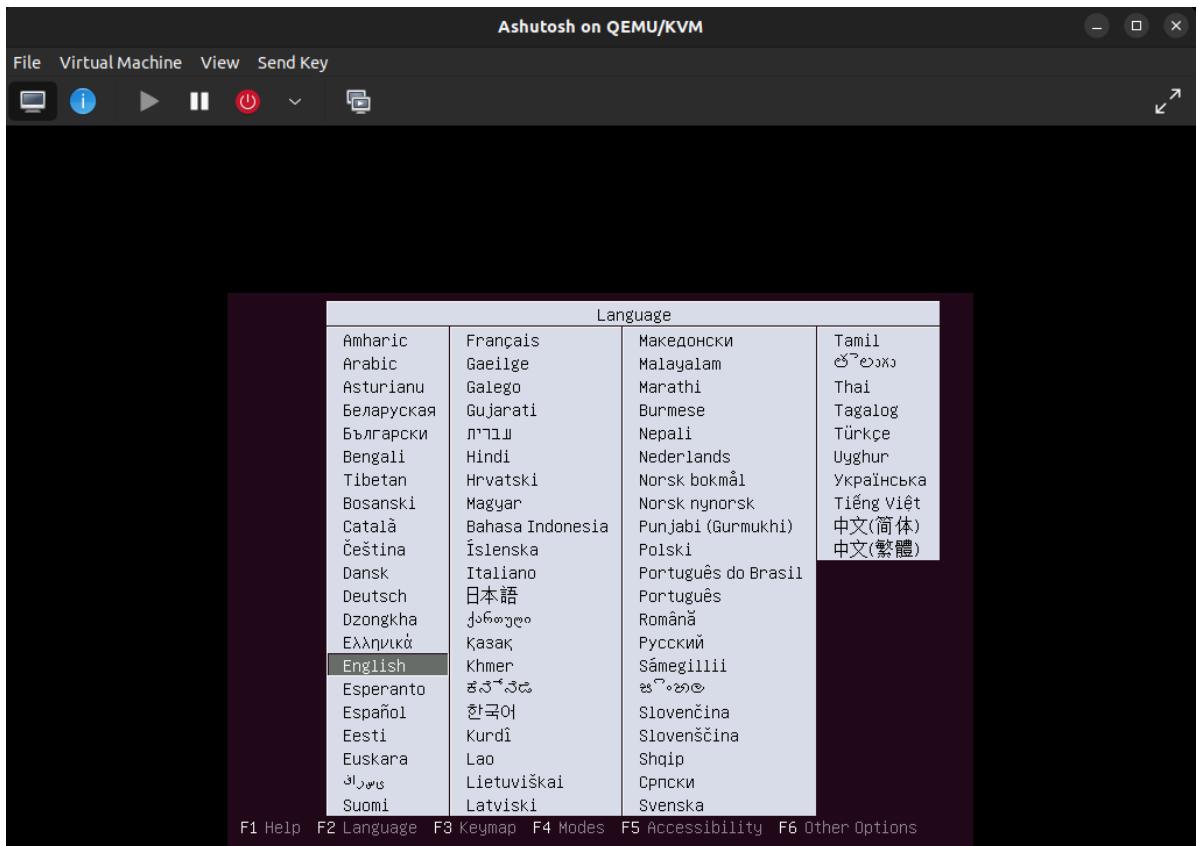
Storage: 15.0 GiB /var/lib/libvirt/images/Ashutosh.qcow2

Customize configuration before install

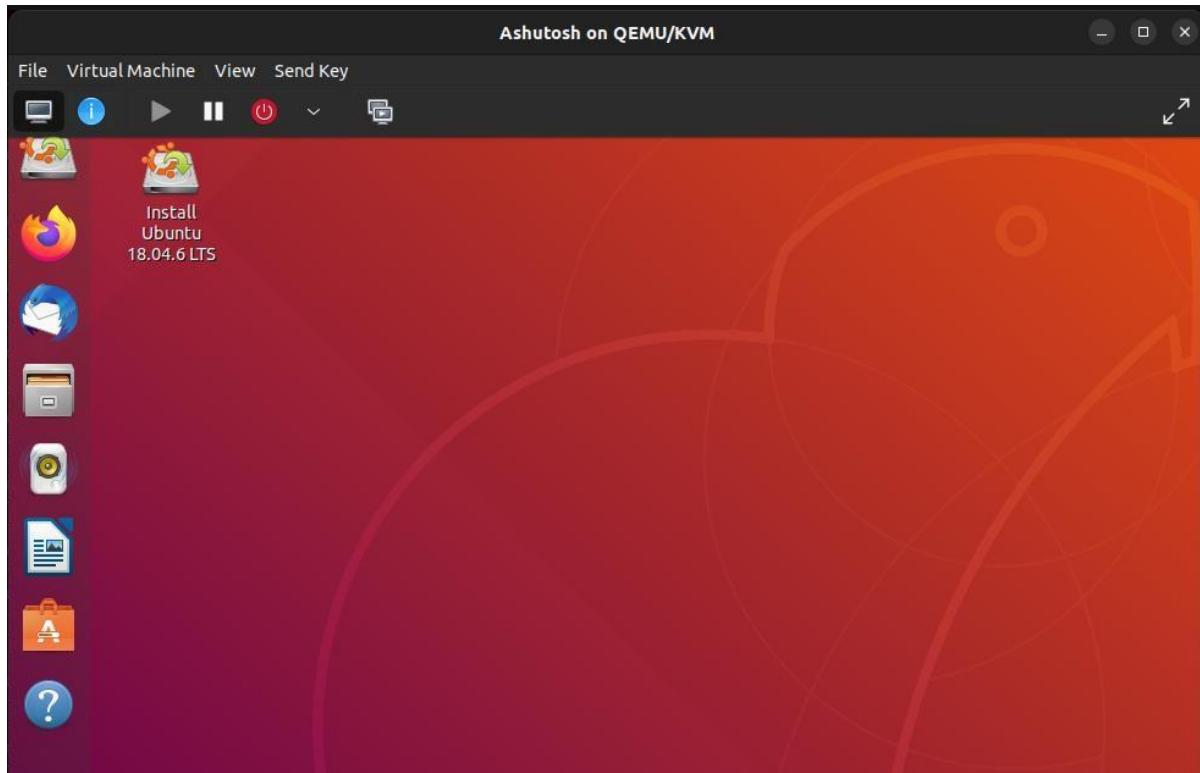
> Network selection

Cancel Back Finish

[Type here]



[Type here]





```
x = input("Type a number: ")
y = input("Type another number: ")
sum = int(x) + int(y)

print("The sum is: ", sum)
```

CONCLUSION:

There are the following advantages of PaaS -Simplified Development , Lower risk, Prebuilt business functionality, Instant community, Scalability

Disadvantages of PaaS cloud computing layer - Vendor lock-in , Data Privacy, Integration with the rest of the systems applications.

Practical No. 03

Aim: Study and implementation of Software as a Service

Theory: SaaS is also known as "On-Demand Software". It is a software distribution model in which services are hosted by a cloud service provider. These services are available to end-users over the internet so, the end-users do not need to install any software on their devices to access these services.

There are the following services provided by SaaS providers -

Business Services - SaaS Provider provides various business services to start-up the business. The SaaS business services include **ERP** (Enterprise Resource Planning), **CRM** (Customer Relationship Management), **billing**, and **sales**.

Document Management - SaaS document management is a software application offered by a third party (SaaS providers) to create, manage, and track electronic documents. Example: Slack, Samepage, Box, and Zoho Forms.

Social Networks - As we all know, social networking sites are used by the general public, so social networking service providers use SaaS for their convenience and handle the general public's information.

Mail Services - To handle the unpredictable number of users and load on e-mail services, many e-mail providers offering their services using SaaS.



[Type here]

Methods and Steps:

A. Using FOSS Server

The terminal window shows the following commands and output:

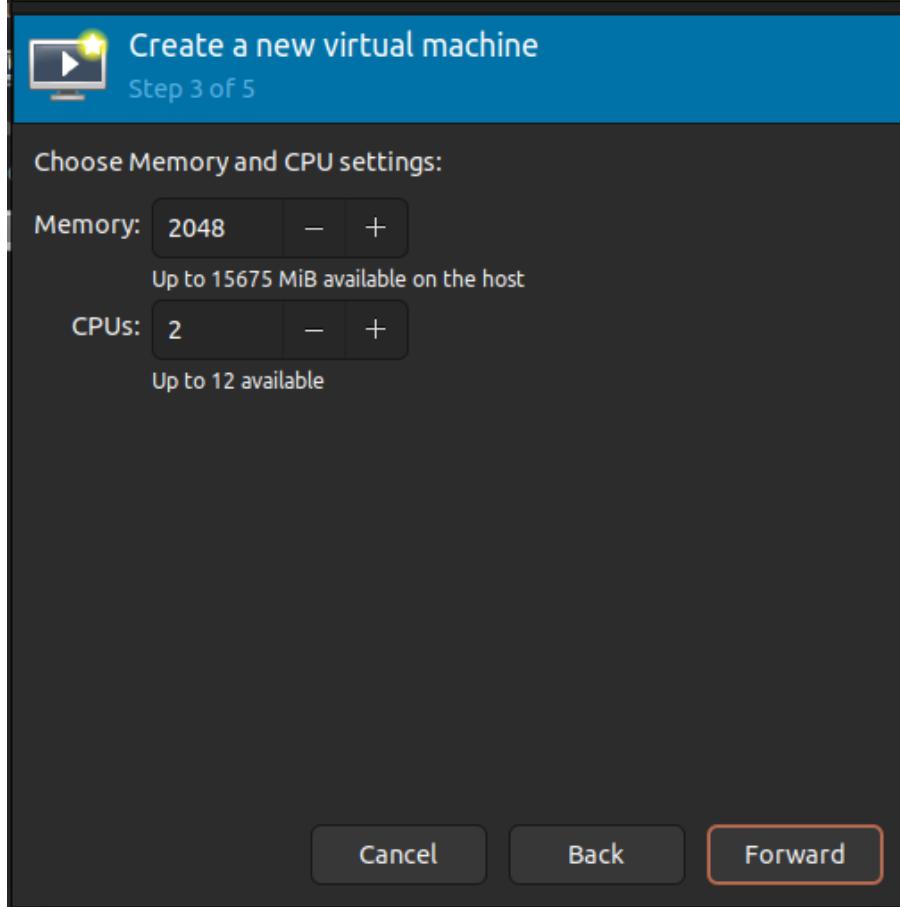
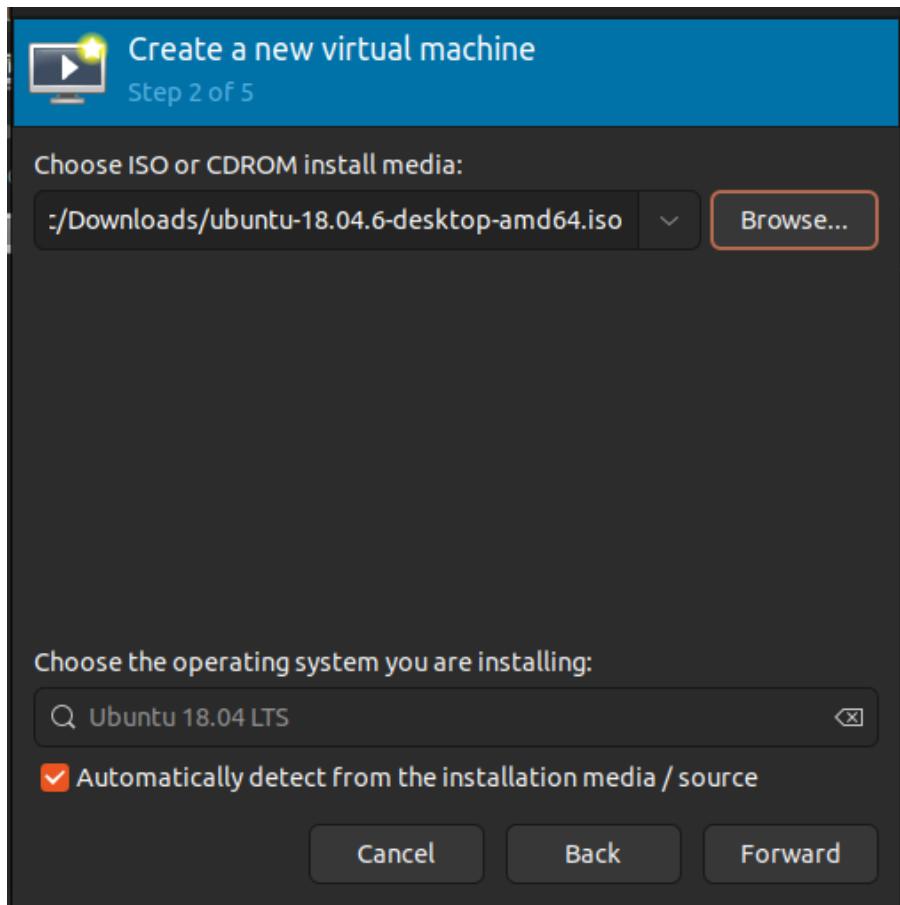
```
ashus@tcsc:~$ sudo adduser ashus libvirt
Adding user 'ashus' to group 'libvirt' ...
Adding user ashus to group libvirt
Done.
ashus@tcsc:~$ sudo adduser ashus kvm
Adding user 'ashus' to group 'kvm' ...
Adding user ashus to group kvm
Done.
ashus@tcsc:~$ sudo systemctl status libvirtd
● libvirtd.service - Virtualization daemon
  Loaded: loaded (/lib/systemd/system/libvirtd.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2023-02-02 10:18:00 IST; 1min ago
TriggeredBy: ● libvirtd-ro.socket
              ● libvirtd-admin.socket
              ● libvirtd.socket
  Docs: man:libvirtd(8)
        https://libvirt.org
 Main PID: 1139 (libvirtd)
   Tasks: 21 (limit: 32768)
  Memory: 42.2M
    CPU: 524ms
   CGroup: /system.slice/libvirtd.service
           ├─1139 /usr/sbin/libvirtd
           ├─1691 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/lib/libvirt/libvirt-dnsmasq
           ├─1692 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/lib/libvirt/libvirt-dnsmasq
Feb 02 10:18:00 tcsc.org systemd[1]: Started Virtualization daemon.
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: started, version 2.86 cachesize 150
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua TFTP conntrack ipset a...
Feb 02 10:18:03 tcsc.org dnsmasq-dhcp[1691]: DHCP, IP range 192.168.122.2 -- 192.168.122.254, lease time 1h
Feb 02 10:18:03 tcsc.org dnsmasq-dhcp[1691]: DHCP, sockets bound exclusively to interface virbr0
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: reading /etc/resolv.conf
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: using nameserver 127.0.0.53#53
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: read /etc/hosts - 7 addresses
ashus@tcsc:~$ sudo virt-manager
ashus@tcsc:~$
```

The Virt-Manager 'New VM' wizard is shown, Step 1 of 5, titled 'Create a new virtual machine'. It asks 'Connection: QEMU/KVM'. Below it, it says 'Choose how you would like to install the operating system' with the following options:

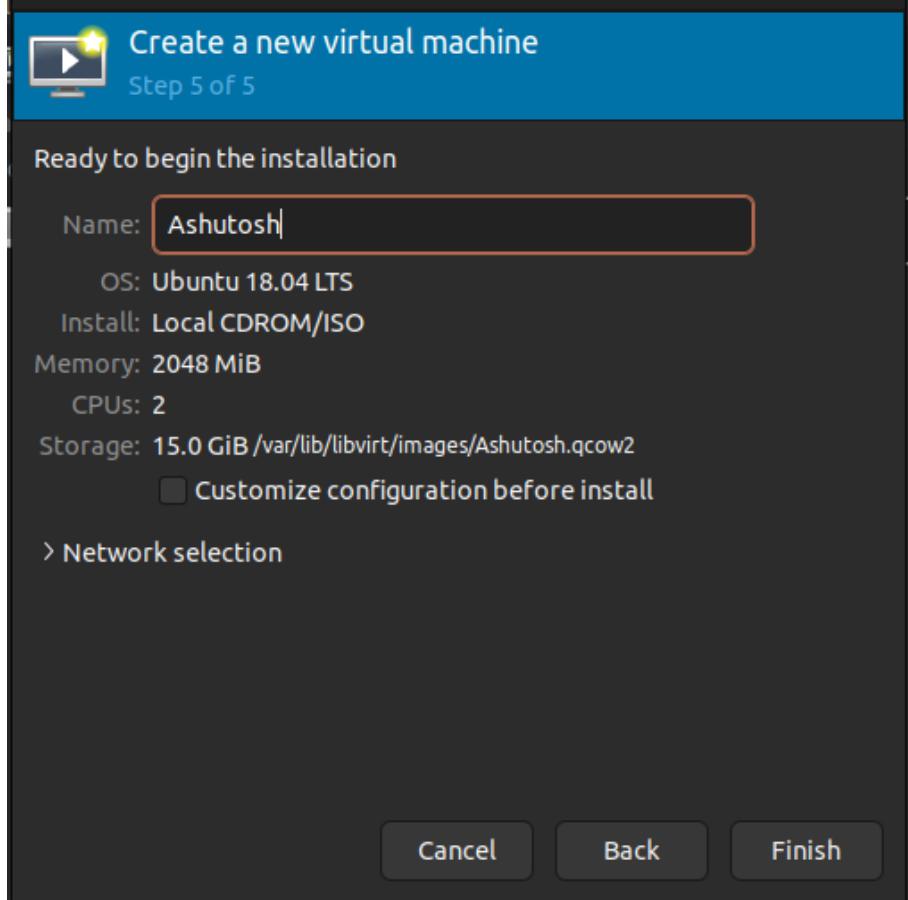
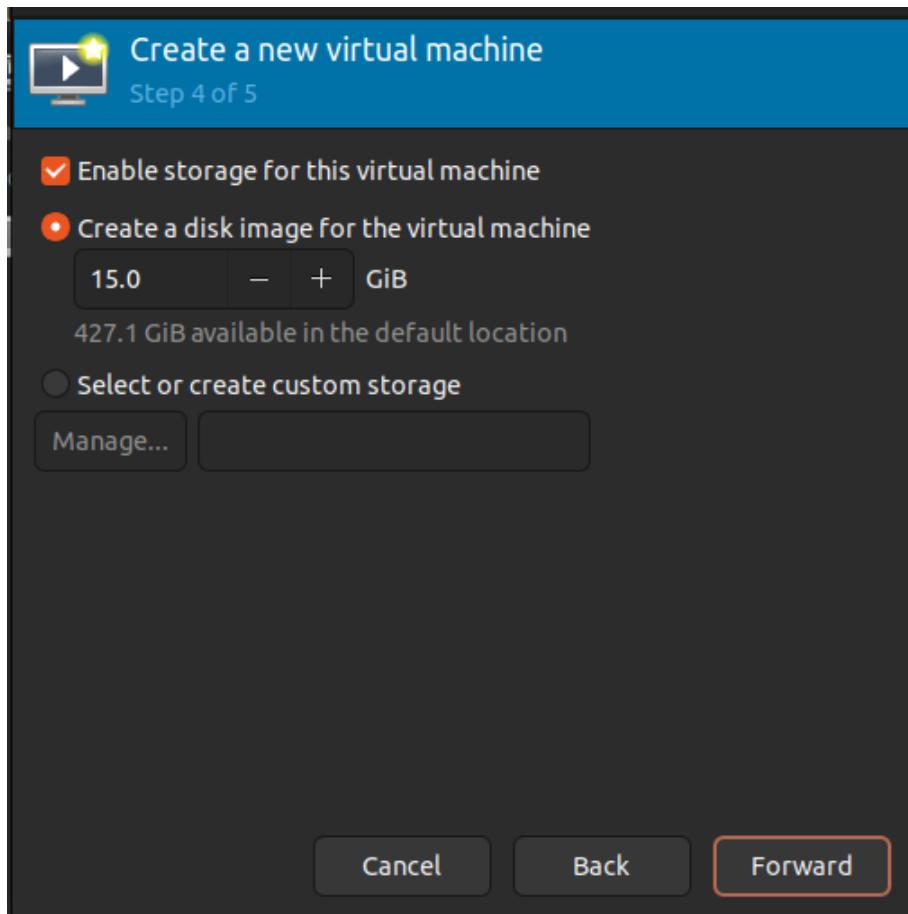
- Local install media (ISO image or CDROM)
- Network Install (HTTP, HTTPS, or FTP)
- Import existing disk image
- Manual install

At the bottom are 'Cancel', 'Back', and 'Forward' buttons.

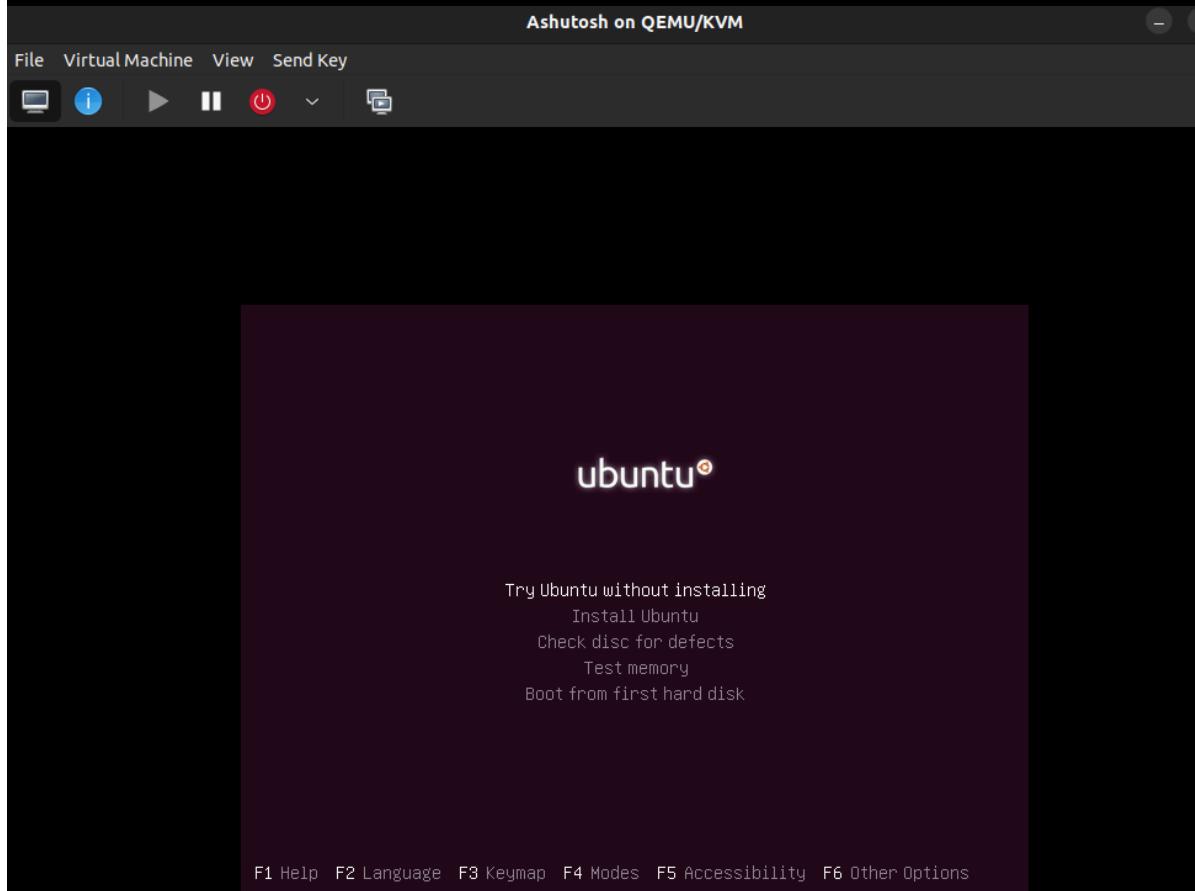
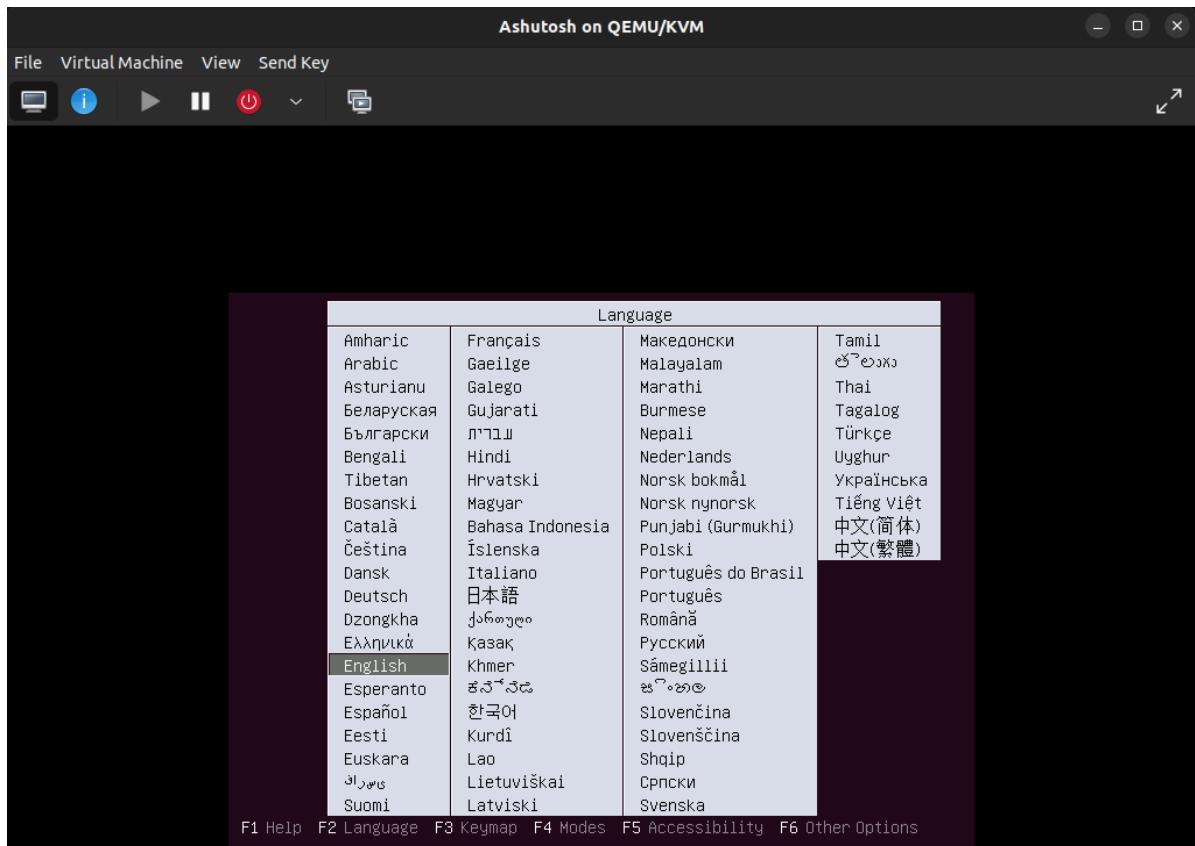
[Type here]



[Type here]



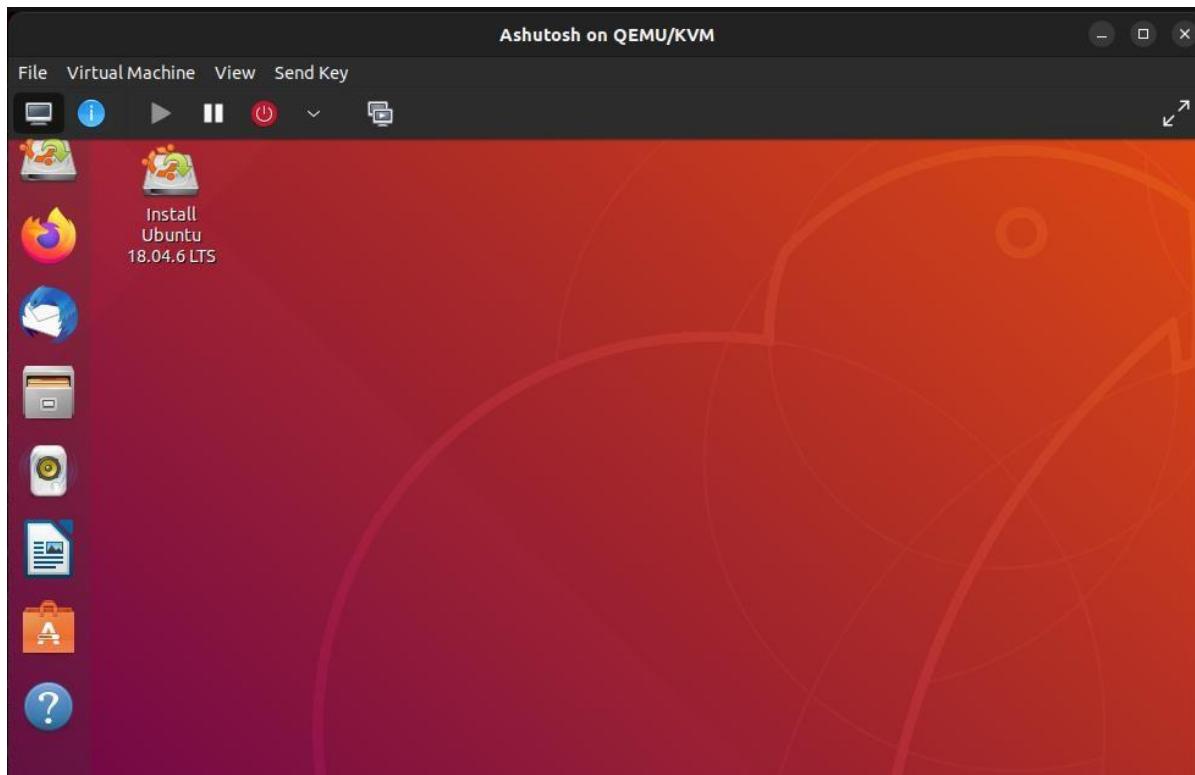
[Type here]



NAME : ASHUTOSH SINGH

ROLL NO : 478

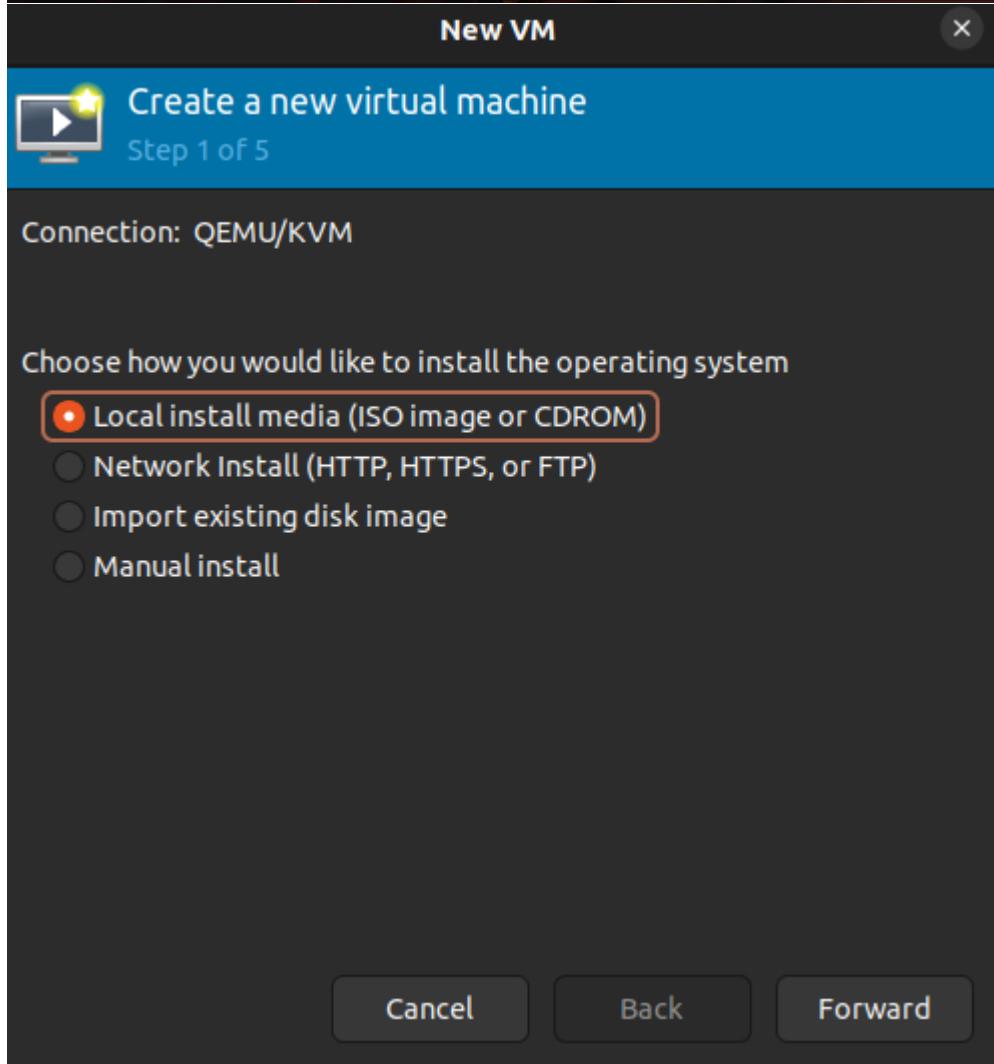
CLOUD COMPUTING JOURNAL



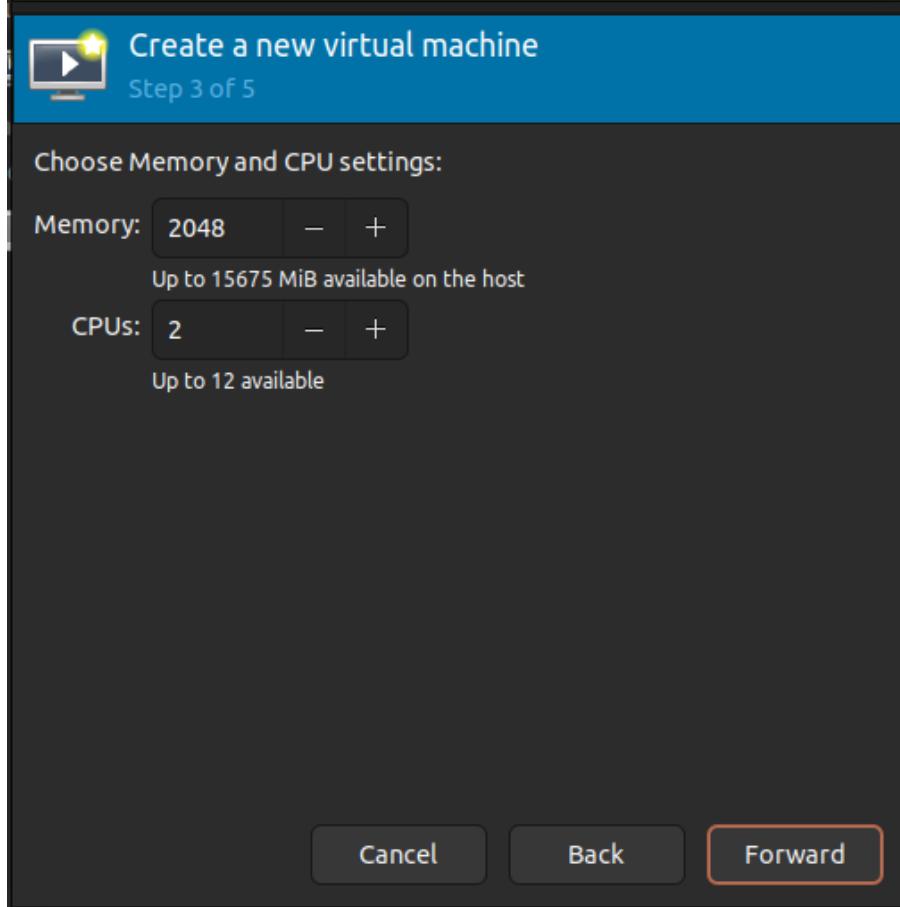
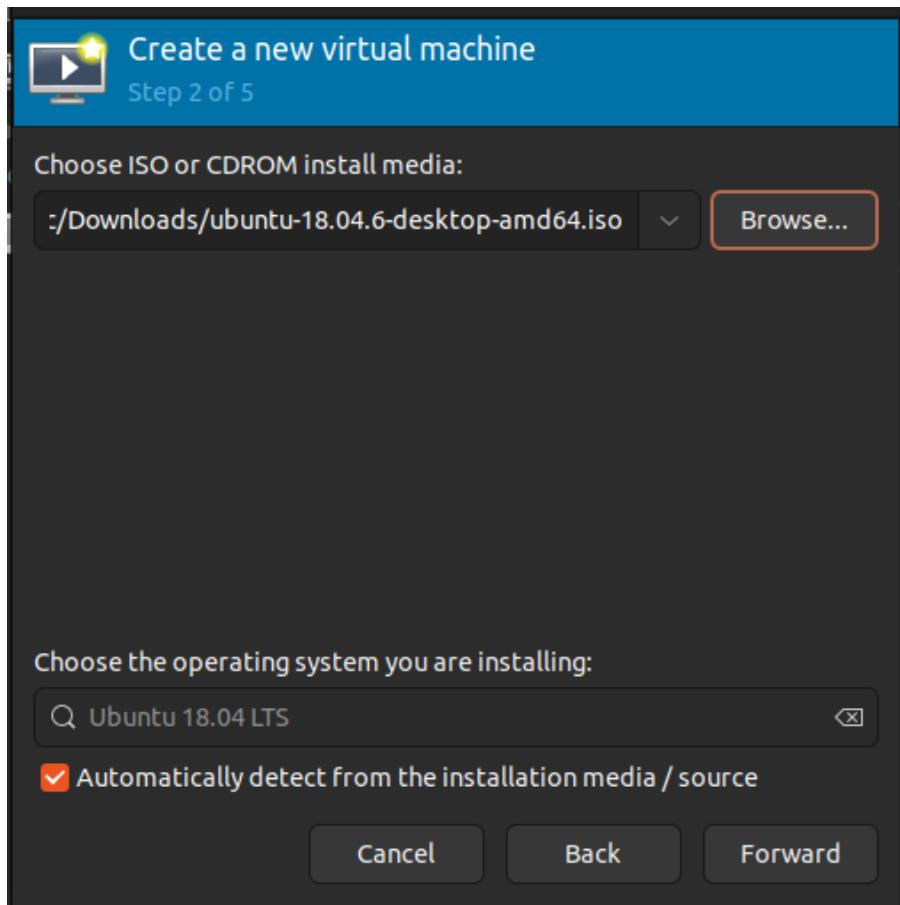
[Type here]

```
ashus@tcsc:~$ sudo adduser libvirt
Adding user 'ashus' to group 'libvirt'
Adding user ashus to group libvirt
Done.
ashus@tcsc:~$ sudo adduser kvm
Adding user 'ashus' to group 'kvm' ...
Adding user ashus to group kvm
Done.
ashus@tcsc:~$ sudo systemctl status libvirtd
● libvirtd.service - Virtualization daemon
   Loaded: loaded (/lib/systemd/system/libvirtd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-02-02 10:18:00 IST; 11min ago
     TriggeredBy: ● libvirtd-ro.socket
                  ● libvirtd-admin.socket
                  ● libvirtd.socket
   Docs: man:libvirtd(8)
         https://libvirt.org
 Main PID: 1139 (libvirtd)
   Tasks: 21 (limit: 32768)
  Memory: 42.2M
    CPU: 524ms
   CGroup: /system.slice/libvirtd.service
           └─1139 /usr/sbin/libvirtd
             ├─1691 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/lib/libvirt/libvirt-dnsmasq
             ├─1692 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/lib/libvirt/libvirt-dnsmasq
             └─1693 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/lib/libvirt/libvirt-dnsmasq

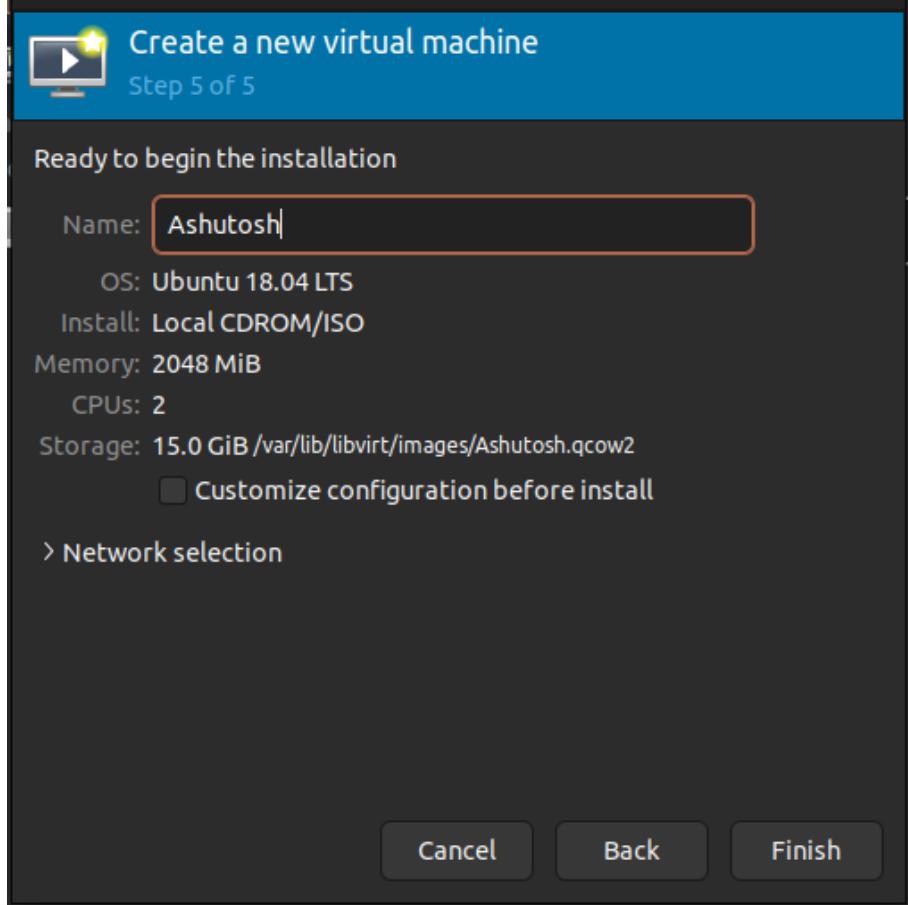
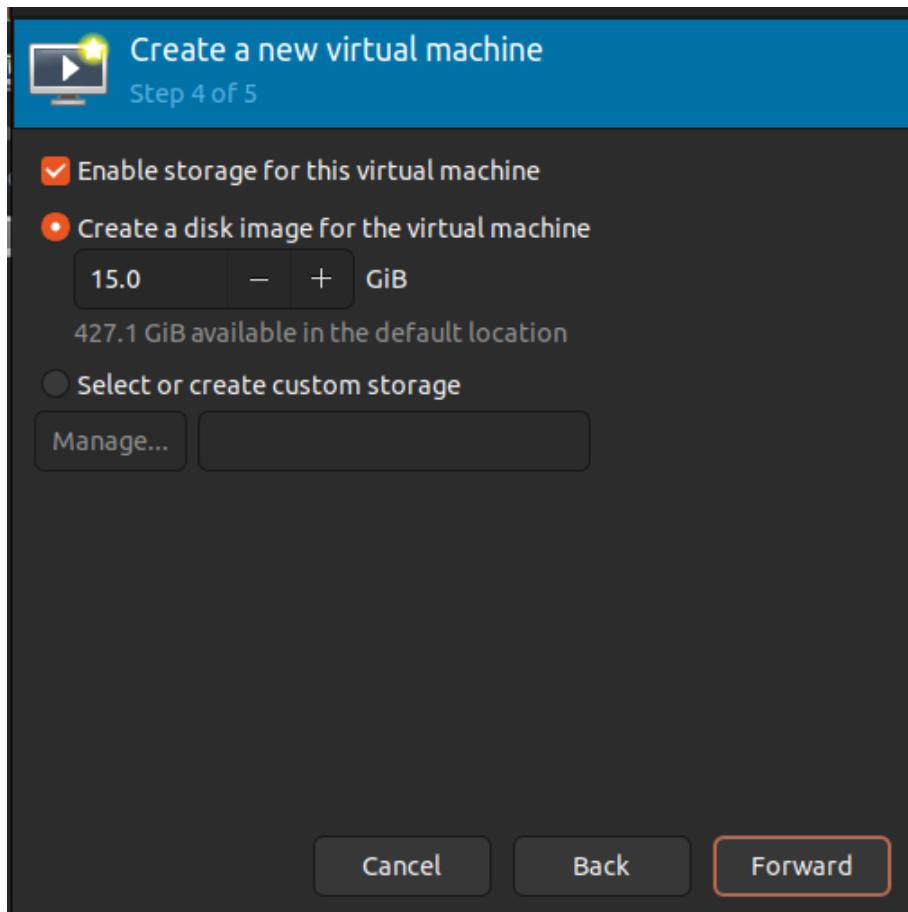
Feb 02 10:18:00 tcsc.org systemd[1]: Started Virtualization daemon.
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: started, version 2.86 cachetime 150
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua TFTP conntrack ipset a
Feb 02 10:18:03 tcsc.org dnsmasq-dhcp[1691]: DHCP, IP range 192.168.122.2 -- 192.168.122.254, lease time 1h
Feb 02 10:18:03 tcsc.org dnsmasq-dhcp[1691]: DHCP, sockets bound exclusively to interface virbr0
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: reading /etc/resolv.conf
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: using nameserver 127.0.0.53#53
Feb 02 10:18:03 tcsc.org dnsmasq[1691]: read /etc/hosts - 7 addresses
ashus@tcsc:~$ sudo virt-manager
ashus@tcsc:~$
```



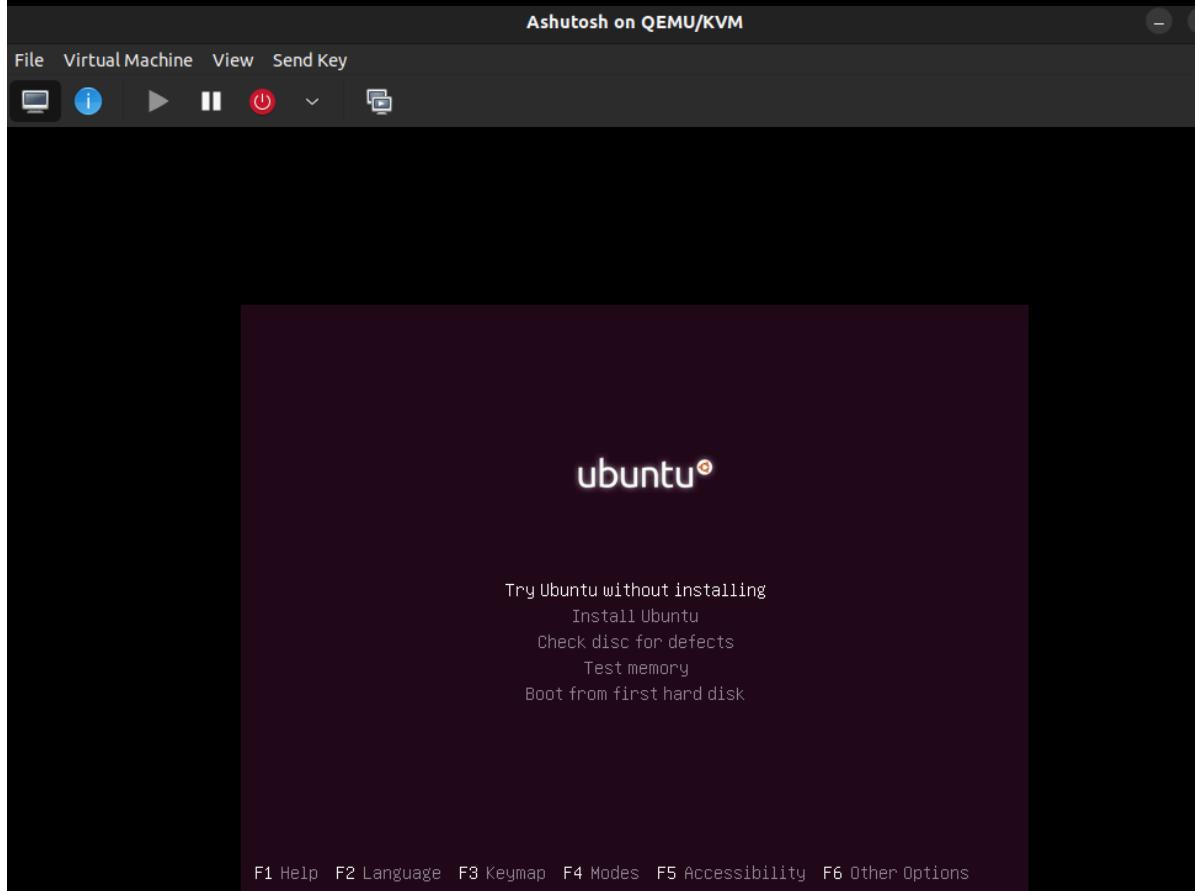
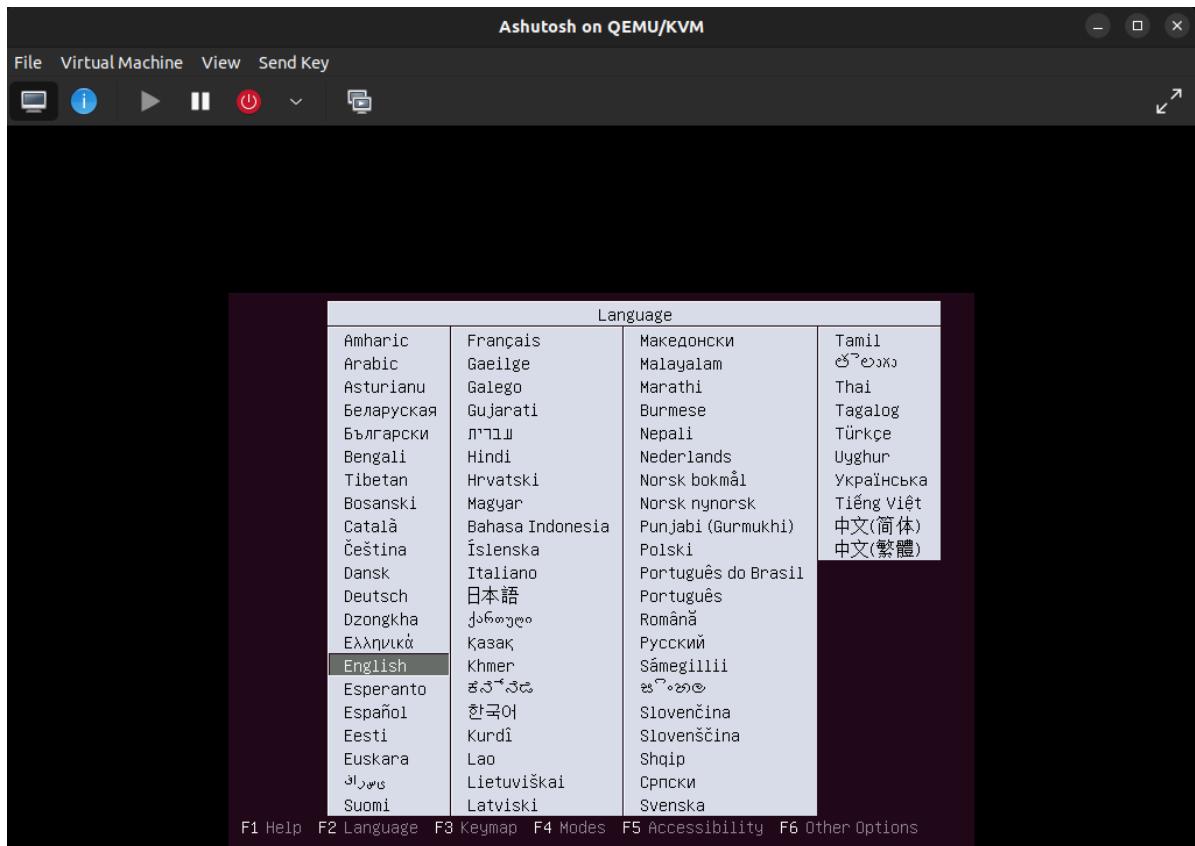
[Type here]



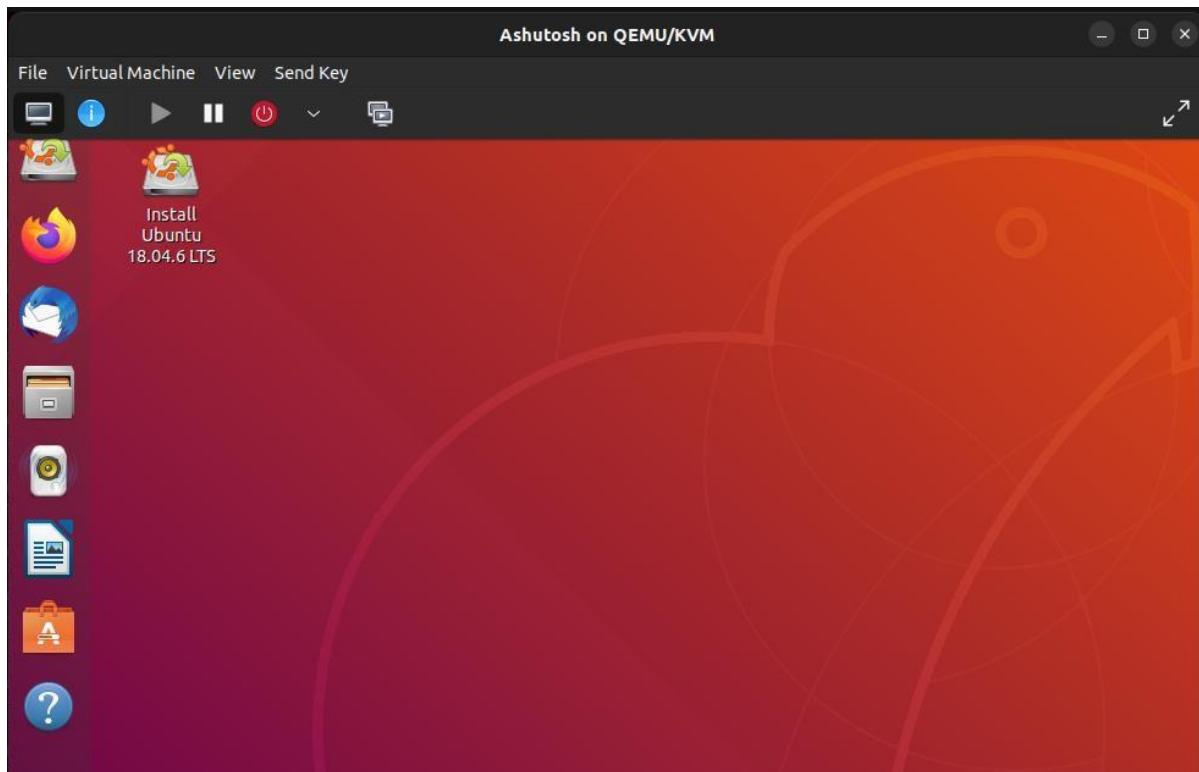
[Type here]

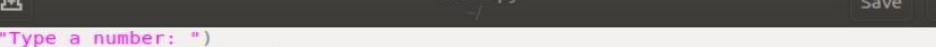


[Type here]



[Type here]





```
x = input("Type a number: ")
y = input("Type another number: ")
sum = int(x) + int(y)

print("The sum is: ", sum)
```

```
ubuntu@ubuntu: ~
File Edit View Search Terminal Help
ubuntu@ubuntu:~$ sudo gedit cloud.py

** (gedit:3549): WARNING **: 05:20:48.343: Set document metadata failed: Setting
attribute metadata::gedit-spell-language not supported

** (gedit:3549): WARNING **: 05:20:48.344: Set document metadata failed: Setting
attribute metadata::gedit-encoding not supported

** (gedit:3549): WARNING **: 05:24:29.149: Set document metadata failed: Setting
attribute metadata::gedit-spell-language not supported

** (gedit:3549): WARNING **: 05:24:29.150: Set document metadata failed: setting
attribute metadata::gedit-encoding not supported

** (gedit:3549): WARNING **: 05:24:30.777: Set document metadata failed: Setting
attribute metadata::gedit-position not supported
ubuntu@ubuntu:~$ python cloud.py
Type a number: 1
Type another number: 5
('The sum is: ', 6)
ubuntu@ubuntu:~$
```

[Type here]

. B.GCP/AWS/IBM/AZure/...

The screenshot shows the 'Launch an instance' wizard on the AWS EC2 service. The first step, 'Name and tags', is completed with the name 'Pradeep'. The 'Add additional tags' button is visible. Below it, the 'Application and OS Images (Amazon Machine Image)' section is expanded, showing a search bar and a 'Quick Start' link.

The screenshot shows the 'Amazon Machine Image (AMI)' details page. It highlights the 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type' entry, which is marked as 'Free tier eligible'. The page also displays the AMI ID 'ami-0aa7d40eeae50c9a9' and indicates '64-bit (x86)' architecture. A 'Verified provider' badge is present. Below this, the 'Instance type' section is partially visible.

[Type here]

The screenshot shows the 'Instance type' configuration step. It displays the selected instance type, t2.micro, which is free tier eligible. The instance has 1 vCPU and 1 GiB Memory. Pricing information is provided for On-Demand Windows, SUSE, RHEL, and Linux. A 'Compare instance types' link is available. Below this, the 'Key pair (login)' section is shown, requiring a key pair name (vockey) and a 'Create new key pair' button. The 'Network settings' section is also visible.

The screenshot shows the 'Network settings' configuration step. It requires selecting a VPC (vpc-0b42b196fd6d6612b) and a Subnet (No preference). An 'Auto-assign public IP' option is set to 'Enable'. Under 'Firewall (security groups)', it says a security group controls traffic to the instance. It offers 'Create security group' (selected) or 'Select existing security group' options. The security group name is specified as 'launch-wizard-1'. A note states the name can't be edited after creation and must be 255 characters long, with valid characters defined.

[Type here]

The screenshot shows the AWS CloudFormation Launch Wizard interface. At the top, there's a navigation bar with the AWS logo, a search bar, and a "Services" dropdown set to "CloudFormation". Below the navigation bar, a message states: "length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#@[]+=&;{}!\$*".

Inbound security groups rules

Security group rule 1 (TCP, 22)

Type: ssh **Protocol**: TCP **Port range**: 22

Source type: Custom **Source**: Add CIDR, prefix list or security group **Description**: e.g. SSH for admin desktop

Add security group rule

Remove

Configure storage

Advanced

1x 8 GiB gp2 ▾ Root volume (Not encrypted)

Allow tags in metadata

Disable

User data - optional

Enter custom user data into the field below

```
#!/bin/bash
yum update -y
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello World!</h1></html>' > /var/www/html/index.html
```

User data has already been base64 encoded

[Type here]

The screenshot shows two main sections of the AWS EC2 interface.

Top Section: This section displays a success message after launching an instance. It includes a green checkmark icon, the word "Success", and the text "Successfully initiated launch of instance (i-027156bede9973c67)". Below this, there is a "Launch log" table with three rows:

Step	Status
Initializing requests	Succeeded
Creating security groups	Succeeded
Launch initiation	Succeeded

Bottom Section: This section is titled "Next Steps - preview". It contains a search bar with the placeholder text "What would you like to do next with this instance, for example "create alarm" or "create backup"" and a list of recommended actions:

- Create a new RDS database (with "Learn more" link)
- Manage detailed monitoring (with "Manage detailed monitoring" button)
- Create Load Balancer (with "Create Load Balancer" button)
- Manage instance tags (with "Manage instance tags" button)

CLOUD COMPUTING JOURNAL

The screenshot shows the AWS EC2 Instances page. At the top, there's a navigation bar with the AWS logo, 'Services' (with a dropdown arrow), a search bar containing 'Search [Alt+S]', and account information for 'N. Virginia'. A blue box highlights the 'New EC2 Experience' link and the 'Tell us what you think' feedback button. The main content area has a title 'Instances (1) Info' with a refresh button, a connect button, and an instance selection button. Below is a search bar with placeholder text 'Find instance by attribute or tag (case-sensitive)'. A table lists one instance: 'pradeep' (Name), 'i-027156bede9973c67' (Instance ID), and 'Running' (Instance state). On the left sidebar, under 'Instances', the 'Instances' option is selected, and a list of related services is shown: Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, and Capacity Reservations.

This screenshot is identical to the one above, showing the AWS EC2 Instances page with one running instance named 'pradeep'. The layout, filters, and sidebar options are exactly the same, including the 'Instances' section being selected in the sidebar.

[Type here]

The screenshot shows the AWS EC2 Instances and Security Groups pages side-by-side.

EC2 Instances Page:

- Left Sidebar:** New EC2 Experience, EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations.
- Header:** Instances (1/1) Info, Find instance by attribute or tag (case-sensitive).
- Table:** status | Availability Zone | Public IPv4 DNS | Public IPv4 ...
rms + us-east-1b ec2-3-238-156-5.comp... 3.238.156.5
- Instance Details:** Instance: i-027156bede9973c67 (pradeep)
Details | Security | Networking | Storage | Status checks | Monitor
- Instance Summary:** Instance ID: i-027156bede9973c67 (pradeep), Public IPv4 address: 3.238.156.5 | open address, IPv6 address: -, Instance state: Running

Security Groups Page:

- Left Sidebar:** Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups selected, Elastic IPs, Placement Groups).
- Header:** Security Groups (1/3) Info, Actions, Export security groups to CSV, Create security group.
- Table:** Name | Security group ID | Security group name | VPC ID | Description
sg-00fd4427ba916ad41 | launch-wizard-1 | vpc-0d72f1ef7a012357a | launch-wizard-1
sg-0ac9940a1585c6e2b | Security group for my ... | vpc-0d72f1ef7a012357a | launch-wizard-1
sg-0e7727e6273695a67 | default | vpc-0d72f1ef7a012357a | default VPC sec
- Inbound Rules:** Manage tags, Edit inbound rules, Filter security group rules
Name | Security group rule... | IP version | Type | Protocol

[Type here]

The screenshot shows two overlapping AWS EC2 interface windows. The top window is titled 'Edit inbound rules' and displays a message stating 'This security group has no inbound rules.' with a 'Add rule' button. The bottom window shows the main EC2 dashboard with a sidebar containing links like 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', 'Instances', 'Launch Templates', and 'Spot Requests'. A green notification bar at the top of the dashboard says 'Inbound security group rules successfully modified on security group (sg-00fd4427ba916ad41 | launch-wizard-1)'. The main content area shows a table of security groups with columns: Name, Security group ID, Security group name, VPC ID, and Description. One row is selected, showing 'sg-00fd4427ba916ad41' under 'Name'.

Name	Security group ID	Security group name	VPC ID	Description
sg-00fd4427ba916ad41	launch-wizard-1	vpc-0d72f1ef7a012357a	launch-wizard-1	SG for launch-wizard-1
sg-0ac9940a1585c6e2b	Security group for my ...	vpc-0d72f1ef7a012357a	launch-wizard-1	SG for my application
sg-0e7727e6273695a67	default	vpc-0d72f1ef7a012357a	default	Default VPC security group

Hello World!

CONCLUSION :

Advantages of SaaS cloud computing layer :SaaS is easy to buy, One to Many ,Less hardware required for SaaS, Low maintenance required for SaaS, No special software or hardware versions required.

Disadvantages of SaaS cloud computing layer :Security, Latency issue, Total Dependency on Internet, Switching between SaaS vendors is difficult.

Practical No 4

Aim: Study and implementation of Storage as a Service

Theory: Storage as a service (STaaS) is a managed service in which the provider supplies the customer with access to a data storage platform. The service can be delivered on premises from infrastructure that is dedicated to a single customer, or it can be delivered from the public cloud as a shared service that's purchased by subscription and is billed according to one or more usage metrics.

STaaS customers access individual storage services through standard system interface protocols or application program interfaces (APIs). Typical offerings include bare-metal storage capacity; raw storage volumes; network file systems; storage objects; and storage applications that support file sharing and backup lifecycle management.

Storage as a service was originally seen as a cost-effective way for small and mid-size businesses that lacked the technical personnel and capital budget to implement and maintain their own storage infrastructure. Today, companies of all sizes use storage as a service.

Storage as a service in cloud computing

Instead of storing data on-premises, organizations that use STaaS will typically utilize a public cloud for storage and backup needs. Public cloud storage may also use different storage methods for STaaS. These storage methods include backup and restore, disaster recovery, block storage, SSD storage, object storage and bulk data transfer. Backup and restore refers to the backing up of data to the cloud, which provides protection in case of data loss. Disaster recovery may refer to protecting and replicating data from virtual machines (VMs).

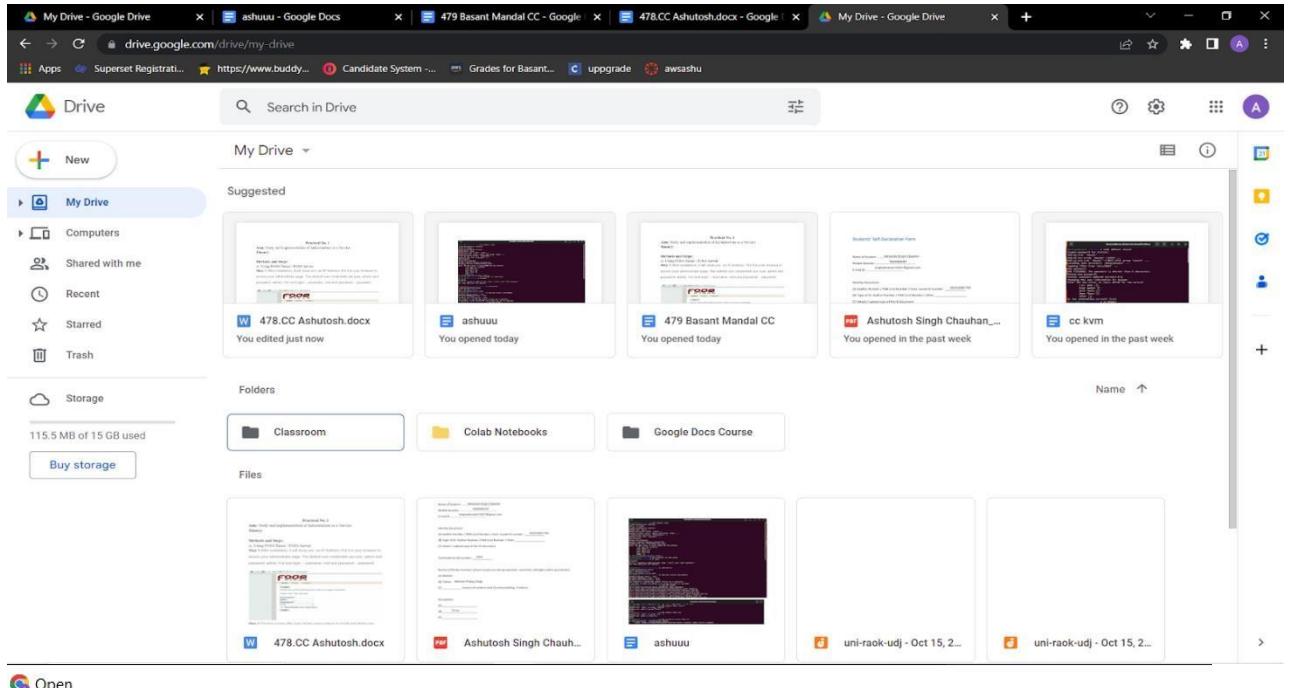
Block storage enables customers to provision block storage volumes for lower-latency I/O. SSD storage is another storage type that is typically used for intensive read/write and I/O operations. Object storage systems are used in data analytics, disaster recovery and cloud applications and tend to have high latency. Cold

[Type here]

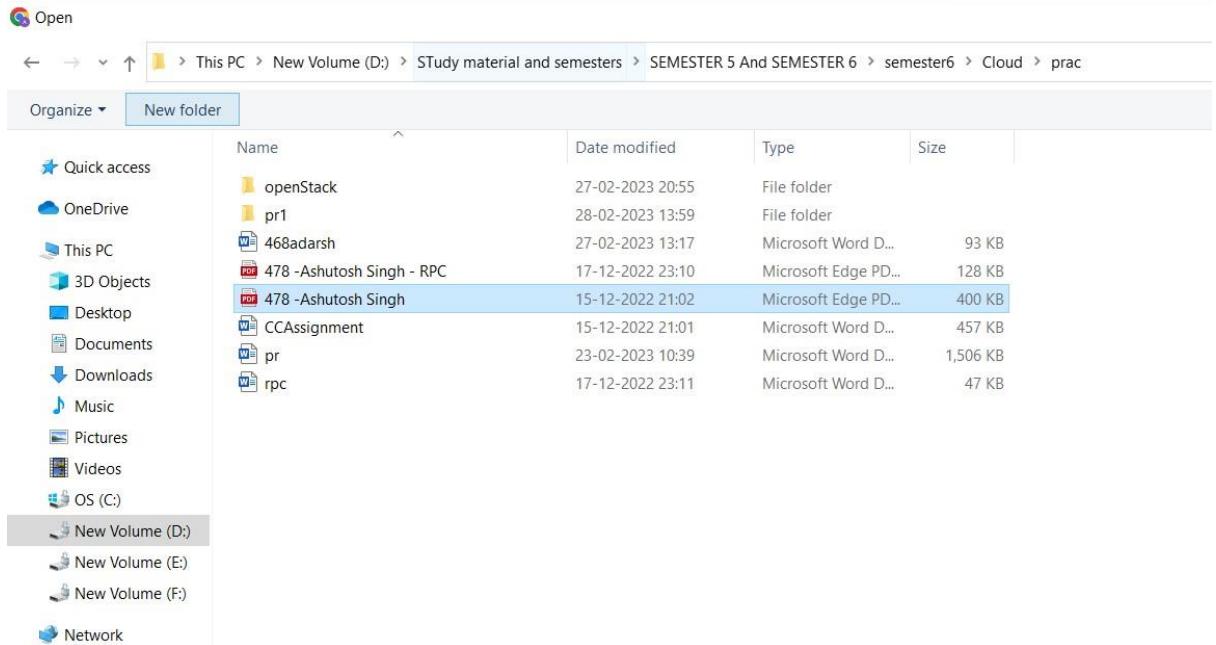
storage is used to create and configure stored data quickly. Bulk data transfers will use disks and other hardware to transfer data.

Methods and Steps:

A. Google Drive

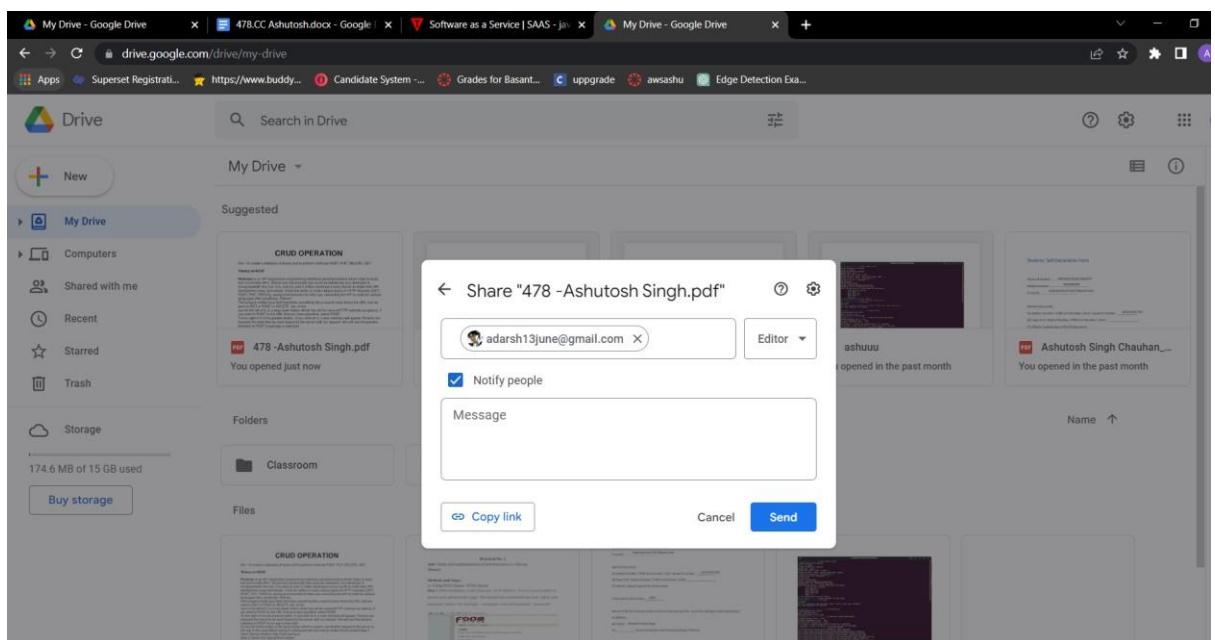
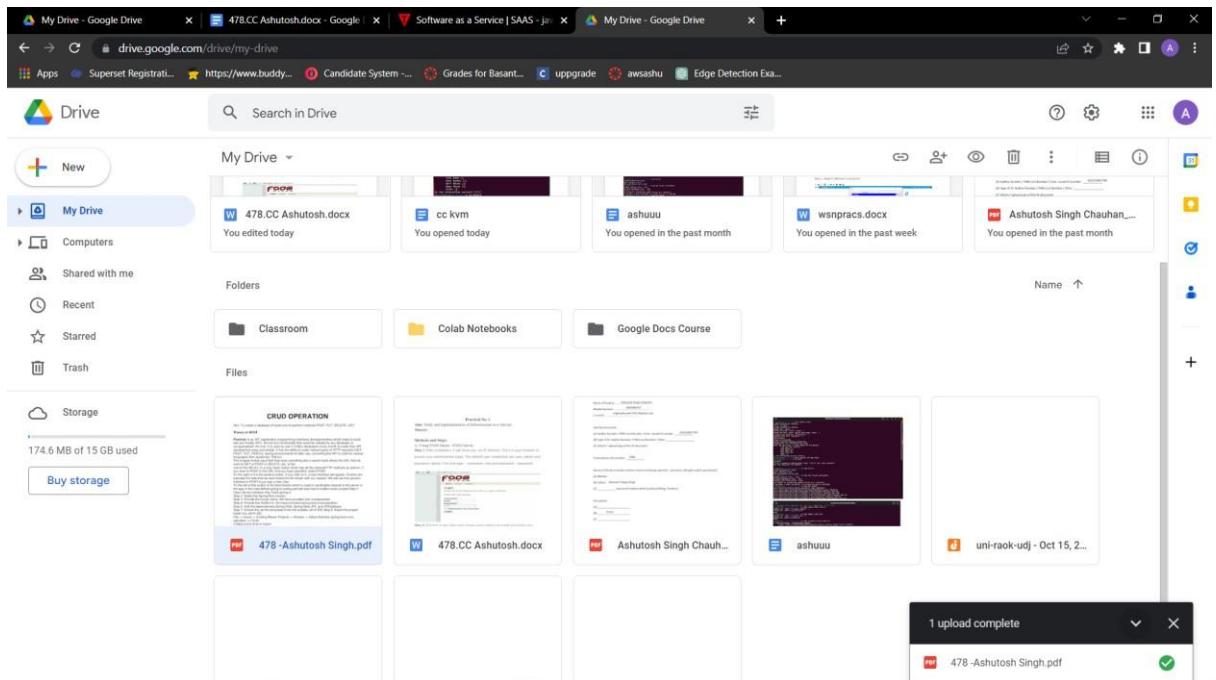


The screenshot shows the Google Drive web interface. On the left, there's a sidebar with 'My Drive' selected. It includes sections for 'Computers', 'Shared with me', 'Recent', 'Starred', 'Trash', 'Storage' (115.5 MB of 15 GB used), and 'Buy storage'. The main area displays 'Suggested' files like '478.CC Ashutosh.docx' and 'ashuuu'. Below that are 'Folders' for 'Classroom', 'Colab Notebooks', and 'Google Docs Course'. Under 'Files', there are several documents and files, including '478.CC Ashutosh.docx', 'Ashutosh Singh Chauhan...', 'ashuuu', 'uni-raok-udj - Oct 15, 2...', and 'cc kvm'. A search bar at the top says 'Search in Drive'.



The screenshot shows a Windows File Explorer window. The address bar indicates the path: 'This PC > New Volume (D:) > Study material and semesters > SEMESTER 5 And SEMESTER 6 > semester6 > Cloud > prac'. The left sidebar shows quick access, OneDrive, This PC, 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, OS (C:), and network locations for 'New Volume (D:)', 'New Volume (E:)', and 'New Volume (F:)'. The main pane lists files and folders in the 'prac' folder, including 'openStack', 'pr1', '468adarsh', '478 -Ashutosh Singh - RPC', '478 -Ashutosh Singh', 'CCAssignment', 'pr', and 'rpc'. The file '478 -Ashutosh Singh' is currently selected.

[Type here]



[Type here]

B. OwnCloud (Offline)

The screenshot shows a terminal window titled "bitnami-owncloud [Running] - Oracle VM VirtualBox". The window displays the following text:

```
*** Welcome to the ownCloud packaged by Bitnami ***
*** Built using Debian 11 - Kernel 5.10.0-19-amd64 (tty1). ***

*** You can access the application at http://192.168.0.115 ***
*** The default username and password is 'user' and '1W6EDyfiOBr1'. ***
*** You can find out more at https://docs.bitnami.com/virtual-machine/apps/owncloud/ ***

***** To access the console, please use login 'bitnami'
and password 'bitnami' *****

debian login: bitnami
Password:
Linux debian 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

At the bottom of the terminal window, there is a toolbar with icons for copy, paste, cut, and others, followed by the text "Right Ctrl".

The screenshot shows a web browser window titled "Settings - ownCloud". The address bar shows "Not secure | 192.168.0.116/index.php/settings/personal". The page displays the following settings:

- Personal** tab selected.
- General** section:
 - Profile picture: A purple circle with a white letter "A".
 - Full name: Ashutosh
 - Email: user@example.com
 - Groups: admin
- Admin** tab selected.
 - Apps**: No apps listed.
 - General**: No general settings listed.
 - Storage**: No storage settings listed.
 - Encryption**: No encryption settings listed.
 - Sharing**: No sharing settings listed.
 - Help & Tips**: No help & tips listed.
 - Additional**: No additional settings listed.

[Type here]

The screenshot shows the 'Users' page of the ownCloud web interface. At the top, there is a search bar and a dropdown menu for 'Ashutosh'. Below the header, there is a table with columns: Username, E-Mail, Groups, Create, Username, Full Name, Password, Groups, Group Admin for, and Quota. There are two users listed: 'Everyone' (Ashutosh) and 'Admins' (user). Both users have 'admin' as their group and 'no group' as their group admin. Their quotas are set to 'Default'.

The screenshot shows the 'Files' page of the ownCloud web interface. At the top, there is a search bar and a dropdown menu for 'Ashutosh'. Below the header, there is a sidebar with links: All files, Favorites, Shared with you, Shared with others, Shared by link, and Tags. The main area shows a list of files in the 'Ty478' folder. The files are: Linu.png, photo.jpg, photo-min.jpg, and sign.jpg. The file sizes are 424 KB, 584 KB, 418 KB, and 99 KB respectively. The total size is 1.5 MB.

C. Owncloud (Online) Demo.owncloud.org

The screenshot shows the login page of the ownCloud website. The page has a dark blue background with the ownCloud logo at the top. A message box contains the text: 'Username: demo', 'Password: demo', and 'Do not upload sensitive or personal data! The instance is automatically reset every hour.' Below the message box, there are input fields for 'Username or email' (containing 'demo') and 'Password' (containing '....'). A 'Login' button is located below the password field. At the bottom of the page, there is a footer with the text 'ownCloud - A safe home for all your data'.

[Type here]

The screenshot shows the ownCloud web interface. On the left, a sidebar lists navigation options: All files, Favorites, Shared with you, Shared with others, Shared by link, and Tags. The main area displays a list of files and folders under the path 'All files > 478Ashutosh'. The list includes:

Name	Type	Size	Last Modified
478Ashutosh	Folder	121 KB	seconds ago
Documents	Folder	35 KB	an hour ago
Learn more about ownCloud	Folder	3.5 MB	an hour ago
Photos	Folder	922.9 MB	37 minutes ago

Below the list, it says '4 folders' and '926.5 MB'. To the right, there's an 'Activities' section showing two recent events:

- You created 478Ashutosh (a minute ago)
- You created 478Ashutosh (a minute ago)

This screenshot shows a detailed view of a file within the '478Ashutosh' folder. The path is 'demo.owncloud.org/apps/files/?dir=478Ashutosh&fileid=339'. The list shows one item:

Name	Type	Size	Modified
Screenshot (88).png	Image	121 KB	4 months ago

Below the list, it says '1 file' and '121 KB'.

CONCLUSION :

Advantages of STaaS

Key advantages to STaaS in the enterprise include the following:

- Storage costs. Personnel, hardware and physical storage space expenses are reduced.
- Disaster recovery. Having multiple copies of data stored in different locations can better enable disaster recovery measures.
- Scalability. With most public cloud services, users only pay for the resources that they use.
- Syncing. Files can be automatically synced across multiple devices.
- Security. Security can be both an advantage and a disadvantage, as security methods may change per vendor. Data tends to be encrypted during transmission and while at rest.

Practical No. 5

Aim: User Management in Cloud .

Theory: User management describes the ability for administrators to manage user access to various IT resources like systems, devices, applications, storage systems, networks, SaaS services, and more.

- User management is a core part to any directory service and is a basic security essential for any organization.
- User management enables admins to control user access and on-board and off-board users to and from IT resources.
- Subsequently a directory service will then authenticate, authorize, and audit user access to IT resources based on what the IT admin had dictated.
- Traditionally, user management has been grounded with on-prem servers, databases, and closed virtual private networks (VPN). However, recent trends are seeing a shift towards cloud-based identity and access management (IAM), granting administrators even greater control over digital assets.

User management allows administrators to manage resources and organize users according to their needs and roles while maintaining the security of IT systems. Administrators need powerful user management capabilities that can allow them to group users and define flexible access policies.

For end-users, many parts of user management are invisible. When users are exposed to user management—for example, when they use a login box to access an application—they expect the interaction to be simple and seamless. Login is a frequently-performed, critical operation, meaning that any delay or malfunction annoys users and hurts productivity. Many organizations recognize that on-premise IdP solutions are insufficient for the modern IT environment. Users increasingly rely on cloud services and access corporate systems remotely, often via personal devices, and traditional IdP cannot address these use cases.

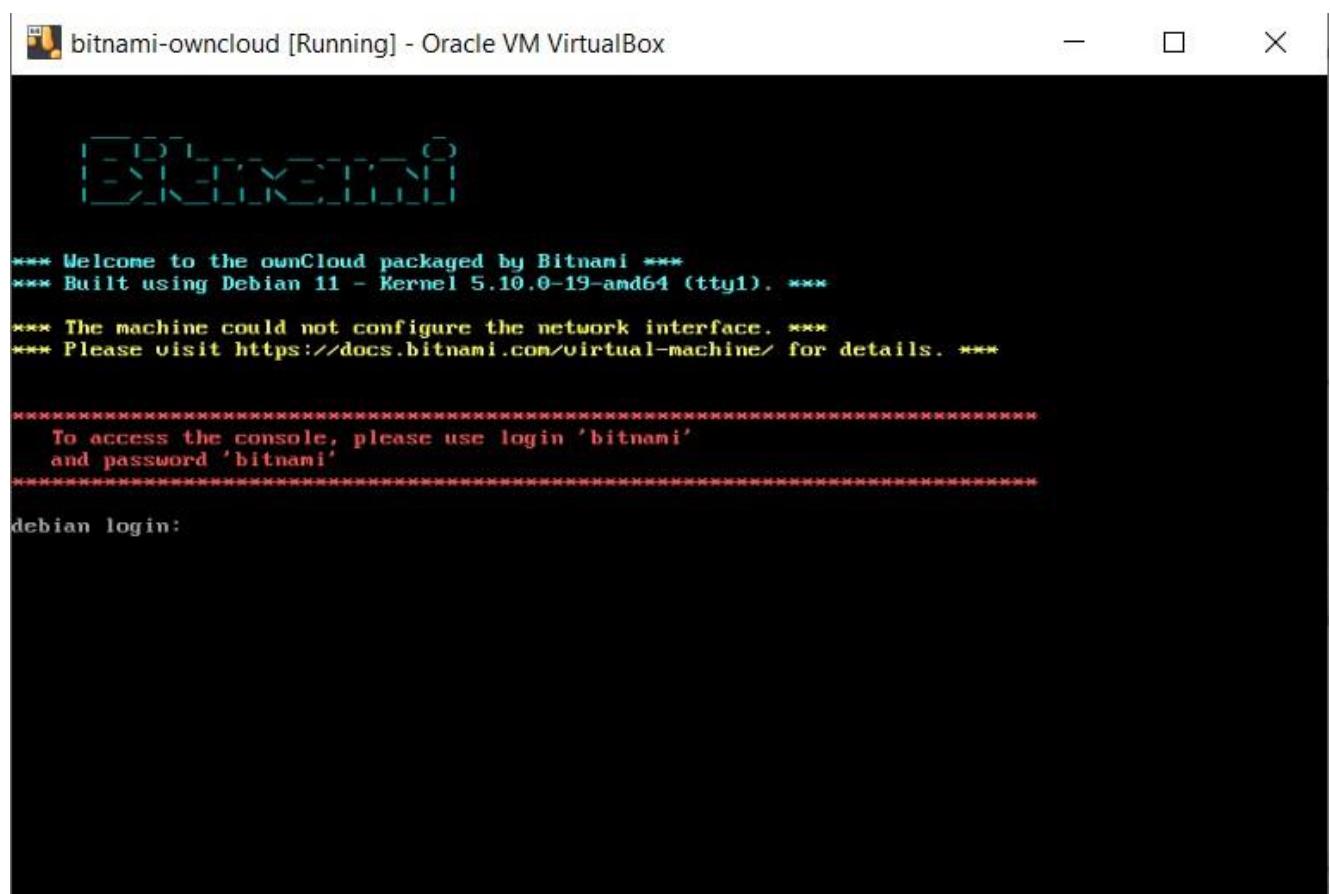
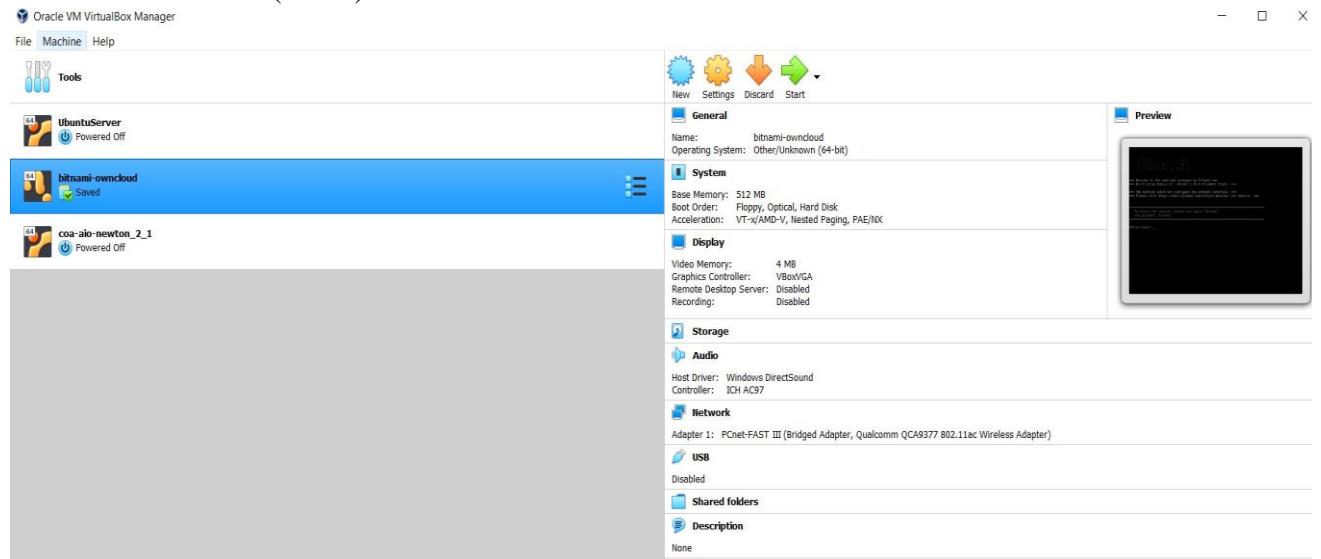
Organizations must find a way to manage secure access for a distributed environment. At the same time, users demand the same simplicity of popular services like Google and Facebook in their work environment. These challenges

CLOUD COMPUTING JOURNAL

are making user management more important and more complex than ever before.

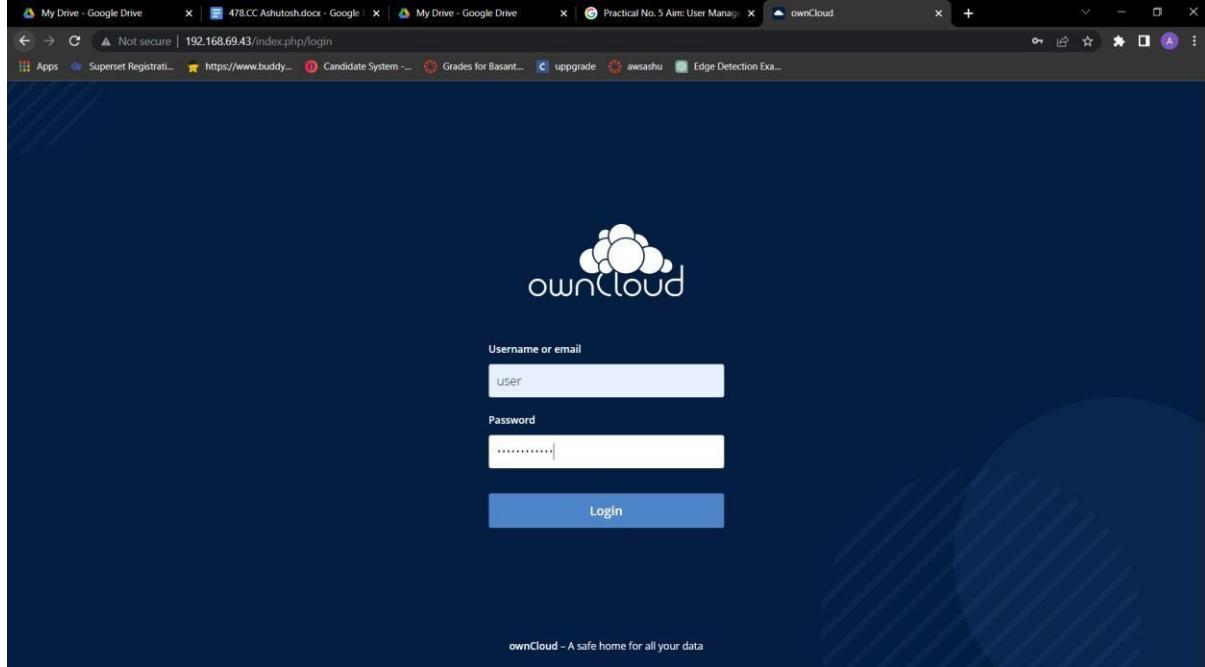
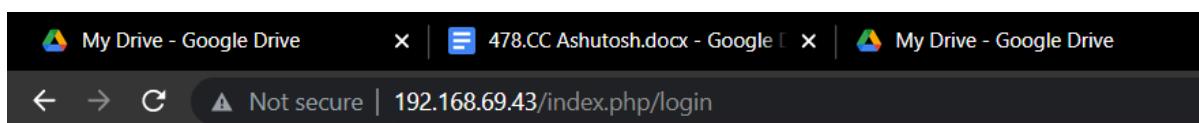
Methods and Steps:

A. OwnCloud(local)

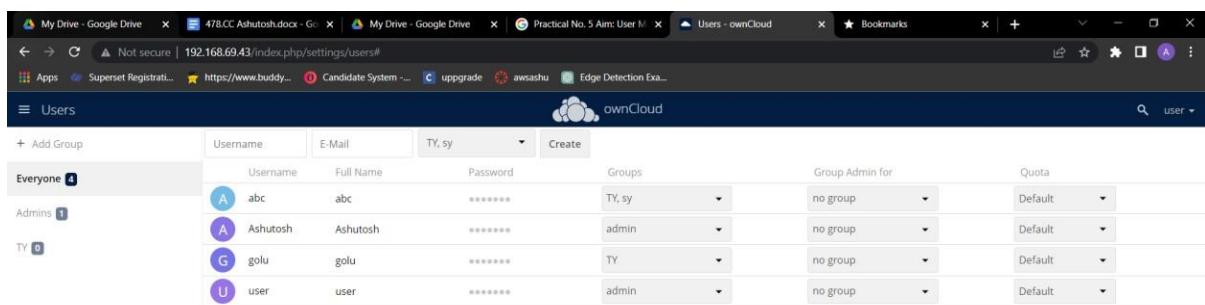
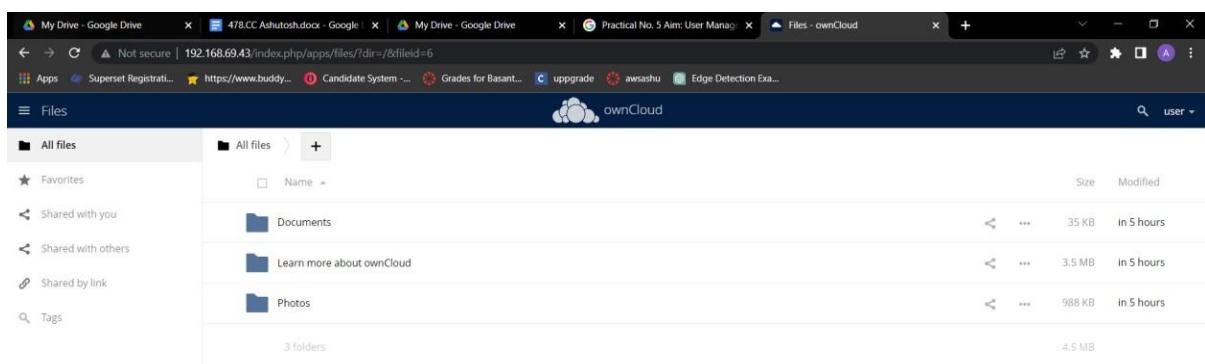
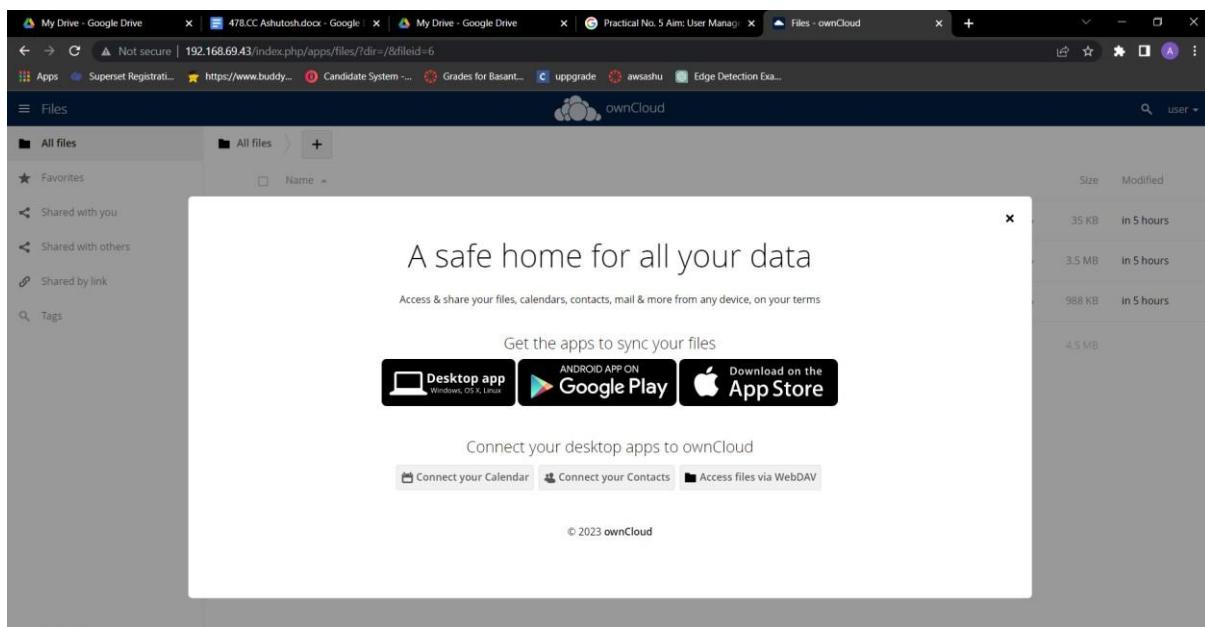


[Type here]

```
bitnami-owncloud [Running] - Oracle VM VirtualBox  
*** You can access the application at http://192.168.69.43 ***  
*** The default username and password is 'user' and 'n1xCJ92NdR8J'. ***  
*** You can find out more at https://docs.bitnami.com/virtual-machine/apps/owncloud/ ***  
  
***** To access the console, please use login 'bitnami'  
and password 'bitnami'*****  
  
debian login: bitnami  
Password:  
Linux debian 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
  
***** Welcome to the ownCloud packaged by Bitnami 10.11.0-9  
*** Documentation: https://docs.bitnami.com/virtual-machine/apps/owncloud/  
*** https://docs.bitnami.com/virtual-machine/  
*** Bitnami Forums: https://github.com/bitnami/oms/  
***  
* Please insert the new user password *  
* The default password is 'bitnami' *  
*****  
Changing password for bitnami.  
Current password:
```



[Type here]



[Type here]

The screenshot shows the ownCloud user management interface. A modal dialog box titled "Delete user" is displayed, asking if you are sure you want to permanently delete the user "golu". The dialog has "No" and "Yes" buttons. In the background, the user list table shows four users: abc, Ashutosh, golu, and user. The "golu" row is selected.

Username	Full Name	Password	Groups	Group Admin for	Quota
abc	abc	*****	TY, sy	no group	Default
Ashutosh	Ashutosh	*****	admin	no group	Default
golu	golu	*****	TY	no group	Default
user	user	*****	admin	no group	Default

DELETE USER GOLU:

The screenshot shows the ownCloud user management interface after the "golu" user has been deleted. The user list table now shows three users: abc, Ashutosh, and user.

Username	Full Name	Password	Groups
abc	abc	*****	TY, sy
Ashutosh	Ashutosh	*****	admin
user	user	*****	admin

USERS :

The screenshot shows the ownCloud user management interface displaying all four users: abc, Ashutosh, golu, and user. The "golu" user is visible in the list.

Username	Full Name	Password	Groups	Group Admin for	Quota
abc	abc	*****	TY, sy	no group	Default
Ashutosh	Ashutosh	*****	admin	no group	Default
golu	golu	*****	TY	no group	Default
user	user	*****	admin	no group	Default

[Type here]

The top screenshot shows the 'Users' page in the ownCloud web interface. The table lists the following users:

Username	E-Mail	Groups	Group Admin for	Quota
Adarsh	Adarsh	TCSC	no group	Default
Ashutosh	Ashu	admin	no group	Default
Sanket	Sanket	TCSC	no group	Default
satyam	satyam	TCSC	no group	Default
saurabh	saurabh	TCSC	no group	Default
Shardanand	Shardanand	TCSC	no group	Default
user	Ashutosh	admin	no group	Default
Vaishakh	Vaishakh	TCSC	no group	Default

The bottom screenshot shows the 'Personal' settings page for a user. The left sidebar shows navigation options like General, Storage, Sharing, Security, Additional, Apps, and General. The main area displays the following information:

- Profile picture: A large purple circle with a white letter 'U'.
- Full name: Ashutosh478
- Email: user@example.com
- Groups: You are member of the following groups: admin

CONCLUSION : Successfully Performed User Management in Cloud.....

Practical No.6

Aim: Study and implement Identity and Access Management (IAM) in AWS..

Theory:

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

IAM features

IAM gives you the following features:

1. Shared access to your AWS account

You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.

2. Granular permissions

You can grant different permissions to different people for different resources. For example, you might allow some users complete access to Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift, and other AWS services. For other users, you can allow read-only access to just some S3 buckets, or permission to administer just some EC2 instances, or to access your billing information but nothing else.

3. Secure access to AWS resources for applications that run on Amazon EC2

You can use IAM features to securely provide credentials for applications that run on EC2 instances. These credentials provide permissions for your application to access other AWS resources. Examples include S3 buckets and DynamoDB tables.

4. Identity federation

You can allow users who already have passwords elsewhere—for example, in your corporate network or with an internet identity provider—to get temporary access to your AWS account.

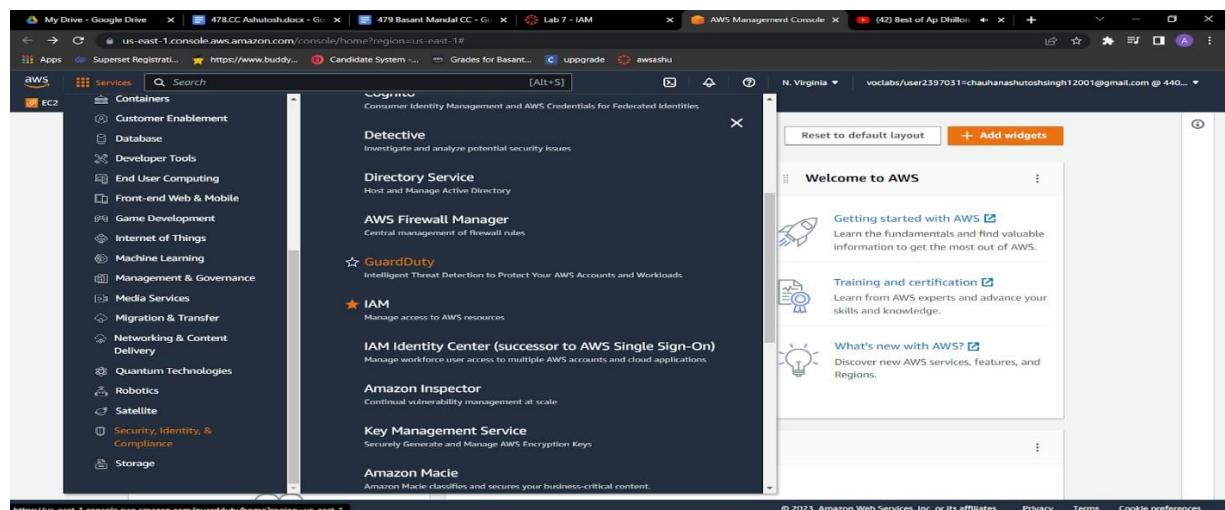
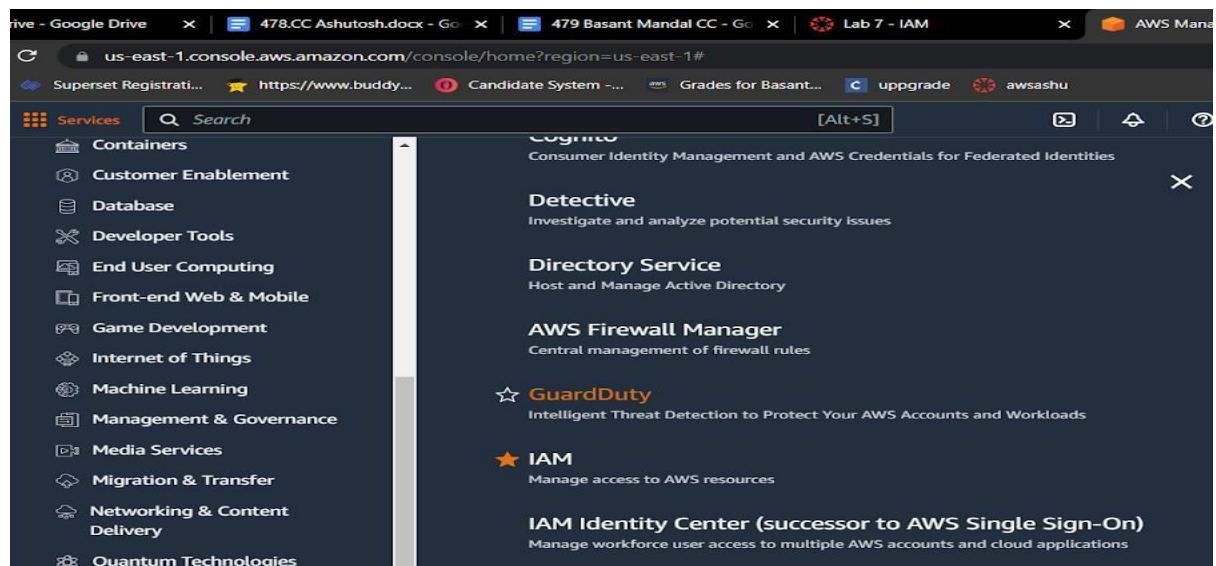
5. Free to use

AWS Identity and Access Management (IAM) and AWS Security Token Service (AWS STS) are features of your AWS account offered at no additional charge. You are charged only when you access other AWS services using your IAM users or AWS STS temporary security credentials

[Type here]

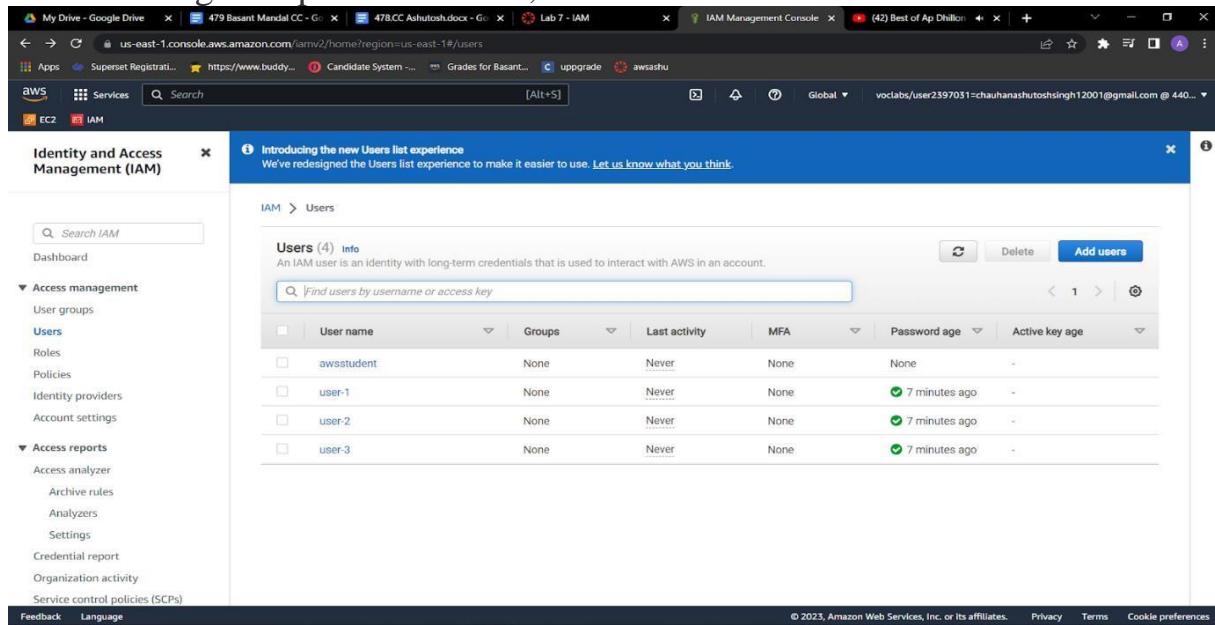
Steps:

1. Choose the **Services** menu, locate the **Security, Identity, & Compliance** services, and choose **IAM**



[Type here]

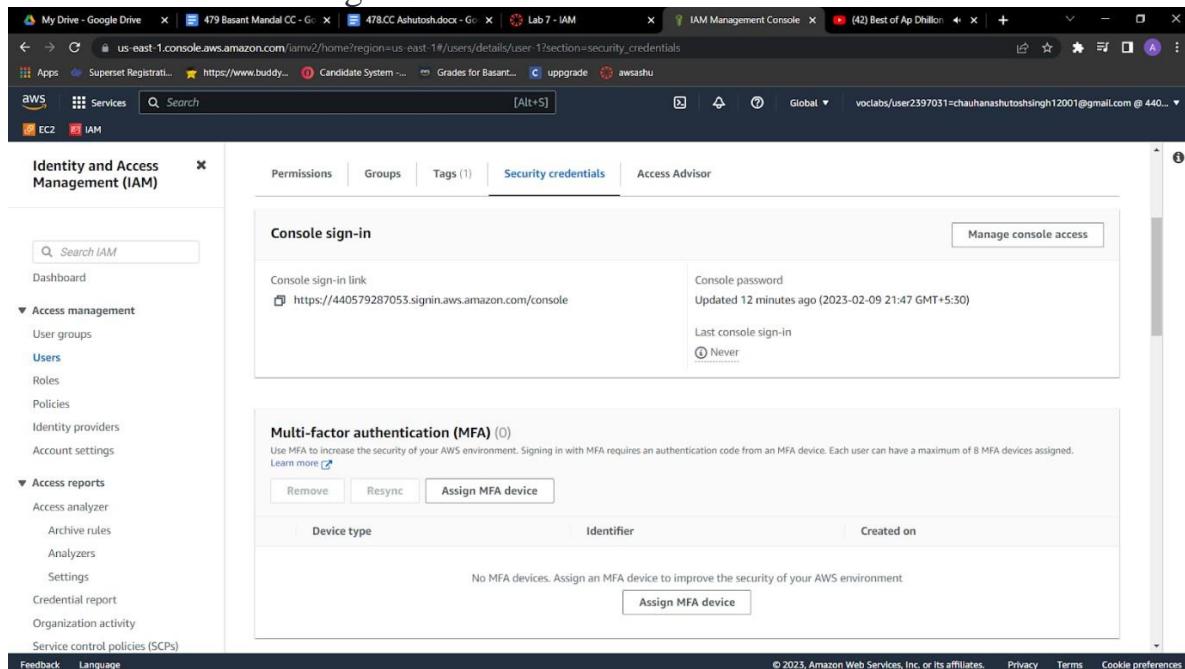
2. In the navigation pane on the left, choose **Users**. Create Users



The screenshot shows the AWS IAM Management Console. On the left, the navigation pane is open with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'Users' is also selected. The main content area displays a table titled 'Users (4) Info'. The table has columns for 'User name', 'Groups', 'Last activity', 'MFA', 'Password age', and 'Active key age'. Four users are listed: 'awsstudent' (None, Never, None, None), 'user-1' (None, Never, None, 7 minutes ago), 'user-2' (None, Never, None, 7 minutes ago), and 'user-3' (None, Never, None, 7 minutes ago). A blue banner at the top says 'Introducing the new Users list experience'.

3. Choose the **Security credentials** tab.

Notice that user-1 is assigned a **Console password**. This allows the user to access the AWS Management Console.



The screenshot shows the AWS IAM Management Console with the 'Security credentials' tab selected for user-1. The 'Console sign-in' section shows a 'Console sign-in link' (https://440579287053.signin.aws.amazon.com/console) and a 'Console password' (Updated 12 minutes ago (2023-02-09 21:47 GMT+5:30)). The 'Multi-factor authentication (MFA)' section indicates 'No MFA devices. Assign an MFA device to improve the security of your AWS environment'.

4. In the navigation pane on the left, choose **User groups**. The following groups have already been created for you: EC2-Admin , EC2-Support , S3-Support

[Type here]

The screenshot shows the AWS IAM Management Console. On the left, there's a navigation sidebar with options like 'Identity and Access Management (IAM)', 'User groups', 'Users', 'Roles', 'Policies', etc. The main area is titled 'User groups' and shows a table with three rows:

Group name	Users	Permissions	Creation time
EC2-Admin	>Loading	>Loading	16 minutes ago
EC2-Support (selected)	▲ 0	>Loading	16 minutes ago
S3-Support	>Loading	>Loading	16 minutes ago

5. Choose the name of the **EC2-Support** group.

This brings you to the summary page for the **EC2-Support** group.

The screenshot shows the AWS IAM Management Console. The left sidebar is identical to the previous screenshot. The main area is titled 'EC2-Support' and has a green header bar with the text 'Users added to this group.' Below this, it says 'Summary' and shows the following details:

User group name	Creation time	ARN
EC2-Support	February 09, 2023, 21:46 (UTC+05:30)	arn:aws:iam::440579287053:group/spl66/EC2-Support

Below this, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Users' tab is selected and shows a table with one row:

User name	Groups	Last activity	Creation time
user-1	1	None	20 minutes ago

6. Choose the **Permissions** tab.

This group has a managed policy called **AmazonEC2ReadOnlyAccess** associated with it. Managed policies are prebuilt policies (built either by AWS or by your administrators) that can be attached to IAM users and groups. When the policy is updated, the changes to the policy are immediately applied against

[Type here]

all users and groups that are attached to the policy.

The screenshot shows the AWS IAM Management Console. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'User groups' is also selected. In the main content area, it shows a 'User groups > EC2-Support' page. A green banner at the top says 'Users added to this group.' Below it, the 'EC2-Support' group is listed with a summary table. The 'Permissions' tab is selected. Under 'Permissions policies (1)', it lists 'AmazonEC2ReadOnlyAccess' as an AWS managed policy. At the bottom right of the main content area, there are links for 'Feedback', 'Language', 'Privacy', 'Terms', and 'Cookie preferences'.

7.Under Policy Name, choose the link for the AmazonEC2ReadOnlyAccess policy.

The screenshot shows the AWS IAM Management Console. The navigation sidebar has 'Policies' selected under 'Access management'. In the main content area, it shows the 'Policies > AmazonEC2ReadOnlyAccess' page. The 'Summary' section shows the Policy ARN as 'arn:aws:iam:aws:policy/AmazonEC2ReadOnlyAccess' and a description 'Provides read only access to Amazon EC2 via the AWS Management Console.'. The 'Permissions' tab is selected. Below it, a table shows the permissions granted to various services:

Service	Access level	Resource	Request condition
CloudWatch	Limited: List, Read	All resources	None
EC2	Limited: List	All resources	None
EC2 Auto Scaling	Full: Read Limited: List	All resources	None
ELB	Full: List, Read	All resources	None
ELB v2	Full: Read	All resources	None

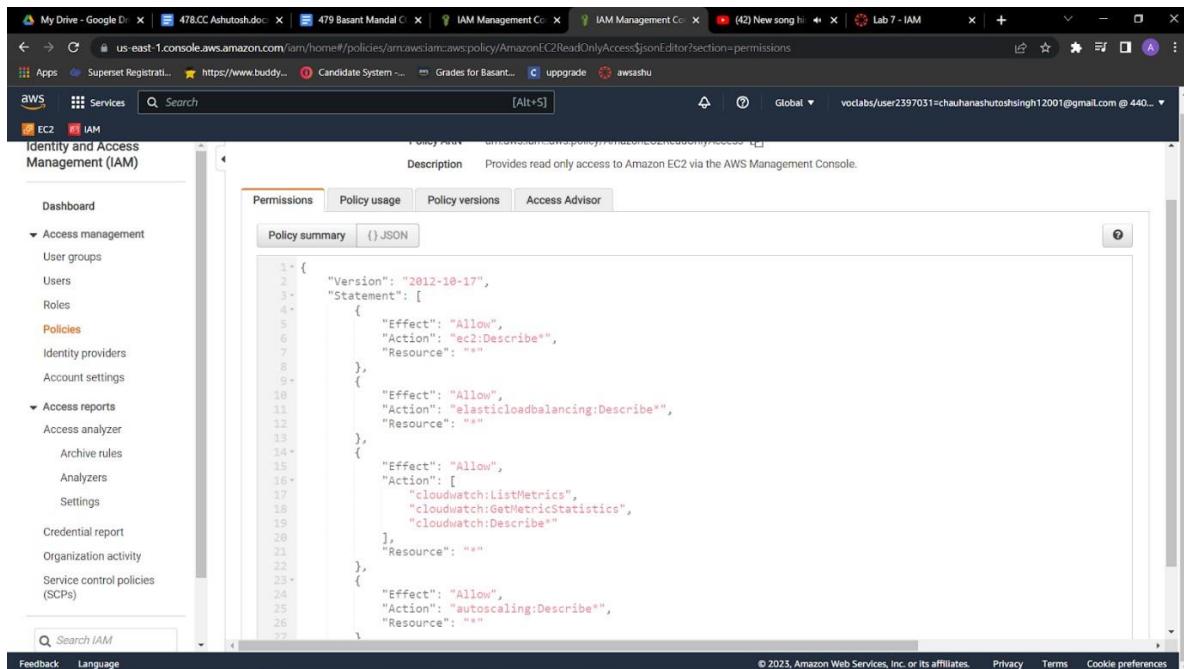
At the bottom right of the main content area, there are links for 'Feedback', 'Language', 'Privacy', 'Terms', and 'Cookie preferences'.

7.Choose the {} JSON tab.

A policy defines what actions are allowed or denied for specific AWS resources. This policy is granting permission to *List* and *Describe* (view) information about Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, Amazon CloudWatch, and Amazon EC2 Auto Scaling. This ability to view resources, but not modify them, is ideal for assigning to a support role.

[Type here]

- o Statements in an IAM policy have the following basic structure:
 - o **Effect** says whether to *Allow* or *Deny* the permissions.
 - o **Action** specifies the API calls that can be made against an AWS service (for example, *cloudwatch>ListMetrics*).
 - o **Resource** defines the scope of entities covered by the policy rule (for example, a specific Amazon Simple Storage Service [Amazon S3] bucket or Amazon EC2 instance; an asterisk [*] means *any resource*).



The screenshot shows the AWS IAM Management Console with the 'Policies' tab selected. On the left, the navigation pane shows 'Identity and Access Management (IAM)' with 'Policies' highlighted. The main area displays the 'AmazonS3ReadOnlyAccess' policy. The 'Permissions' tab is active, showing the JSON code for the policy:

```
1+ {
2+     "Version": "2012-10-17",
3+     "Statement": [
4+         {
5+             "Effect": "Allow",
6+             "Action": "ec2:Describe*",
7+             "Resource": "*"
8+         },
9+         {
10+            "Effect": "Allow",
11+            "Action": "elasticloadbalancing:Describe*",
12+            "Resource": "*"
13+        },
14+        {
15+            "Effect": "Allow",
16+            "Action": [
17+                "cloudwatch:ListMetrics",
18+                "cloudwatch:GetMetricStatistics",
19+                "cloudwatch:Describe*"
20+            ],
21+            "Resource": "*"
22+        },
23+        {
24+            "Effect": "Allow",
25+            "Action": "autoscaling:Describe*",
26+            "Resource": "*"
27+        }
    ],
```

8. In the navigation pane on the left, choose **User groups**. Choose the name of the **S3-Support** group. Choose the **Permissions** tab.

The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached. Under **Policy Name**, choose the link for the **AmazonS3ReadOnlyAccess** policy. Choose the **{ } JSON** tab.

This policy has permissions to *Get* and *List* for *all* resources in Amazon S3.

[Type here]

The screenshot shows the AWS IAM Management Console. In the left navigation pane, under 'Policies', the 'AmazonS3ReadOnlyAccess' policy is selected. The main content area displays the policy's summary, including its ARN (arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess), a brief description ('Provides read only access to all buckets via the AWS Management Console.'), and the JSON code for the inline policy:

```
1 * {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get",
        "s3>List",
        "s3-object-lambda:Get",
        "s3-object-lambda>List"
      ],
      "Resource": "*"
    }
  ]
}
```

9. In the navigation pane on the left, choose **User groups**. Choose the name of the **EC2-Admin** group.

The screenshot shows the AWS IAM Management Console. In the left navigation pane, 'User groups' is selected under 'Access management'. The main content area shows the 'User groups' table with three entries:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	48 minutes ago
EC2-Support	1	Defined	48 minutes ago
S3-Support	0	Defined	48 minutes ago

10. Choose the **Permissions** tab.

This group is different from the other two. Instead of a managed policy, the group has an *inline policy*, which is a policy assigned to just one user or group.

[Type here]

Inline policies are typically used to apply permissions for specific situations.

The screenshot shows the AWS IAM Management Console. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'User groups' is selected, showing the 'EC2-Admin' group. The main panel displays the 'Summary' of the 'EC2-Admin' group. It includes fields for 'User group name' (EC2-Admin), 'Creation time' (February 09, 2023, 21:46 (UTC+05:30)), and 'ARN' (arn:aws:iam::440579287053:group/spl66/EC2-Admin). Below this, the 'Permissions' tab is active, showing a table with one policy entry: 'EC2-Admin-Policy' (Customer inline). There are buttons for 'Edit', 'Delete', 'Simulate', 'Remove', and 'Add permissions'.

11.Under Policy Name, choose the name of the **EC2-Admin-Policy** policy. Choose the **JSON** tab.

This policy grants permission to *Describe* information about Amazon EC2 instances, and also the ability to *Start* and *Stop* instances.

The screenshot shows the 'inlineEdit' screen for the 'EC2-Admin-Policy'. The 'JSON' tab is selected. The policy code is displayed in a code editor:

```
1+ {
2  "Version": "2012-10-17",
3  "Statement": [
4    {
5      "Action": [
6        "ec2:Describe",
7        "ec2:StartInstances",
8        "ec2:StopInstances"
9      ],
10     "Resource": [
11       "*"
12     ],
13     "Effect": "Allow"
14   }
15 }
16 }
```

Below the code editor, a message box says 'You need permissions' with a red exclamation mark icon. It states: 'You do not have the permission required to perform this operation. Ask your administrator to add permissions.' A list follows: 'User: arn:aws:sts::440579287053:assumed-role/voclabs/user2397031=chauhanashutoshsingh12001@gmail.com is not authorized to perform: access-analyzer:ValidatePolicy on resource: arn:aws:access-analyzer:us-east-1:440579287053:*'.

[Type here]

Review policy

Review this policy before you save your changes.

Service	Access level	Resource	Request condition
Allow (1 of 365 services) Show remaining 364	Limited: List, Write	All resources	None

Tags

Key	Value
No tags associated with the resource.	

* Required

Cancel Previous Save changes

12. At the bottom of the screen, choose **Cancel** to close the policy.

Add user-1 to the S3-Support group

13. In the left navigation pane, choose User groups. Choose the name of the S3-Support group. On the Users tab, choose Add users. Select user-1, and choose Add users. On the Users tab, notice that *user-1* has been added to the group.

Identity and Access Management (IAM)

EC2-Support

Summary

User group name	Creation time	ARN
EC2-Support	February 10, 2023, 21:02 (UTC+05:30)	arn:aws:iam::512365191267:group/spl66/EC2-Support

Users Permissions Access Advisor

Users in this group (Selected 1/1)

User name	Groups	Last activity	Creation time
user-1	1	None	10 minutes ago

Search

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

Add user-2 to the EC2-Support group

You have hired *user-2* into a role where they will provide support for Amazon EC2. You will add them to the *EC2-Support* group so that they inherit the necessary permissions via the attached *AmazonEC2ReadOnlyAccess* policy.

[Type here]

14. Use what you learned from the previous steps to add *user-2* to the *EC2-Support* group.*user-2* should now be part of the *EC2-Support* group.

The screenshot shows the 'Users in this group' section of the IAM Management Console. It displays a table with two rows, each representing a user. The columns are: User name, Groups, Last activity, and Creation time. The users listed are 'user-1' and 'user-2'. Both users have 1 group assigned, last activity is 'None', and creation time is '15 minutes ago'.

User name	Groups	Last activity	Creation time
user-1	1	None	15 minutes ago
user-2	1	None	15 minutes ago

Add user-3 to the EC2-Admin group

You have hired *user-3* as your Amazon EC2 administrator to manage your EC2 instances. You will add them to the *EC2-Admin* group so that they inherit the necessary permissions via the attached *EC2-Admin-Policy*.

15. Use what you learned from the previous steps to add *user-3* to the *EC2-Admin* group.*user-3* should now be part of the *EC2-Admin* group. In the navigation pane on the left, choose **User groups**. Each group should have a 1 in the **Users** column. This indicates the number of users in each group. If you do not have a 1 for the **Users** column for a group, revisit the previous steps to ensure that each user is assigned to a group, as shown in the table in the **Business scenario** section.

The screenshot shows the 'Users in this group' section of the IAM Management Console for the 'EC2-Admin' group. It displays a table with one row, representing the user 'user-3'. The columns are: User name, Groups, Last activity, and Creation time. The user 'user-3' has 1 group assigned, last activity is 'None', and creation time is '21 minutes ago'.

User name	Groups	Last activity	Creation time
user-3	1	None	21 minutes ago

Sign in and test users

Get the console sign-in URL

16. In the navigation pane on the left, choose Dashboard. Notice the Sign-in URL for IAM users in this account section at the top of the page. The sign-in URL looks similar to the following: <https://123456789012.sigin.aws.amazon.com/console>

[Type here]

This link can be used to sign in to the AWS account that you are currently using. Copy the sign-in link to a text editor.

The screenshot shows the AWS IAM Management Console dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Dashboard', 'Access management', 'Access reports', and 'What's new'. The main area has sections for 'Security recommendations' (with alerts for 'Add MFA for root user' and 'Update your access permissions for AWS Billing, Cost Management, and Account consoles'), 'IAM resources' (showing 3 User groups, 4 Users, 13 Roles, 1 Policies, and 0 Identity providers), and 'Tools' (including 'Policy simulator' and 'Web identity federation playground'). A right sidebar displays 'AWS Account' details: Account ID (512365191267), Account Alias (512365191267 Create), and a 'Sign in URL' (https://512365191267.signin.aws.amazon.com/console). The bottom of the page includes a footer with copyright information and links to 'Feedback', 'Language', 'Privacy', 'Terms', and 'Cookie preferences'.

Test user-1 permissions

17. Open a private or incognito window in your browser. Paste the sign-in link into the private browser, and press ENTER. You will now sign-in as *user-1*, who has been hired as your Amazon S3 storage support staff. Sign in with the following credentials: **IAM user name:** user-1, **Password:** Lab-Password1

The screenshot shows the AWS sign-in page for user-1. It features the AWS logo at the top. The form fields are: 'Account ID (12 digits) or account alias' (512365191267), 'IAM user name' (user-1), and 'Password' (Lab-Password1). There's also a checkbox for 'Remember this account'. Below the form is a 'Sign in' button. To the right, there's a promotional section with the heading 'Scale and innovate globally' and a subtext 'Experience increased application performance, lower costs, and speed of innovation with AWS.' It includes a 'Learn how' button and a graphic of a globe with network connections. At the bottom, there are links for 'Sign in using root user email' and 'Forgot password?'. The footer includes language selection ('English') and links to 'Terms of Use' and 'Privacy Policy'.

[Type here]

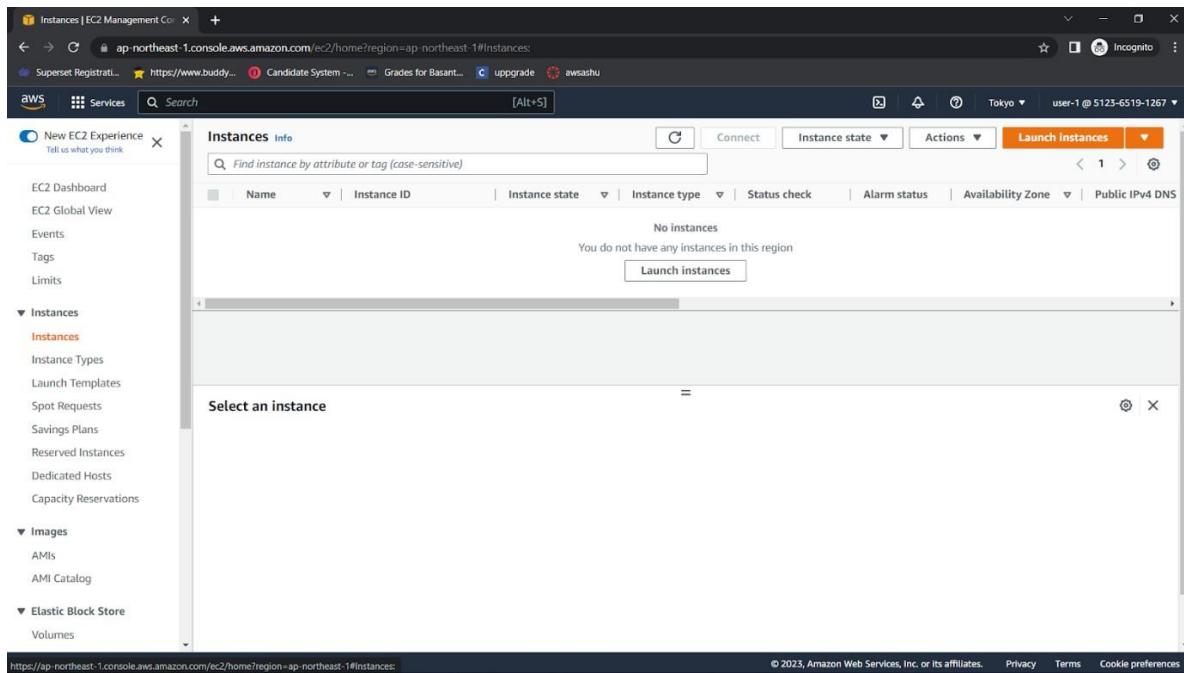
The screenshot shows the AWS Management Console Home page. At the top, there's a search bar and a navigation bar with tabs like 'Services' and 'Search'. Below the search bar, the 'Console Home' section has a 'Recently visited' panel showing a single service icon (S3) with the message 'No recently visited services'. It also features a 'Welcome to AWS' panel with three cards: 'Getting started with AWS' (Learn the fundamentals), 'Training and certification' (Learn from AWS experts), and 'What's new with AWS?' (Discover new AWS services). Below these are sections for 'AWS Health' and 'Cost and usage'.

18. Choose the **Services** menu, and choose **S3**. Choose the name of one of your buckets, and browse the contents. Because this user is part of the *S3-Support* group in IAM, they have permissions to view a list of Amazon S3 buckets and their contents. Now, test whether the user has access to Amazon EC2.

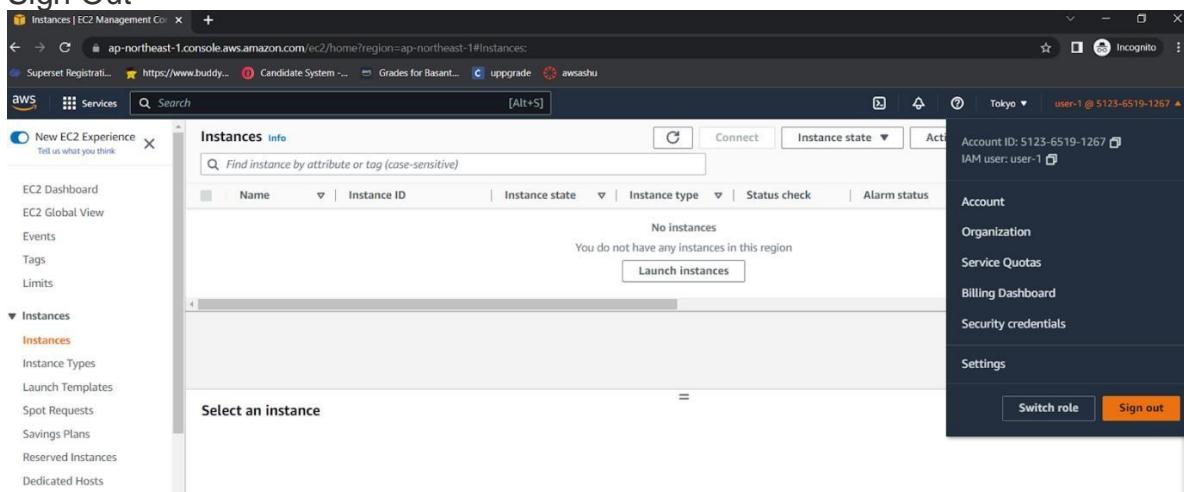
The screenshot shows the AWS S3 Management Console Buckets page. The left sidebar has a 'Buckets' section with links for Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. It also includes a 'Block Public Access settings for this account' section and a 'Storage Lens' section with 'Dashboards' and 'AWS Organizations settings'. A 'Feature spotlight' section is also present. The main content area shows an 'Account snapshot' with a 'Buckets' table. The table has columns for Name, AWS Region, Access, and Creation date. A note says 'No buckets' and there is a 'Create bucket' button.

19. Choose the **Services** menu, and choose **EC2**. In the left navigation pane, choose **Instances**. You cannot see any instances. Instead, an error message says *you are not authorized to perform this operation*. This user has not been assigned any permissions to use Amazon EC2. You will now sign in as *user-2*, who has been hired as your Amazon EC2 support person.

[Type here]



Sign Out



20. Paste the sign-in link into the private browser again, and press ENTER. Sign in with the following credentials:**IAM user name:** user-2 **Password:** Lab-Password2

Account ID (12 digits) or account alias

IAM user name

Password

Remember this account

Sign in

21. Choose the **Services** menu, and choose **EC2**. In the navigation pane on the left, choose **Instances**. You are now able to see an EC2 instance. However, you cannot

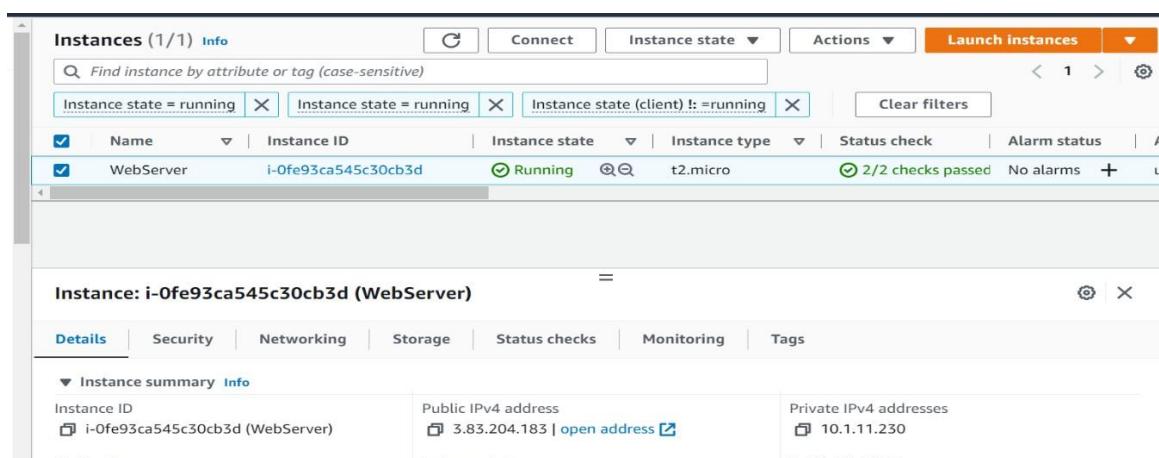
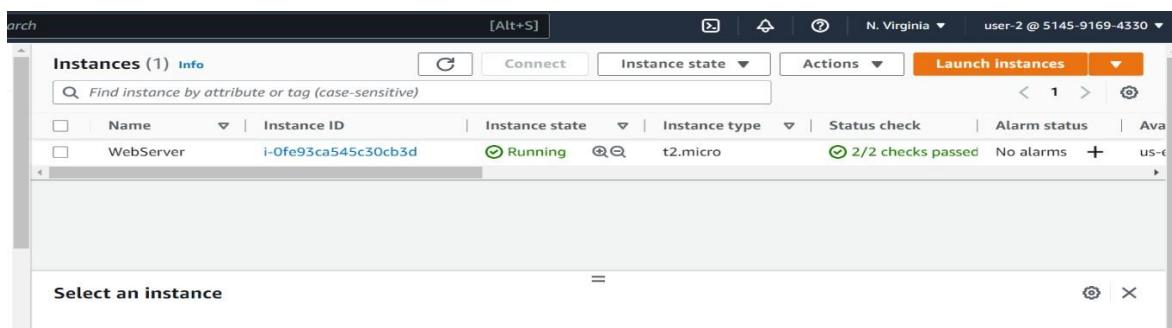
[Type here]

make any changes to Amazon EC2 resources because you have read-only permissions. If you cannot see an EC2 instance, then your Region might be incorrect. In the upper-right corner of the page, choose the Region name, and then choose the Region that you were in at the beginning of the lab (for example, **N. Virginia**).



22. Select the EC2 instance. Choose the **Instance state** menu, and then choose **Stop instance**. To confirm that you want to stop the instance, choose **Stop**.

An error message appears and says that *You are not authorized to perform this operation*. This demonstrates that the policy only allows you to view information without making changes. Next, check if user-2 can access Amazon S3.



CONCLUSION : Identity and access management (IAM) is one of the foundations of **cloud security**. As more organizations turn to mobile-friendly and cloud-based platforms, the need to provide a safe and secure place to store identifiable information becomes more important.

Practical No.7

Aim: Study and implement MFA in the environment of popular Cloud Service Provider in AWS.

THEORY :

AWS multi-factor authentication (MFA) is an AWS Identity and Access Management (IAM) best practice that requires a second authentication factor in addition to user name and password sign-in credentials. You can enable MFA at the AWS account level and for root and IAM users you have created in your account.

AWS is expanding eligibility for its free MFA security key program. Verify your eligibility and order your free MFA key.

With MFA enabled, when a user signs in to the AWS Management Console, they are prompted for their user name and password— something they know—and an authentication code from their MFA device— something they have (or if they use a biometrics-enabled authenticator, something they are). Taken together, these factors improve security for your AWS accounts and resources.

We recommend that you require your human users to use temporary credentials when accessing AWS. Your users can use an identity provider to federate into AWS, where they can authenticate with their corporate credentials and MFA configurations. To manage access to AWS and business applications, we recommend that you use AWS IAM Identity Center. For more information, see the IAM Identity Center User Guide.

See the following available MFA options that you can use with your IAM MFA implementation. You can download virtual authenticator apps through the links provided, or you can acquire a hardware MFA device from the respective manufacturer. After you've acquired a supported virtual or hardware MFA device, AWS does not charge additional fees for using MFA.

Available MFA methods for IAM

You can manage your MFA devices in the IAM console. The following options are the MFA methods that IAM supports.

FIDO security keys

FIDO-certified hardware security keys are provided by third-party providers such as Yubico. The FIDO Alliance maintains a list of all FIDO-certified products that are compatible with FIDO specifications. FIDO authentication

CLOUD COMPUTING JOURNAL

standards are based on public key cryptography, which enables strong, phishing-resistant authentication that is more secure than passwords. FIDO security keys support multiple root accounts and IAM users using a single security key. For more information about enabling FIDO security keys, see [Enabling a FIDO security key](#).

AWS offers a [free MFA security key](#) to eligible AWS account owners in the United States. To determine eligibility and order a key, see the [Security Hub console](#).

Virtual authenticator apps

Virtual authenticator apps implement the [time-based one-time password](#) (TOTP) algorithm and support multiple tokens on a single device. Virtual authenticators are supported for IAM users in the [AWS GovCloud \(US\) Regions](#) and in other AWS Regions. For more information about enabling virtual authenticators, see [Enabling a virtual multi-factor authentication \(MFA\) device](#). You can install apps for your smartphone from the app store that is specific to your type of smartphone. Some app providers also have web and desktop applications available. See the following table for examples.

Android

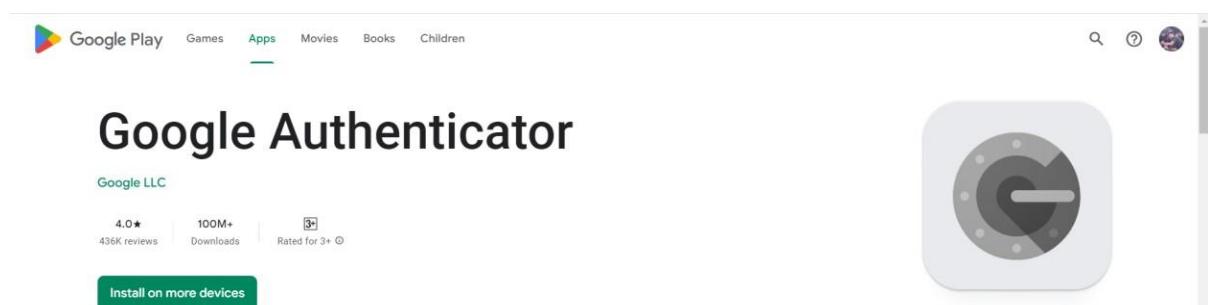
[Twilio Authy Authenticator](#), [Duo Mobile](#), [LastPass Authenticator](#), [Microsoft Authenticator](#), [Google Authenticator](#), [Symantec VIP](#)

iOS

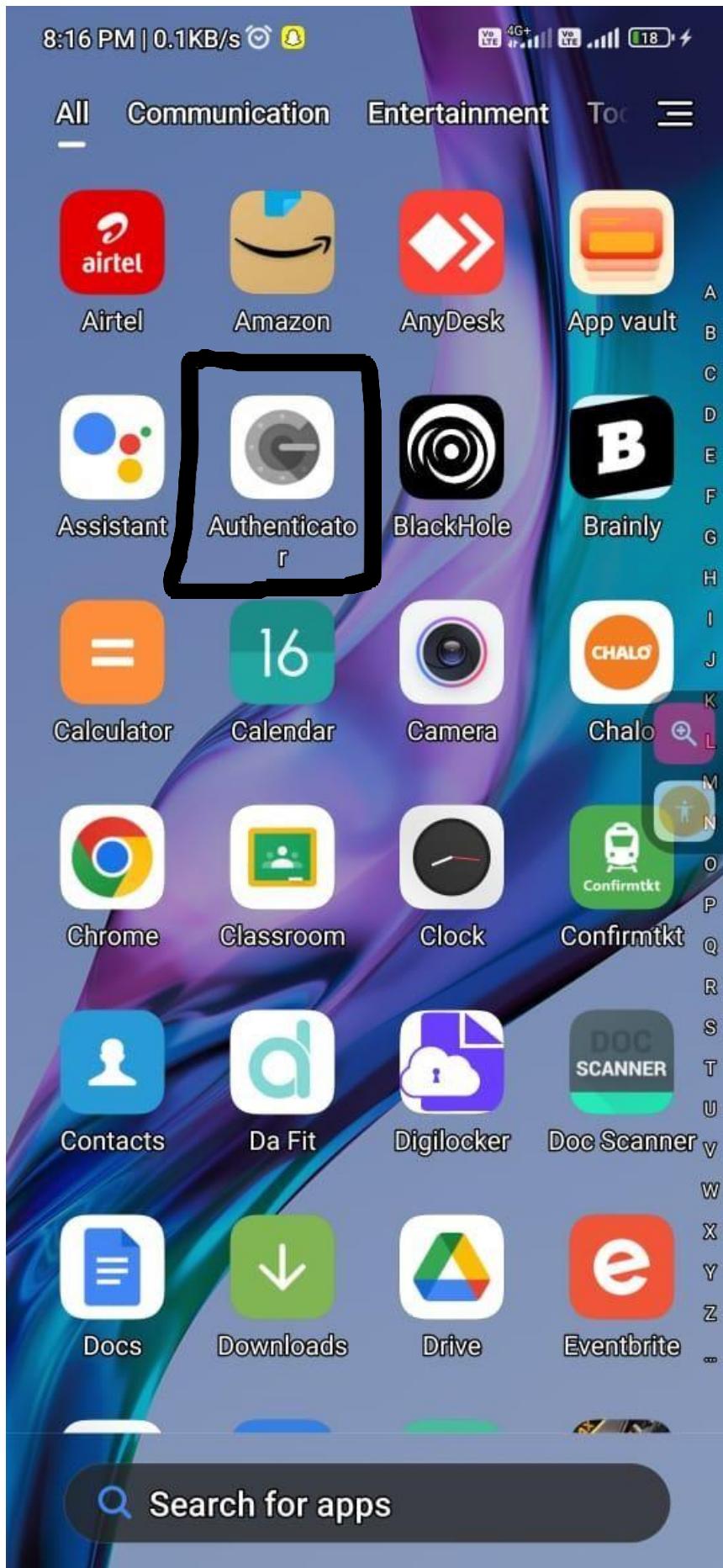
[Twilio Authy Authenticator](#), [Duo Mobile](#), [LastPass Authenticator](#), [Microsoft Authenticator](#), [Google Authenticator](#), [Symantec VIP](#)

GOOGLE APP FOR AUTHENTICATION :

<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>



[Type here]



[Type here]

IMPLEMENTATION:

The screenshot shows the AWS Identity and Access Management (IAM) console. The main content area displays "My security credentials (root user)" with a note about the new Security Credentials experience. It includes fields for "Account name" and "Email address". The top right corner shows the Account ID: 2303-8293-0038. A navigation bar on the right lists "Account", "Organization", "Service Quotas", "Billing Dashboard", "Security credentials" (which is highlighted in orange), and "Settings".

The screenshot shows the AWS Account navigation menu. The "Security credentials" option is highlighted in orange. Other options include "Account", "Organization", "Service Quotas", "Billing Dashboard", and "Settings". A "Sign out" button is located at the bottom right.

The screenshot shows the AWS IAM Multi-factor authentication (MFA) configuration page. It displays a table with one row of data: a virtual MFA device assigned to the root user. The table columns are "Device type", "Identifier", and "Created on". Buttons for "Remove", "Resync", and "Assign MFA device" are visible at the top of the table.

Device type	Identifier	Created on
Virtual	arn:aws:iam::230382930038:mfa/Mobile	17 minutes ago

[Type here]

Screenshot of the AWS IAM Management Console showing the Multi-factor authentication (MFA) section.

Multi-factor authentication (MFA) (1)
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned.
[Learn more](#)

Device type Identifier Created on
 Virtual arn:aws:iam::230382930038:mfa/pradeepmobile 2 days ago

Access keys (0)
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Create access key

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
No access keys					

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

Create access key

Select MFA device

Step 1
Select MFA device

Step 2
Set up device

Specify MFA device name

Device name
Enter a meaningful name to identify this device.

Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.

Select MFA device [Info](#)

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

 **Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.

 **Security Key**
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

 **Hardware TOTP token**

[Type here]

Enter a meaningful name to identify this device.

Ashutosh478

Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.

Select MFA device Info

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

 **Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.

USE GOOGLE AUTHENTICATOR APP FOR OTP:

aws | Services | Search [Alt+S]

code.

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2 

Open your authenticator app, chose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key.
[Show secret key](#)

3 Fill in two consecutive codes from your MFA device.

MFA code 1
610820

MFA code 2
647502

Cancel Previous Add MFA

[Type here]

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there's a sidebar with 'Identity and Access Management (IAM)' at the top, followed by a search bar labeled 'Search IAM' and a 'Dashboard' link. Below that is a section titled 'Access management' with links for 'User groups', 'Users', 'Roles', and 'Policies'. The main content area has a blue header bar with the text 'Introducing the new Security Credentials experience' and a message about redesigning the experience. Below this, a green bar contains the message 'MFA device assigned' with a note about registering up to 8 MFA devices. The main content area shows the 'Security credentials' page for the 'root user'. It displays the text 'My security credentials (root user)' and a note that the root user has access to all AWS resources. There's also a link to 'AWS Security Credentials In AWS General Reference'.

CONCLUSION : Successfully Implemented AWS multi-factor authentication (MFA).

Practical No.8

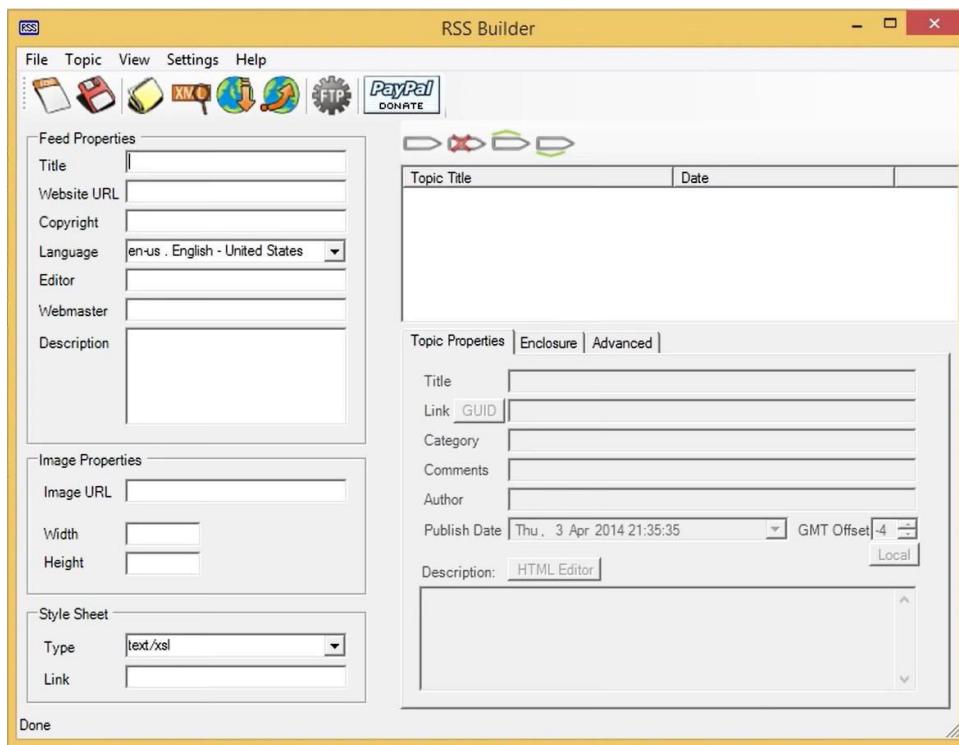
AIM: Write a program for web feed.

THEORY: RSS builder allows you to create a feed from specific sections of the webpage. You can generate a feed using RSS builder in two modes: **Quick mode** and **Advanced mode**.

An RSS feed is a feed that delivers **auto-updated** content to users without having to manually go to a specific website. It is formatted into an XML file that can be read in an RSS reader or embedded into your website.

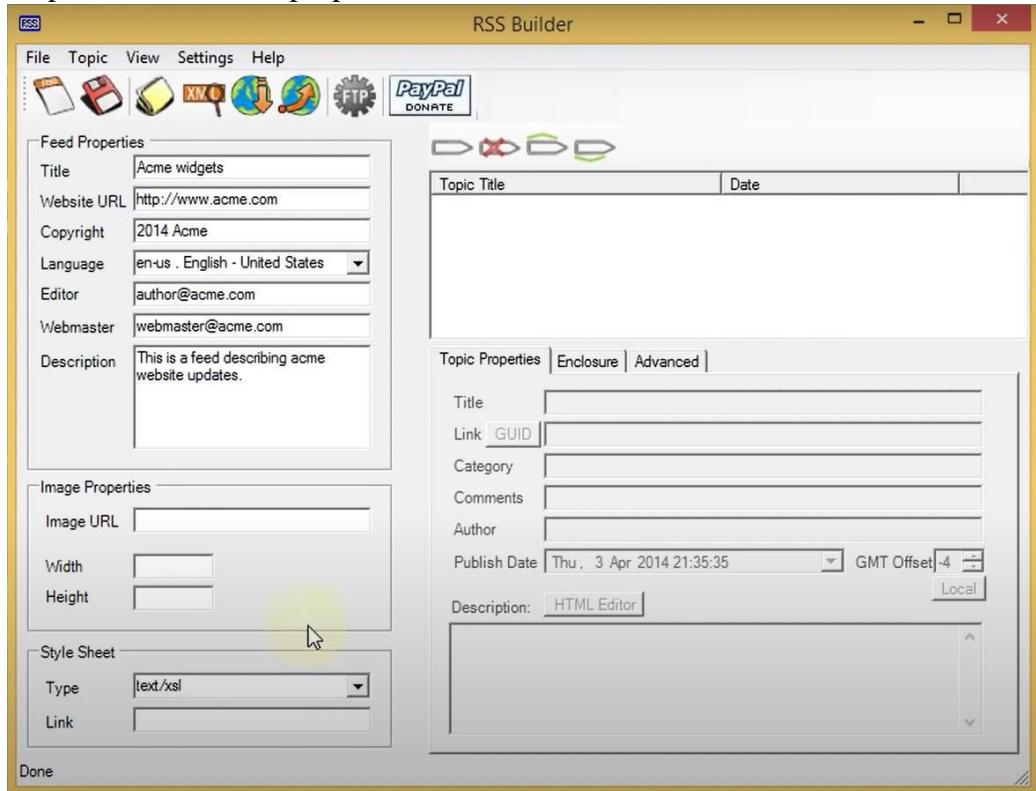
IMPLEMENTATION:

Step 01: Open RSS builder



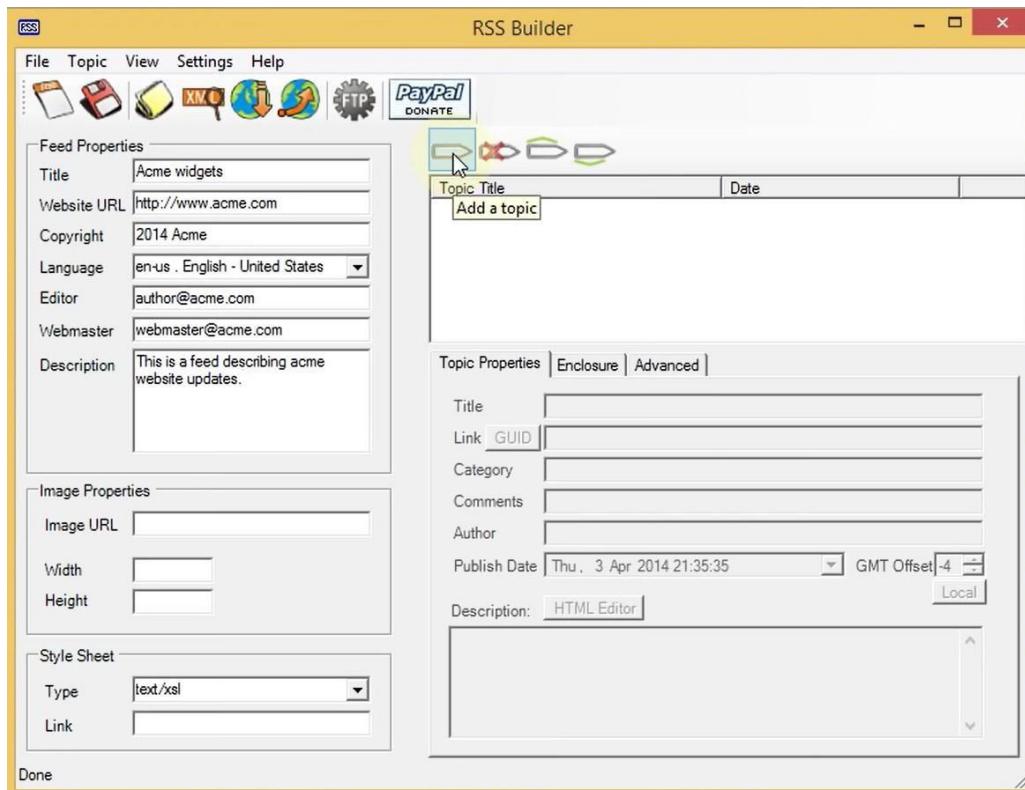
[Type here]

Step 02: Fill the Feed properties

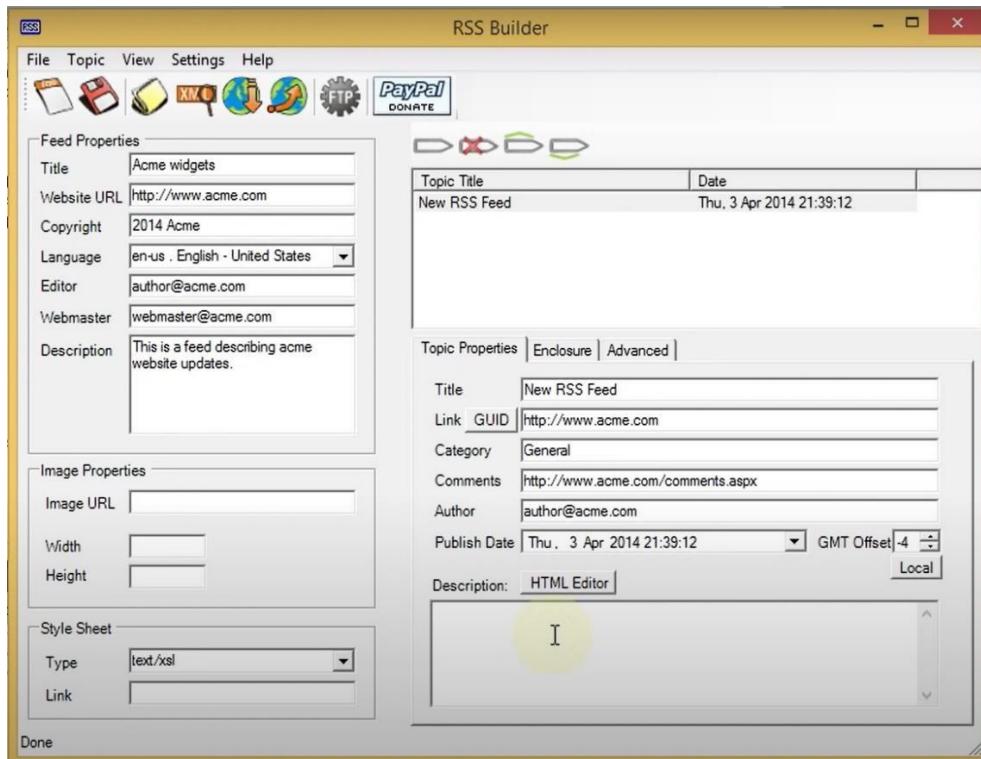


Step 03: Click on Add a Topic to add new topic to your feed

[Type here]

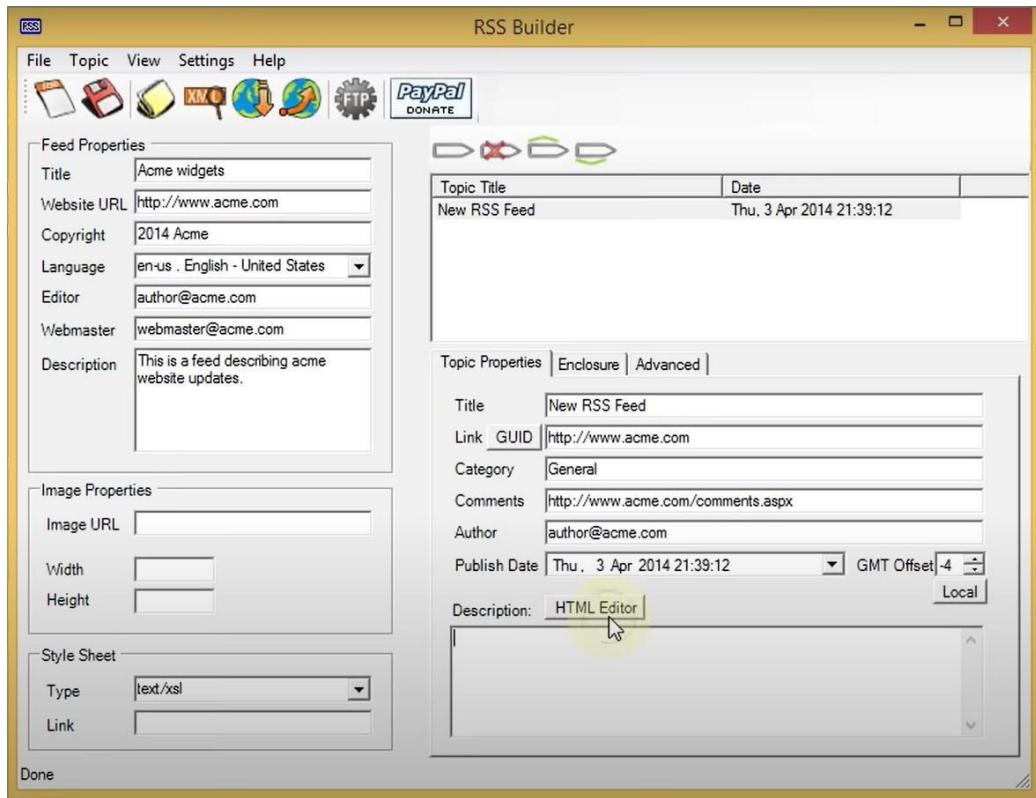


Step 04: Fill the topic properties



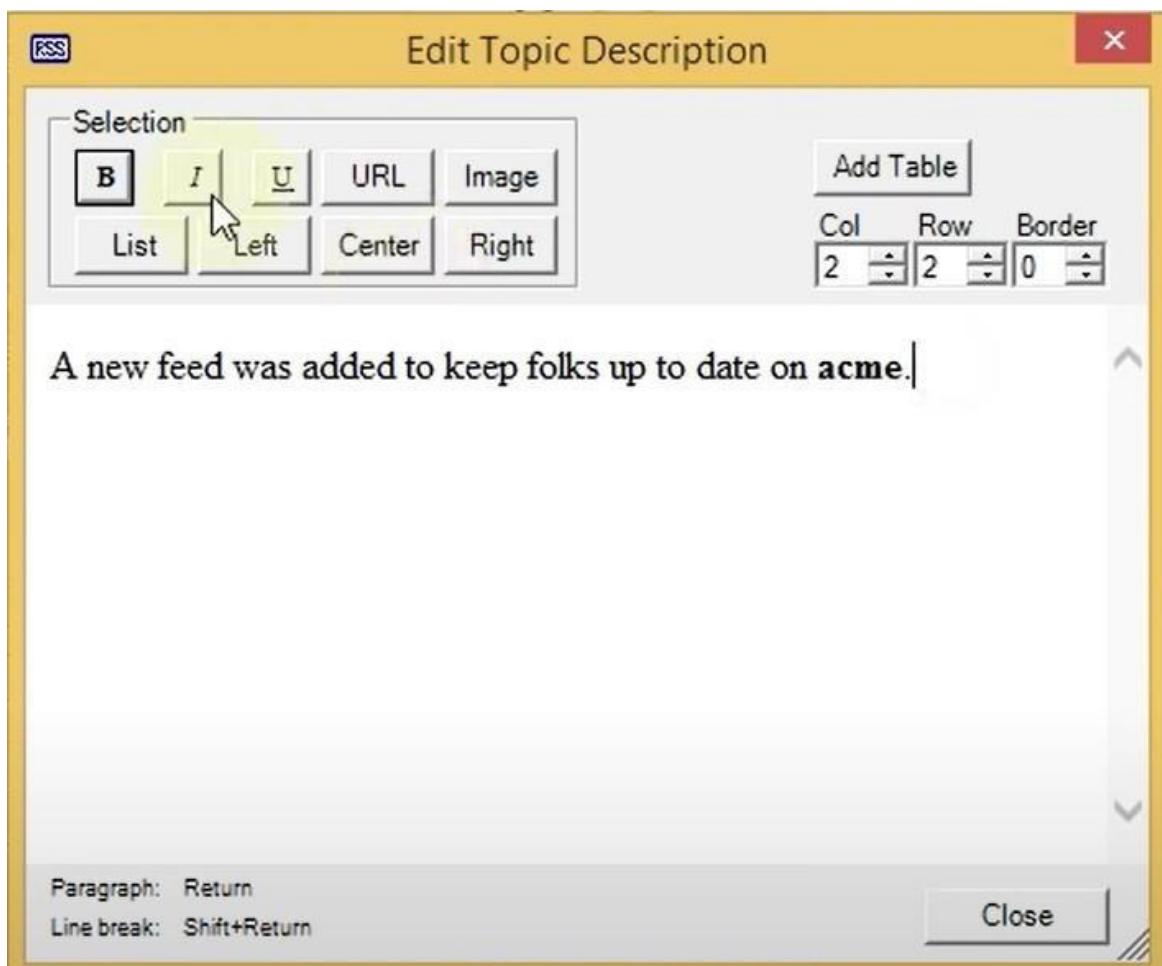
[Type here]

Step 05: To add description on web feed click on HTML editor



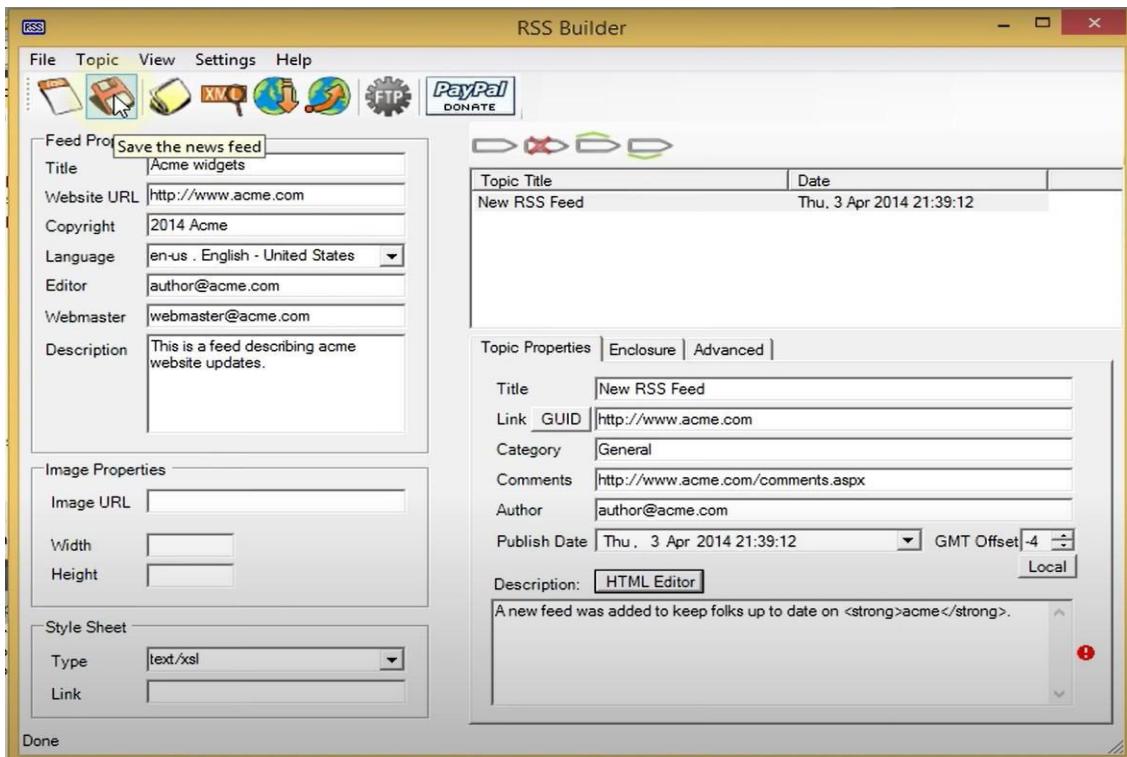
Step 06: Add topic description to show in feed

[Type here]

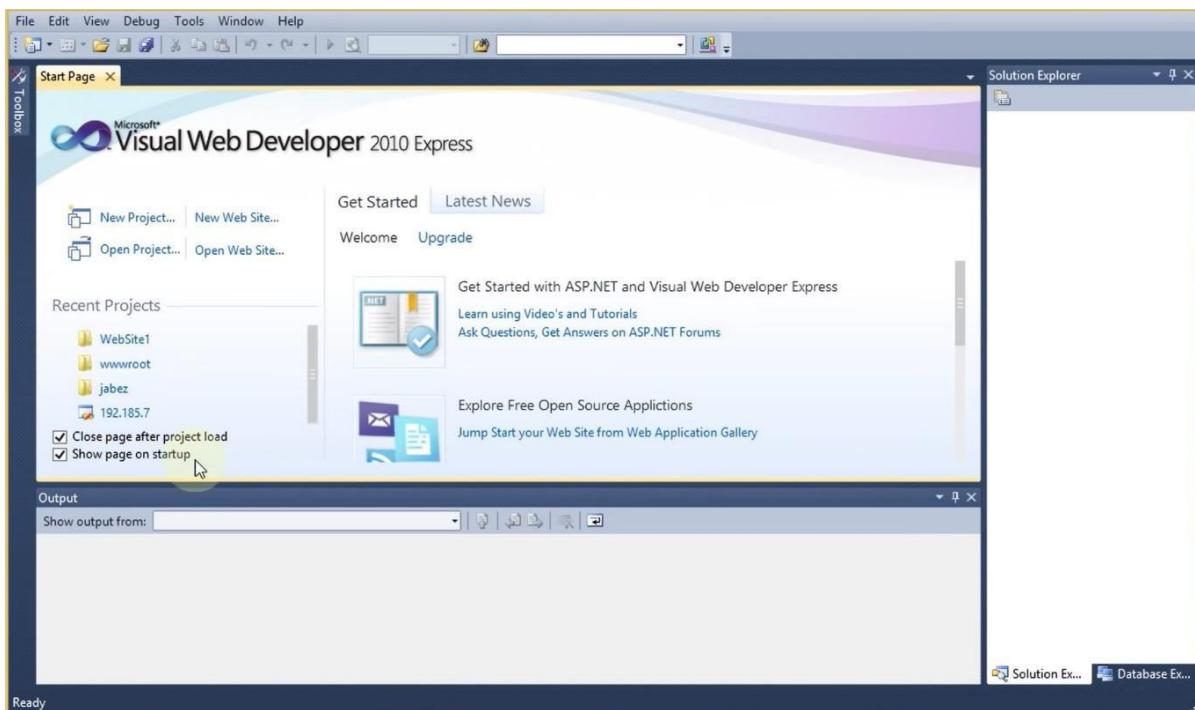


Step 07: Save the feed in xml format(defaultly saved in .xml)

[Type here]

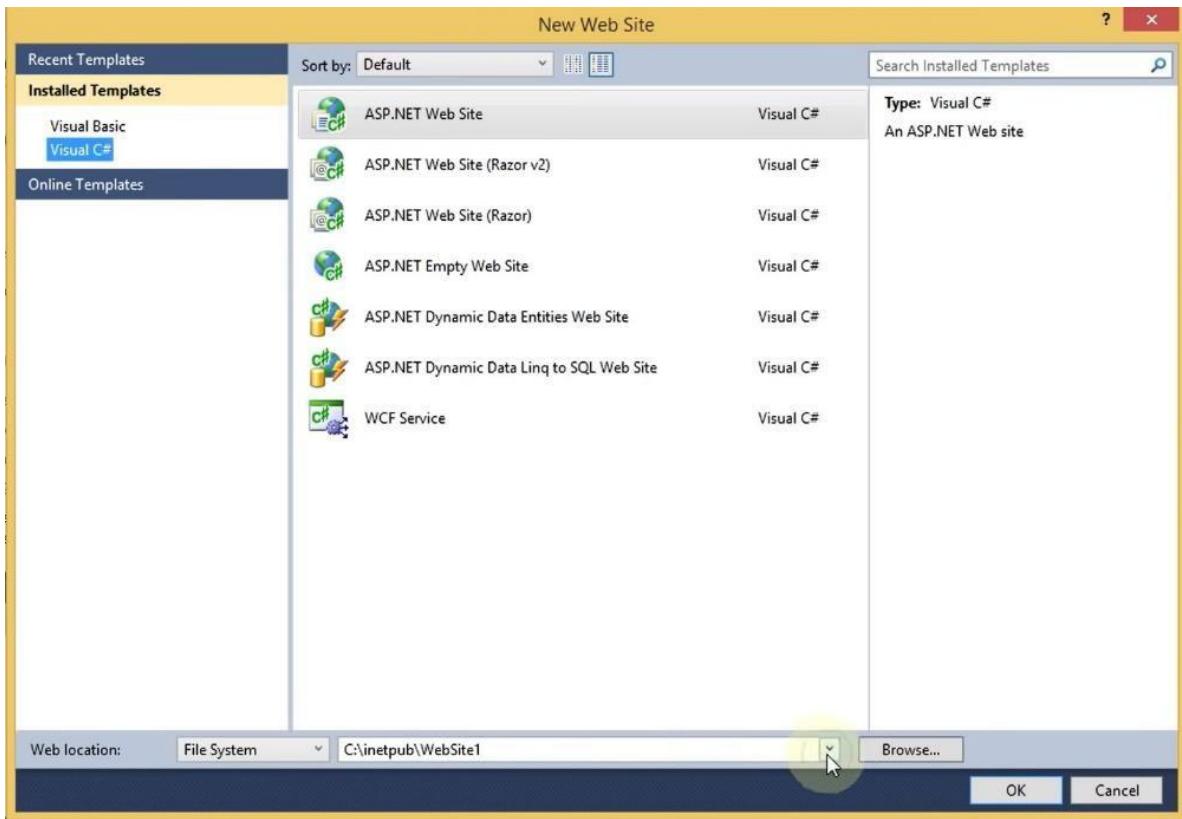


Step 08: launch Visual Studio 2010 to launch the sample website

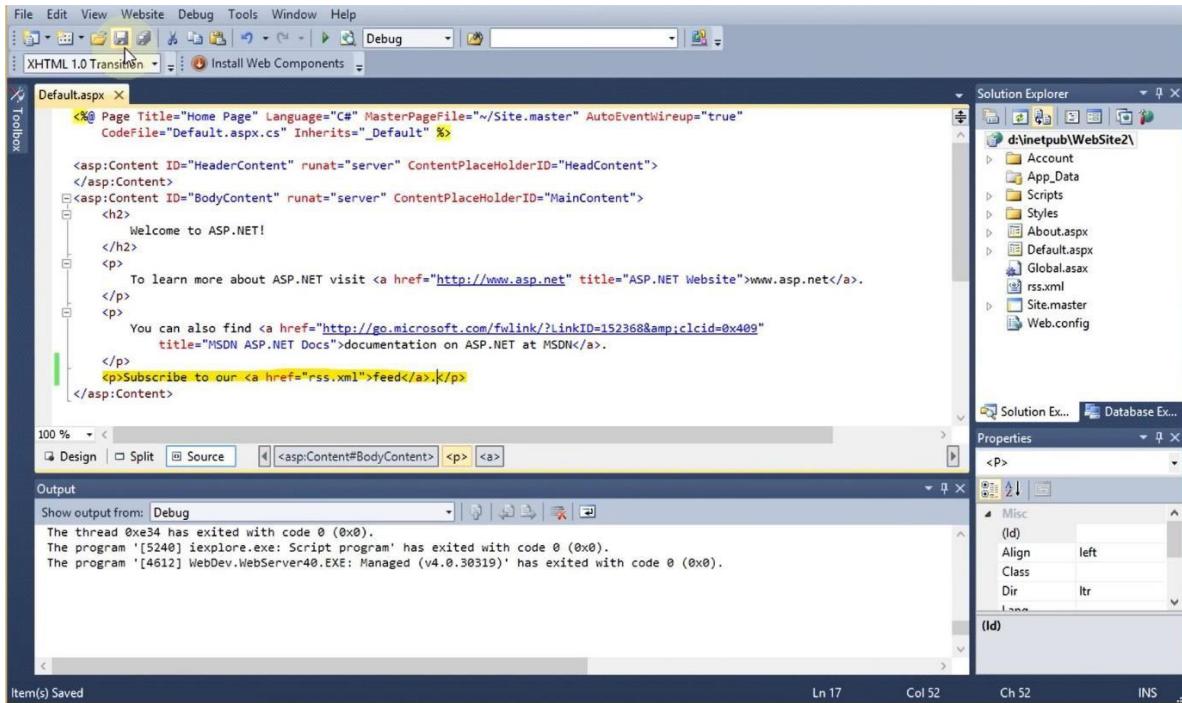


Step 09: Create new website on asp.net web site

[Type here]

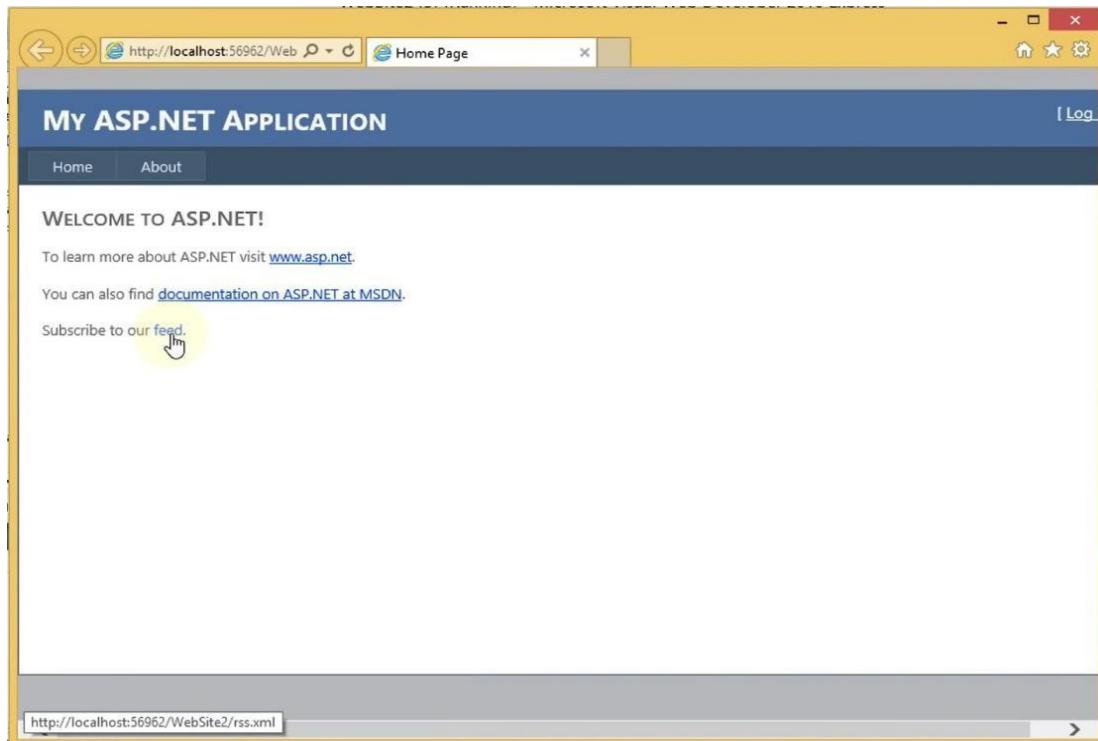


Step 10: Add new paragraph in default.aspx file and provide a link to server to access your website



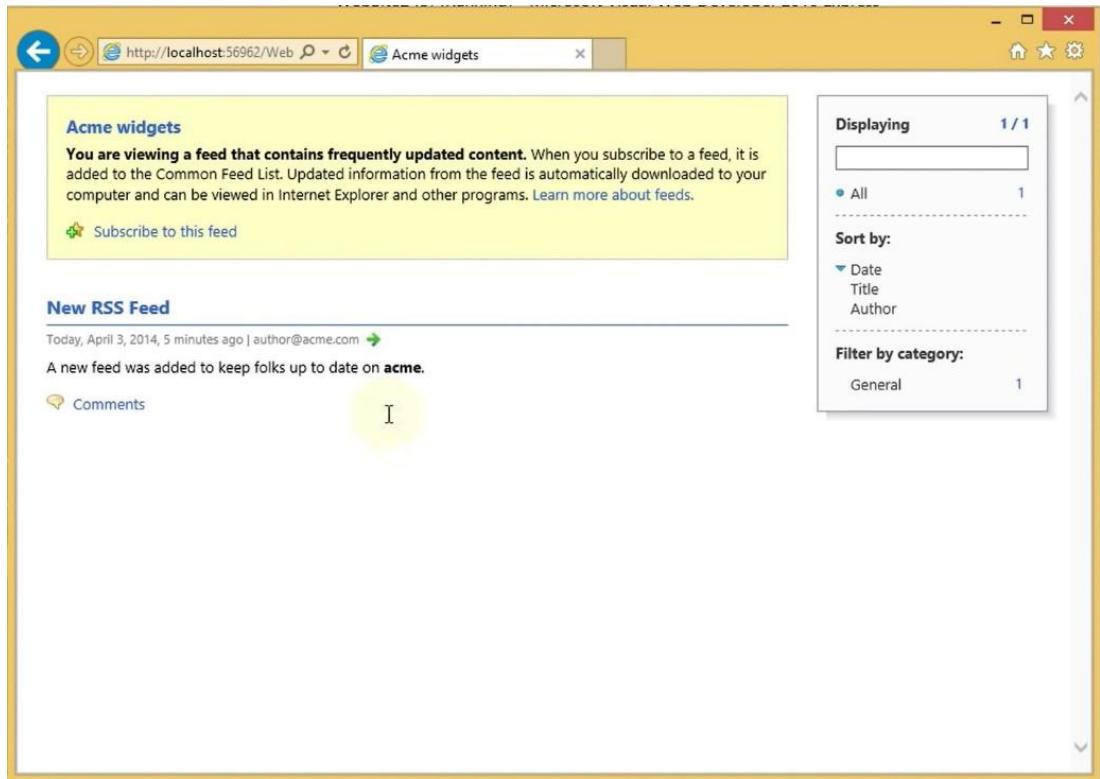
[Type here]

Step 11: Run the program the page will appear as shown in the figure where the given link is provided click on it.



Step 12: New RSS feed will be created after clicking on the link to see the final output.

[Type here]



CONCLUSION :Successfully Performed, Your feed is now ready to be embedded and shared.

PRACTICAL NO : 09

Aim: Study and implementation of Single-Sign-On (SSO).

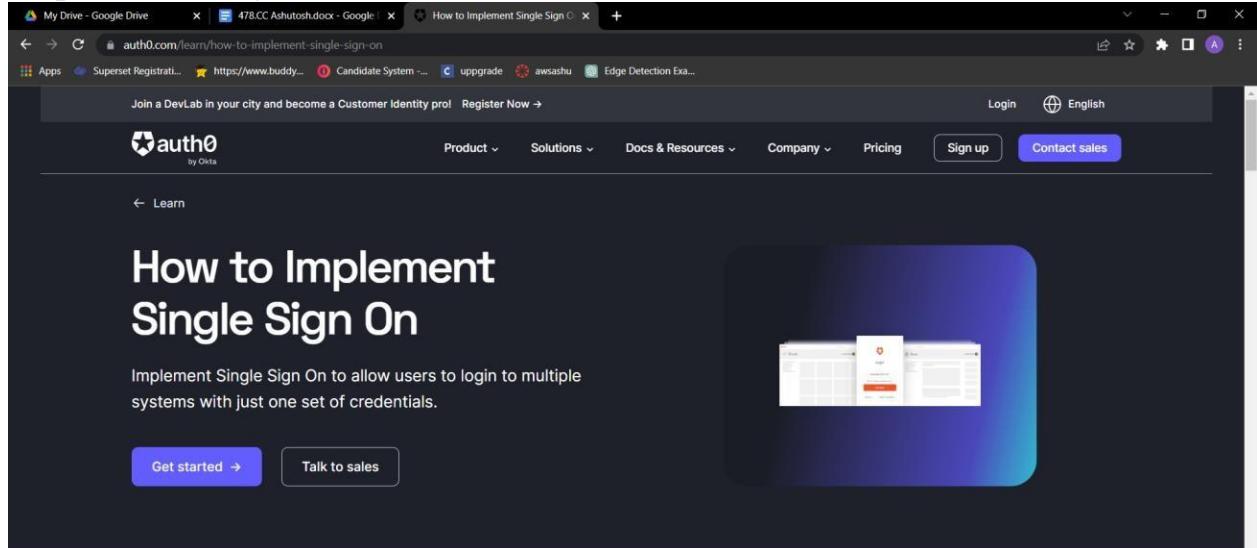
THEORY :

- Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications
- The service authenticates the end user for all the applications the user has been given rights to and eliminates further prompts when the user switches applications during the same session. On the back end, SSO is helpful for logging user activities as well as monitoring user accounts.
- In a basic web SSO service, an agent module on the application server retrieves the specific authentication credentials for an individual user from a dedicated SSO policy server, while authenticating the user against a user repository such as a lightweight directory access protocol (LDAP) directory.

[Type here]

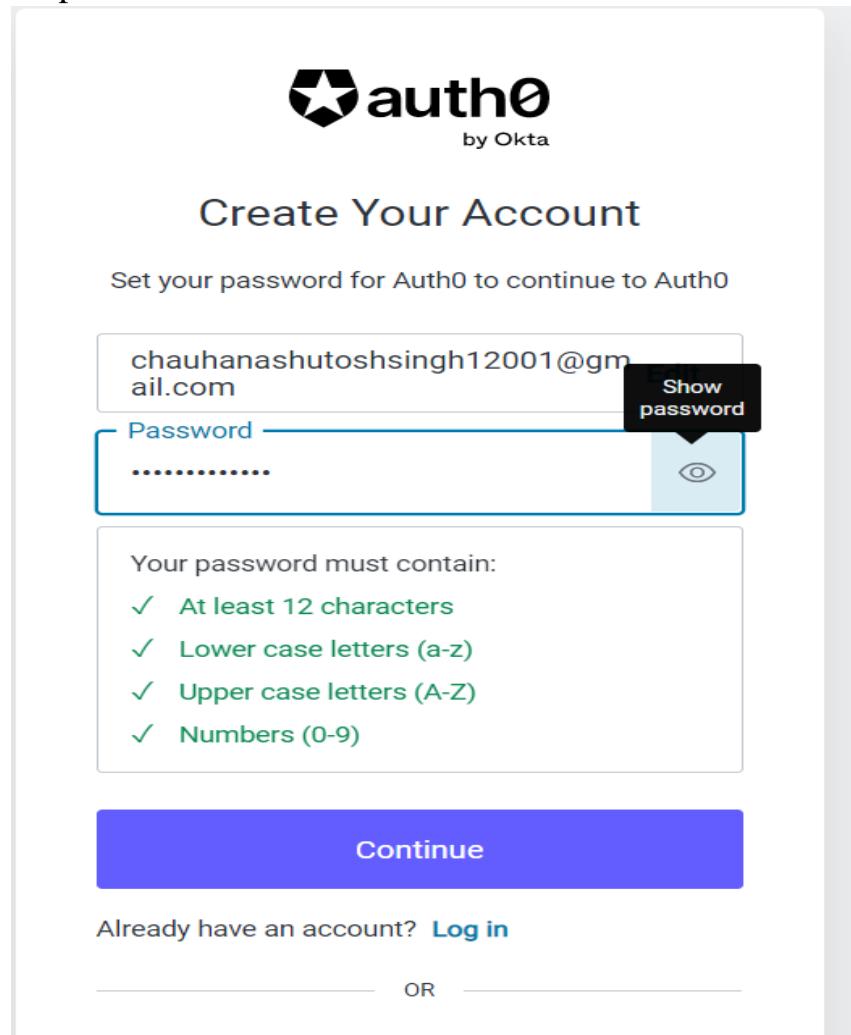
Procedure:- Step1:got to the following link <https://auth0.com/learn/how-to-implement> single-sign-on/

Step2:click on try autho for free → fill the details

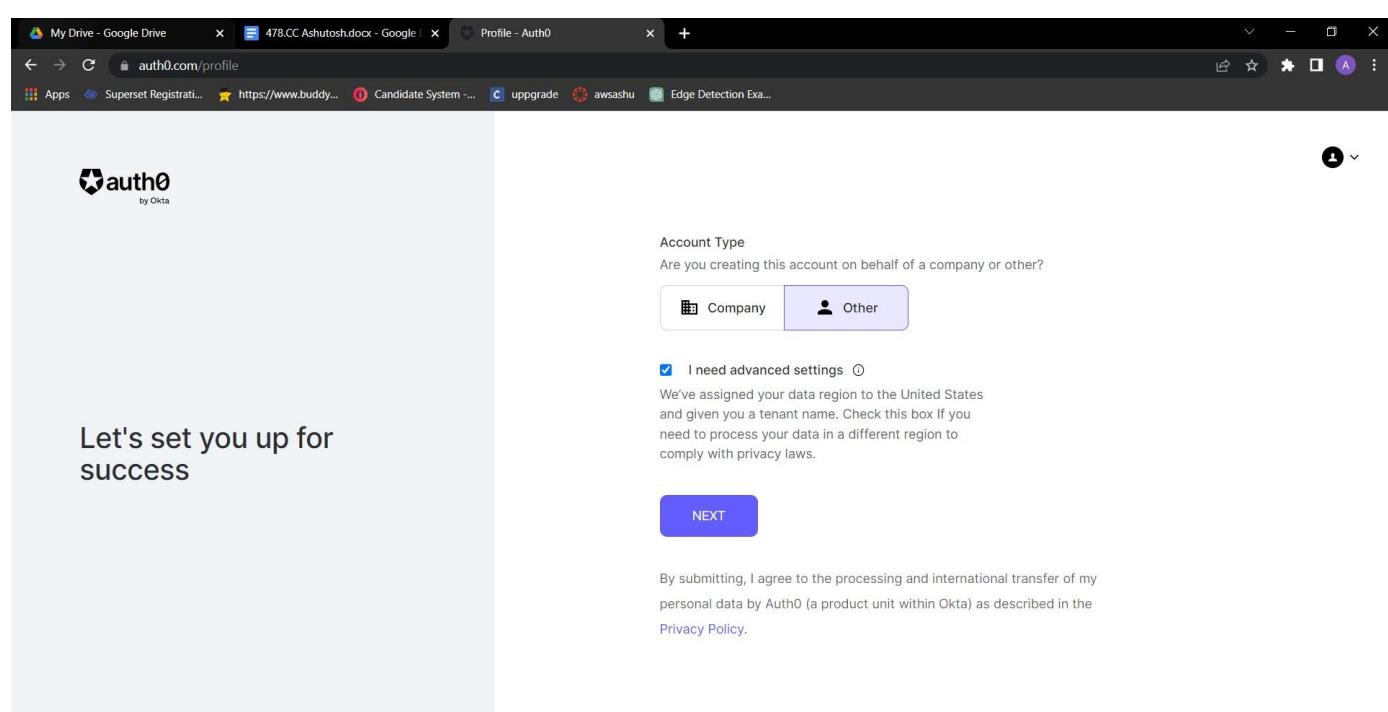


[Type here]

Step3: Provide the username and Password and click on Signup



The screenshot shows the 'Create Your Account' page for Auth0. At the top, the Auth0 logo is displayed with the text 'by Okta'. Below it, the heading 'Create Your Account' is centered. A sub-instruction 'Set your password for Auth0 to continue to Auth0' is present. The main input fields are 'Email' (containing 'chauhanashutoshsingh12001@gmail.com') and 'Password' (containing '.....'). To the right of the password field is a 'Show password' button and an eye icon. Below these fields, a box lists password requirements: 'At least 12 characters', 'Lower case letters (a-z)', 'Upper case letters (A-Z)', and 'Numbers (0-9)'. A large blue 'Continue' button is at the bottom of the form. Below the form, a link 'Already have an account? [Log in](#)' is visible.

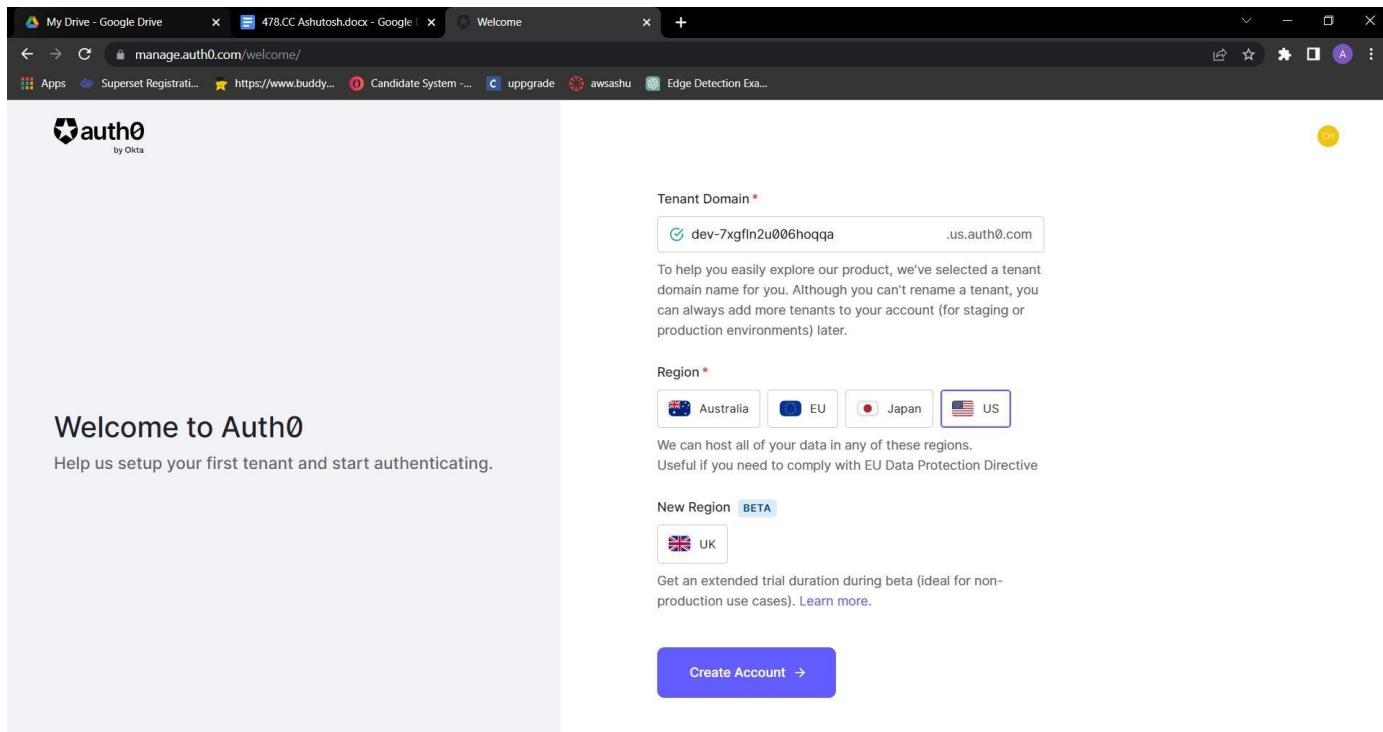


The screenshot shows the 'Account Type' selection screen for Auth0. The header 'auth0.com/profile' is visible. On the left, a message 'Let's set you up for success' is displayed. On the right, there is a question 'Are you creating this account on behalf of a company or other?' with two options: 'Company' and 'Other', where 'Other' is selected. Below this, a checkbox 'I need advanced settings' is checked. A note explains that data is assigned to the United States and provides a link to change region if needed. At the bottom, a 'NEXT' button is available, and a privacy policy link is at the very bottom.

[Type here]

Step 4: Provide the tenant name and click on next

Step5: Fill all the Details and click on create account



Step6: In this step you will get Dashboard . First create one user

[Type here]

The screenshot shows the Auth0 dashboard interface. At the top, there are tabs for 'My Drive' and '478.CC Ashutosh.docx - Google'. Below the tabs, the URL is manage.auth0.com/dashboard. The main navigation menu on the left includes 'Getting Started', 'Activity' (which is highlighted in blue), 'Applications', 'Authentication', 'Organizations', 'User Management' (which has a dropdown menu for 'Users' and 'Roles'), and other sections like 'Branding', 'Security', 'Actions', etc. The central area displays a message: 'Thank you for signing up for Auth0! You have 22 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here.' A 'View Plans' button is visible. Below this message, there's a section titled 'Users' with a sub-section 'You don't have any users yet.' and a 'Create User' button.

This screenshot is identical to the one above, showing the Auth0 dashboard with the 'User Management' section selected. The central area displays the same message about the trial period and the 'Users' section with the message 'You don't have any users yet.' and the 'Create User' button.

Step 7: click on create user

Create user



Email *

ashusingh478@gmail.com

Password *

Repeat Password *

Connection *

Username-Password-Authentication

Cancel

Create

Step 8: fill all the details and click on save

The screenshot shows the Auth0 dashboard under the 'User Details' section. A new user account has been created for the email address ashusingh478@gmail.com. The user's name is listed as 'ashusingh478@gmail.com'. The 'Details' tab is selected, displaying the following information:

Name	Email	Signed Up
ashusingh478@gmail.com	ashusingh478@gmail.com (pending)	February 28th 2023, 9:37:12 PM

Other tabs visible include 'Devices', 'History', 'Raw JSON', 'Authorized Applications', 'Permissions', and 'Roles'. The left sidebar shows navigation links such as 'Getting Started', 'Activity', 'Applications', 'Authentication', 'Organizations', 'User Management', 'Users', 'Roles', 'Branding', 'Security', 'Actions', 'Auth Pipeline', 'Monitoring', 'Marketplace', 'Extensions', 'Settings', and 'Get support'.

Create user

X

Email *

chauhanashutoshsingh12001@gmail.com

Password *

Repeat Password *

*****|

Connection *

Username-Password-Authentication

Cancel

Create

RESULTS :

 chauhanashutoshsingh12001@gmail.com Actions ▾

user_id: auth0|63fe279b2cef38f4fa3da33c

Details	Devices	History	Raw JSON	Authorized Applications	Permissions	Roles

COPY JSON

```

1  {
2      "created_at": "2023-02-28T16:11:07.930Z",
3      "email": "chauhanashutoshsingh12001@gmail.com",
4      "email_verified": false,
5      "identities": [
6          {
7              "connection": "Username-Password-Authentication",
8              "user_id": "63fe279b2cef38f4fa3da33c",
9              "provider": "auth0",
10             "isSocial": false
11         }
12     ],
13     "name": "chauhanashutoshsingh12001@gmail.com",
14     "nickname": "chauhanashutoshsingh12001",
15     "picture": "https://s.gravatar.com/avatar/88c660c32998ea8b732b6ccf86b7d239?s=480&r=pg&d=https%3A%2F%2Fcdn.%s",
16     "updated_at": "2023-02-28T16:11:07.930Z",
17     "user_id": "auth0|63fe279b2cef38f4fa3da33c",
18     "blocked_for": [],
19     "guardian_authenticators": []
20 }
```

[← Back to Users](#)


chauhanashutoshsingh12001@gmail.com
user_id: auth0|63fe279b2cef38f4fa3da33c

[Actions](#)

Details Devices History Raw JSON Authorized Applications Permissions Roles

Max. Log Storage: 1 days

Event	When	App	Identity Provider	From
🕒 Success Signup	a minute ago	N/A	Username-Pass...	IP: 35.166.202.113 Boardman, United States

[Newer <](#)
Page 1
> Older

Verification Mail :

[← Back to Users](#)


chauhanashutoshsingh12001@gmail.com
user_id: auth0|63fe279b2cef38f4fa3da33c

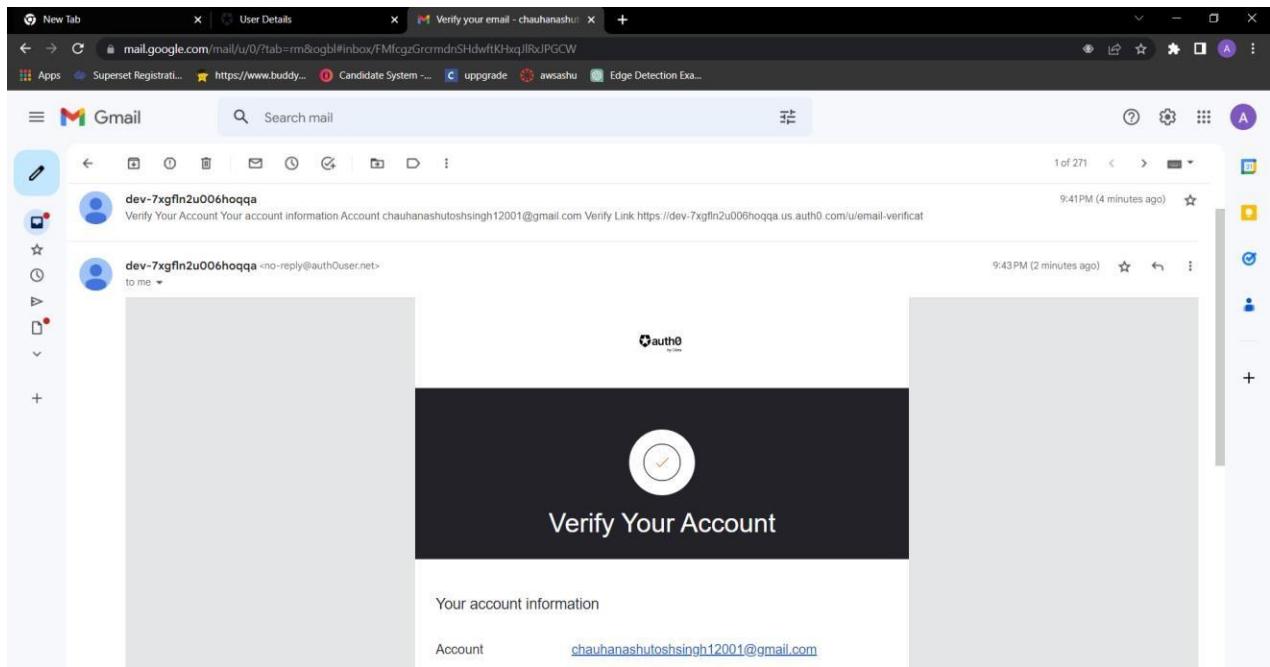
[Actions](#)

Details Devices History Raw JSON Authorized Applications Permissions Roles

Name chauhanashutoshsingh12001@gma... Edit	Email chauhanashutoshsingh12001@gma... (pending) Edit	Signed Up February 28th 2023, 9:41:07 PM
Primary Identity Provider Database	Latest Login Never	Accounts Associated None
Browser Other 0.0.0 / Other 0.0.0		

- [✉️ Send Verification Email](#)
- [✉️ Change Email](#)
- [✉️ Change Password](#)
-
- [🚫 Block](#)
- [🗑️ Delete](#)

[Type here]



MAIL VERIFIED:

Details Devices History Raw JSON Authorized Applications Permissions Roles

Name chauhanashutoshsingh12001@gma... Edit	Email chauhanashutoshsingh12001@gma... (verified) Edit	Signed Up February 28th 2023, 9:41:07 PM
Primary Identity Provider Database	Latest Login Never	Accounts Associated None
Browser Chrome Mobile 110.0.0 / Android 0....		

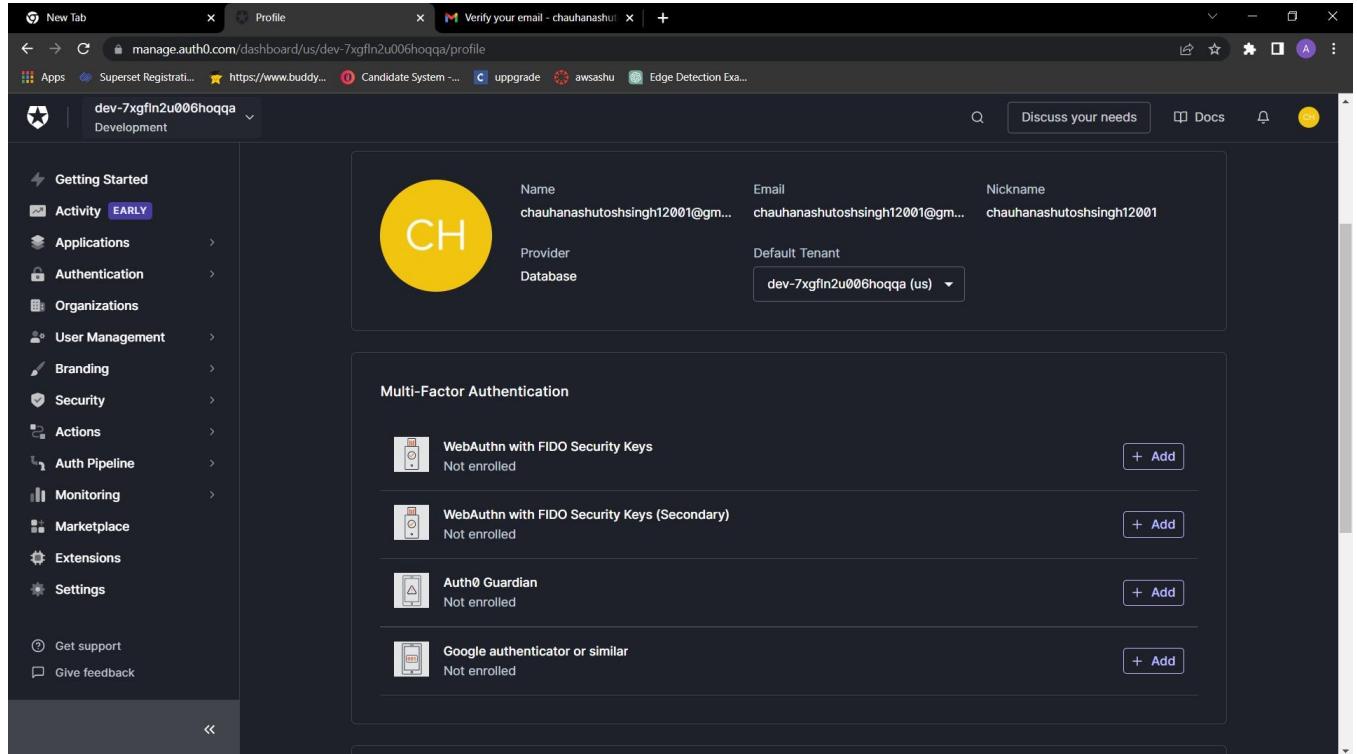
[Type here]

Users

+ Create User

An easy to use UI to help administrators manage user identities including password resets, creating and provisioning, blocking and deleting users.
[Learn more →](#)

Q Search for users	Search by User	X Reset		
Name	Connection	Logins	Latest Login	⋮
 chauhanashutoshsingh12001@gmail.com chauhanashutoshsingh12001@gmail.com	Username-Password-Authenti...	0	never	⋮
 ashusingh478@gmail.com ashusingh478@gmail.com	Username-Password-Authenti...	0	never	⋮



The screenshot shows the Auth0 dashboard interface. On the left, there's a sidebar with navigation links like Getting Started, Activity (EARLY), Applications, Authentication, Organizations, User Management, Branding, Security, Actions, Auth Pipeline, Monitoring, Marketplace, Extensions, and Settings. Below these are links for Get support and Give feedback.

The main content area displays a user profile for 'chauhanashutoshsingh12001@gmail.com'. The profile includes fields for Name, Email, Nickname, Provider, and Database, all set to 'dev-7xgfln2u006hoqqa (us)'. Below the profile, there's a section for Multi-Factor Authentication (MFA) with four options: WebAuthn with FIDO Security Keys, WebAuthn with FIDO Security Keys (Secondary), Auth0 Guardian, and Google authenticator or similar, all listed as 'Not enrolled'.

[Type here]

BYAWS/.

The screenshot shows the IAM Identity Center landing page. At the top, it says "Security, Identity, and Compliance". The main title is "IAM Identity Center (successor to AWS Single Sign-On)". Below the title, there's a subtitle: "Manage workforce access to multiple AWS accounts and cloud applications." A call-to-action button labeled "Enable" is visible. A note at the bottom says: "Use IAM Identity Center to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications." A "Getting started" link is at the bottom right.

This screenshot is identical to the one above, but the "Enable" button has changed to a grey "Enabling" button with a circular progress icon. The rest of the content, including the subtitle and the "Getting started" link, remains the same.

The screenshot shows the IAM Identity Center console. The left sidebar includes "Dashboard", "Users", "Groups", "Settings", "Multi-account permissions" (with "AWS accounts" and "Permission sets" listed), and "Application assignments" (with "Applications" listed). A "Related consoles" section shows "IAM" with a "New" button. The main content area has a blue header bar with the text: "AWS IAM Identity Center is the updated console for the features of AWS Single Sign-On (AWS SSO). The features that comprised AWS Single Sign-On (AWS SSO) are available through the IAM Identity Center console. They offer a better way to connect or create a workforce directory, and to manage users' access across AWS accounts and integrated applications. Learn more." Below this, there are two sections: "Recommended setup steps" (with steps for choosing an identity source, managing accounts, and setting up applications) and "Settings summary" (with options for "Go to settings", "Identity source" set to "Identity Center directory", "Region" set to "Asia Pacific (Mumbai) | ap-south-1", "AWS access portal URL" showing "https://d-9f671c3e1.awsapps.com/start", and a "Customize" button).

CLOUD COMPUTING JOURNAL

Group details

Group name
MYGROUP
Maximum of 128 characters

Description - optional
Group description detailing the permissions assigned to this group.
Enter description
Maximum of 256 characters

Add users to group - optional (0)
Select workforce users to add to this group.

Username	Find users	<	1	>	Cancel	Create group

No users found

Maximum of 128 characters

Description - optional
Group description detailing the permissions assigned to this group.
Enter description
Maximum of 256 characters

Add users to group - optional (0)
Select workforce users to add to this group.

Username	Find users	<	1	>	Cancel	Create group

No users found

Add user

IAM Identity Center

- Dashboard
- Users
- Groups**
- Settings

- Multi-account permissions
 - AWS accounts
 - Permission sets
- Application assignments
 - Applications

Related consoles
IAM 

The group "MYGROUP" has been successfully created.
You can now grant this group permissions to accounts or applications so that users in this group can access assigned AWS accounts and cloud applications when they sign in to the AWS access portal.

View group details 

IAM Identity Center > Groups

Groups (1)
With groups, you can grant or deny permissions to groups of workforce users, rather than having to apply those permissions to each user. [Learn more](#)

 Delete group	Create group
 Find groups by group name	< 1 > 
<input type="checkbox"/> Group name	Description
<input type="checkbox"/> MYGROUP	-
	Created by
	Manual

Create users

CLOUD COMPUTING JOURNAL

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +,=,_,@,-

Password
Choose how you want this user to receive their password. [Learn more](#)

Send an email to this user with password setup instructions.

Generate a one-time password that you can share with this user.

Email address
cvd@gmail.com

Confirm email address
cvd@gmail.com

IAM Identity Center > Users > Add user

Step 1
[Specify user details](#)

Step 2 - optional
Add user to groups

You can assign this user to one or more groups.

Groups (1/1)

Group name [Edit](#)

MYGROUP

[Create group](#)

< 1 > [Cancel](#) [Previous](#) [Next](#)

Preferences - optional

Additional attributes - optional

Step 2: Add user to groups - optional [Edit](#)

Groups (1)

Group name [Edit](#)

MYGROUP

< 1 > [Cancel](#) [Previous](#) [Add user](#)

IAM Identity Center

- Dashboard
- Users**
- Groups
- Settings
- Multi-account permissions
 - AWS accounts
 - Permission sets
- Application assignments

The user "PRADEEP" was successfully added.
The user will receive an email with a link to set up a password and instructions to connect to the AWS access portal. The link will be valid for up to 7 days. You can grant this user permissions to [accounts](#) or [applications](#) so that they can access their assigned AWS accounts and cloud applications when they sign in to the AWS access portal.

[View user details](#) [X](#)

IAM Identity Center > Users

Users (1)

Users listed here can sign in to the AWS access portal to access AWS accounts and assigned cloud applications. [Learn more](#)

[Delete users](#) [Add user](#)

Username [Edit](#) [Find users](#)

< 1 > [Cancel](#) [Previous](#) [Add user](#)

CLOUD COMPUTING JOURNAL

IAM Identity Center X

2 users were successfully added to the "MYGROUP" group.

Group ID	Created by	Updated by
a1037dfa-b0e1-7054-1cd3-946c6815c508	Manual	Manual

Dashboard

Users

Groups

Settings

CONCLUSION : Successfully implemented Single-Sign-On(SSO).