Index

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.

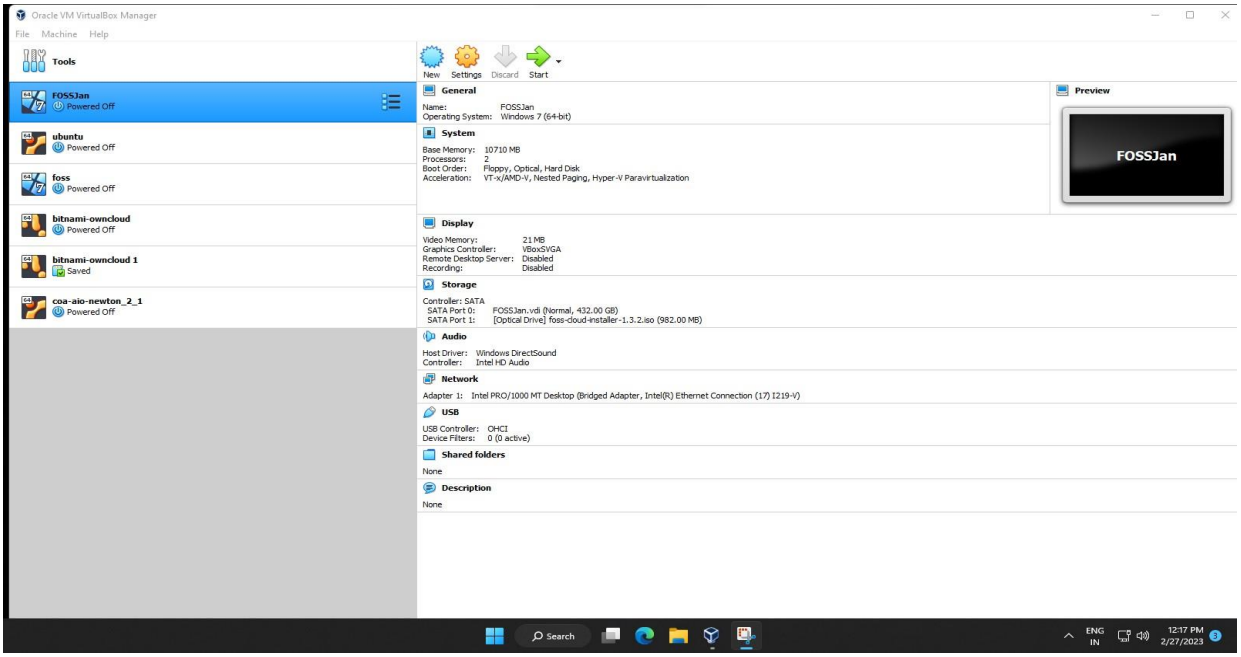
5. On-demand scalability

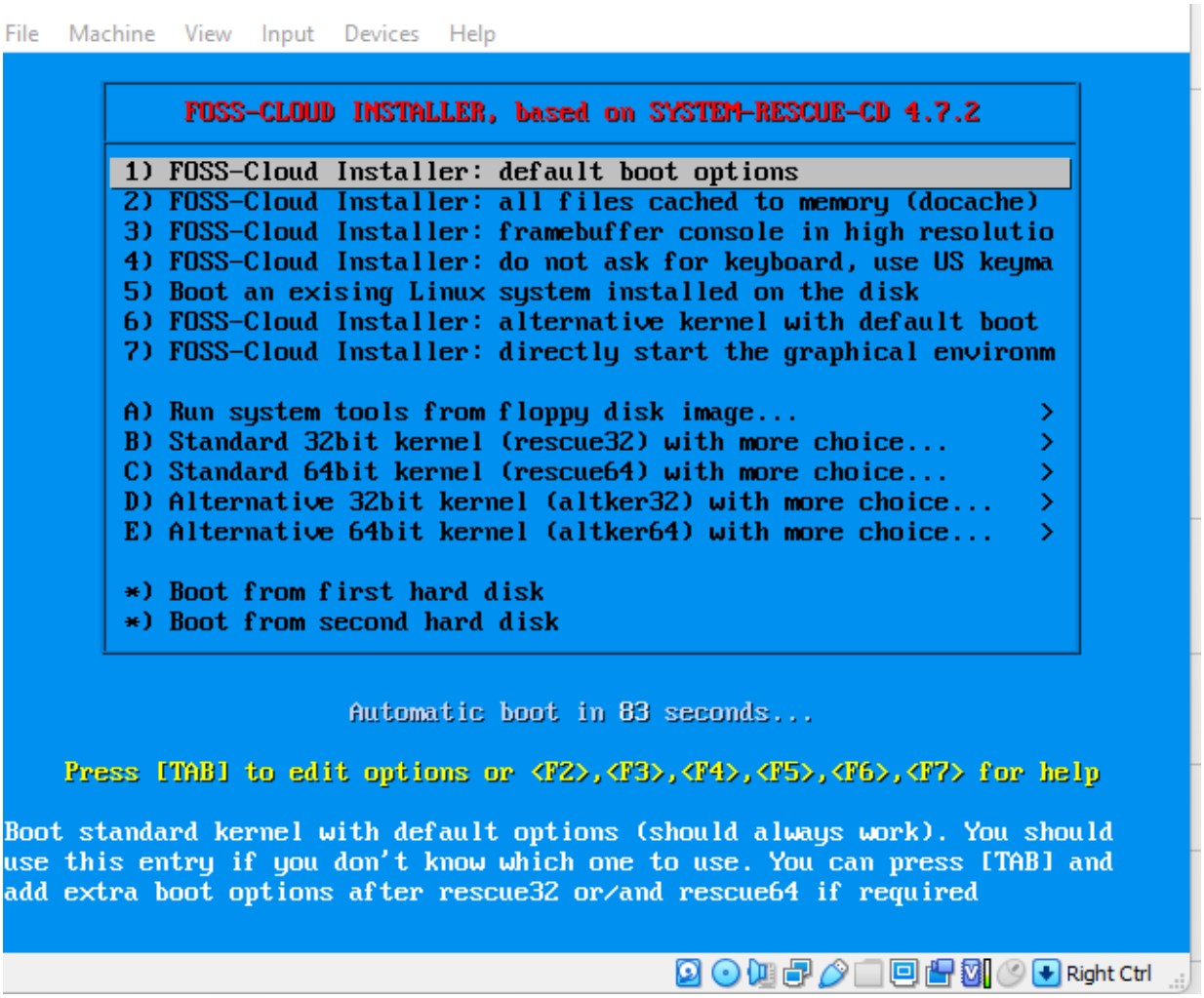
On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

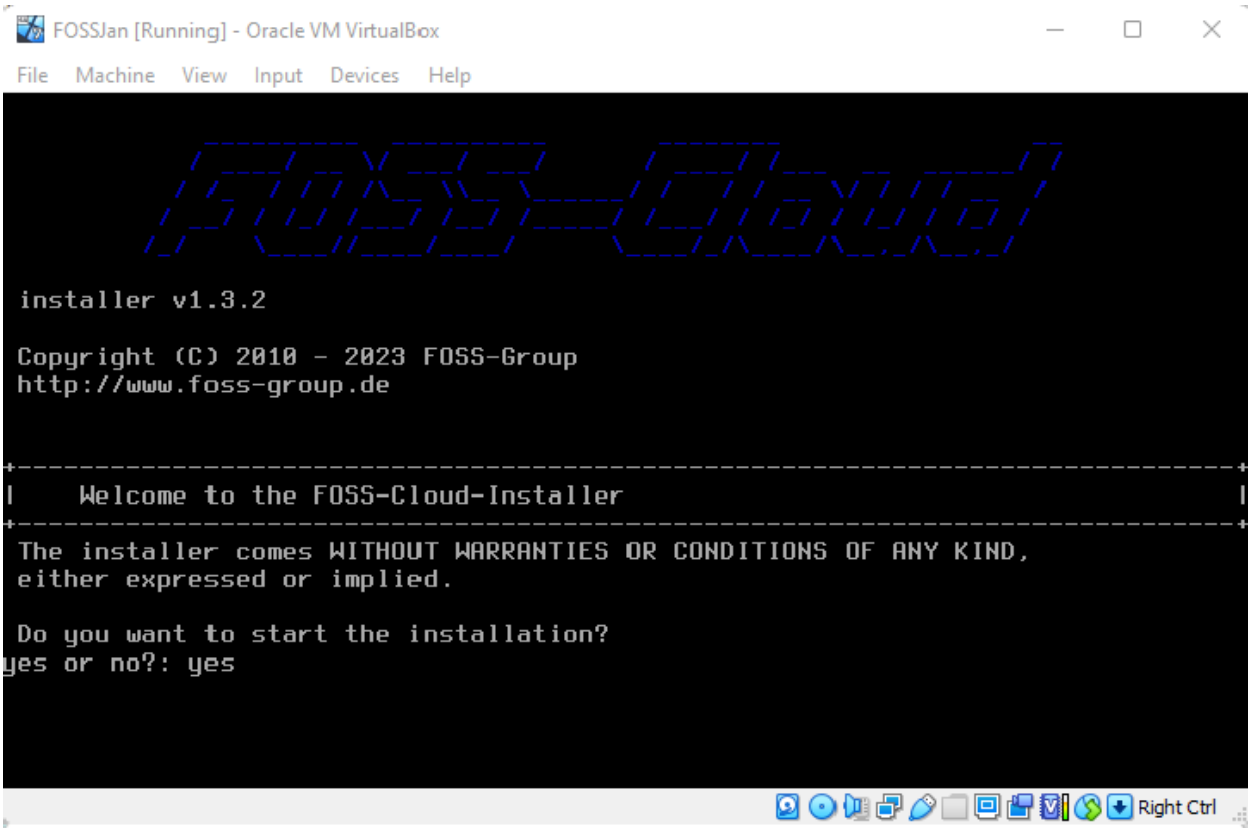
Methods and Steps:

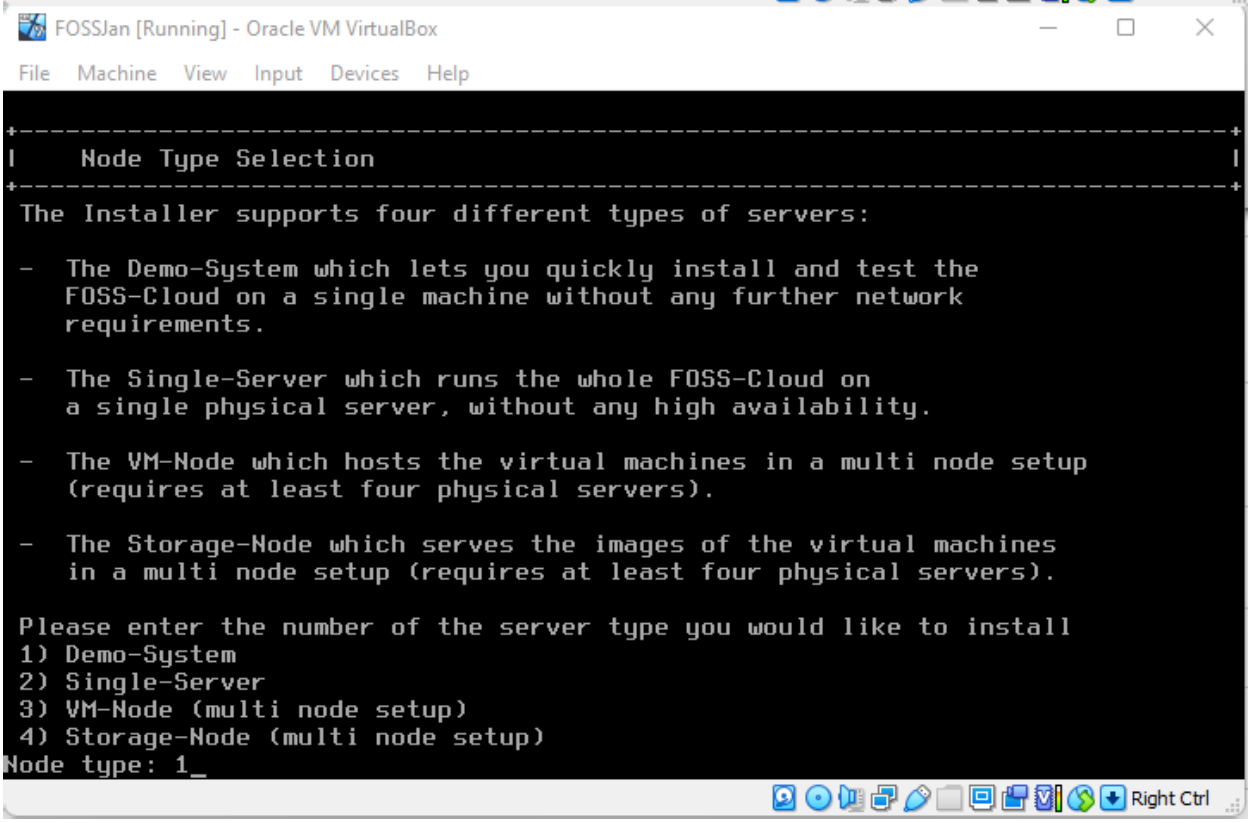
A. Using FOSS Demo / FOSS Server.

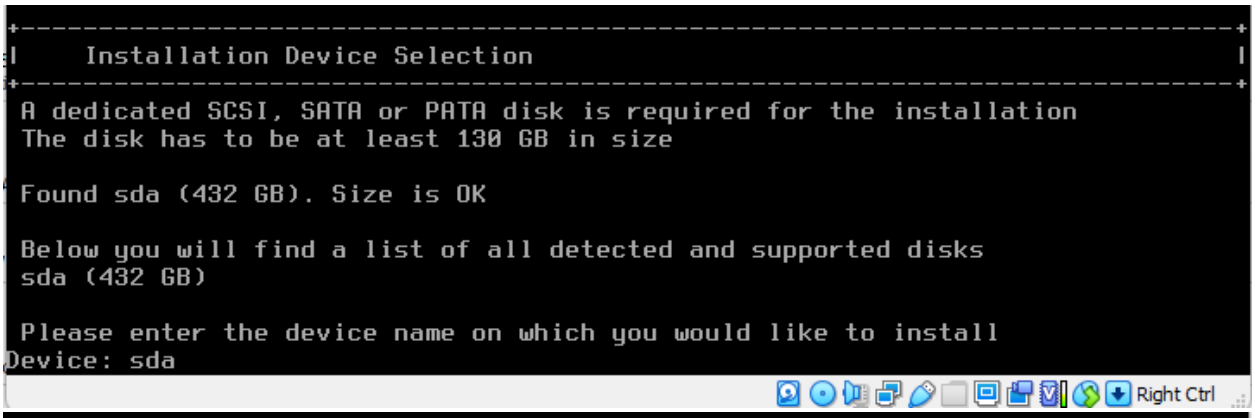
INSTALLATION:

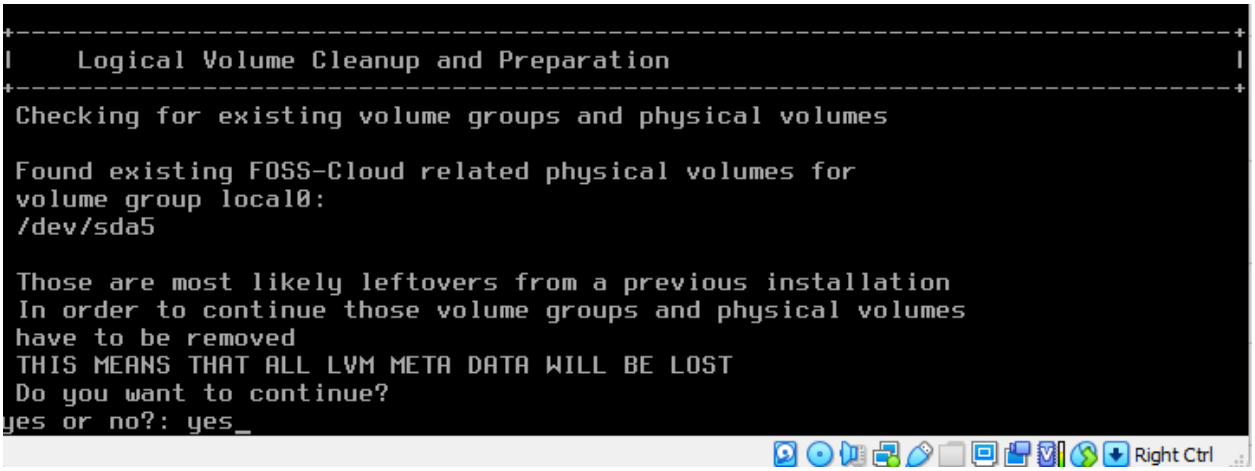


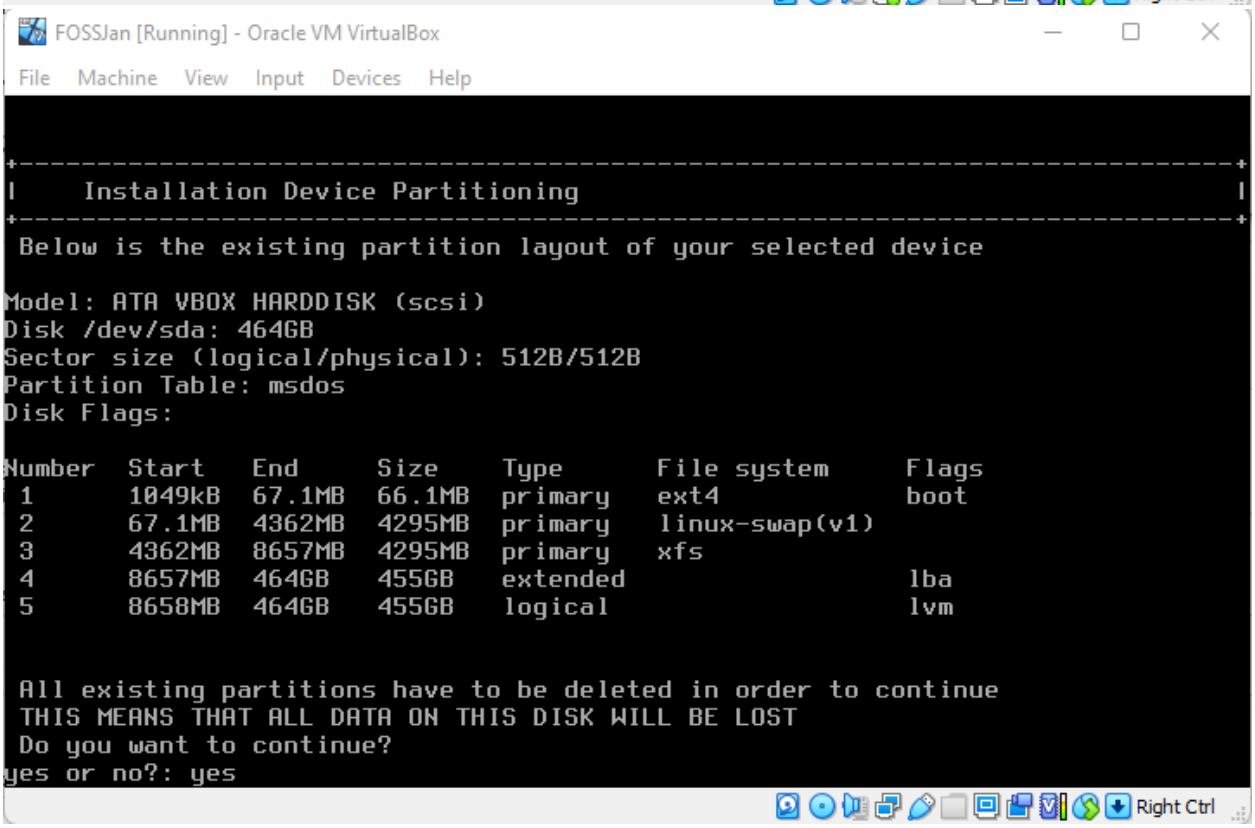


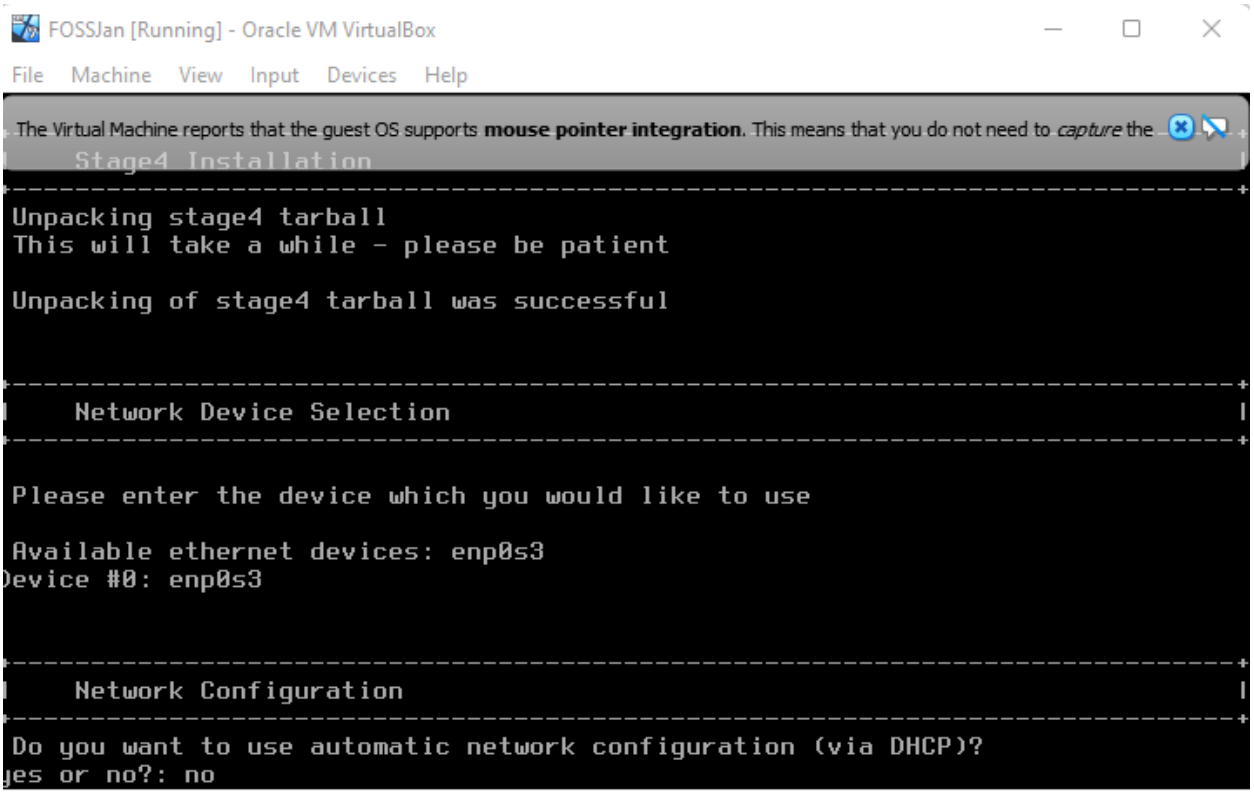

FOSSJan [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
installer v1.3.2
Copyright (C) 2010 - 2023 FOSS-Group
http://www.foss-group.de
Welcome to the FOSS-Cloud-Installer
The installer comes WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND,
either expressed or implied.
Do you want to start the installation?
yes or no?: yes
Right Ctrl

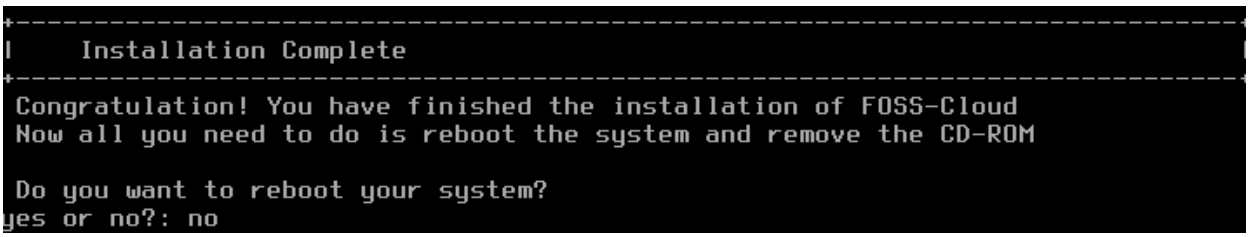

FOSSJan [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Node Type Selection
The Installer supports four different types of servers:
- The Demo-System which lets you quickly install and test the
FOSS-Cloud on a single machine without any further network
requirements.
- The Single-Server 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_
Right Ctrl

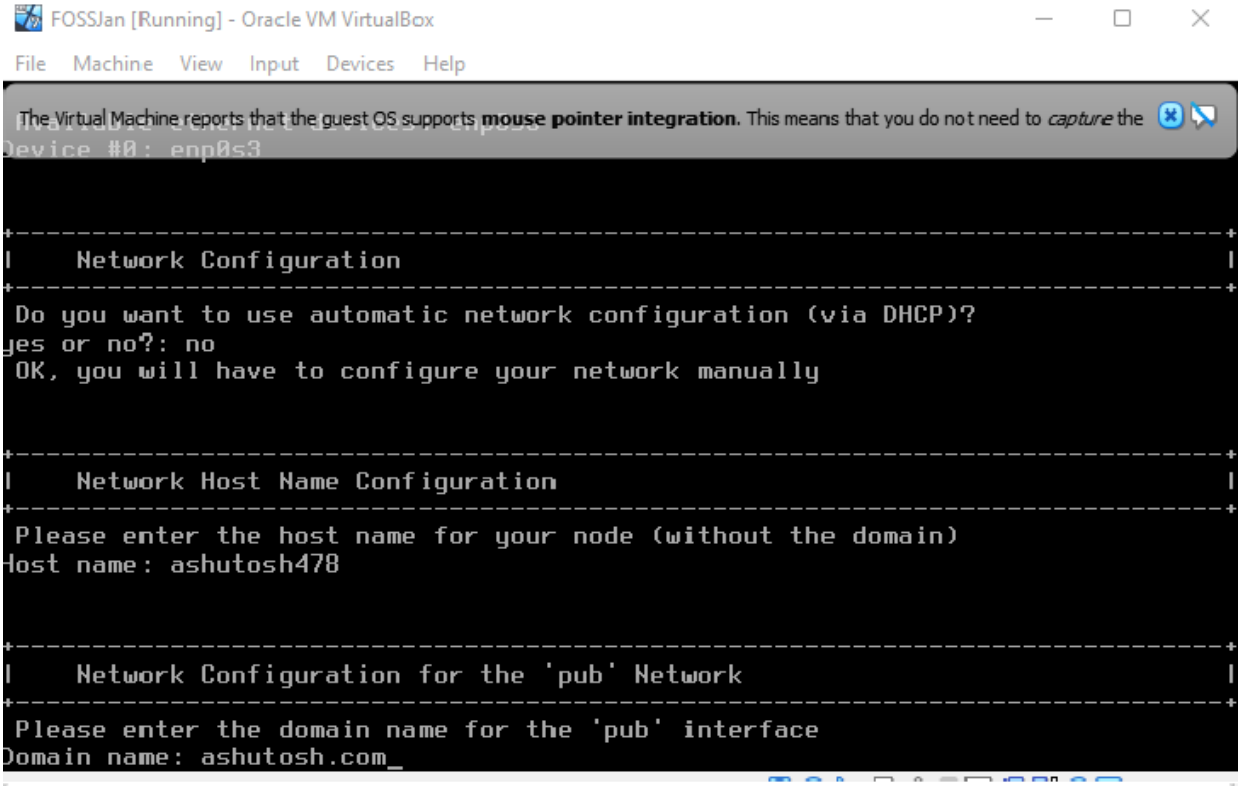

Installation Device Selection
A dedicated SCSI, SATA or PATA disk is required for the installation
The disk has to be at least 130 GB in size
Found sda (432 GB). Size is OK
Below you will find a list of all detected and supported disks
sda (432 GB)
Please enter the device name on which you would like to install
Device: sda
Right Ctrl

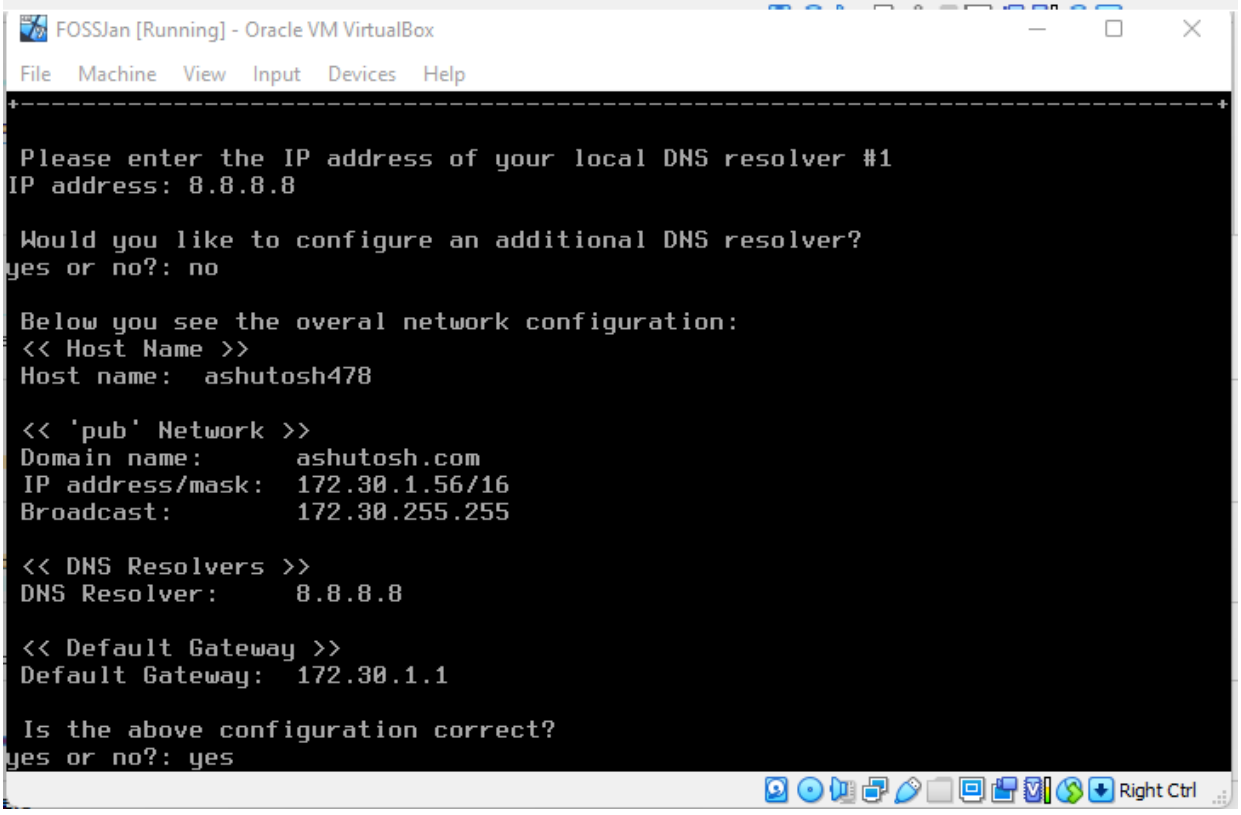

Logical Volume Cleanup and Preparation
Checking for existing volume groups and physical volumes
Found existing FOSS-Cloud related physical volumes for
volume group local0:
/dev/sda5
Those are most likely leftovers from a previous installation
In order to continue those volume groups and physical volumes
have to be removed
THIS MEANS THAT ALL LVM META DATA WILL BE LOST
Do you want to continue?
yes or no?: yes
Right Ctrl

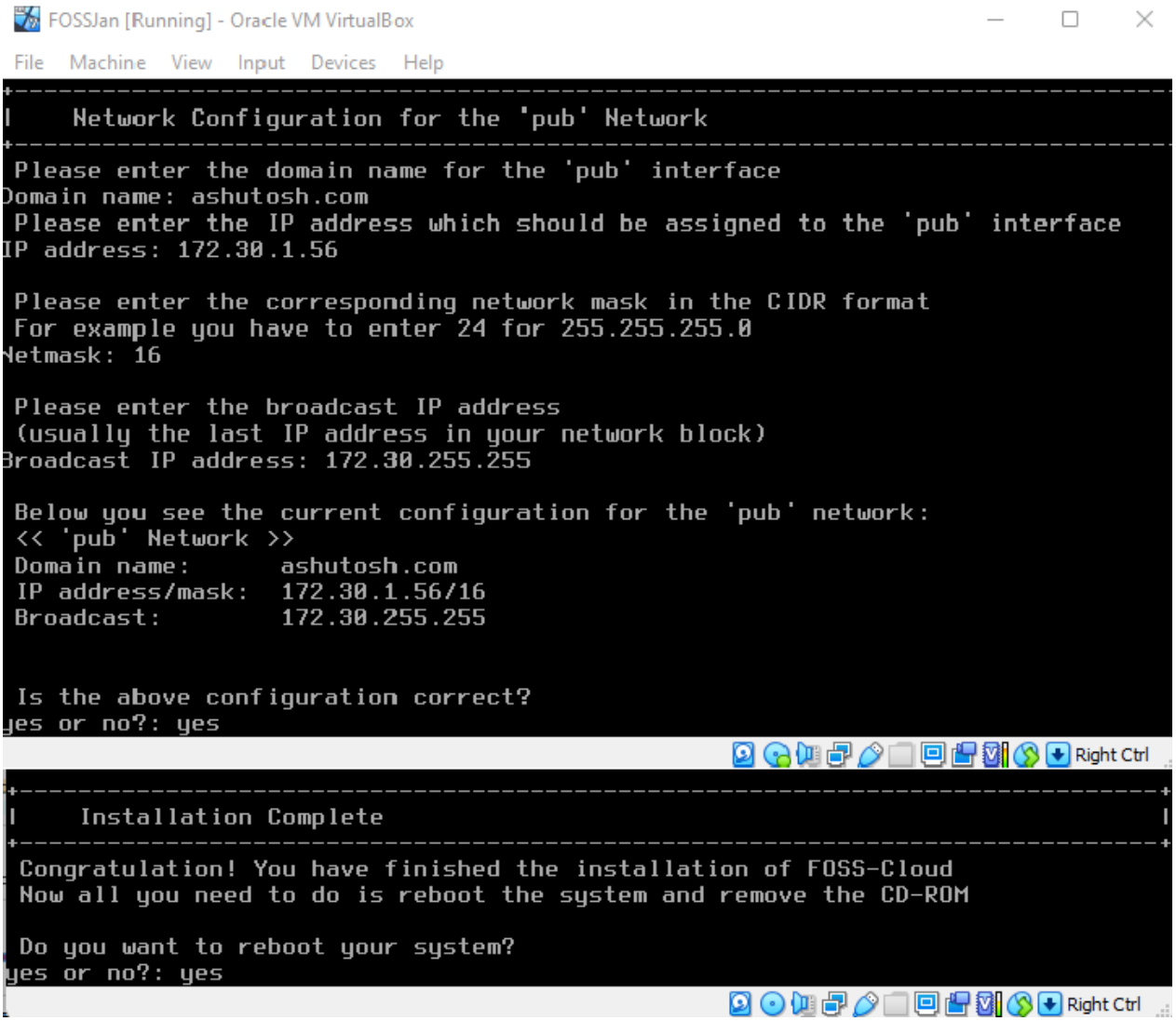

FOSSJan [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Installation Device Partitioning
Below is the existing partition layout of your selected device
Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sda: 464GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
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
Right Ctrl


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
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

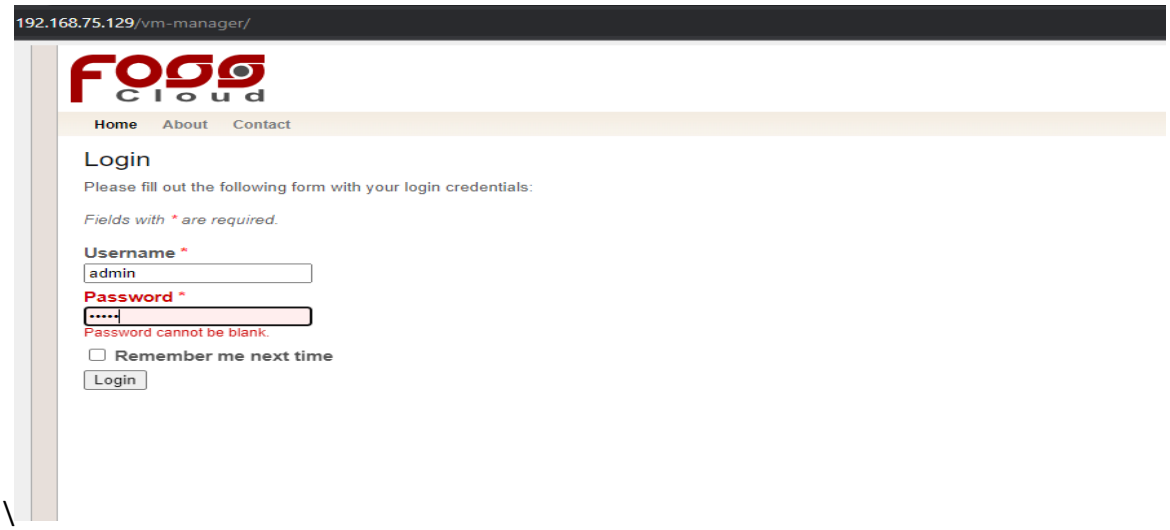

Installation Complete
Congratulation! You have finished the installation of FOSS-Cloud
Now all you need to do is reboot the system and remove the CD-ROM
Do you want to reboot your system?
yes or no?: no


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
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 overal 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
Right Ctrl

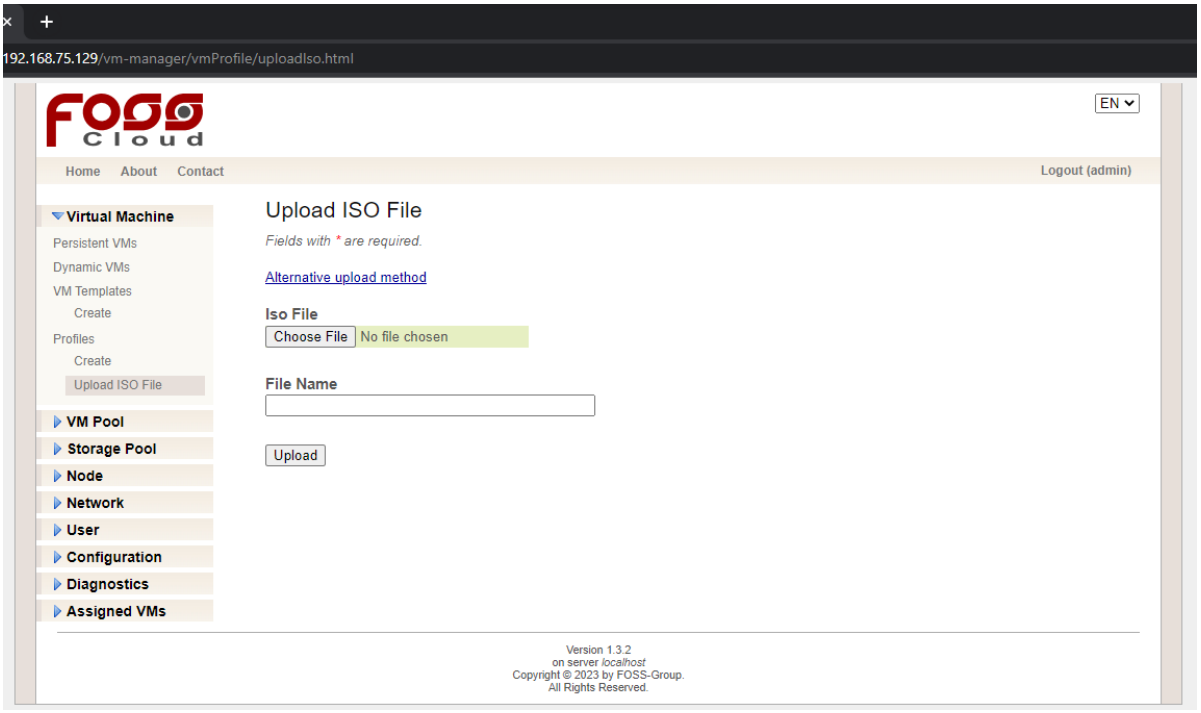


Step 1: After installation, it will show you an IP Address. Put it in your browser to access your administrator page. The default user credentials are user: admin and password: admin. For root login – username- root and password – password.

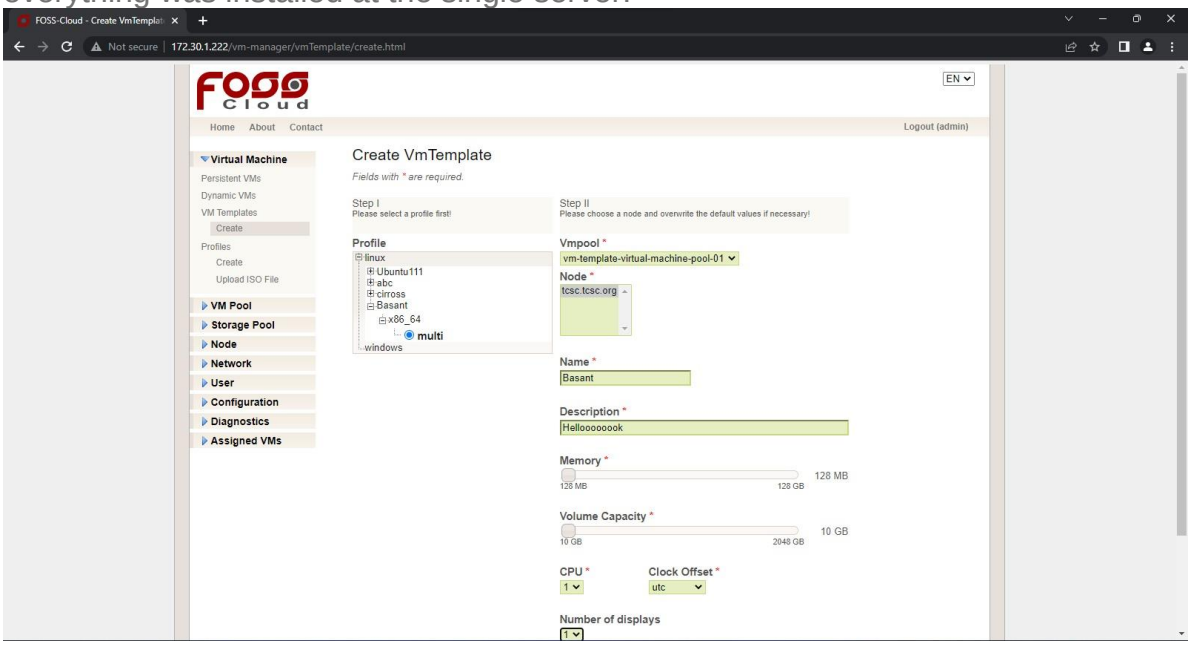


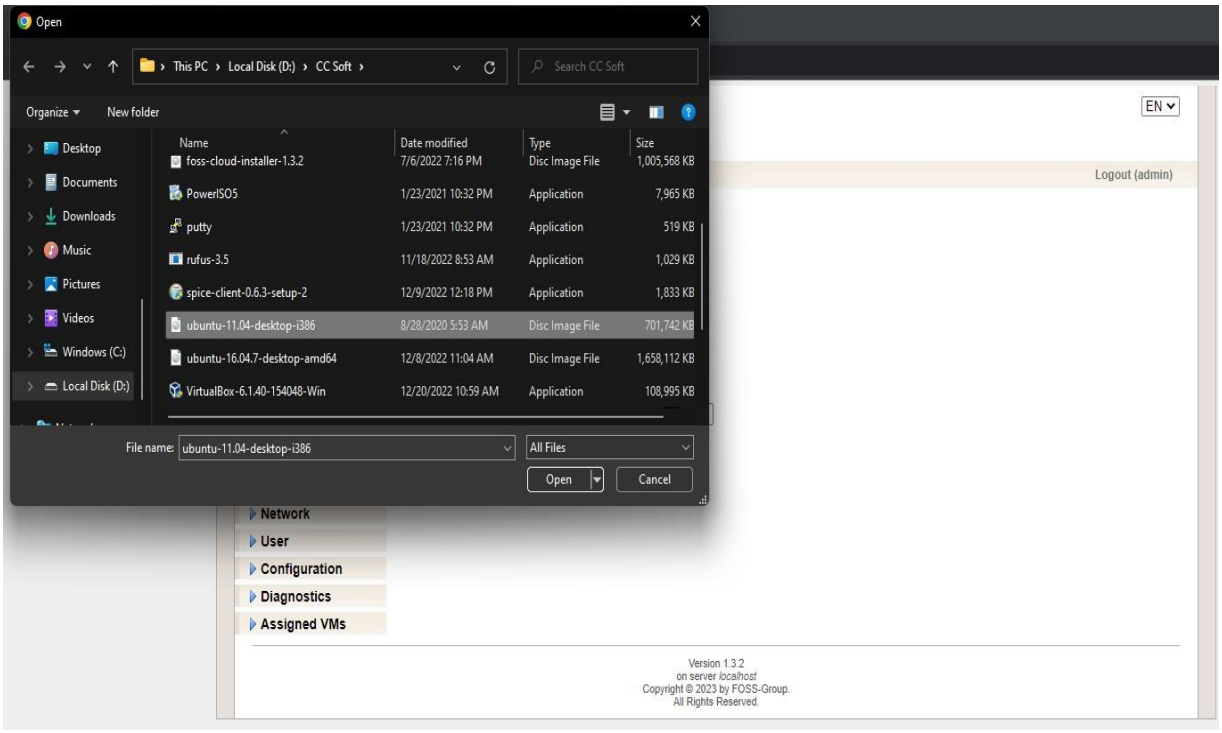
\

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.

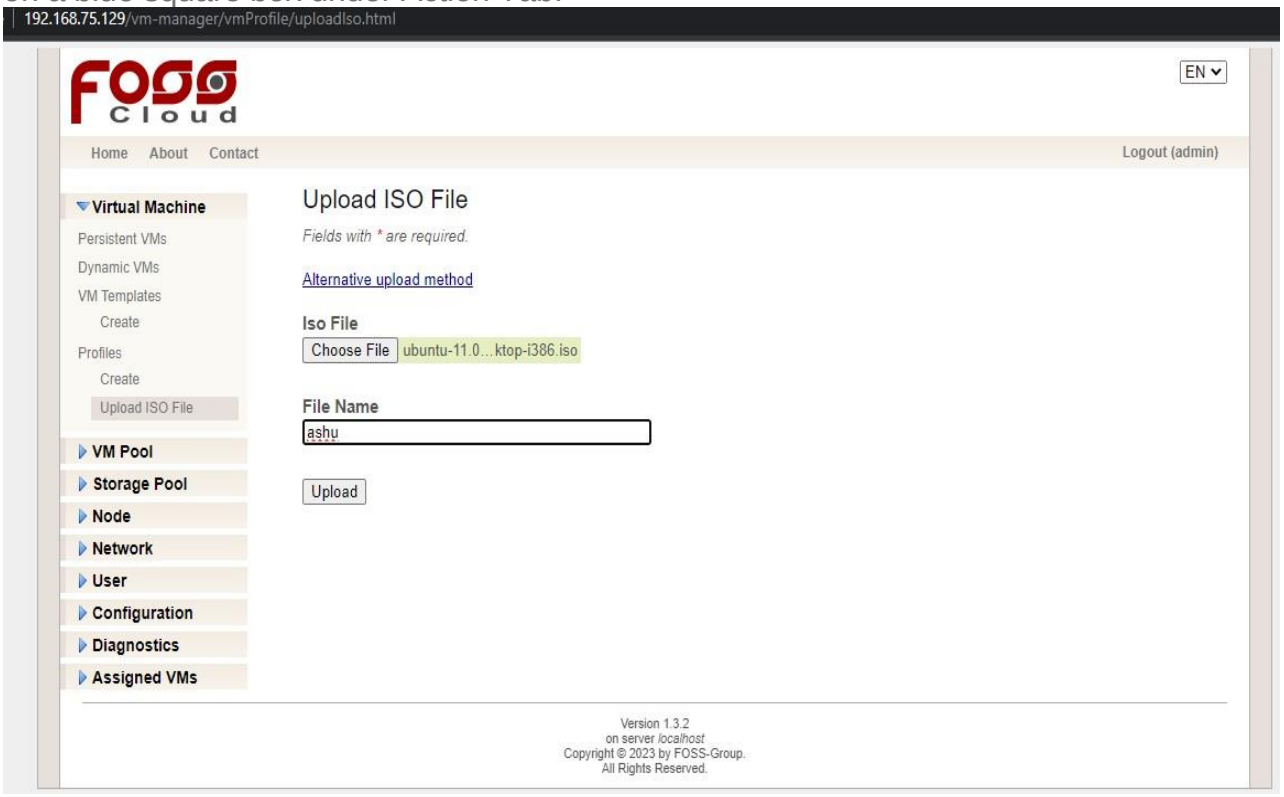


Step 3: Once you uploaded the file, create VmTemplate. In this option you are basically configuring your virtual machine's storage location, CPU, Memory, Node etc. Here, you will find single nodes and VM pool in respective options because everything was installed at the single server.

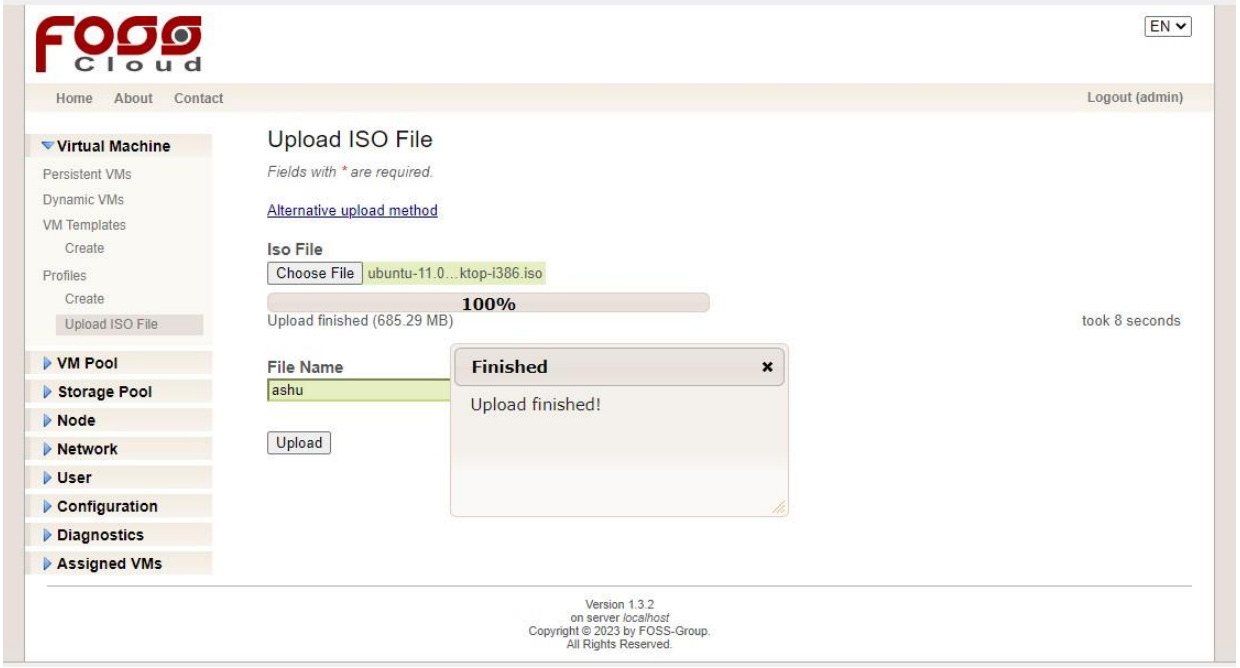


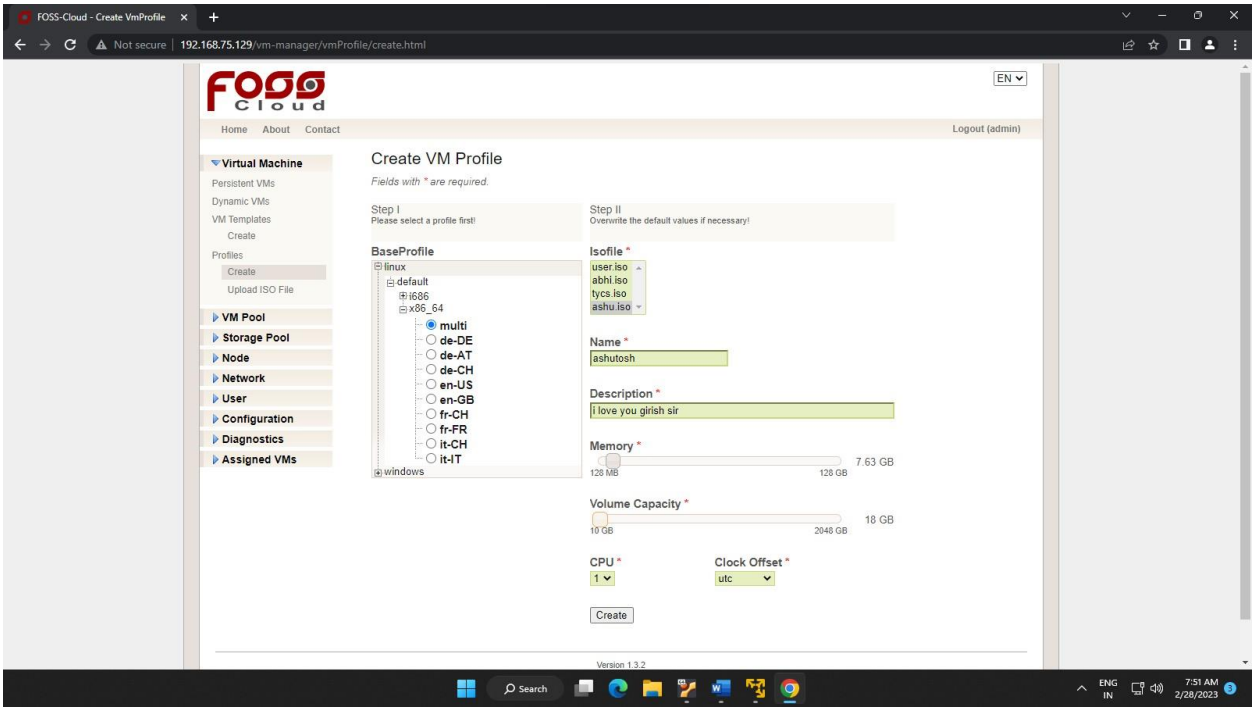


Step 4: Now, click on VMTemplates and you will see a template which you have created in step 4. To start your machine go to Run action Tab and click on the green arrow. Under status tab, it shows the running text with the green circle which shows that your machine is running without any errors. To view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



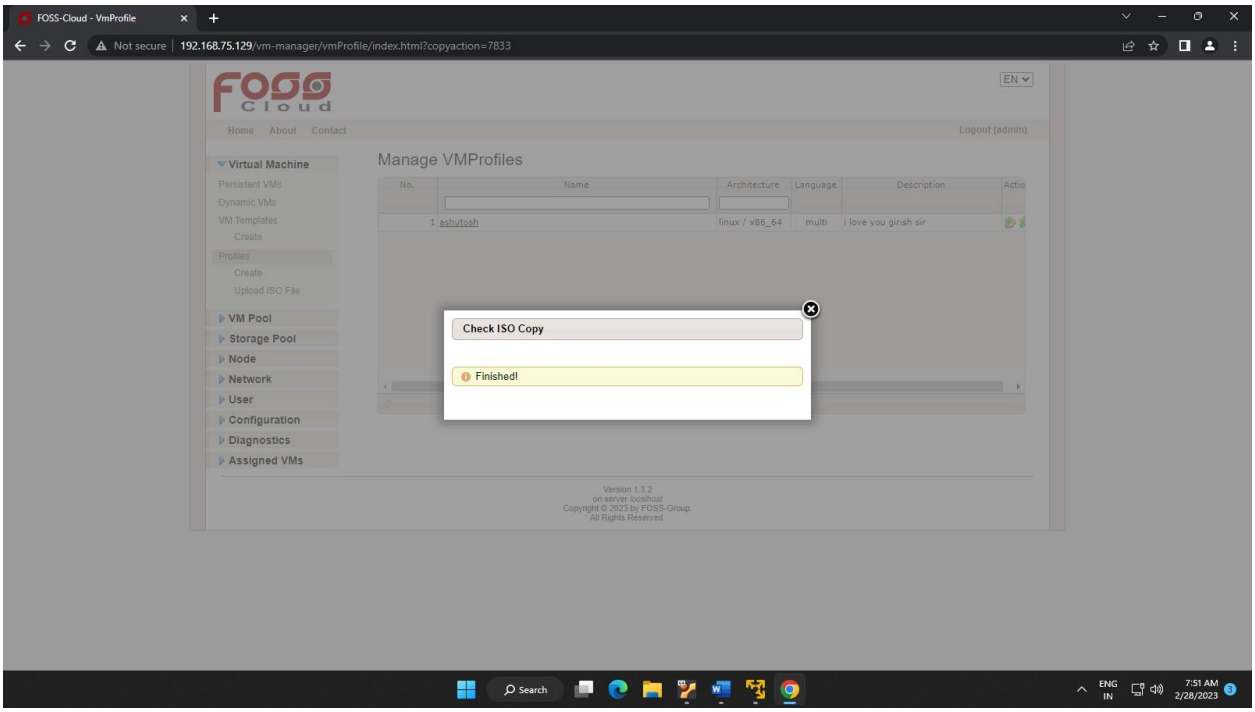
CLOUD COMPUTING JOURNAL

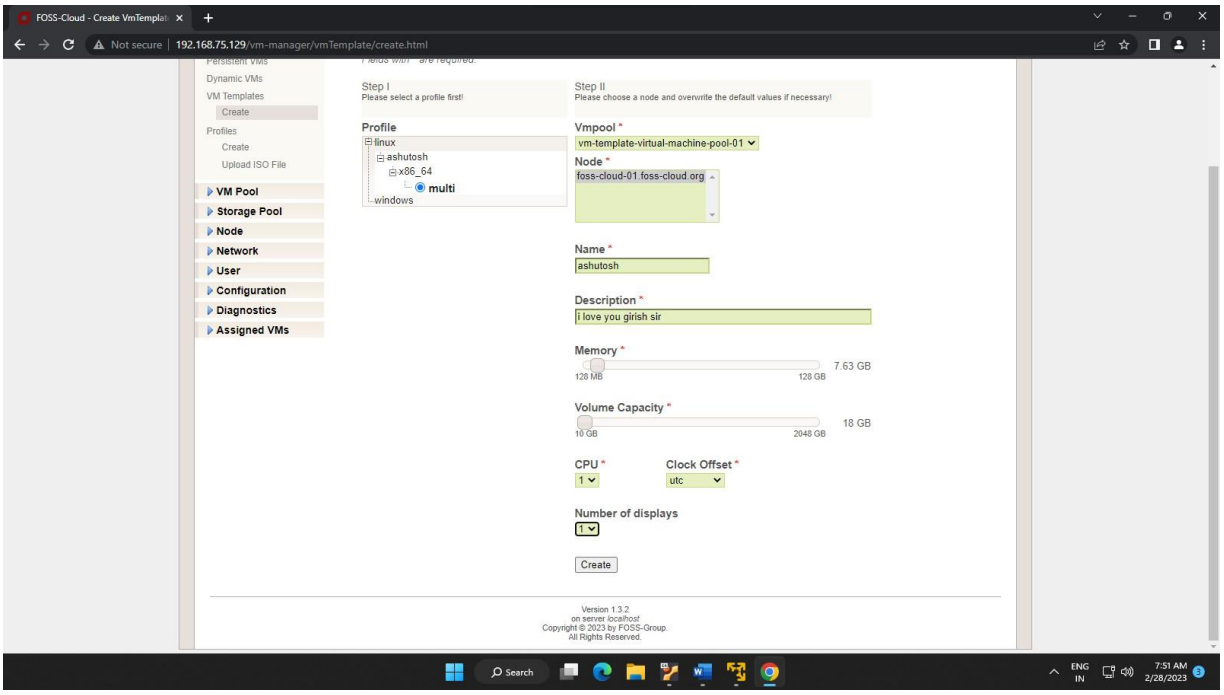


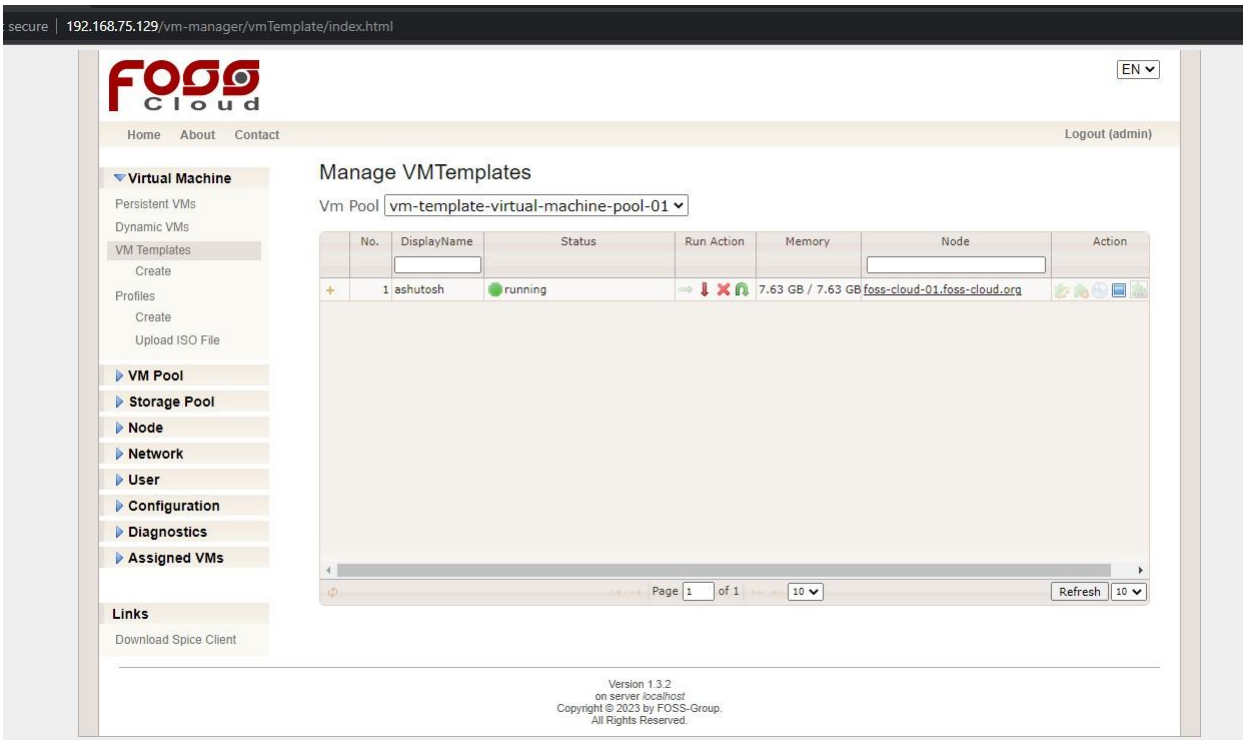


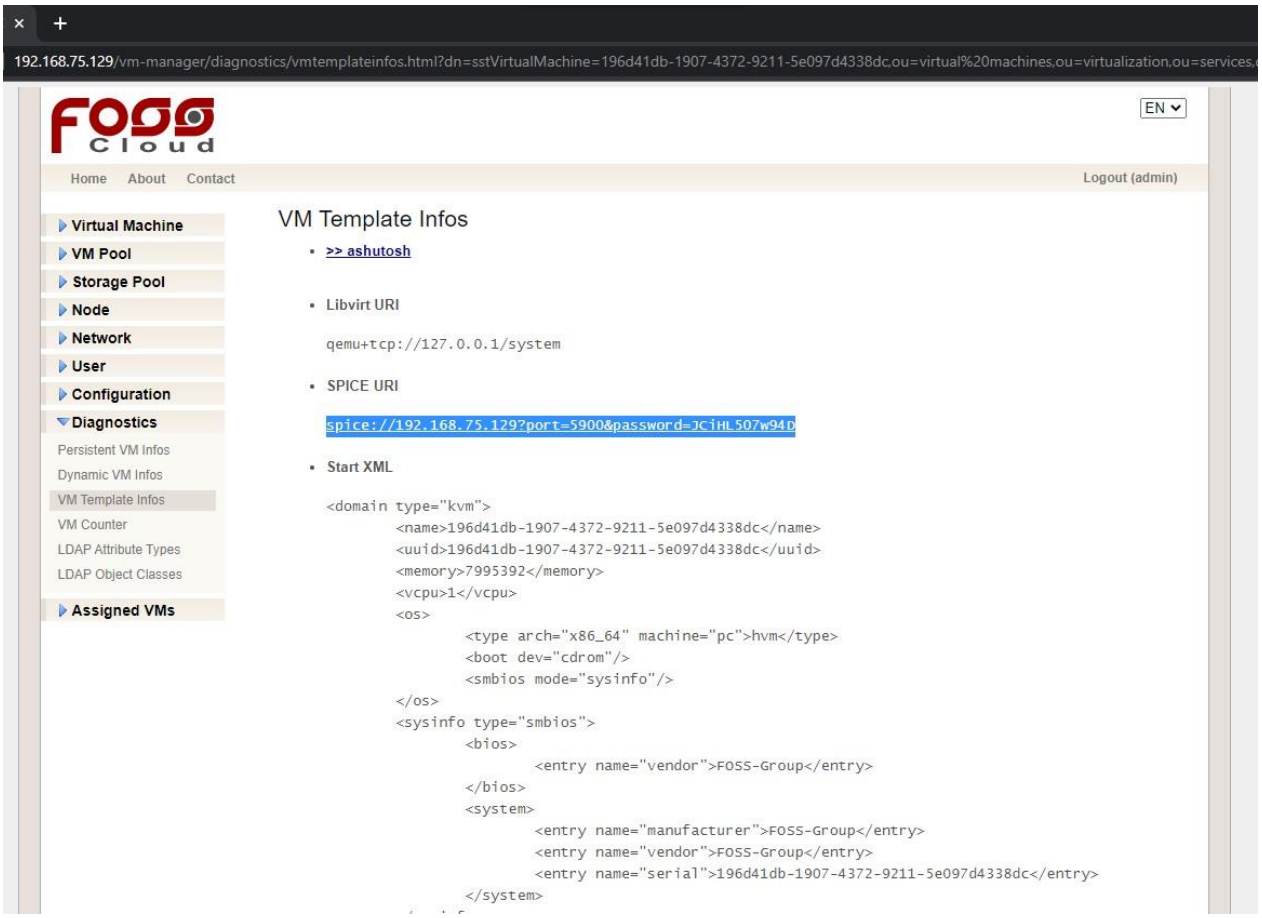
NAME : ASHUTOSH SINGH **ROLL NO : 478**

CLOUD COMPUTING JOURNAL



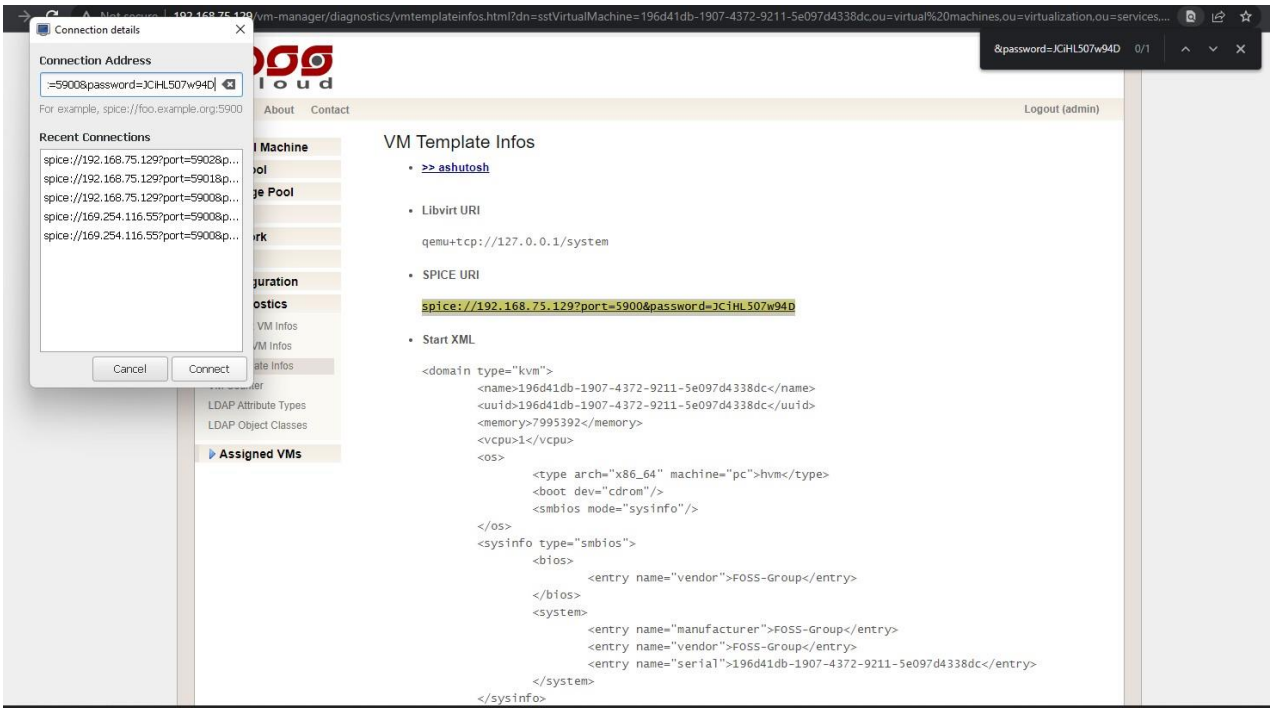


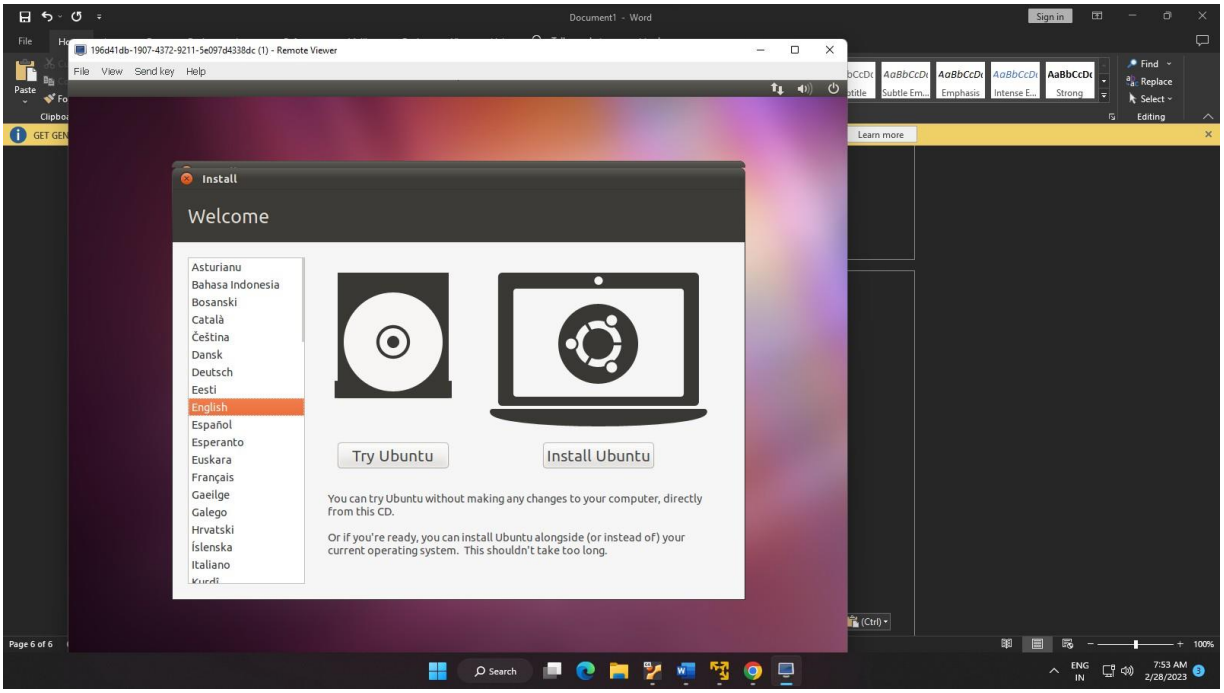

secure | 192.168.75.129/vm-manager/vmTemplate/index.html
FOSS Cloud
EN
Home
About
Contact
Logout (admin)
Virtual Machine
Persistent VMs
Dynamic VMs
VM Templates
Create
Profiles
Create
Upload ISO File
VM Pool
Storage Pool
Node
Network
User
Configuration
Diagnostics
Assigned VMs
Links
Download Spice Client
Manage VMTemplates
Vm Pool vm-template-virtual-machine-pool-01
No.
DisplayName
Status
Run Action
Memory
Node
Action
1
ashutosh
running
7.63 GB / 7.63 GB
foss-cloud-01.foss-cloud.org
Page 1 of 1
10
Refresh
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,
FOSS Cloud
EN
Home
About
Contact
Logout (admin)
Virtual Machine
VM Pool
Storage Pool
Node
Network
User
Configuration
Diagnostics
Persistent VM Infos
Dynamic VM Infos
VM Template Infos
VM Counter
LDAP Attribute Types
LDAP Object Classes
Assigned VMs
VM Template Infos
>> ashutosh
Libvirt URI
qemu+tcp://127.0.0.1/system
SPICE URI
spice://192.168.75.129?port=5900&password=JCiHL507w94D
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>

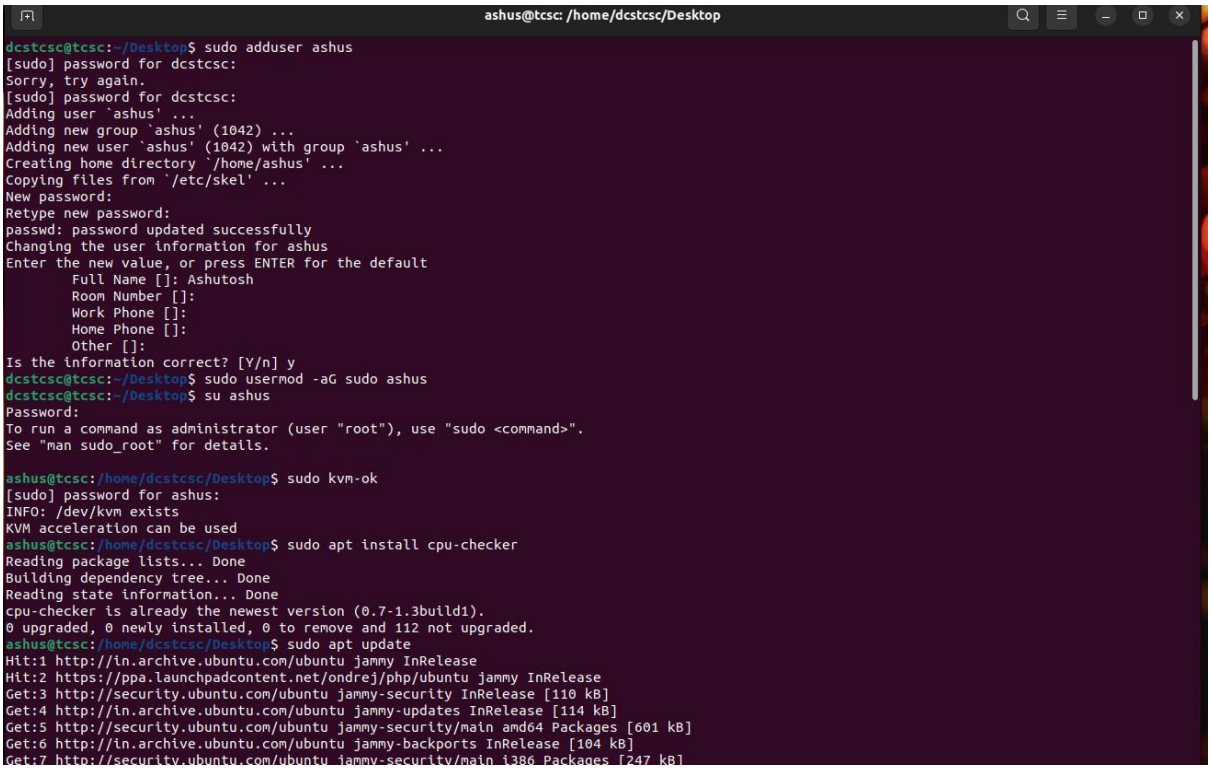
NAME : ASHUTOSH SINGH **ROLL NO : 478**

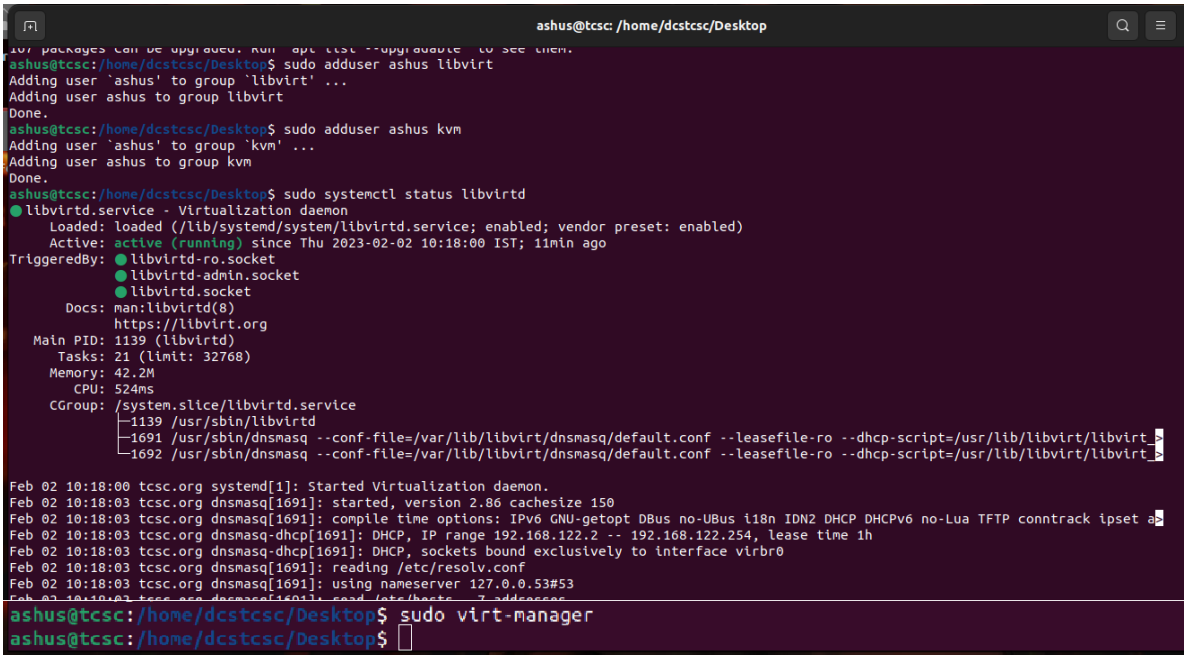
CLOUD COMPUTING JOURNAL

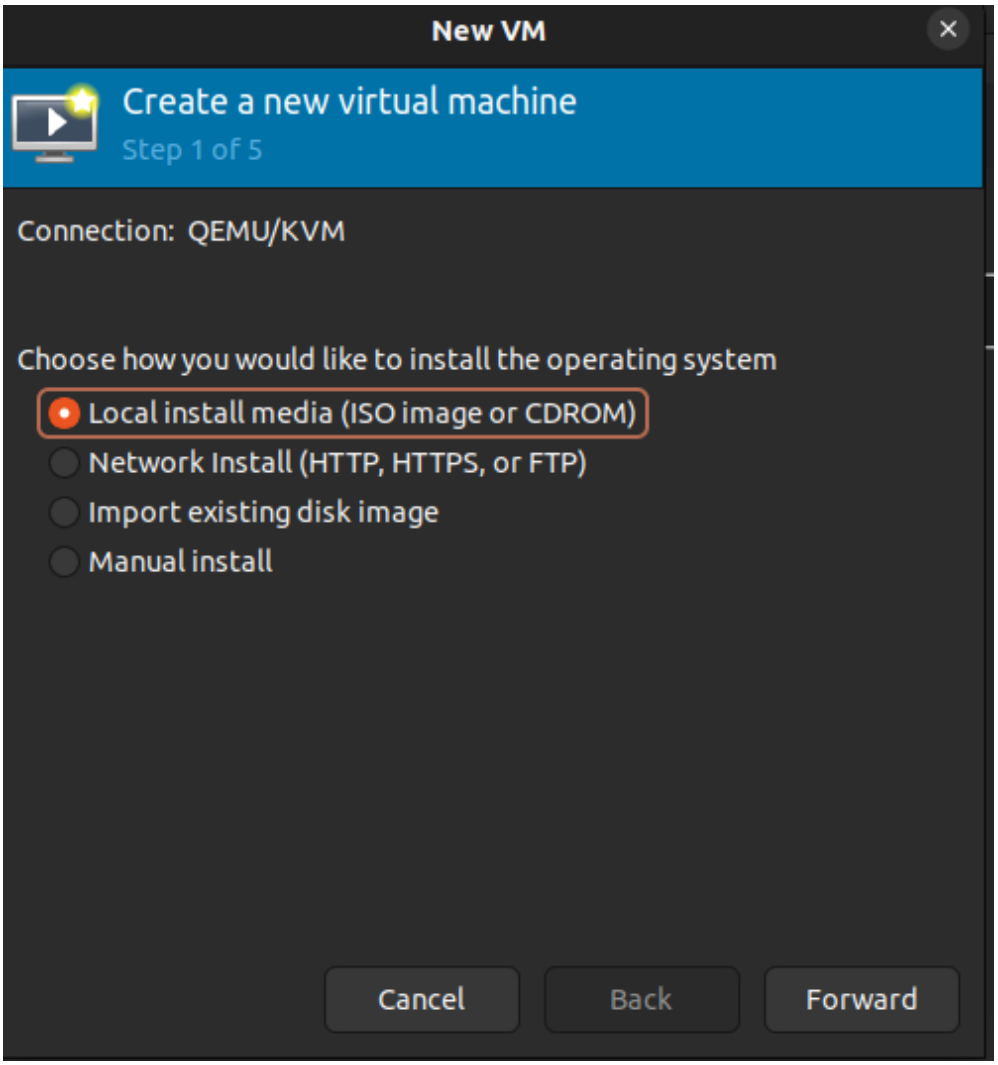




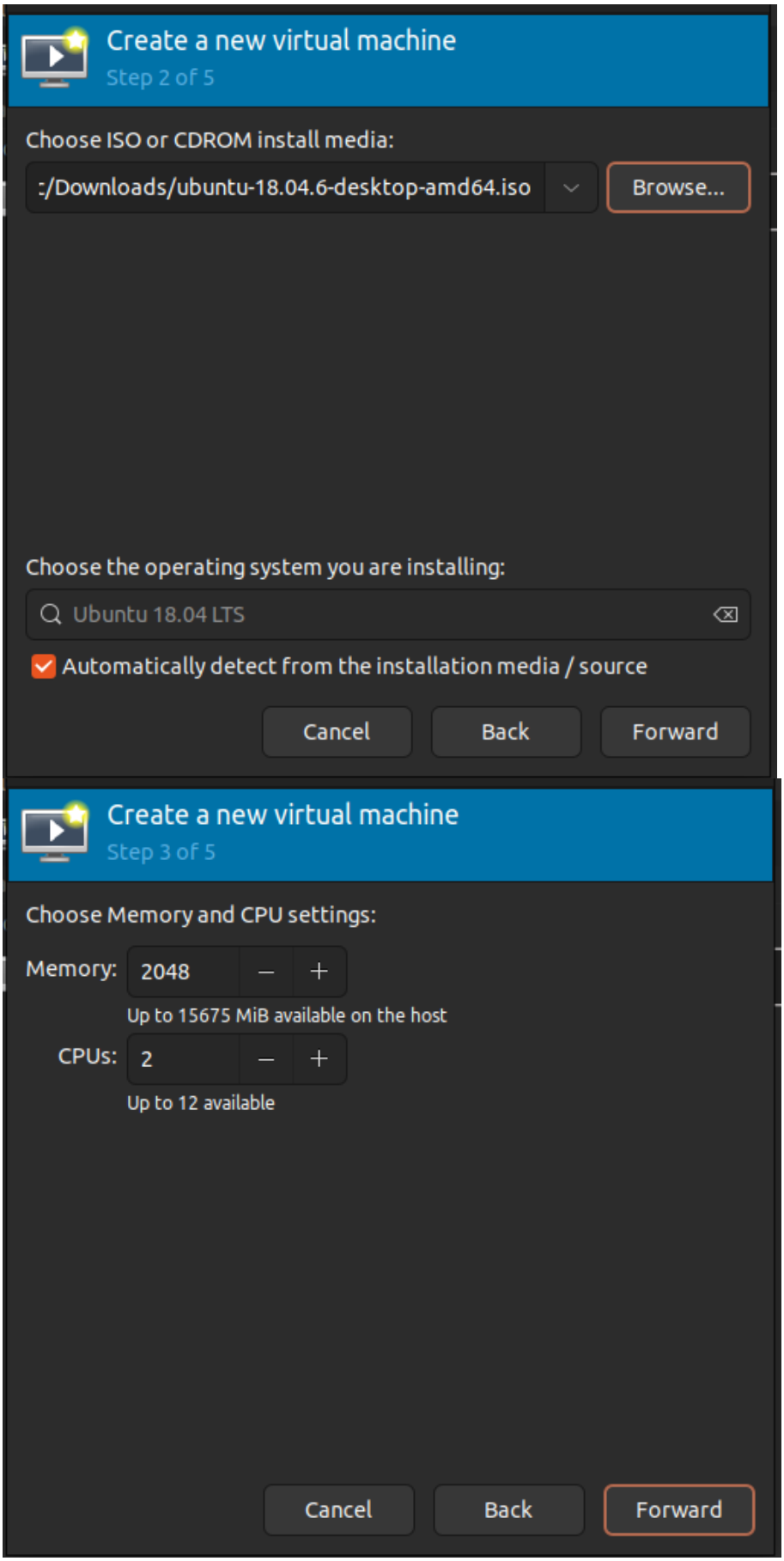
B. USING Ubuntu and KVM

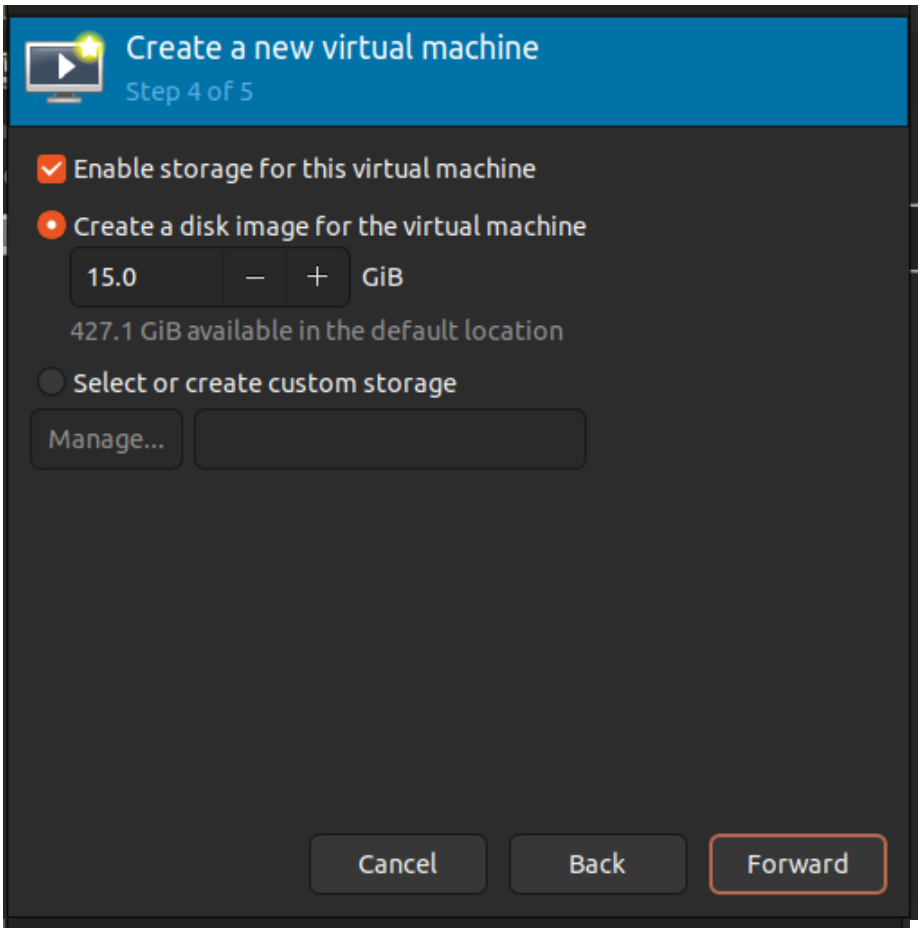


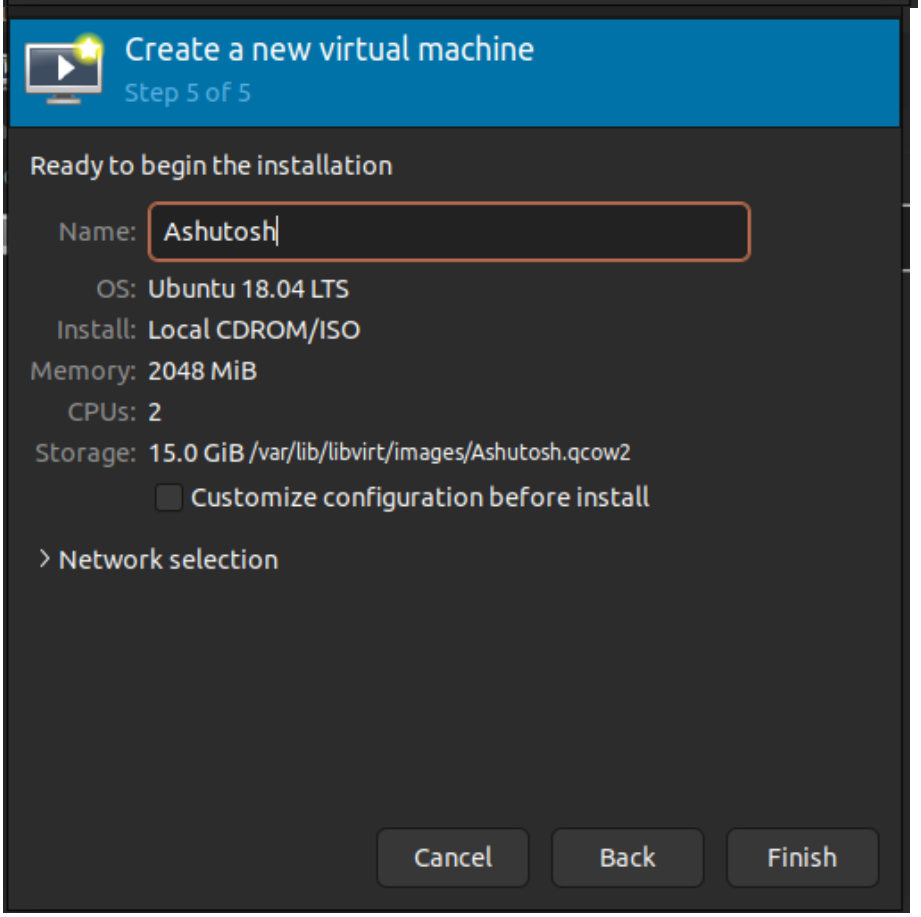



New VM
Create a new virtual machine
Step 1 of 5
Connection: QEMU/KVM
Choose how you would like to install the operating system
Local install media (ISO image or CDROM)
Network Install (HTTP, HTTPS, or FTP)
Import existing disk image
Manual install
Cancel
Back
Forward

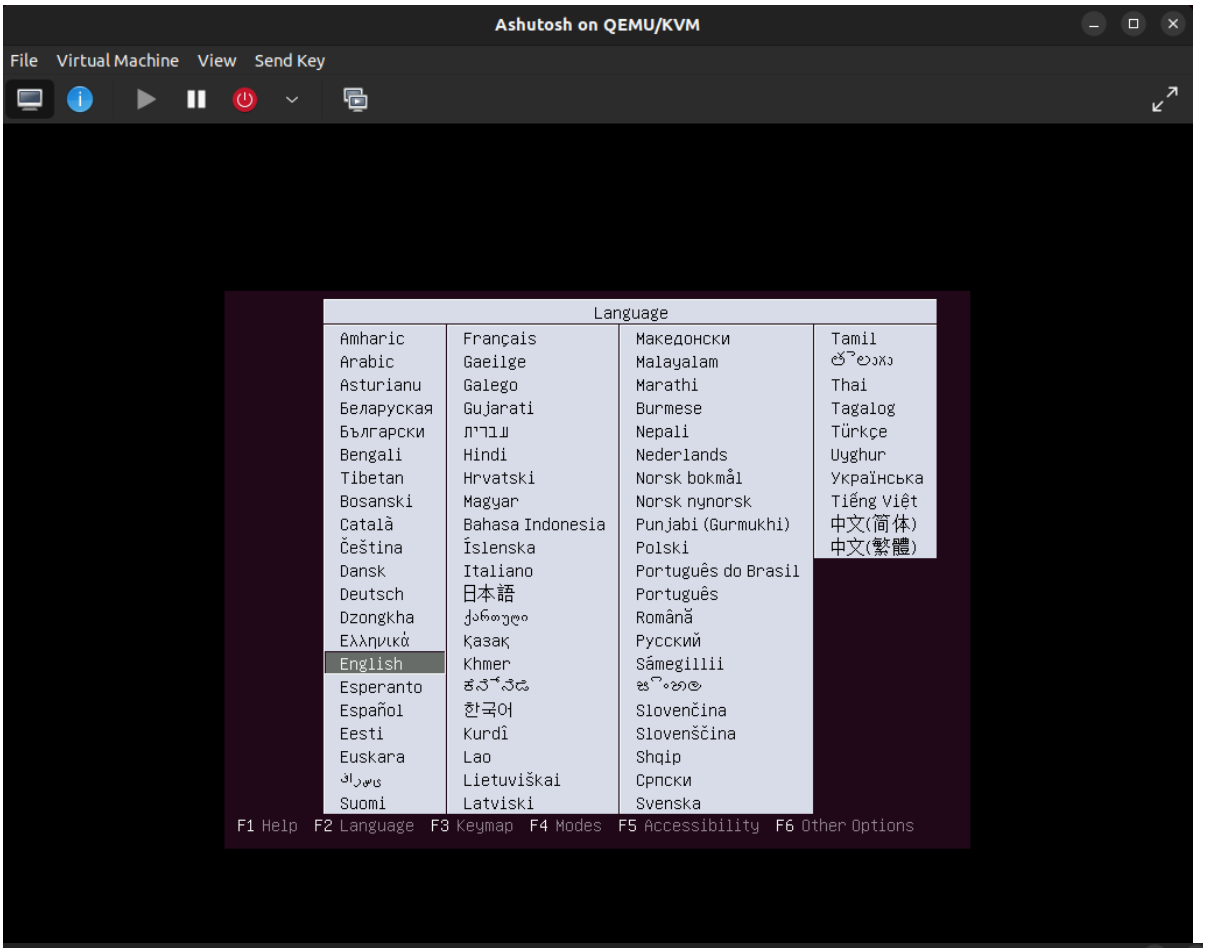
CLOUD COMPUTING JOURNAL

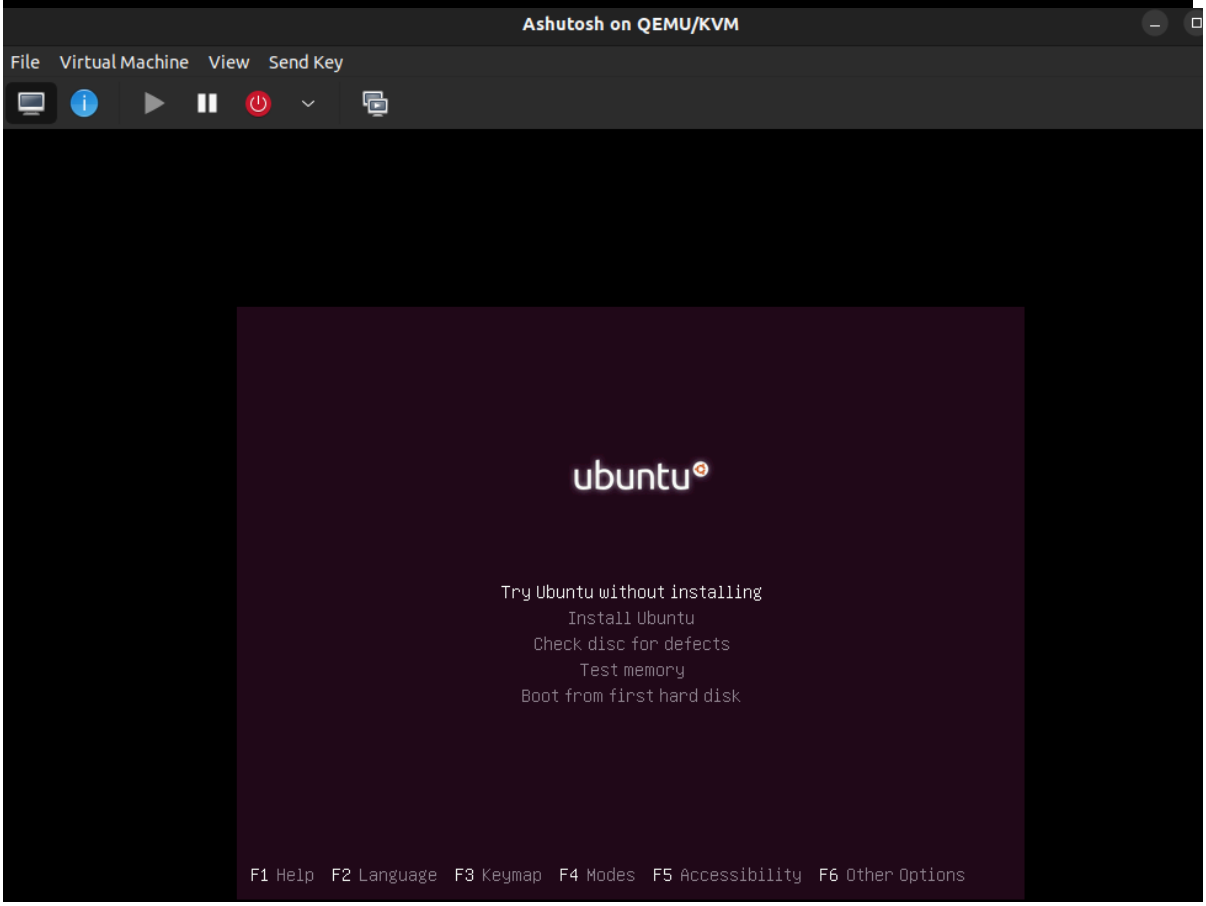


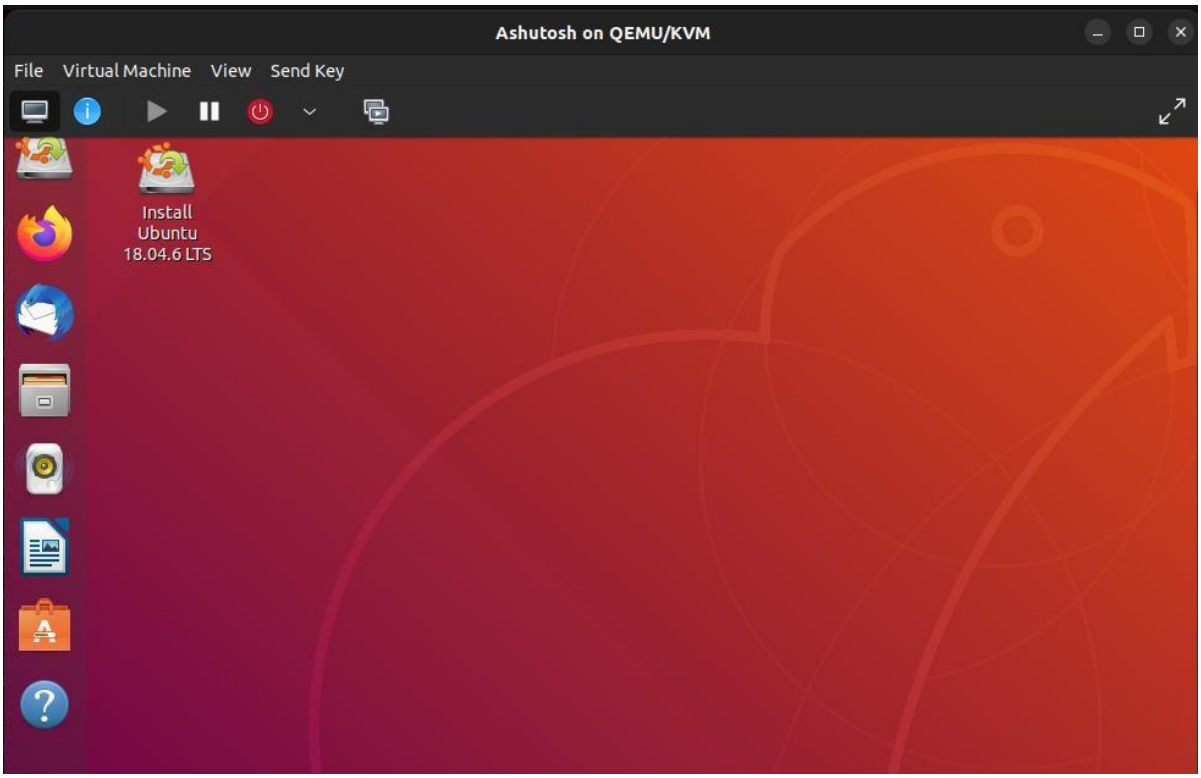

Create a new virtual machine
Step 4 of 5
Enable storage for this virtual machine
Create a disk image for the virtual machine
15.0
GiB
427.1 GiB available in the default location
Select or create custom storage
Manage...
Cancel
Back
Forward


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

CLOUD COMPUTING JOURNAL

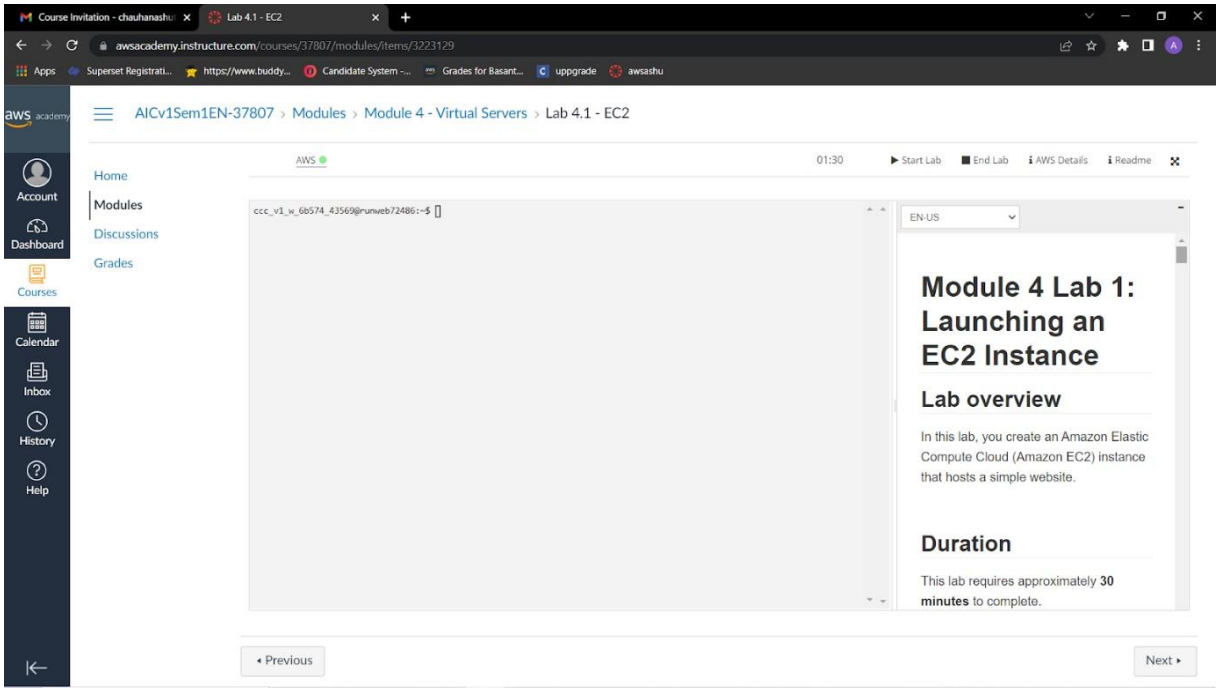




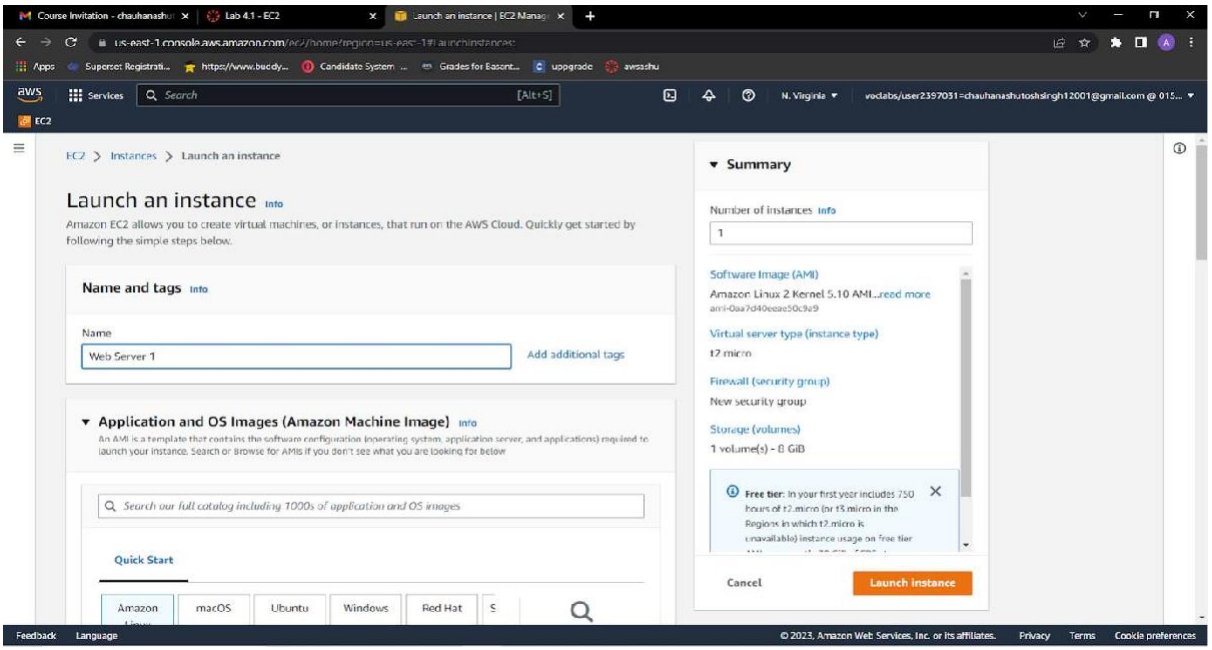


D. GCP/AWS/IBM/Azure/…

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

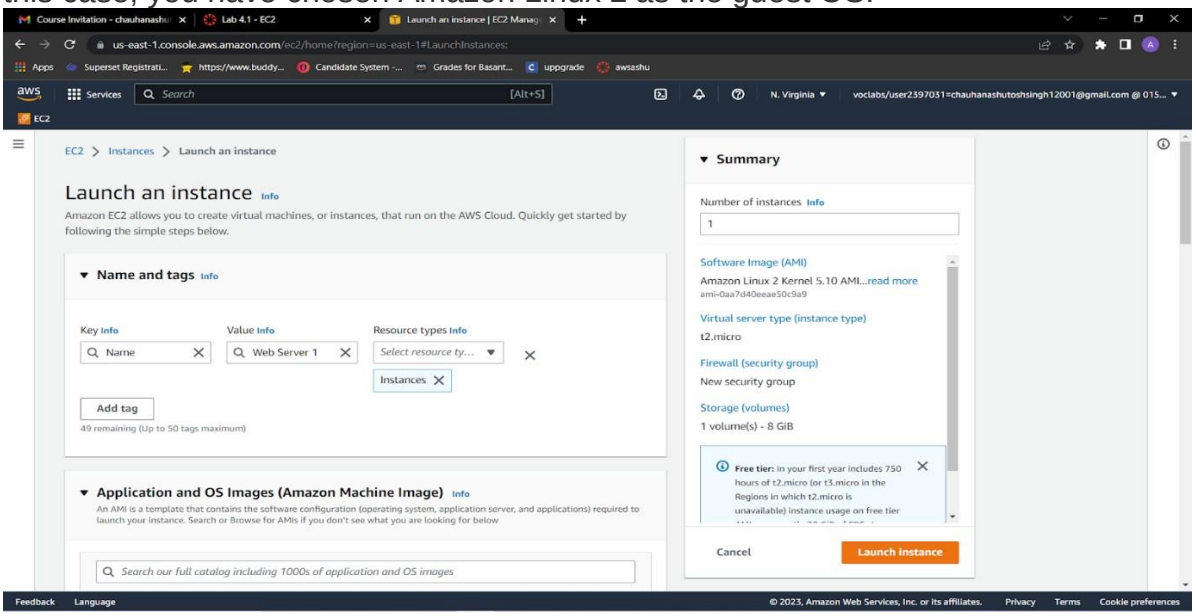


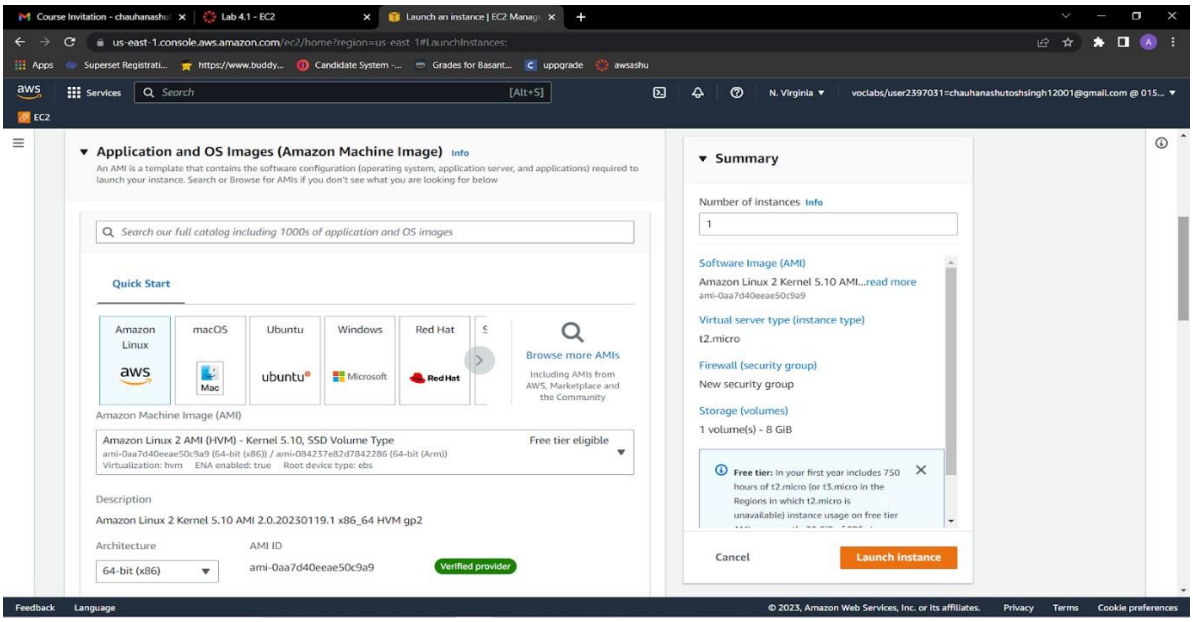
2.Choose the **Launch instance** button in the middle of the page, and then select **Launch instance** from the dropdown menu.
3.Give it the name Web Server 1



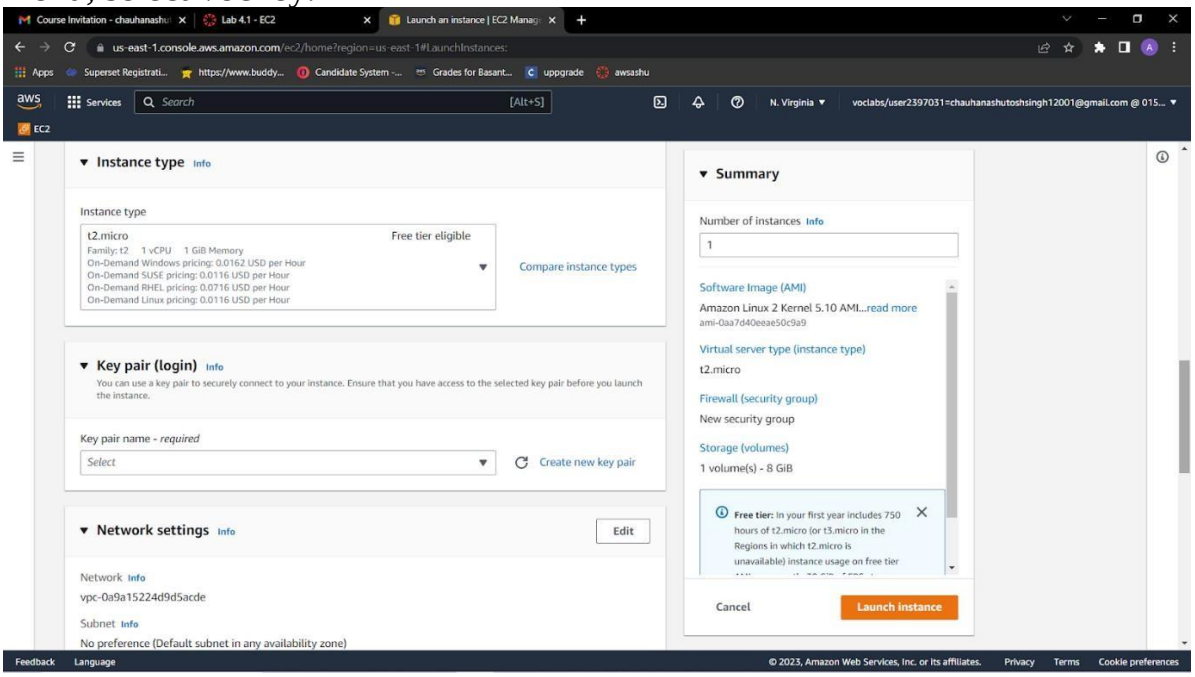
4. Choose an AMI from which to create the instance:

- 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.

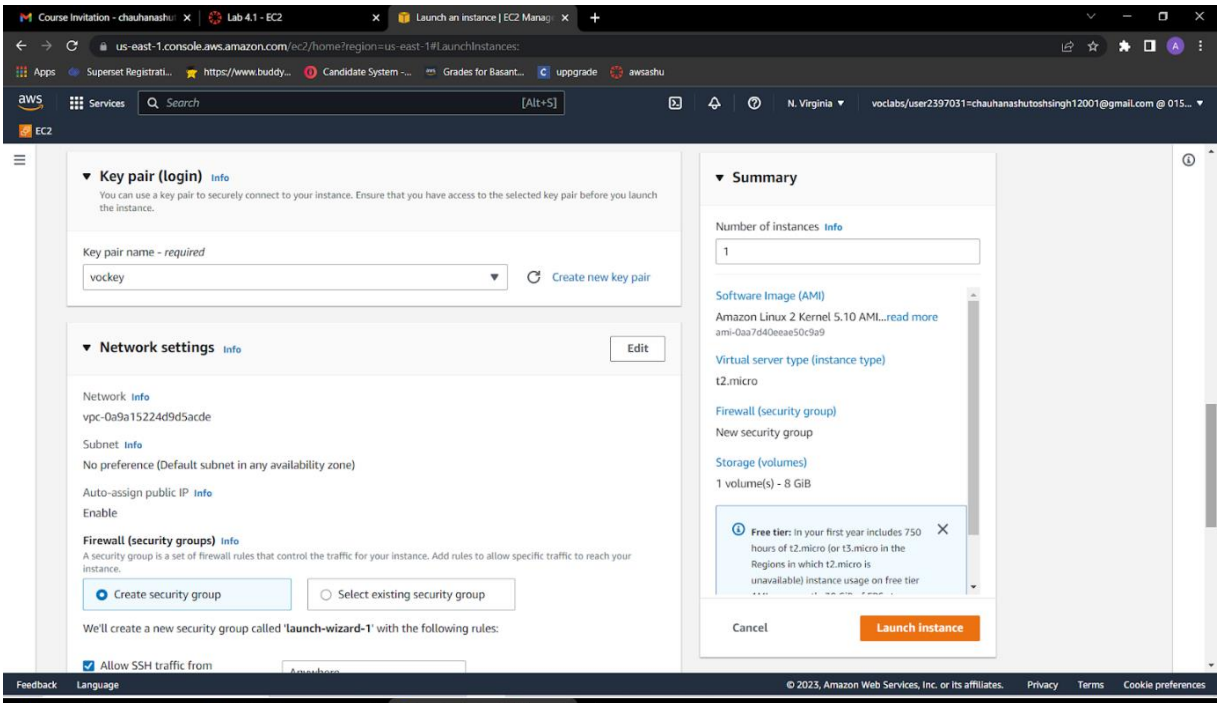


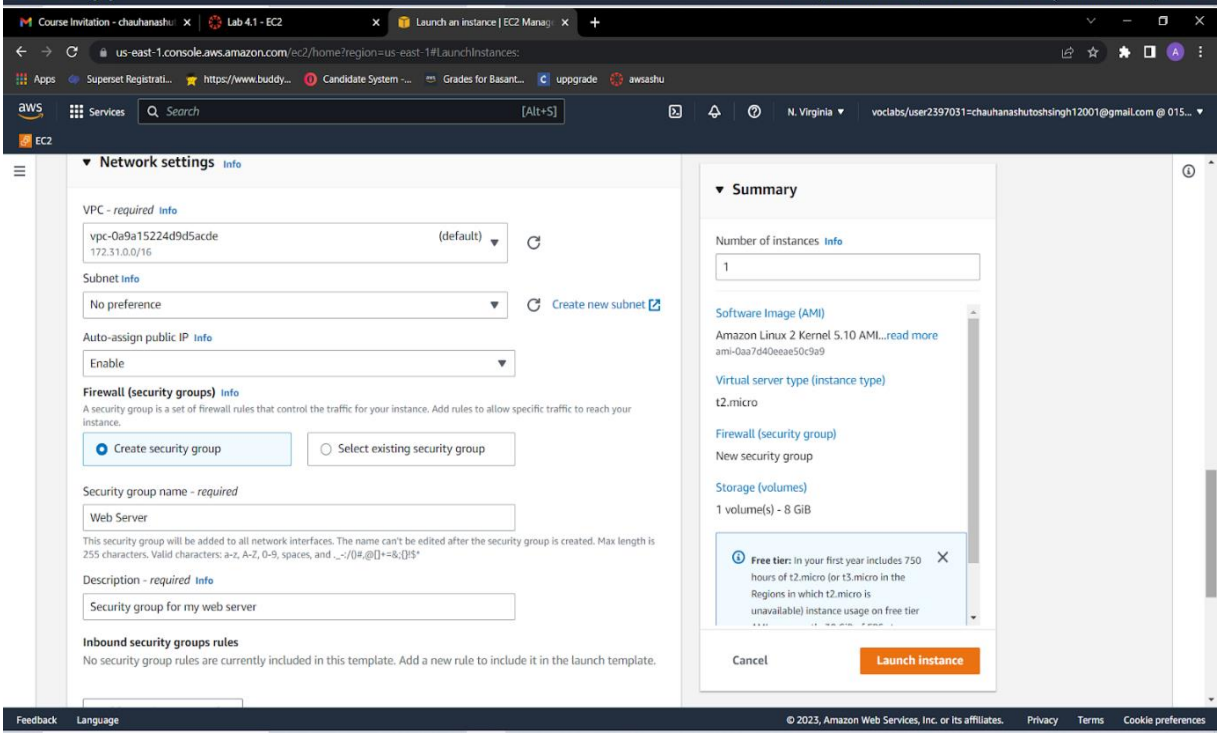


5. In the *Instance type* panel, keep the default t2.micro selected.
6. Select the key pair to associate with the instance From the Key pair name menu, select vockey.



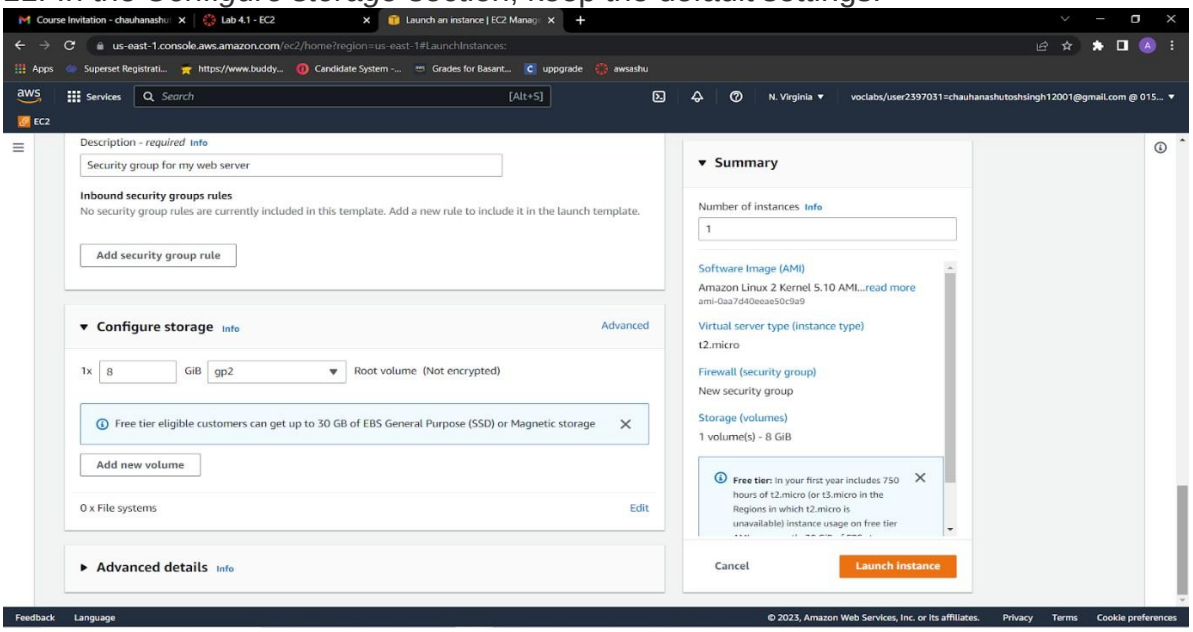
7. Next to Network settings, choose **Edit**.
8. Keep the default *VPC* and *subnet* settings. Also keep the **Auto-assign public IP** setting set to **Enable**.
9. Under *Firewall (security groups)*, keep the default **Create security group** option chosen.





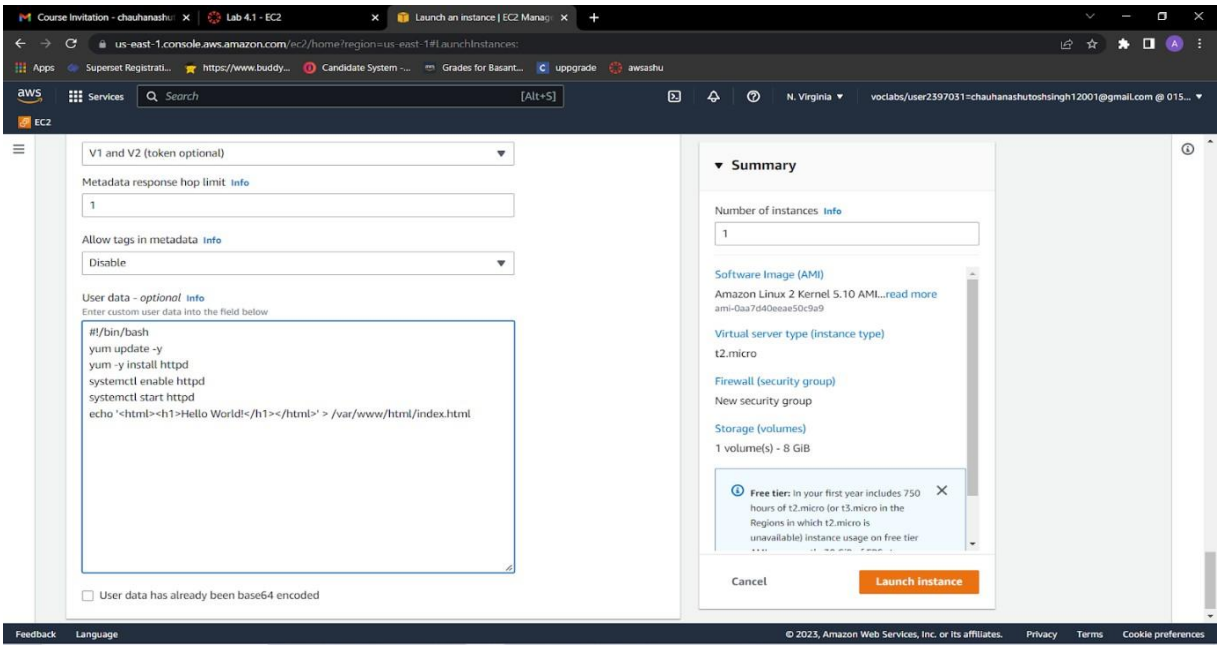
10. Configure a new security group:
    - Keep the default selection **Create a new security group**.
    - **Security group name:** Clear the text and enter Web Server
    - **Description:** Clear the text and enter Security group for my web server
    - Choose **Remove** to remove the default SSH inbound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

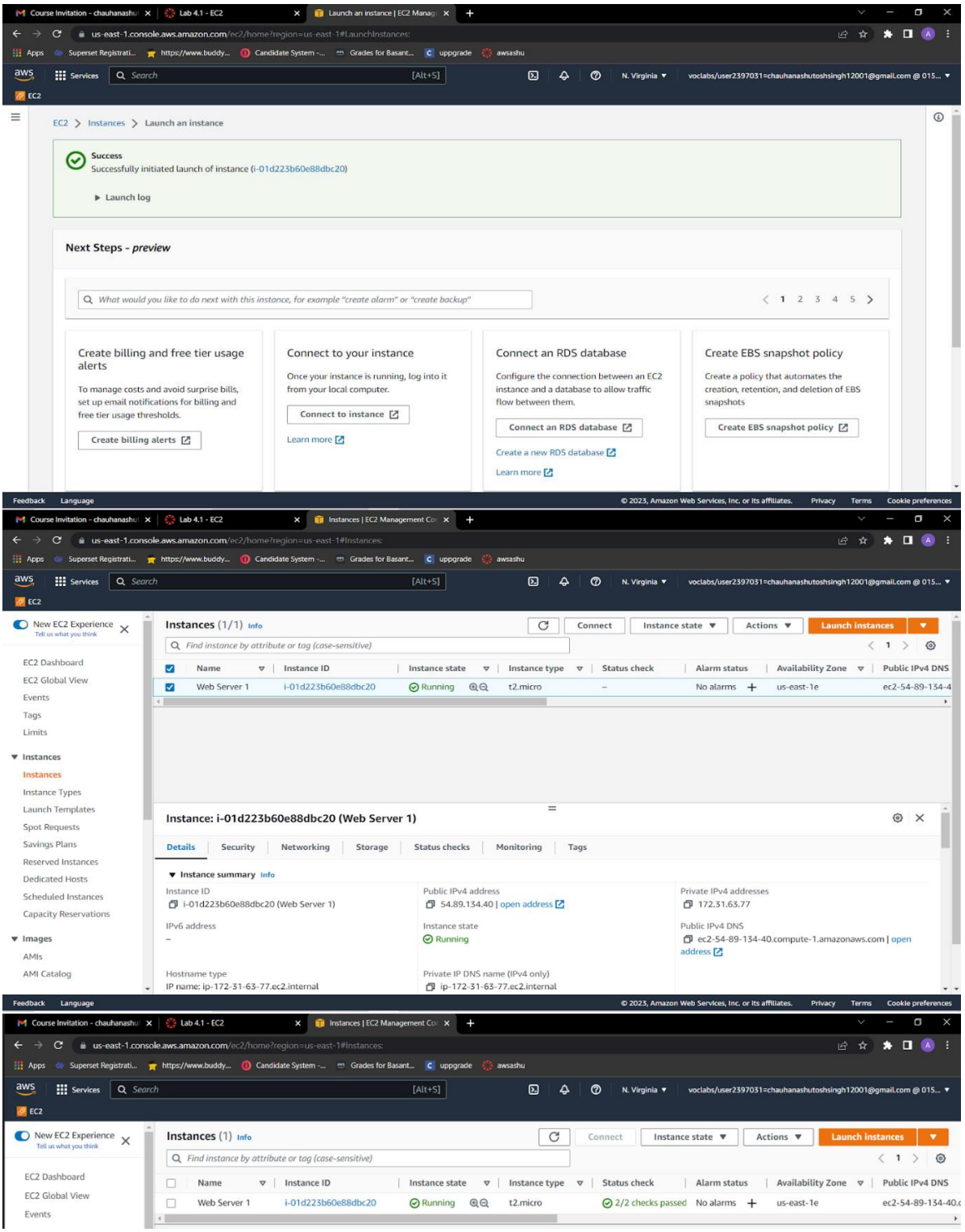


13. At the bottom of the **Summary** panel on the right side of the screen choose **Launch instance** You will see a Success message.

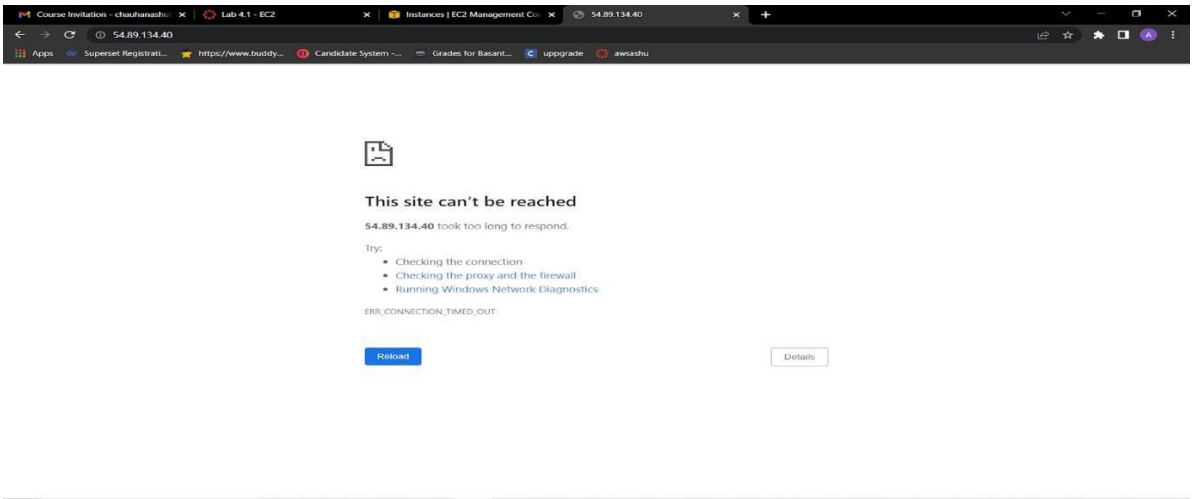
14. Go to **View all instances**

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

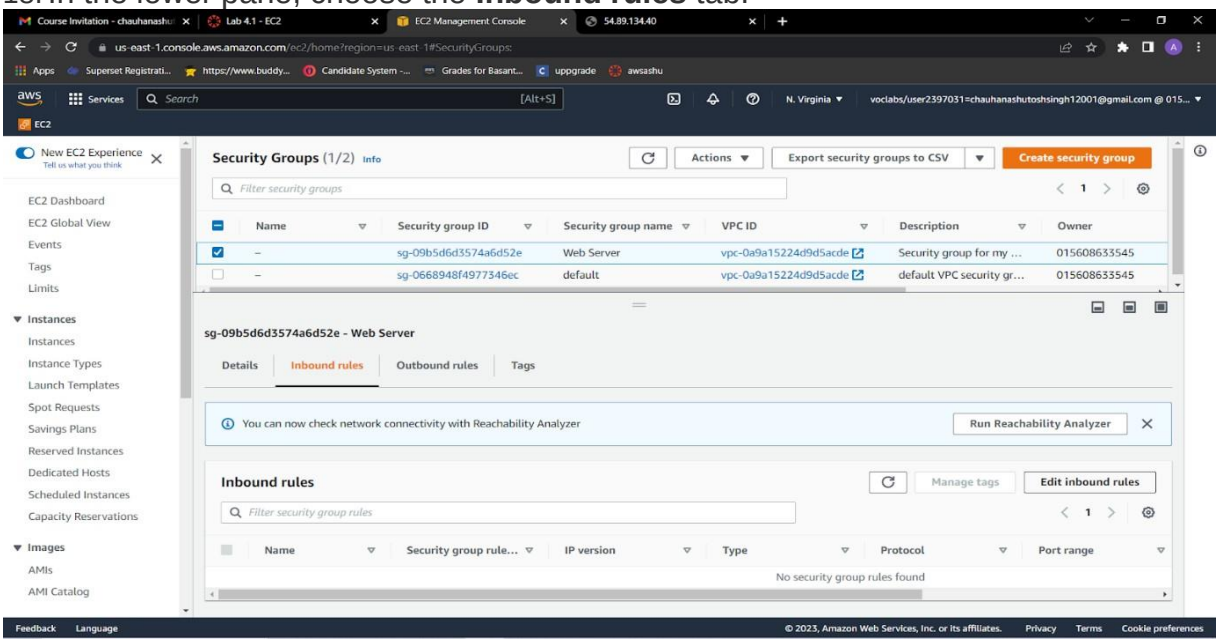
- **Instance state:** *Running*
- **Status check:** *2/2 checks passed*



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.



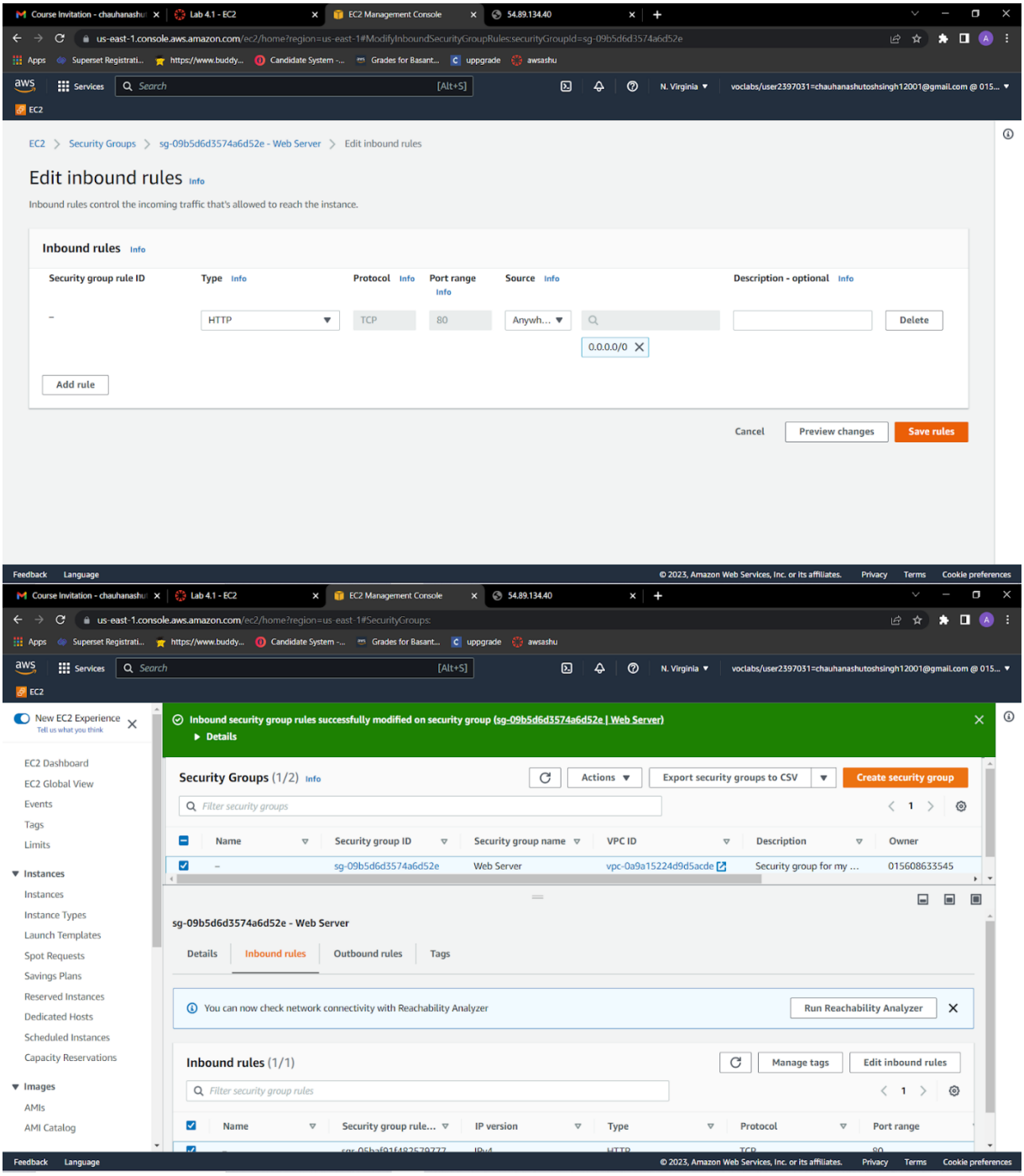
15. Return to the **EC2 Management Console** browser tab.
16. In the left navigation pane, under **Network & Security**, choose **Security Groups**.
17. Select the **Web Server** security group, which you created when launching your EC2 instance.
18. In the lower pane, choose the **Inbound rules** tab.



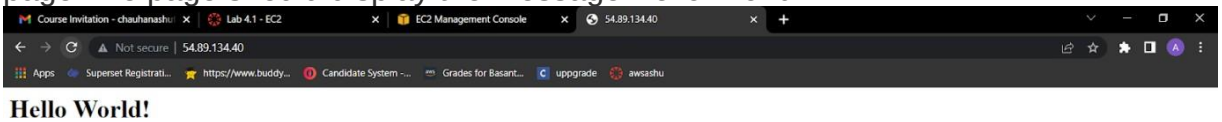
19. Choose **Edit inbound rules**, and then choose **Add rule**.Configure the following:

- **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!*



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

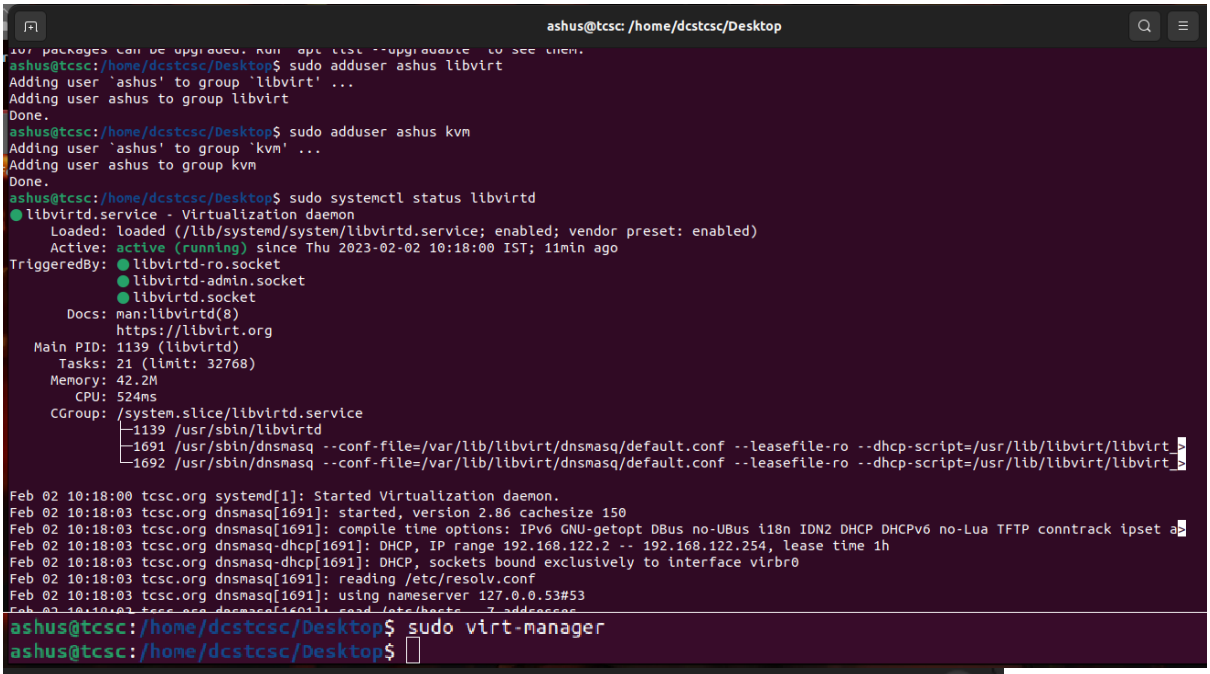
PaaS providers provide various databases such as ClearDB, PostgreSQL, MongoDB, and Redis to communicate with the applications.

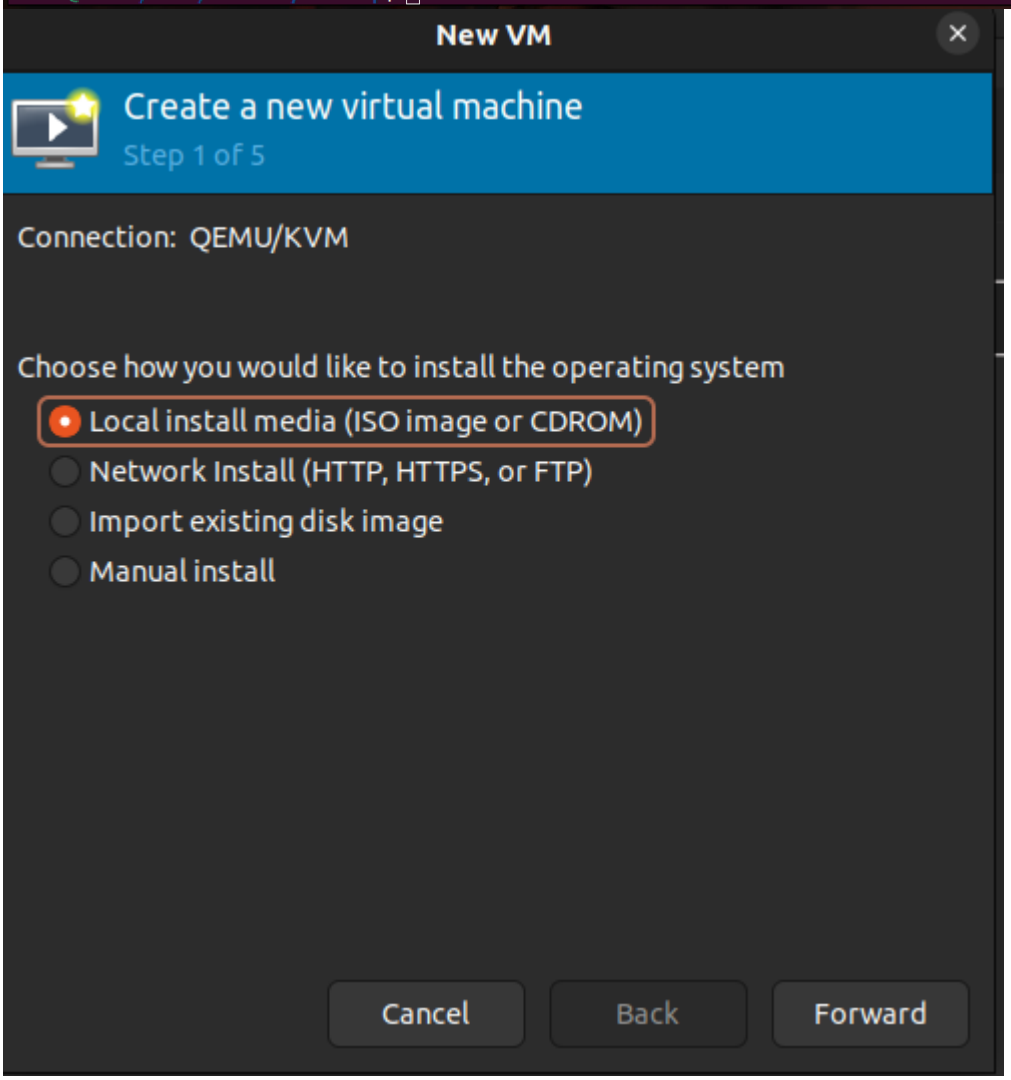
4. Other tools

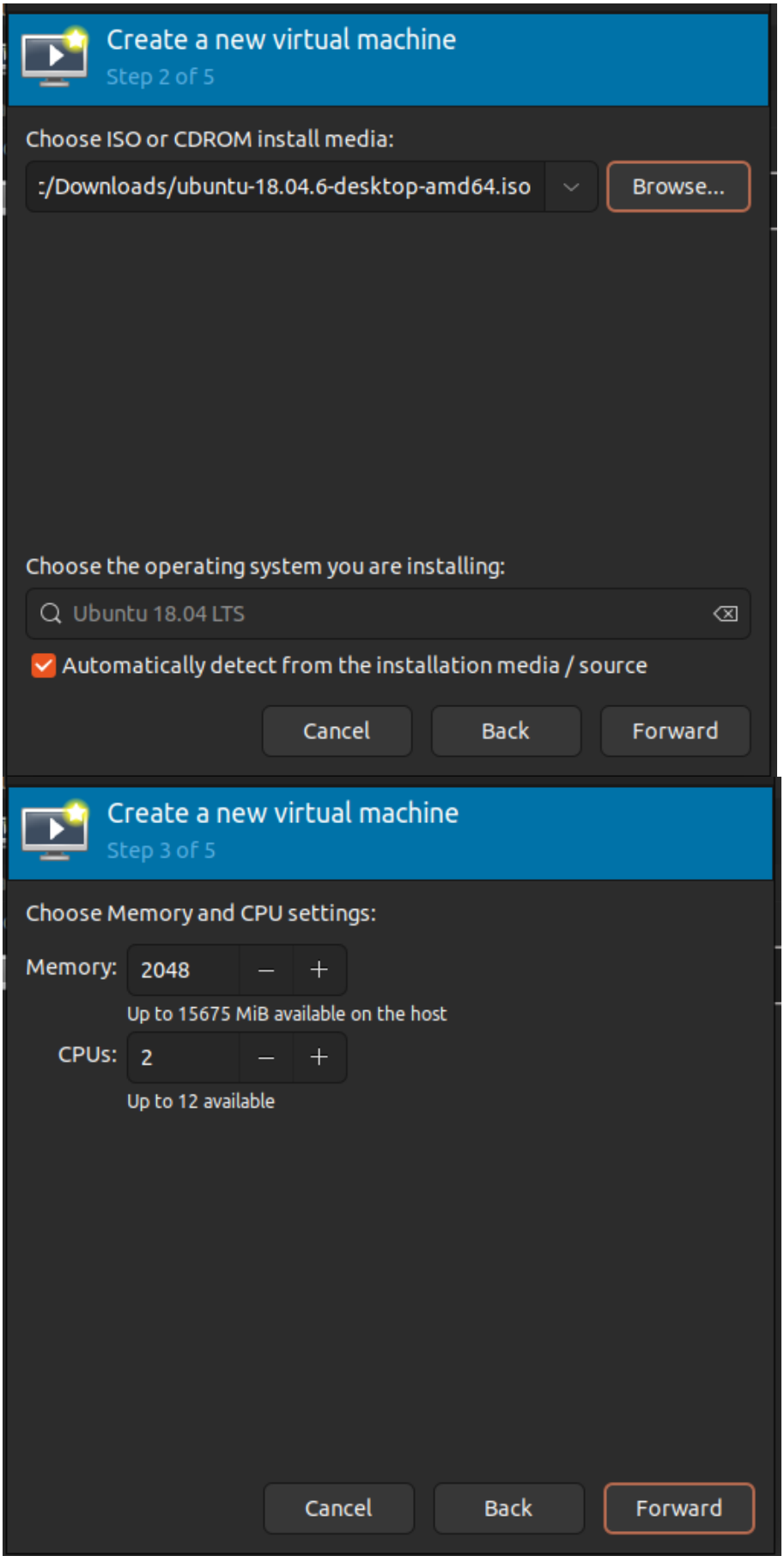
PaaS providers provide various other tools that are required to develop, test, and deploy the applications.

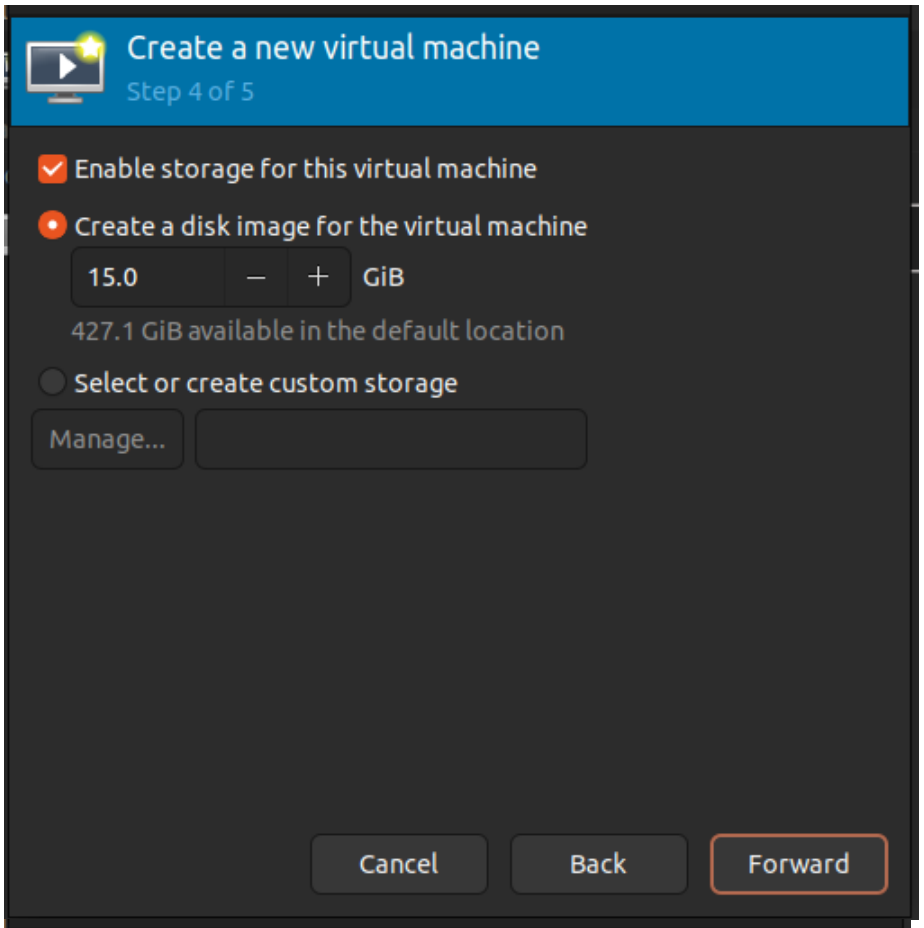
Method and Steps:

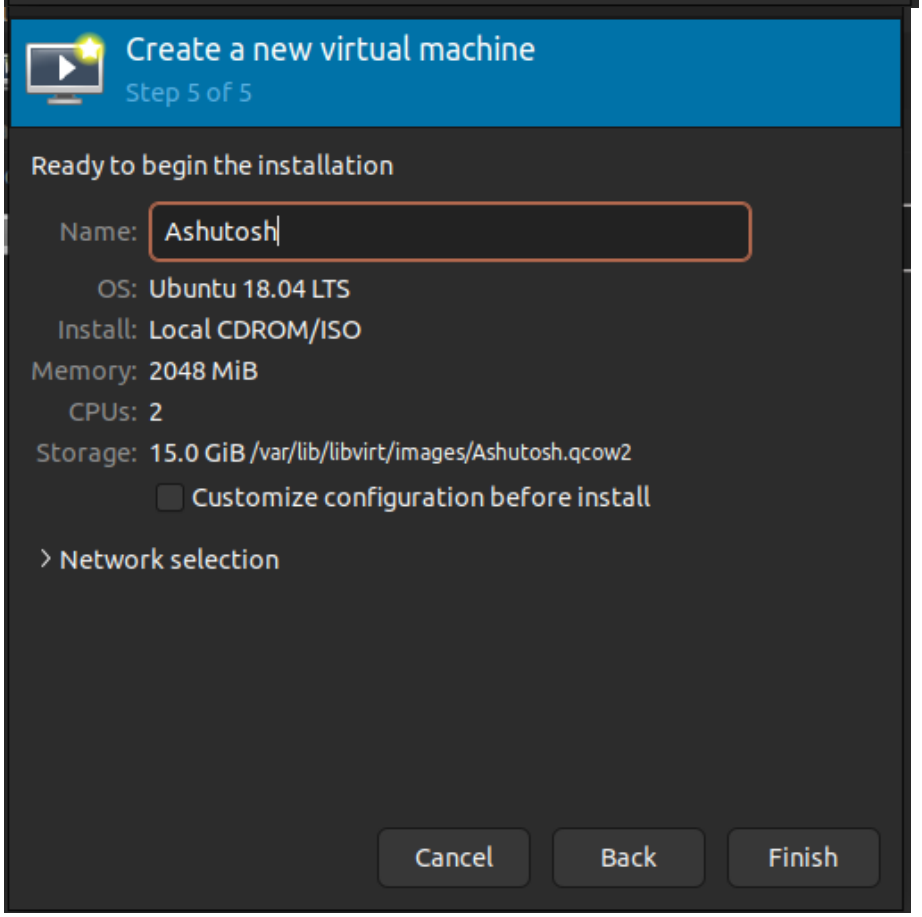
A. Using KVM.

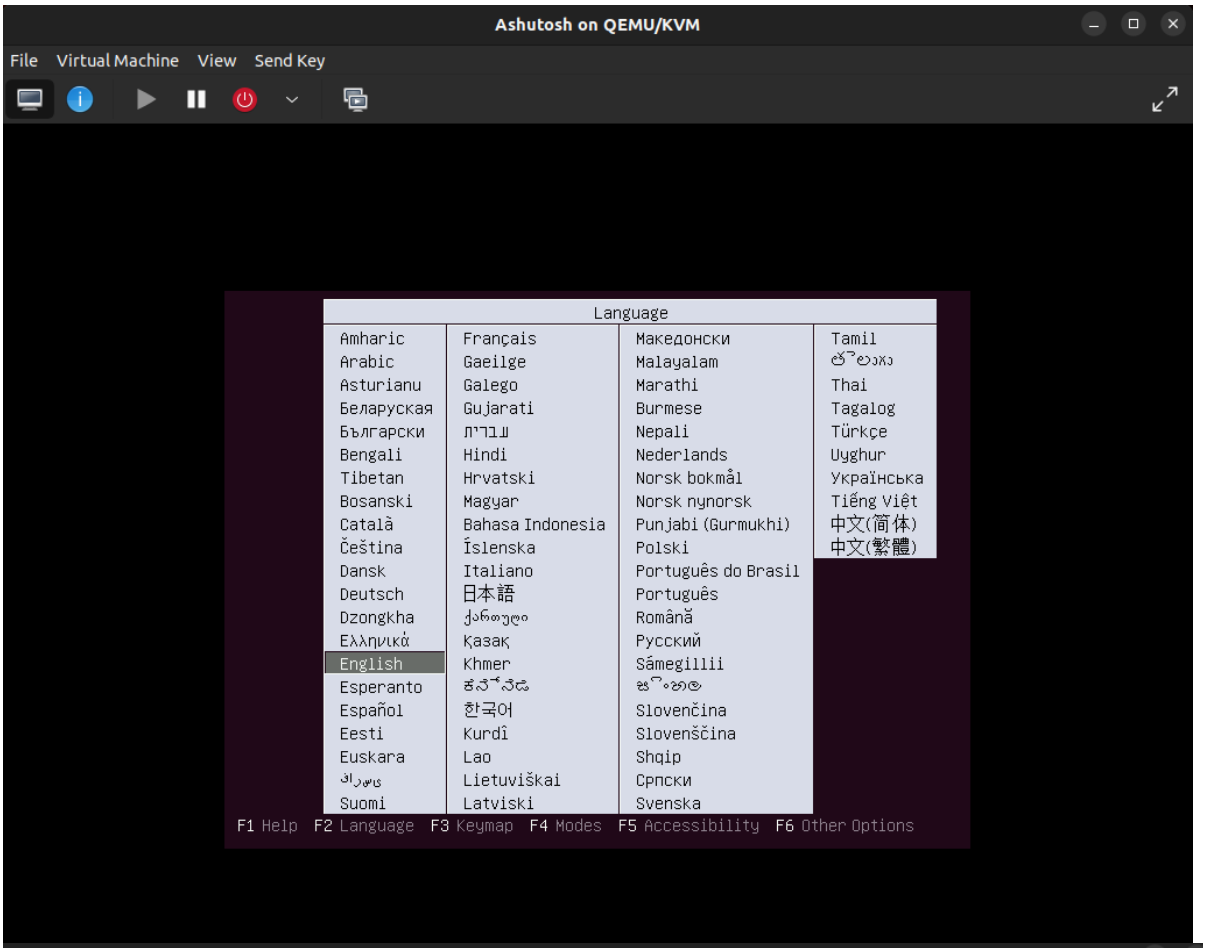


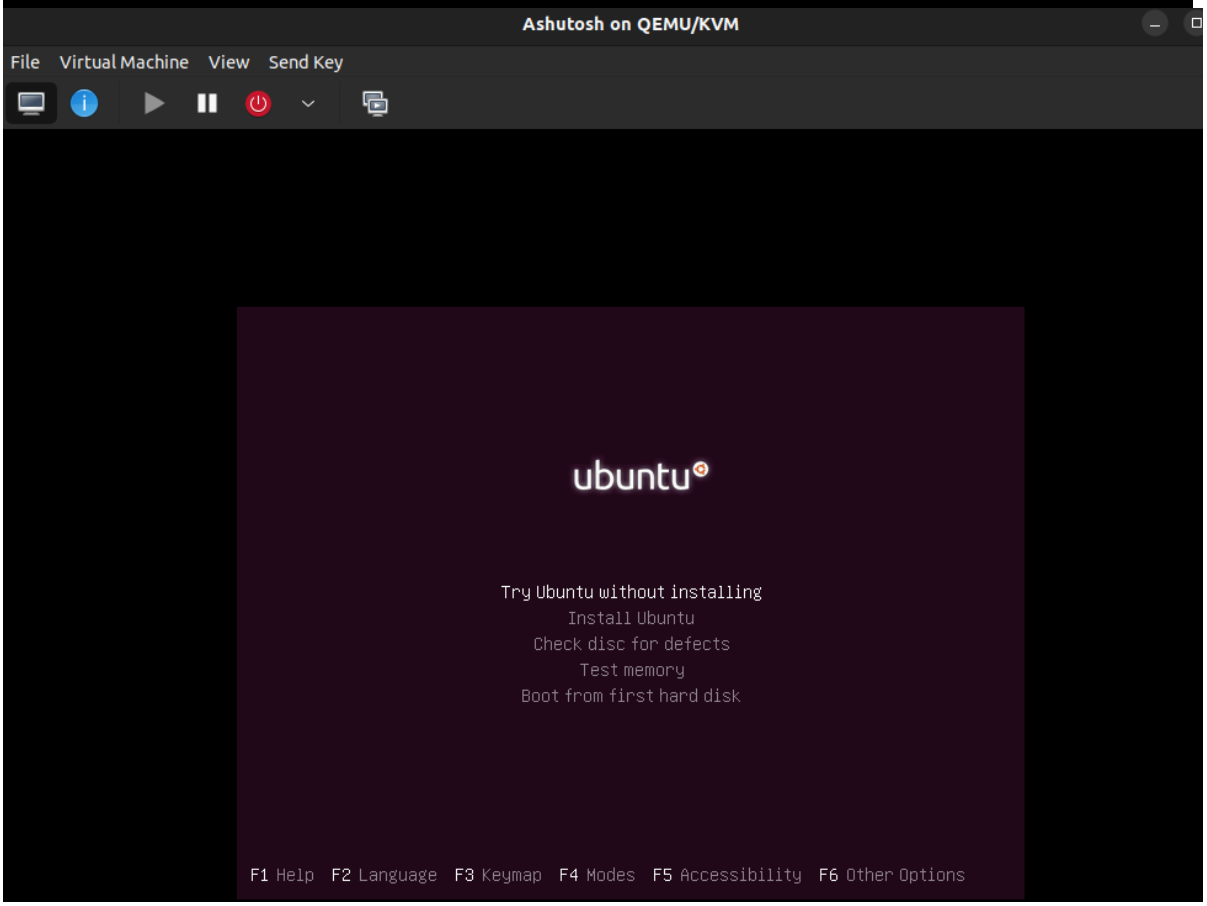


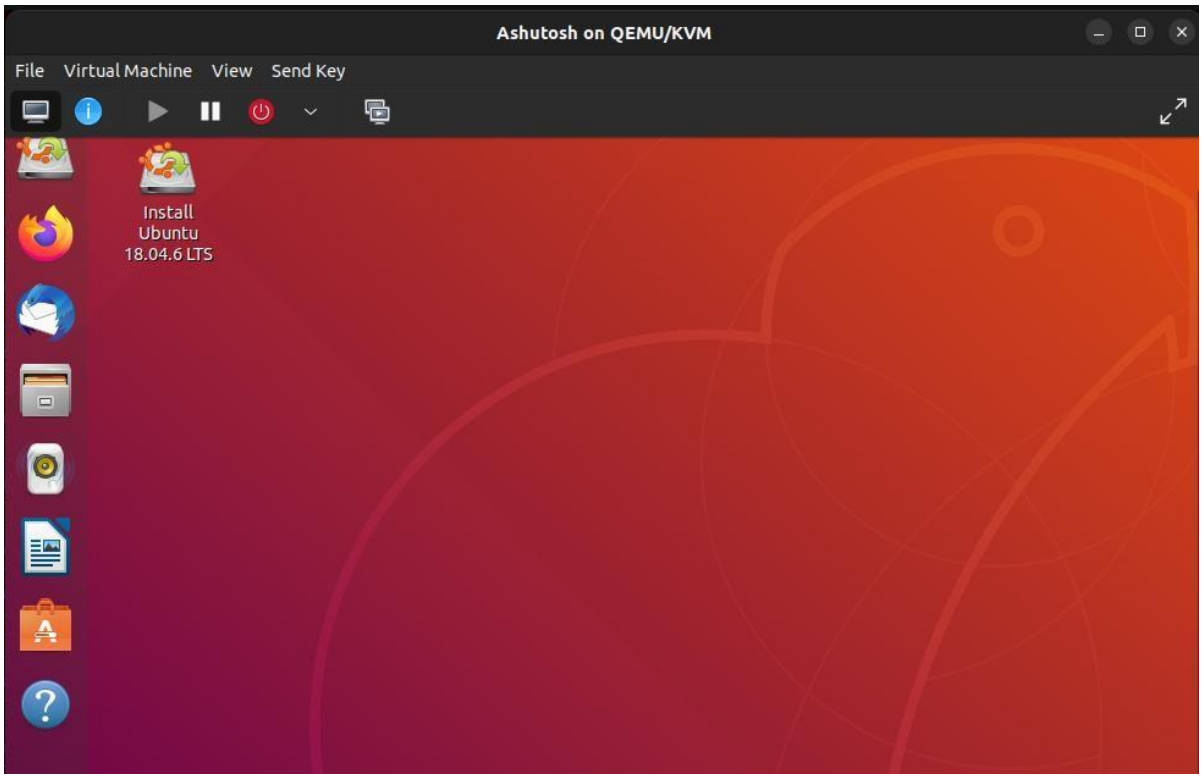

Create a new virtual machine
Step 2 of 5
Choose ISO or CDROM install media:
:/Downloads/ubuntu-18.04.6-desktop-amd64.iso
Browse...
Choose the operating system you are installing:
Ubuntu 18.04 LTS
Automatically detect from the installation media / source
Cancel
Back
Forward
Create a new virtual machine
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
Cancel
Back
Forward

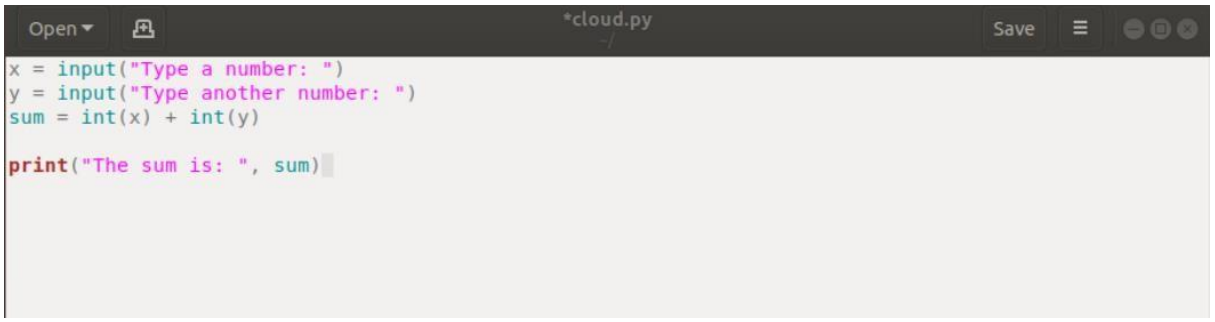

Create a new virtual machine
Step 4 of 5
Enable storage for this virtual machine
Create a disk image for the virtual machine
15.0
GiB
427.1 GiB available in the default location
Select or create custom storage
Manage...
Cancel
Back
Forward


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


Ashutosh on QEMU/KVM
File Virtual Machine View Send Key
Language
Amharic
Arabic
Asturianu
Беларуская
Български
Bengali
Tibetan
Bosanski
Català
Čeština
Dansk
Deutsch
Dzongkha
Ελληνικά
English
Esperanto
Español
Eesti
Euskara
Suomi
Français
Gaeilge
Galego
Gujarati
Hindi
Hrvatski
Magyar
Bahasa Indonesia
Íslenska
Italiano
日本語
ქართული
Қазақ
Khmer
한국어
Kurdî
Lao
Lietuviškai
Latviski
Македонски
Malayalam
Marathi
Burmese
Nepali
Nederlands
Norsk bokmål
Norsk nynorsk
Punjabi (Gurmukhi)
Polski
Português do Brasil
Português
Română
Русский
Sámegillii
Slovenčina
Slovenščina
Shqip
Српски
Svenska
Tamil
Thai
Tagalog
Türkçe
Uyghur
Українська
Tiếng Việt
中文(简体)
中文(繁體)
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options


Ashutosh on QEMU/KVM
File Virtual Machine View Send Key
ubuntu
Try Ubuntu without installing
Install Ubuntu
Check disc for defects
Test memory
Boot from first hard disk
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options





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**.

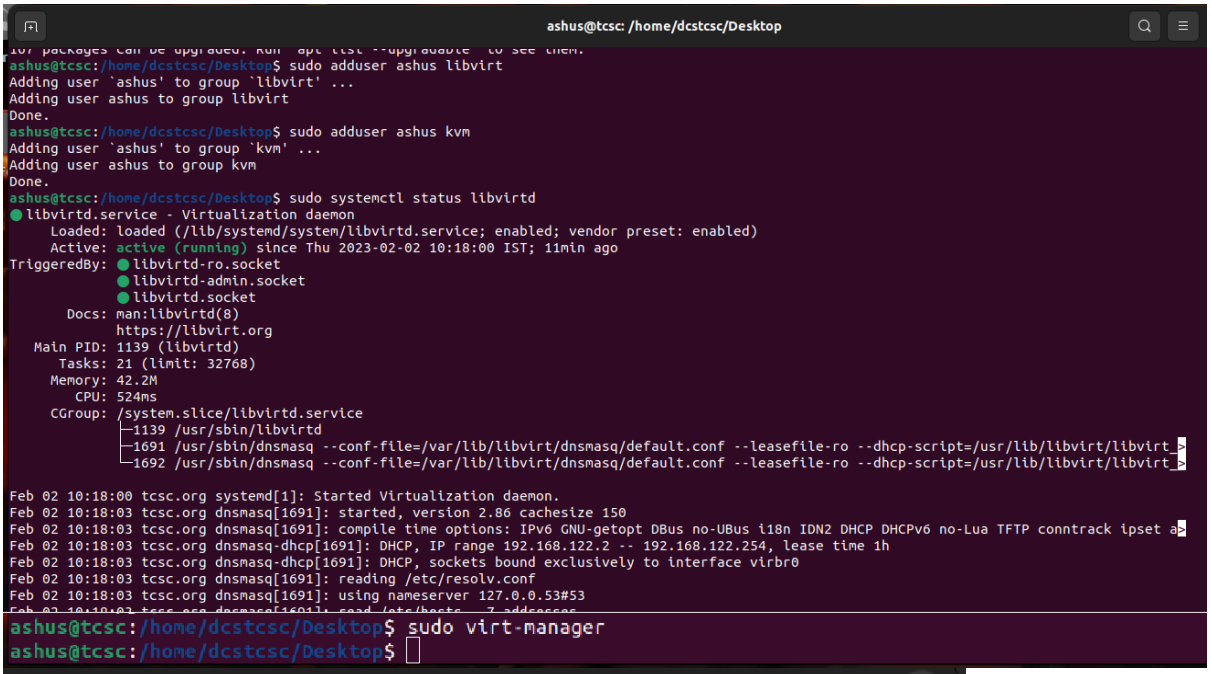
Document Management - SaaS document management is a software application offered by a third party (SaaS providers) to create, manage, and track electronic documents.**Example:** Slack, Samepage, Box, and Zoho Forms.

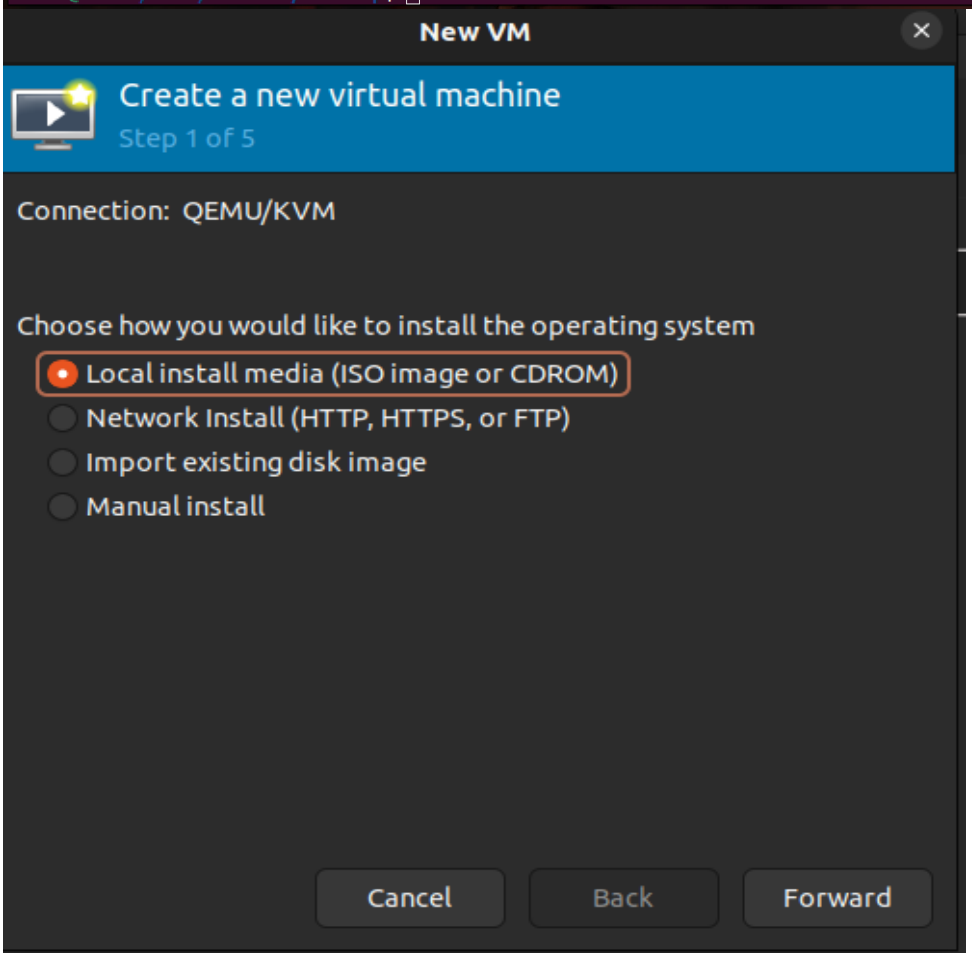
Social Networks - As we all know, social networking sites are used by the general public, so social networking service providers use SaaS for their convenience and handle the general public's information.

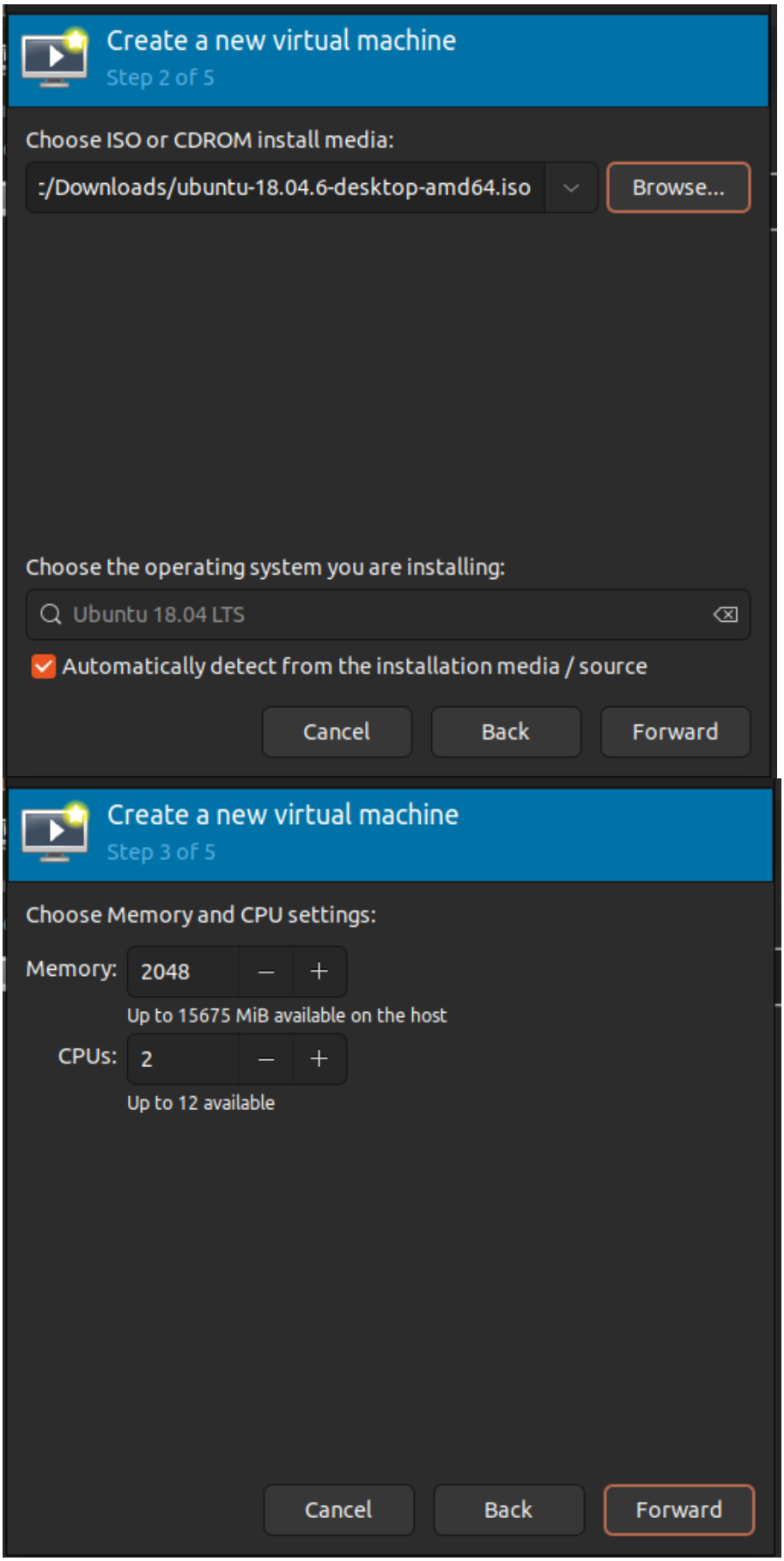
Mail Services - To handle the unpredictable number of users and load on e-mail services, many e-mail providers offering their services using SaaS.

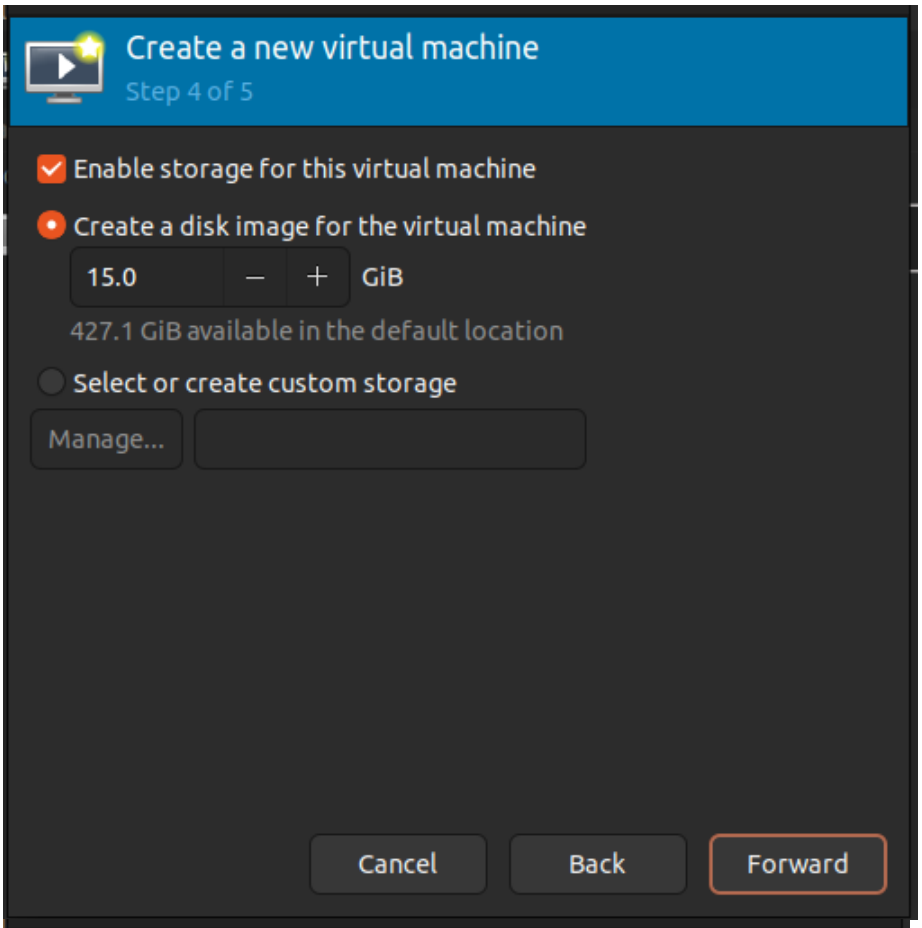
Methods and Steps:

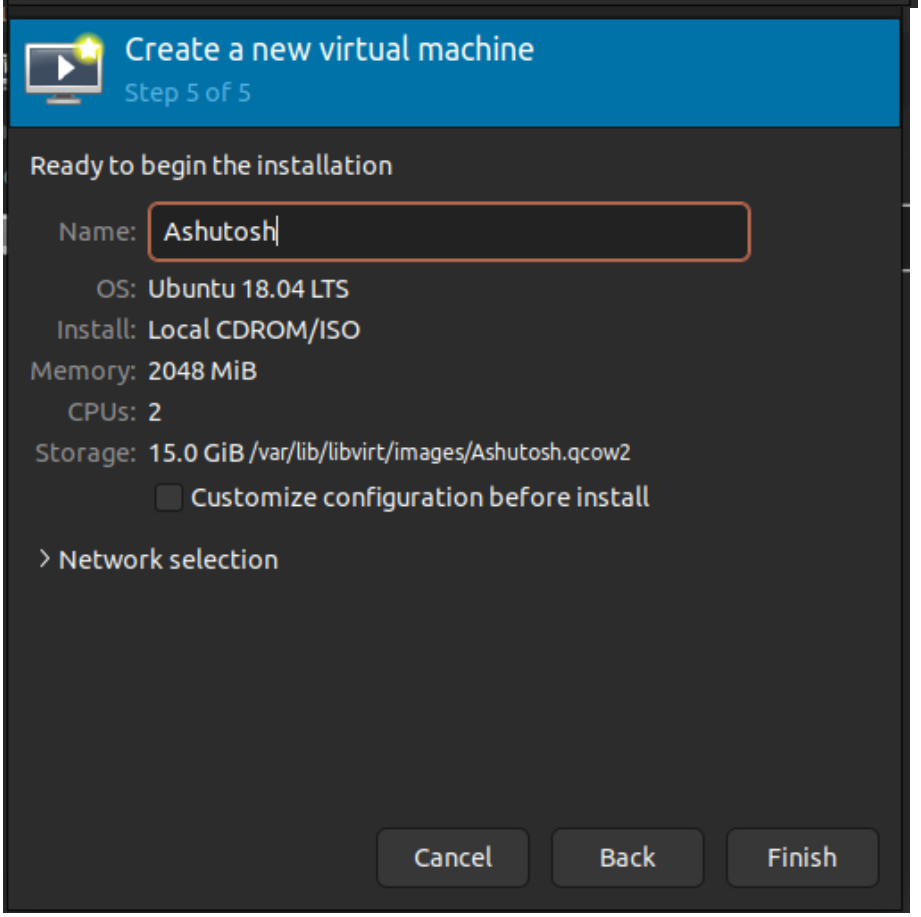
A. Using FOSS Server

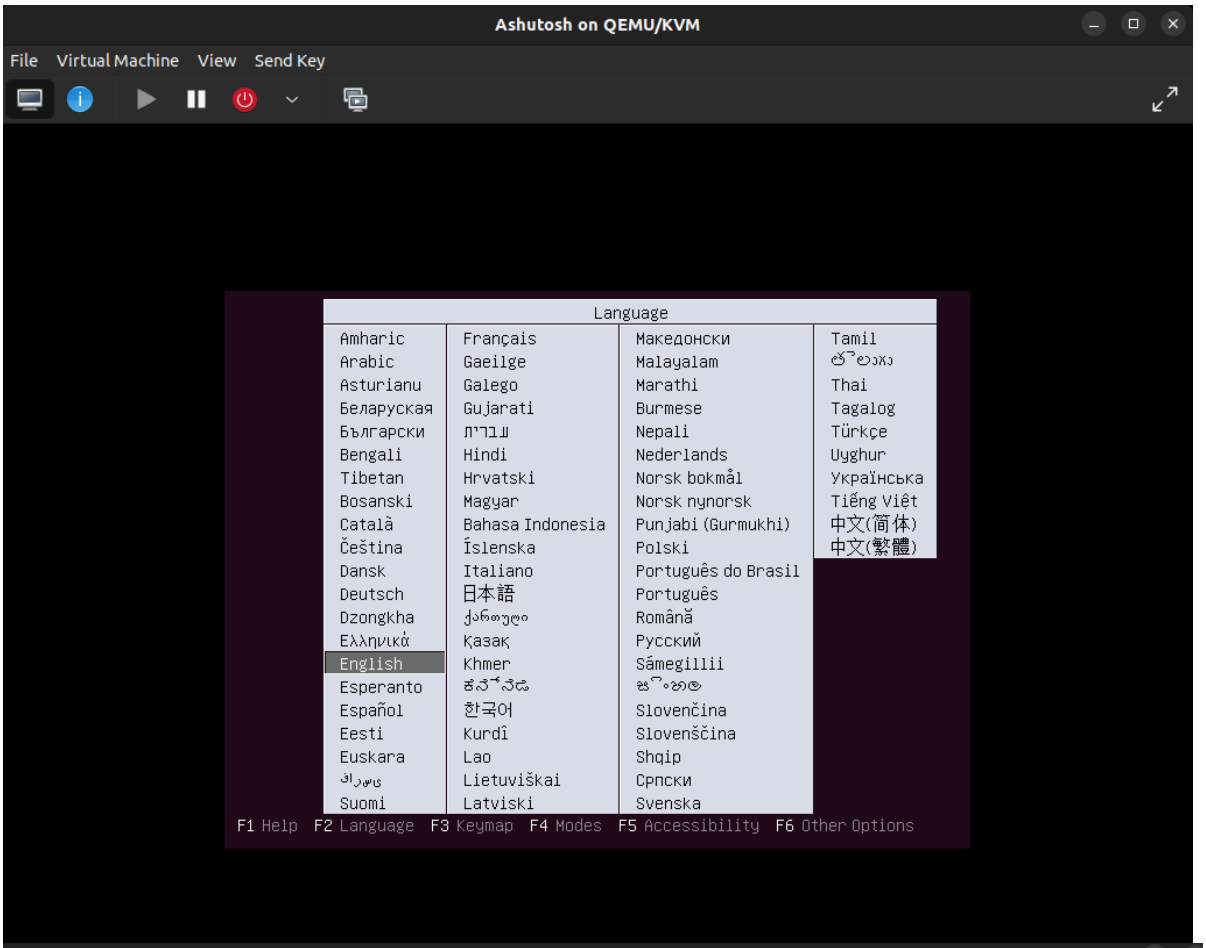


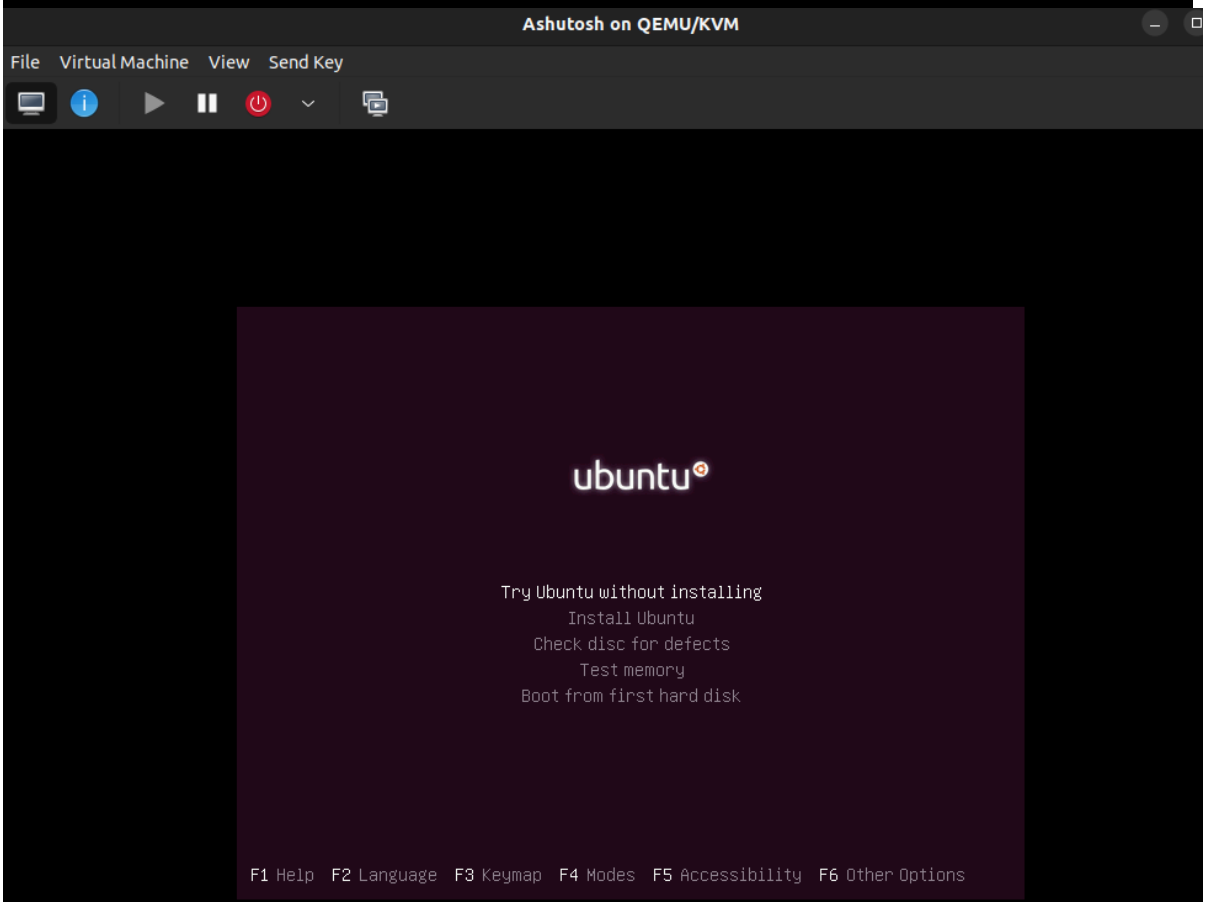



Create a new virtual machine
Step 2 of 5
Choose ISO or CDROM install media:
:/Downloads/ubuntu-18.04.6-desktop-amd64.iso
Browse...
Choose the operating system you are installing:
Ubuntu 18.04 LTS
Automatically detect from the installation media / source
Cancel
Back
Forward
Create a new virtual machine
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
Cancel
Back
Forward

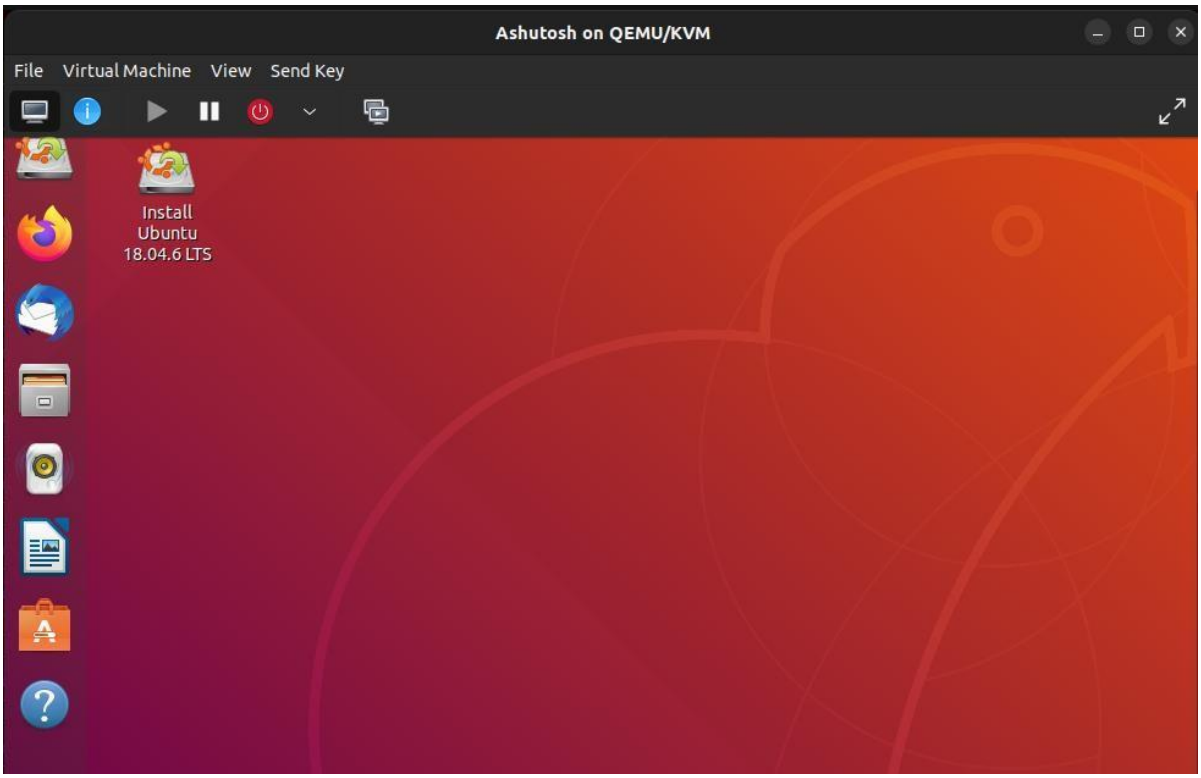

Create a new virtual machine
Step 4 of 5
Enable storage for this virtual machine
Create a disk image for the virtual machine
15.0
GiB
427.1 GiB available in the default location
Select or create custom storage
Manage...
Cancel
Back
Forward

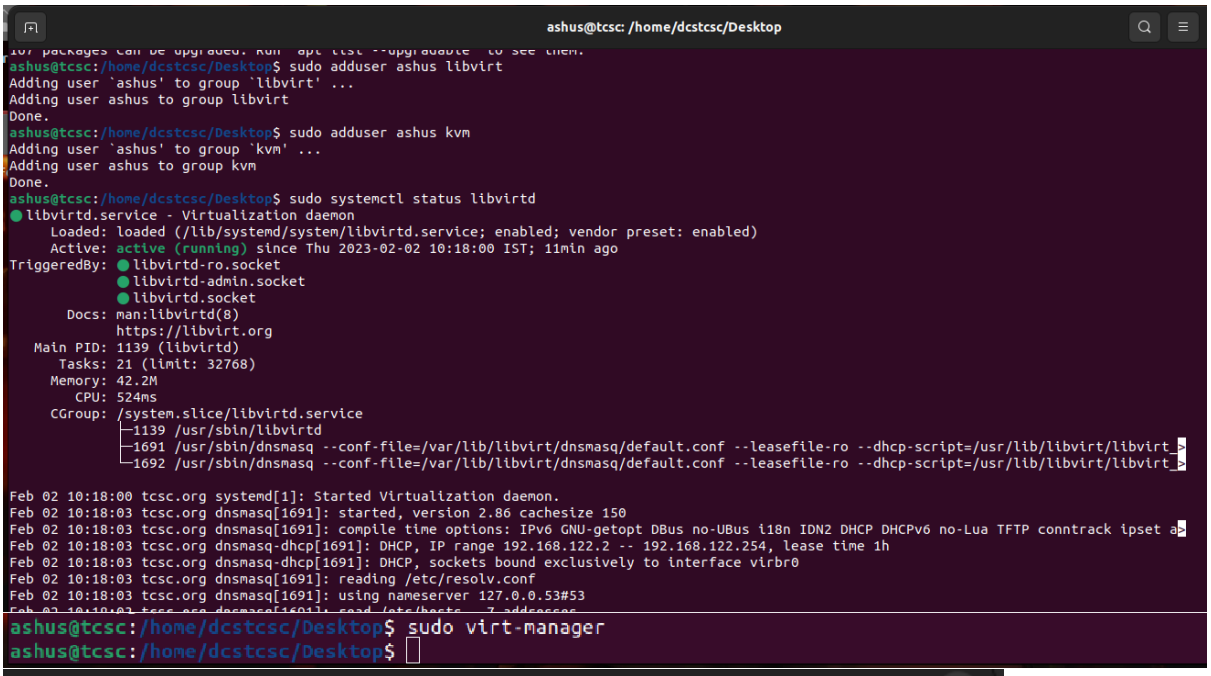

Create a new virtual machine
Step 5 of 5
Ready to begin the installation
Name: Ashutosh
OS: Ubuntu 18.04 LTS
Install: Local CDROM/ISO
Memory: 2048 MiB
CPUs: 2
Storage: 15.0 GiB /var/lib/libvirt/images/Ashutosh.qcow2
Customize configuration before install
Network selection
Cancel
Back
Finish

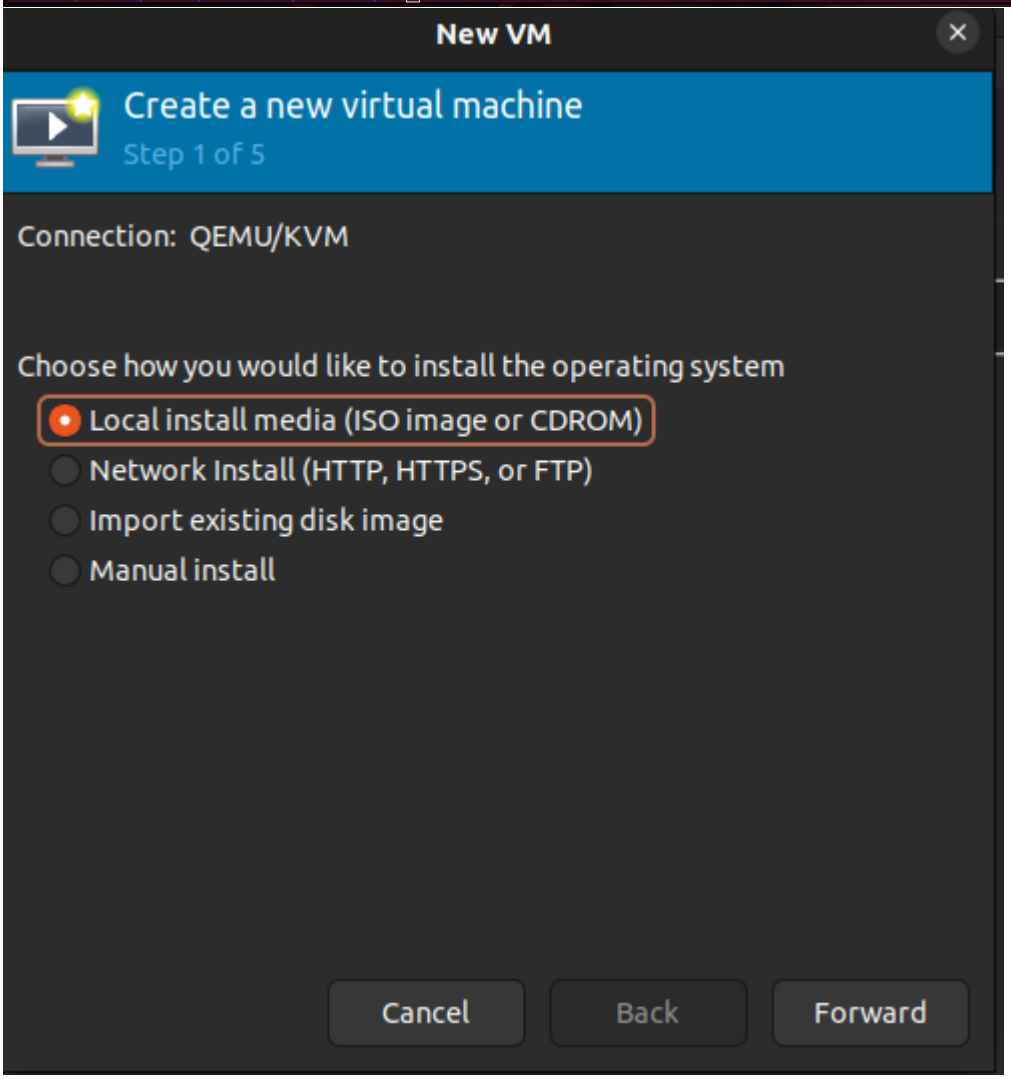

Ashutosh on QEMU/KVM
File Virtual Machine View Send Key
Language
Amharic
Arabic
Asturianu
Беларуская
Български
Bengali
Tibetan
Bosanski
Català
Čeština
Dansk
Deutsch
Dzongkha
Ελληνικά
English
Esperanto
Español
Eesti
Euskara
فارسی
Suomi
Français
Gaeilge
Galego
Gujarati
עברית
Hindi
Hrvatski
Magyar
Bahasa Indonesia
Íslenska
Italiano
日本語
ქართული
Қазақ
Khmer
ಕನ್ನಡ
한국어
Kurdî
Lao
Lietuviškai
Latviski
Македонски
Malayalam
Marathi
Burmese
Nepali
Nederlands
Norsk bokmål
Norsk nynorsk
Punjabi (Gurmukhi)
Polski
Português do Brasil
Português
Română
Русский
Sámegillii
සිංහල
Slovenčina
Slovenščina
Shqip
Српски
Svenska
Tamil
తెలుగు
Thai
Tagalog
Türkçe
Uyghur
Українська
Tiếng Việt
中文(简体)
中文(繁體)
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

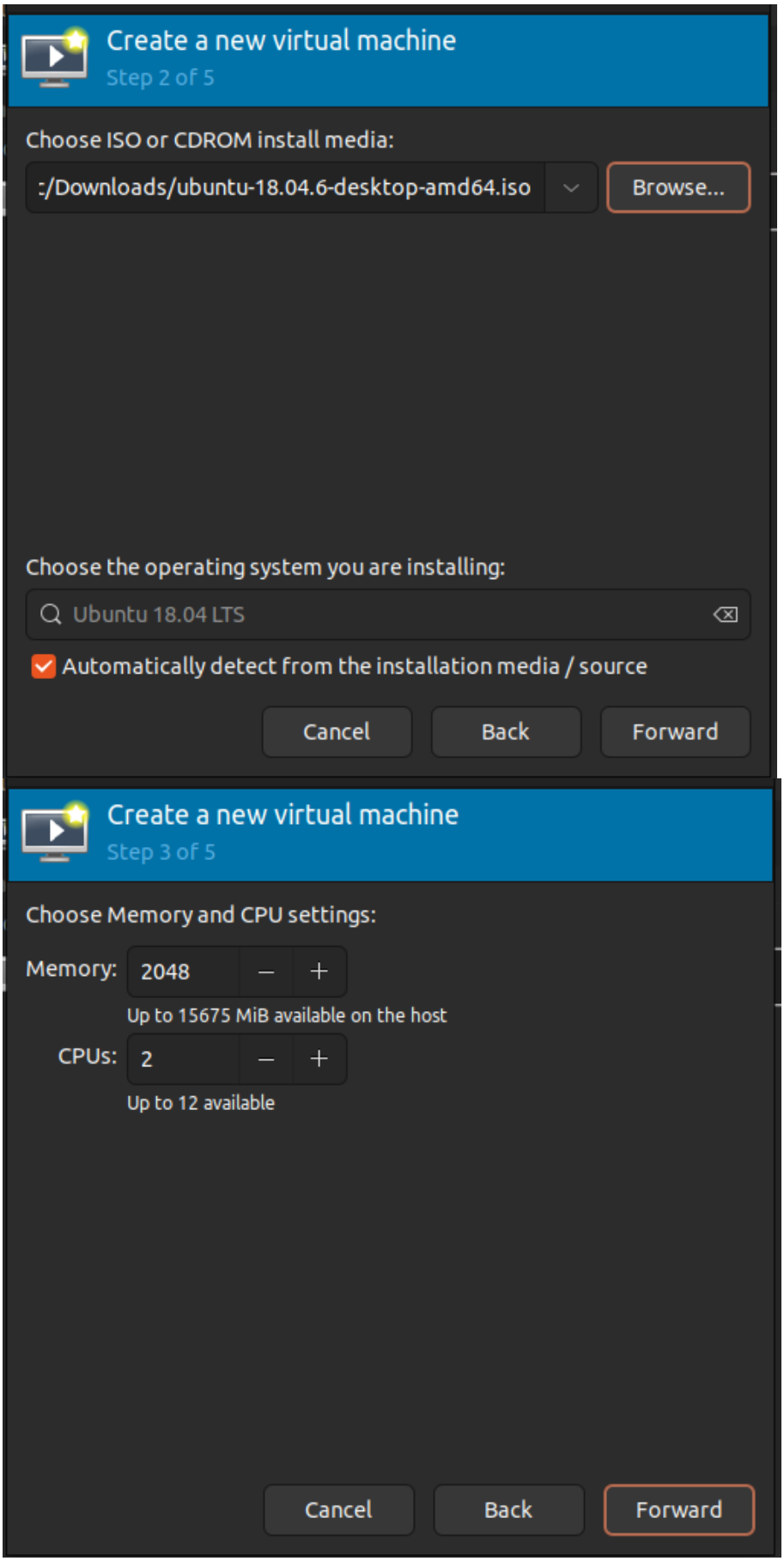

Ashutosh on QEMU/KVM
File Virtual Machine View Send Key
ubuntu
Try Ubuntu without installing
Install Ubuntu
Check disc for defects
Test memory
Boot from first hard disk
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

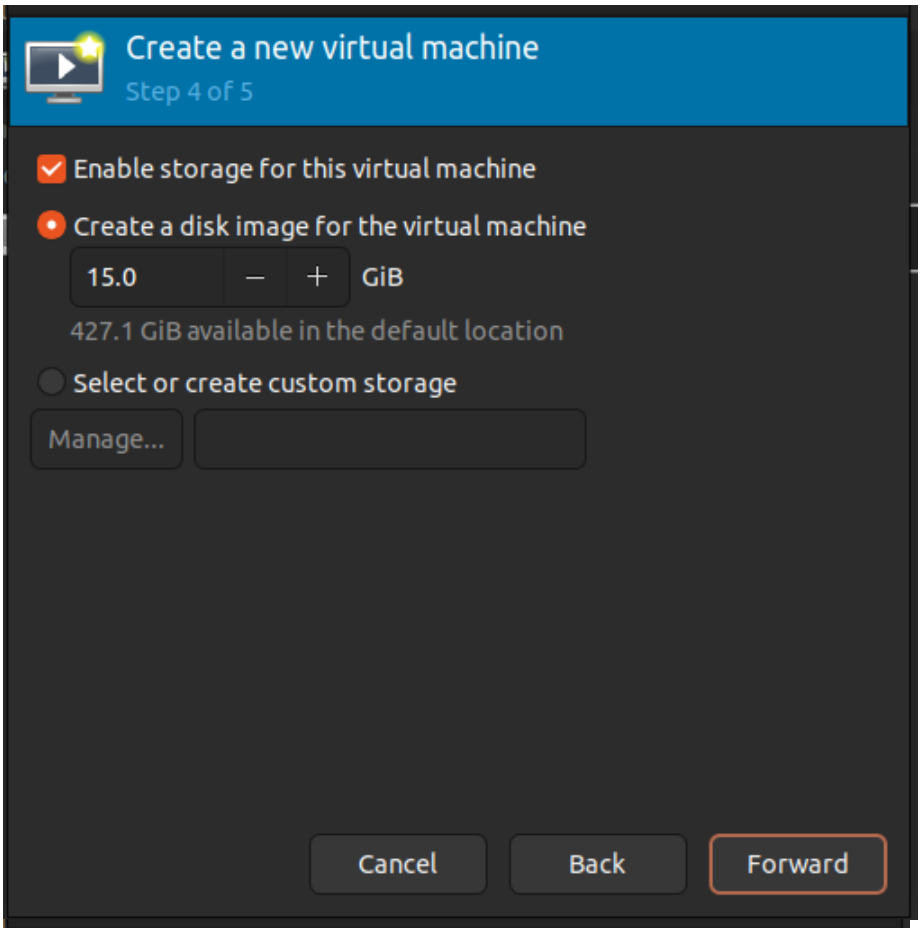
CLOUD COMPUTING JOURNAL

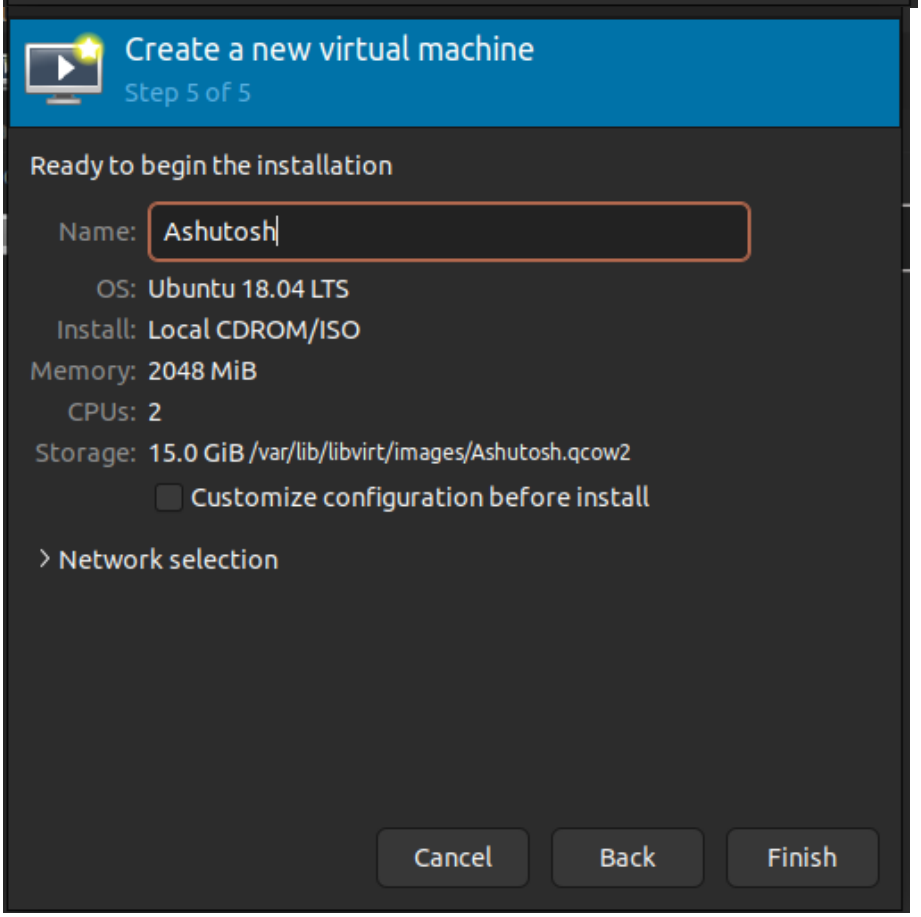


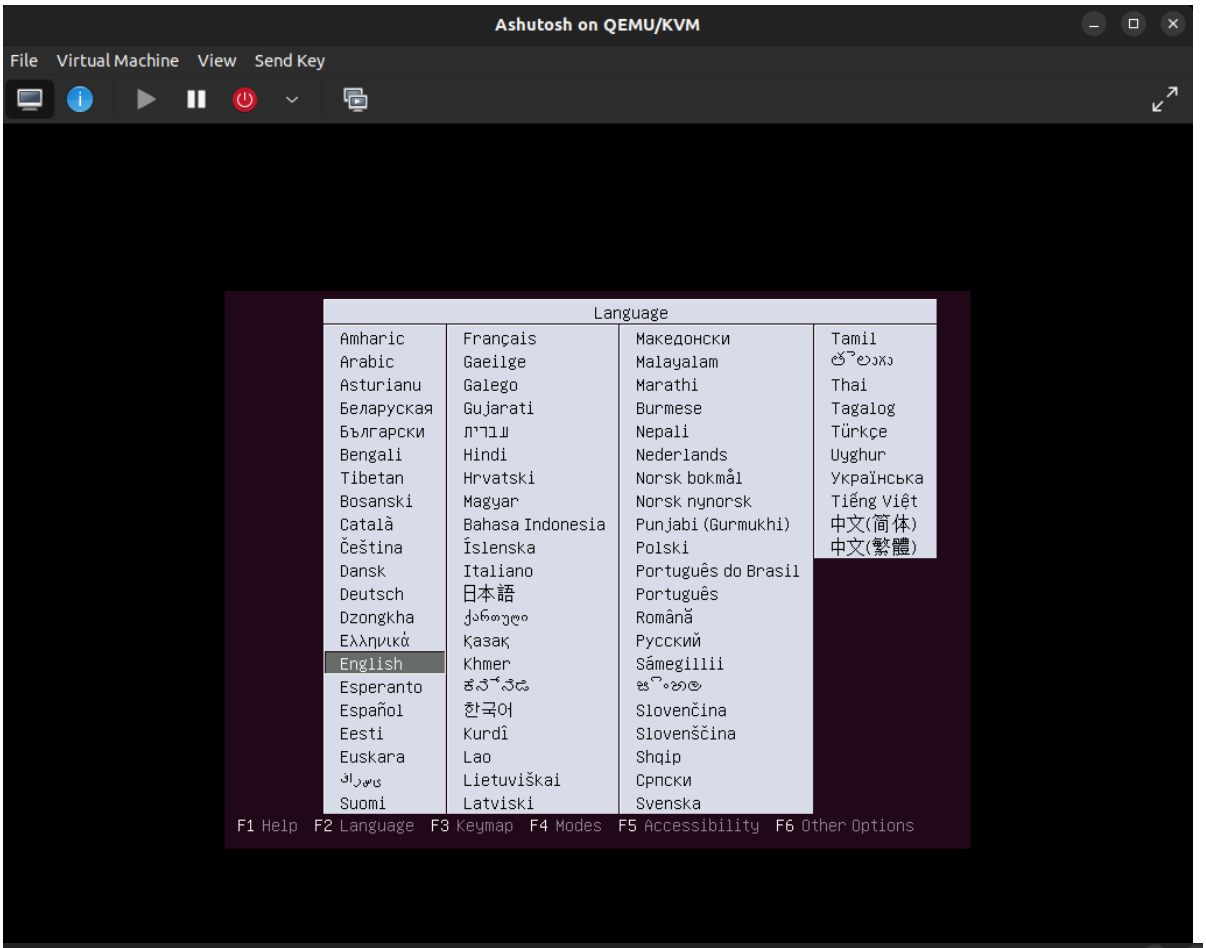

ashus@tcsc: /home/dcstcsc/Desktop
ashus@tcsc:/home/dcstcsc/Desktop$ sudo adduser ashus libvirt
Adding user `ashus' to group `libvirt' ...
Adding user ashus to group libvirt
Done.
ashus@tcsc:/home/dcstcsc/Desktop$ sudo adduser ashus kvm
Adding user `ashus' to group `kvm' ...
Adding user ashus to group 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
1692 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/lib/libvirt/libvirt
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
ashus@tcsc:/home/dcstcsc/Desktop$ sudo virt-manager
ashus@tcsc:/home/dcstcsc/Desktop$

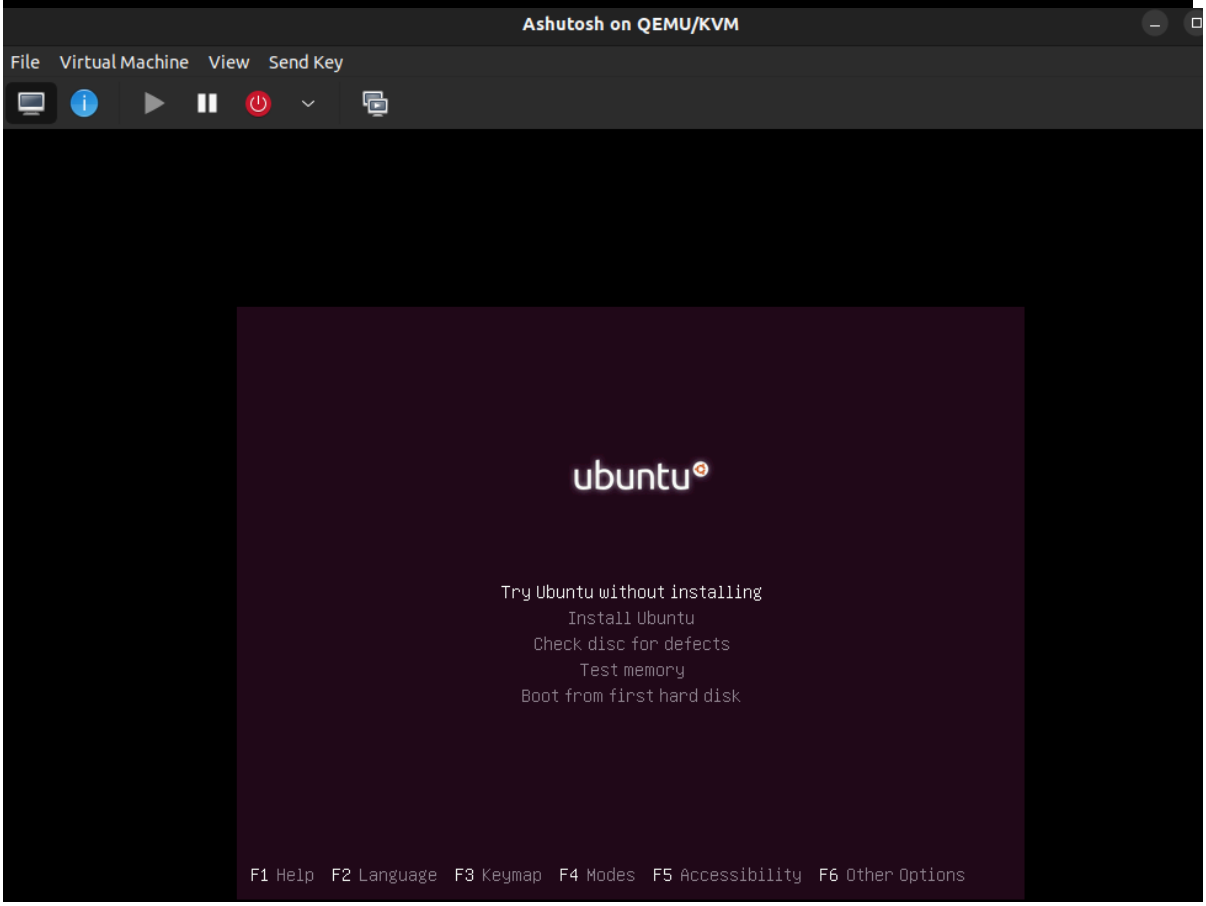

New VM
Create a new virtual machine
Step 1 of 5
Connection: QEMU/KVM
Choose how you would like to install the operating system
Local install media (ISO image or CDROM)
Network Install (HTTP, HTTPS, or FTP)
Import existing disk image
Manual install
Cancel
Back
Forward

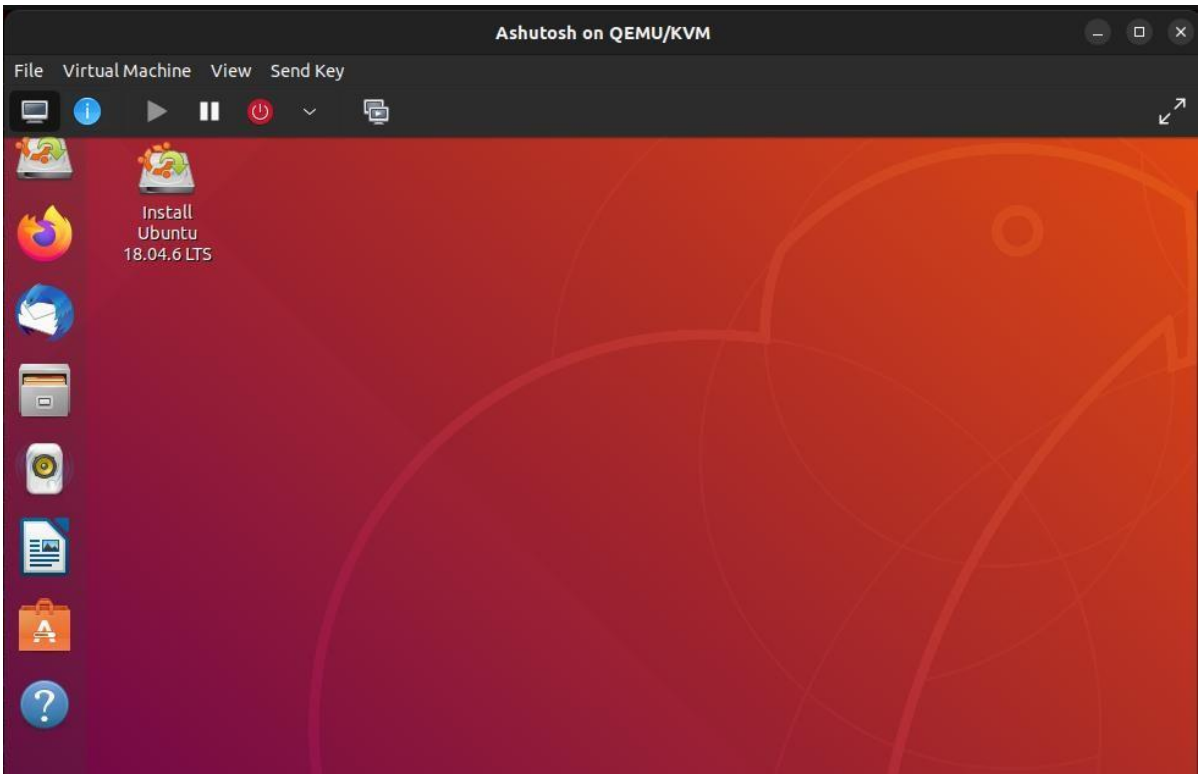

Create a new virtual machine
Step 2 of 5
Choose ISO or CDROM install media:
:/Downloads/ubuntu-18.04.6-desktop-amd64.iso
Browse...
Choose the operating system you are installing:
Ubuntu 18.04 LTS
Automatically detect from the installation media / source
Cancel
Back
Forward
Create a new virtual machine
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
Cancel
Back
Forward

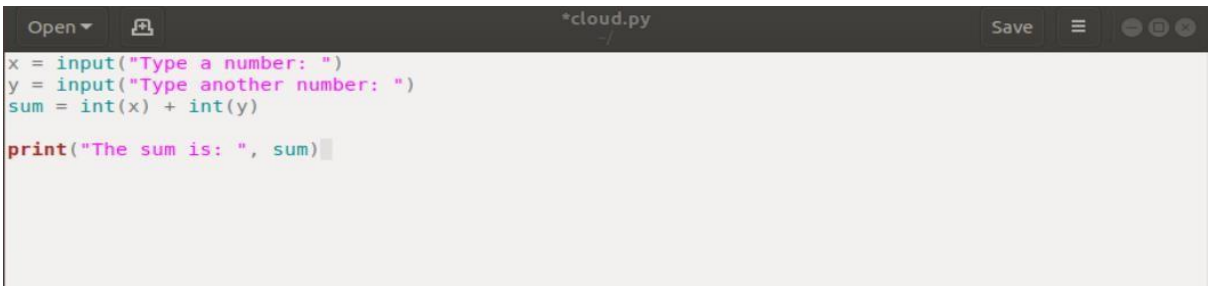

Create a new virtual machine
Step 4 of 5
Enable storage for this virtual machine
Create a disk image for the virtual machine
15.0
GiB
427.1 GiB available in the default location
Select or create custom storage
Manage...
Cancel
Back
Forward

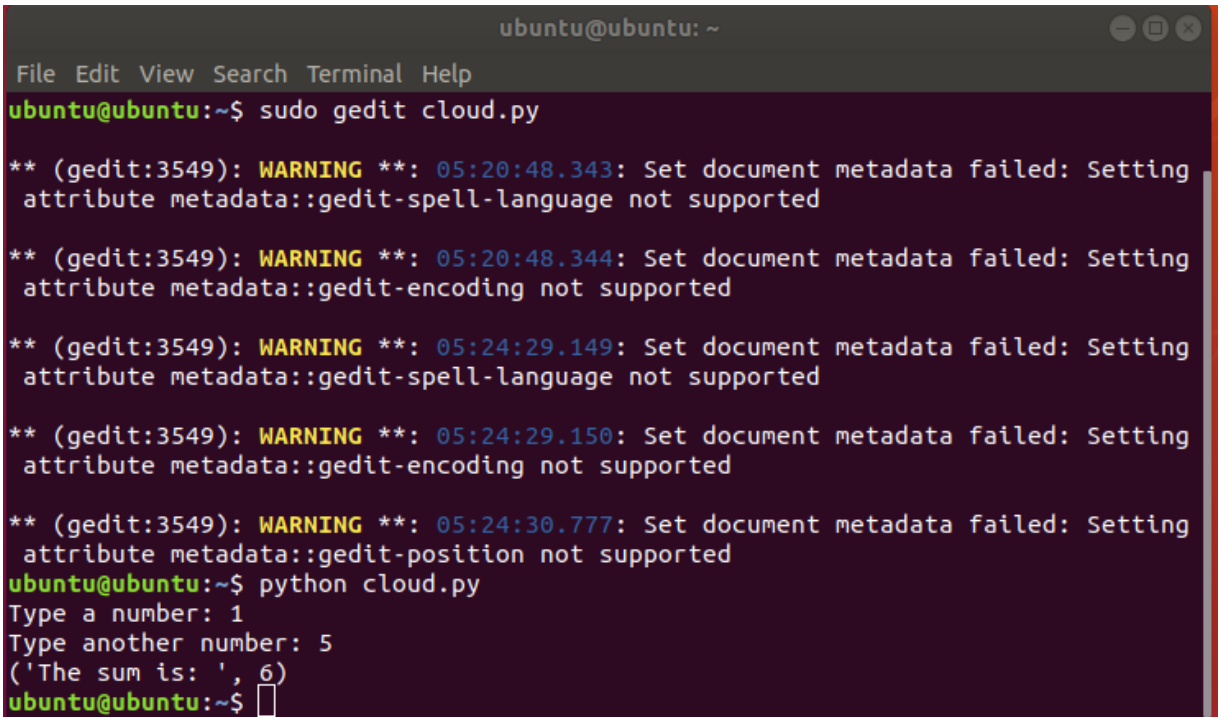

Create a new virtual machine
Step 5 of 5
Ready to begin the installation
Name: Ashutosh
OS: Ubuntu 18.04 LTS
Install: Local CDROM/ISO
Memory: 2048 MiB
CPUs: 2
Storage: 15.0 GiB /var/lib/libvirt/images/Ashutosh.qcow2
Customize configuration before install
Network selection
Cancel
Back
Finish


Ashutosh on QEMU/KVM
File Virtual Machine View Send Key
Language
Amharic
Arabic
Asturianu
Беларуская
Български
Bengali
Tibetan
Bosanski
Català
Čeština
Dansk
Deutsch
Dzongkha
Ελληνικά
English
Esperanto
Español
Eesti
Euskara
فارسی
Suomi
Français
Gaeilge
Galego
Gujarati
עברית
Hindi
Hrvatski
Magyar
Bahasa Indonesia
Íslenska
Italiano
日本語
ქართული
Қазақ
Khmer
ಕನ್ನಡ
한국어
Kurdî
Lao
Lietuviškai
Latviski
Македонски
Malayalam
Marathi
Burmese
Nepali
Nederlands
Norsk bokmål
Norsk nynorsk
Punjabi (Gurmukhi)
Polski
Português do Brasil
Português
Română
Русский
Sámegillii
සිංහල
Slovenčina
Slovenščina
Shqip
Српски
Svenska
Tamil
తెలుగు
Thai
Tagalog
Türkçe
Uyghur
Українська
Tiếng Việt
中文(简体)
中文(繁體)
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

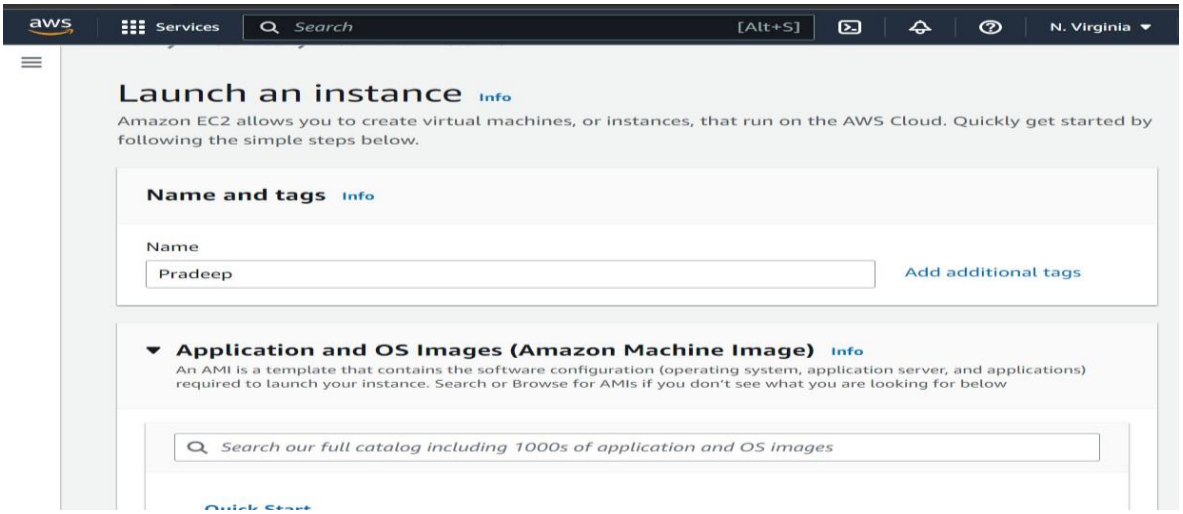

Ashutosh on QEMU/KVM
File Virtual Machine View Send Key
ubuntu
Try Ubuntu without installing
Install Ubuntu
Check disc for defects
Test memory
Boot from first hard disk
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

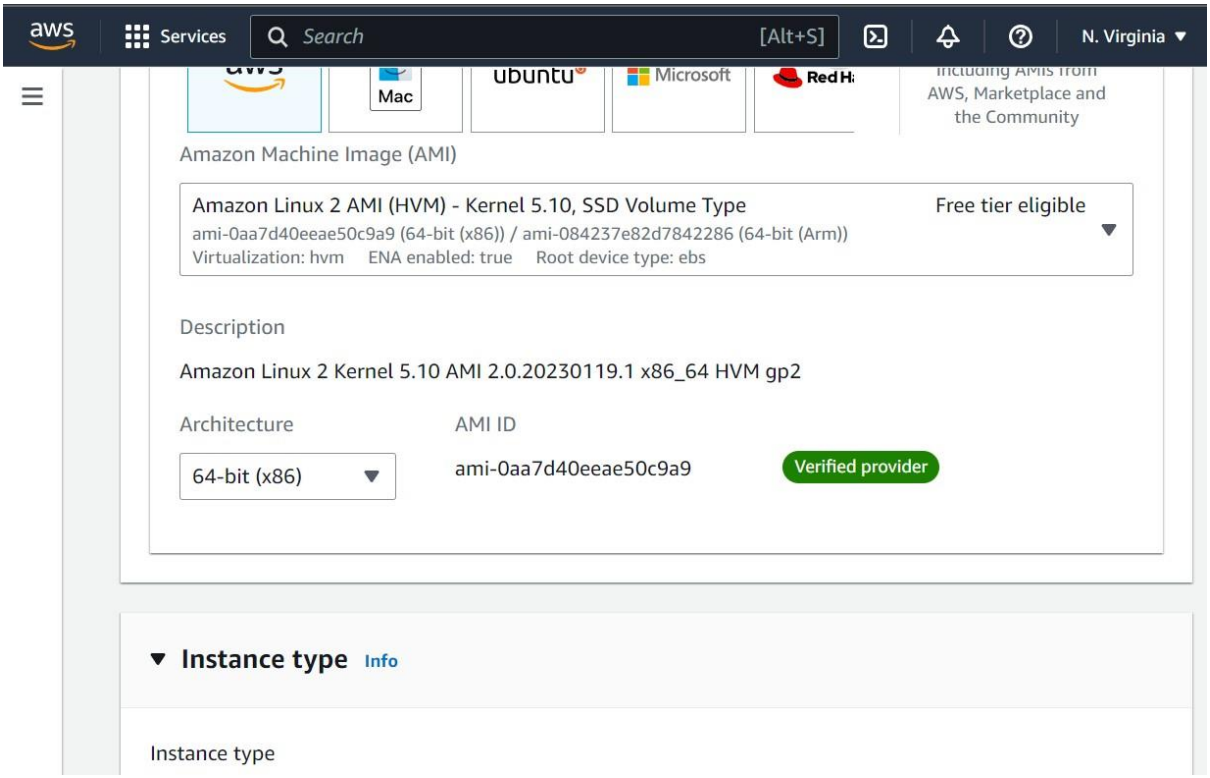

Ashutosh on QEMU/KVM
File Virtual Machine View Send Key
Install Ubuntu 18.04.6 LTS

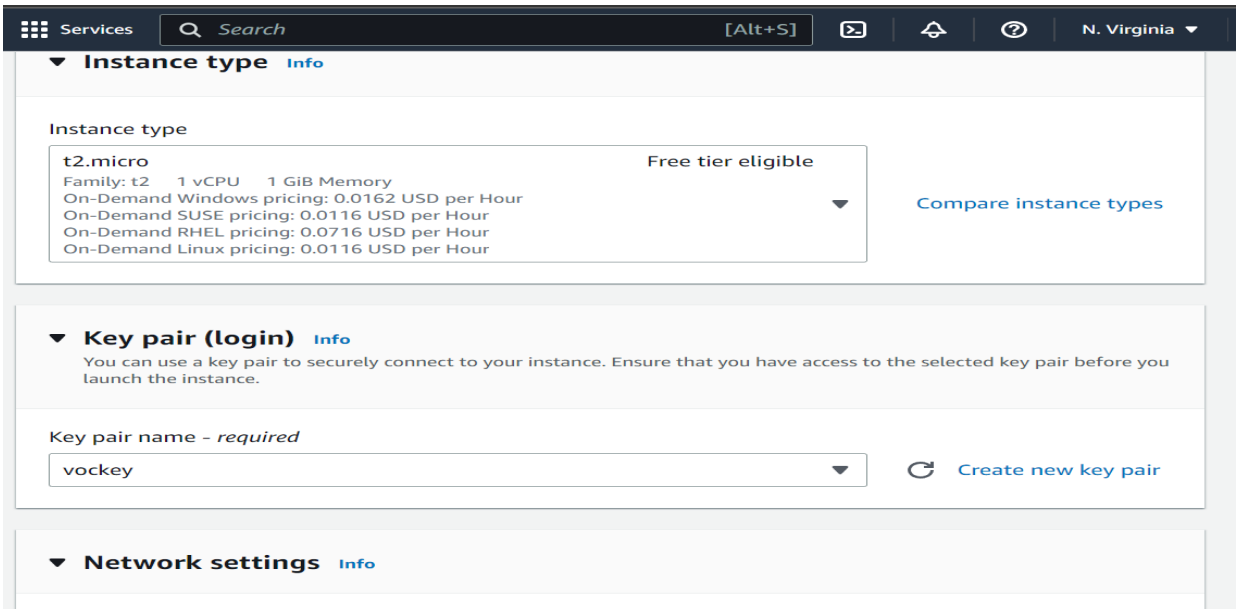

Open
*cloud.py
Save
x = input("Type a number: ")
y = input("Type another number: ")
sum = int(x) + int(y)
print("The sum is: ", sum)

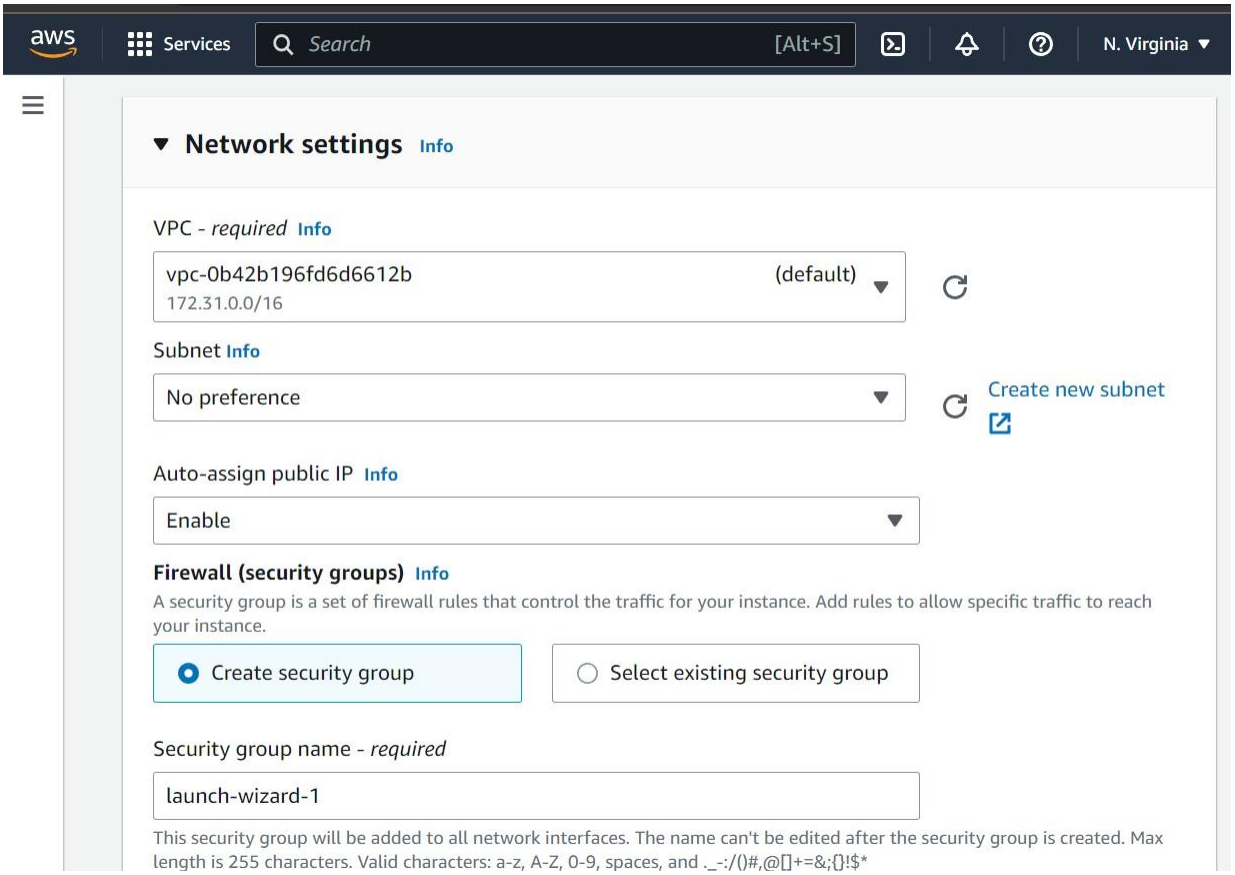

ubuntu@ubuntu: ~
File Edit View Search Terminal Help
ubuntu@ubuntu:~$ sudo gedit cloud.py
** (gedit:3549): WARNING **: 05:20:48.343: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:3549): WARNING **: 05:20:48.344: Set document metadata failed: Setting 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:~$

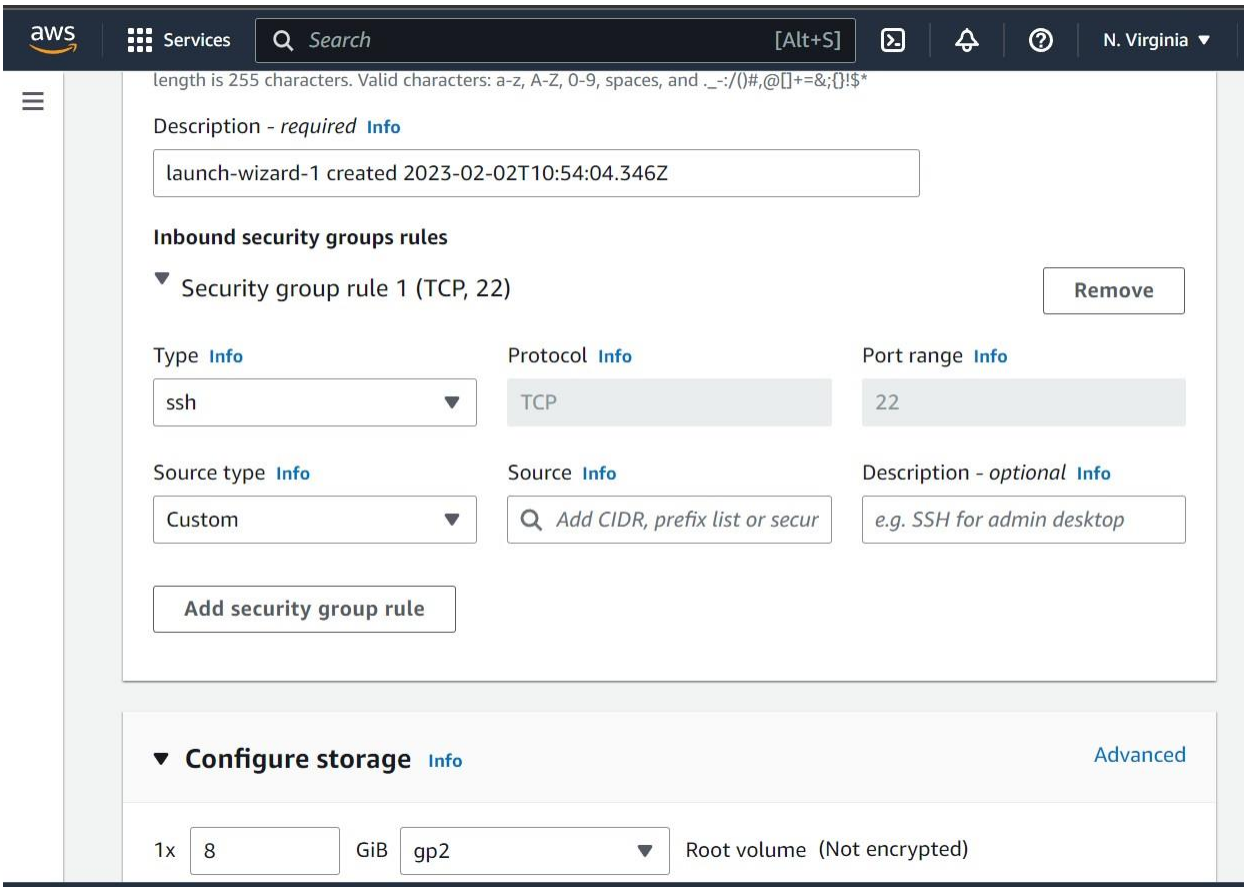
. B.GCP/AWS/IBM/AZure/...

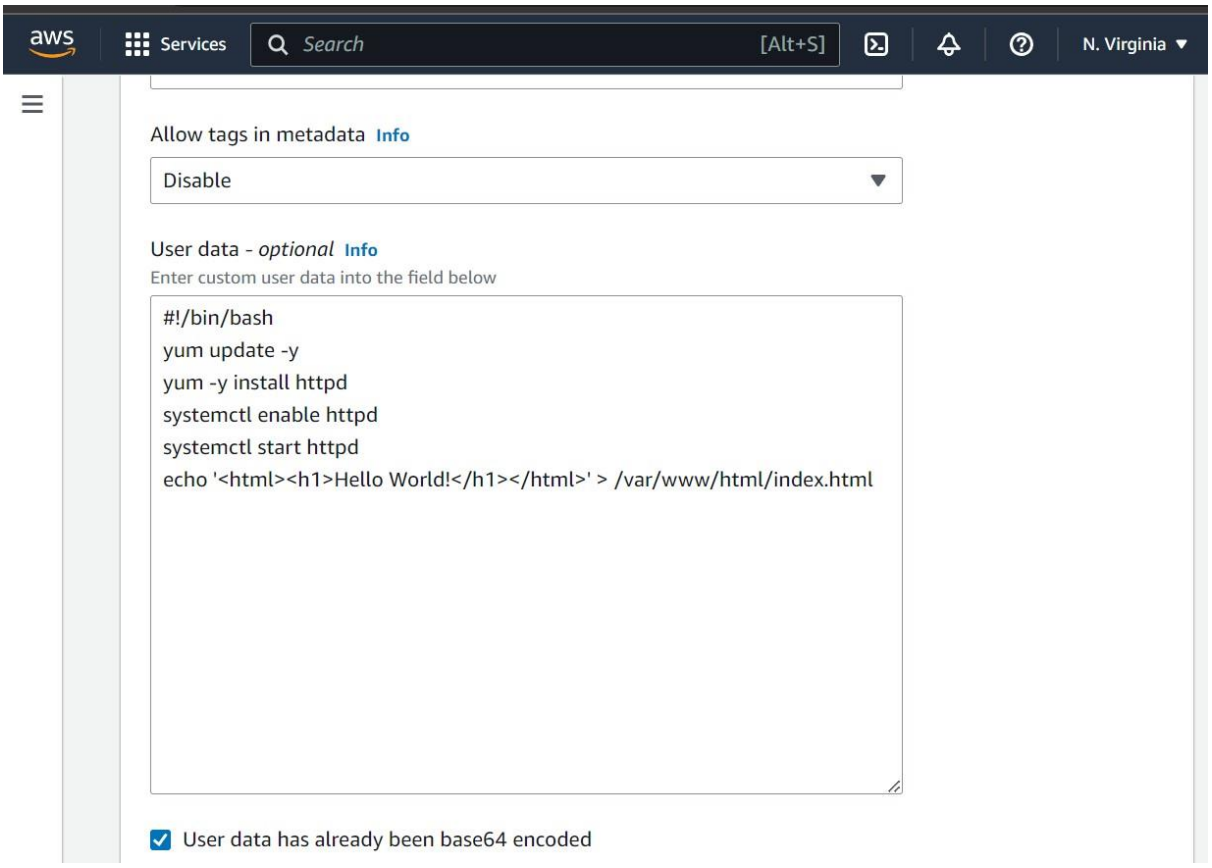


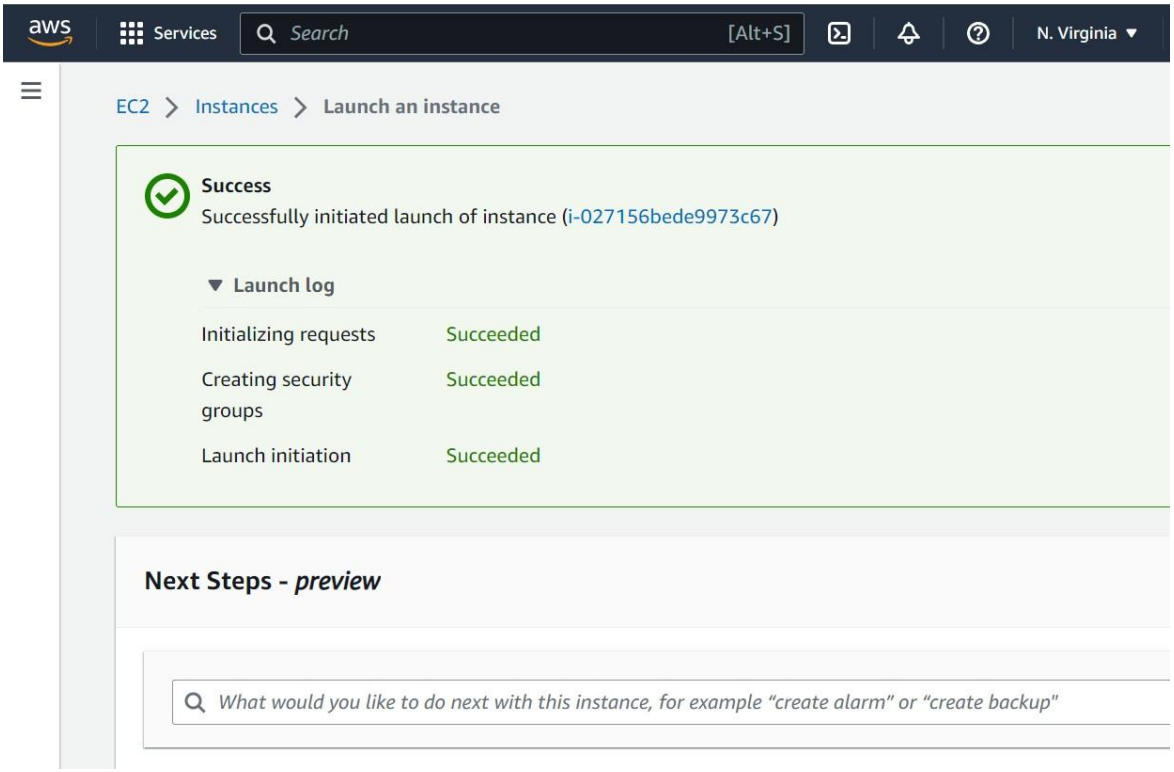


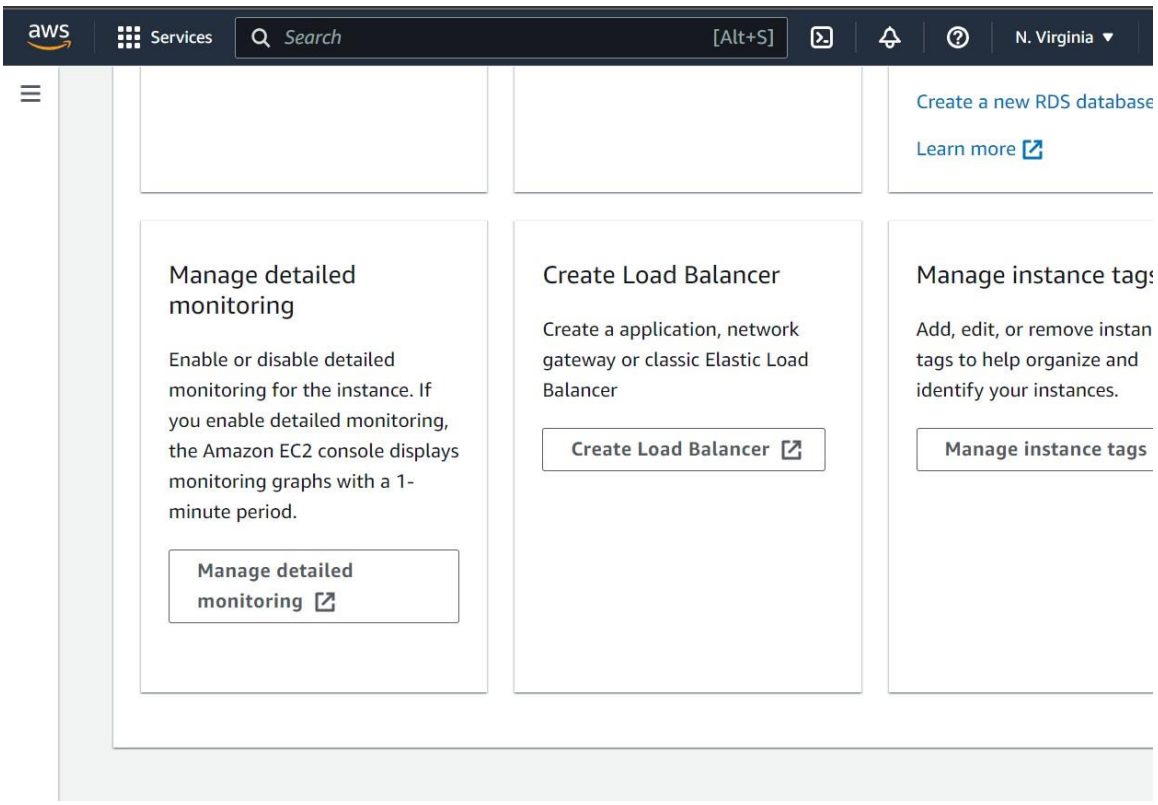

Services
Search
[Alt+S]
N. Virginia
Instance type Info
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour
Compare instance types
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
Create new key pair
Network settings Info


aws
Services
Search
[Alt+S]
N. Virginia
Network settings Info
VPC - required Info
vpc-0b42b196fd6d6612b
(default)
172.31.0.0/16
Subnet Info
No preference
Create new subnet
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
Security group name - required
launch-wizard-1
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

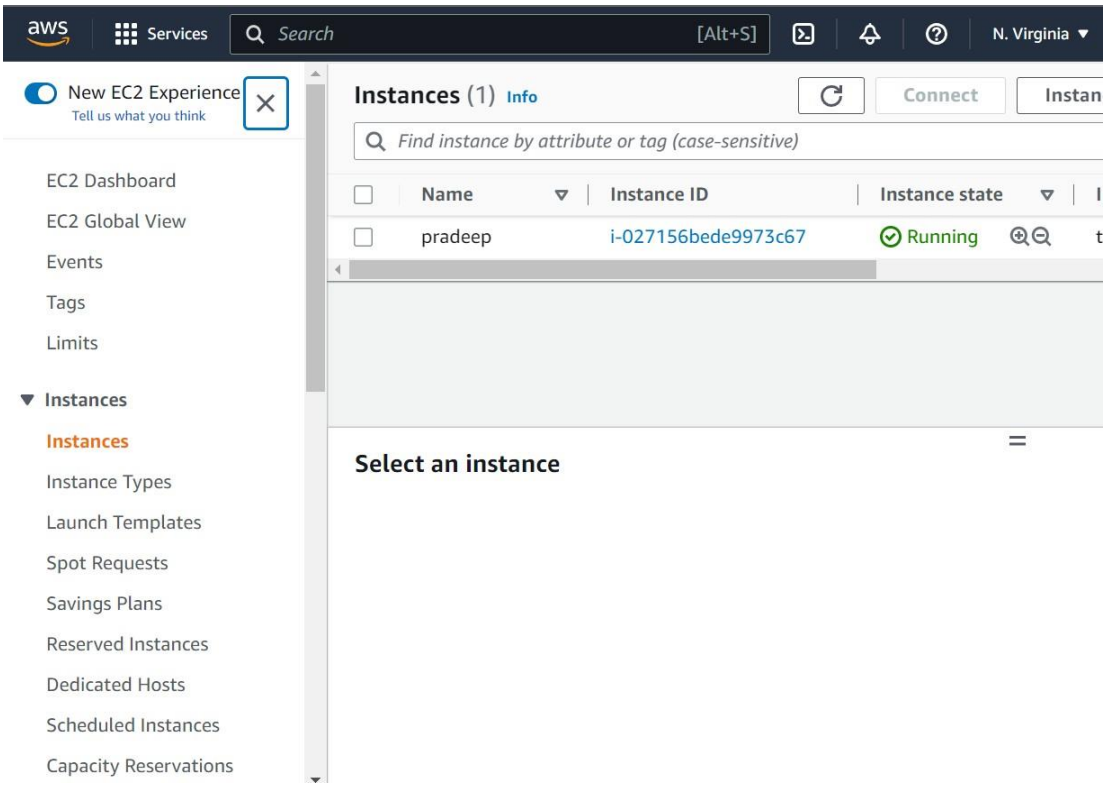

aws
Services
Search
[Alt+S]
N. Virginia
length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard-1 created 2023-02-02T10:54:04.346Z
Inbound security groups rules
Security group rule 1 (TCP, 22)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Custom
Source Info
Add CIDR, prefix list or secur
Description - optional Info
e.g. SSH for admin desktop
Add security group rule
Configure storage Info
Advanced
1x
8
GiB
gp2
Root volume (Not encrypted)

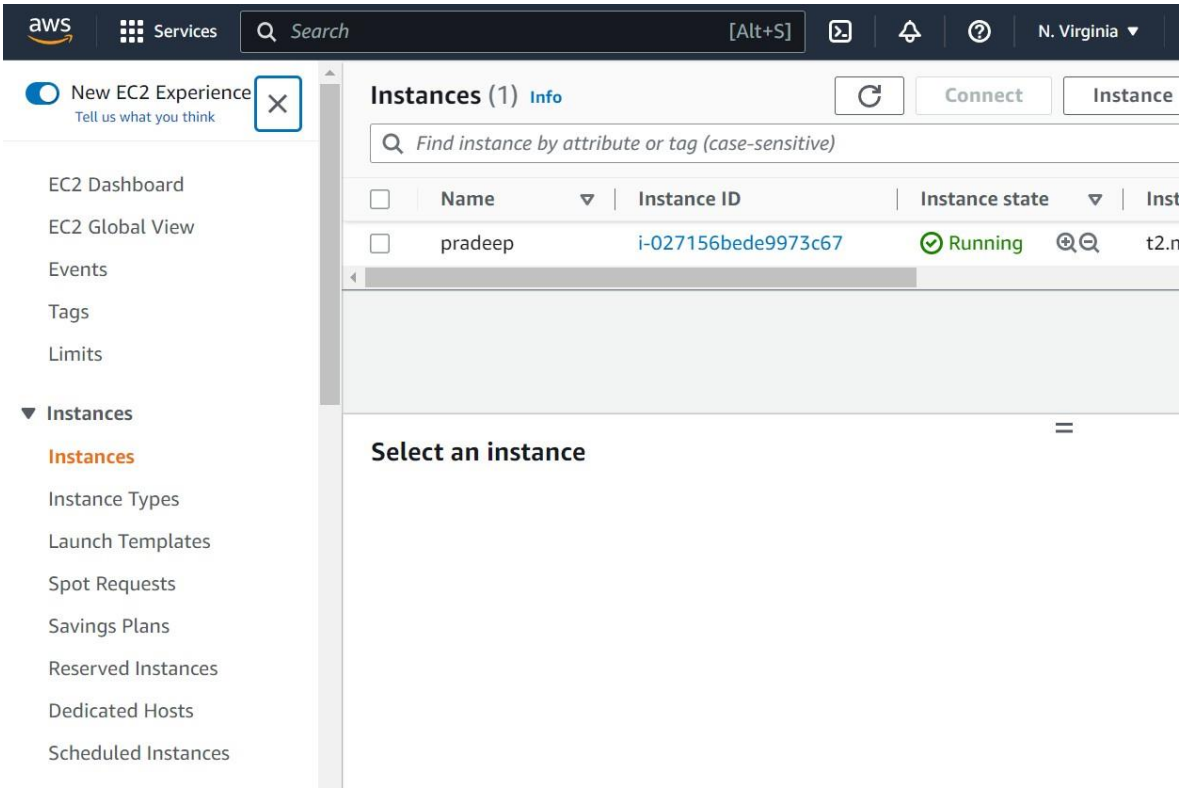

aws
Services
Search
[Alt+S]
N. Virginia
Allow tags in metadata Info
Disable
User data - optional Info
Enter custom user data into the field below
#!/bin/bash
yum update -y
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello World!</h1></html>' > /var/www/html/index.html
User data has already been base64 encoded

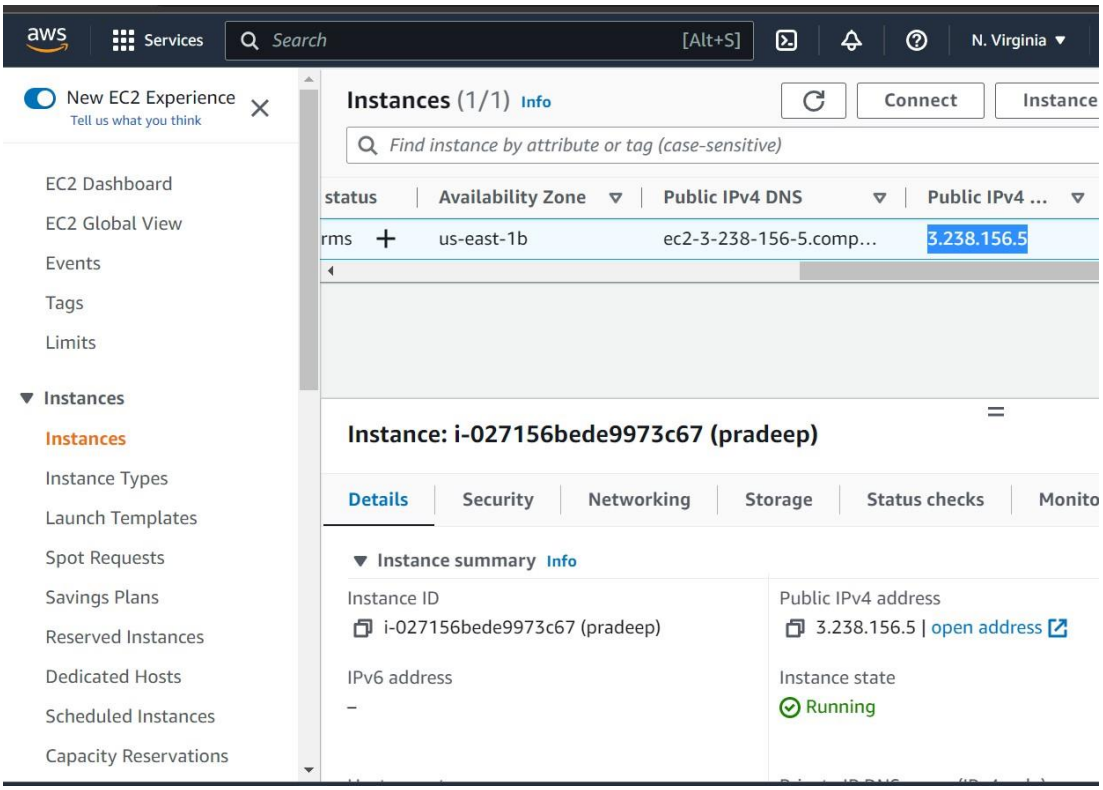

aws
Services
Search
[Alt+S]
N. Virginia
EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-027156bede9973c67)
Launch log
Initializing requests
Succeeded
Creating security groups
Succeeded
Launch initiation
Succeeded
Next Steps - preview
What would you like to do next with this instance, for example "create alarm" or "create backup"

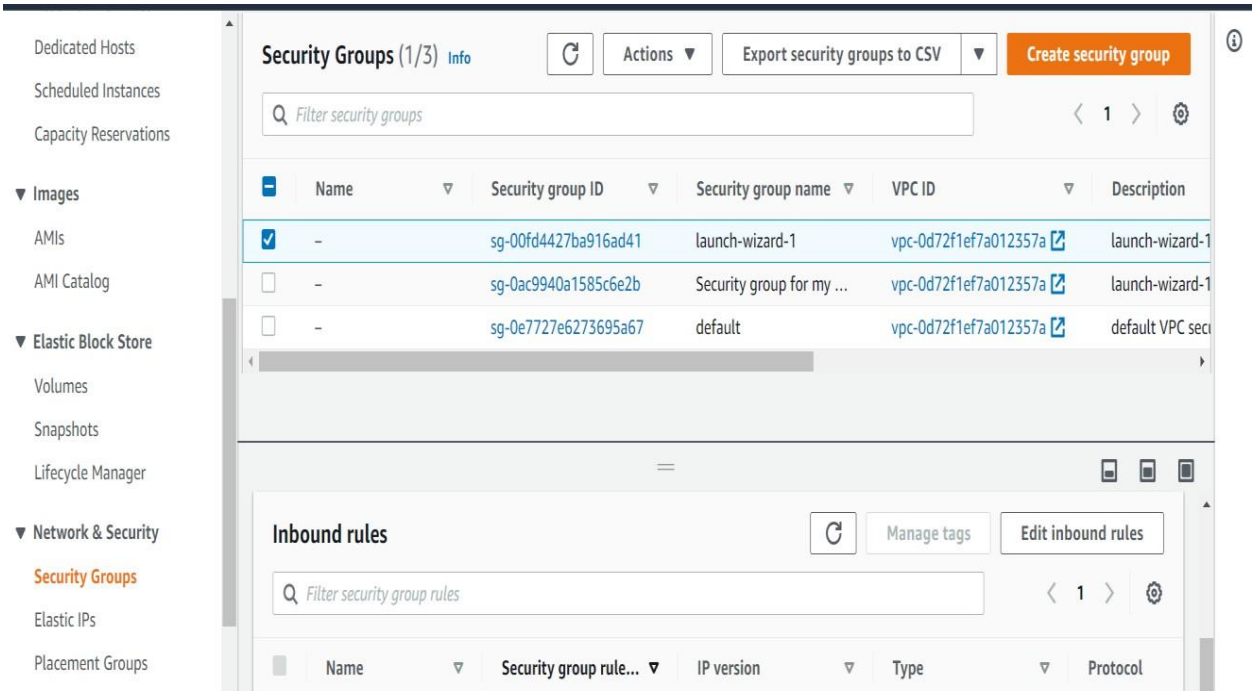

aws
Services
Search
[Alt+S]
N. Virginia
Create a new RDS database
Learn more
Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.
Manage detailed monitoring
Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer
Create Load Balancer
Manage instance tags
Add, edit, or remove instan tags to help organize and identify your instances.
Manage instance tags

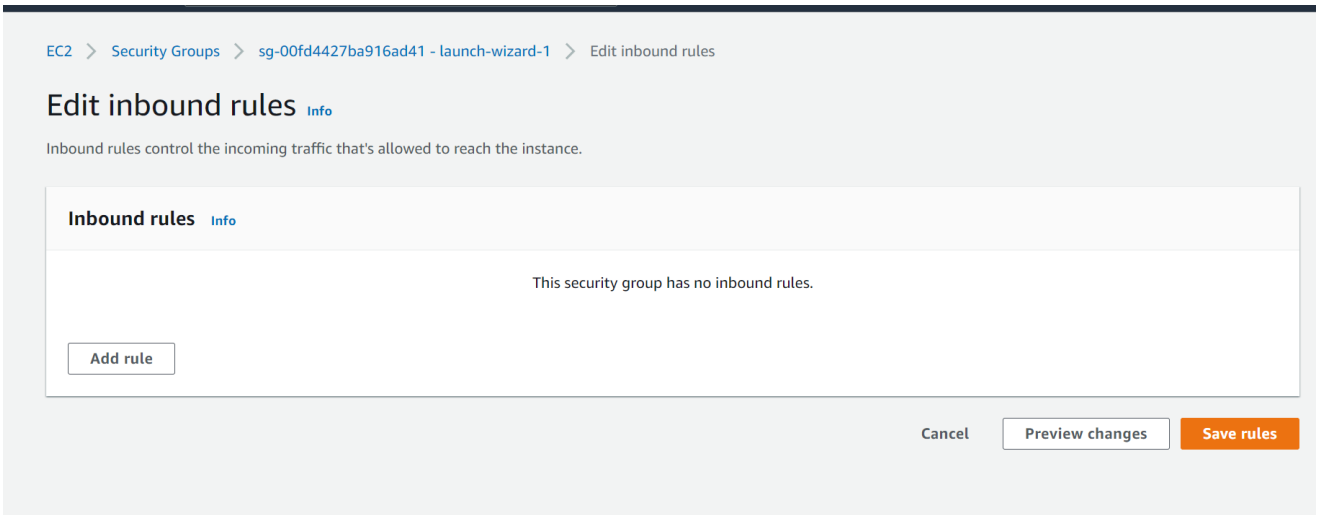
CLOUD COMPUTING JOURNAL

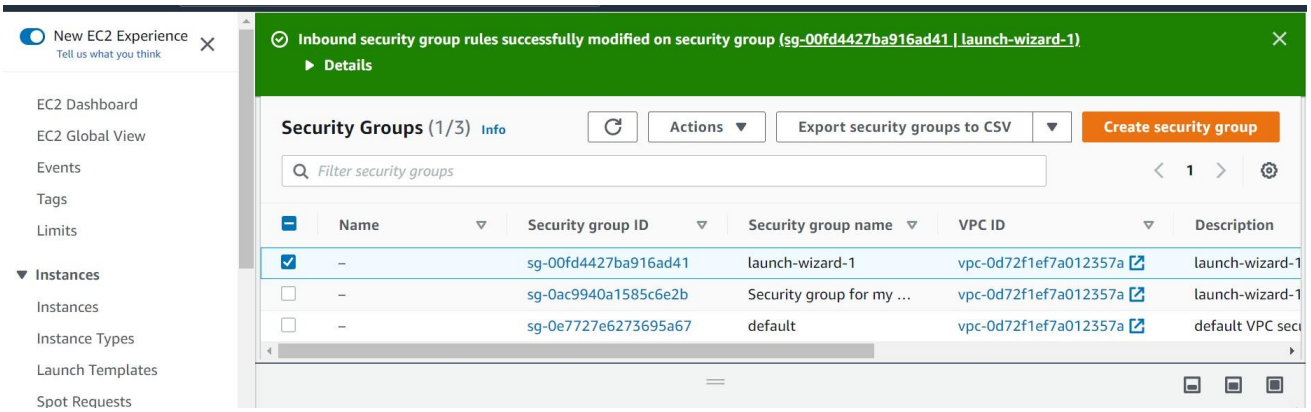





aws
Services
Search
[Alt+S]
N. Virginia
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Instances (1/1) Info
Connect
Instance
Find instance by attribute or tag (case-sensitive)
status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
us-east-1b
ec2-3-238-156-5.comp...
3.238.156.5
Instance: i-027156bede9973c67 (pradeep)
Details
Security
Networking
Storage
Status checks
Monito
Instance summary Info
Instance ID
i-027156bede9973c67 (pradeep)
Public IPv4 address
3.238.156.5 | open address
IPv6 address
Instance state
Running


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





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

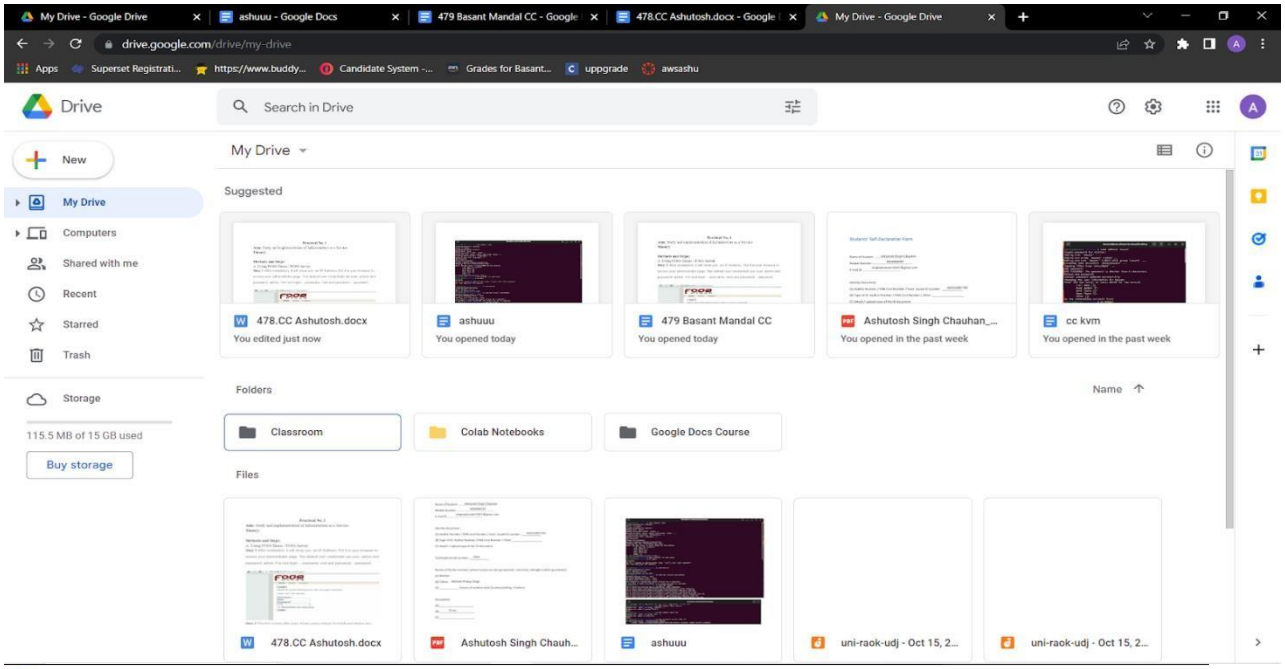
Instead of storing data on-premises, organizations that use STaaS will typically utilize a public cloud for storage and backup needs. Public cloud storage may also use different storage methods for STaaS. These storage methods include backup and restore, disaster recovery, block storage, SSD storage, 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).

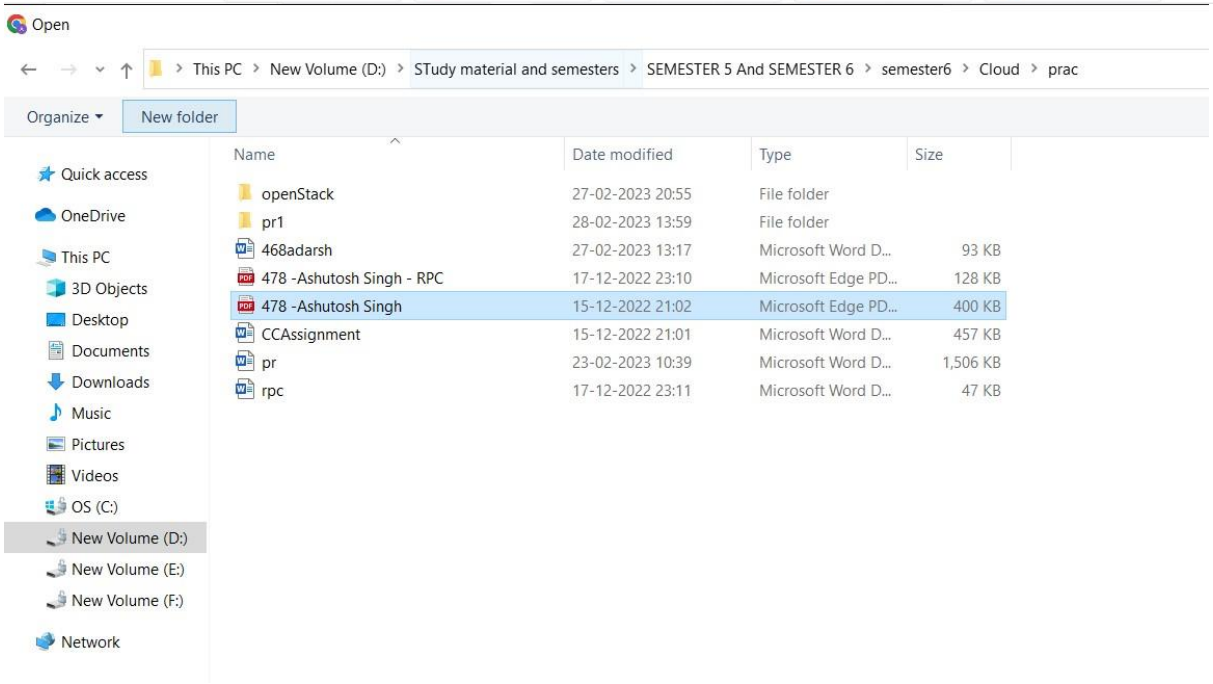
Block storage enables customers to provision block storage volumes for lower-latency I/O. SSD storage is another storage type that is typically used for intensive read/write and I/O operations. Object storage systems are used in data analytics, disaster recovery and cloud applications and tend to have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

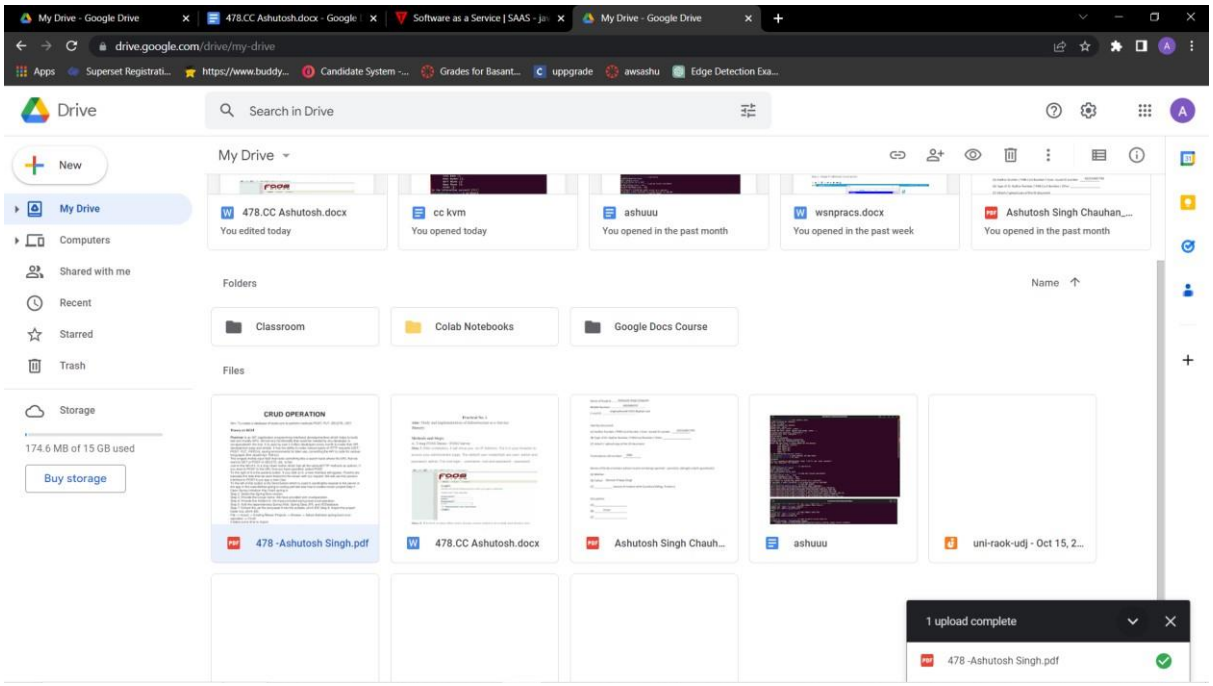
storage is used to create and configure stored data quickly. Bulk data transfers will use disks and other hardware to transfer data.

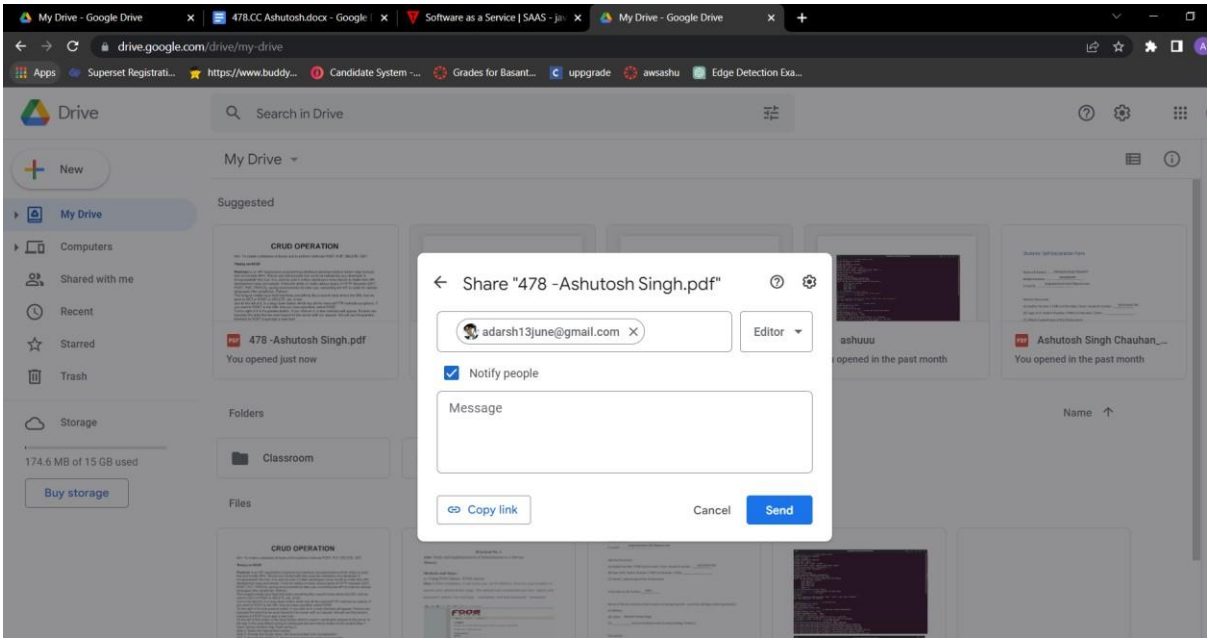
Methods and Steps:

A. Google Drive

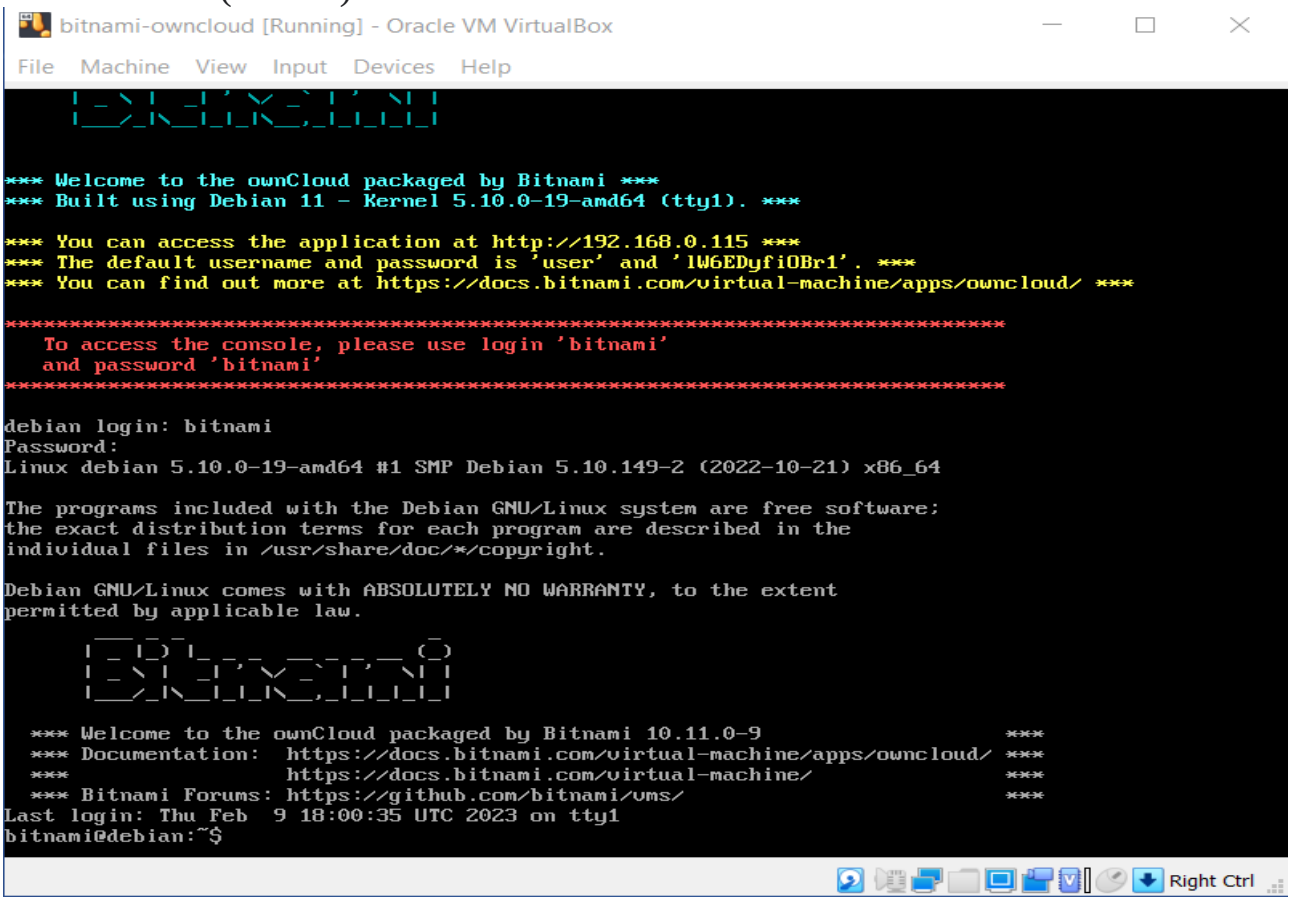


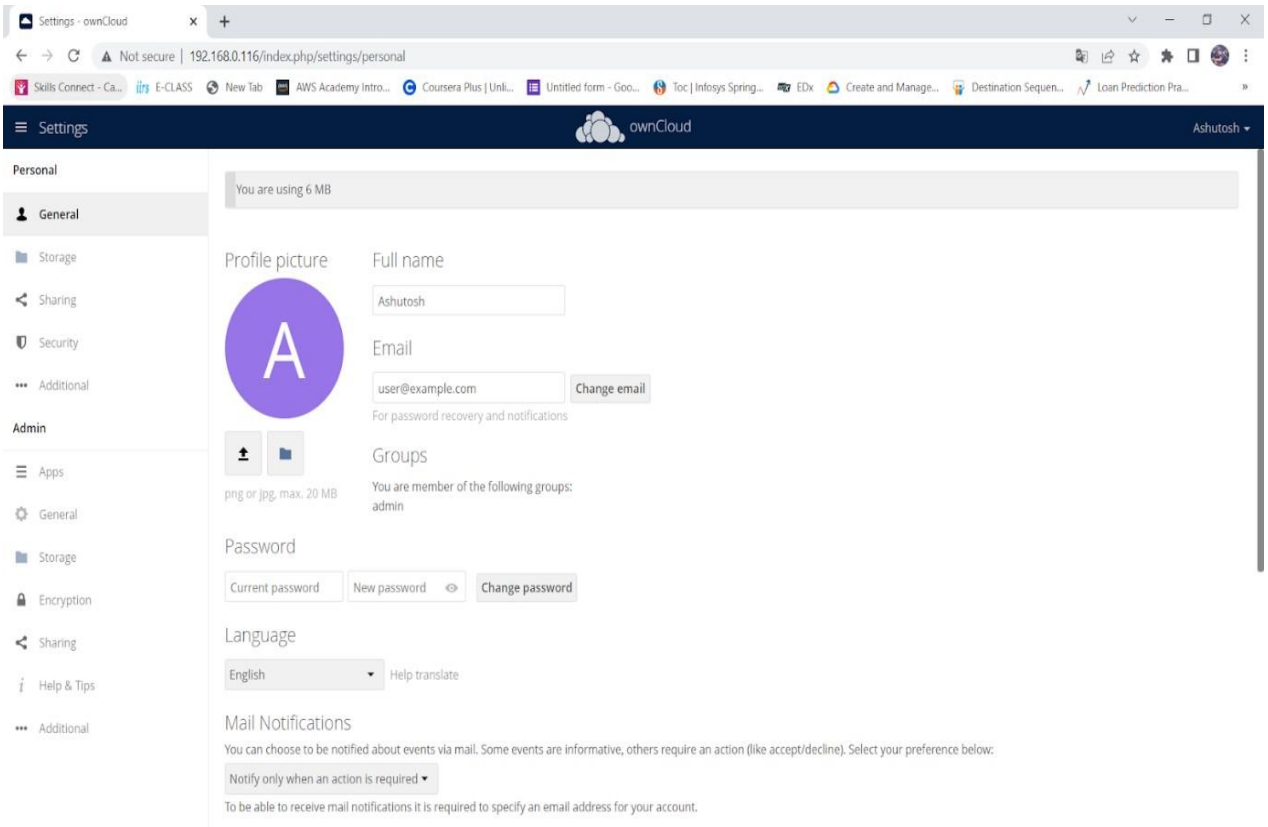


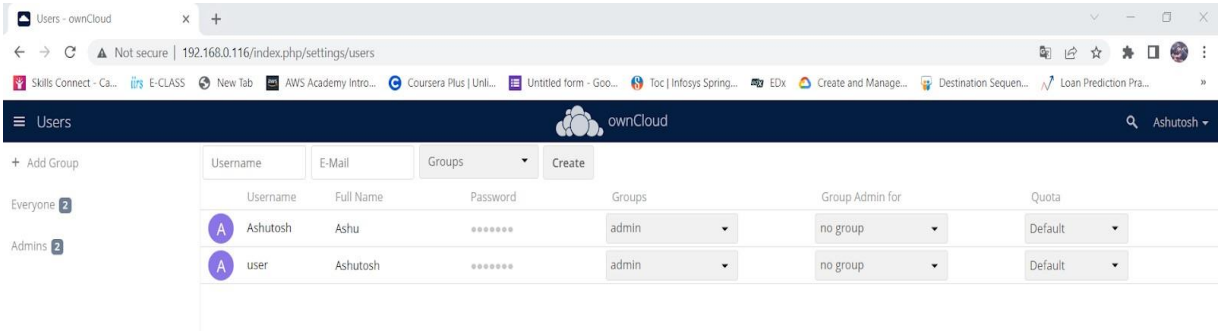

My Drive - Google Drive
drive.google.com/drive/my-drive
Drive
Search in Drive
New
My Drive
Computers
Shared with me
Recent
Starred
Trash
Storage
174.6 MB of 15 GB used
Buy storage
478.CC Ashutosh.docx
You edited today
cc kvm
You opened today
ashuuu
You opened in the past month
wsnpracs.docx
You opened in the past week
Ashutosh Singh Chauhan_...
You opened in the past month
Folders
Name
Classroom
Colab Notebooks
Google Docs Course
Files
478 -Ashutosh Singh.pdf
478.CC Ashutosh.docx
Ashutosh Singh Chauh...
ashuuu
uni-raok-udj - Oct 15, 2...
1 upload complete
478 -Ashutosh Singh.pdf

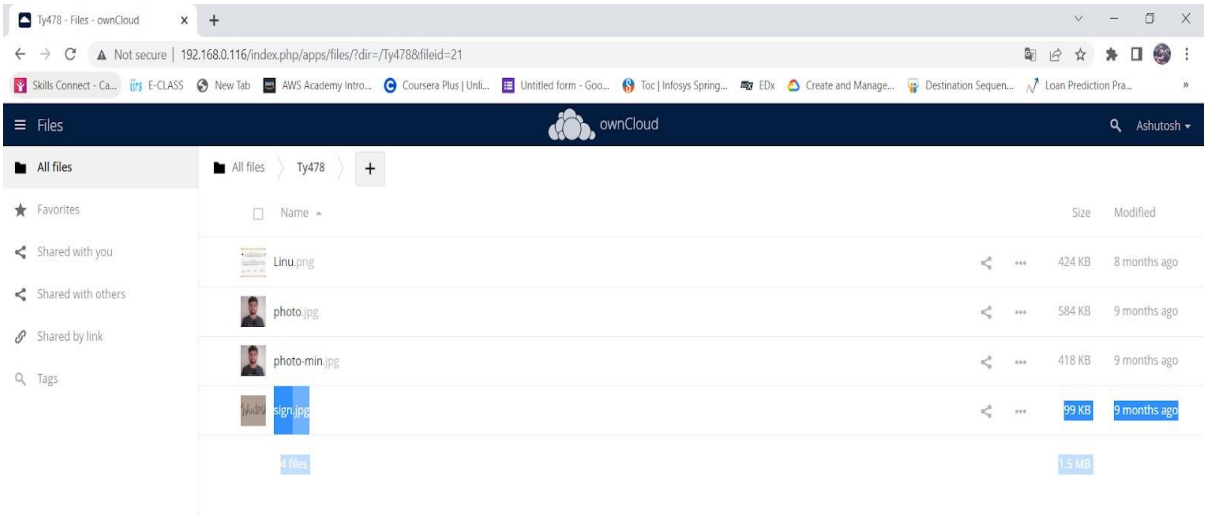

My Drive - Google Drive
drive.google.com/drive/my-drive
Drive
Search in Drive
New
My Drive
Suggested
Computers
Shared with me
Recent
Starred
Trash
Storage
174.6 MB of 15 GB used
Buy storage
478 -Ashutosh Singh.pdf
You opened just now
Folders
Classroom
Files
Share "478 -Ashutosh Singh.pdf"
adarsh13june@gmail.com
Editor
Notify people
Message
Copy link
Cancel
Send
ashuuu
Ashutosh Singh Chauhan_...
You opened in the past month
Name

B. OwnCloud (Offline)

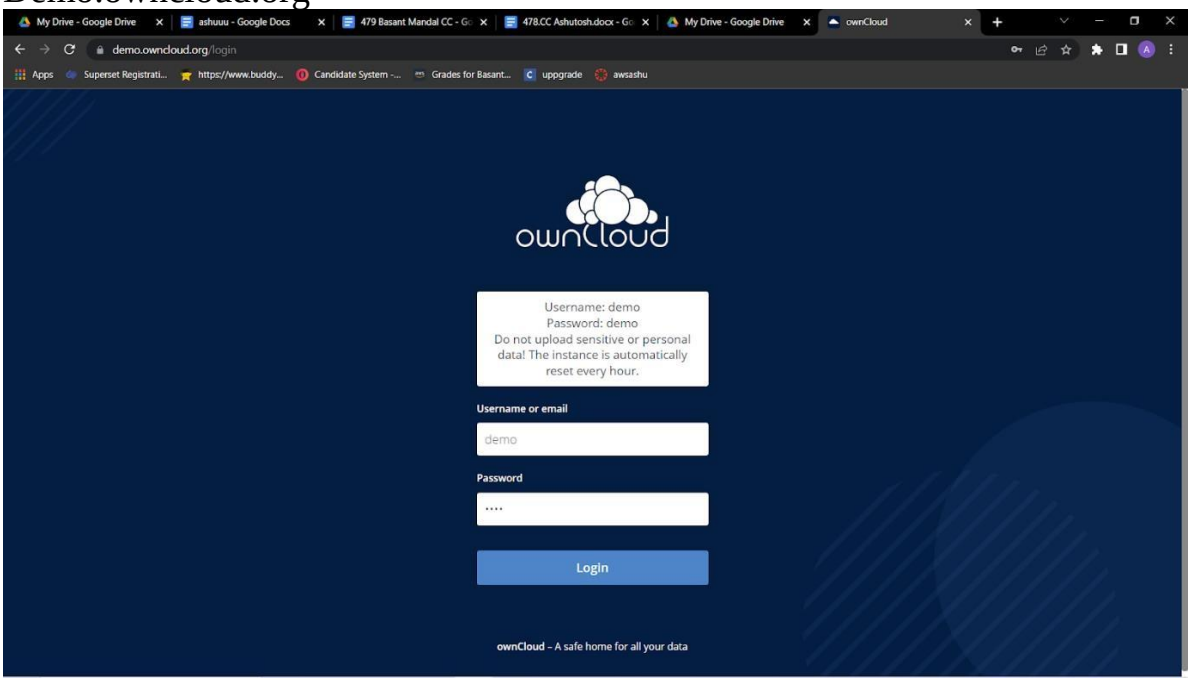


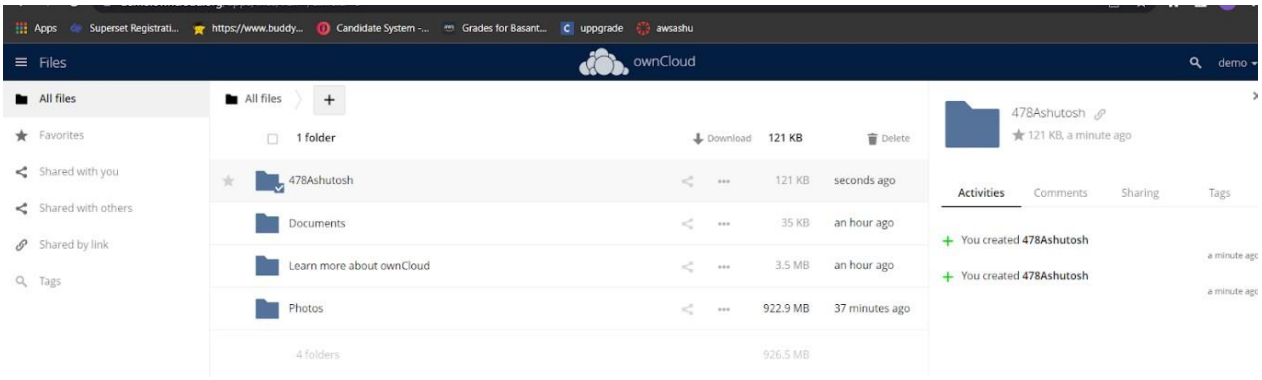


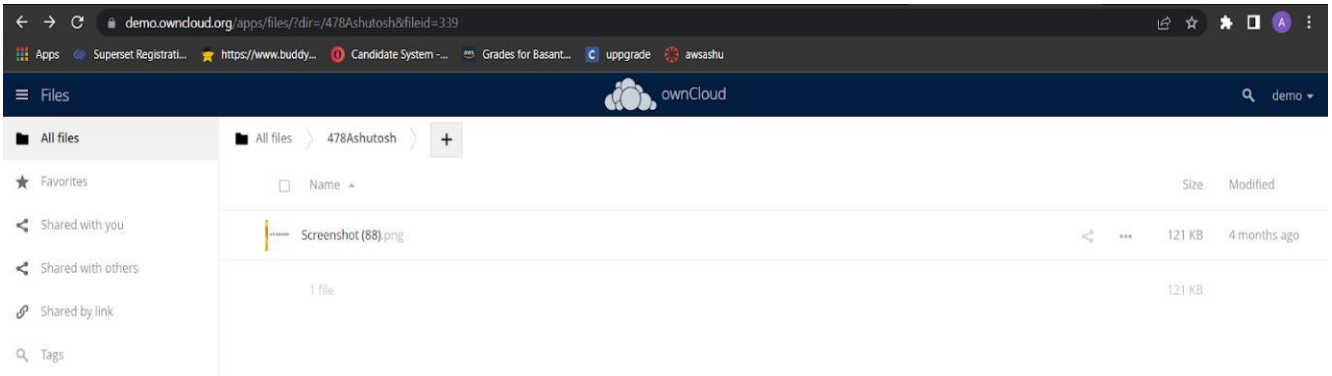




C. Owncloud (Online)
Demo.owncloud.org







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.

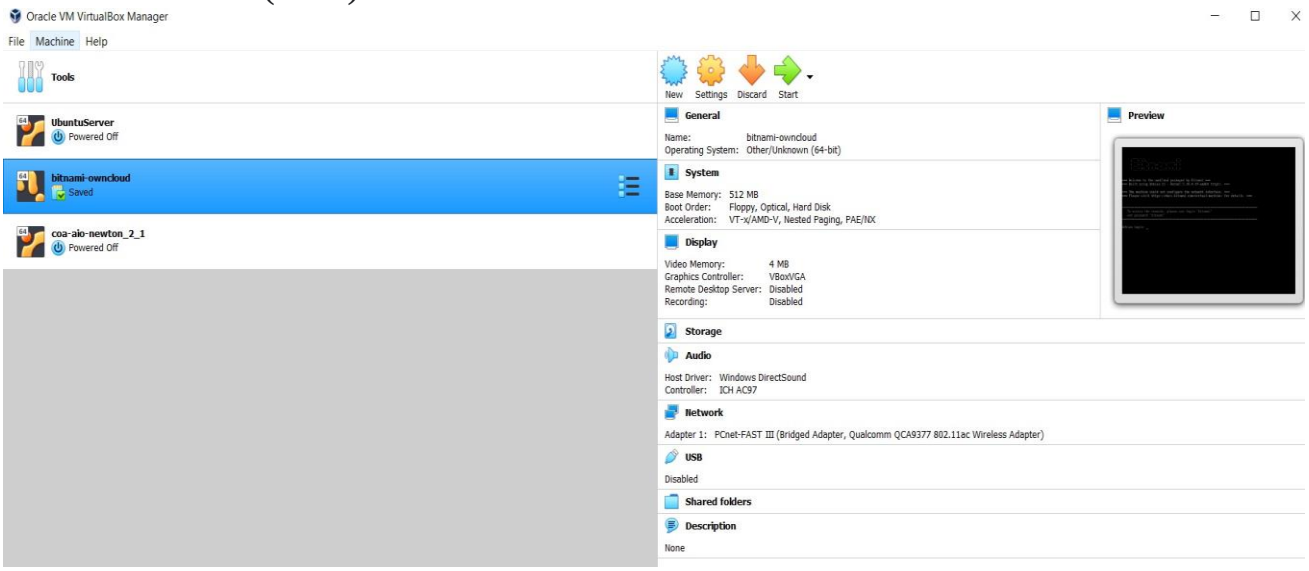
For end-users, many parts of user management are invisible. When users are exposed to user management—for example, when they use a login box to access an application—they expect the interaction to be simple and seamless. Login is a frequently-performed, critical operation, meaning that any delay or malfunction 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.

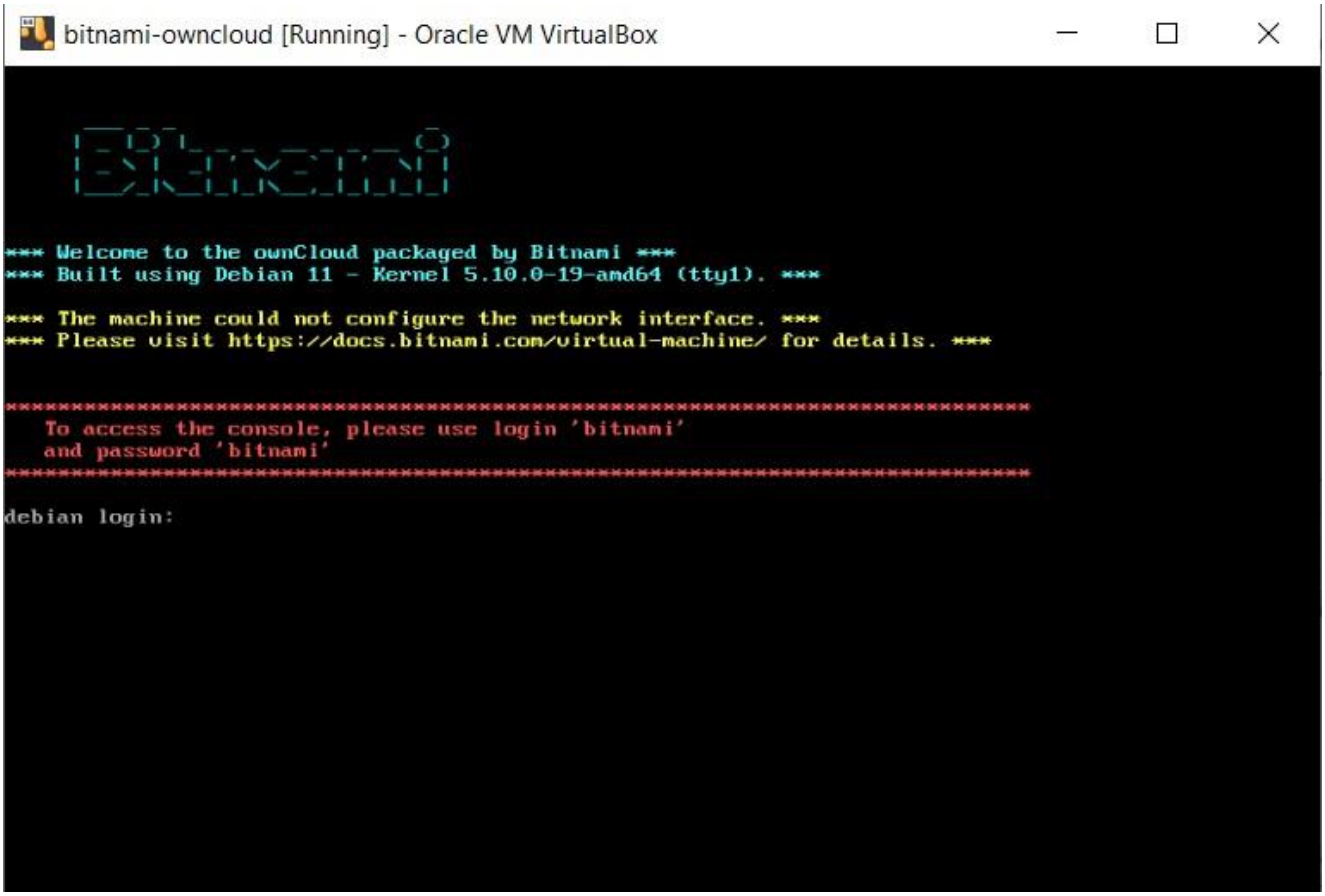
Organizations must find a way to manage secure access for a distributed environment. At the same time, users demand the same simplicity of popular services like Google and Facebook in their work environment. These challenges

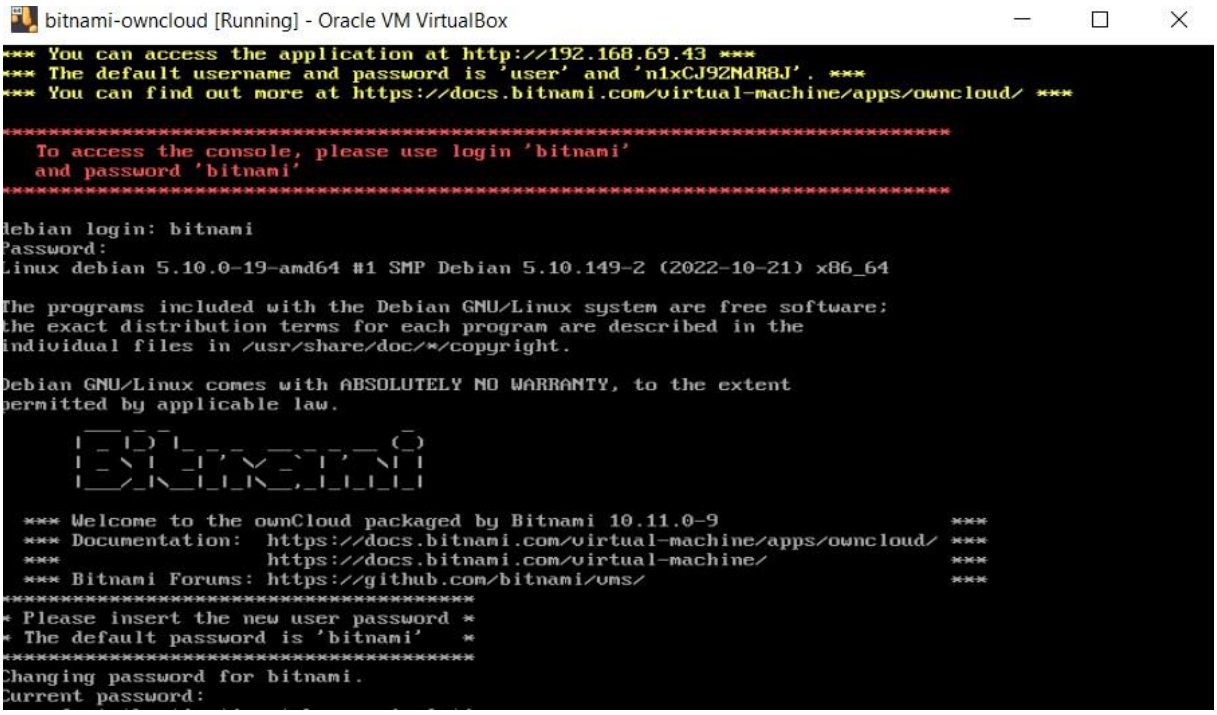
are making user management more important and more complex than ever before.

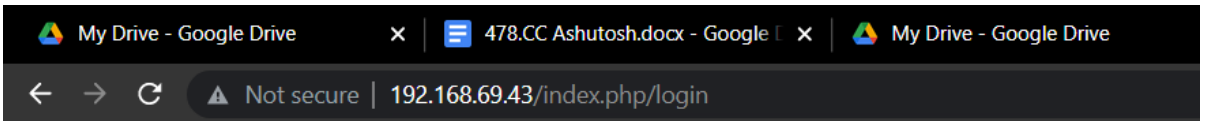
Methods and Steps:

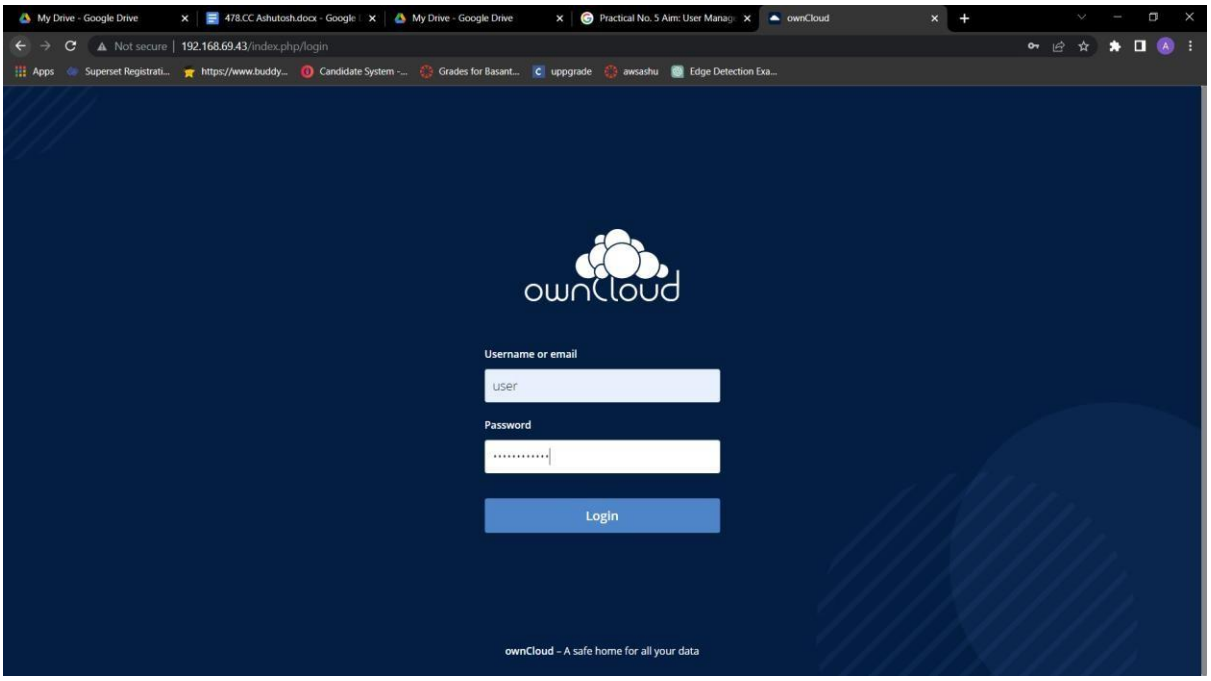
A. OwnCloud(local)

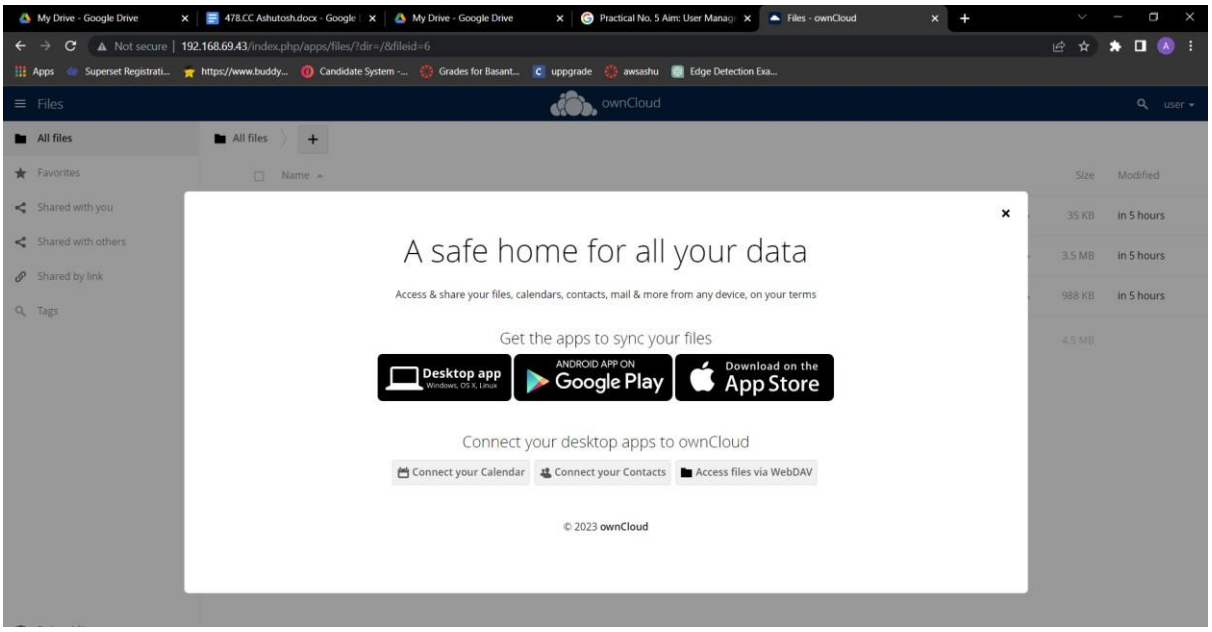


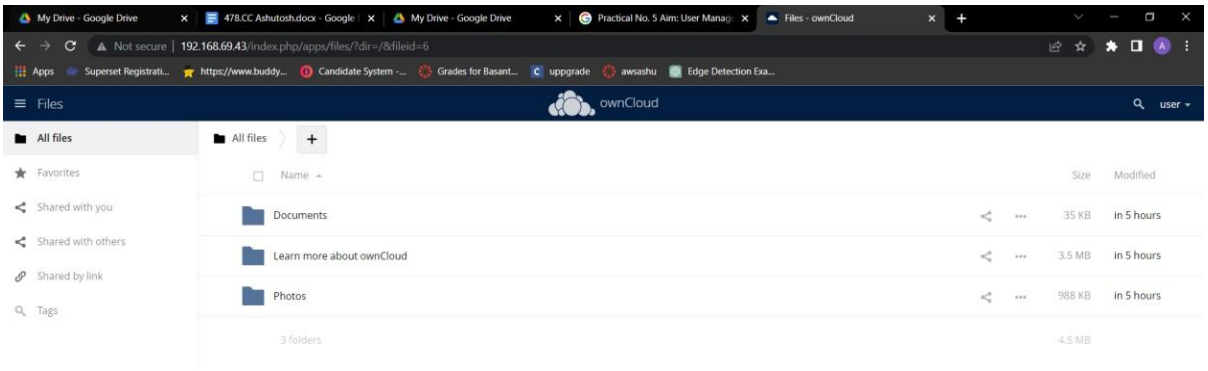


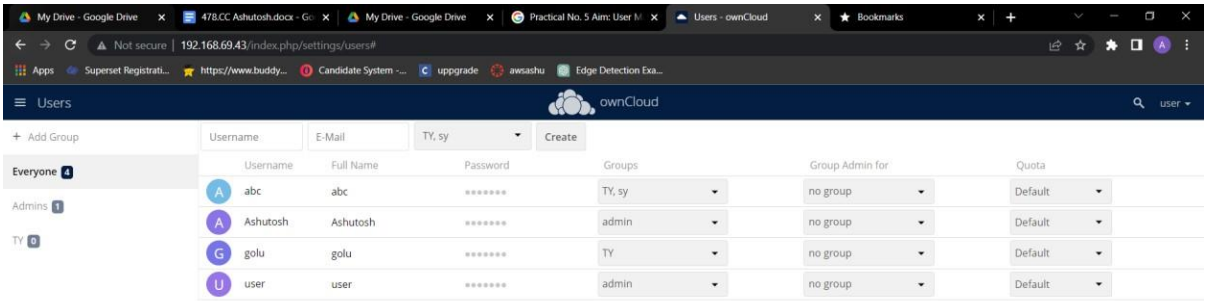

bitnami-owncloud [Running] - Oracle VM VirtualBox
*** You can access the application at http://192.168.69.43 ***
*** The default username and password is 'user' and 'n1xCJ9ZNdR8J'. ***
*** You can find out more at https://docs.bitnami.com/virtual-machine/apps/owncloud/ ***
To access the console, please 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/vms/ ***
* Please insert the new user password *
* The default password is 'bitnami' *
Changing password for bitnami.
Current password:

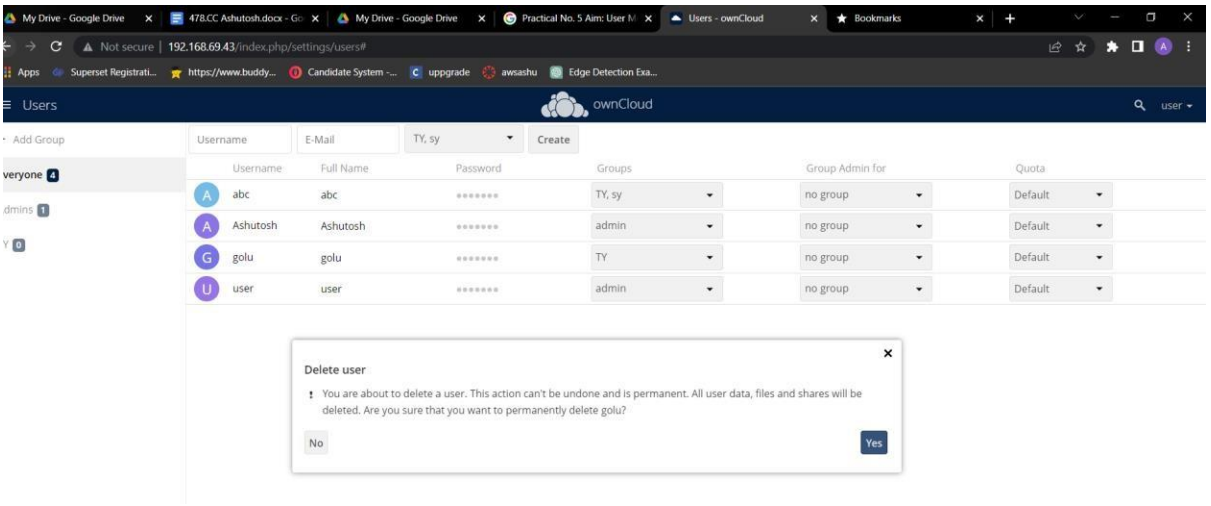

My Drive - Google Drive
478.CC Ashutosh.docx - Google
My Drive - Google Drive
Not secure | 192.168.69.43/index.php/login


ownCloud
Username or email
user
Password
Login
ownCloud - A safe home for all your data

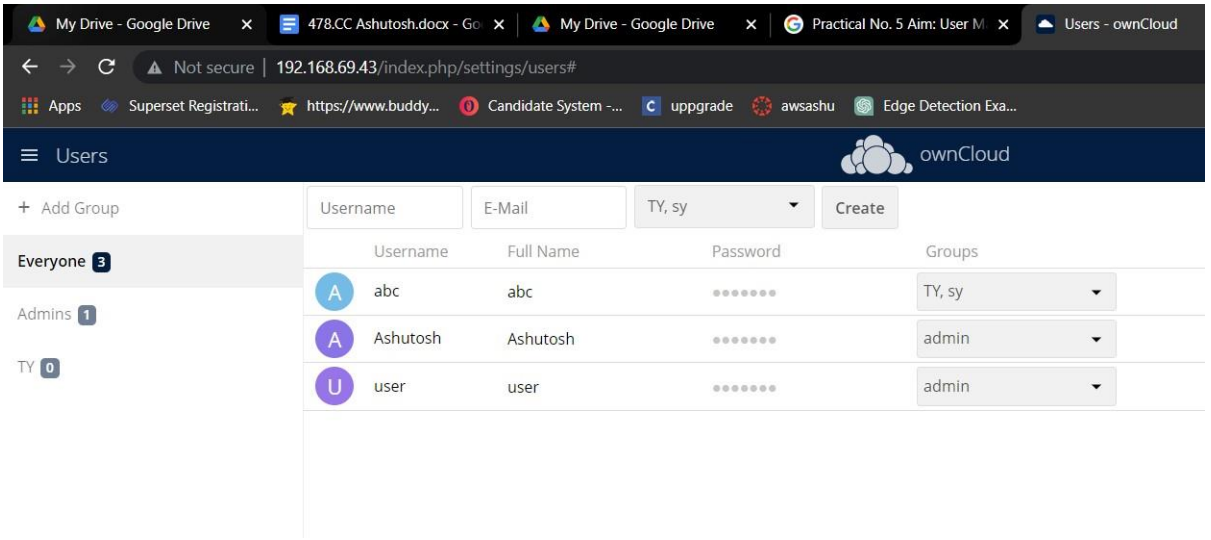

Files - ownCloud
192.168.69.43/index.php/apps/files/?dir=/&fileid=6
ownCloud
A safe home for all your data
Access & share your files, calendars, contacts, mail & more from any device, on your terms
Get the apps to sync your files
Desktop app
ANDROID APP ON Google Play
Download on the App Store
Connect your desktop apps to ownCloud
Connect your Calendar
Connect your Contacts
Access files via WebDAV
© 2023 ownCloud


Files - ownCloud
192.168.69.43/index.php/apps/files/?dir=/&fileid=6
Files
ownCloud
user
All files
Favorites
Shared with you
Shared with others
Shared by link
Tags
Name
Size
Modified
Documents
35 KB
in 5 hours
Learn more about ownCloud
3.5 MB
in 5 hours
Photos
988 KB
in 5 hours
3 folders
4.5 MB

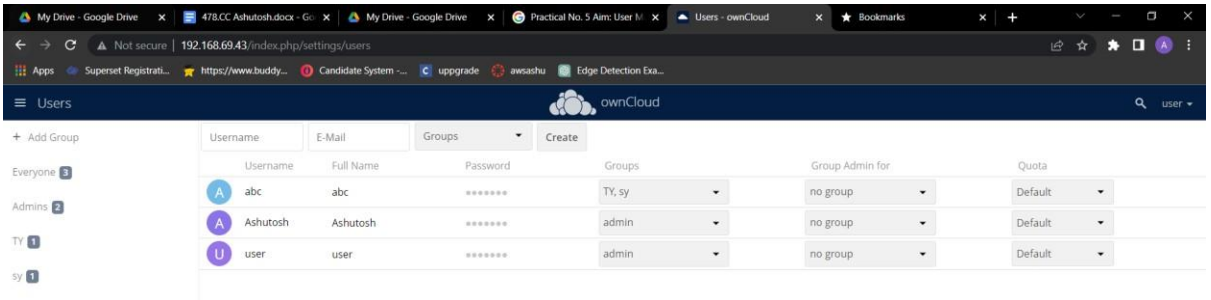

Users - ownCloud
192.168.69.43/index.php/settings/users#
Users
ownCloud
user
Add Group
Everyone 4
Admins 1
TY 0
Username
E-Mail
TY, sy
Create
Username
Full Name
Password
Groups
Group Admin for
Quota
abc
abc
TY, sy
no group
Default
Ashutosh
Ashutosh
admin
no group
Default
golu
golu
TY
no group
Default
user
user
admin
no group
Default

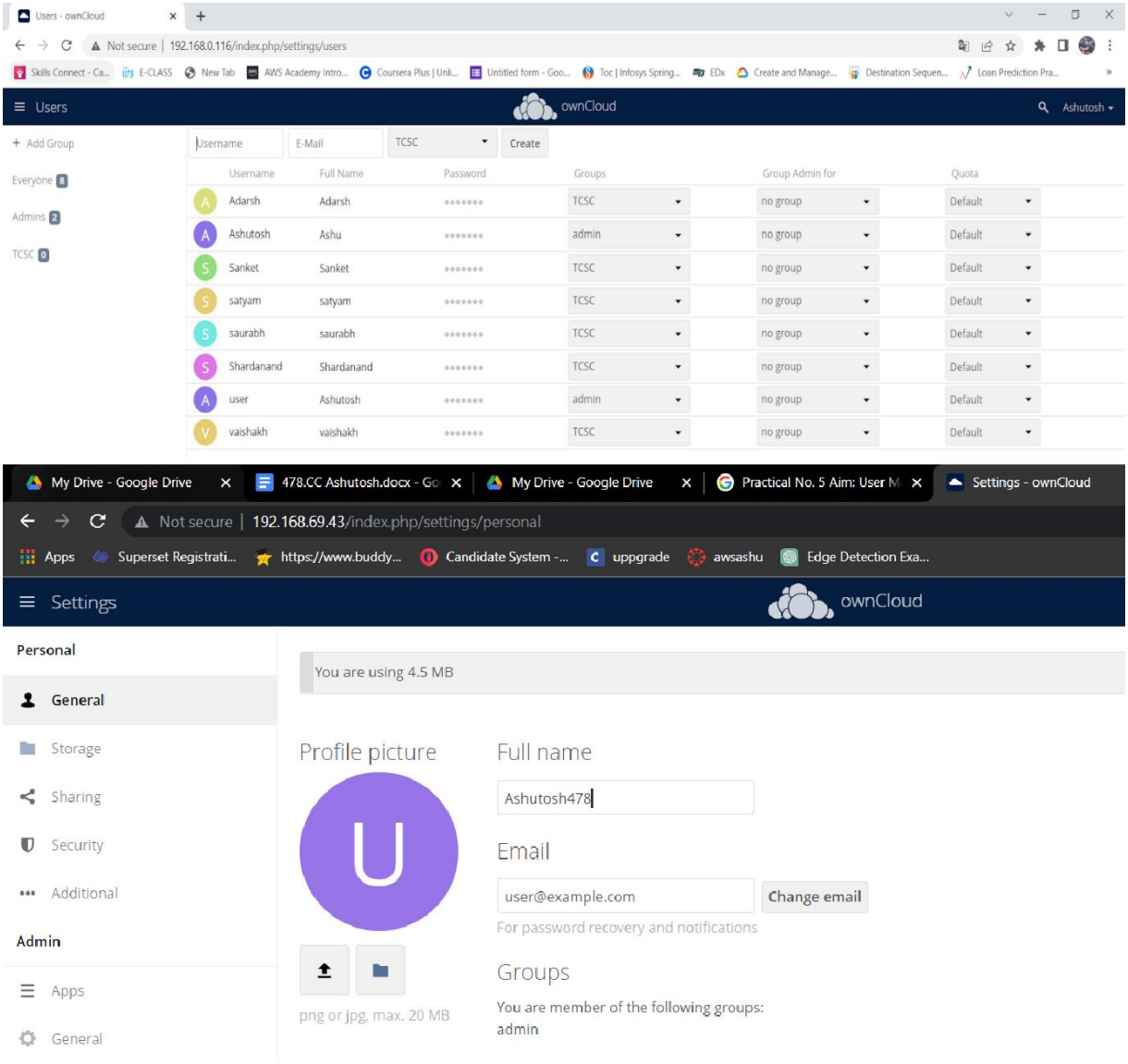


DELETE USER GOLU:



USERS :





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**

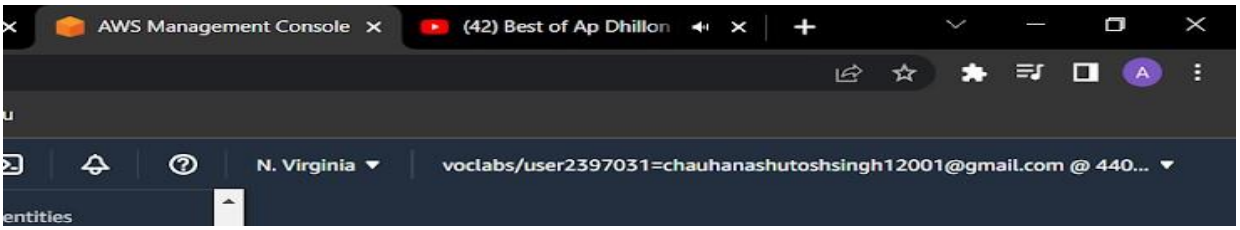
   You can allow users who already have passwords elsewhere—for example, in your corporate network or with an internet identity provider—to get temporary access to your AWS account.

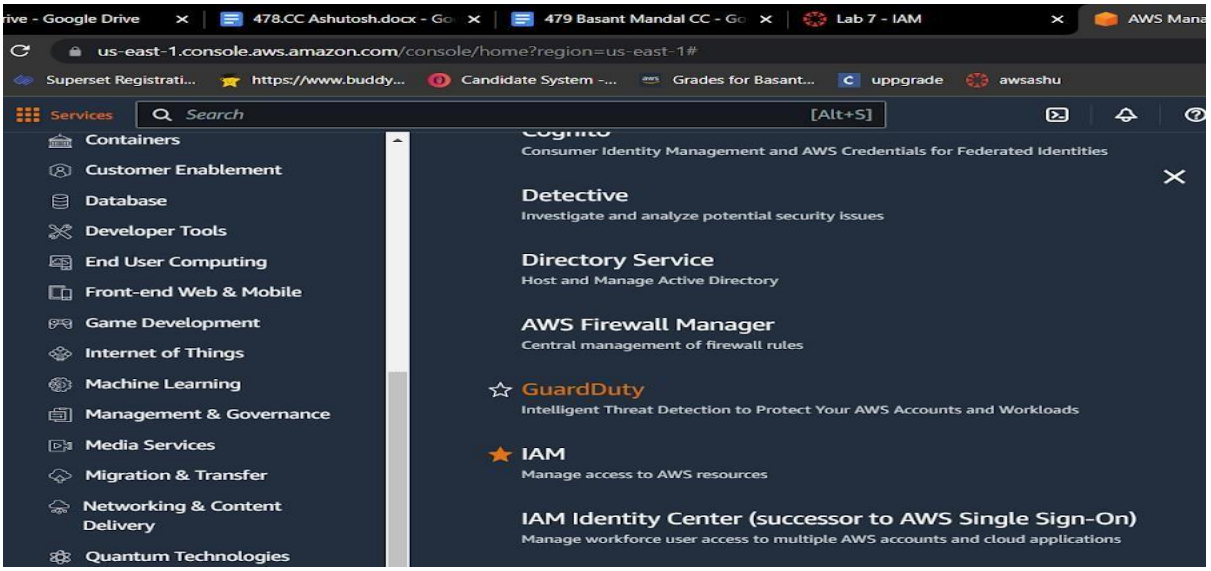
5. **Free to use**

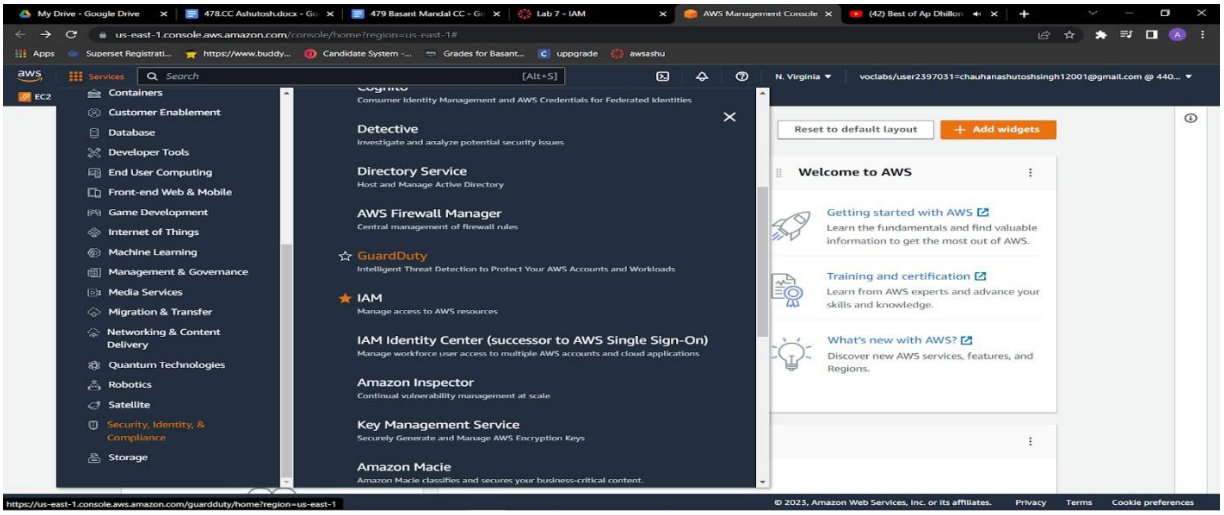
   AWS Identity and Access Management (IAM) and AWS Security Token Service (AWS STS) are features of your AWS account offered at no additional charge. You are charged only when you access other AWS services using your IAM users or AWS STS temporary security credentials

Steps:

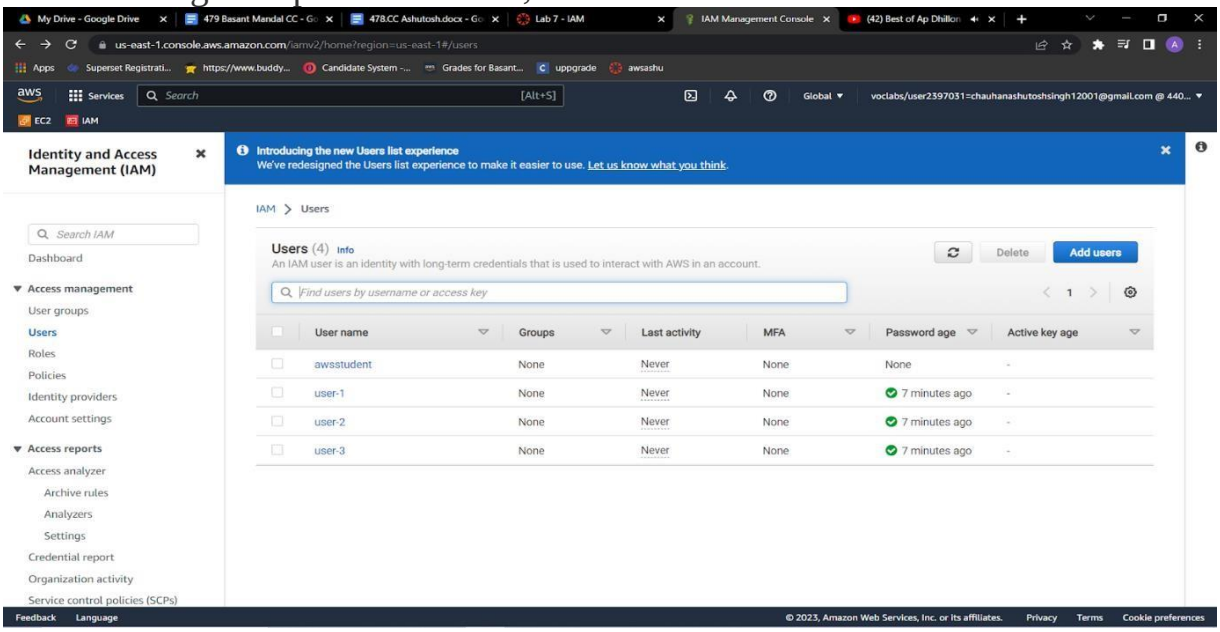
1. Choose the **Services** menu, locate the **Security, Identity, & Compliance** services, and choose **IAM**



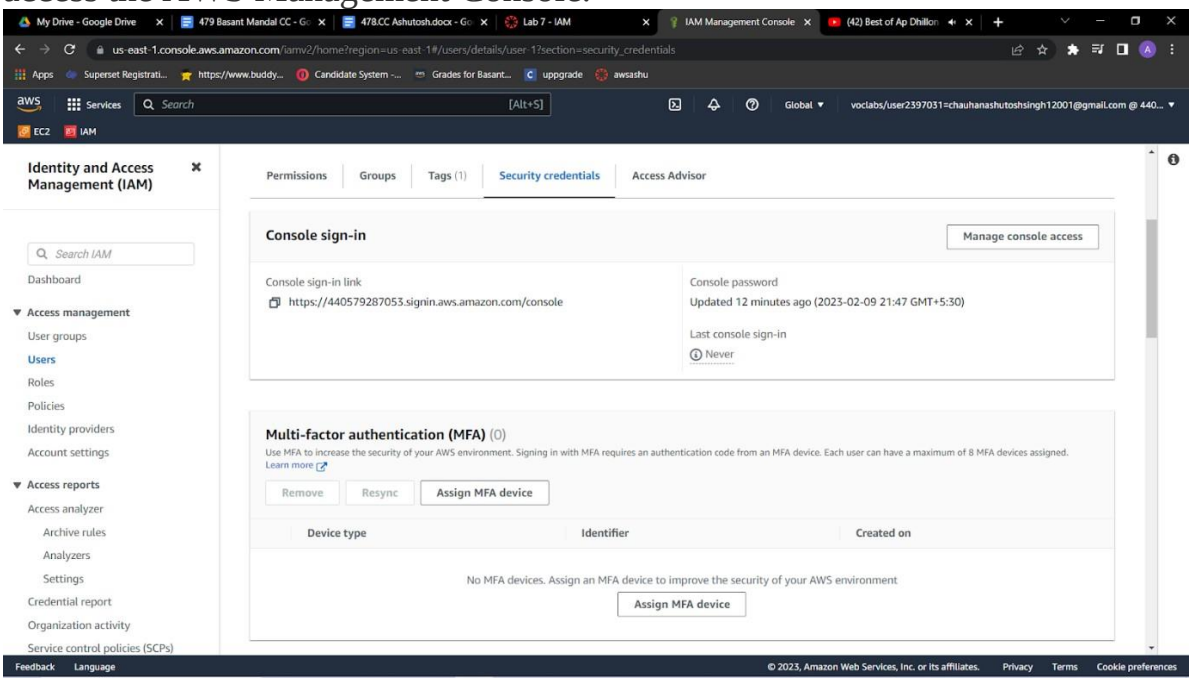




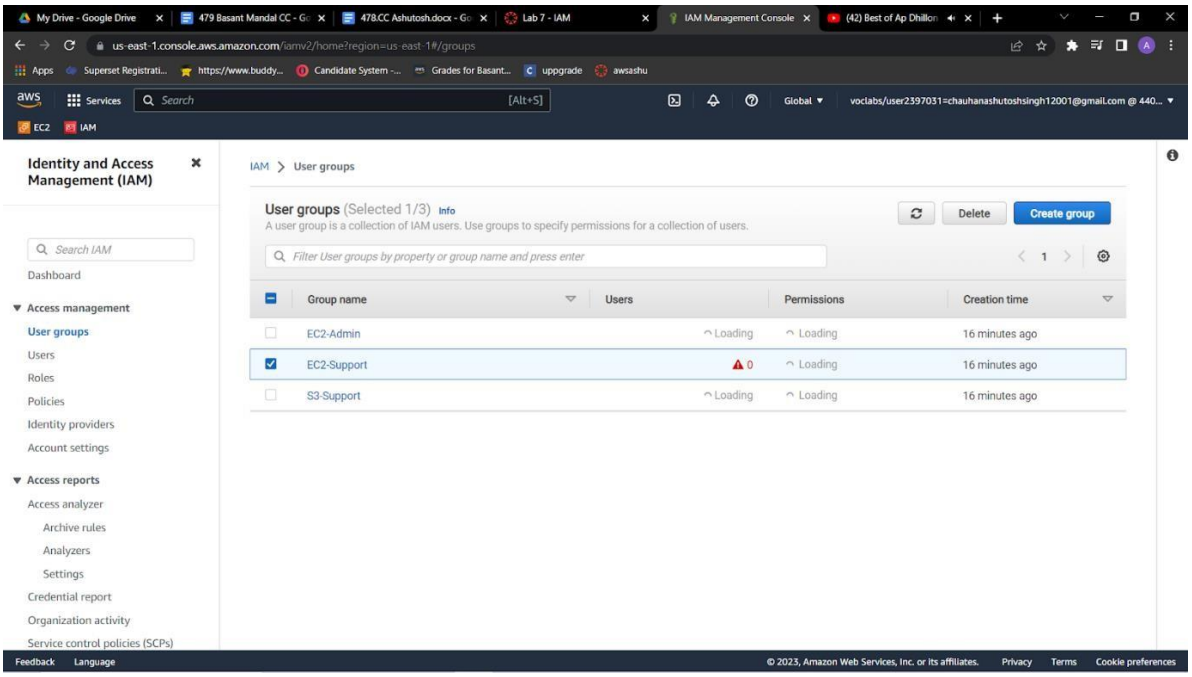
2. In the navigation pane on the left, choose **Users**.Create Users



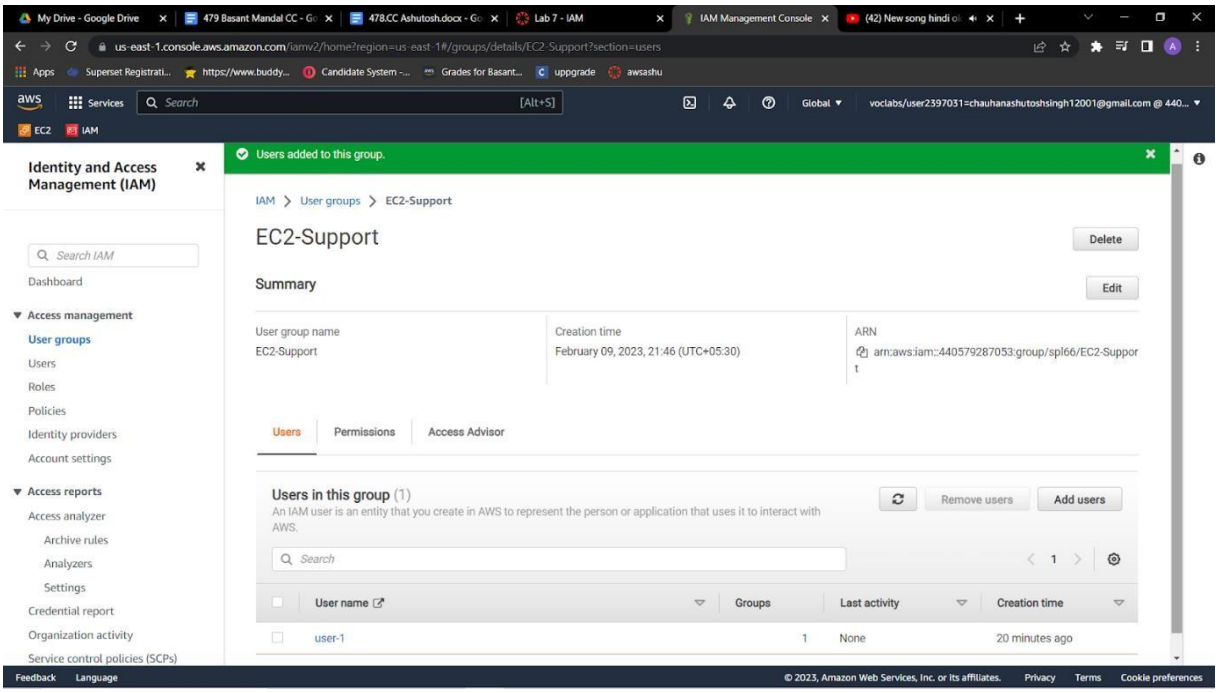
3. Choose the **Security credentials** tab.
Notice that user-1 is assigned a **Console password**. This allows the user to access the AWS Management Console.



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

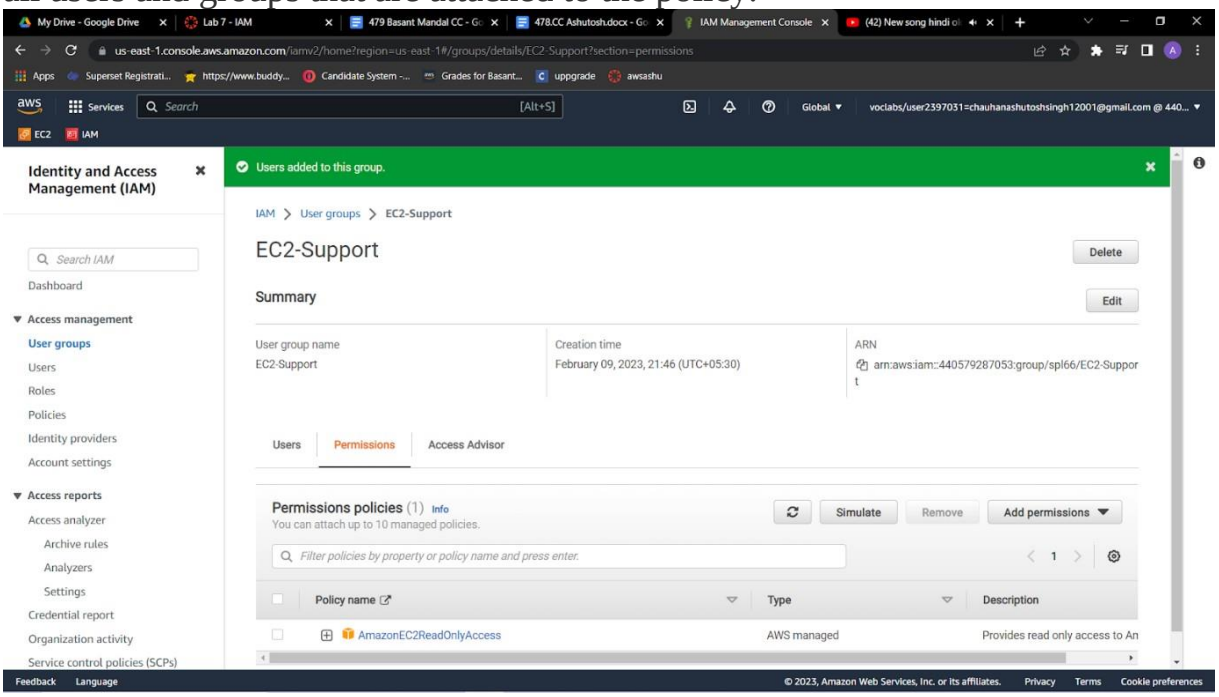


5. Choose the name of the **EC2-Support** group.
This brings you to the summary page for the **EC2-Support** group.

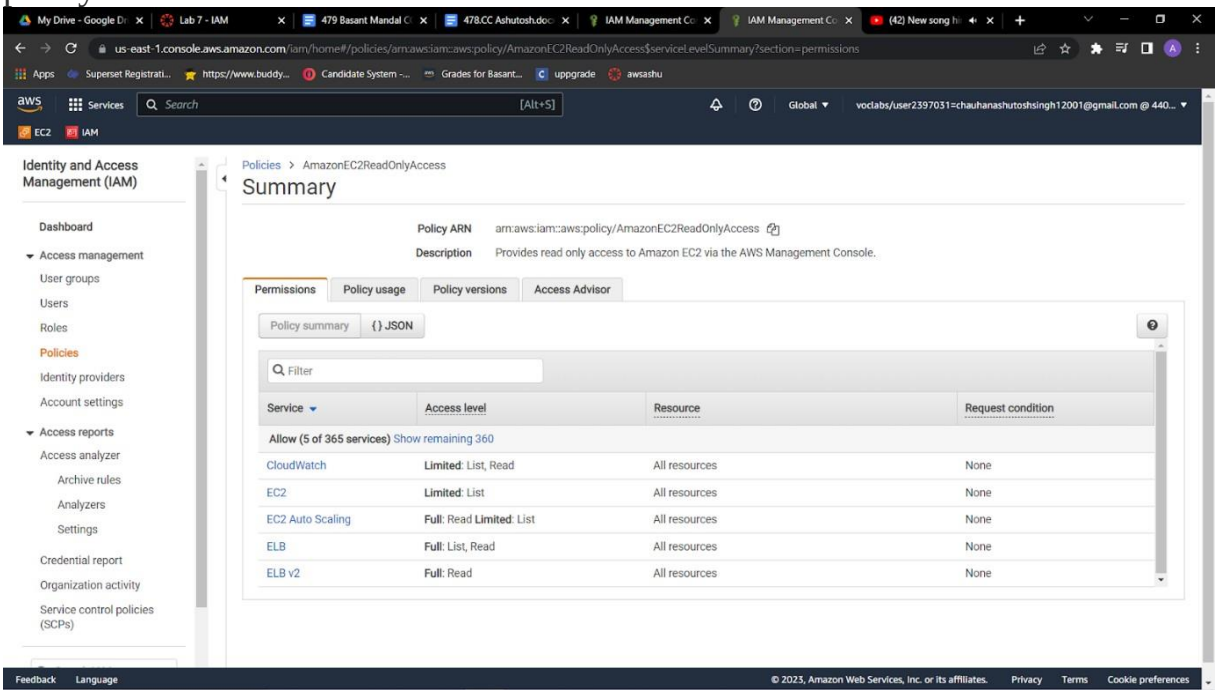


6. Choose the **Permissions** tab.
This group has a managed policy called **AmazonEC2ReadOnlyAccess** associated with it. Managed policies are prebuilt policies (built either by AWS or by your administrators) that can be attached to IAM users and groups. When the policy is updated, the changes to the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

all users and groups that are attached to the policy.



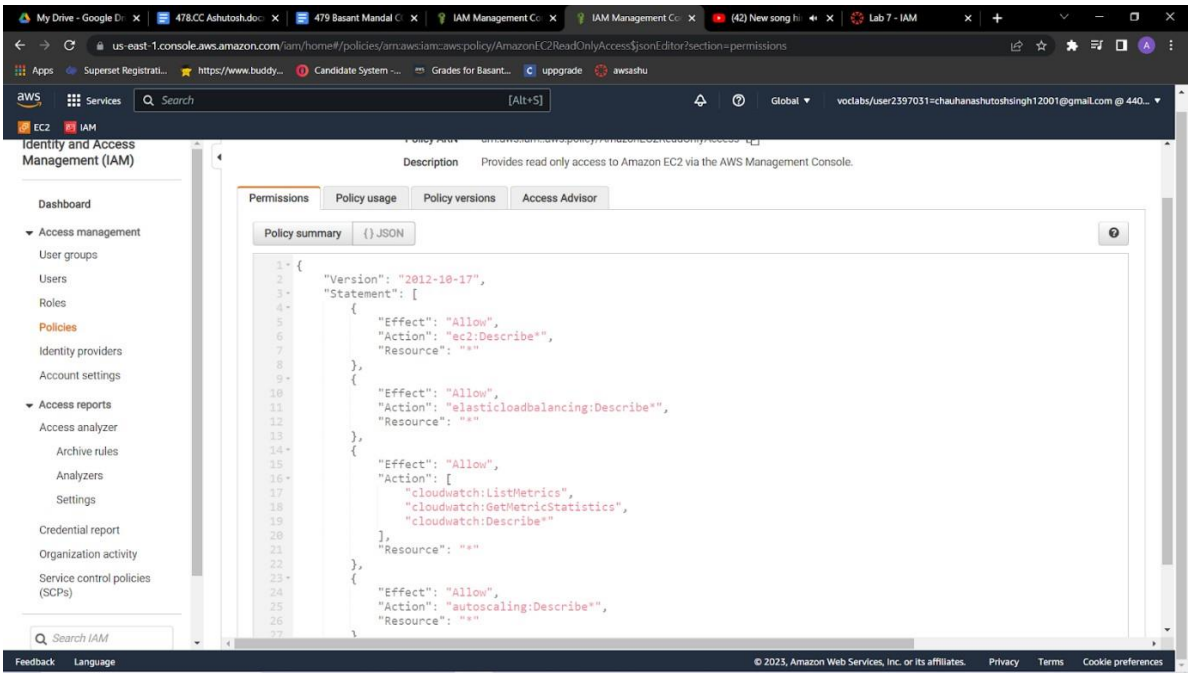
7. Under **Policy Name**, choose the link for the **AmazonEC2ReadOnlyAccess** policy.



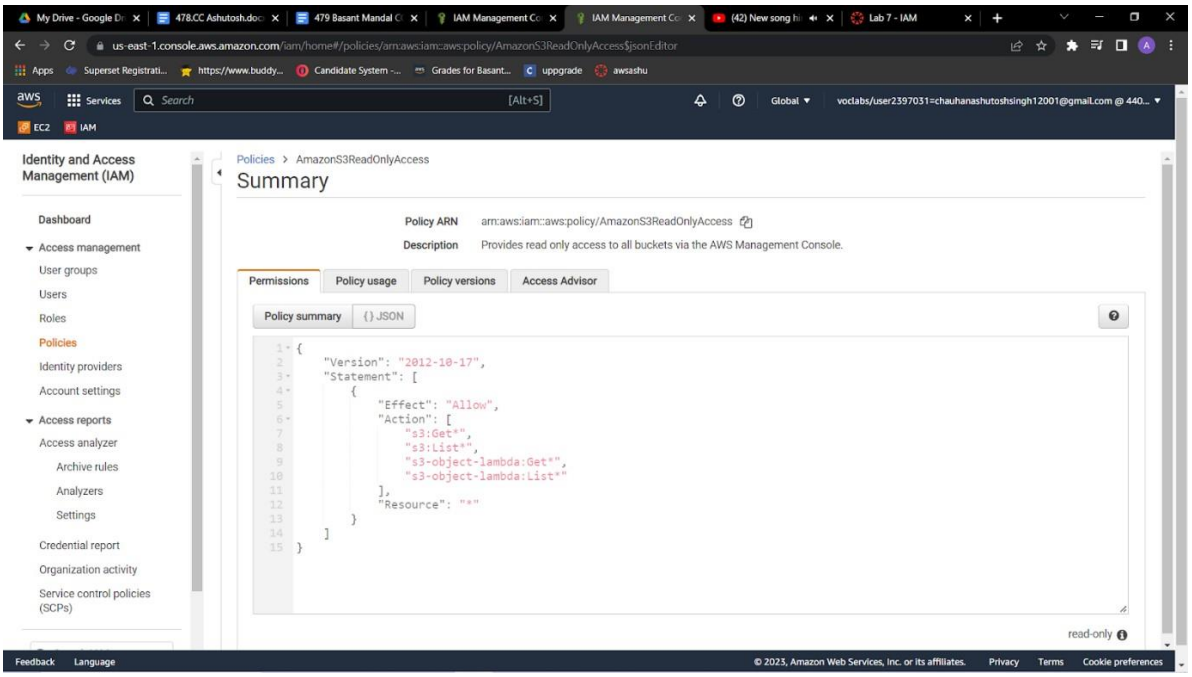
7. Choose the **{} JSON** tab.

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.

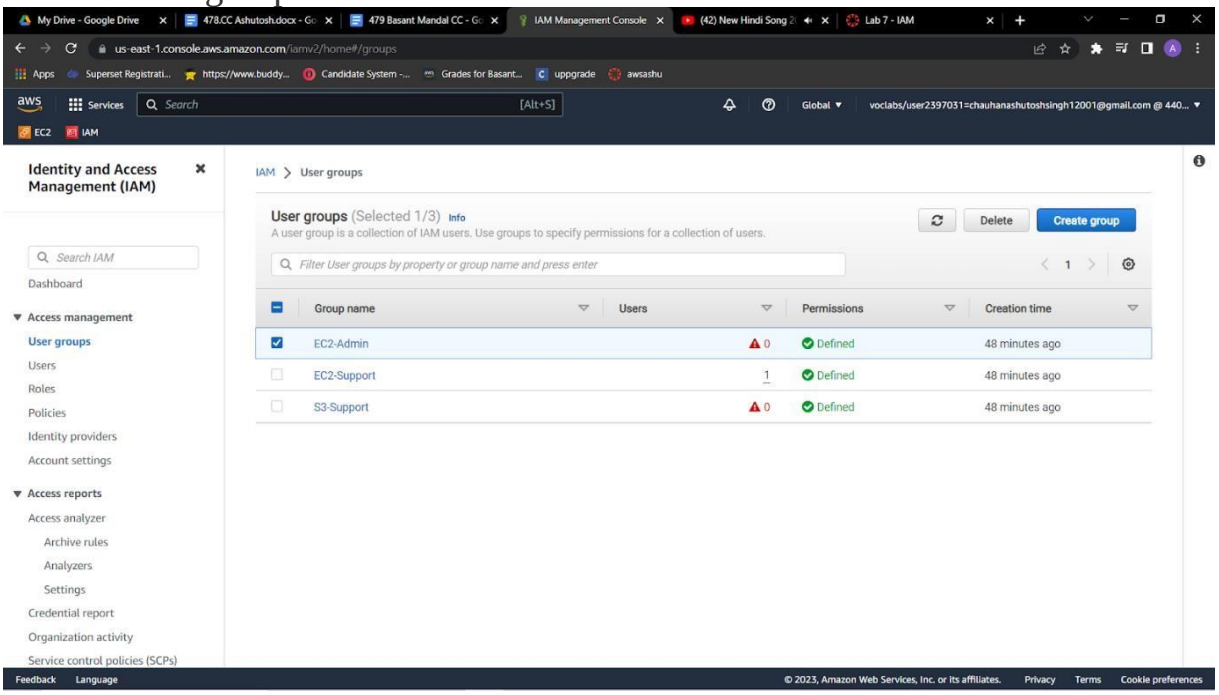
- Statements in an IAM policy have the following basic structure:
  - **Effect** says whether to *Allow* or *Deny* the permissions.
  - **Action** specifies the API calls that can be made against an AWS service (for example, *cloudwatch:ListMetrics*).
  - **Resource** defines the scope of entities covered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



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.



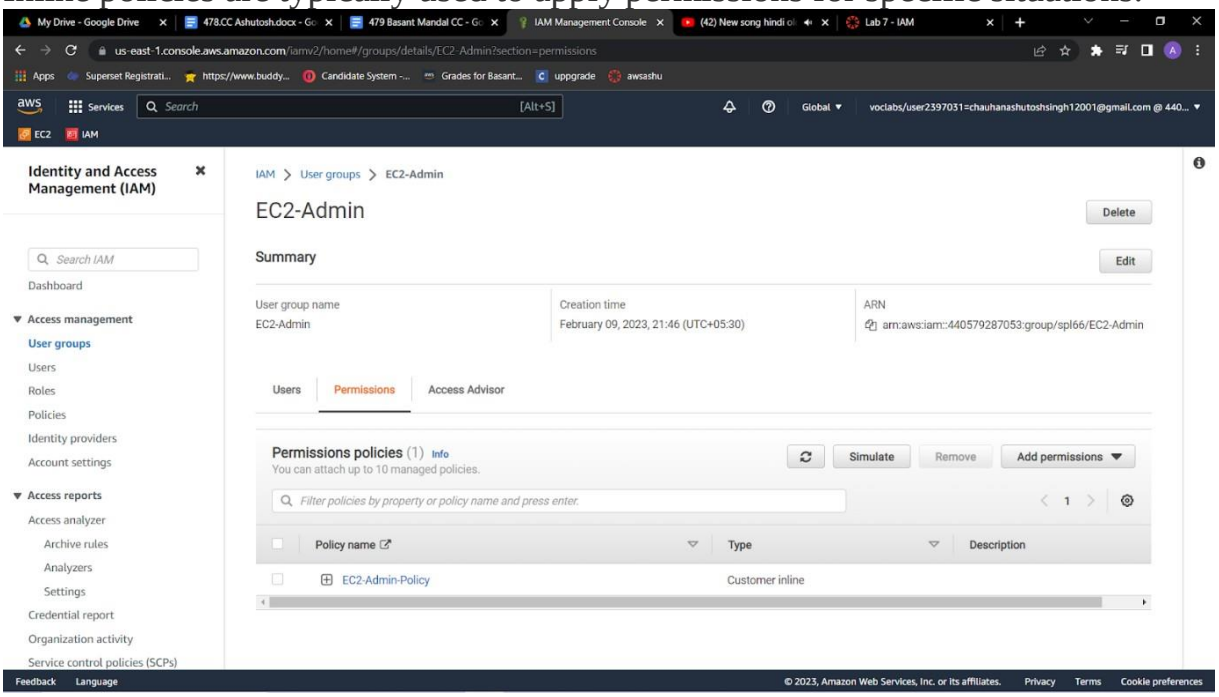
9. In the navigation pane on the left, choose **User groups**.Choose the name of the **EC2-Admin** group.



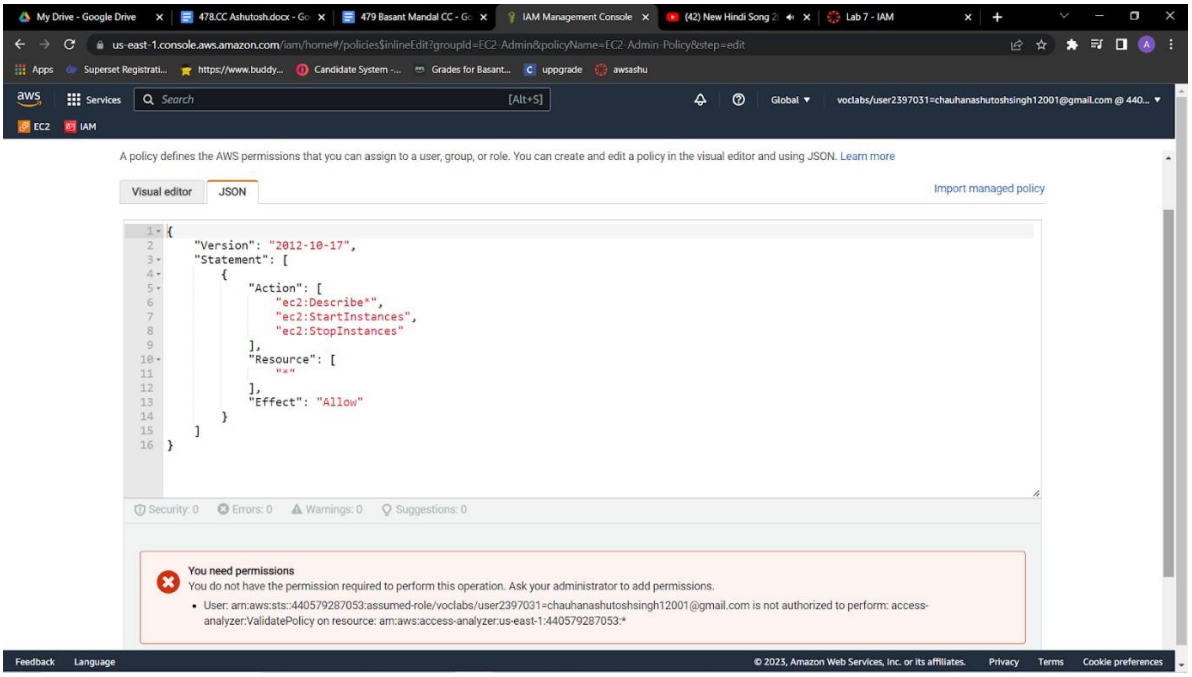
10. Choose the **Permissions** tab.

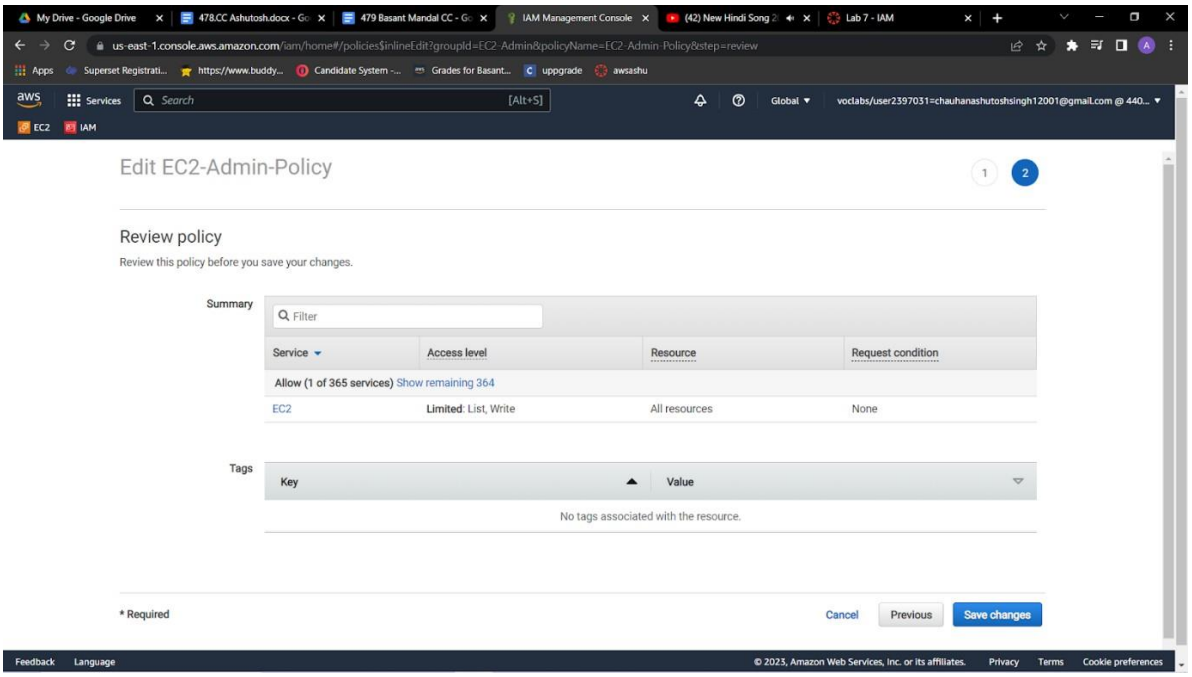
This group is different from the other two. Instead of a managed policy, the group has an *inline policy*, which is a policy assigned to just one user or group.

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



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.

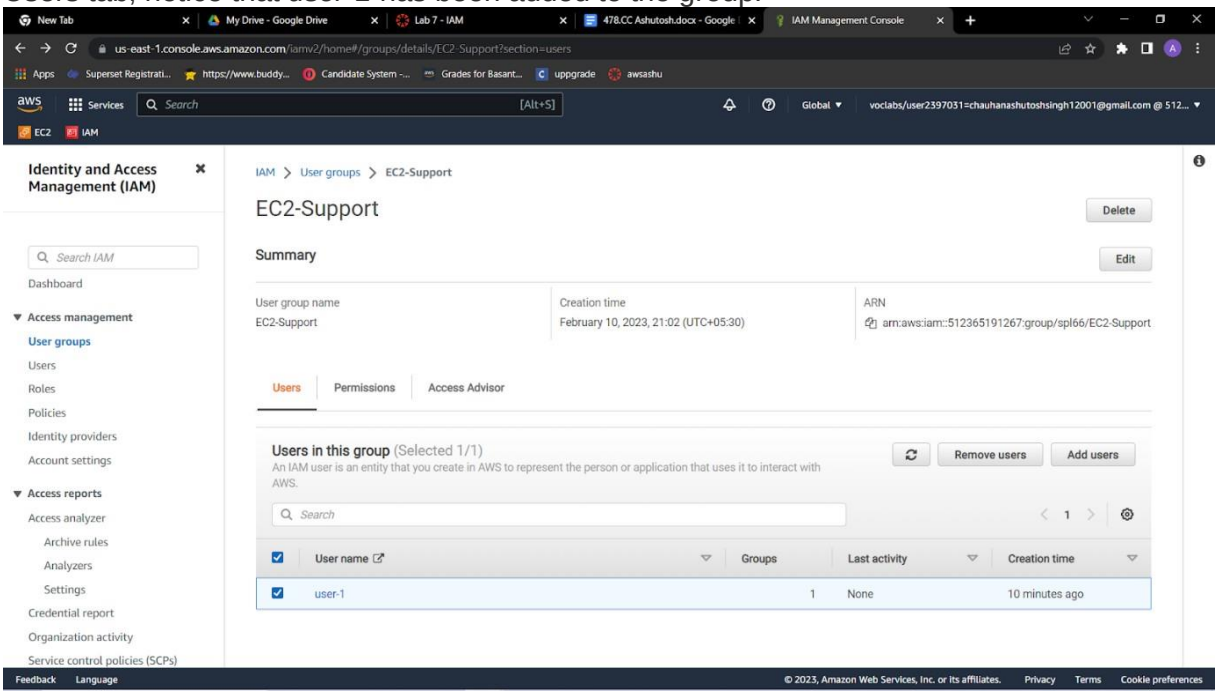




12. At the bottom of the screen, choose **Cancel** to close the policy.

Add user-1 to the S3-Support group

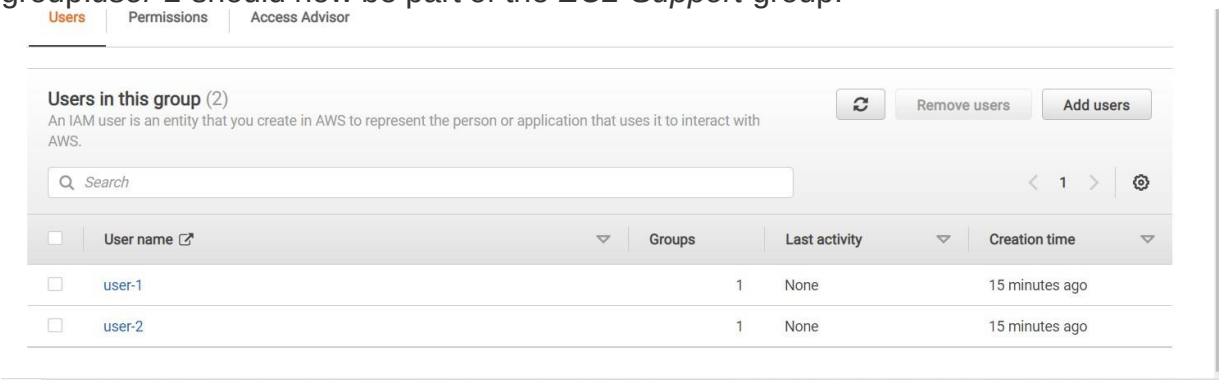
13. In the left navigation pane, choose User groups.Choose the name of the S3-Support group.On the Users tab, choose Add users.Select user-1, and choose Add usersOn the Users tab, notice that *user-1* has been added to the group.



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.

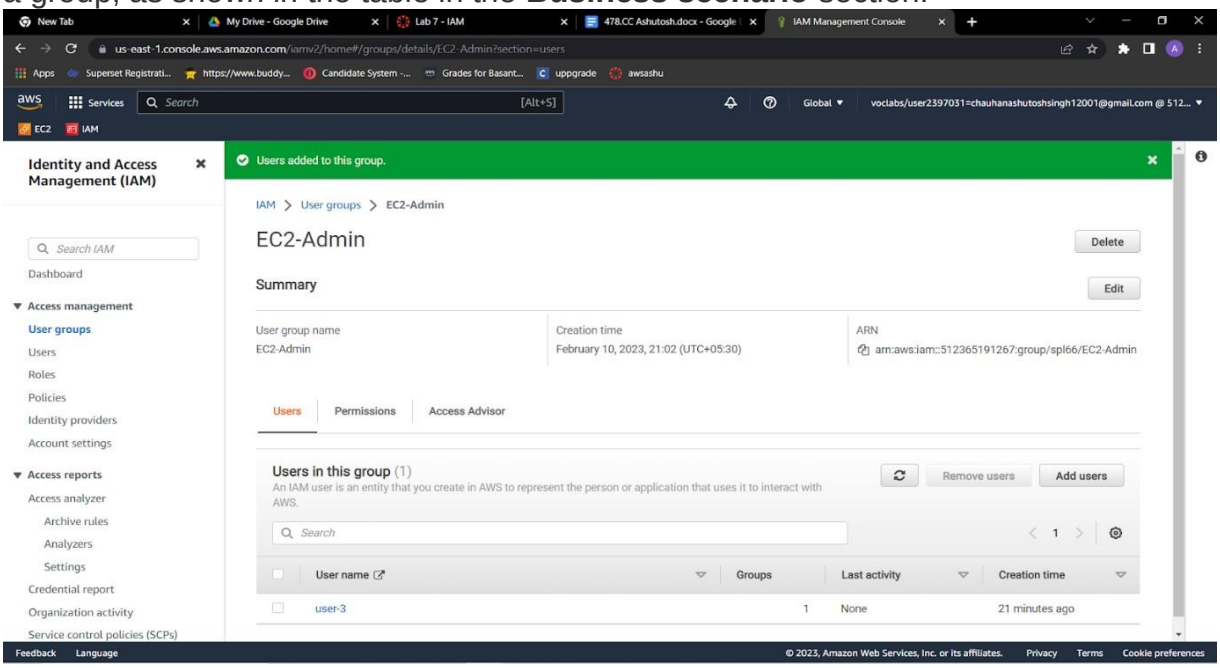
14. Use what you learned from the previous steps to add *user-2* to the *EC2-Support* group.*user-2* should now be part of the *EC2-Support* group.



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.

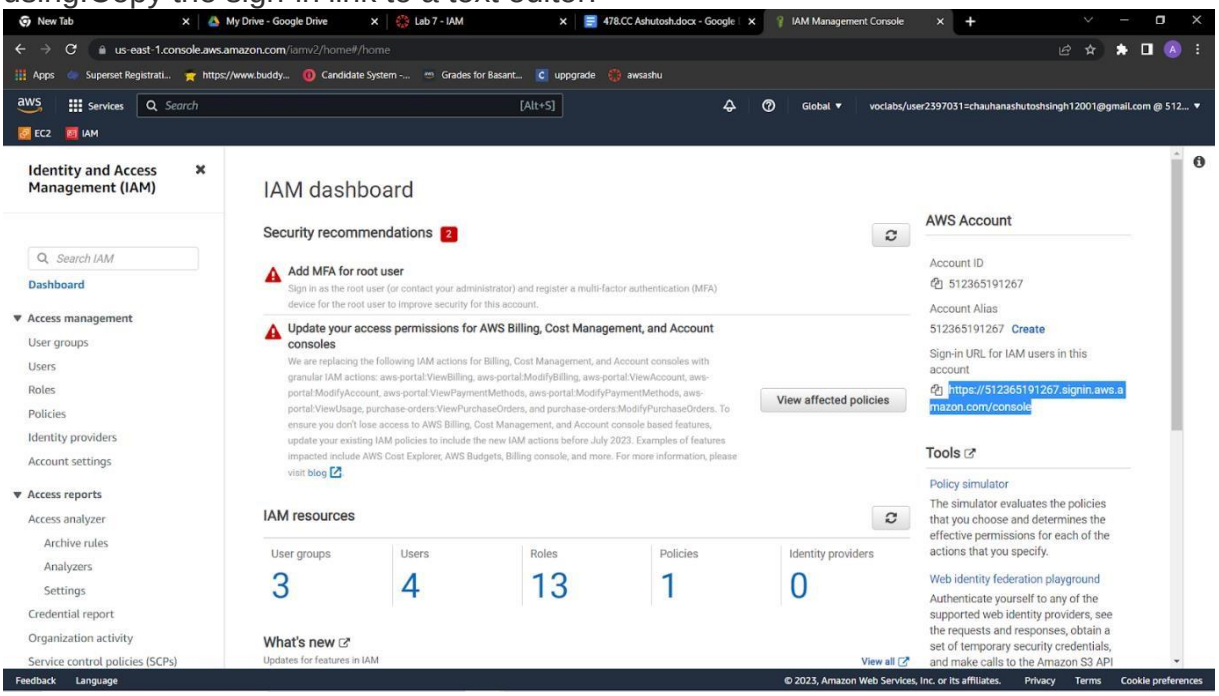


Sign in and test users

Get the console sign-in URL

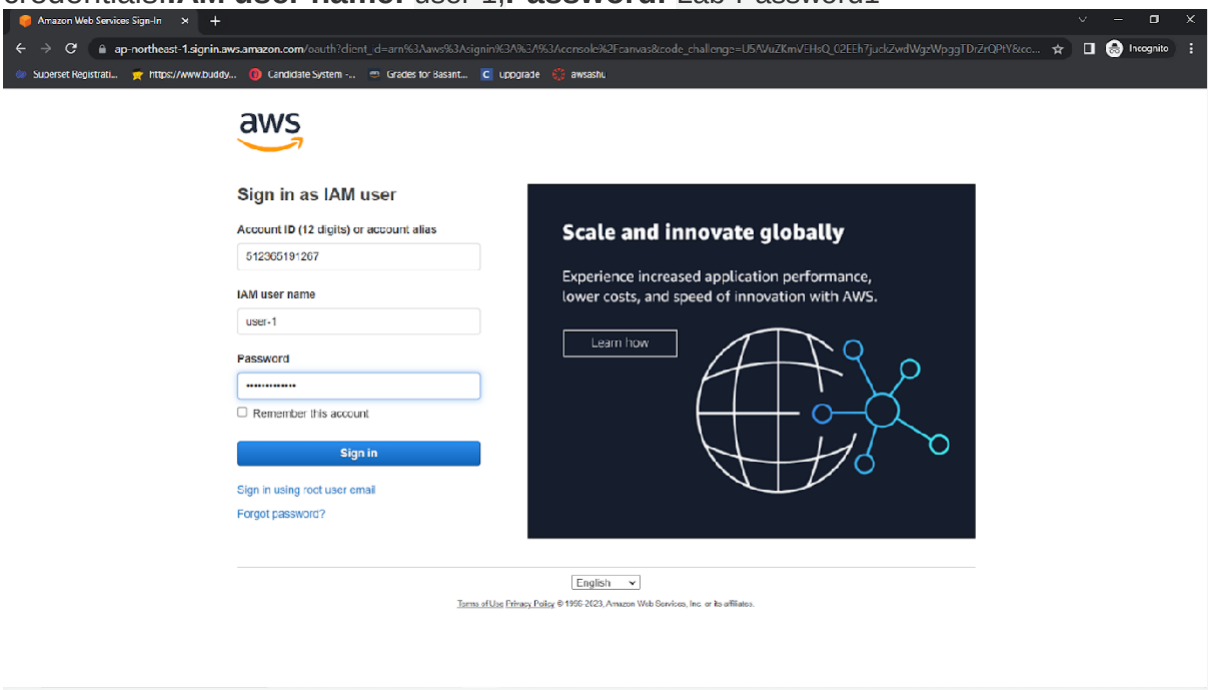
16. In the navigation pane on the left, choose Dashboard.Notice the Sign-in URL for IAM users in this account section at the top of the page. The sign-in URL looks similar to the following: https://123456789012.signin.aws.amazon.com/console

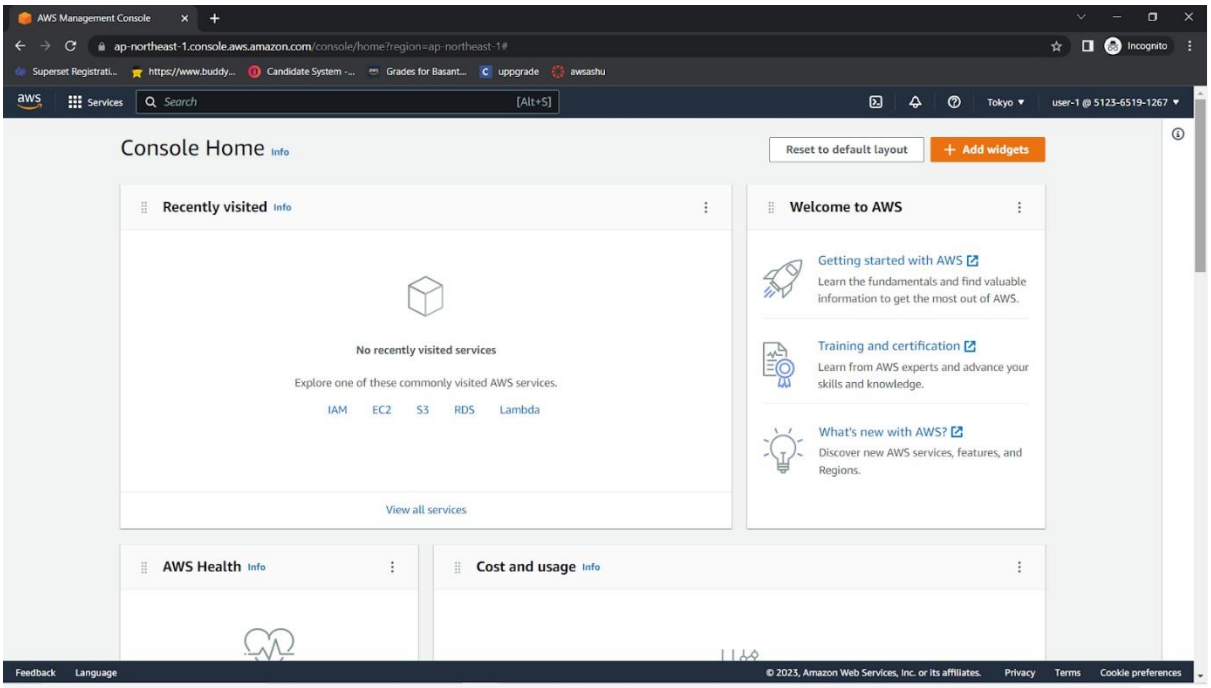
This link can be used to sign in to the AWS account that you are currently using.Copy the sign-in link to a text editor.



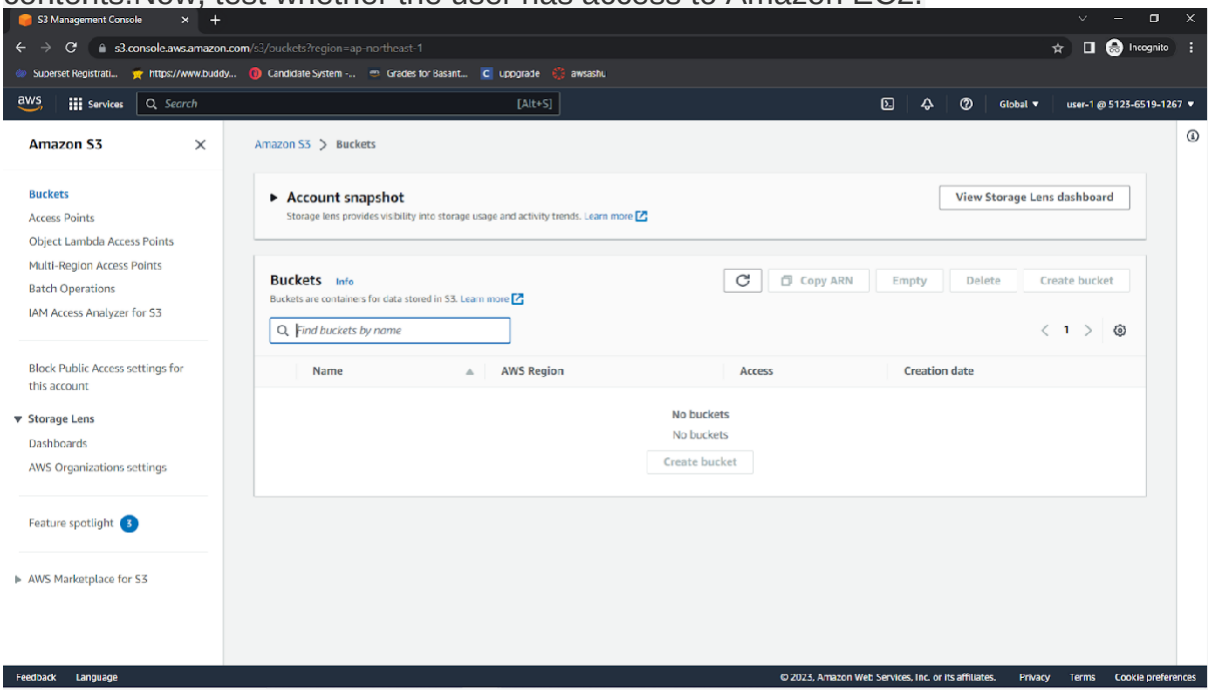
Test user-1 permissions

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

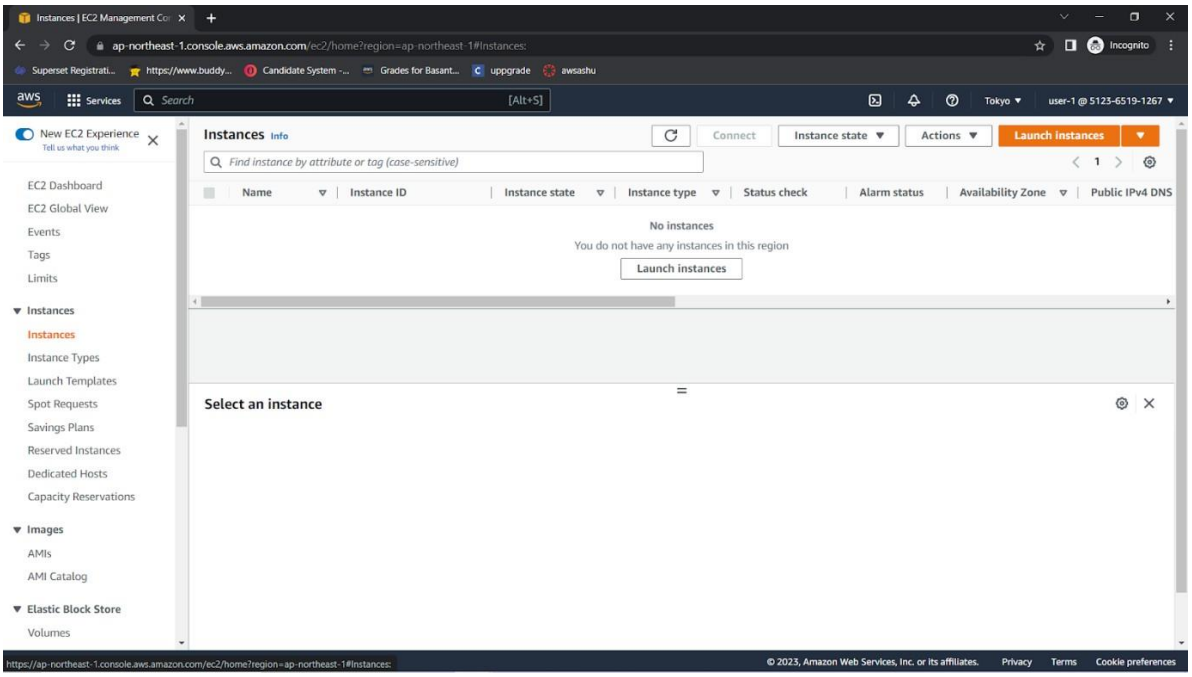




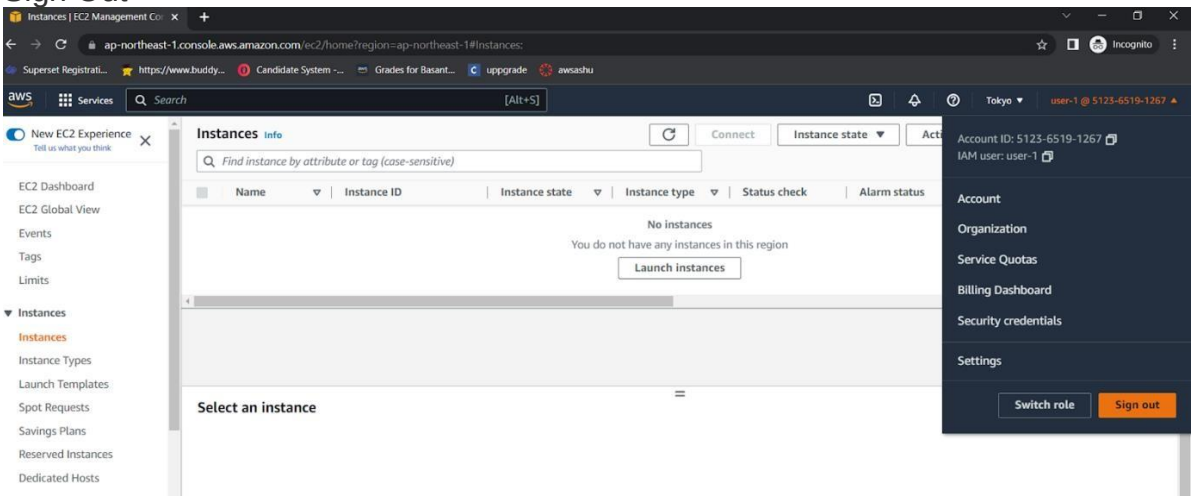
18.Choose the **Services** menu, and choose **S3**.Choose the name of one of your buckets, and browse the contents.Because this user is part of the *S3-Support* group in IAM, they have permissions to view a list of Amazon S3 buckets and their contents.Now, test whether the user has access to Amazon EC2.



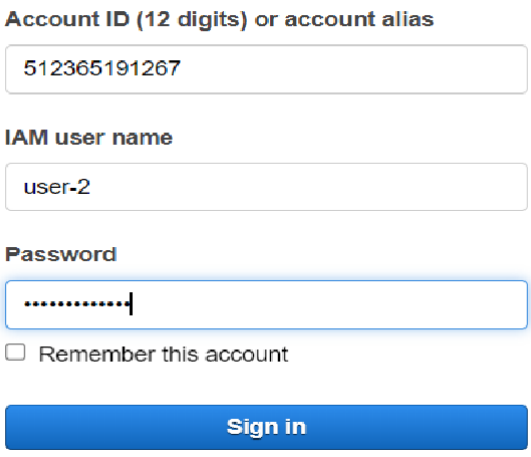
19. Choose the **Services** menu, and choose **EC2**.In the left navigation pane, choose **Instances**.You cannot see any instances. Instead, an error message says *you are not authorized to perform this operation*. This user has not been assigned any permissions to use Amazon EC2.You will now sign in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



Sign Out

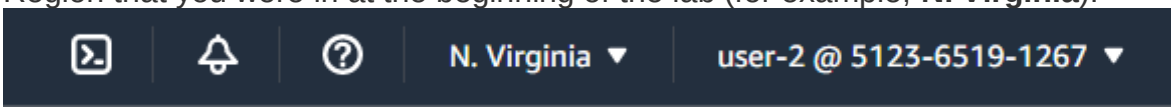


20. Paste the sign-in link into the private browser again, and press ENTER.Sign in with the following credentials:**IAM user name:** user-2 **Password:** Lab-Password2

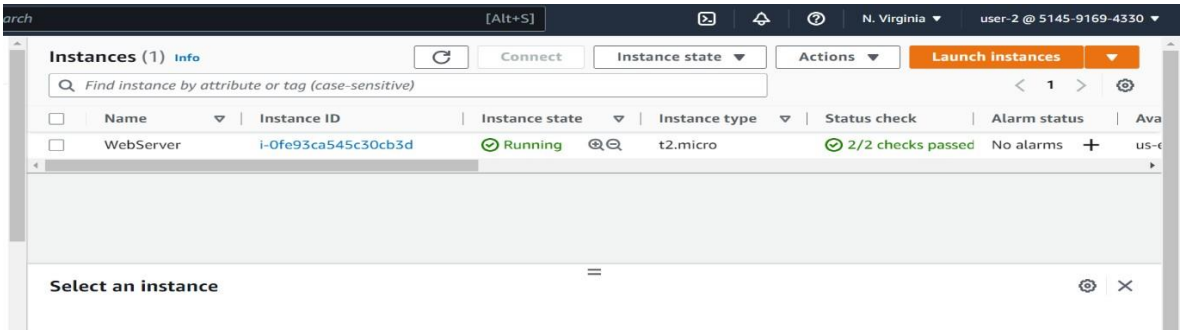


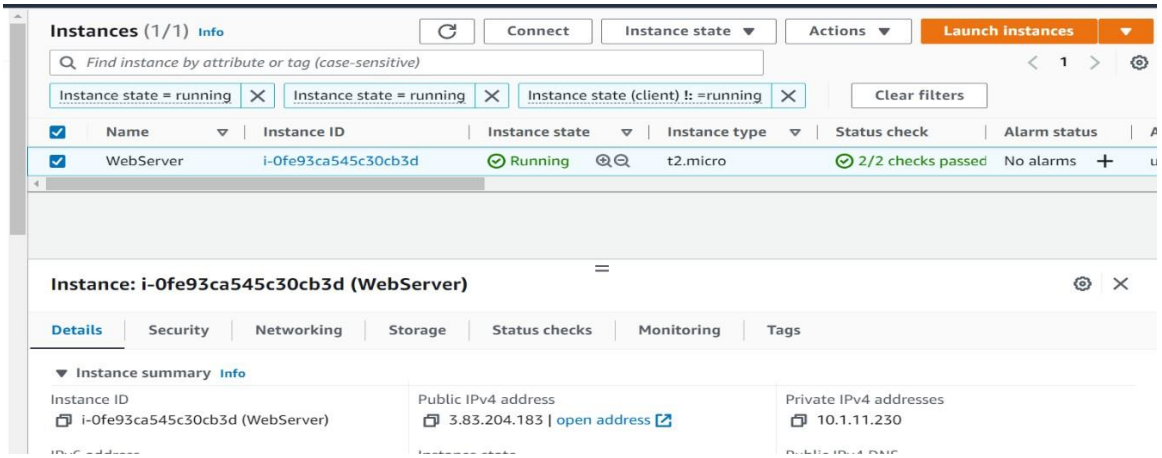
21. Choose the **Services** menu, and choose **EC2**.In the navigation pane on the left, choose **Instances**.You are now able to see an EC2 instance. However, you cannot

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

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.

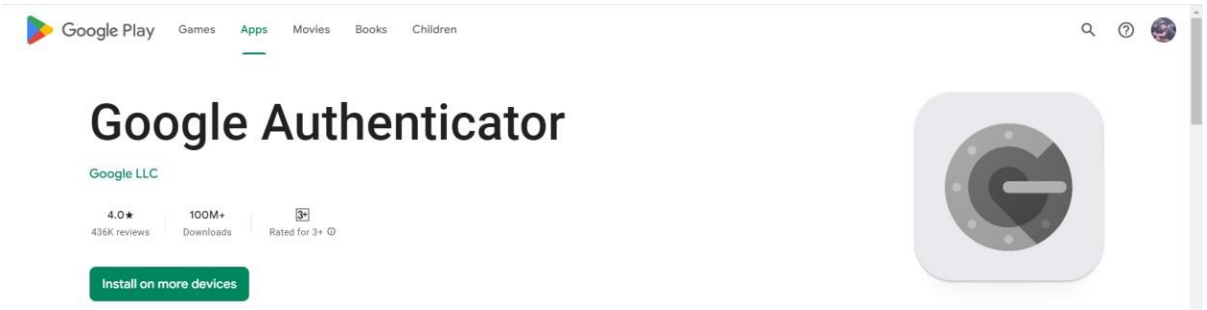
AWS offers a free MFA security key to eligible AWS account owners in the United States. To determine eligibility and order a key, see the Security Hub console.

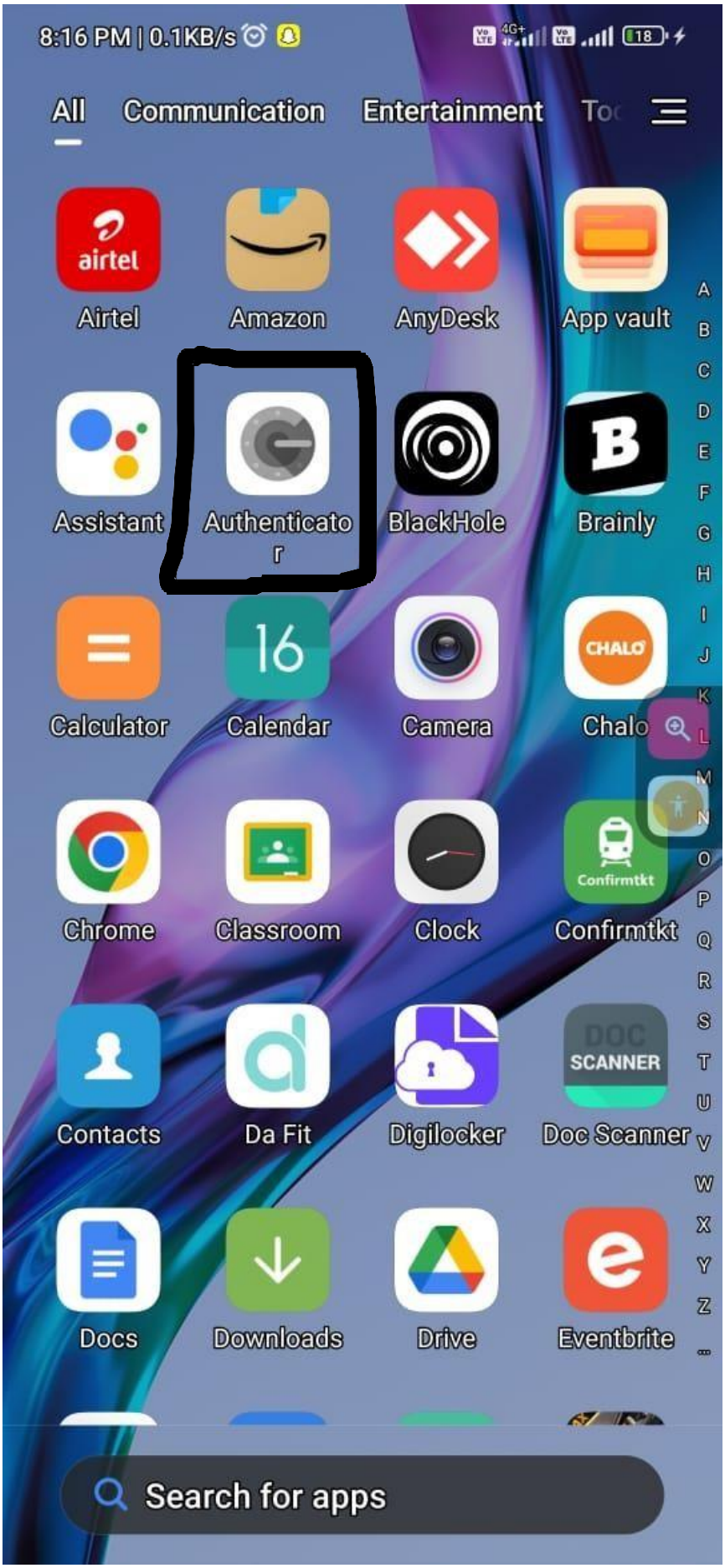
Virtual authenticator apps

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.

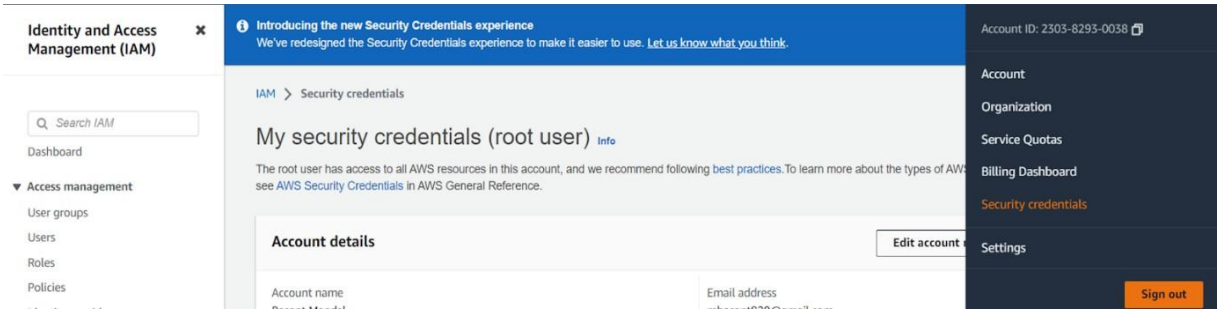
Android	Twilio Authy Authenticator, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator, Symantec VIP
iOS	Twilio Authy Authenticator, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator, Symantec VIP

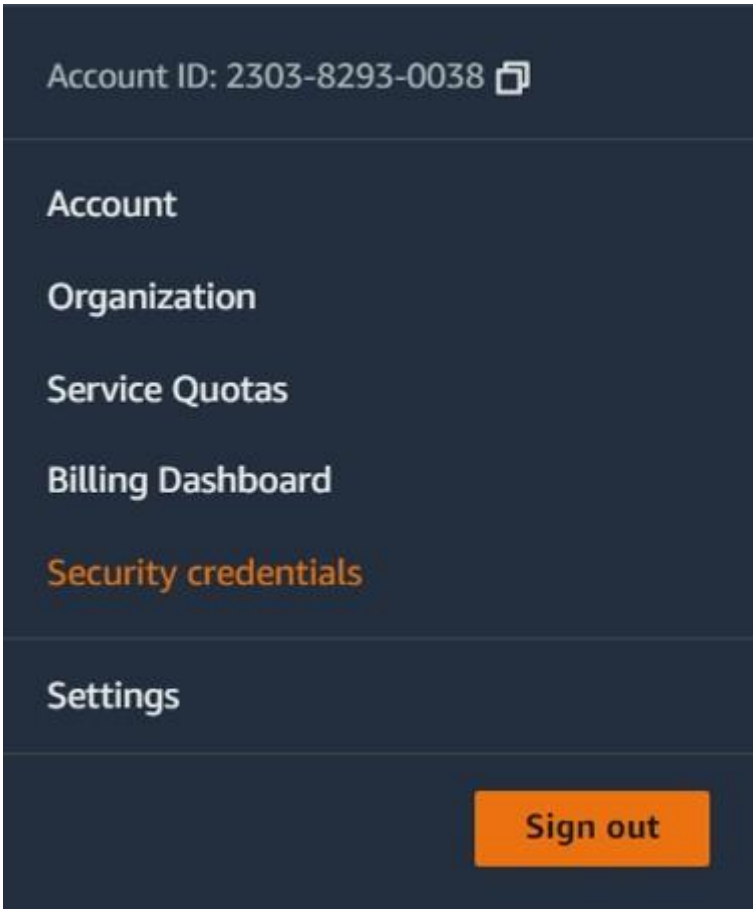
GOOGLE APP FOR AUTHENTICATION :
https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

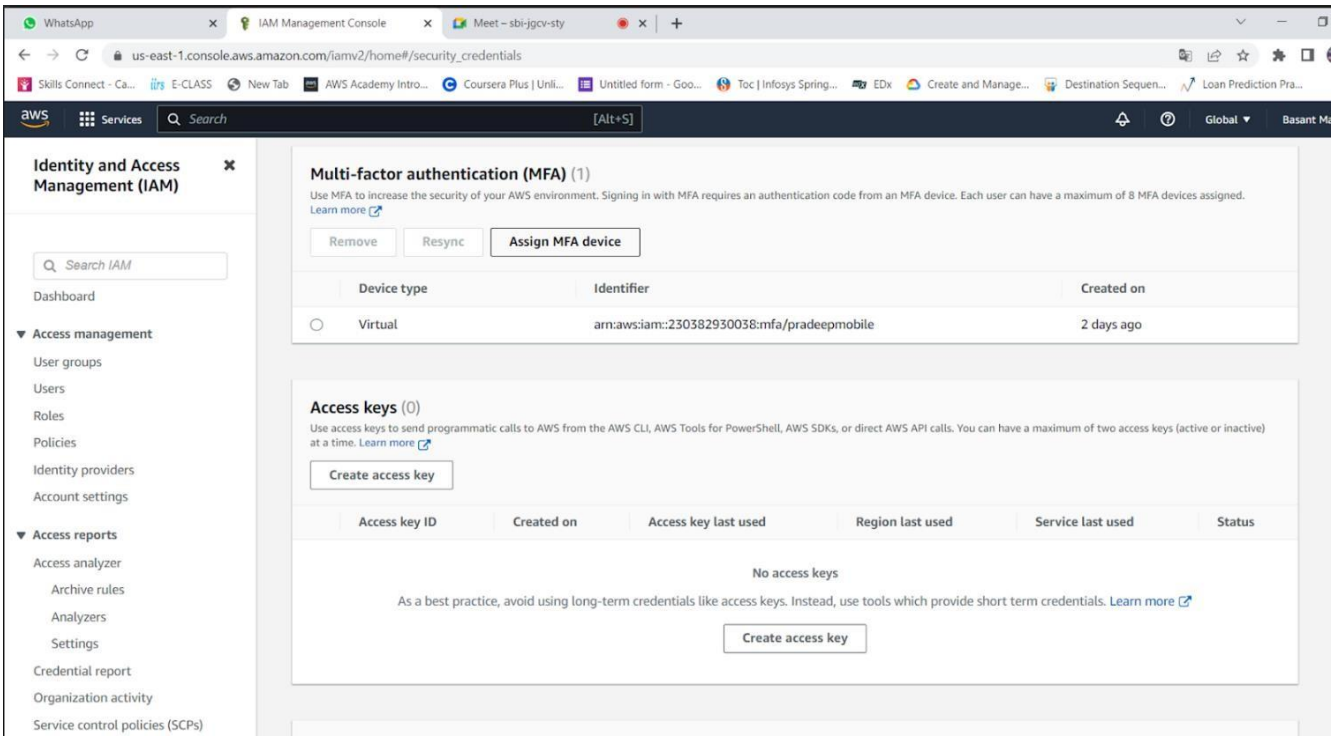


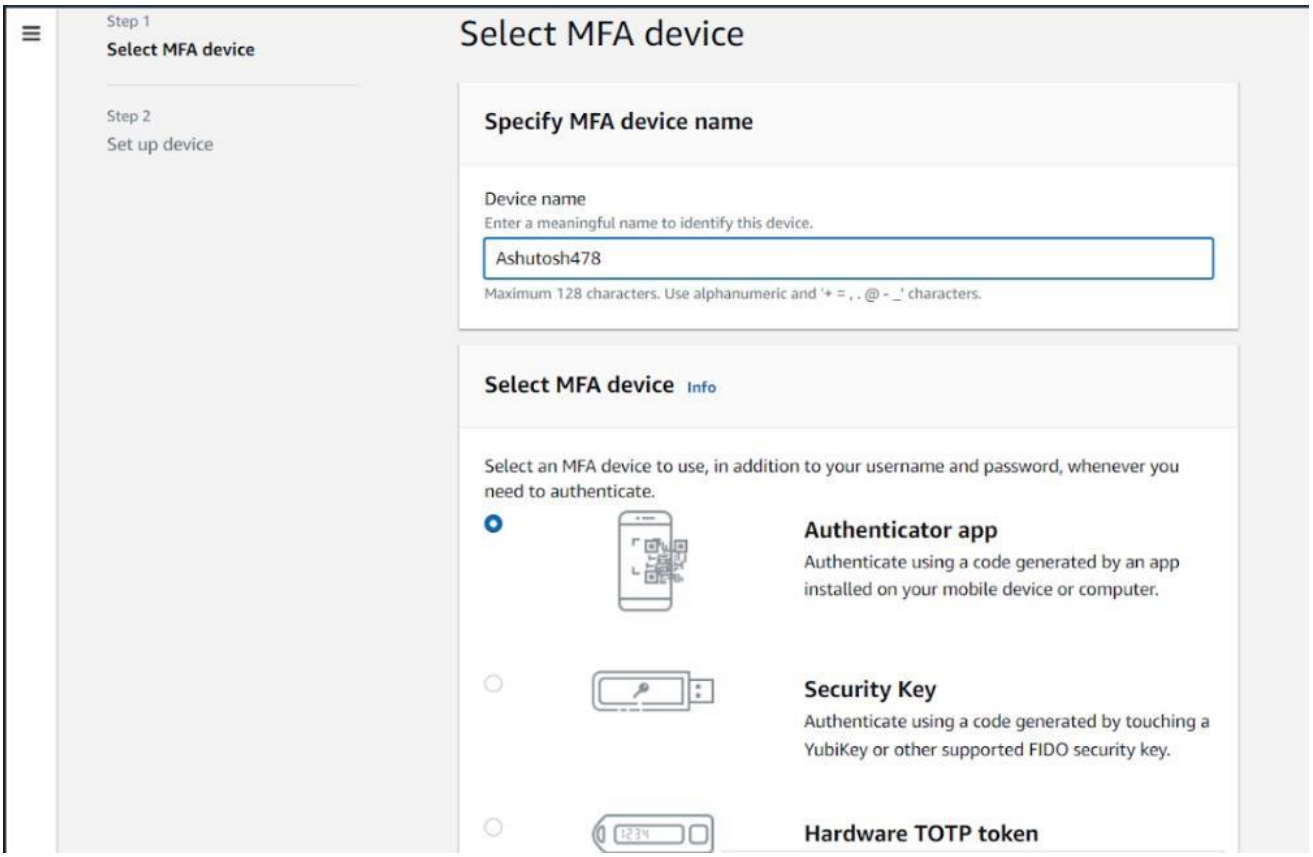

8:16 PM | 0.1KB/s
All
Communication
Entertainment
Airtel
Amazon
AnyDesk
App vault
Assistant
Authenticato r
BlackHole
Brainly
Calculator
Calendar
Camera
Chalo
Chrome
Classroom
Clock
Confirmtkt
Contacts
Da Fit
Digilocker
Doc Scanner
Docs
Downloads
Drive
Eventbrite
Search for apps

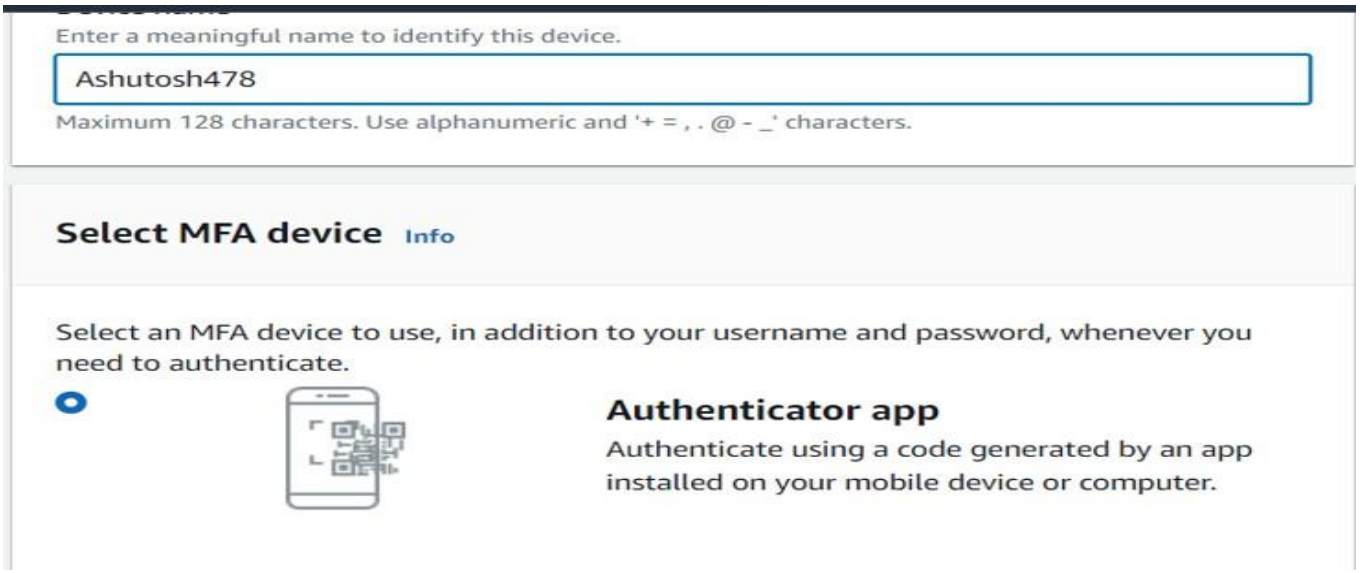
IMPLEMENTATION:



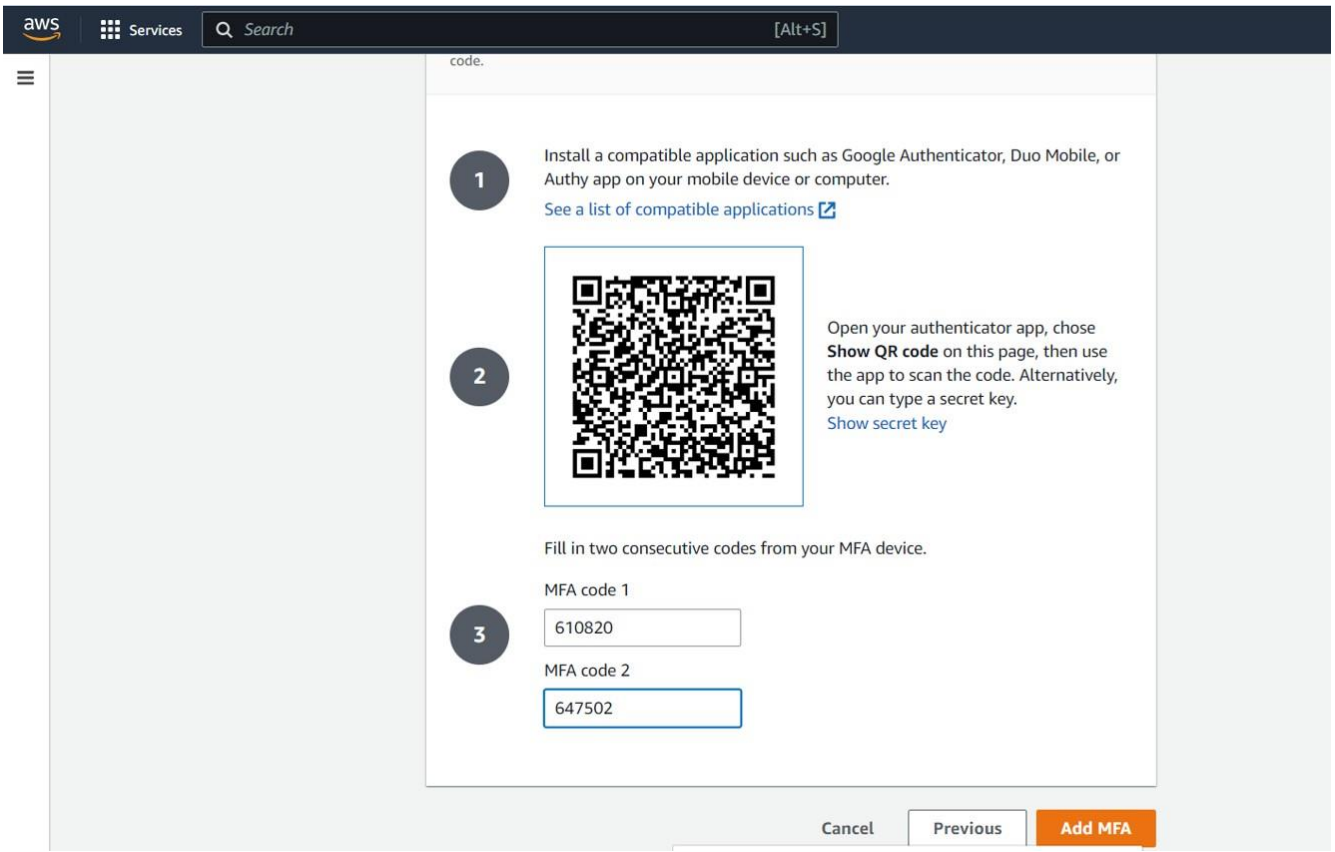


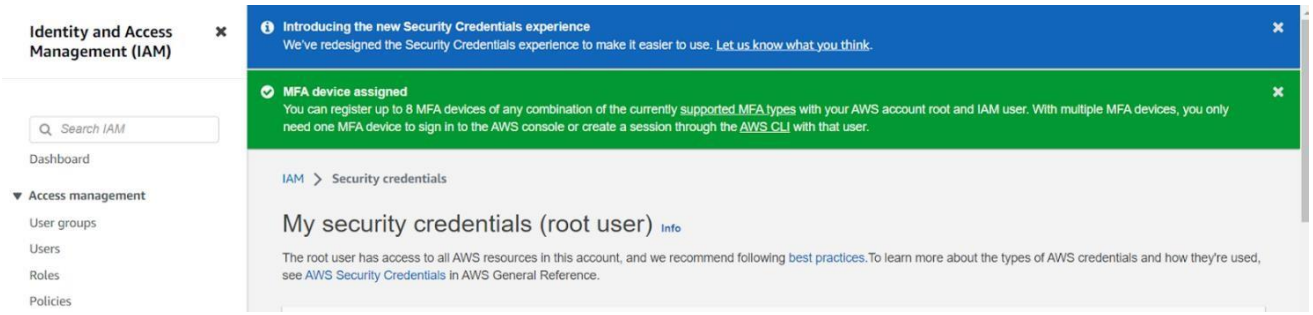

WhatsApp
IAM Management Console
Meet – sbi-jgcv-sty
us-east-1.console.aws.amazon.com/iamv2/home#/security_credentials
Skills Connect - Ca...
E-CLASS
New Tab
AWS Academy Intro...
Coursera Plus | Unli...
Untitled form - Goo...
Toc | Infosys Spring...
EDx
Create and Manage...
Destination Sequen...
Loan Prediction Pra...
aws
Services
Search
[Alt+S]
Global
Basant M
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
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
Remove
Resync
Assign MFA device
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


Step 1
Select MFA device
Step 2
Set up device
Select MFA device
Specify MFA device name
Device name
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.
Security Key
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.
Hardware TOTP token



USE GOOGLE AUTHENTICATOR APP FOR OTP:





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

Practical No.8

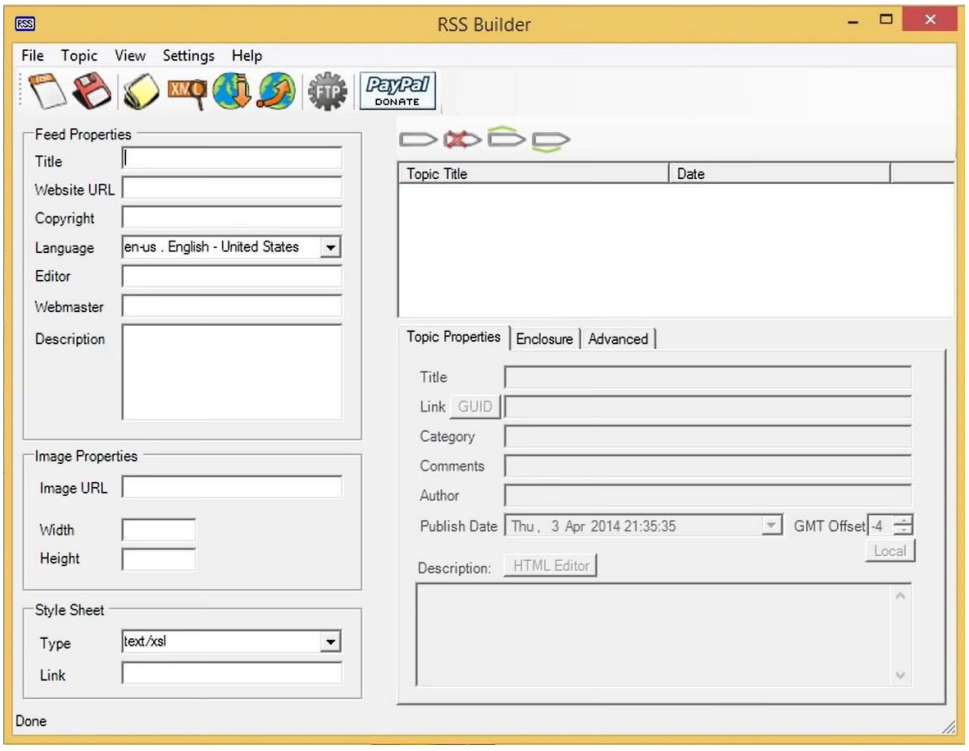
AIM: Write a program for web feed.

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.**

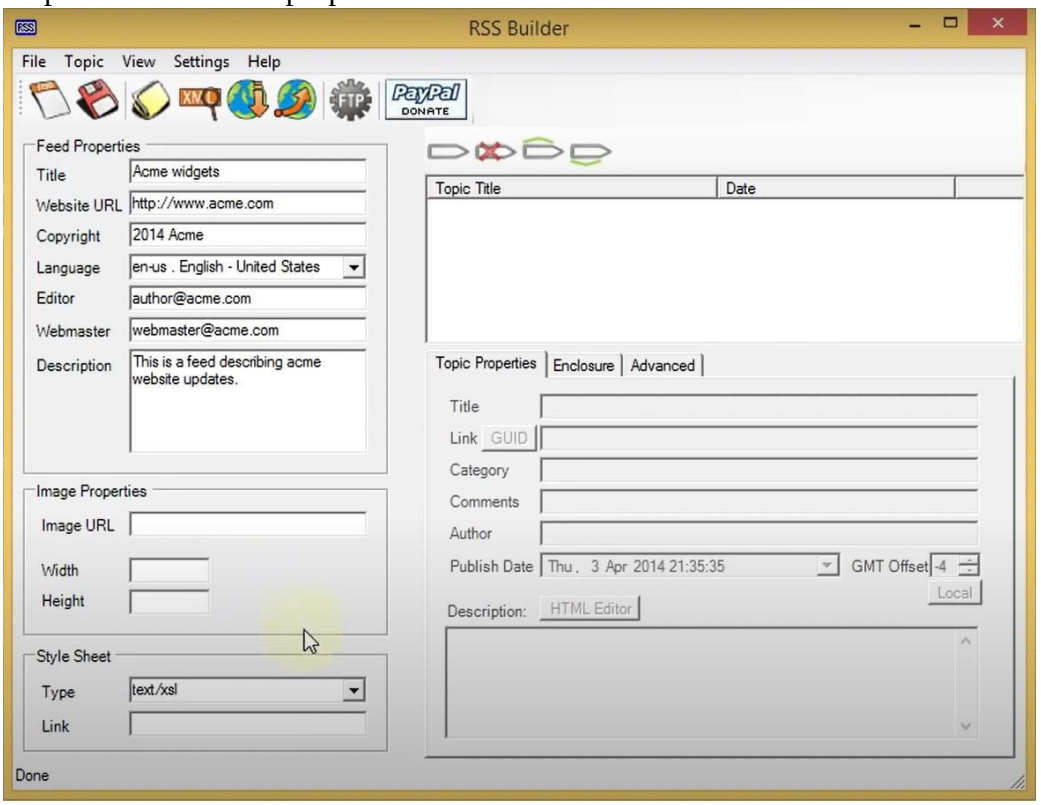
An RSS feed is a feed that delivers **auto-updated** content to users without having to manually go to a specific website. It is formatted into an XML file that can be read in an RSS reader or embedded into your website.

IMPLEMENTATION:

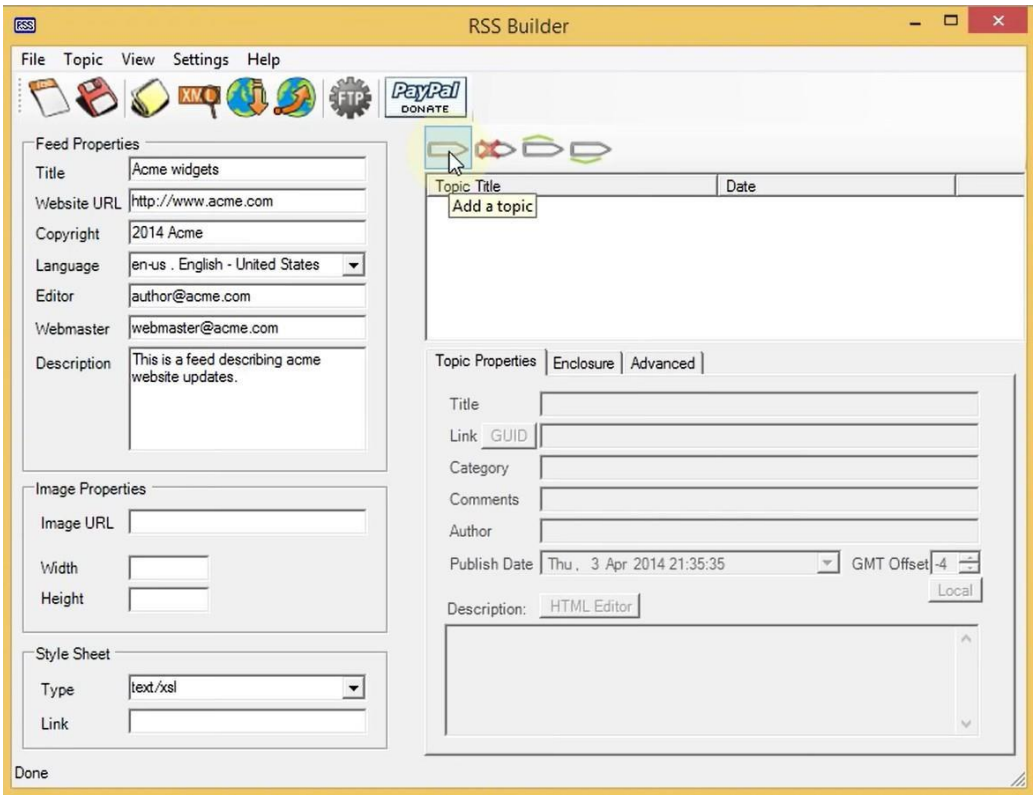
Step 01: Open RSS builder



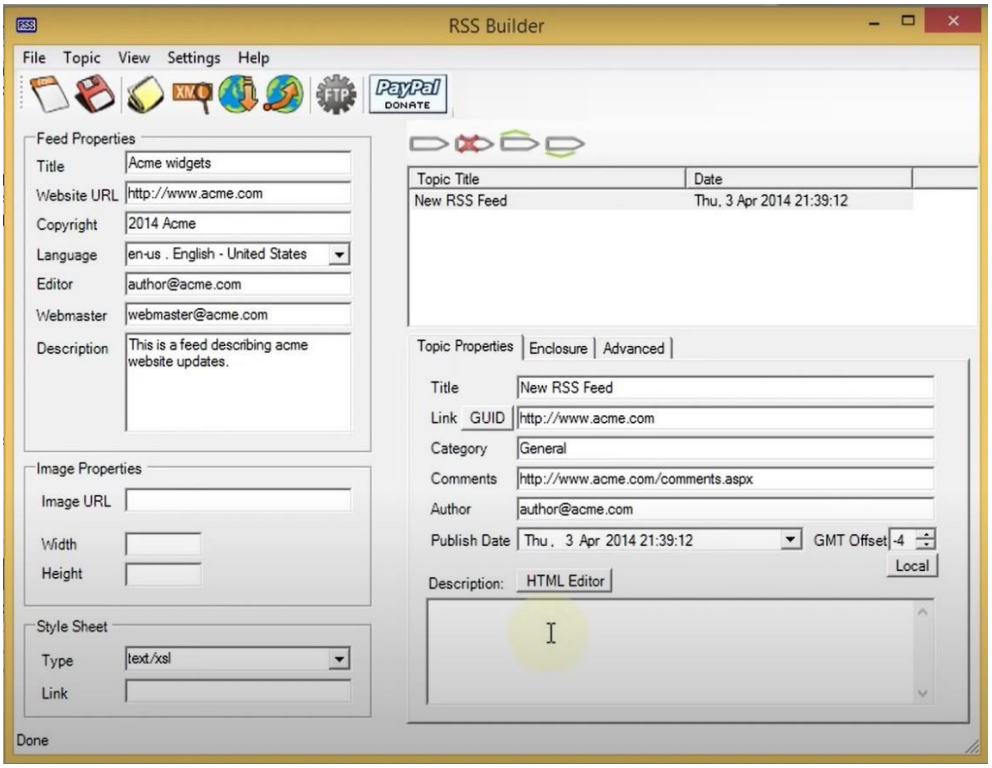
Step 02: Fill the Feed properties



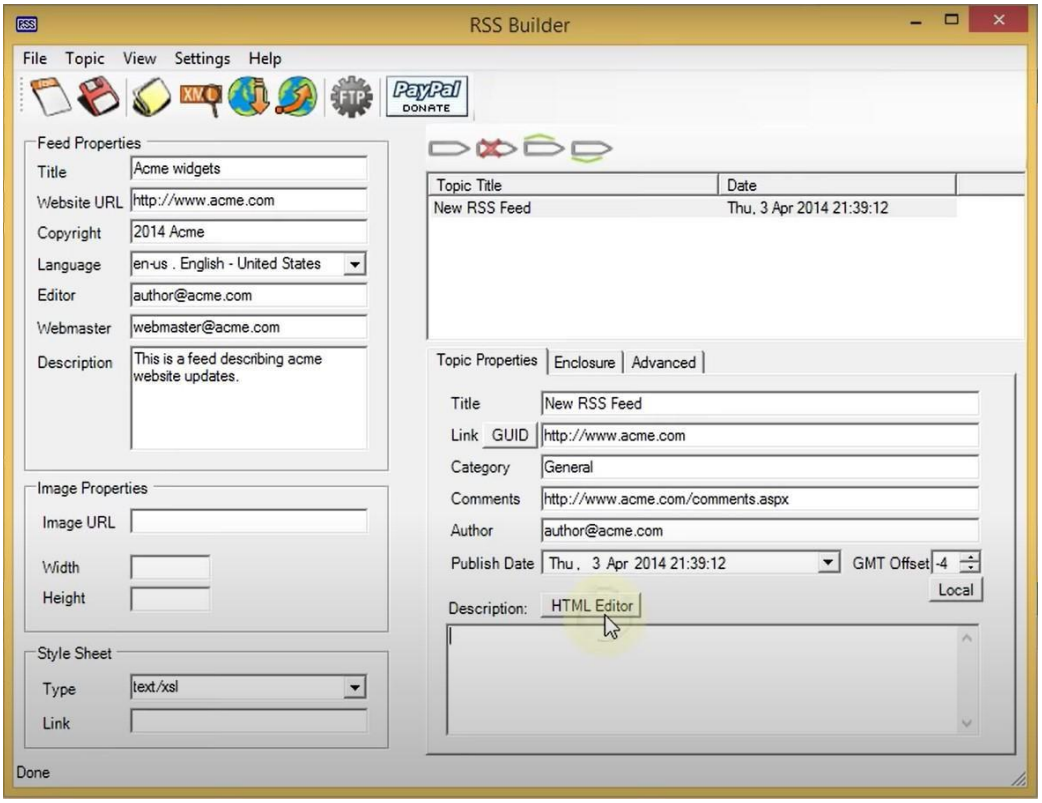
Step 03: Click on Add a Topic to add new topic to your feed



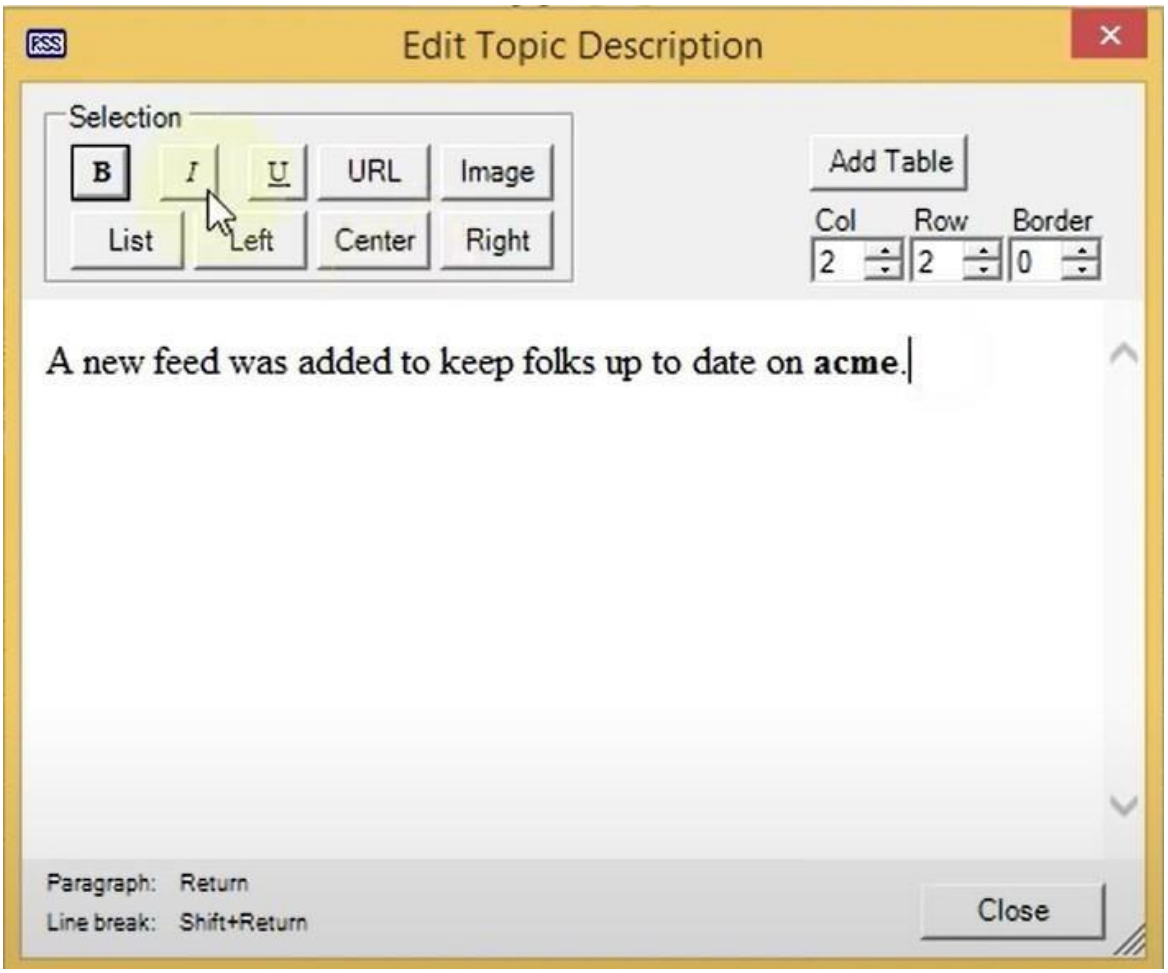
Step 04: Fill the topic properties



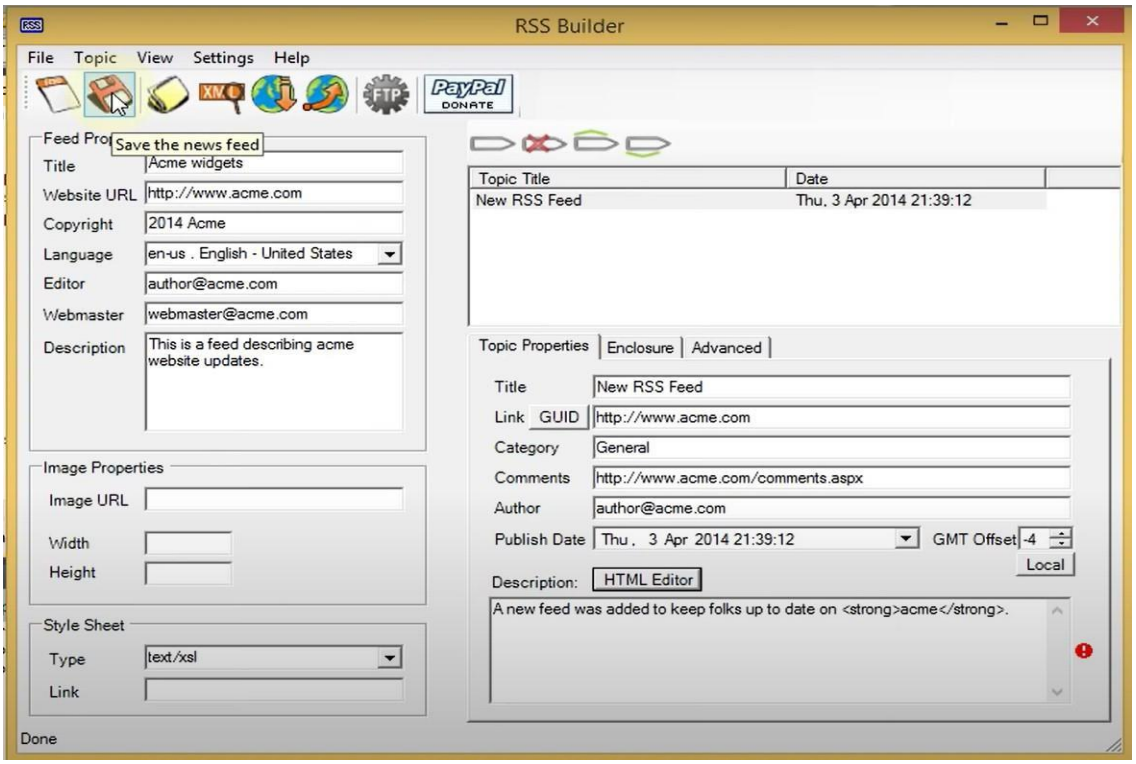
Step 05:To add description on web feed click on HTML editor



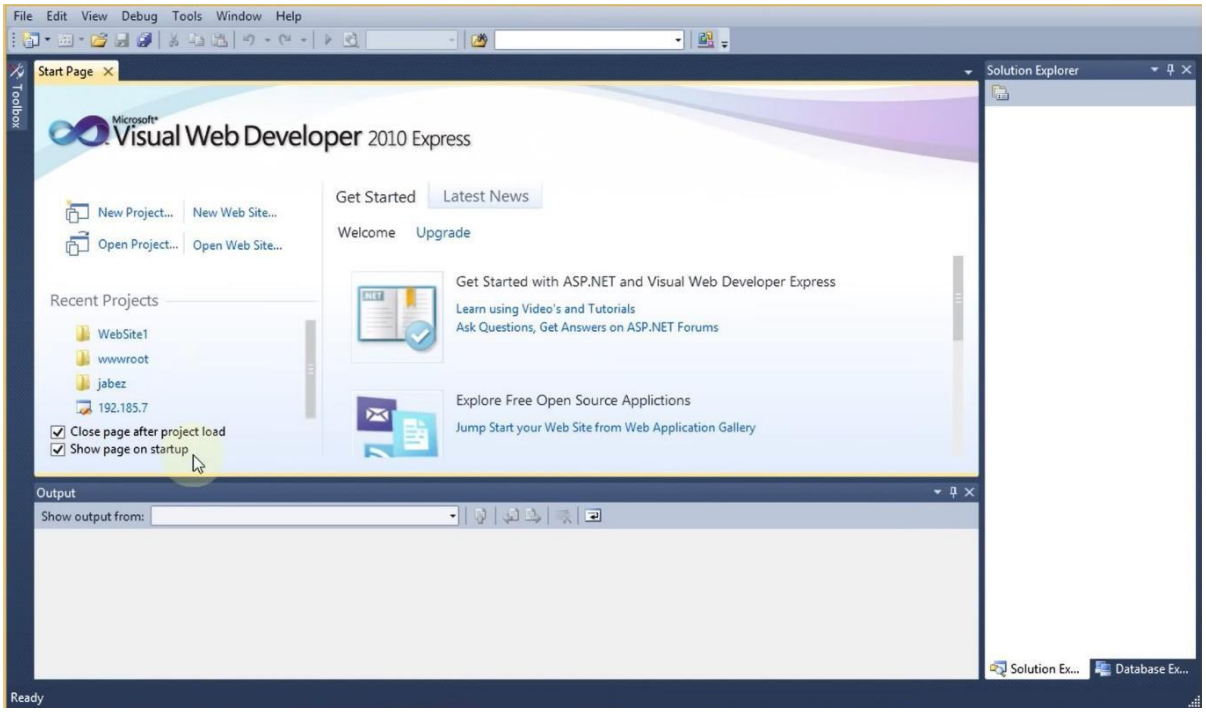
Step 06:Add topic description to show in feed



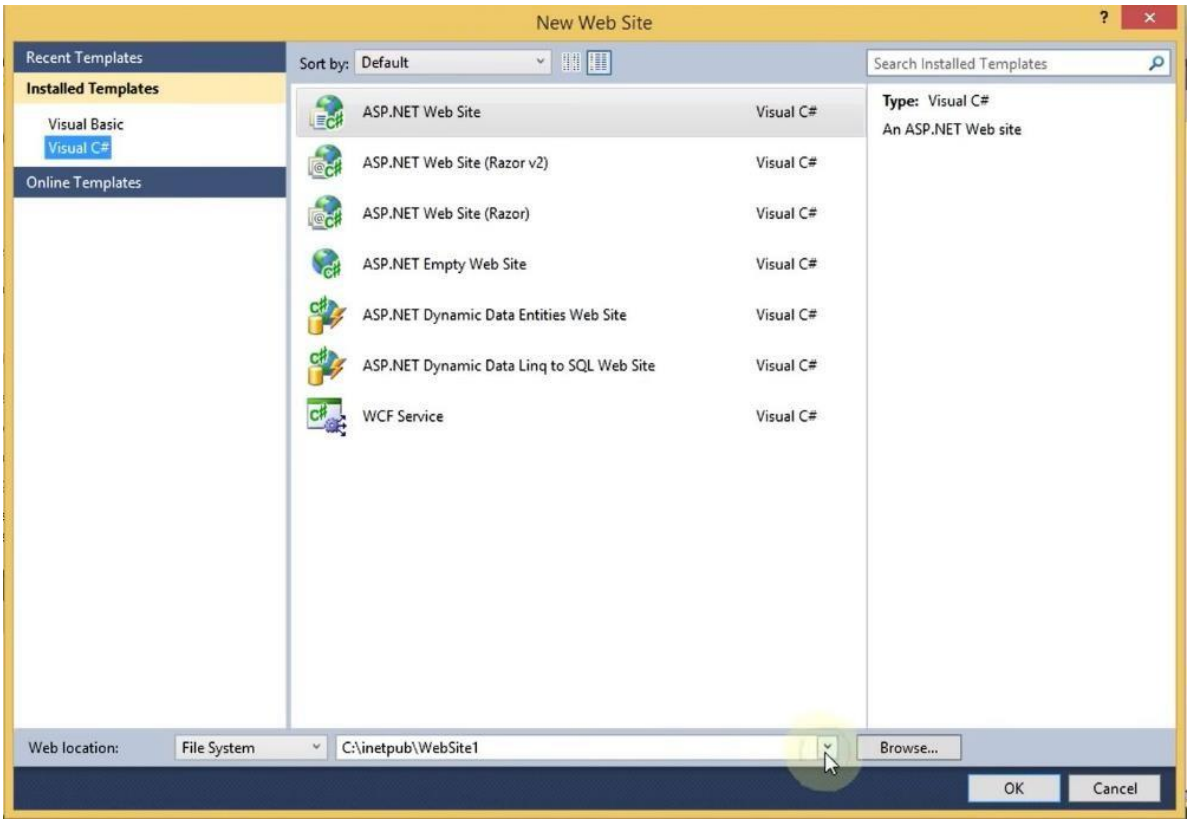
Step 07:Save the feed in xml format(defaultly saved in .xml)



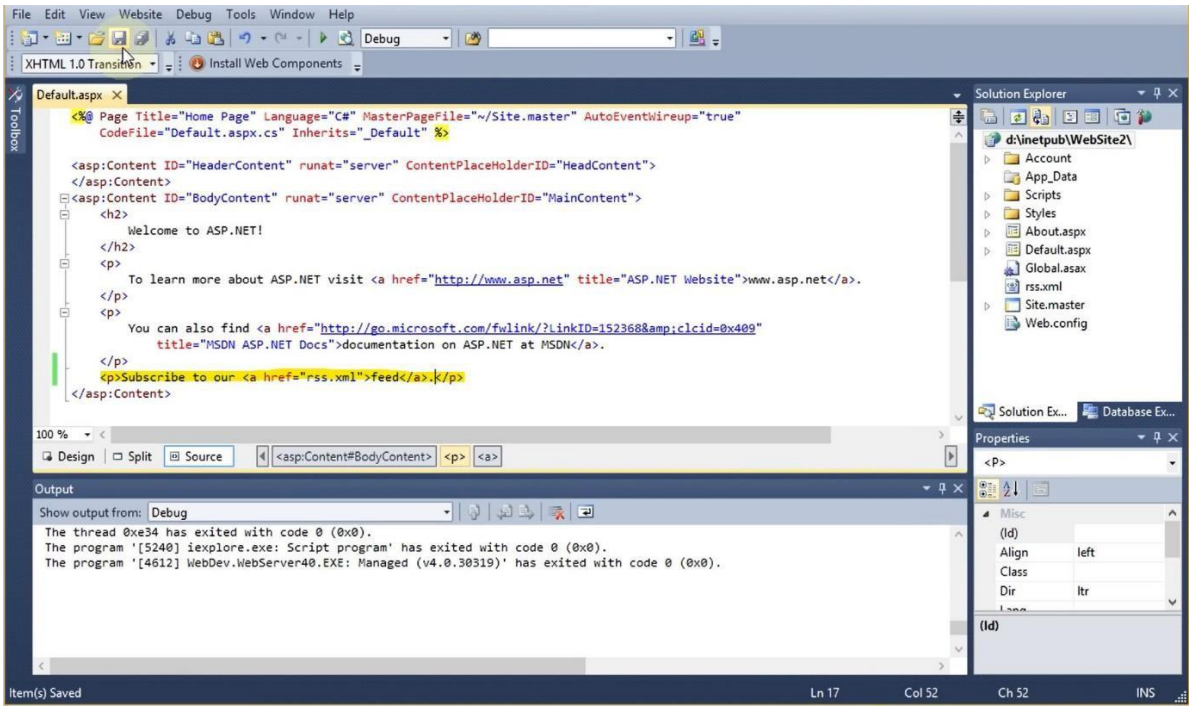
Step 08:launch Visual Studios 2010 to launch the sample website



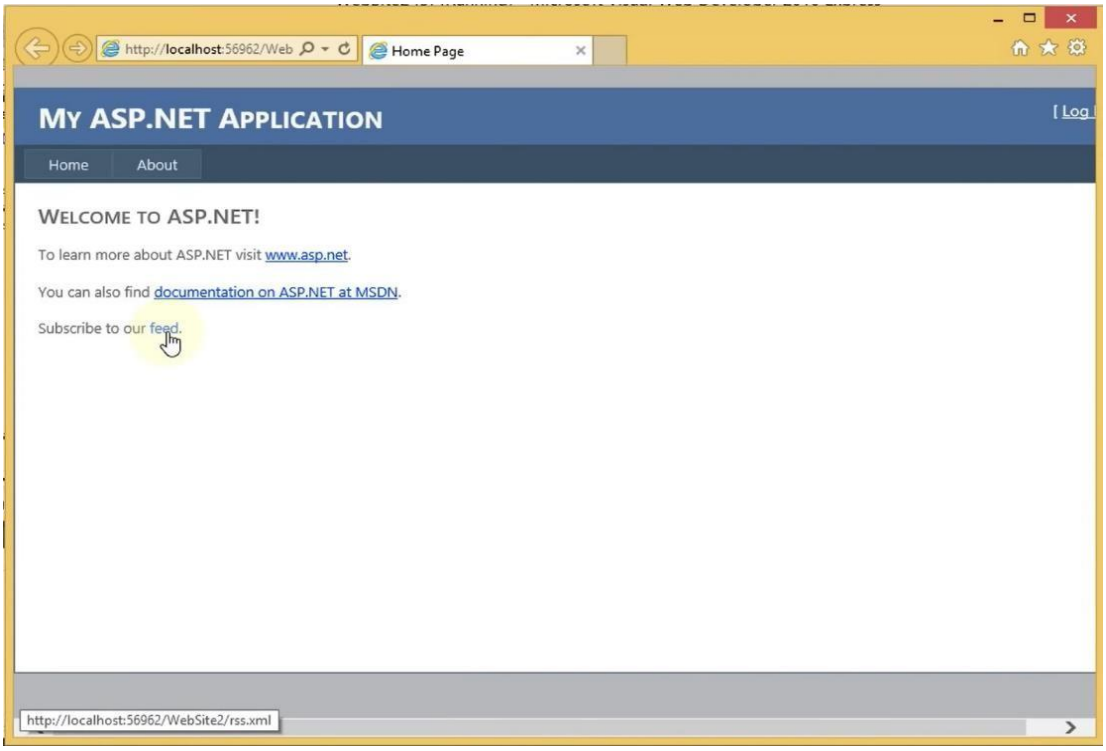
Step 09:Create new website on asp.net web site



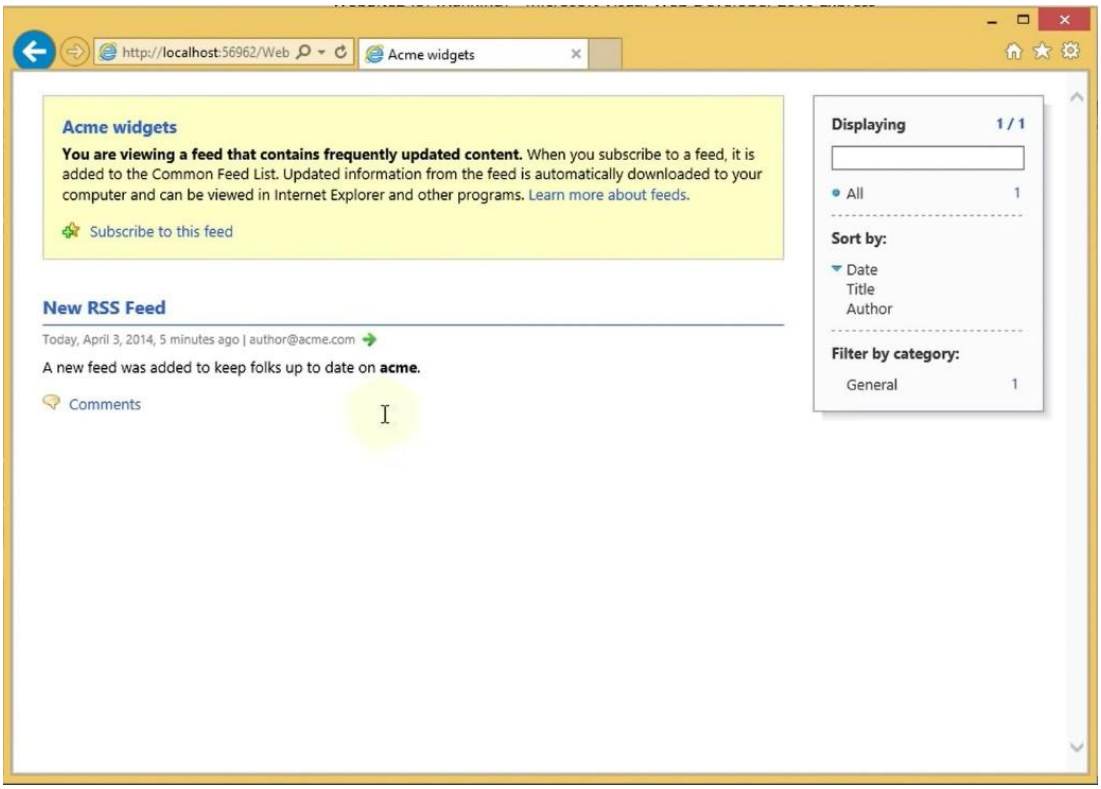
Step 10:Add new paragraph in default.aspx file and provide a link to server to access your website



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.



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 :

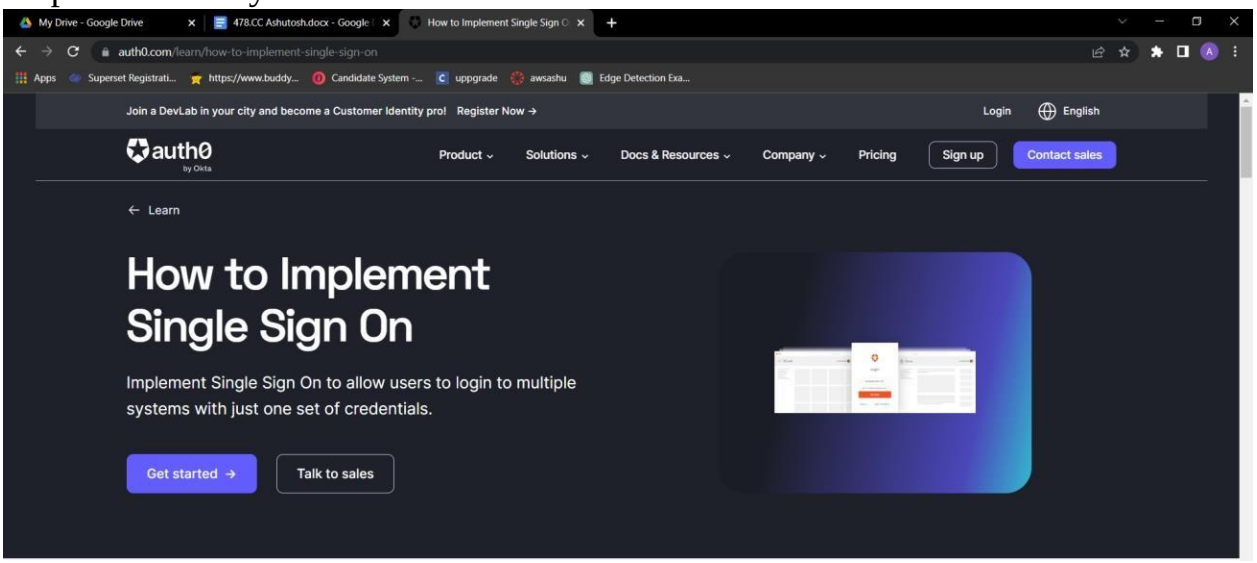
• Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications

• 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.

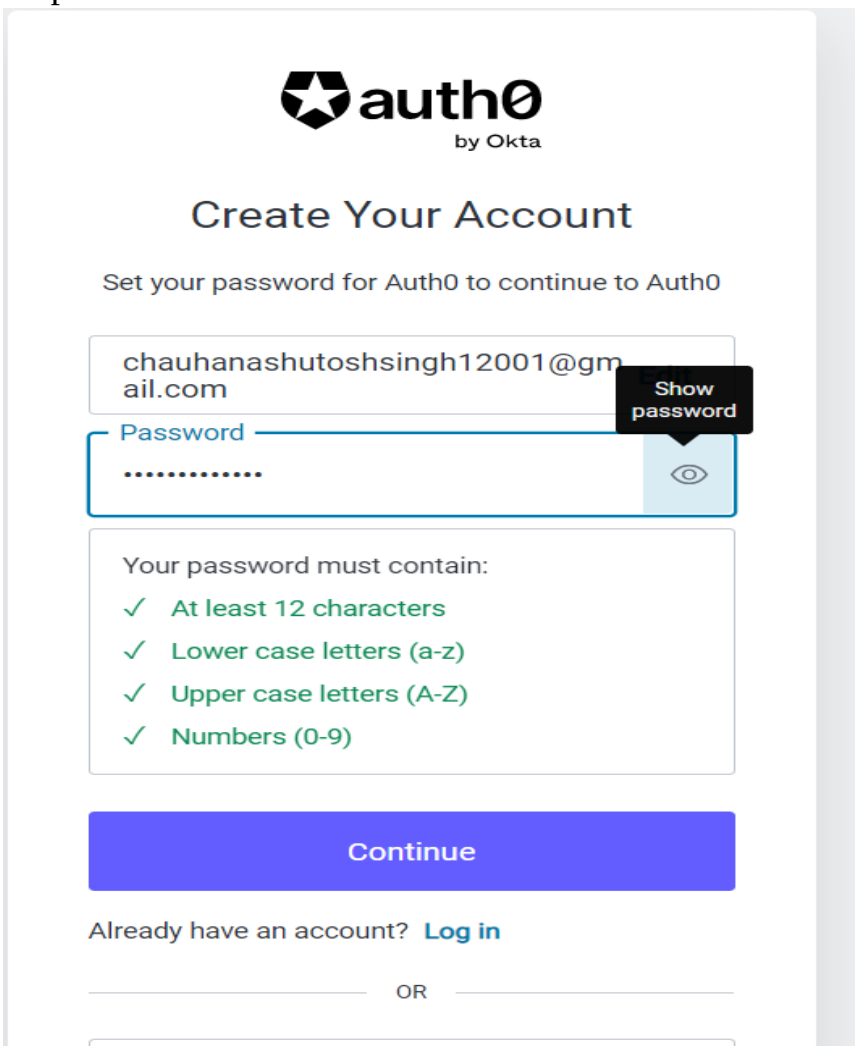
• In a basic web SSO service, an agent module on the application server retrieves the specific authentication credentials for an individual user from a dedicated SSO policy server, while authenticating the user against a user repositorysuch as a lightweight directory access protocol (LDAP) directory.

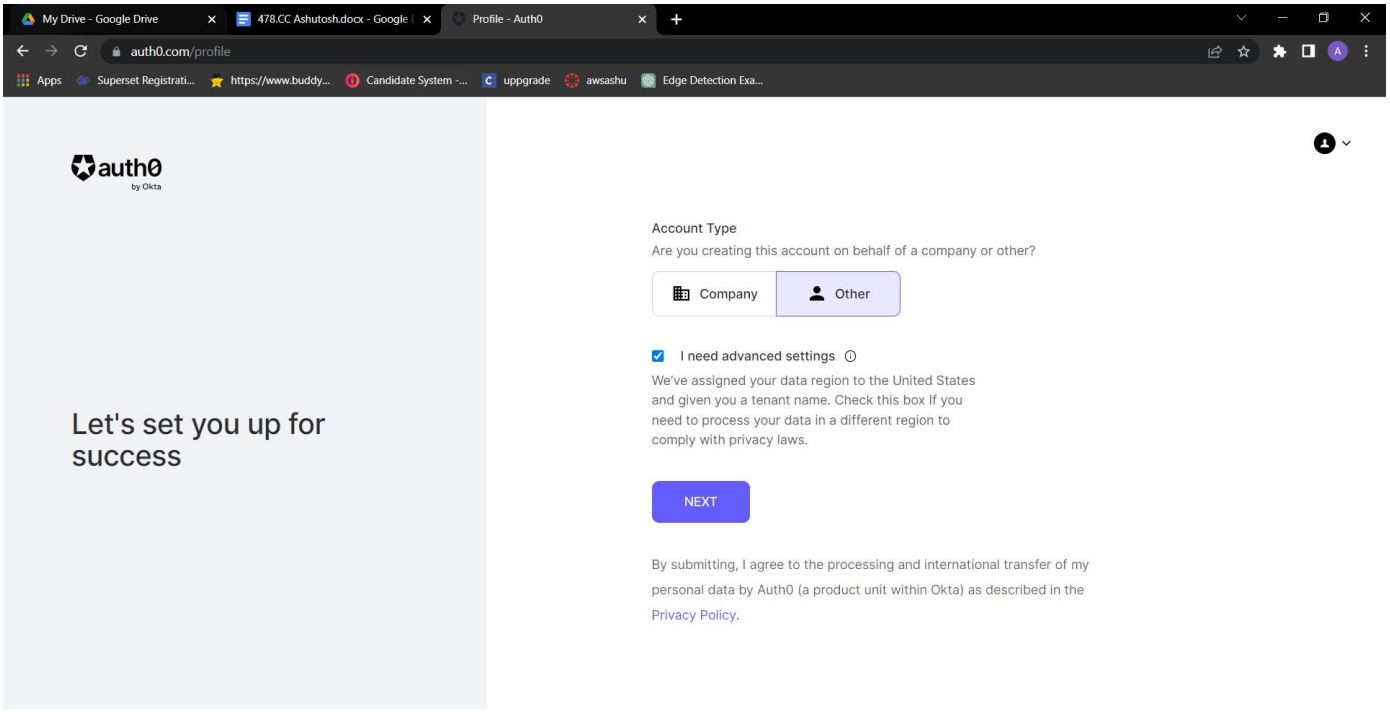
Procedure:- Step1:got to the following link https://auth0.com/learn/how-to-implement single-sign-on/

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



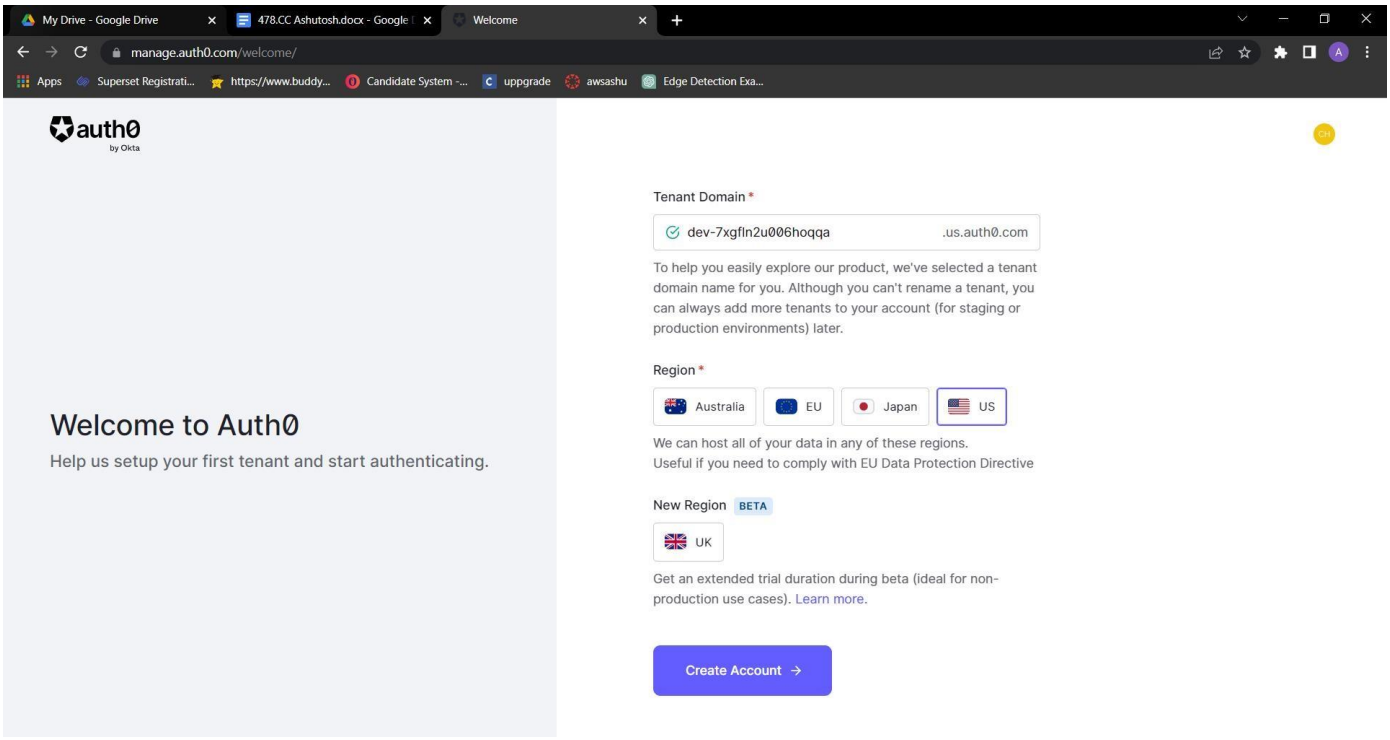
Step3: Provide the username and Password and click on Signup



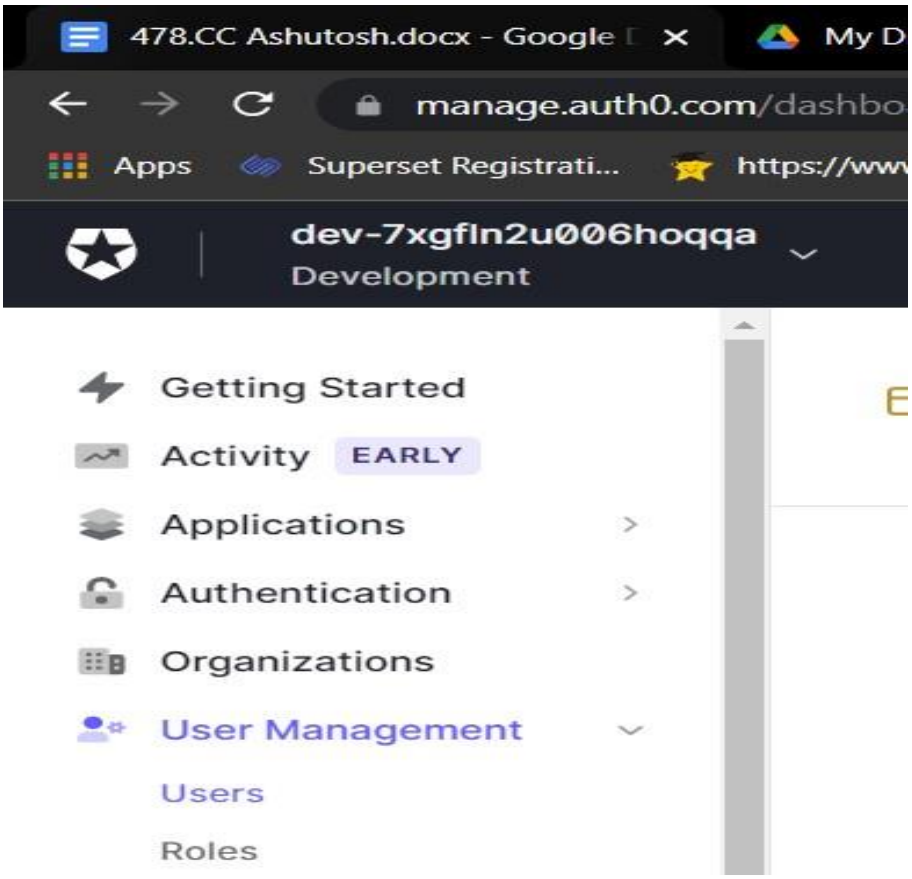


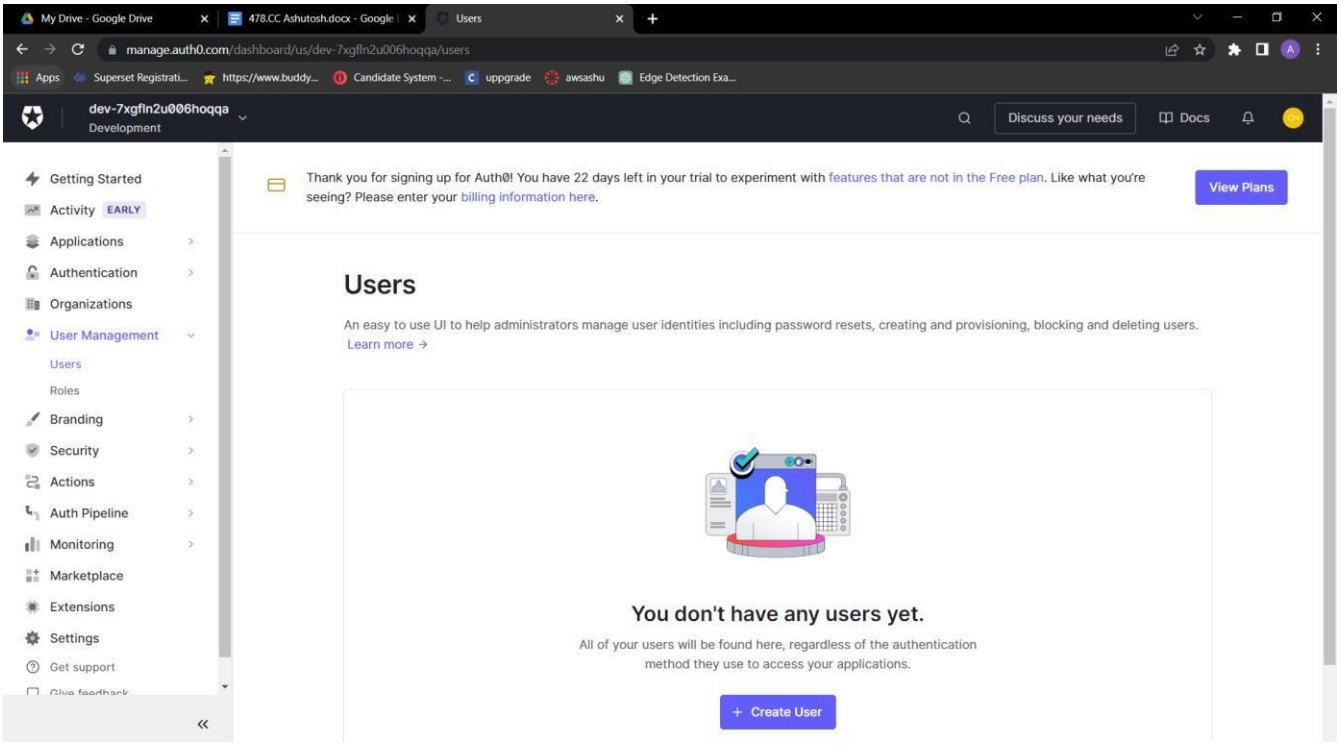
Step 4: Provide the tenant name and click on next

Step5: Fill all the Details and click on create account

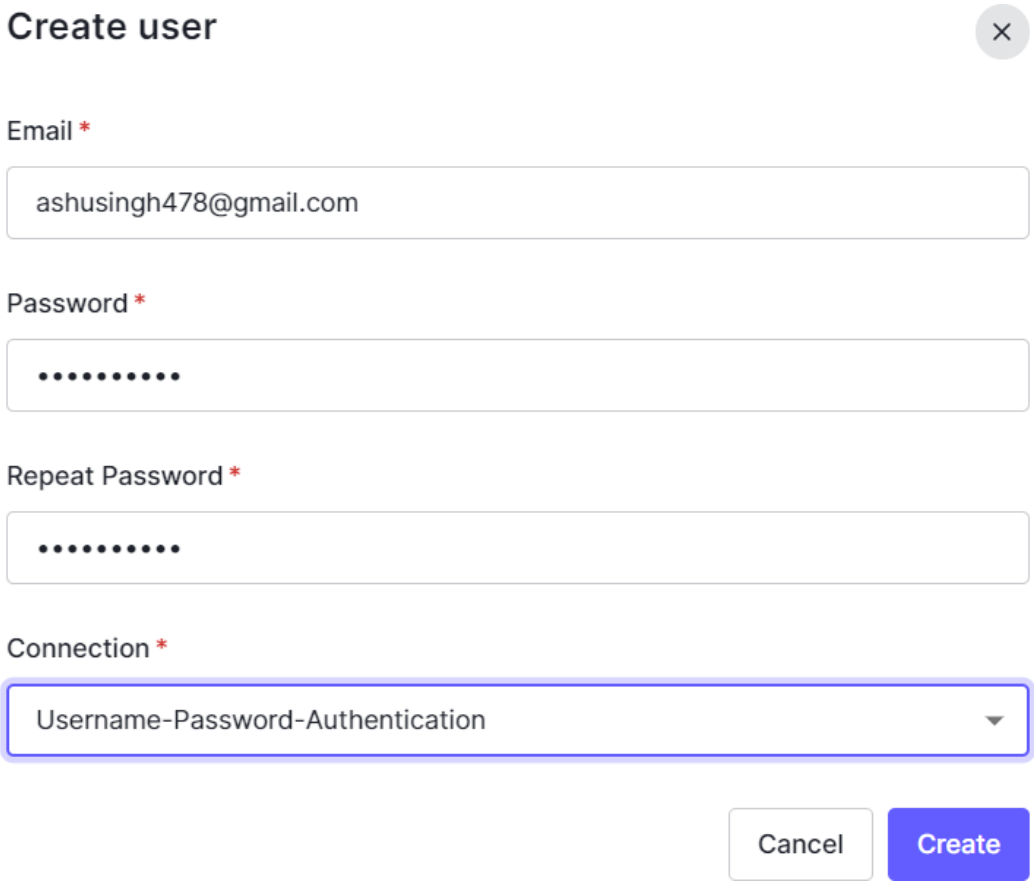


Step6: In this step you will get Dashbord . First create one user

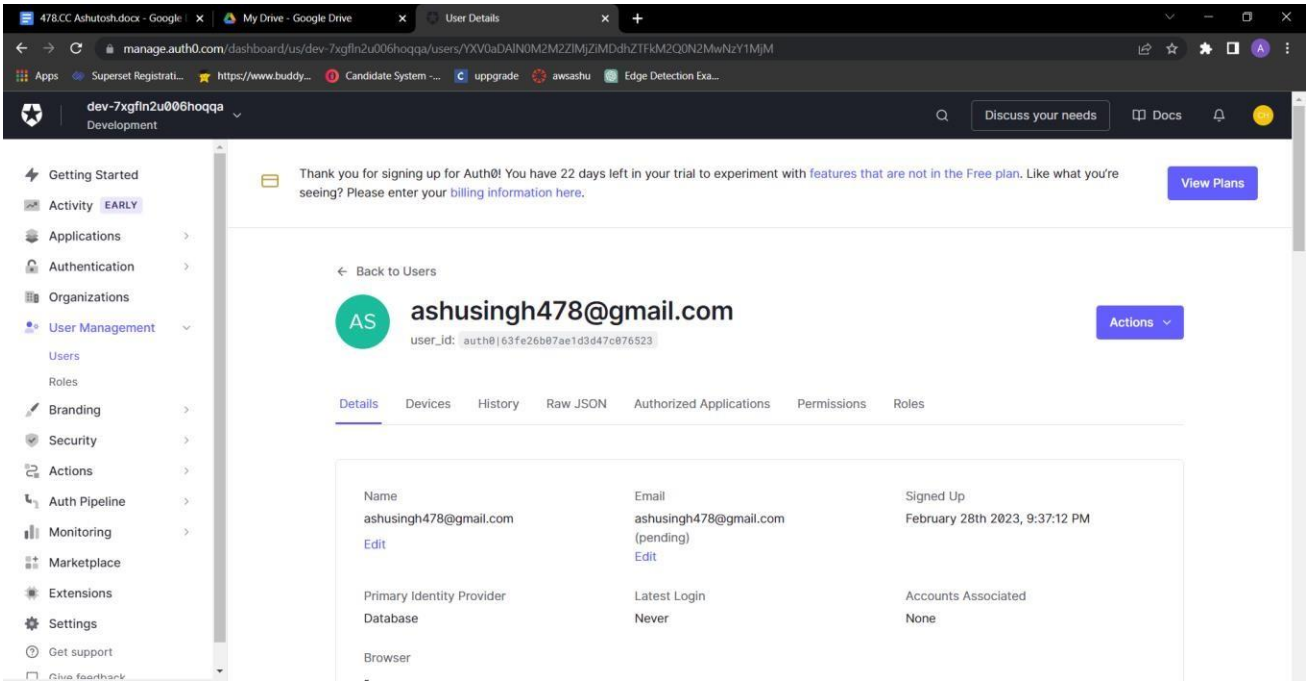


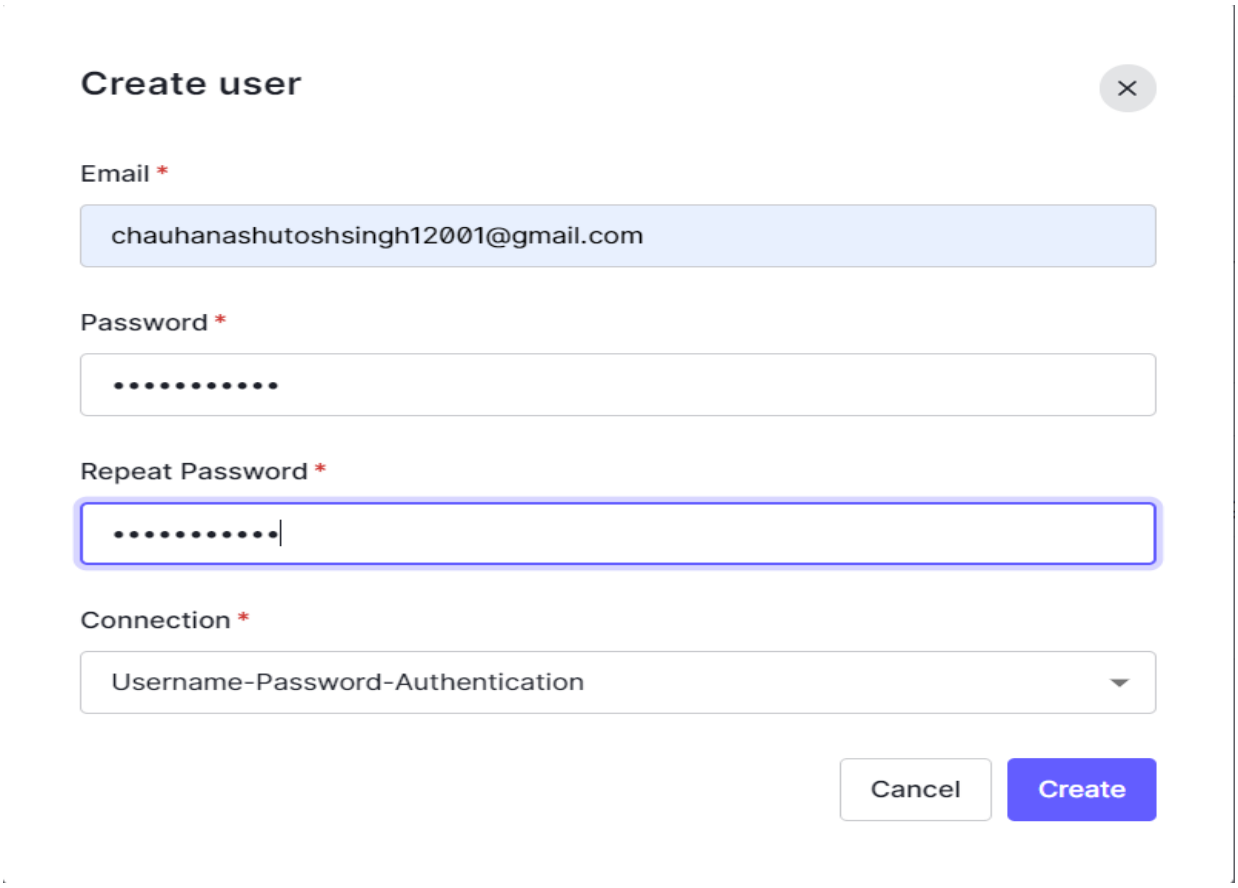


Step 7: click on create user

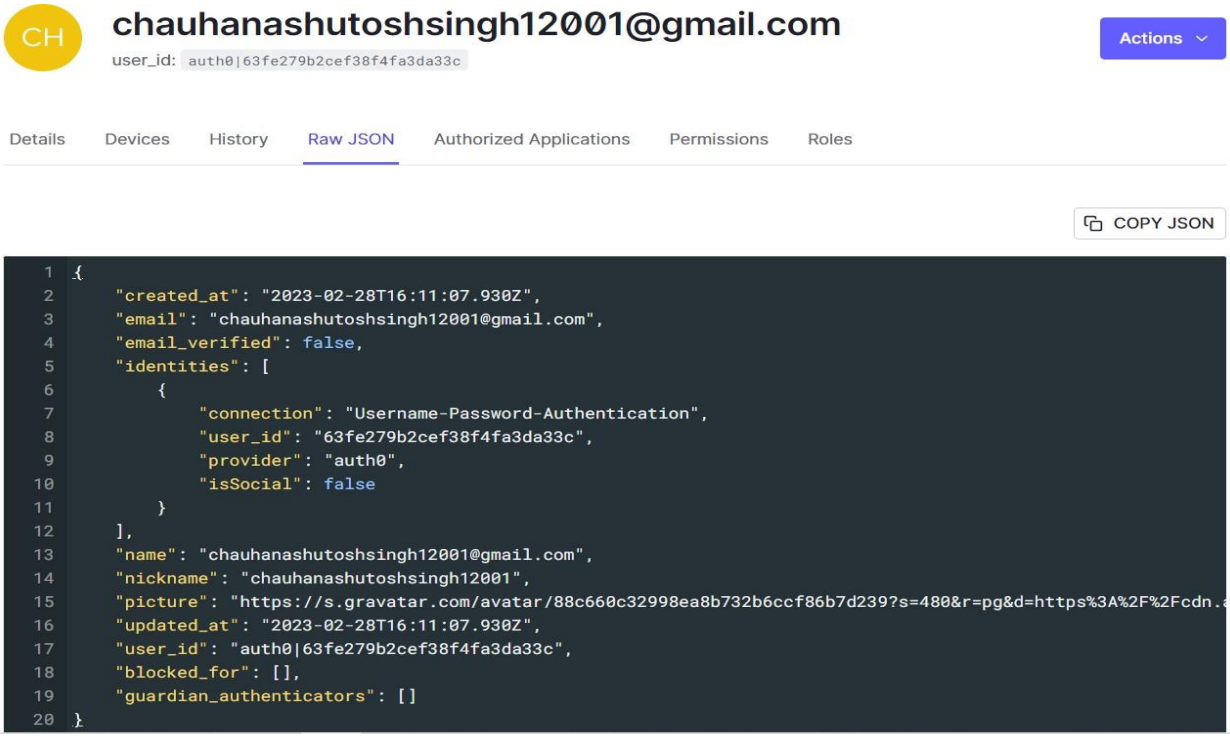


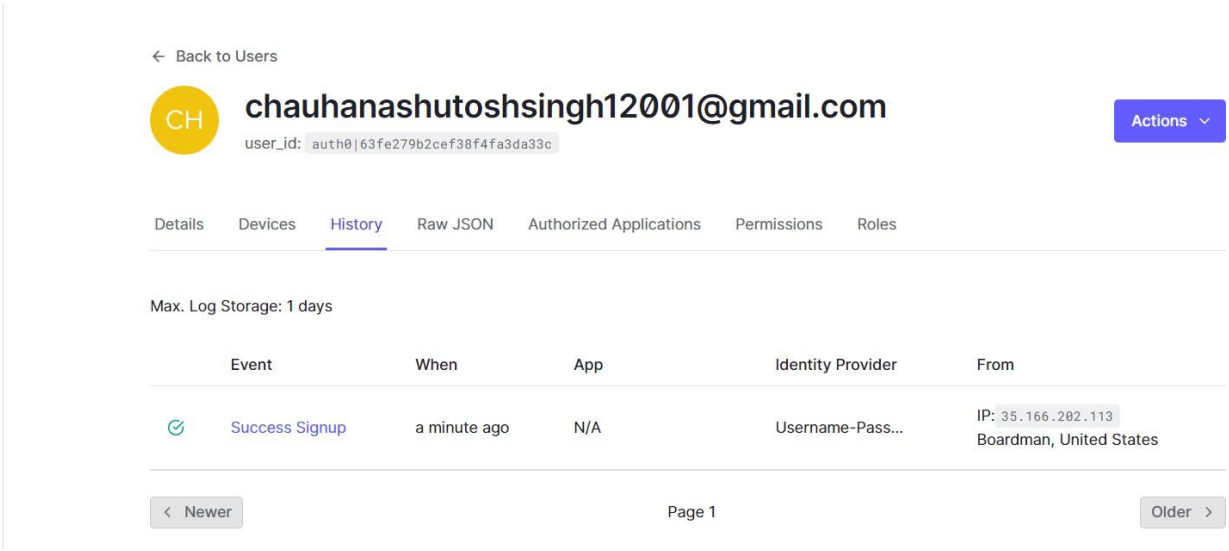
Step 8: fill all the details and click on save



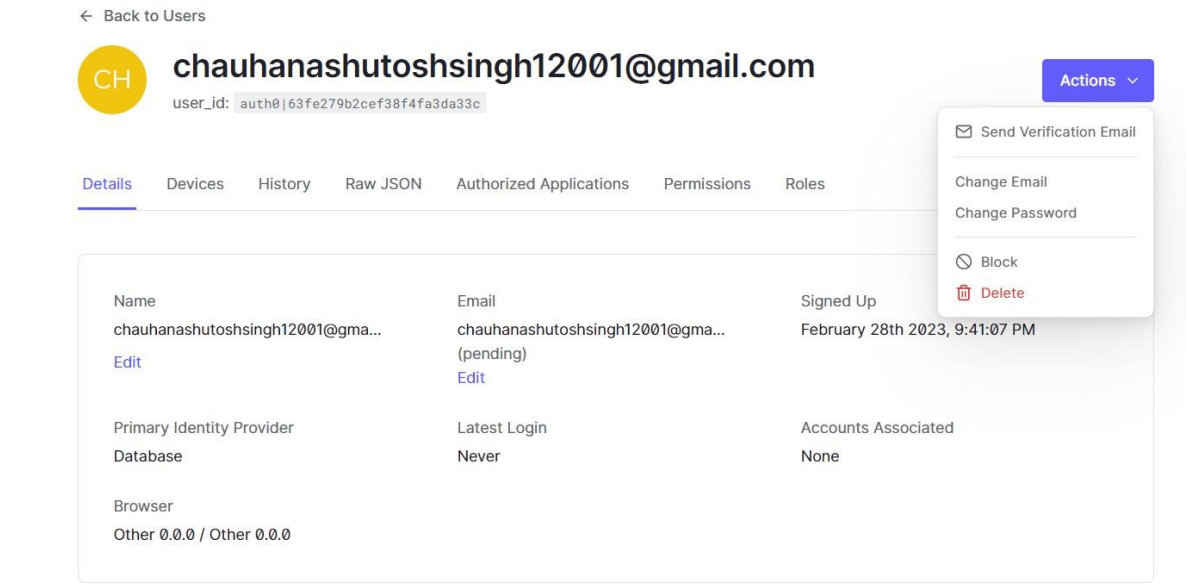

Create user
Email *
chauhanashutoshsingh12001@gmail.com
Password *
Repeat Password *
Connection *
Username-Password-Authentication
Cancel
Create

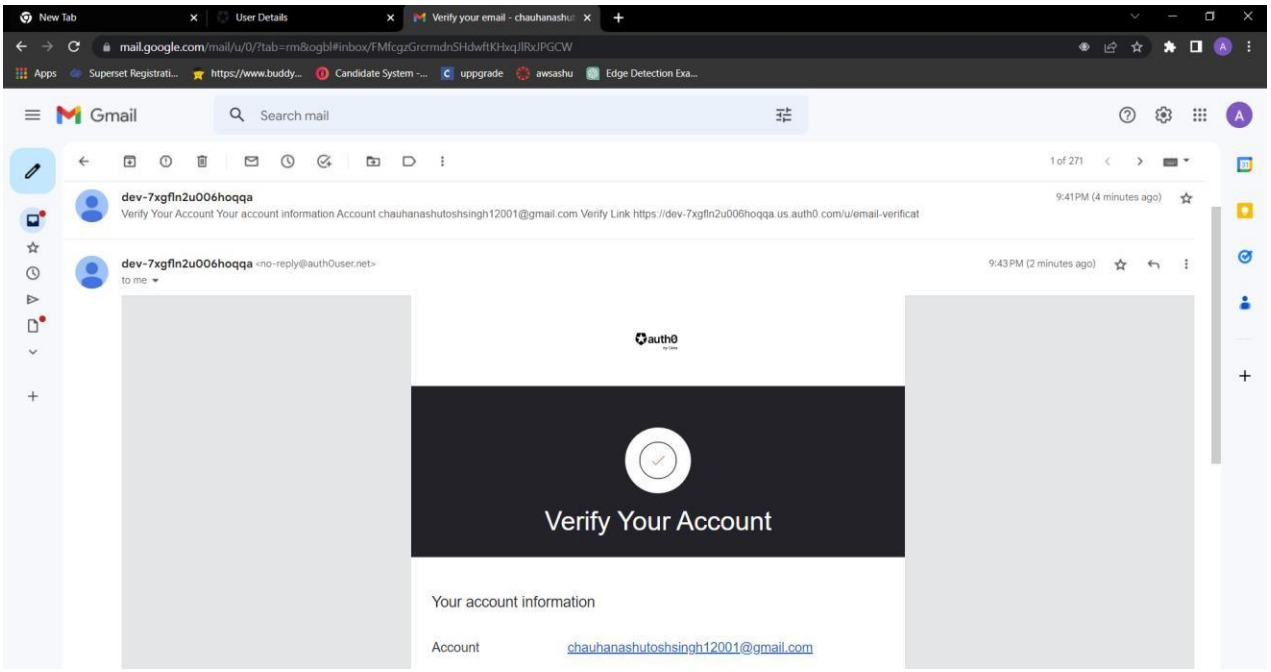
RESULTS :


CH
chauhanashutoshsingh12001@gmail.com
user_id: auth0|63fe279b2cef38f4fa3da33c
Actions
Details
Devices
History
Raw JSON
Authorized Applications
Permissions
Roles
COPY JSON
{
"created_at": "2023-02-28T16:11:07.930Z",
"email": "chauhanashutoshsingh12001@gmail.com",
"email_verified": false,
"identities": [
{
"connection": "Username-Password-Authentication",
"user_id": "63fe279b2cef38f4fa3da33c",
"provider": "auth0",
"isSocial": false
}
],
"name": "chauhanashutoshsingh12001@gmail.com",
"nickname": "chauhanashutoshsingh12001",
"picture": "https://s.gravatar.com/avatar/88c660c32998ea8b732b6ccf86b7d239?s=480&r=pg&d=https%3A%2F%2Fcdn.
"updated_at": "2023-02-28T16:11:07.930Z",
"user_id": "auth0|63fe279b2cef38f4fa3da33c",
"blocked_for": [],
"guardian_authenticators": []
}

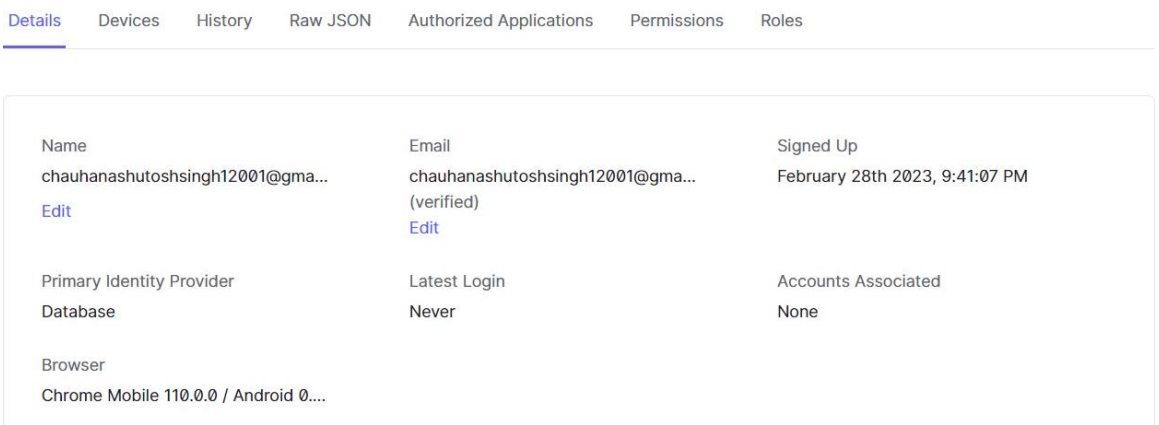


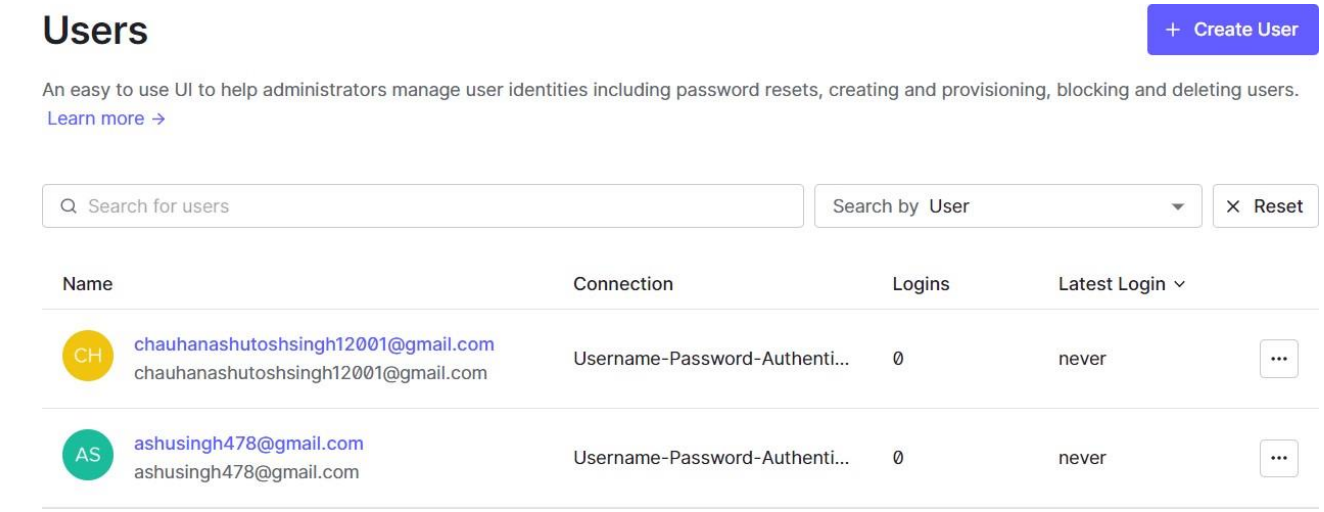
Verification Mail :

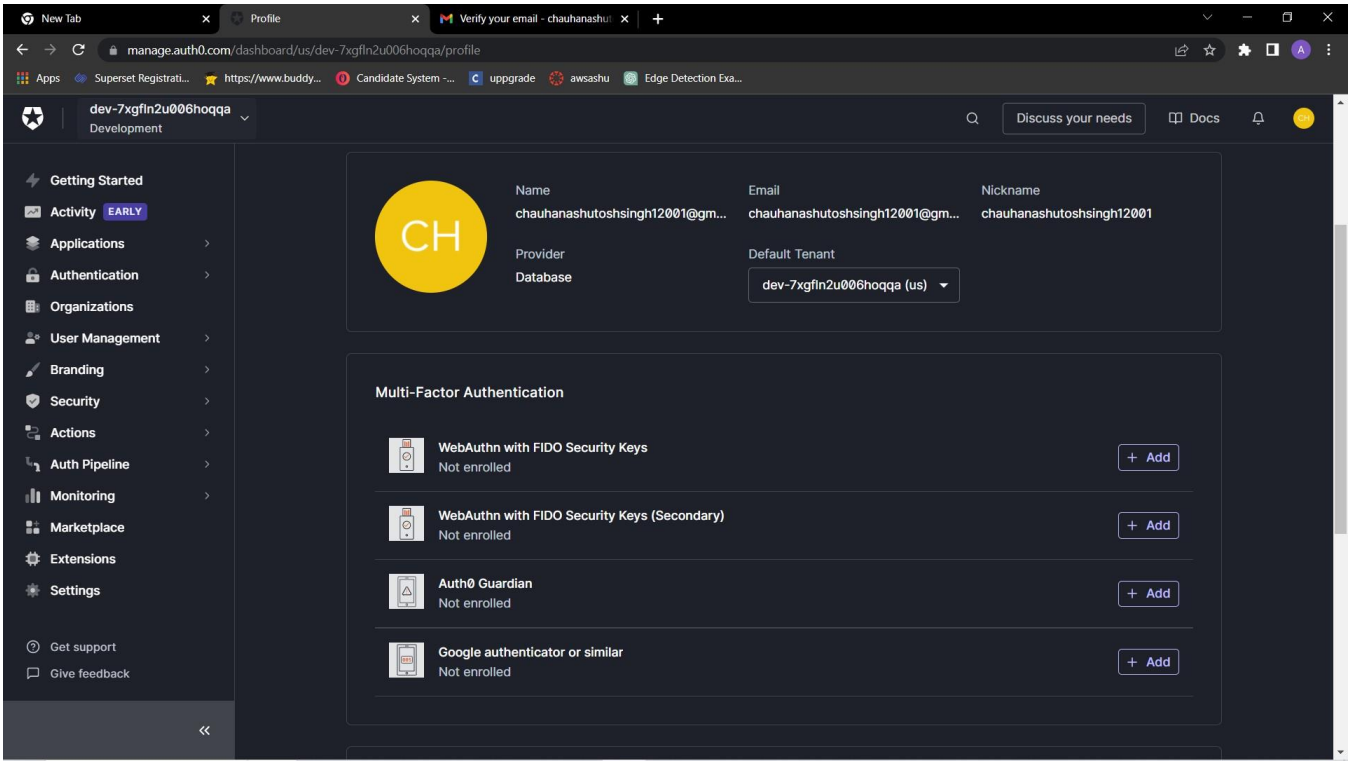




MAIL VERIFIED:

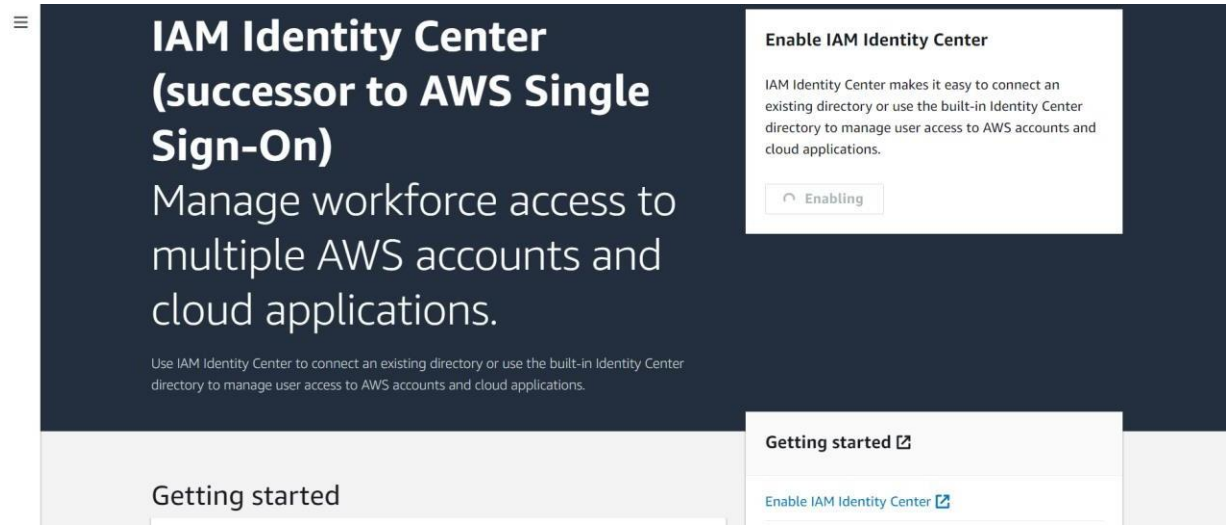


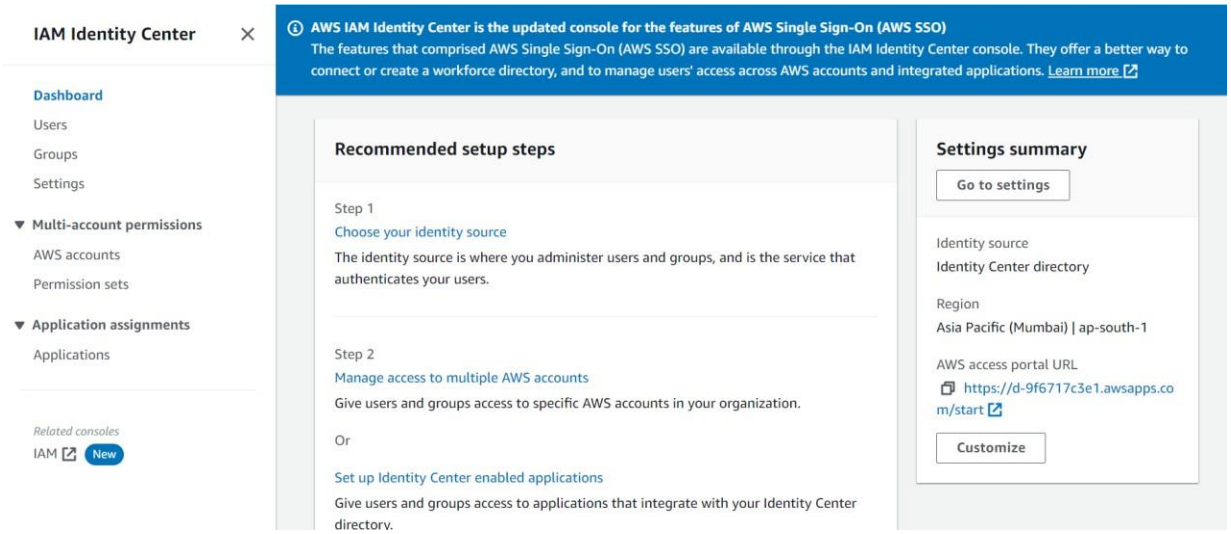

Users
+ Create User
An easy to use UI to help administrators manage user identities including password resets, creating and provisioning, blocking and deleting users.
Learn more →
Search for users
Search by User
Reset
Name
Connection
Logins
Latest Login
CH
chauhanashutoshsingh12001@gmail.com
chauhanashutoshsingh12001@gmail.com
Username-Password-Authenti...
0
never
AS
ashusingh478@gmail.com
ashusingh478@gmail.com
Username-Password-Authenti...
0
never

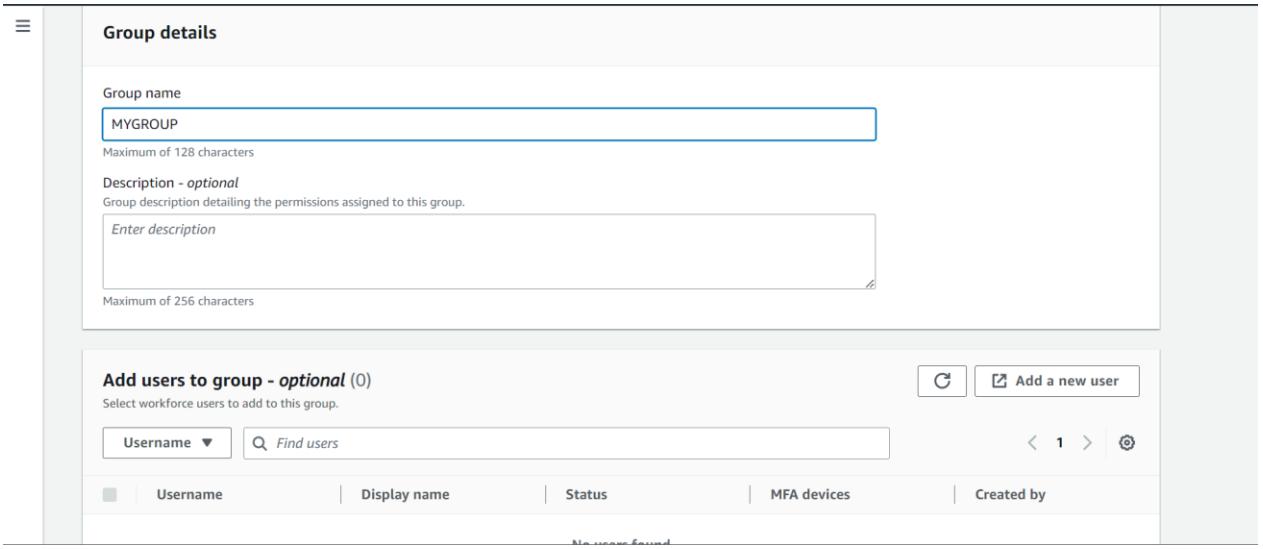

New Tab
Profile
Verify your email - chauhanashut
manage.auth0.com/dashboard/us/dev-7xgfln2u006hoqqa/profile
dev-7xgfln2u006hoqqa
Development
Discuss your needs
Docs
Getting Started
Activity EARLY
Applications
Authentication
Organizations
User Management
Branding
Security
Actions
Auth Pipeline
Monitoring
Marketplace
Extensions
Settings
Get support
Give feedback
CH
Name
chauhanashutoshsingh12001@gm...
Email
chauhanashutoshsingh12001@gm...
Nickname
chauhanashutoshsingh12001
Provider
Database
Default Tenant
dev-7xgfln2u006hoqqa (us)
Multi-Factor Authentication
WebAuthn with FIDO Security Keys
Not enrolled
+ Add
WebAuthn with FIDO Security Keys (Secondary)
Not enrolled
+ Add
Auth0 Guardian
Not enrolled
+ Add
Google authenticator or similar
Not enrolled
+ Add

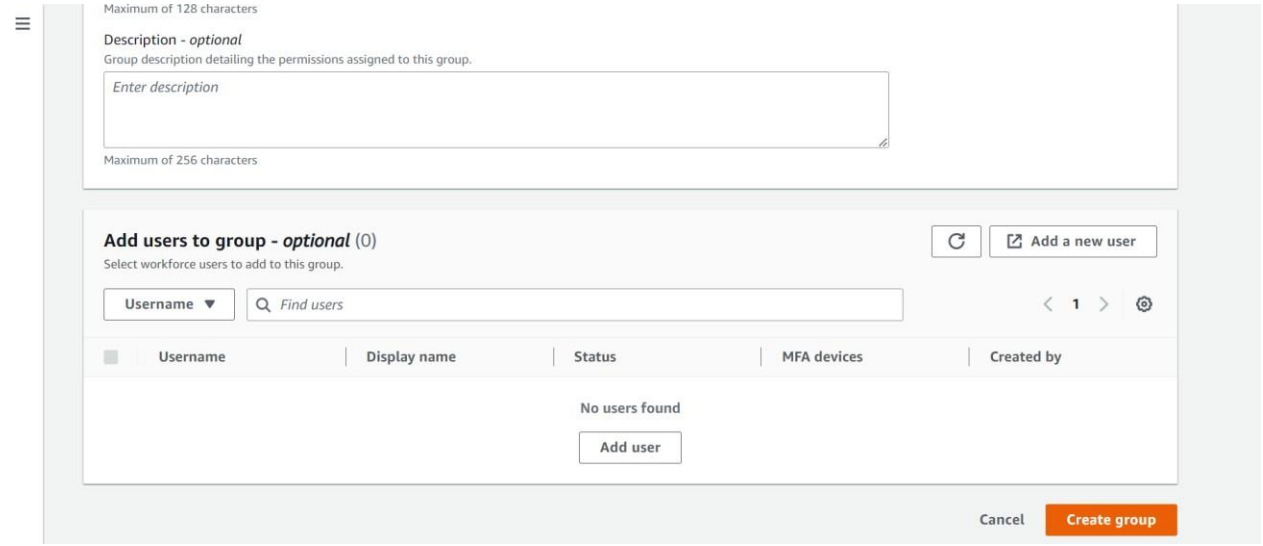
BYAWS/.

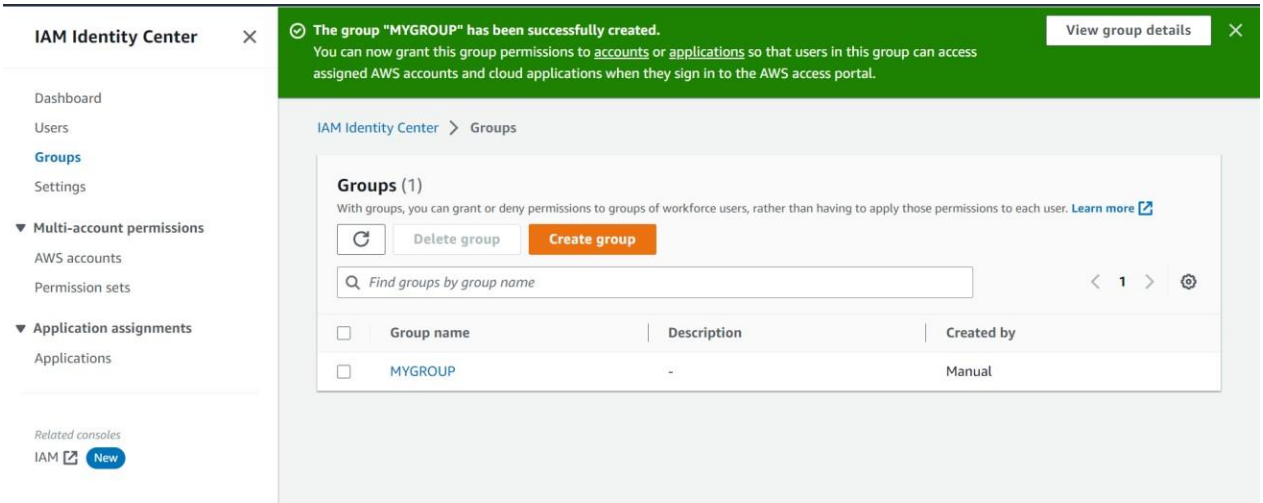

Security, Identity, and Compliance
IAM Identity Center (successor to AWS Single Sign-On)
Manage workforce access to multiple AWS accounts and cloud applications.
Use IAM Identity Center to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.
Enable IAM Identity Center
IAM Identity Center makes it easy to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.
Enable
Getting started


IAM Identity Center (successor to AWS Single Sign-On)
Manage workforce access to multiple AWS accounts and cloud applications.
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.
Enable IAM Identity Center
IAM Identity Center makes it easy to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.
Enabling
Getting started
Enable IAM Identity Center
Getting started


IAM Identity Center
Dashboard
Users
Groups
Settings
Multi-account permissions
AWS accounts
Permission sets
Application assignments
Applications
Related consoles
IAM
New
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
Recommended setup steps
Step 1
Choose your identity source
The identity source is where you administer users and groups, and is the service that authenticates your users.
Step 2
Manage access to multiple AWS accounts
Give users and groups access to specific AWS accounts in your organization.
Or
Set up Identity Center enabled applications
Give users and groups access to applications that integrate with your Identity Center directory.
Settings summary
Go to settings
Identity source
Identity Center directory
Region
Asia Pacific (Mumbai) | ap-south-1
AWS access portal URL
https://d-9f6717c3e1.awsapps.com/start
Customize

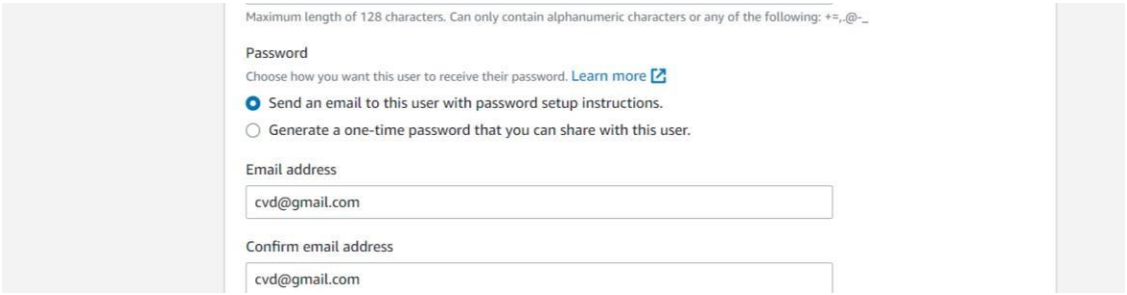


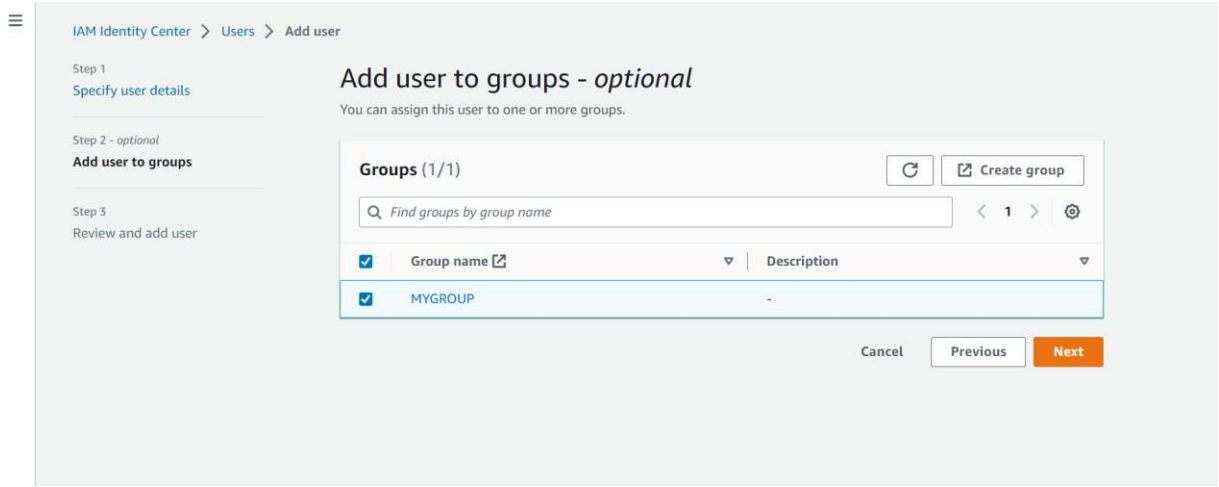


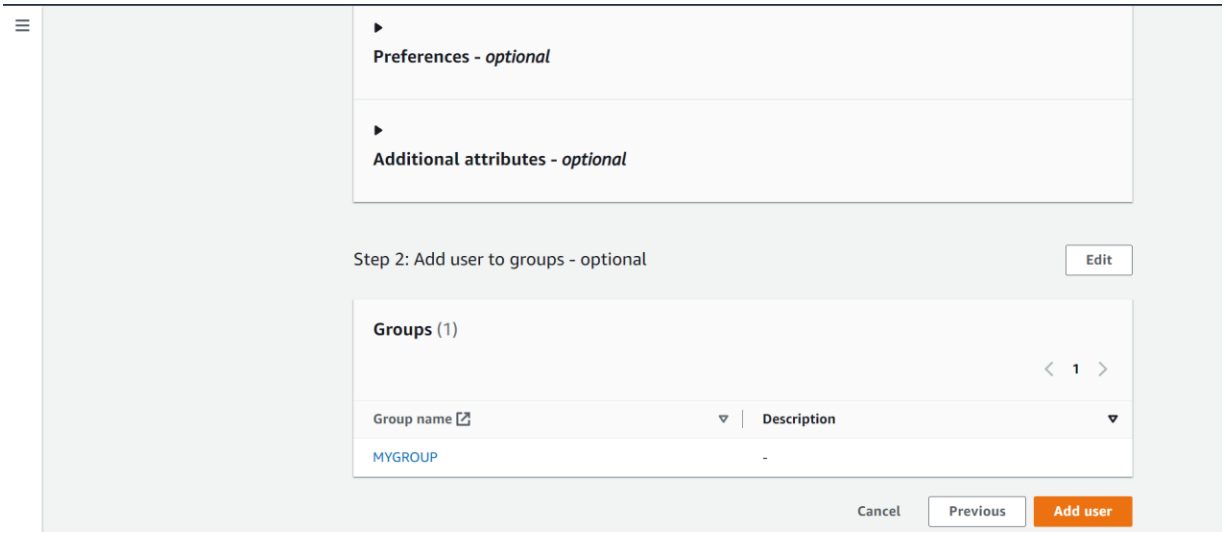


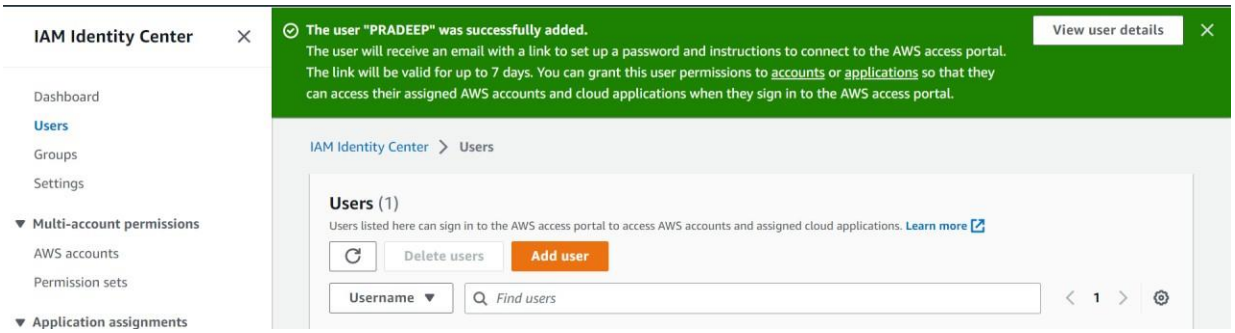
Create users

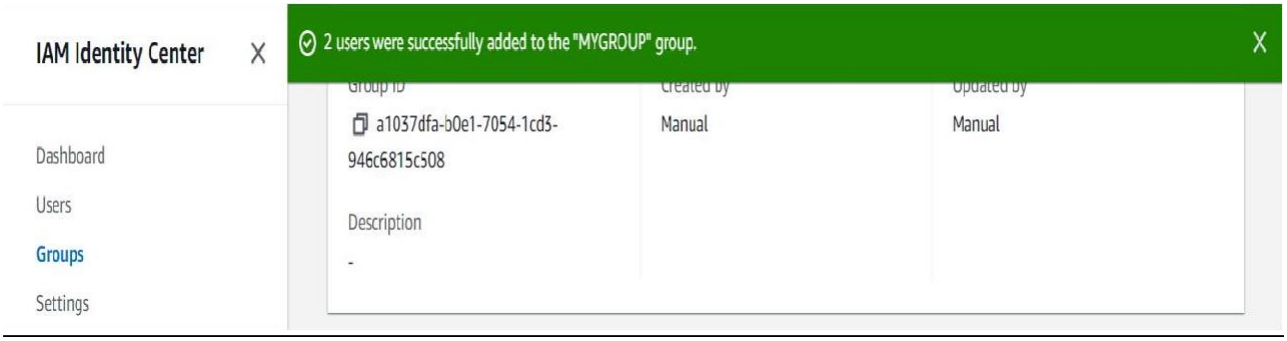
CLOUD COMPUTING JOURNAL











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