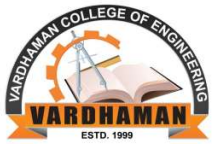


VARDHAMAN COLLEGE OF ENGINEERING

(AUTONOMOUS)

Affiliated to **JNTUH,** Approved by **AICTE,** Accredited by **NAAC** with **A++** Grade, **ISO 9001:2015** Certified
Kacharam, Shamshabad, Hyderabad - 501218, Telangana, India

www.vardhaman.org

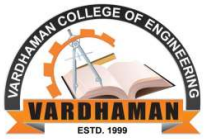
DEPARTMENT OF

COMPUTER SCIENCE & ENGINEERING

(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)

LABORATORY RECORD

Registration Number	:	21881A6691
Student Name	:	Kalam Sujith Reddy
Class / Semester	:	III B. TECH II
Course Name	:	Cloud Computing & Virtualization
Course Code	:	A7514
Academic Year	:	2023-24
Regulation	:	VCE-R21



VARDHAMAN COLLEGE OF ENGINEERING
(AUTONOMOUS)
Affiliated to JNTUH, Approved by AICTE, Accredited by NAAC with A++ Grade, ISO 9001:2015 Certified
Kacharam, Shamshabad, Hyderabad - 501218, Telangana, India
www.vardhaman.org

DEPARTMENT OF

COMPUTER SCIENCE & ENGINEERING

(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)

CERTIFICATE

Certified that this is the bonafied record of practical work done by Mr. Kalam Sujith Reddy Roll Number 21881A6691 of B.Tech III Year CSE(AI&ML) in the Cloud Computing & Virtualization laboratory during the year 2023-24.

Date: ***HOD*** ***Staff Incharge***

Internal Examiner *External Examiner*

1. **Course Description:**

Course Overview

This course provides a hands-on comprehensive study of Cloud concepts and capabilities across the various Cloud service models including Infrastructure as a Service (IaaS), Plat- form as a Service (PaaS) and Software as a Service (SaaS). In IaaS mainstream Cloud infrastructure services and related vendor solutions are covered in detail. The course also covers the Cloud migration and security model. Students will gain hands-on experience on virtual box and advanced open-source tools like Azure, Open stack and Eucalyptus. The major motto of this course is to not just stick with the academic portion but also to encourage students to for cloud certifications to brighten their future endeavours in IT sectors.

2. **Course Outcomes (COs)**

After the completion of the course, the student will be able to:

A7514.1 Demonstrate cloud services, architecture and layers in cloud environment.

A7514.2 Identify the cloud migration model and challenges of integration in cloud sectors.

A7514.3 Make use of virtualization concepts in cloud.

A7514.4 Select cloud storage, privacy approaches for efficient implementation of cloud.

A7514.5 Implement IaaS / PaaS service on a public cloud using any open-source tool.

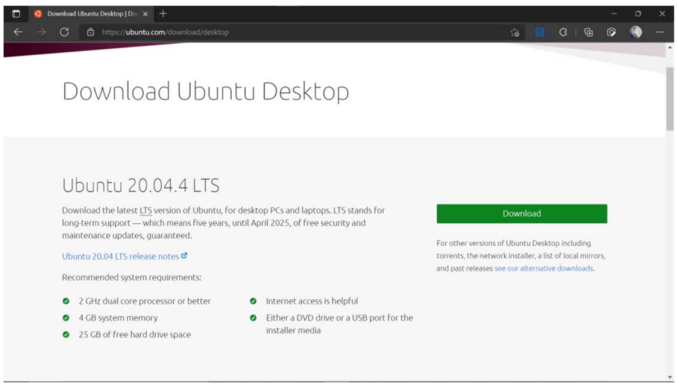
INDEX

Q1. Install the Virtual Box (or) a Malware work station and launch Linux Server.

Step-1: Download VirtualBox for Windows and install it on your computer

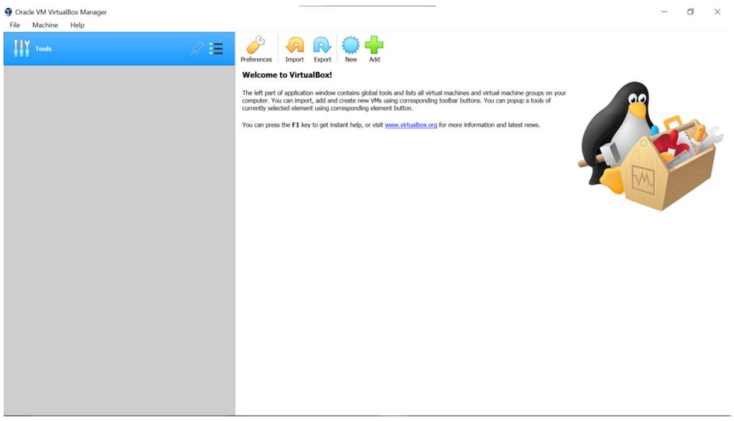
https://www.virtualbox.org/wiki/Downloads

Step-2: Download the Ubuntu ISO file you want to install from the Ubuntu download page.

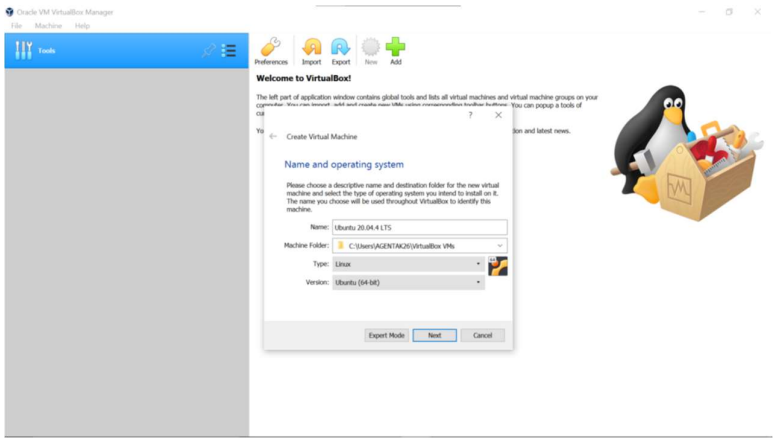


Note: The current version of Ubuntu only works on 64-bit machines.

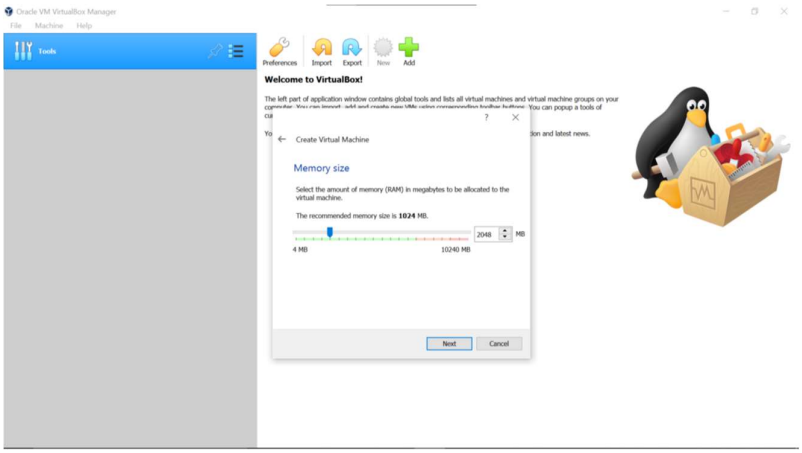
Step-3: Open VirtualBox and select New in the top taskbar.



Step-4: Give your VM a name, choose Linux as the Type, then choose Ubuntu as the Version and select Next.



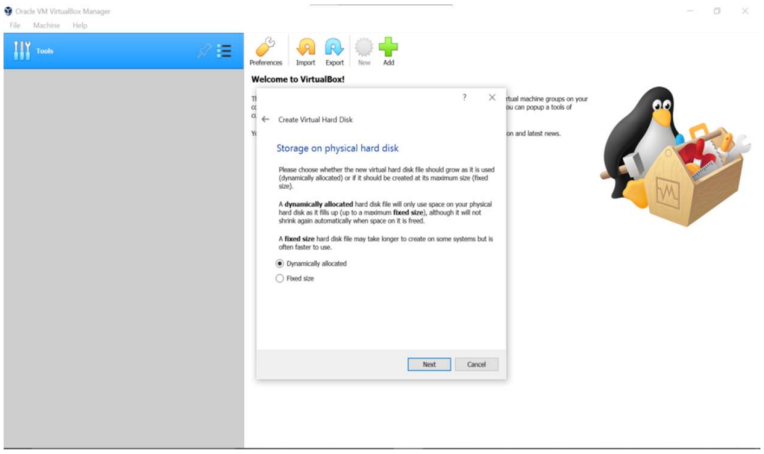
Step-5: Choose how much RAM you want to assign to the virtual machine and select Next. The recommended minimum is 1024 MB.



Step-6: Choose Create a virtual hard disk now and select Create.

Step-7: Choose VDI (VirtualBox Disk Image) and select Next.
Note on (VDI): Normally, Oracle VM VirtualBox uses its own container format for guest hard disks. This is called a Virtual Disk Image (VDI) file. This format is used when you create a new virtual machine with a new disk.

Step-8: Choose Dynamically allocated or Fixed size for the storage type and select Next.

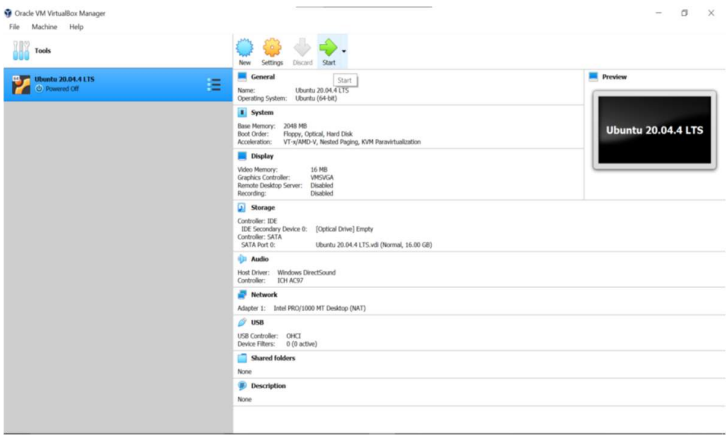


Tip: A fixed size disk performs better because the virtual machine doesn't have to increase the file size as you install software.

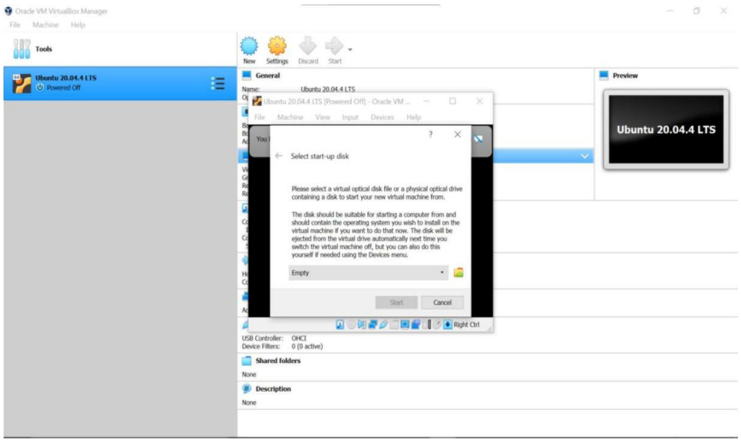
Step-9: Choose how much space you wish to set aside for Ubuntu and select Create.

Note: The amount of space you allocate for your virtual machine determines how much room you must install applications, so set aside a sample amount.

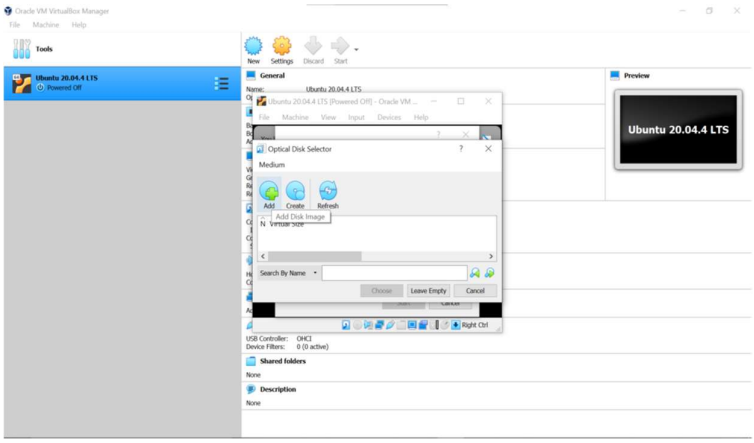
Step-10: The name of your virtual machine will now appear on the left side of the VirtualBox manager. Select Start in the toolbar to launch your VM.



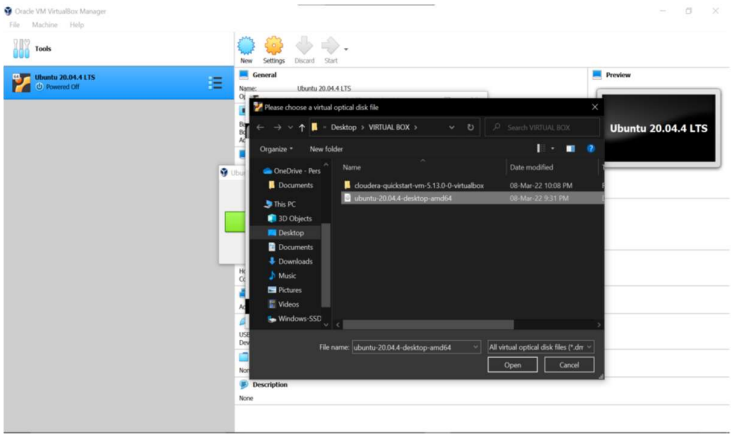
Step-11: This is the point where you need to choose the Ubuntu ISO file you downloaded earlier. If the VM doesn't automatically detect it, select the folder next to the Empty field.



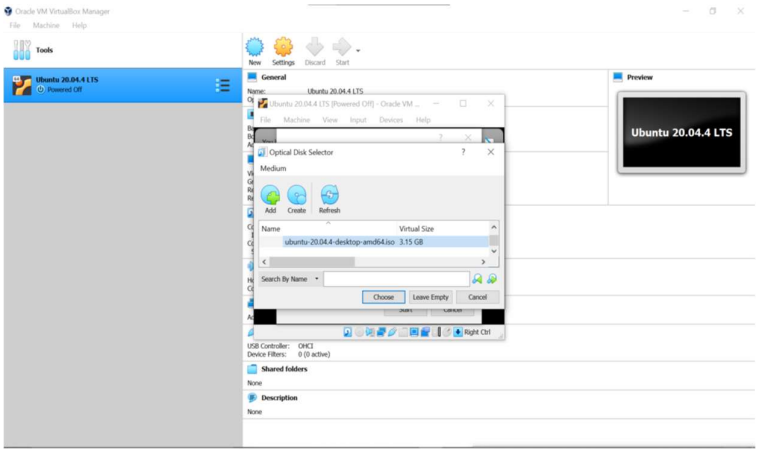
Step-12: Select Add in the window that pops up.



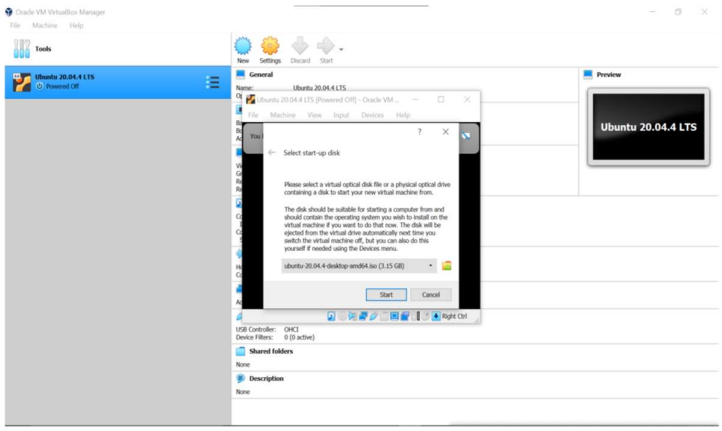
Step-13: Choose your Ubuntu disk image and select Open.



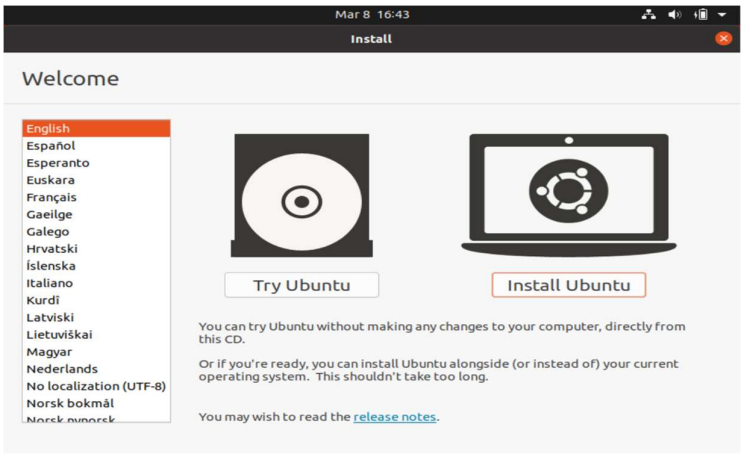
Step-14: - Select Choose



Step-15: Select Start.



Step-16: Your VM will now boot into a live version of Ubuntu. Choose your language and select Install Ubuntu



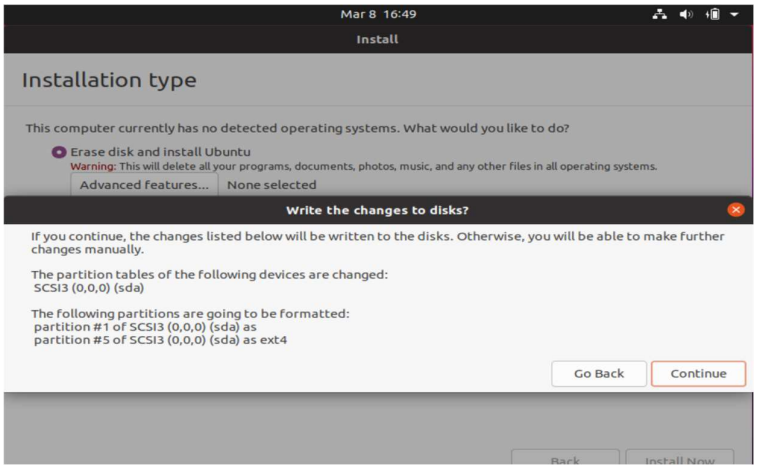
u.

Step-17: Choose your keyboard layout and select Continue.

Step-18: Choose Normal installation or Minimal installation, then select Continue.

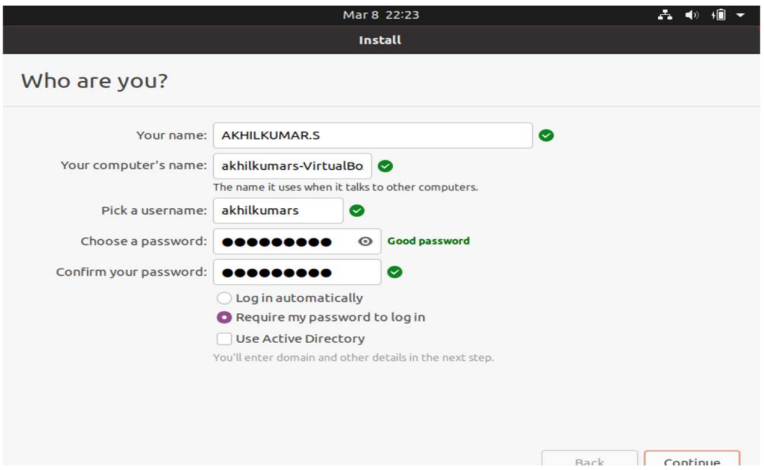
Step-19: Choose Erase disk and install Ubuntu and select Install Now, then select Continue to ignore the warning.

Note: This step will not erase your computer's physical hard drive; it only applies to the virtual machine.

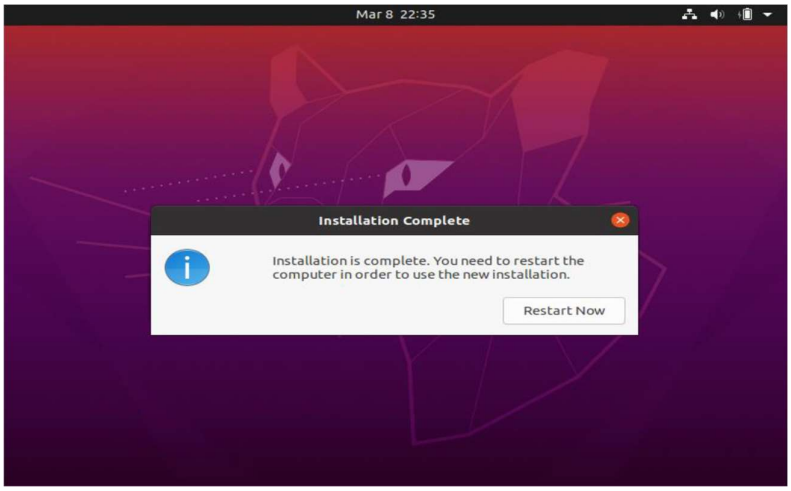


Step-20: - Choose your time zone on the map, then select Continue.

Step-21: - Set up your user account and select Continue.

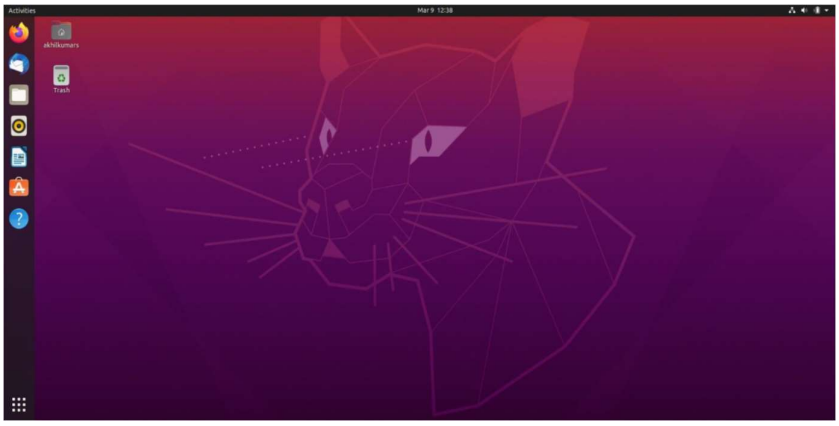


Step-22: - Select Restart Now.



Step-23: - After restarting your VM and booting into Ubuntu, you may notice that the desktop doesn't scale correctly if you choose to view it in full-screen mode. You can fix this problem by selecting the VBox_Gas icon to install VirtualBox Guest Additions.

Output:

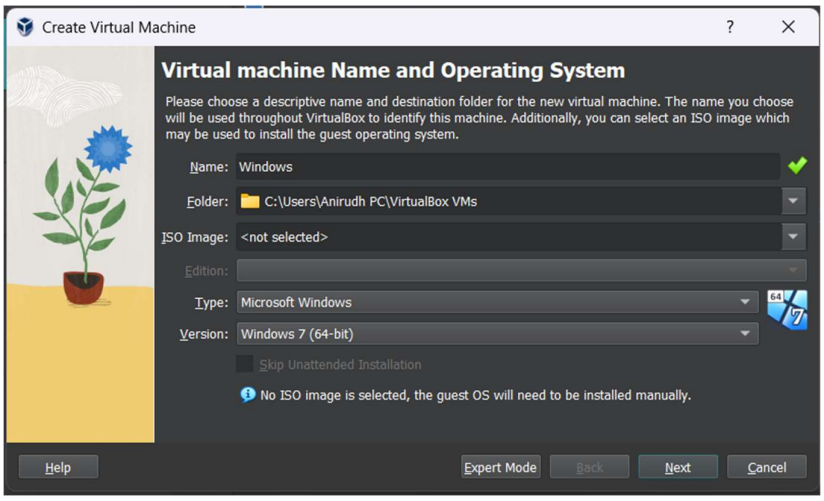


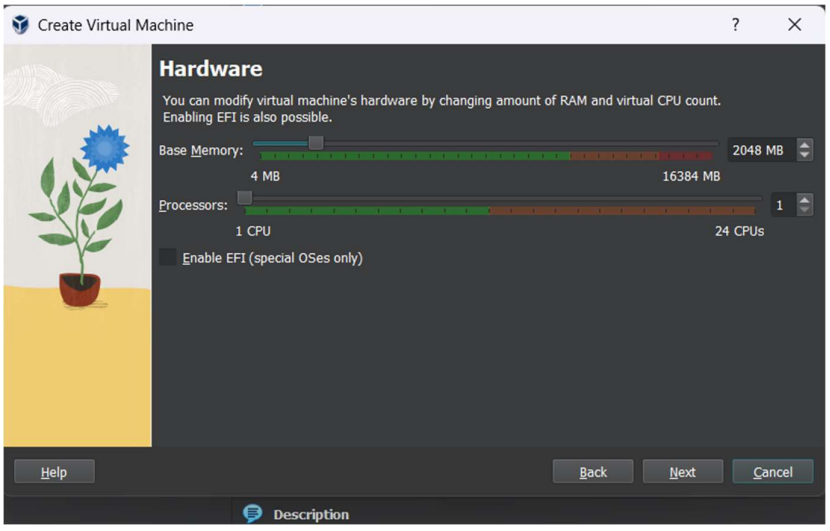
Result:

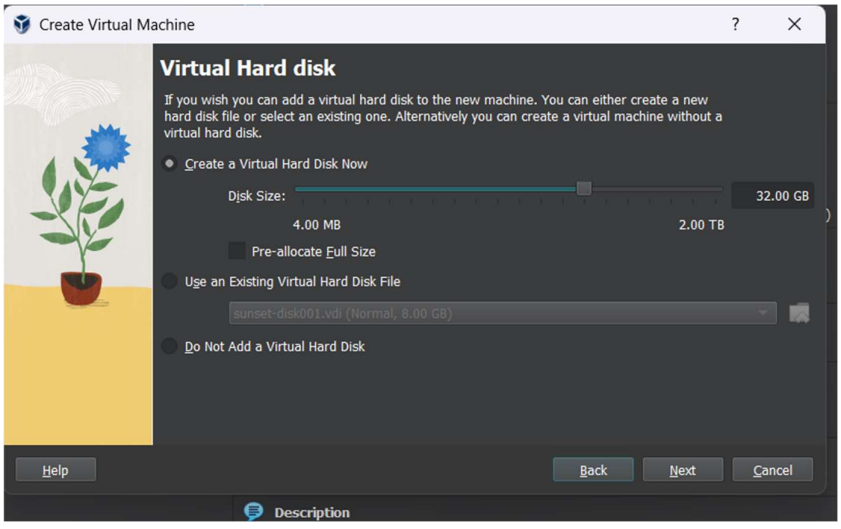
Successfully installed VirtualBox and launched a Linux server. The server was responsive, and basic operations were verified to ensure proper installation and functionality.

Q2. Install the Virtual Box (or) a Malware work station and launch Linux Server.

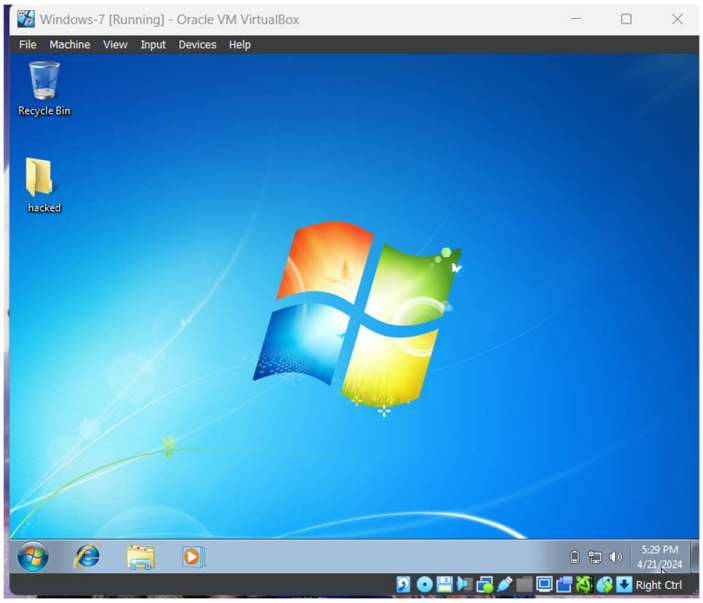
Similarly, Follow the same steps above to Build Windows Virtual Machine.







Output:



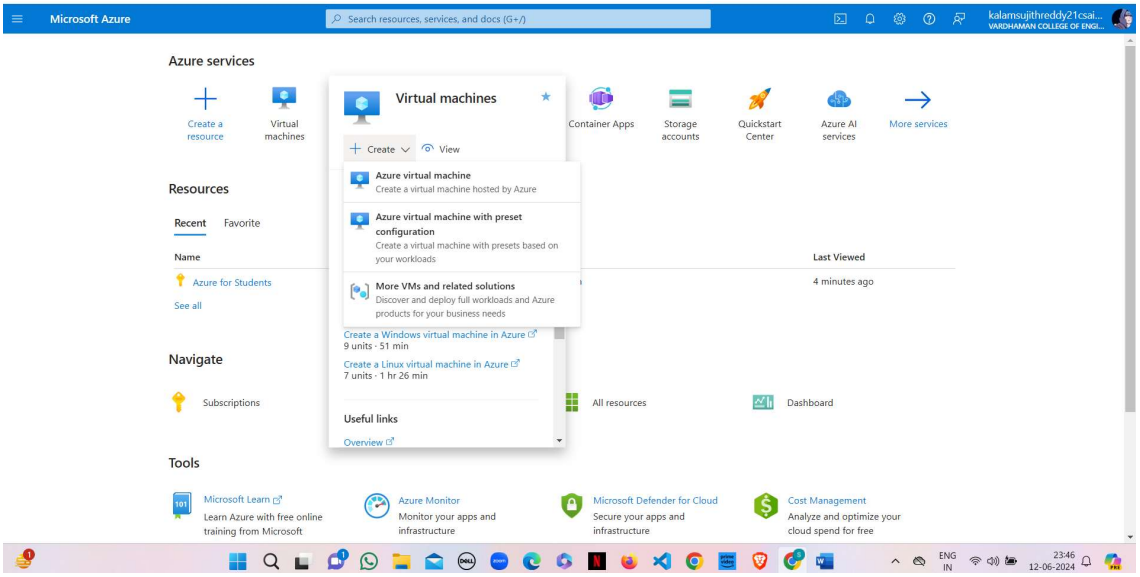
Result:

VirtualBox installation was followed by launching a Windows server. The server ran smoothly, with all core services operational, confirming the successful setup of the Windows environment.

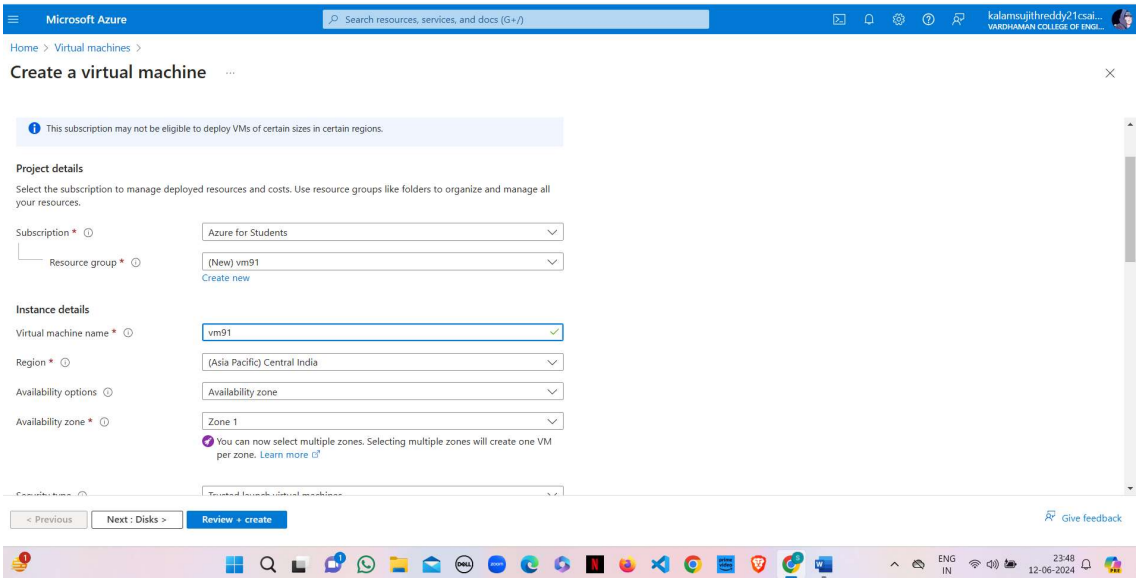
Q3) Create an instance in Virtual Machine & Launch Windows Server through Azure Portal.

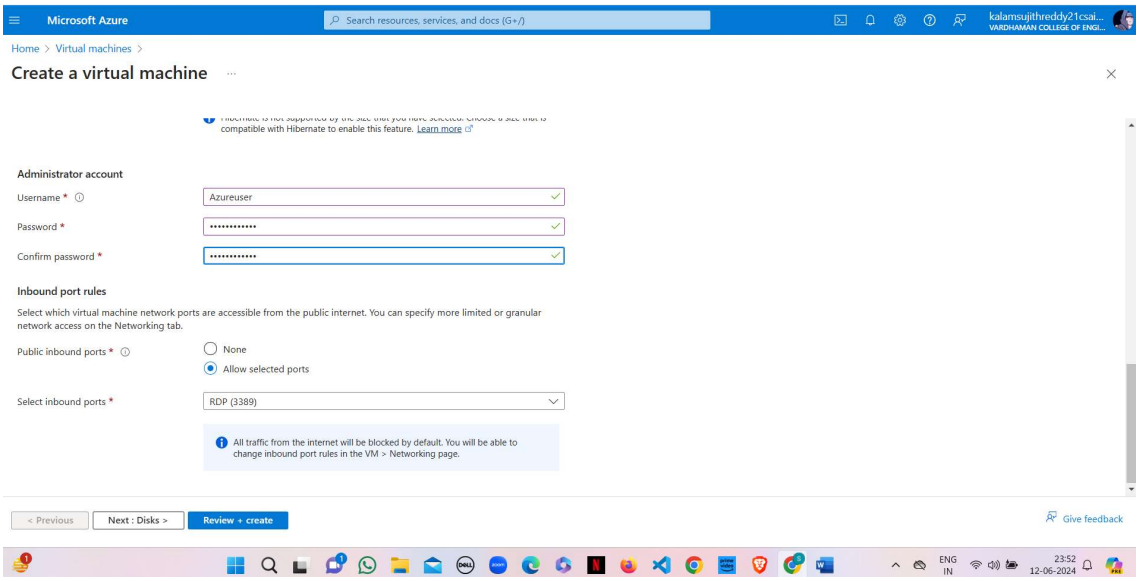
Step-1: Sign in to your Microsoft Azure account.

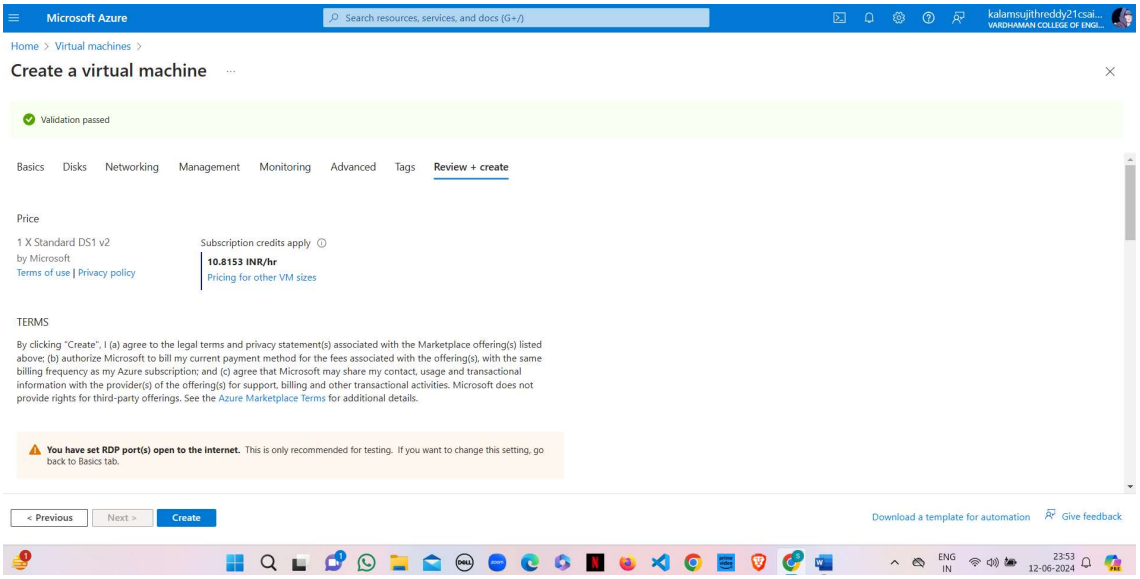
Step-2: Go To Virtual machine, and click on “Create” to create a window virtual machine.



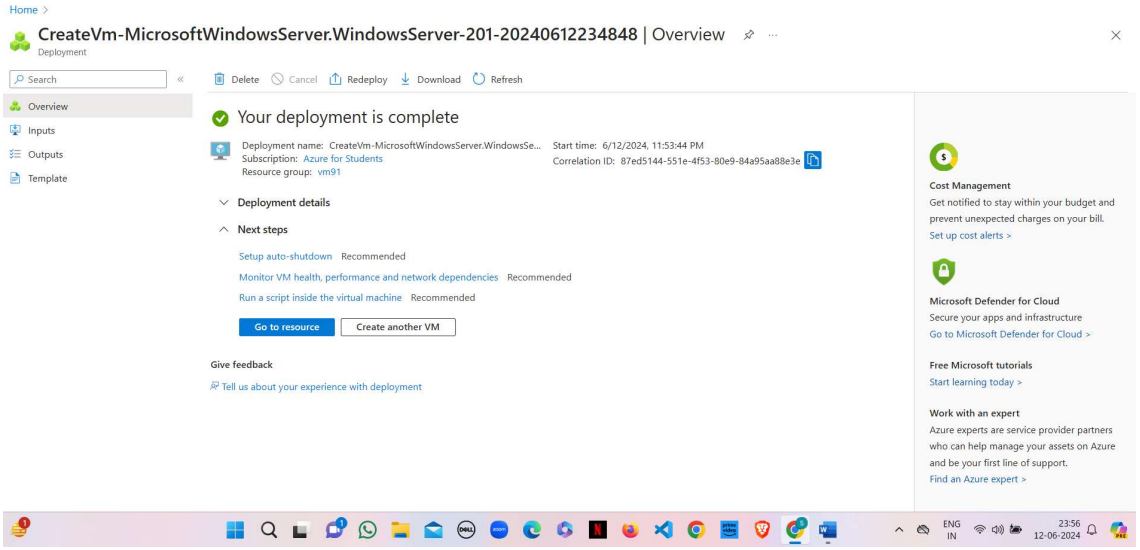
Step-3: Fill the details in that window by creating a “Resource Group”, Zone: Asia, Image: window, Select the disk storage and so on. After that click on “Create + Review”. And Finally click on “Create”

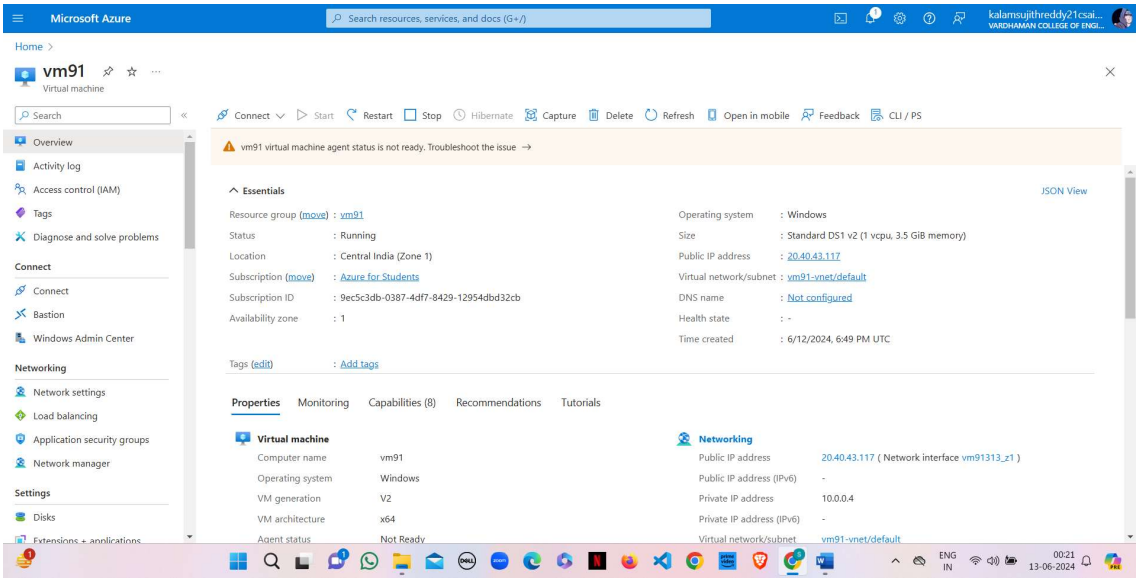




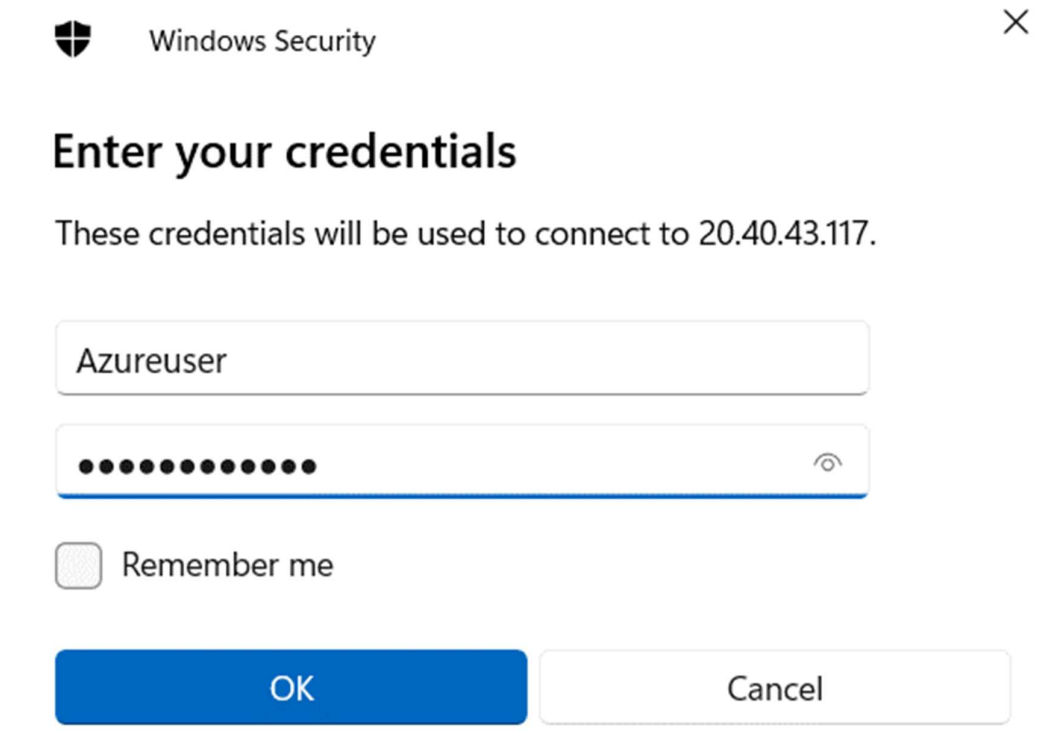


Step-4: After Deployment is over, Go to the remote desktop connection.



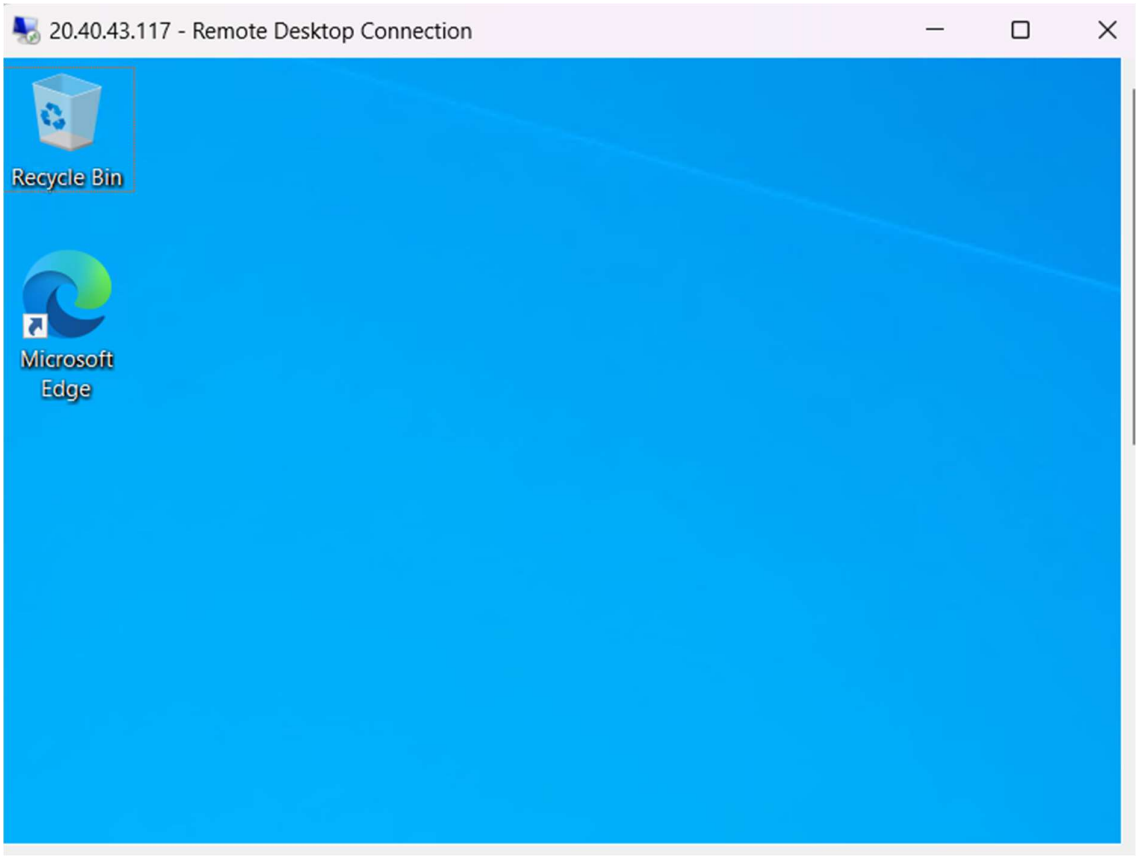


Step-5: Firstly, copy the public IP Address of that created virtual machine.



Step-6: By using that copied IP Address open the window virtual machine through remote desktop connection.

Output:



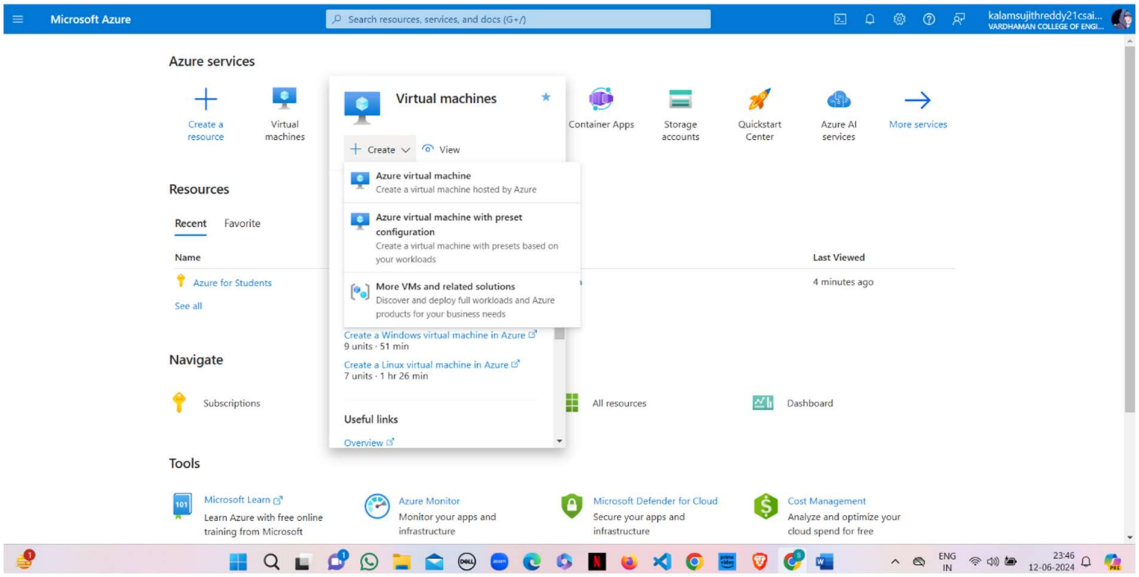
Result:

Created a new virtual machine instance on the Azure portal and launched a Windows server. The server instance was up and running with no issues, and connectivity was confirmed through remote desktop access.

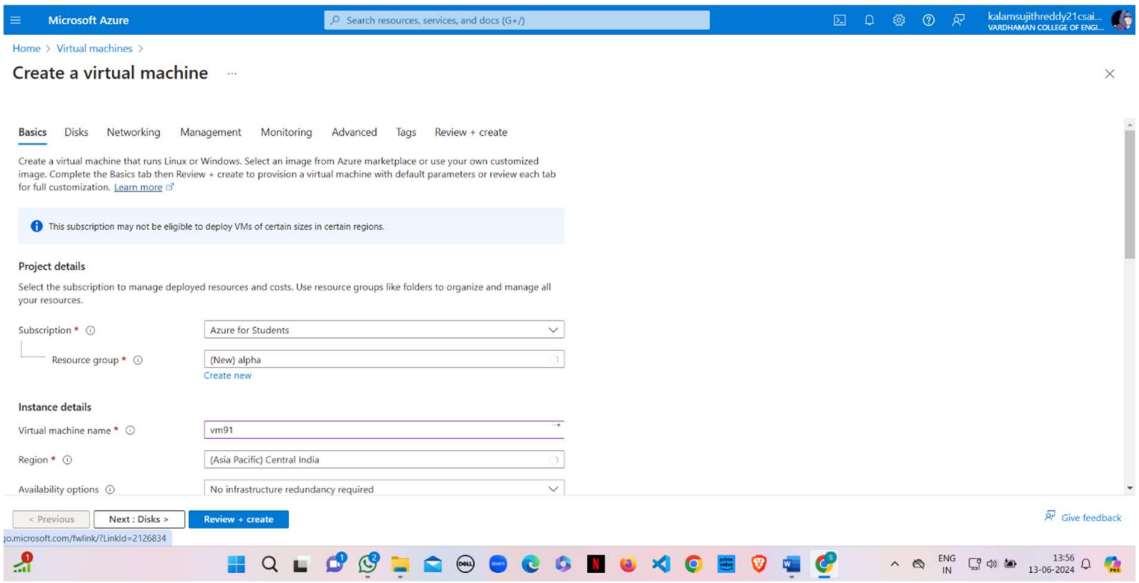
Q4) Launch Linux Server through Azure Portal.

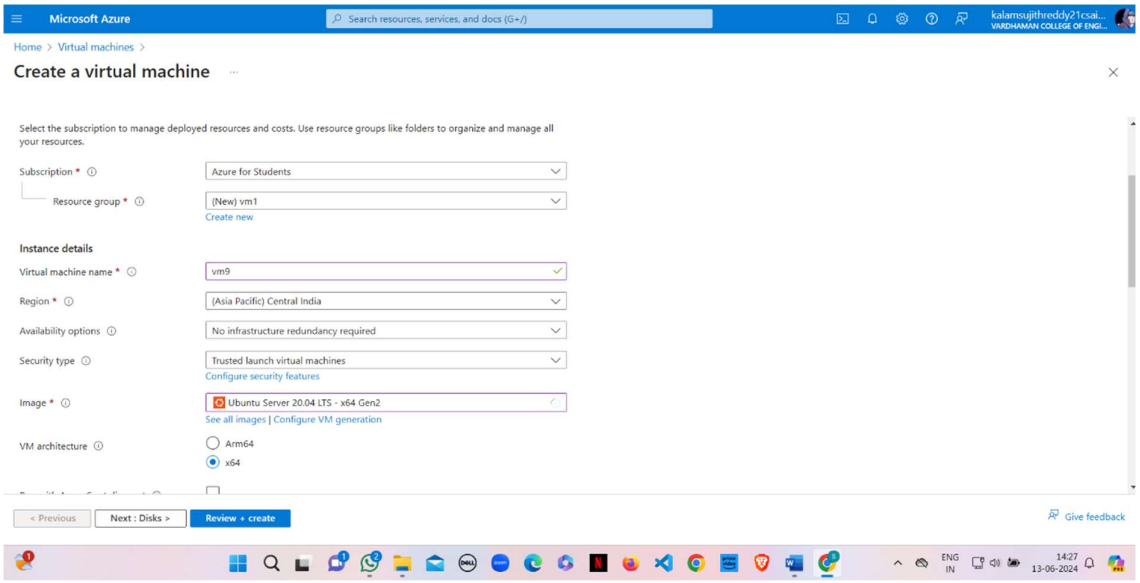
Step-1: Sign in to your Microsoft Azure account.

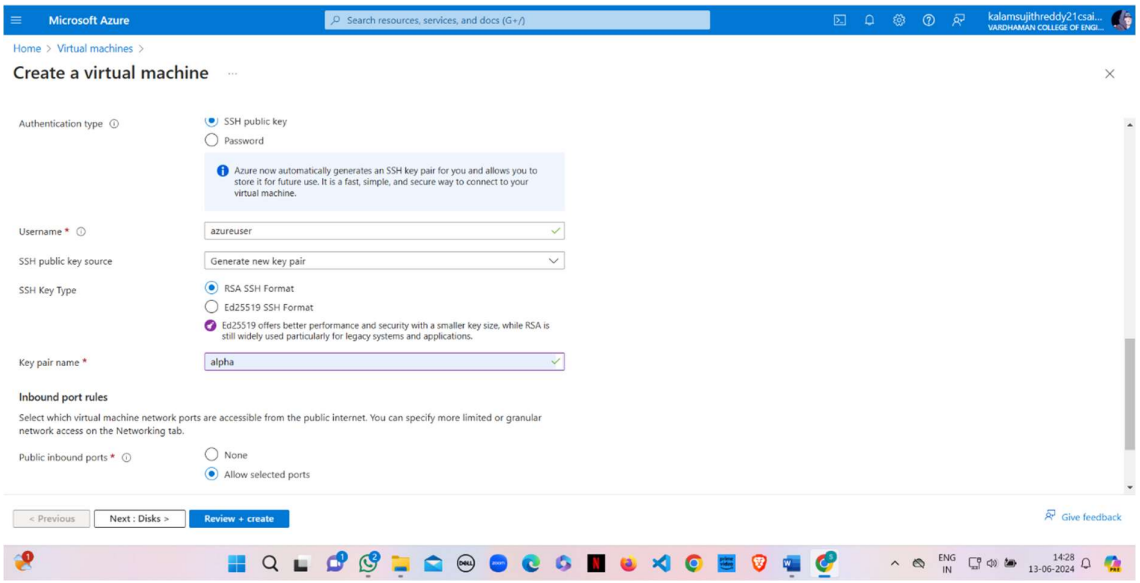
Step-2: Go To Virtual machine, and click on “Create” to create a Ubuntu virtual machine.



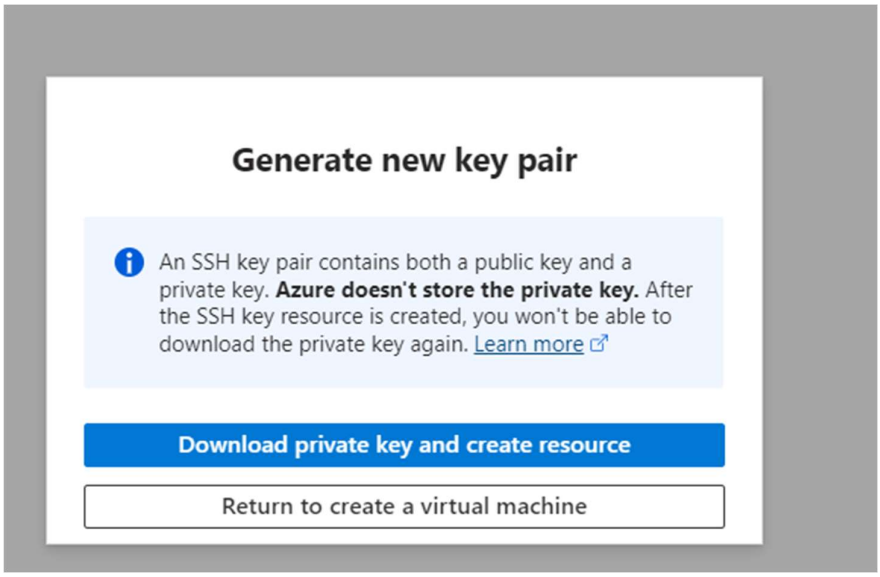
Step-3: Fill the details in that ubuntu by creating a “Resource Group”, Zone: Asia, Image: ubuntu, select “SSH”, Select the disk storage and so on. After that click on “Create + Review”. And finally click on “Create”.



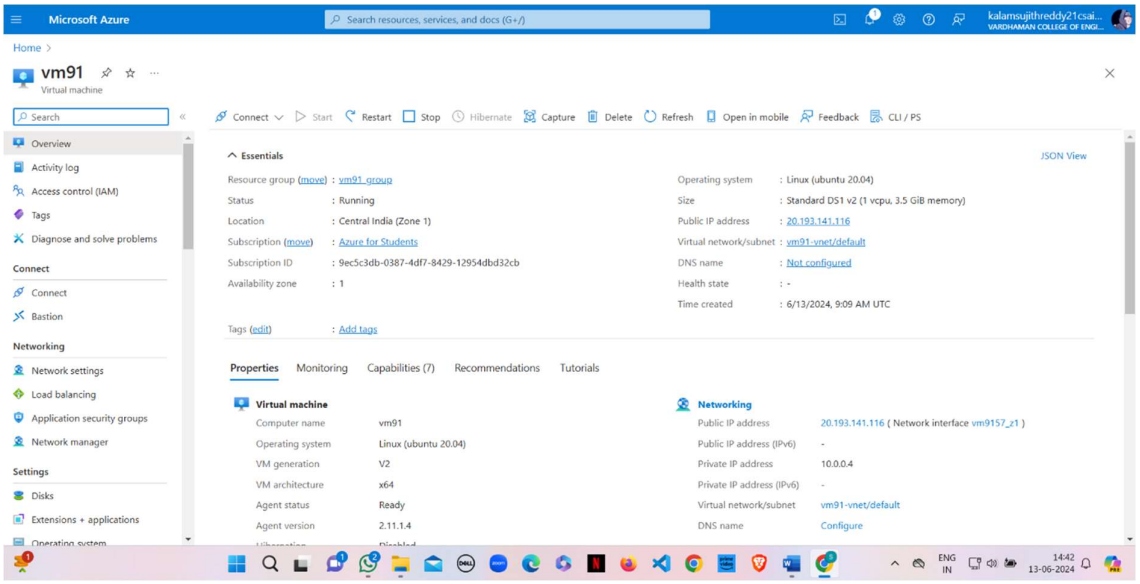

Microsoft Azure
Search resources, services, and docs (G+/)
kalamsujithreddy21csai...
VARDHAMAN COLLEGE OF ENGI...
Home > Virtual machines >
Create a virtual machine
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription * Azure for Students
Resource group * (New) vm1
Create new
Instance details
Virtual machine name * vm9
Region * (Asia Pacific) Central India
Availability options No infrastructure redundancy required
Security type Trusted launch virtual machines
Configure security features
Image * Ubuntu Server 20.04 LTS - x64 Gen2
See all images | Configure VM generation
VM architecture Arm64
x64
< Previous
Next : Disks >
Review + create
Give feedback
ENG IN
14:27
13-06-2024


Microsoft Azure
Search resources, services, and docs (G+/)
kalamsujithreddy21csai...
VARDHAMAN COLLEGE OF ENGI...
Home > Virtual machines >
Create a virtual machine
Authentication type
SSH public key
Password
Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.
Username * azureuser
SSH public key source Generate new key pair
SSH Key Type
RSA SSH Format
Ed25519 SSH Format
Ed25519 offers better performance and security with a smaller key size, while RSA is still widely used particularly for legacy systems and applications.
Key pair name * alpha
Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.
Public inbound ports *
None
Allow selected ports
< Previous
Next : Disks >
Review + create
Give feedback
ENG IN
14:28
13-06-2024

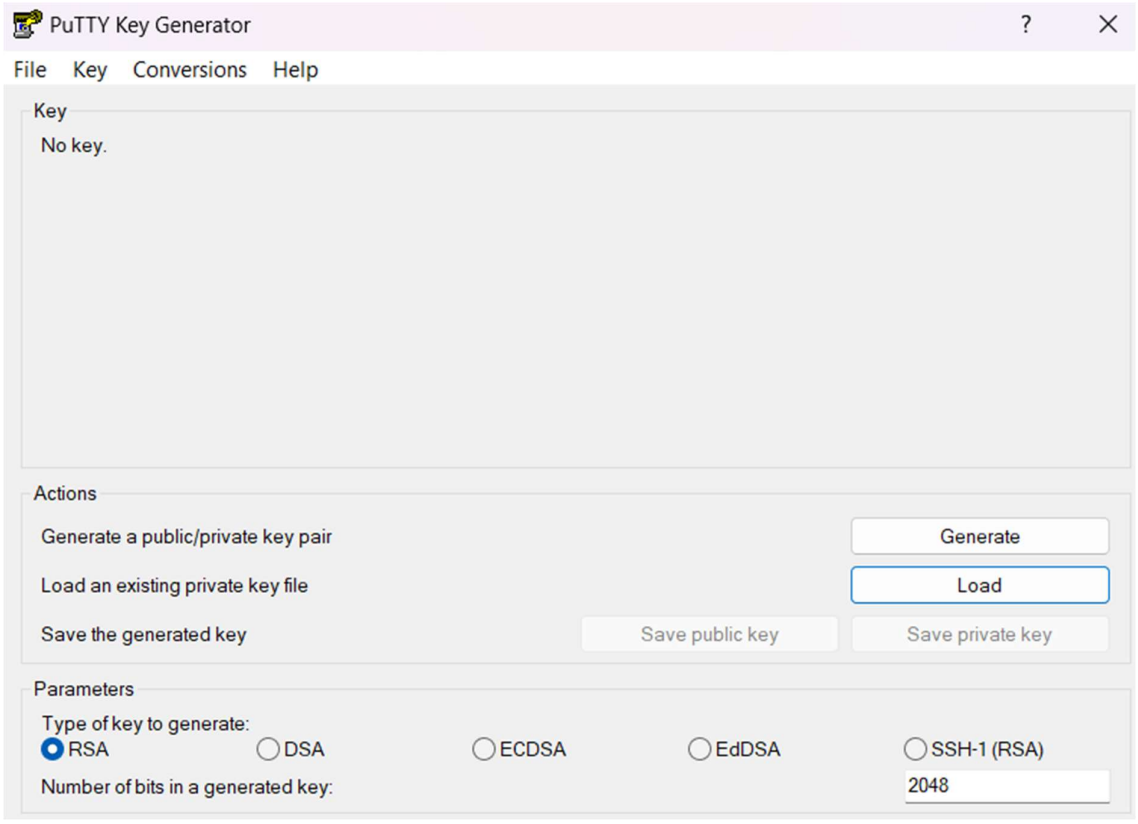
Step-4: After Deployment is over, download the private key pair.

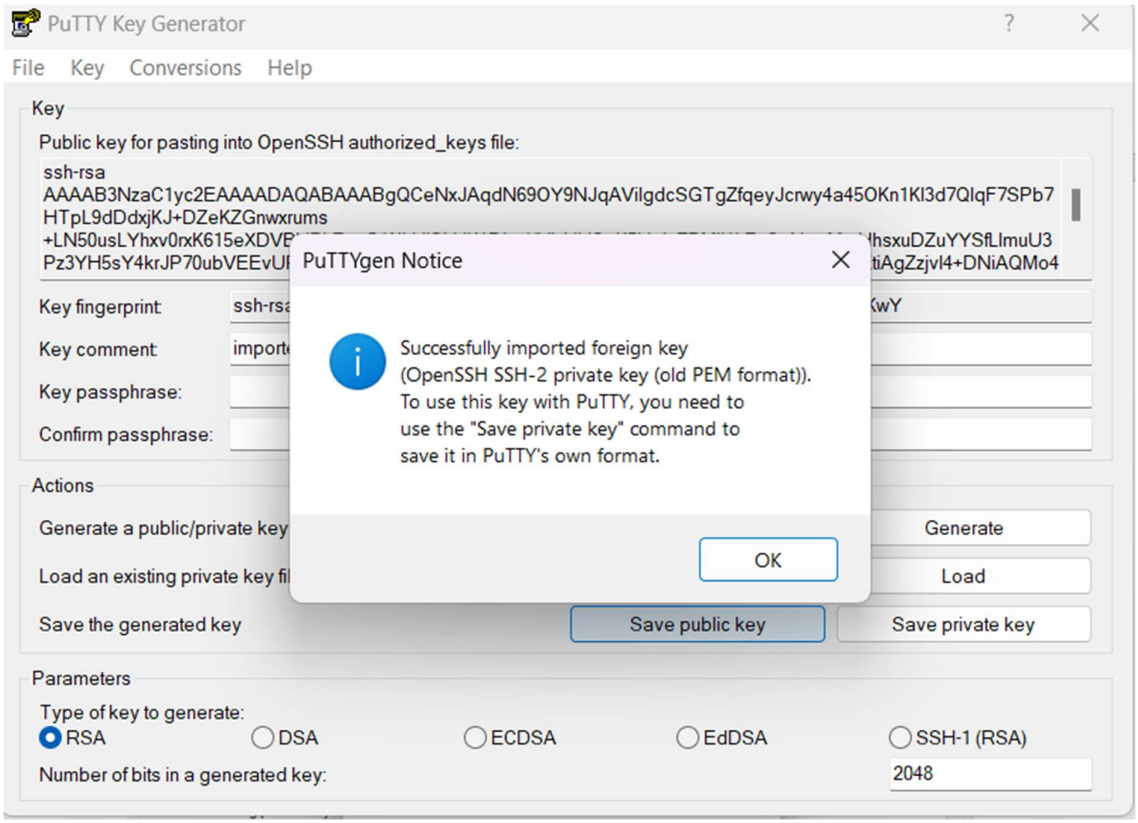


Step-5: Firstly, copy the public IP Address of that created virtual machine.

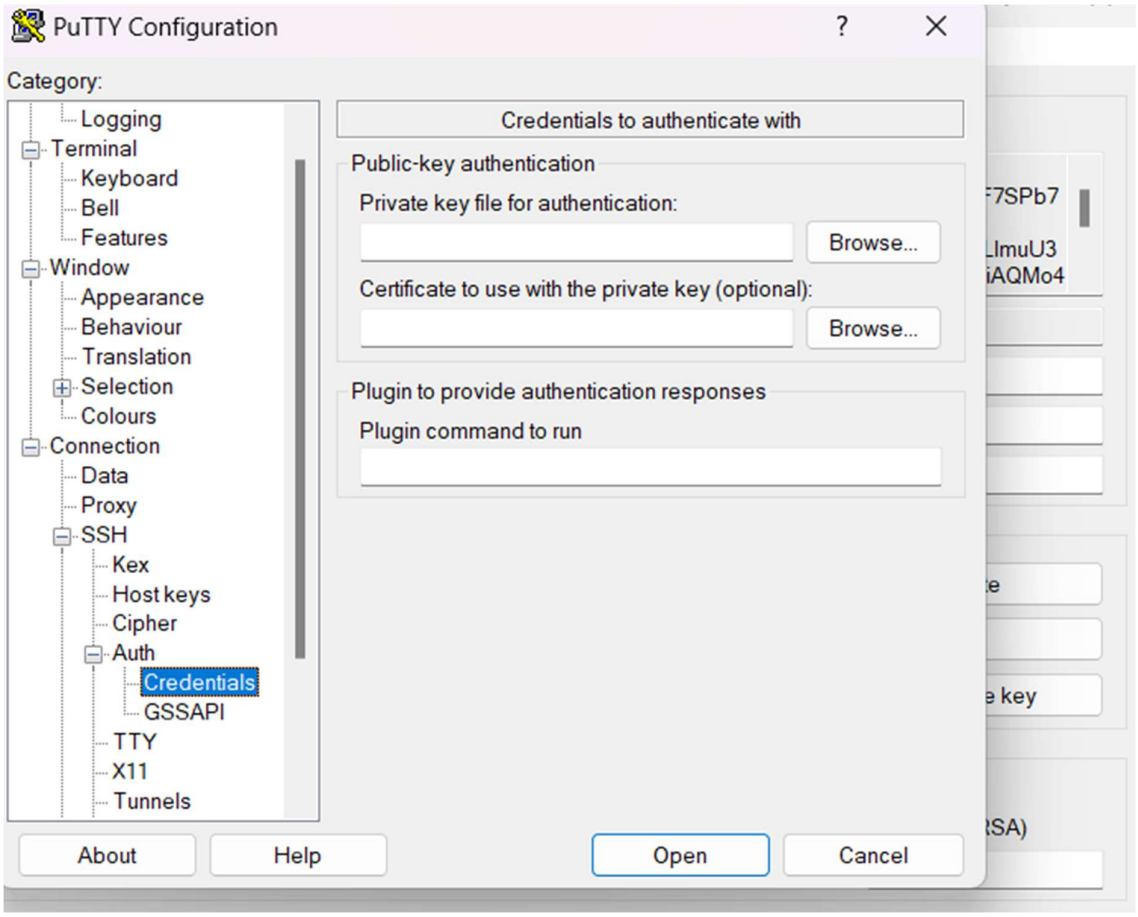


Step-6: Go to putty gen and click on load the key generator that you have downloaded.


PuTTY Key Generator
File Key Conversions Help
Key
No key.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Number of bits in a generated key:
2048

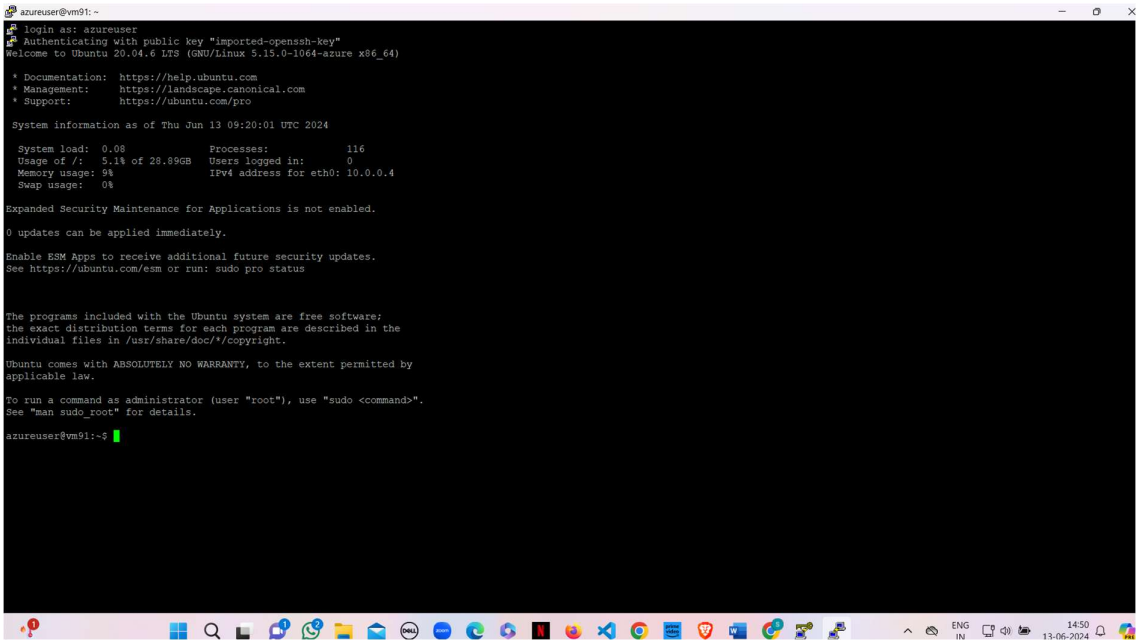

PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCeNxJAqdN69OY9NJqAVilgdcSGTgZfqeyJcrwy4a45OKn1KI3d7QIqF7SPb7
HTpL9dDdxjKJ+DZeKZGnwxrums
+LN50usLYhxv0rxK615eXDVP
Pz3YH5sY4krJP70ubVEEvUI
hsxuDZuYYSfLlmuU3
tiAgZzjvl4+DNiAQMo4
PuTTYgen Notice
Successfully imported foreign key
(OpenSSH SSH-2 private key (old PEM format)).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.
OK
Key fingerprint:
Key comment:
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key
Generate
Load an existing private key fi
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Number of bits in a generated key:
2048

Step-7: In putty, put the Copied IP Adress into it, and then go to ssh->auth->credentials and the put the generated private key.



Step-8: A login page will be opened in that type your username and you will be into the ubuntu.

Output:



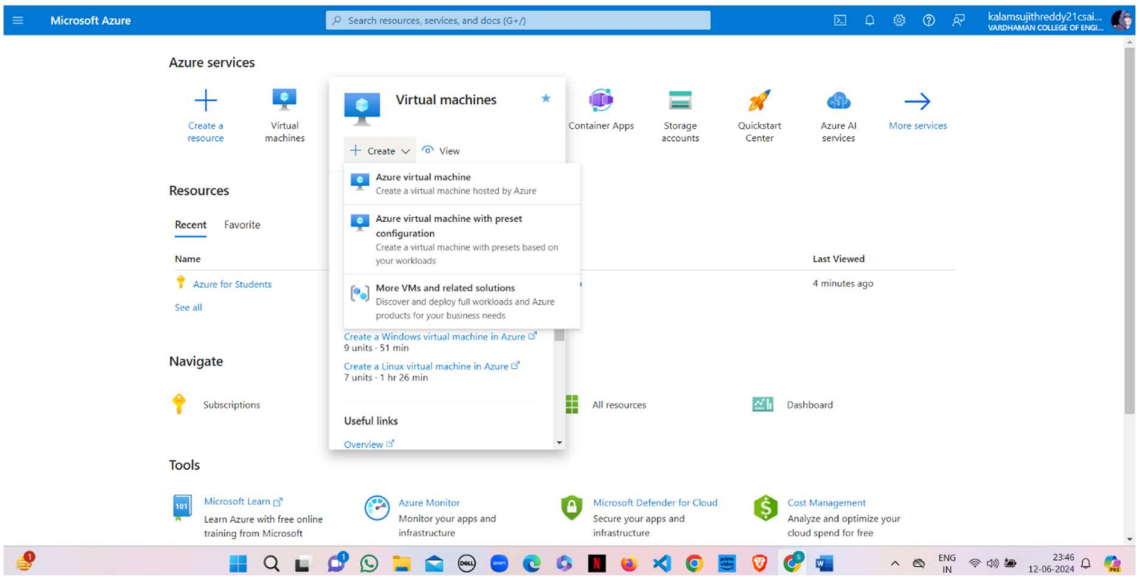
Result:

Launched a Linux server instance via the Azure portal. The server started without any hitches, and SSH access was established to perform basic system checks and updates.

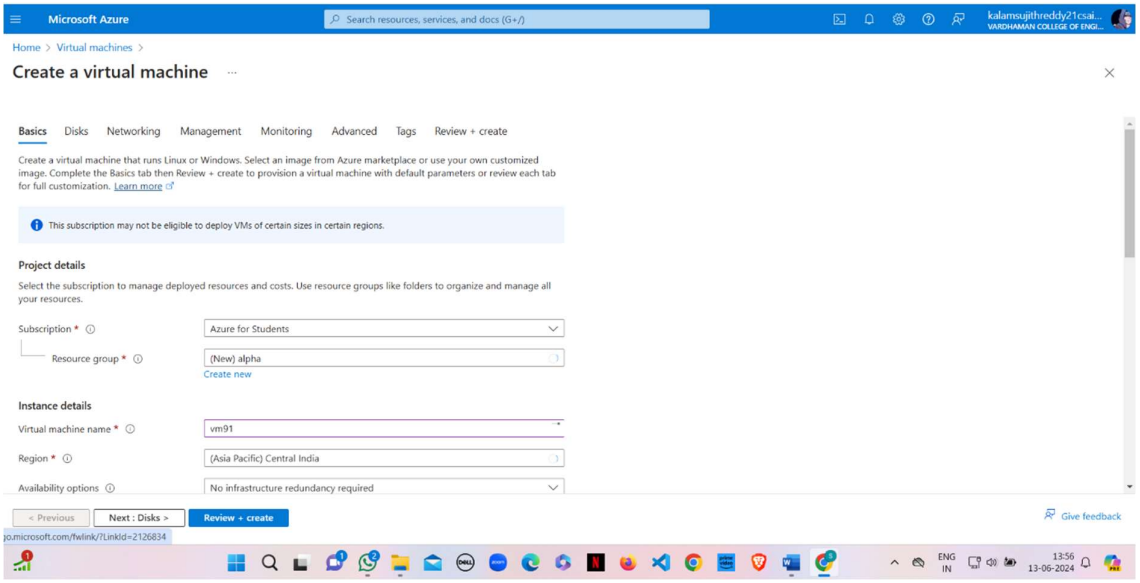
Q5) Create SSH tunnel between the host system and guest system and transfer files from local machine to Linux server (WinSCP).

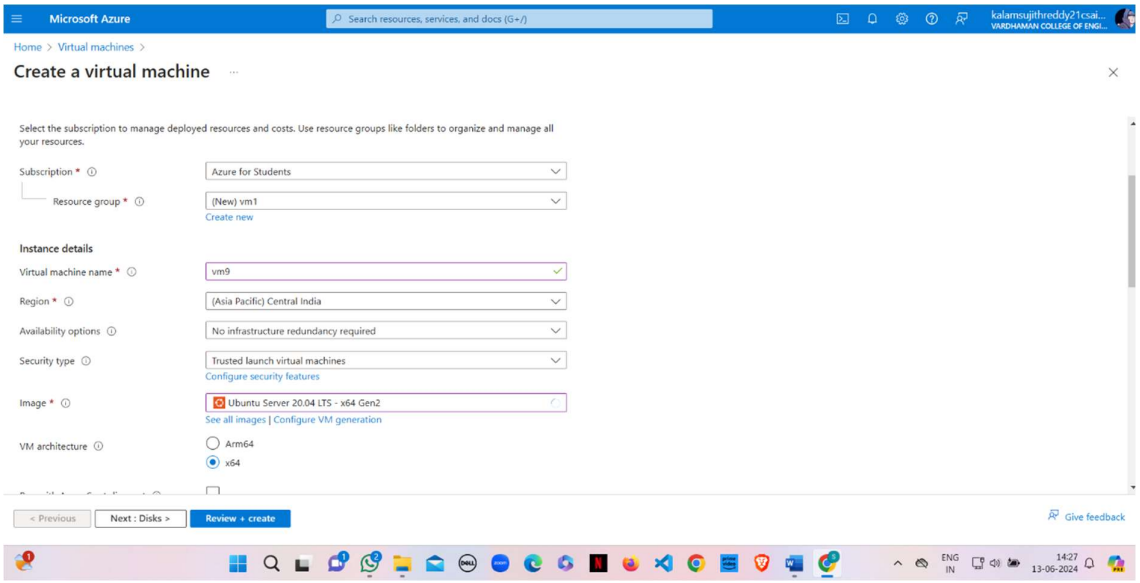
Step-1: Sign in to your Microsoft Azure account.

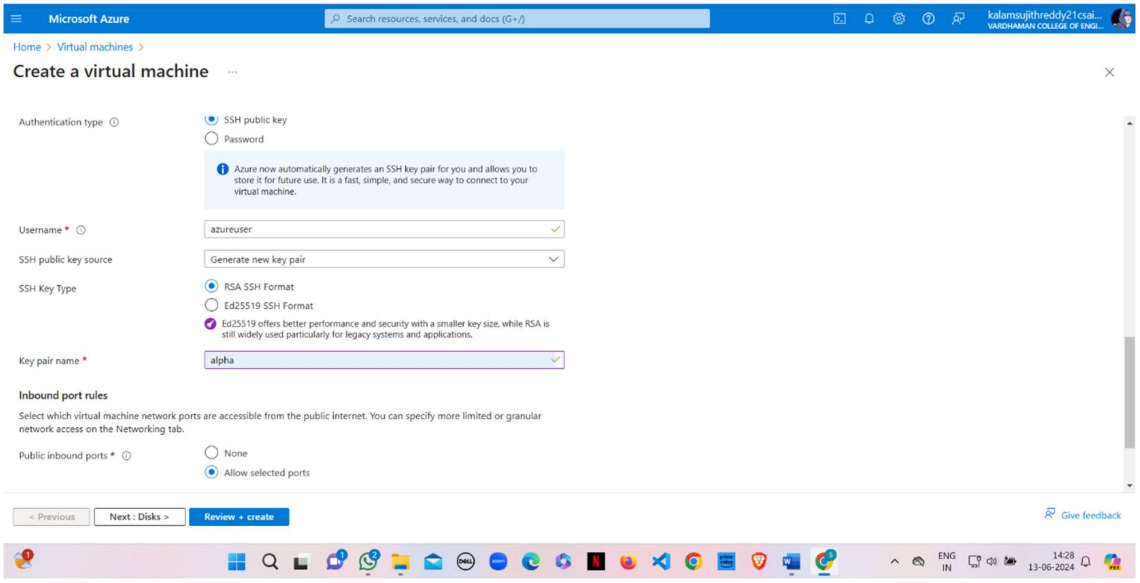
Step-2: Go To Virtual machine, and click on “Create” to create a Linux virtual machine.



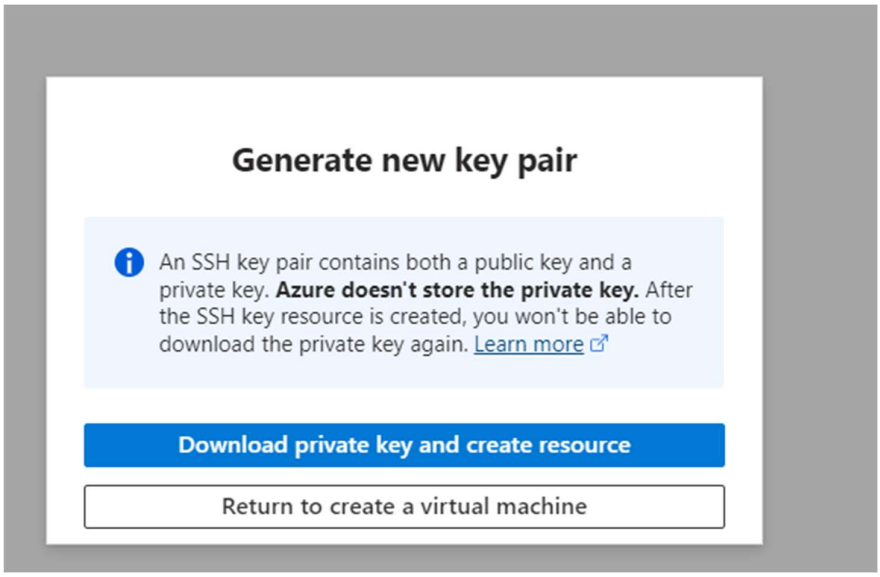
Step-3: Fill the details in that ubuntu by creating a “Resource Group”, Zone: Asia, Image: ubuntu, select “SSH”, Select the disk storage and so on. After that click on “Create + Review”. And finally click on “Create”.



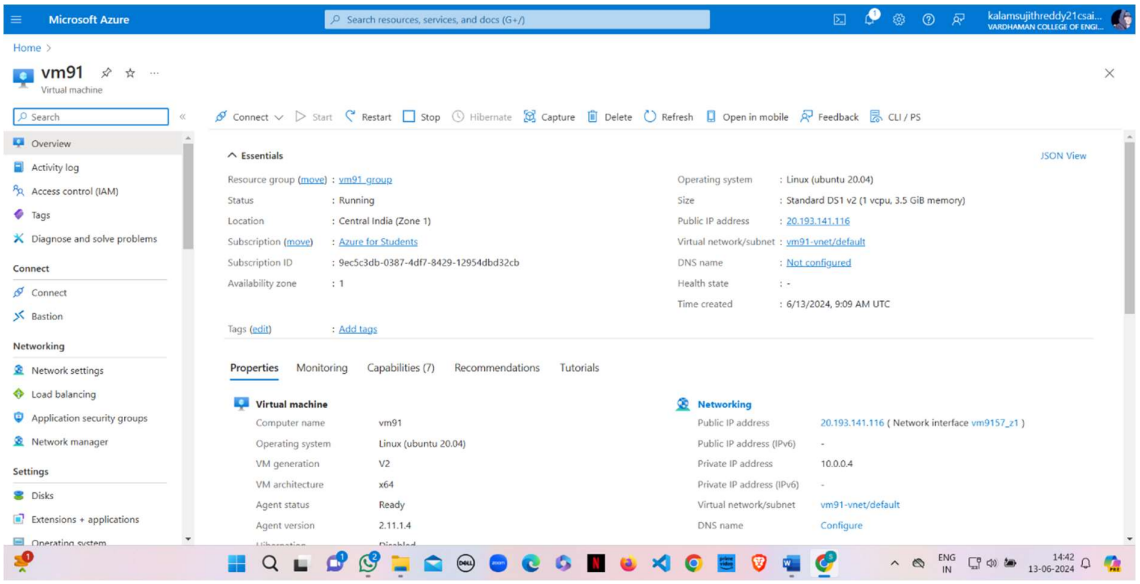

Microsoft Azure
Search resources, services, and docs (G+/)
kalamsujithreddy21csai...
VARDHAMAN COLLEGE OF ENGI...
Home > Virtual machines >
Create a virtual machine
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Azure for Students
Resource group *
(New) vm1
Create new
Instance details
Virtual machine name *
vm9
Region *
(Asia Pacific) Central India
Availability options
No infrastructure redundancy required
Security type
Trusted launch virtual machines
Configure security features
Image *
Ubuntu Server 20.04 LTS - x64 Gen2
See all images | Configure VM generation
VM architecture
Arm64
x64
< Previous
Next : Disks >
Review + create
Give feedback
ENG
IN
14:27
13-06-2024


Microsoft Azure
Search resources, services, and docs (G+/)
kalamsujithreddy21csai...
VARDHAMAN COLLEGE OF ENGI...
Home > Virtual machines >
Create a virtual machine
Authentication type
SSH public key
Password
Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.
Username *
azureuser
SSH public key source
Generate new key pair
SSH Key Type
RSA SSH Format
Ed25519 SSH Format
Ed25519 offers better performance and security with a smaller key size, while RSA is still widely used particularly for legacy systems and applications.
Key pair name *
alpha
Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.
Public inbound ports *
None
Allow selected ports
< Previous
Next : Disks >
Review + create
Give feedback
ENG
IN
14:28
13-06-2024

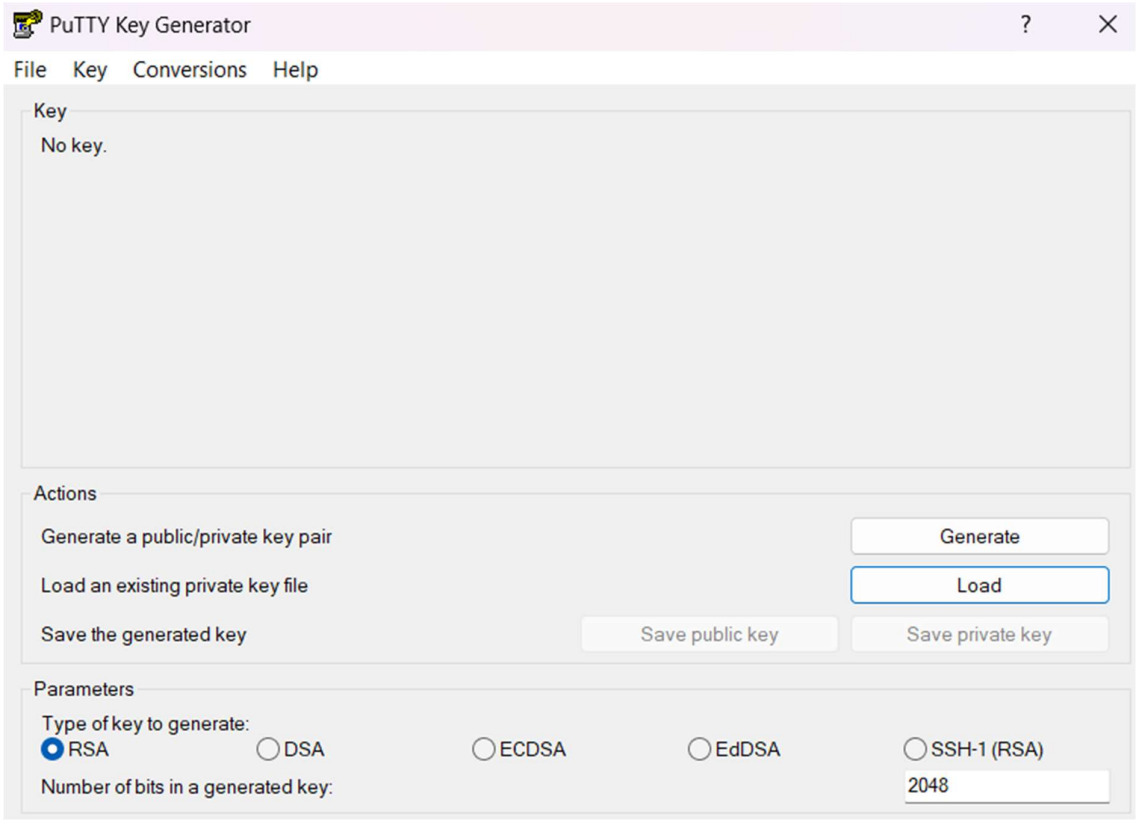
Step-4: Download the private key pair and create new resource.

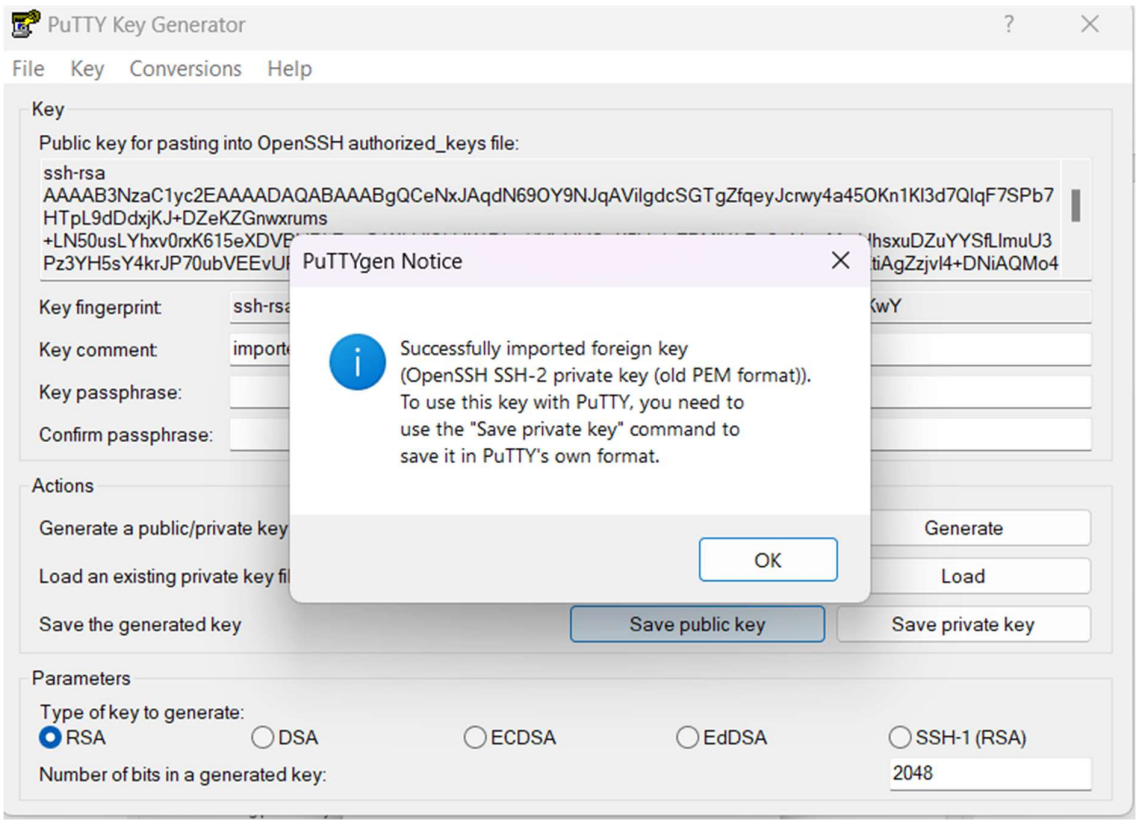


Step-5: Firstly, copy the public IP Address of that created virtual machine.

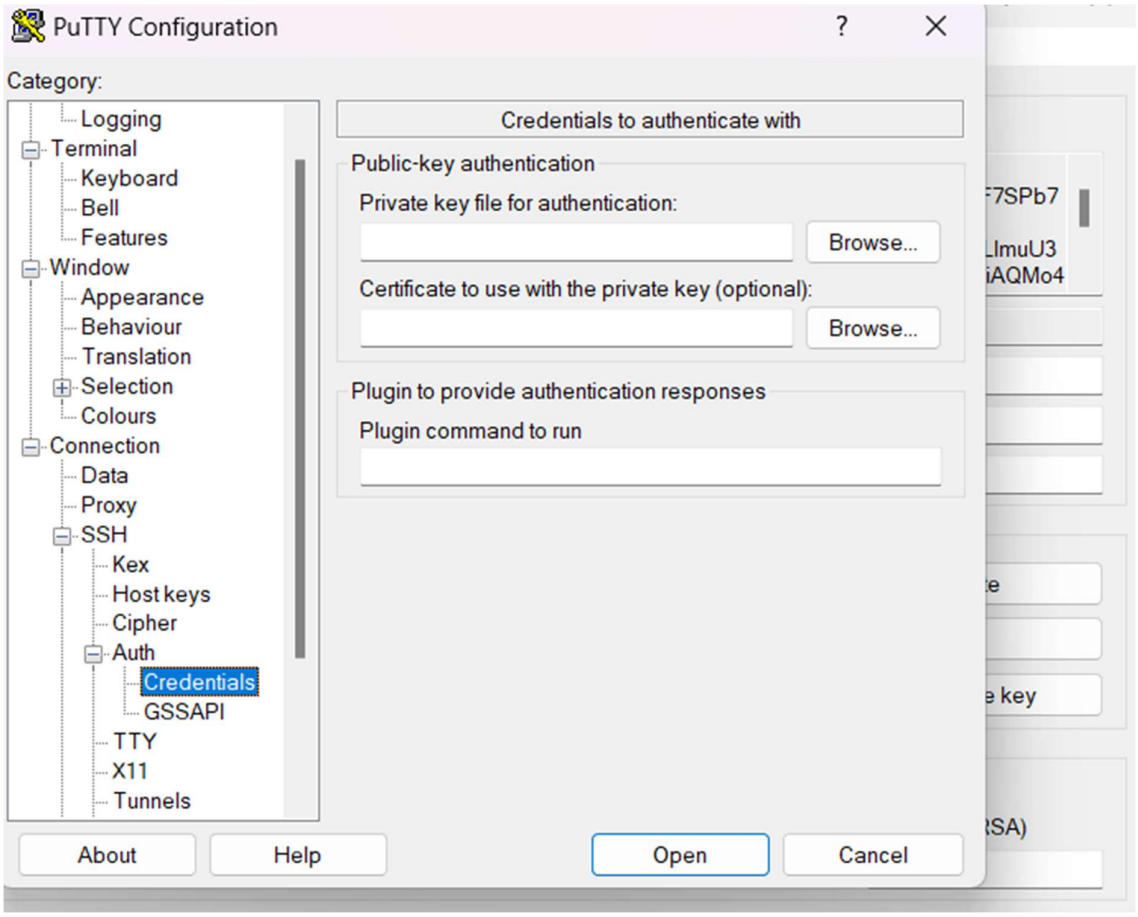


Step-6: Go to putty gen and click on load the key generator that you have downloaded.


PuTTY Key Generator
File Key Conversions Help
Key
No key.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Number of bits in a generated key:
2048

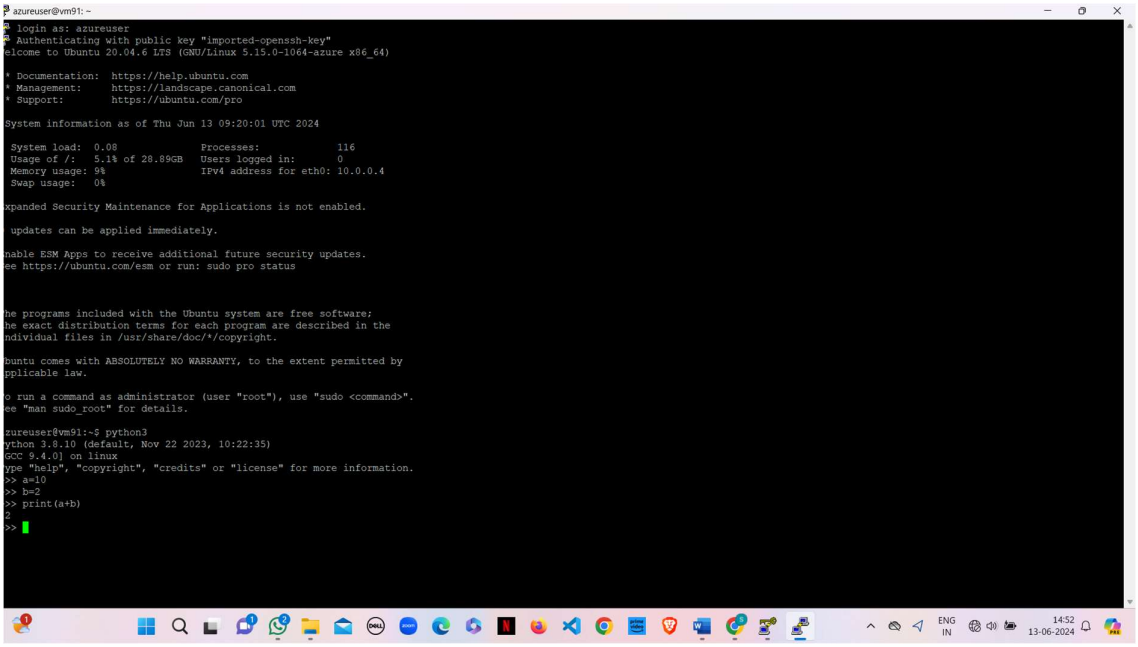

PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCeNxJAqdN69OY9NJqAVilgdcSGTgZfqeyJcrwy4a45OKn1KI3d7QIqF7SPb7
HTpL9dDdxjKJ+DZeKZGnwxrums
+LN50usLYhxv0rxK615eXDVP
Pz3YH5sY4krJP70ubVEEvUI
hsxuDZuYYSfLlmuU3
tiAgZzjvl4+DNiAQMo4
PuTTYgen Notice
Successfully imported foreign key
(OpenSSH SSH-2 private key (old PEM format)).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.
OK
Key fingerprint:
Key comment:
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key
Generate
Load an existing private key fi
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Number of bits in a generated key:
2048

Step-7: In putty, put the Copied IP Adress into it, and then go to ssh->auth->credentials and the put the generated private key.



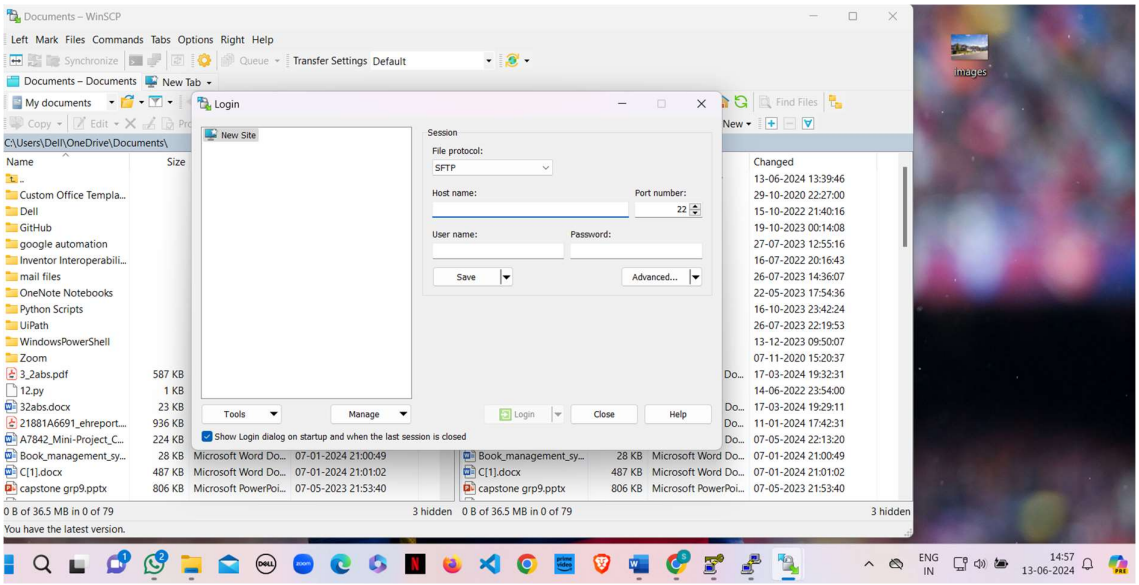
Step-8: A login page will be opened in that type your username and you will be into the ubuntu.

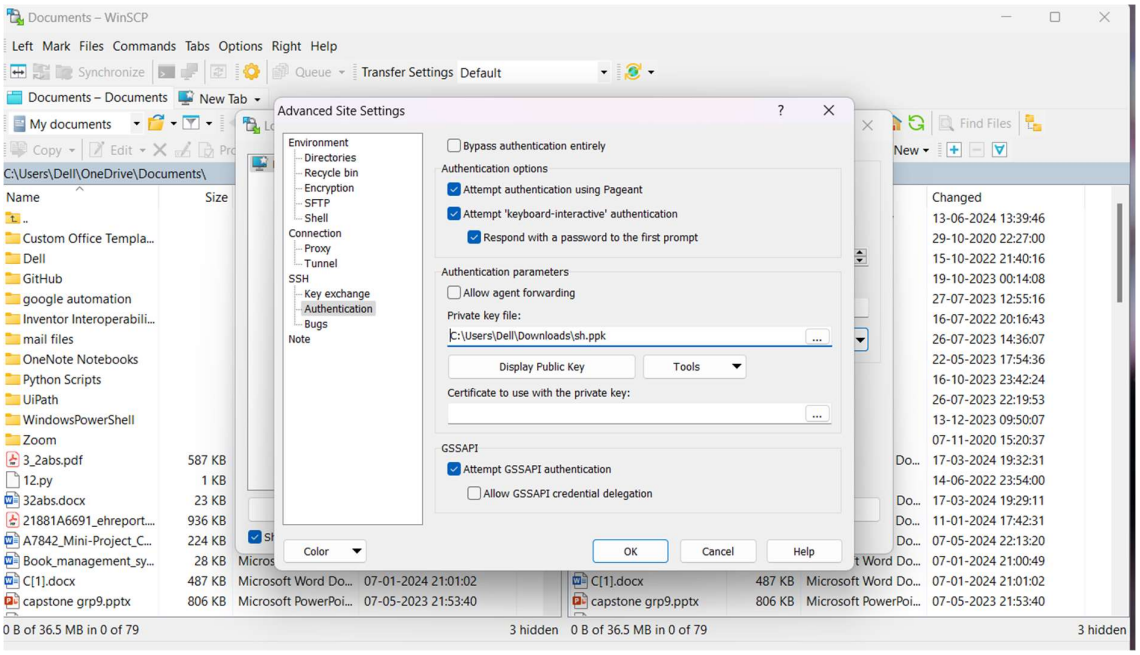
Step-9: Login into your ubuntu VM using PUTTY and type ls command as you can see nothing.



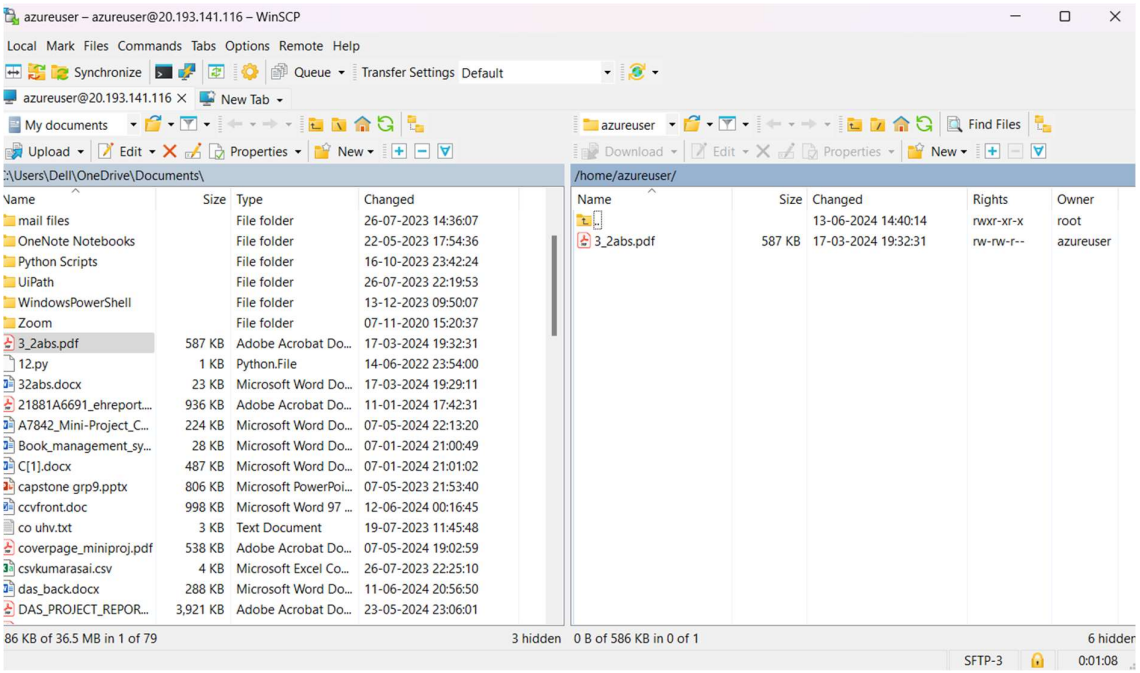
Step-10: Open WinScp at right bottom you can see Advanced option->SSH->Authentication->In that drag private key file and click on ok.

At last Login into your account using public IP address and username in WinScp.

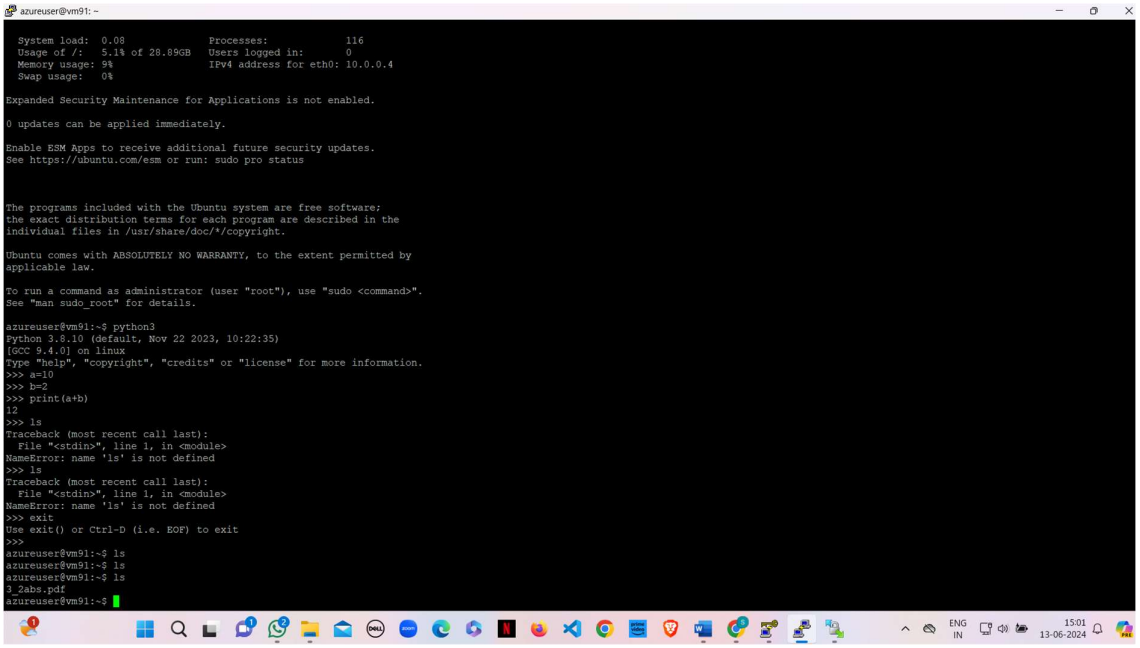




Now, you can drag your files from your desktop to ubuntu VM in WinScp.



Step-11: Now again type ls command as you can see file inside ubuntu VM.



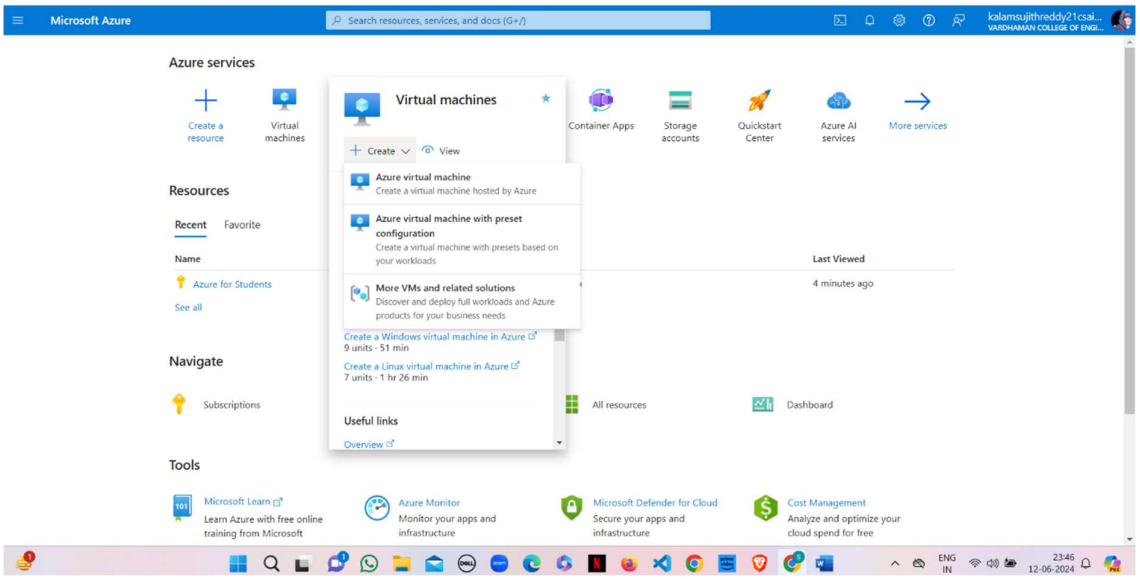
Result:

Established an SSH tunnel between the host and guest systems and successfully transferred files using WinSCP. The file transfer was smooth and error-free, confirming a secure and functional connection.

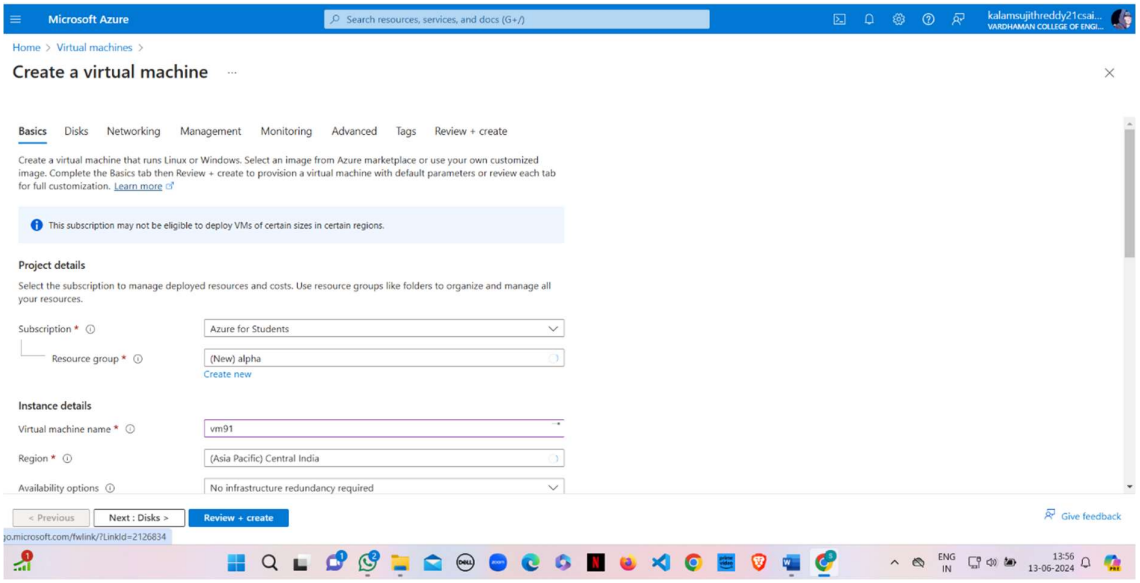
Q6) Setup and Configure Linux Server as Web Server in Azure Portal. (nginx web server)

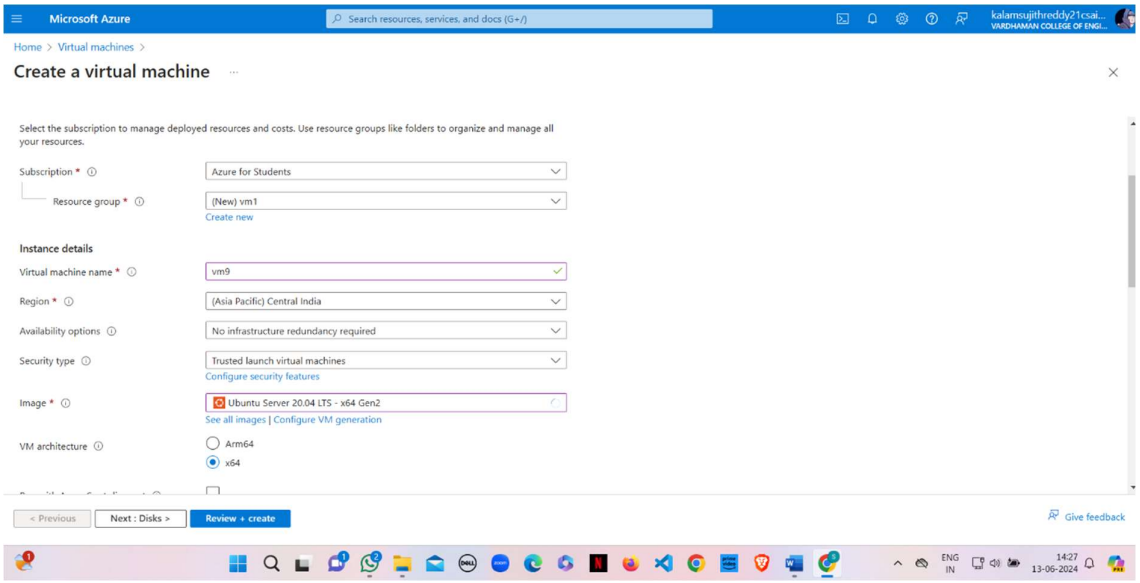
Step-1: Sign in to your Microsoft Azure account.

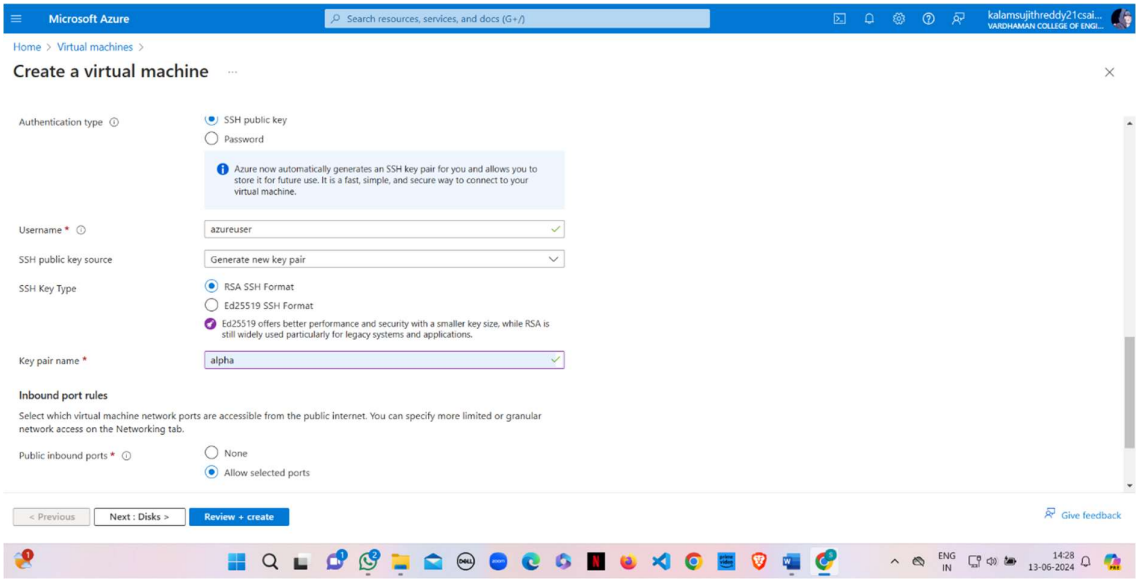
Step-2: Go To Virtual machine, and click on “Create” to create a window virtual machine.



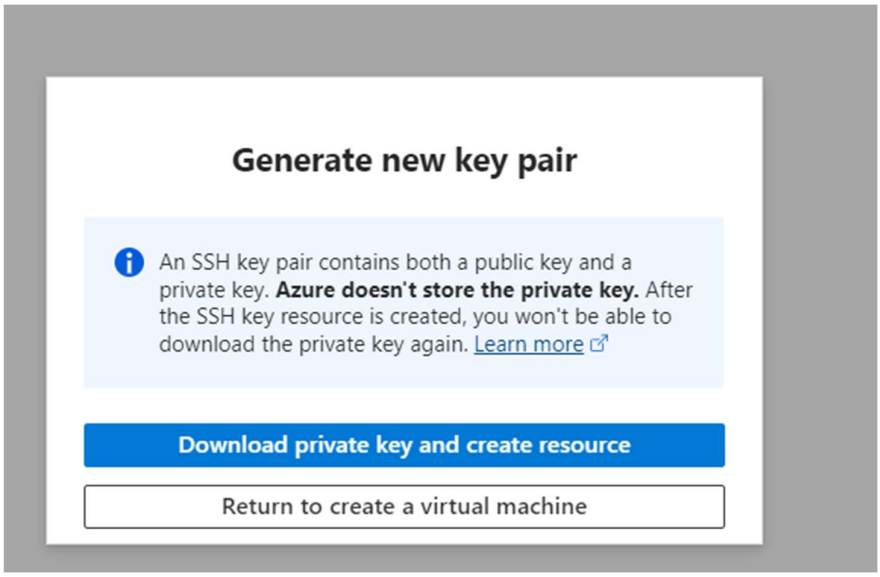
Step-3: Fill the details in that ubuntu by creating a “Resource Group”, Zone: Asia, Image: ubuntu, select “SSH”, Select the disk storage and so on. After that click on “Create + Review”. And finally click on “Create”.



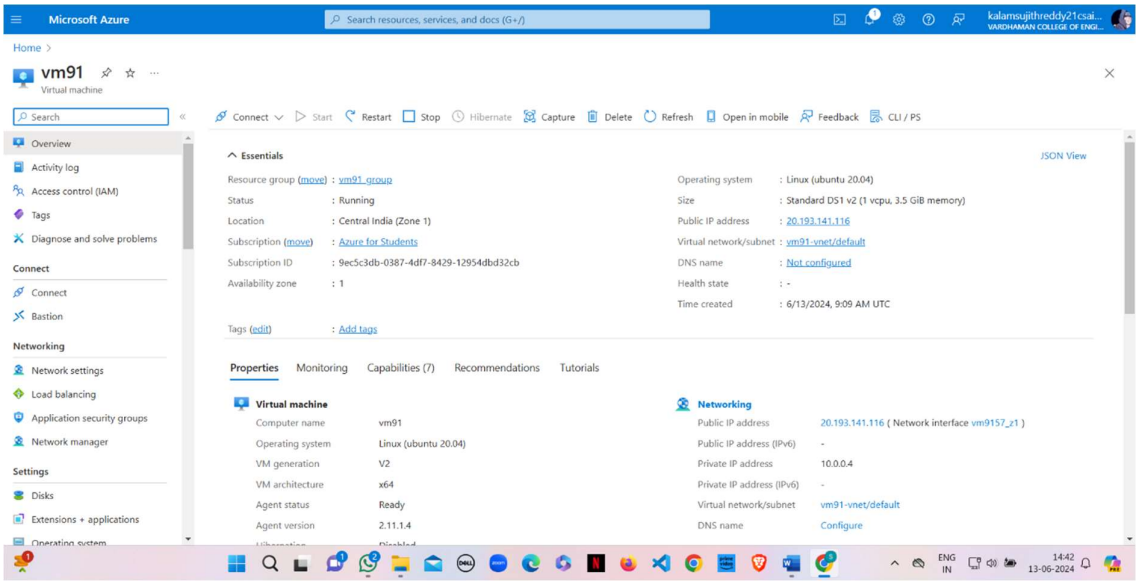

Microsoft Azure
Search resources, services, and docs (G+/)
kalamsujithreddy21csai...
VARDHAMAN COLLEGE OF ENGI...
Home > Virtual machines >
Create a virtual machine
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Azure for Students
Resource group *
(New) vm1
Create new
Instance details
Virtual machine name *
vm9
Region *
(Asia Pacific) Central India
Availability options
No infrastructure redundancy required
Security type
Trusted launch virtual machines
Configure security features
Image *
Ubuntu Server 20.04 LTS - x64 Gen2
See all images | Configure VM generation
VM architecture
Arm64
x64
< Previous
Next : Disks >
Review + create
Give feedback
ENG
IN
14:27
13-06-2024


Microsoft Azure
Search resources, services, and docs (G+/)
kalamsujithreddy21csai...
VARDHAMAN COLLEGE OF ENGI...
Home > Virtual machines >
Create a virtual machine
Authentication type
SSH public key
Password
Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.
Username *
azureuser
SSH public key source
Generate new key pair
SSH Key Type
RSA SSH Format
Ed25519 SSH Format
Ed25519 offers better performance and security with a smaller key size, while RSA is still widely used particularly for legacy systems and applications.
Key pair name *
alpha
Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.
Public inbound ports *
None
Allow selected ports
< Previous
Next : Disks >
Review + create
Give feedback
ENG
IN
14:28
13-06-2024

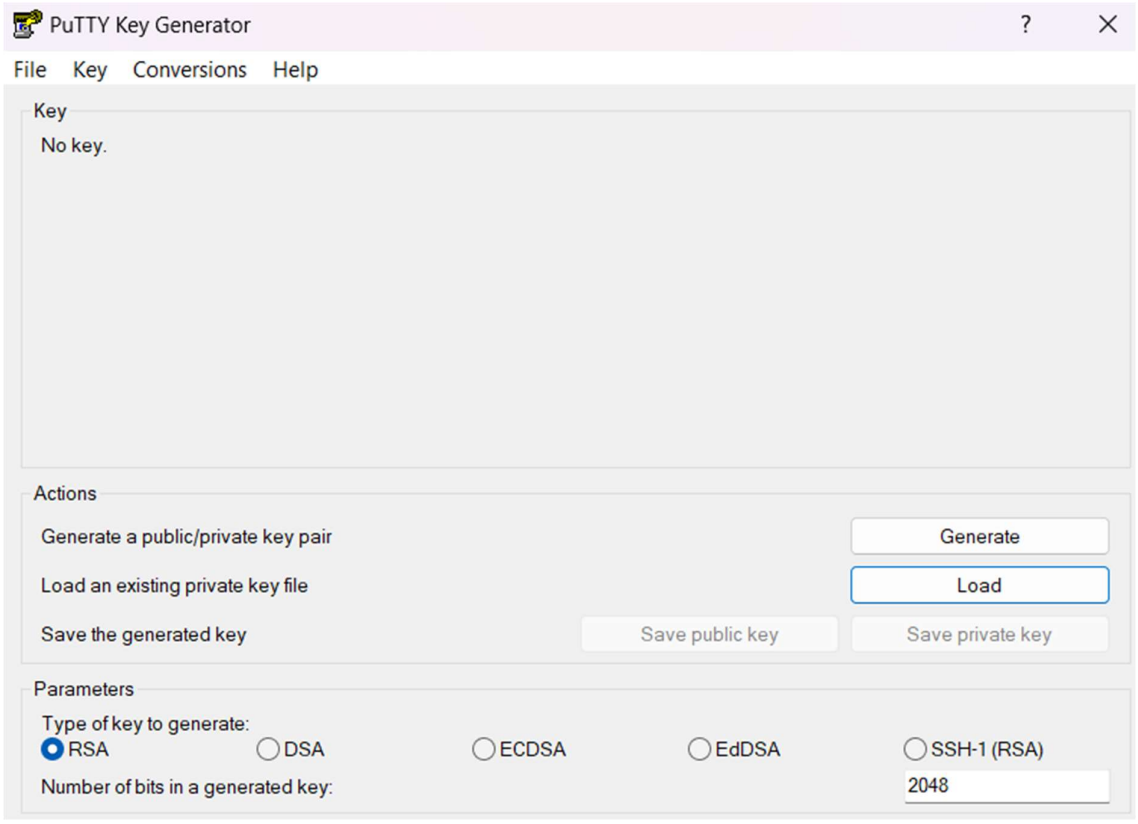
Step-4: Download private key pair and create resource.

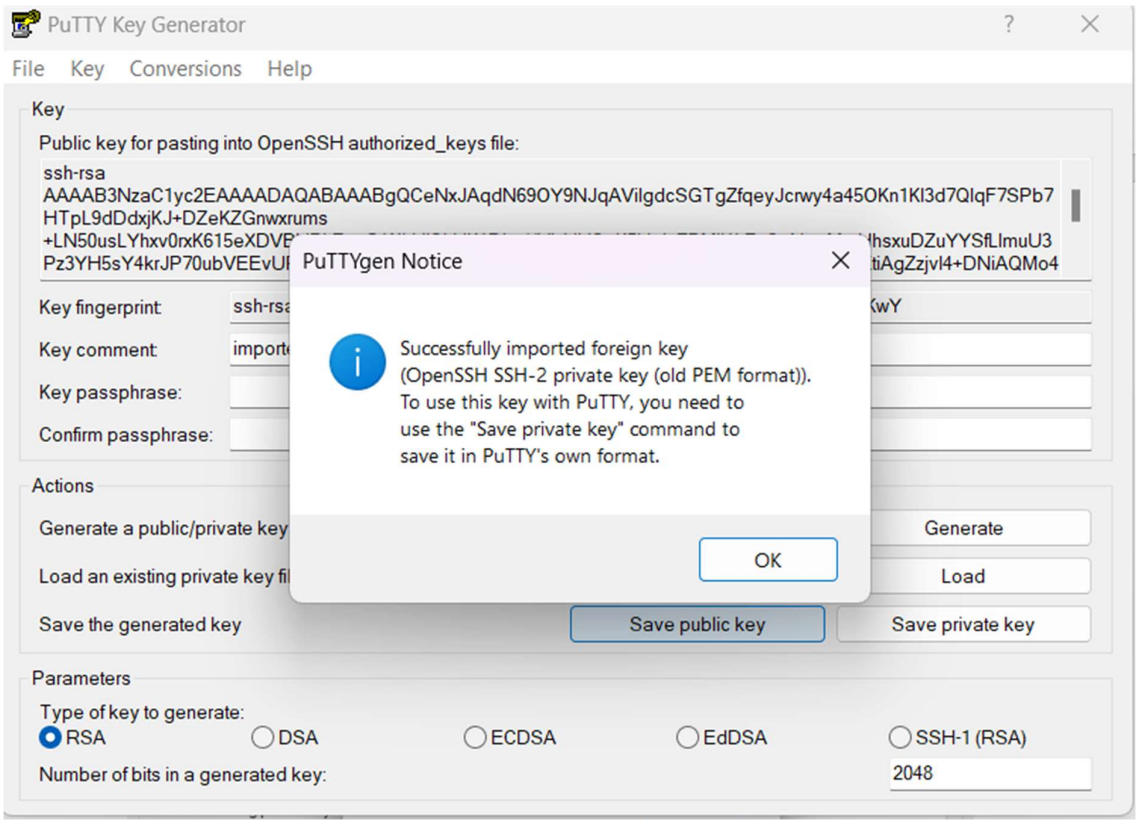


Step-5: Firstly, copy the public IP Address of that created virtual machine.

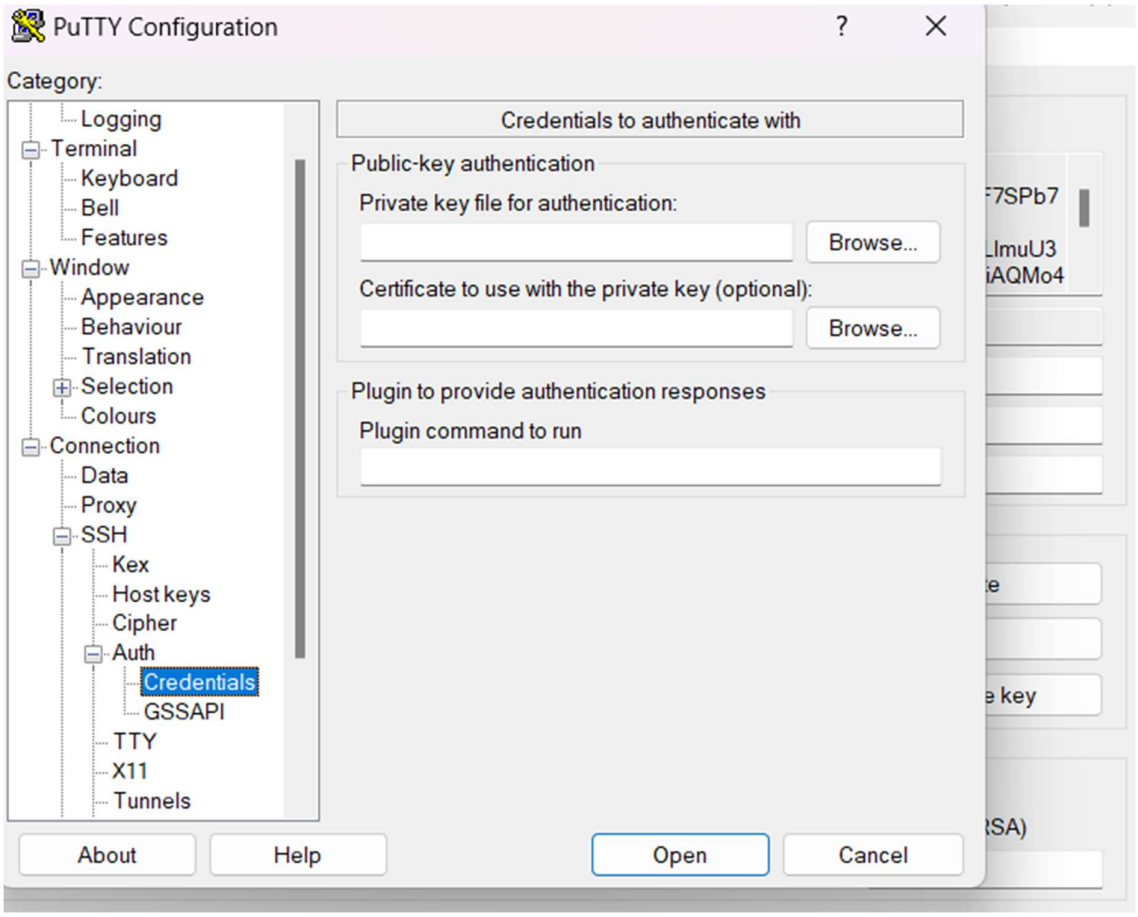


Step-6: Go to putty gen and click on load the key generator that you have downloaded.

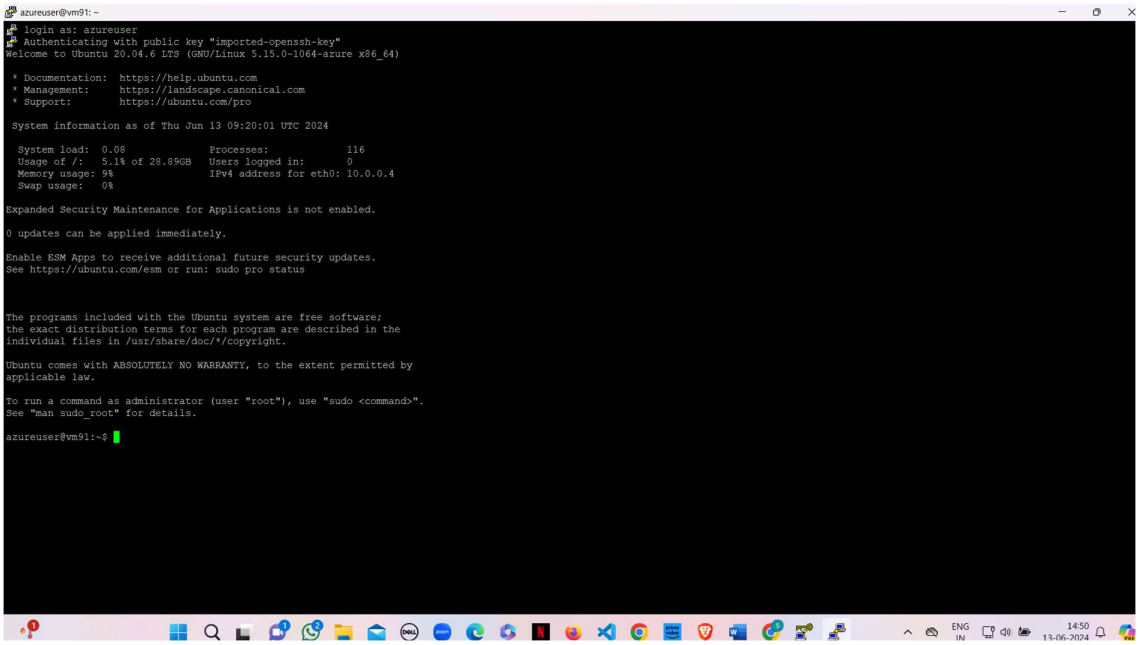

PuTTY Key Generator
File Key Conversions Help
Key
No key.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Number of bits in a generated key:
2048


PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCeNxJAqdN69OY9NJqAVilgdcSGTgZfqeyJcrwy4a45OKn1KI3d7QIqF7SPb7
HTpL9dDdxjKJ+DZeKZGnwxrums
Key fingerprint:
Key comment:
Key passphrase:
Confirm passphrase:
PuTTYgen Notice
Successfully imported foreign key
(OpenSSH SSH-2 private key (old PEM format)).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.
OK
Actions
Generate a public/private key
Generate
Load an existing private key fi
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Number of bits in a generated key:
2048

Step-7: In putty, put the Copied IP Adress into it, and then go to ssh->auth->credentials and the put the generated private key.



Step-8: A login page will be opened in that type your username and you will be into the ubuntu.



Step-9: Login into your Ubuntu VM using your username and type the following commands.

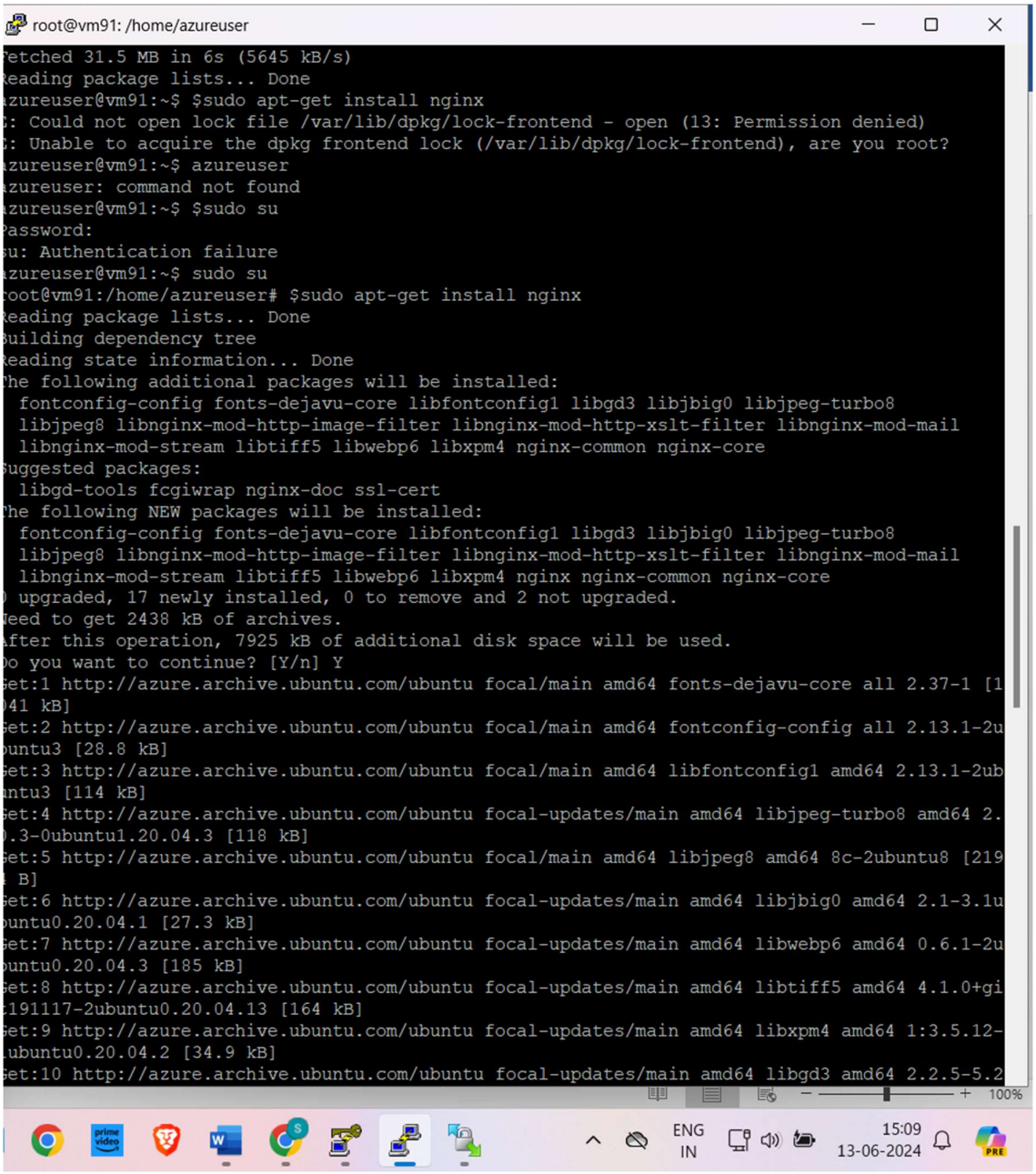
$sudo su

$sudo apt-get update

After typing the two commands, now install web server using the below command

$sudo apt-get install nginx

After installing in VM, paste the public ip address in desktop browser and you can see.

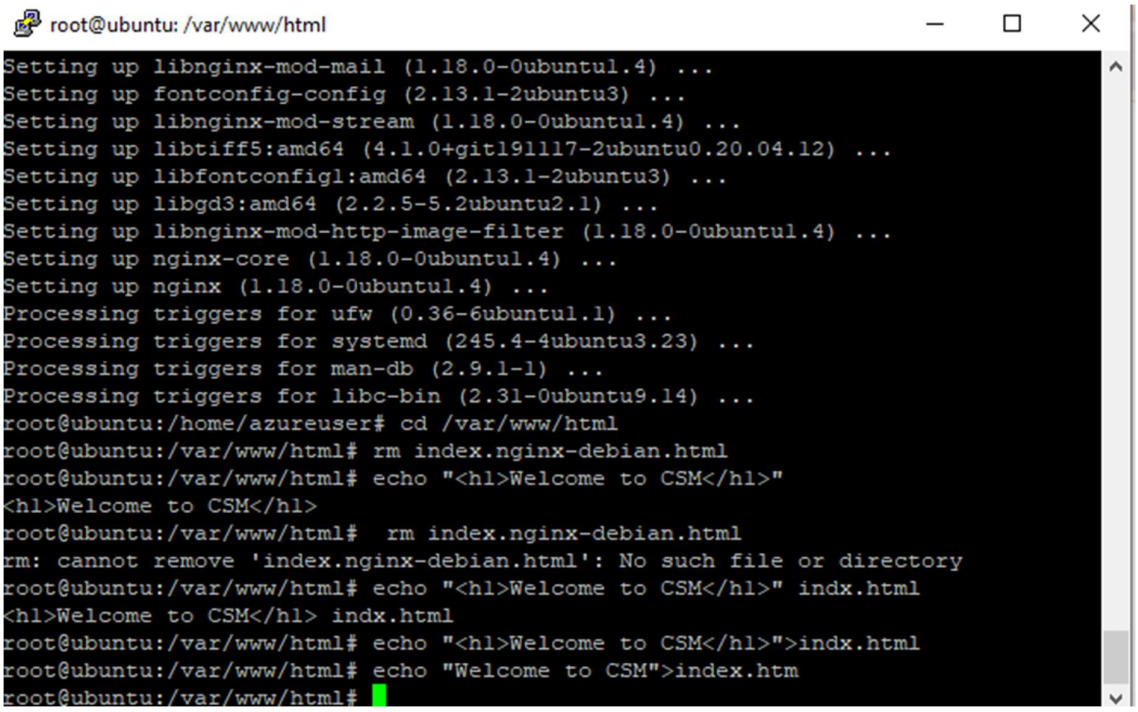


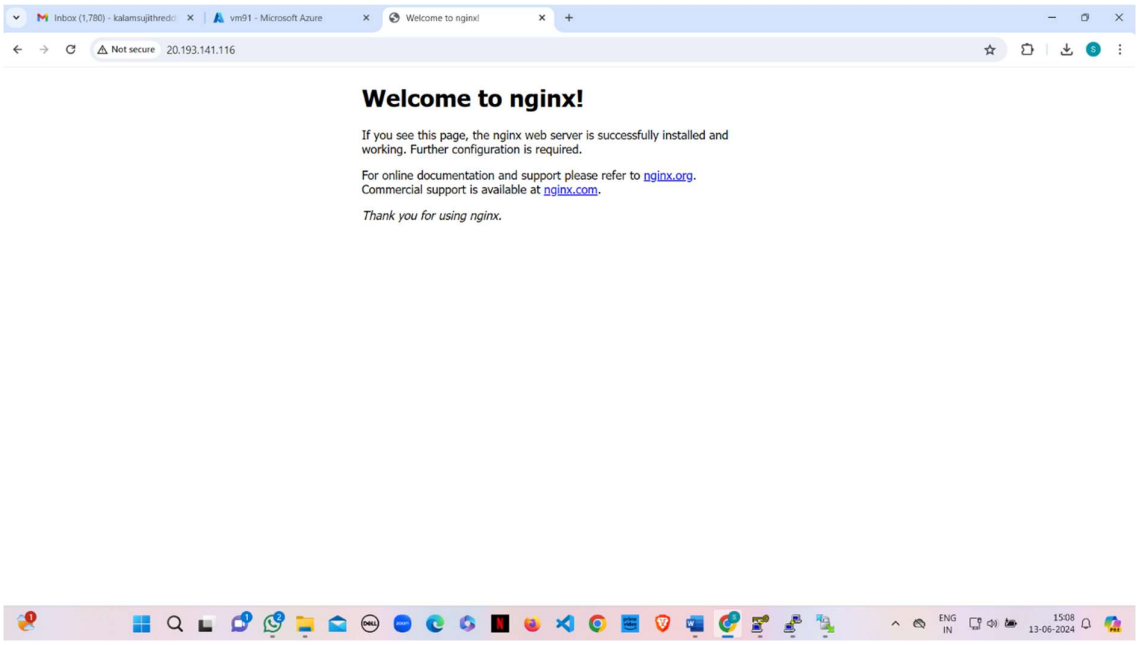
Step-10: To remove following information and keep new information in that page type the following command and refresh the browser page.

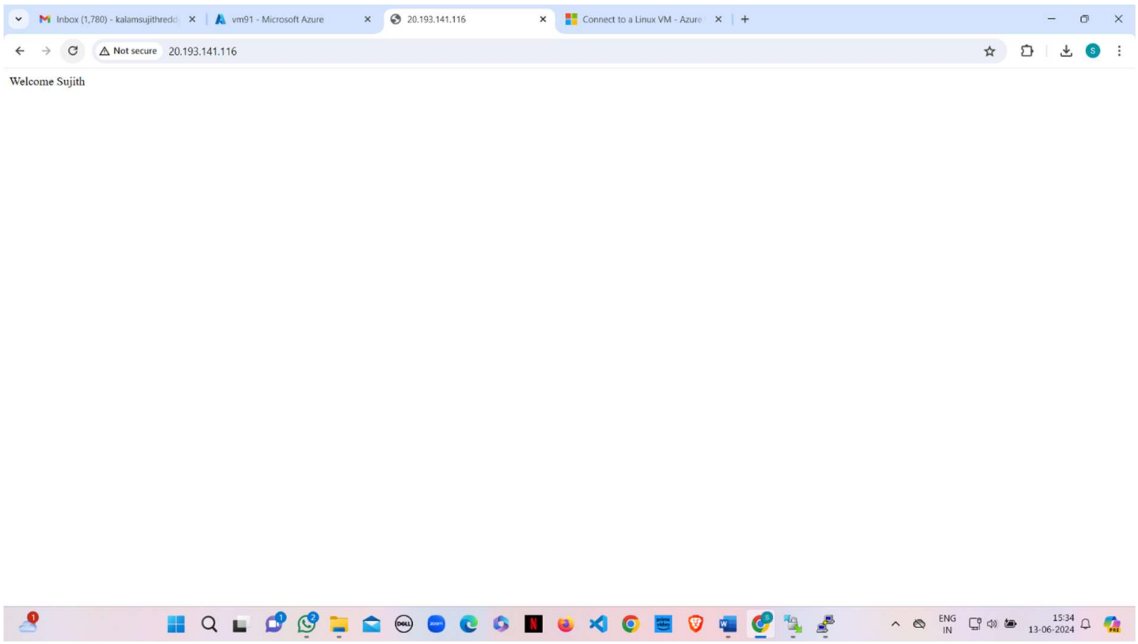
$cd /var/www/html

$rm index.nginx-debian.html

$echo “Welcome to CSM “>index.html


root@ubuntu: /var/www/html
Setting up libnginx-mod-mail (1.18.0-0ubuntu1.4) ...
Setting up fontconfig-config (2.13.1-2ubuntu3) ...
Setting up libnginx-mod-stream (1.18.0-0ubuntu1.4) ...
Setting up libtiff5:amd64 (4.1.0+git191117-2ubuntu0.20.04.12) ...
Setting up libfontconfig1:amd64 (2.13.1-2ubuntu3) ...
Setting up libgd3:amd64 (2.2.5-5.2ubuntu2.1) ...
Setting up libnginx-mod-http-image-filter (1.18.0-0ubuntu1.4) ...
Setting up nginx-core (1.18.0-0ubuntu1.4) ...
Setting up nginx (1.18.0-0ubuntu1.4) ...
Processing triggers for ufw (0.36-6ubuntu1.1) ...
Processing triggers for systemd (245.4-4ubuntu3.23) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.14) ...
root@ubuntu:/home/azureuser# cd /var/www/html
root@ubuntu:/var/www/html# rm index.nginx-debian.html
root@ubuntu:/var/www/html# echo "<h1>Welcome to CSM</h1>"
<h1>Welcome to CSM</h1>
root@ubuntu:/var/www/html# rm index.nginx-debian.html
rm: cannot remove 'index.nginx-debian.html': No such file or directory
root@ubuntu:/var/www/html# echo "<h1>Welcome to CSM</h1>" indx.html
<h1>Welcome to CSM</h1> indx.html
root@ubuntu:/var/www/html# echo "<h1>Welcome to CSM</h1>">indx.html
root@ubuntu:/var/www/html# echo "Welcome to CSM">index.htm
root@ubuntu:/var/www/html#


Not secure 20.193.141.116
Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.



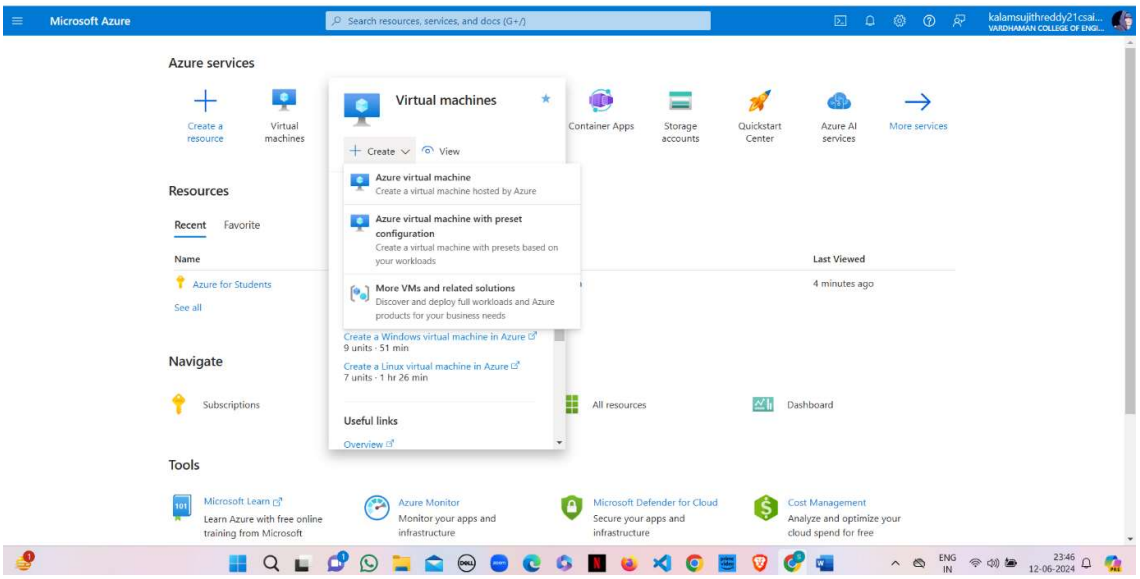
Result:

Configured a nginx web server on a Linux server in Azure. The web server was tested and found to be serving web pages correctly, confirming successful setup and configuration.

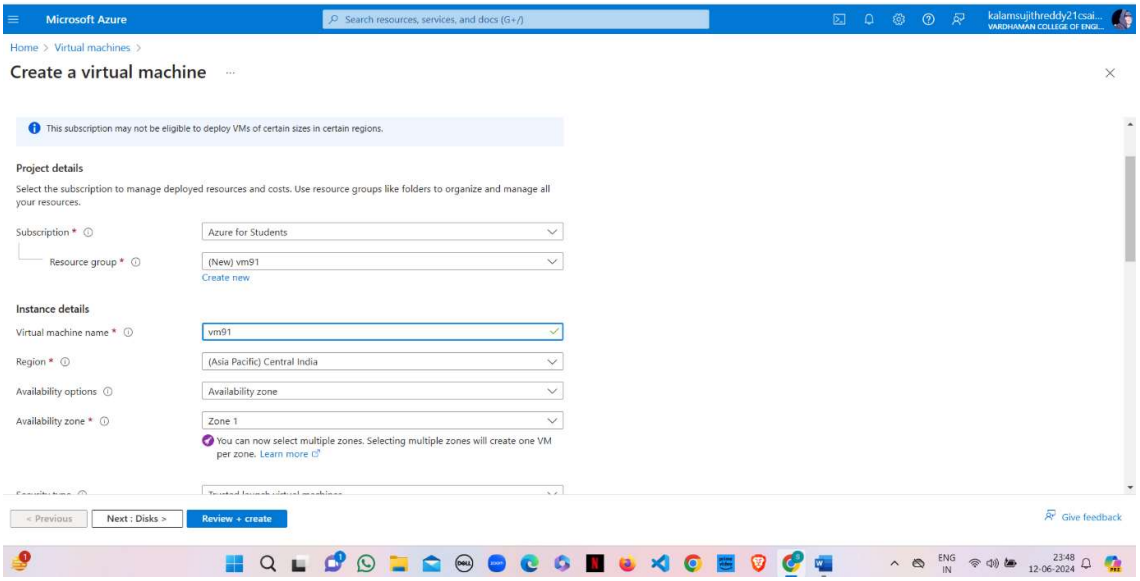
Q7) Setup and Configure Windows Server as Web Server in Azure Portal. (nginx web server)

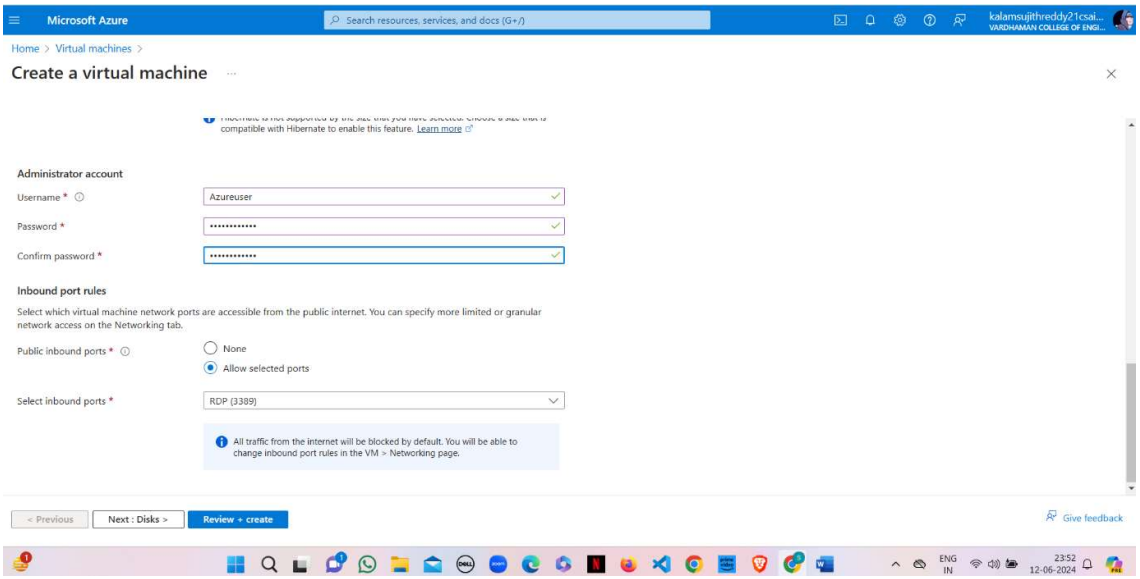
Step-1: Sign in to your Microsoft Azure account.

Step-2: Go To Virtual machine, and click on “Create” to create a window virtual machine.



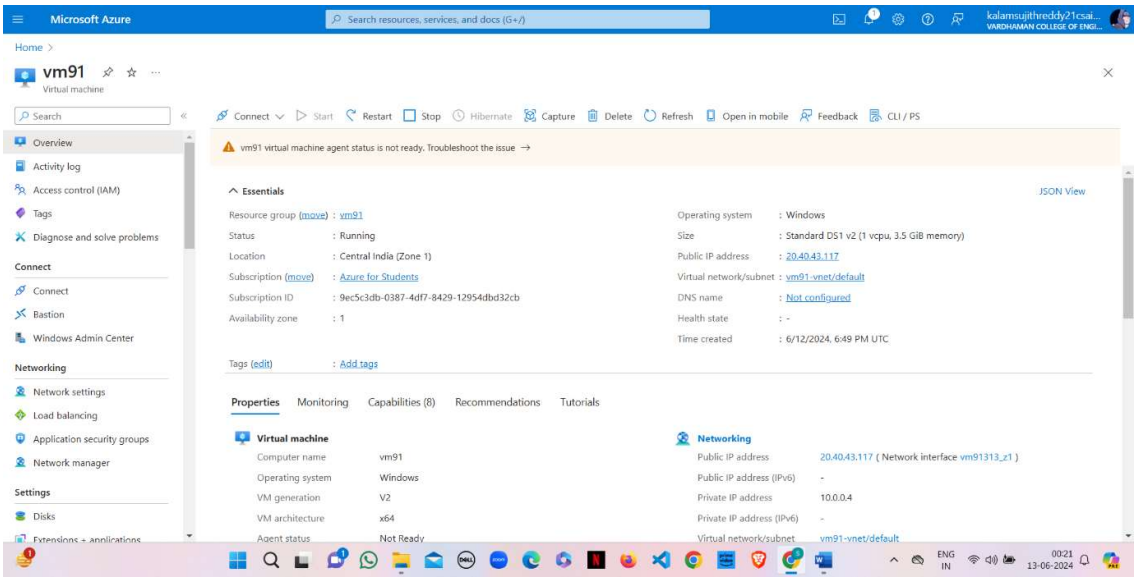
Step-3: Fill the details in that window by creating a “Resource Group”, Zone: Asia, Image: window, Select the disk storage and so on. After that click on “Create + Review”. And Finally click on “Create”



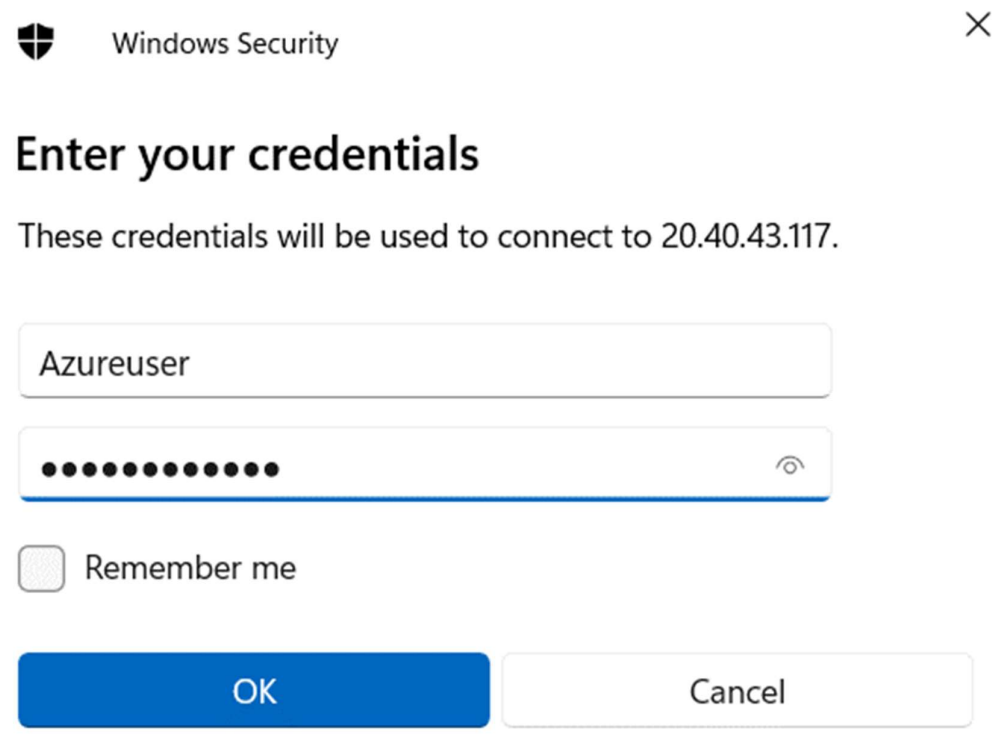


Step-4: After Deployment is over, Go to the remote desktop connection.

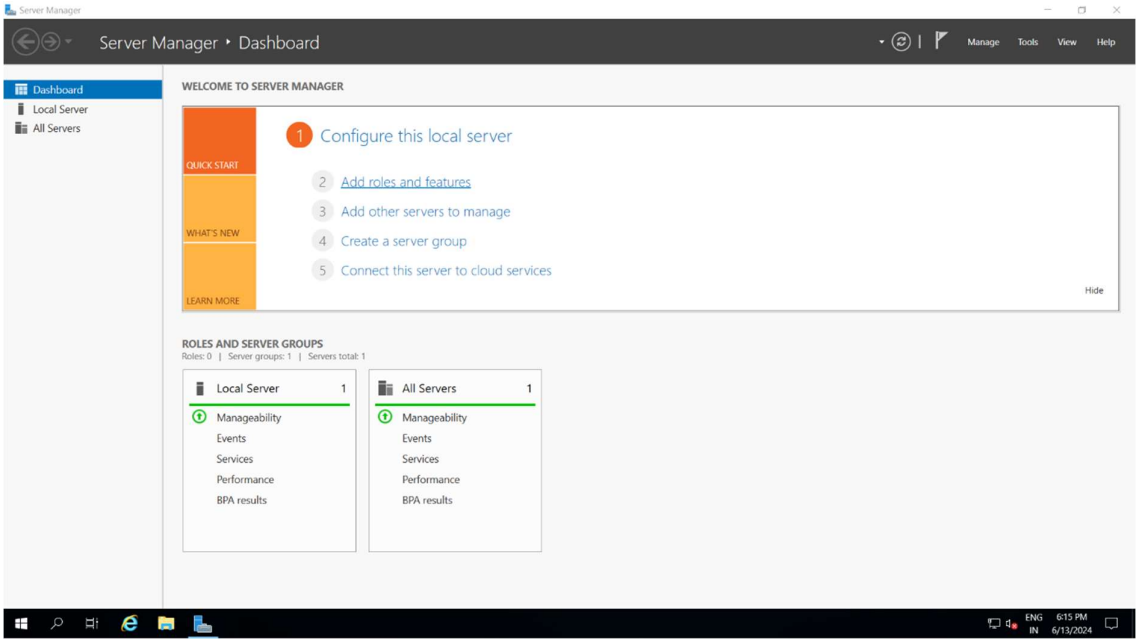
Step-5: Firstly, copy the public IP Address of that created virtual machine.



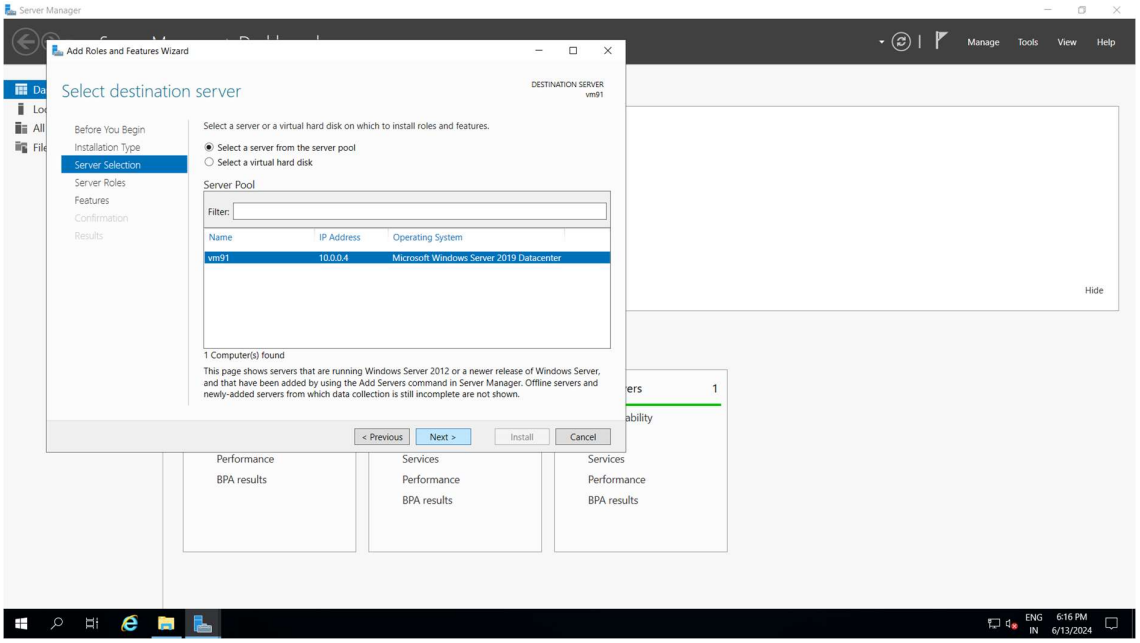
Step-6: By using that copied IP Address open the window virtual machine through remote desktop connection.

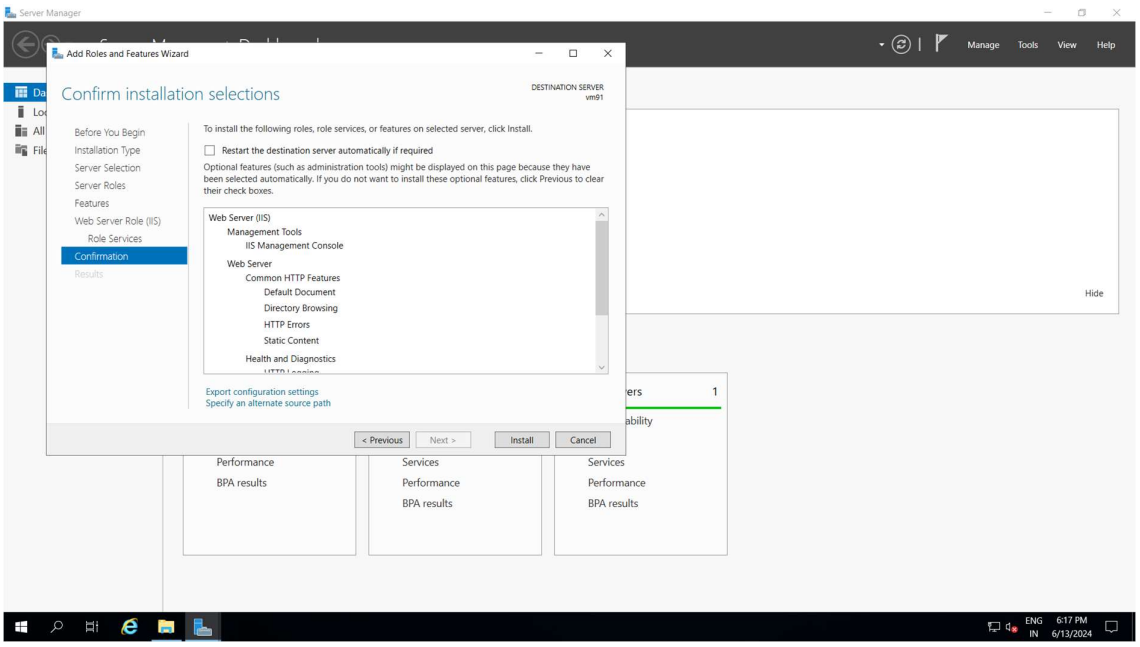


Step-7: When remote desktop will start (windows VM) you can see there will be Sever Manager will be opened and in that you can see Configure this local server, click on “Add roles and features”.

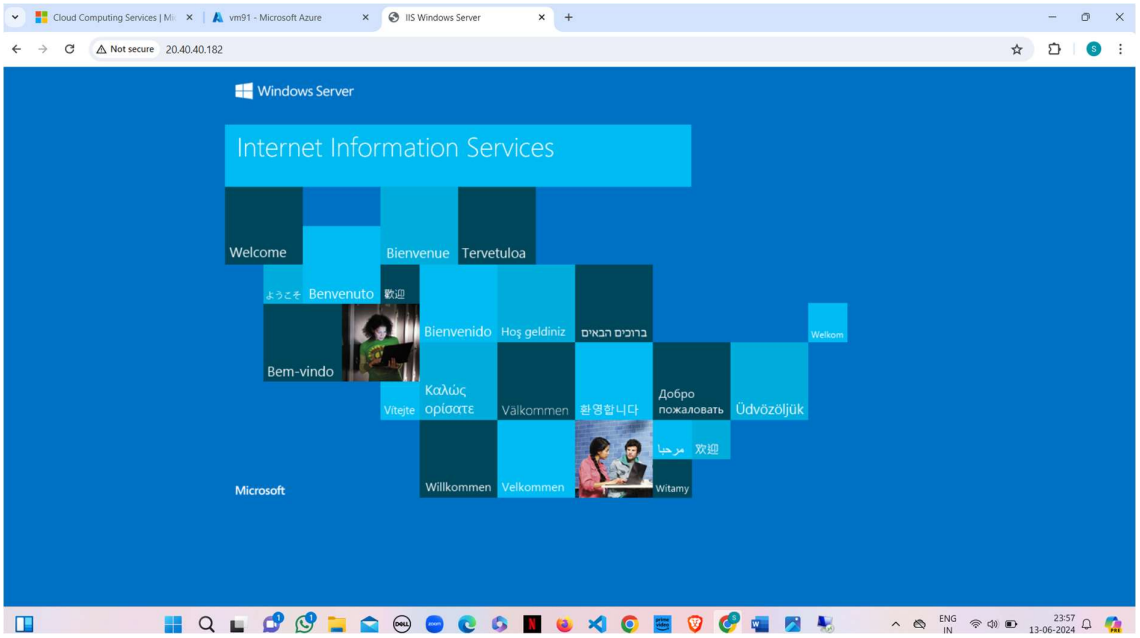


Step-8: Click on next, next and in Server Roles select Web Server (IIS) click on add feature, click on next, next till you can get install button and click on install.

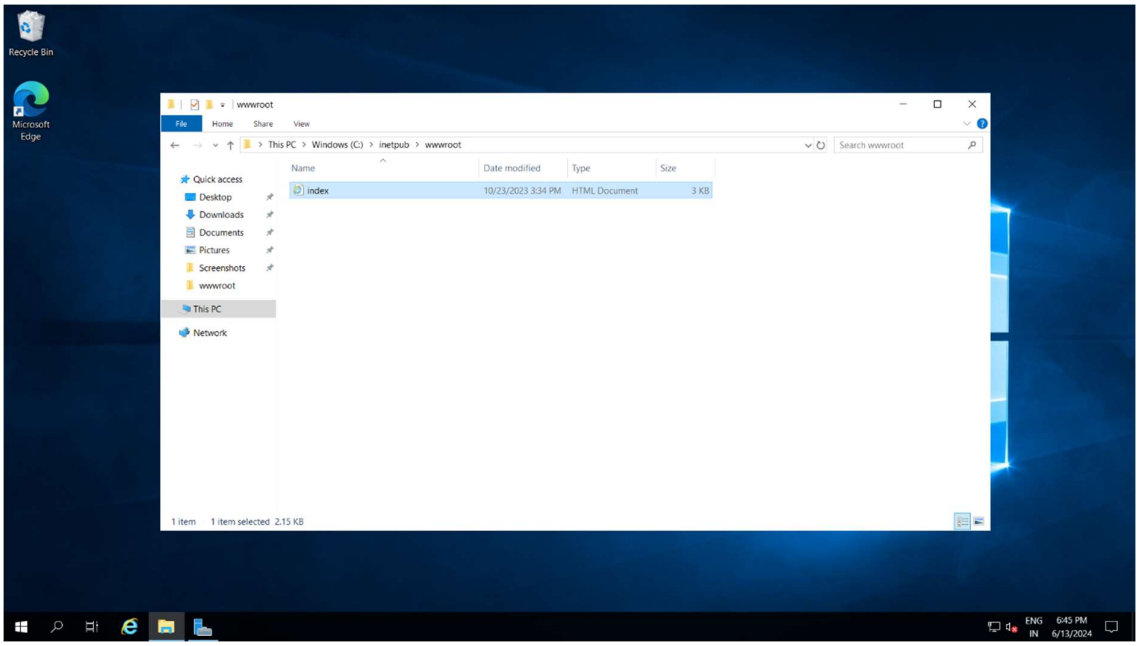




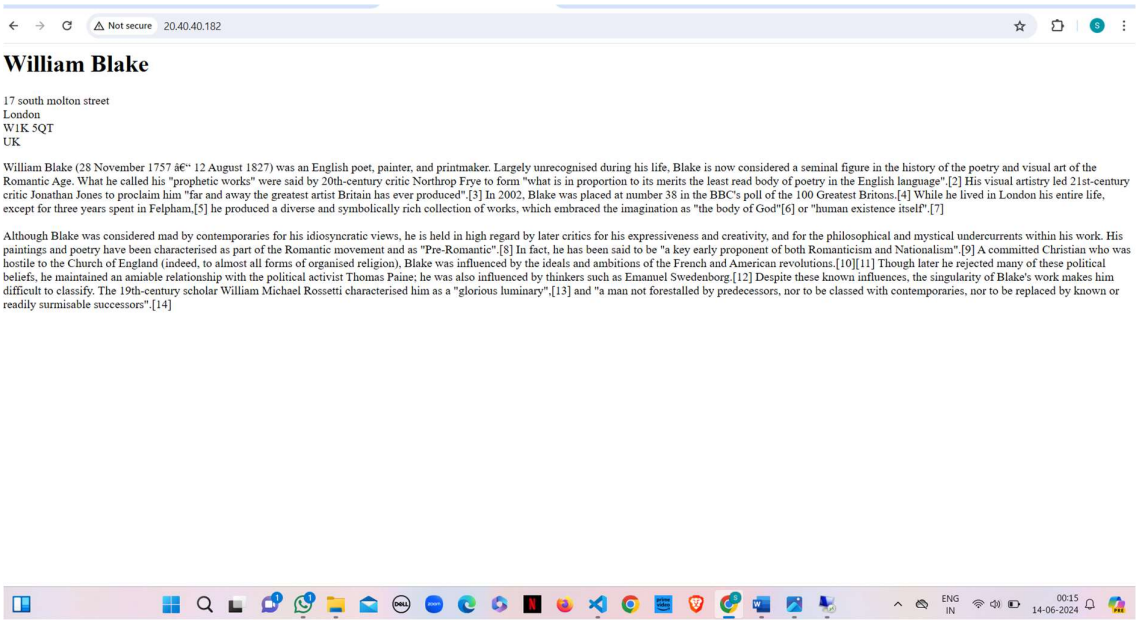
Step- 9: paste the public IP address in desktop browser and you can see.



Now to remove this all information first of all create index.html in desktop and that should paste in the specified location of remote desktop VM that is ThisPC->windows(c)- >inetup->wwwroot and remove iistart png.



Step-10: Refresh the browser page.

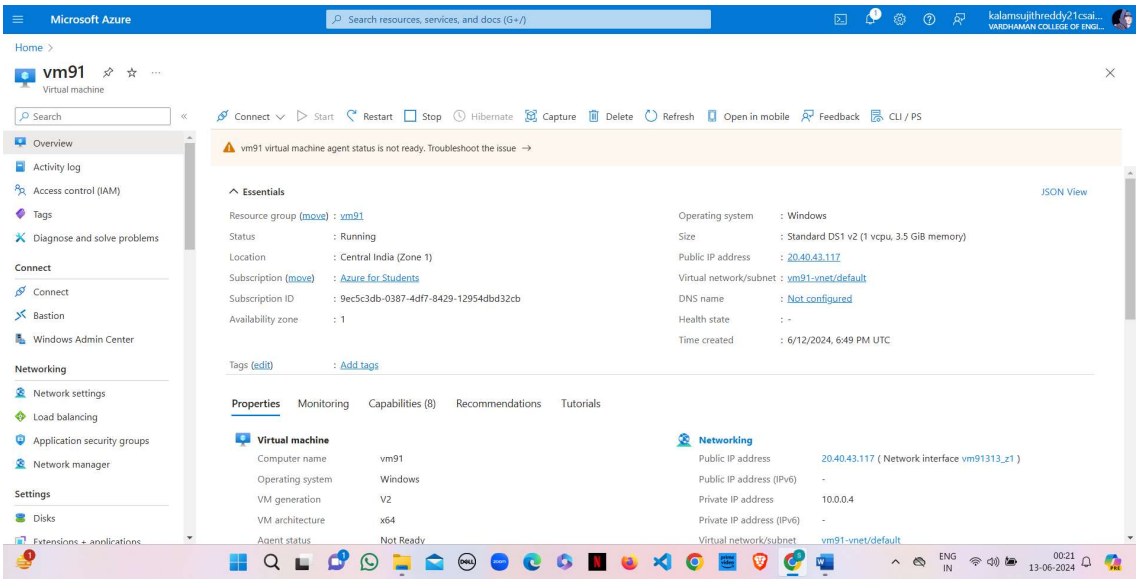


Result:

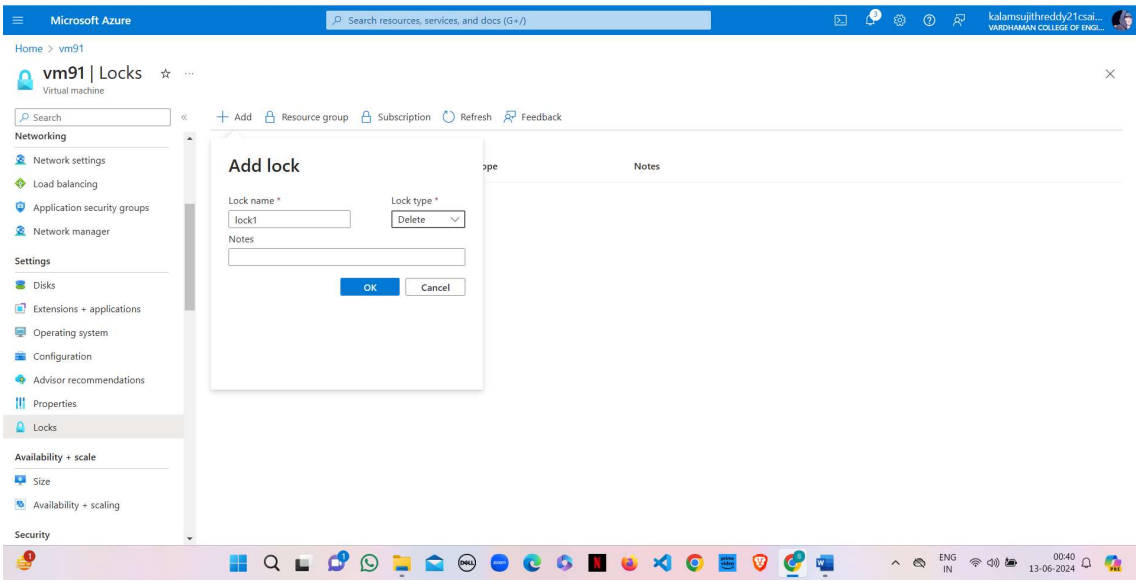
Set up and configured an web server on a Windows server in Azure. The server was operational, and web pages were accessible, indicating a successful configuration.

Q8) Implementing locks in Azure Portal.

Step-1: Create a virtual machine (ubuntu or windows).

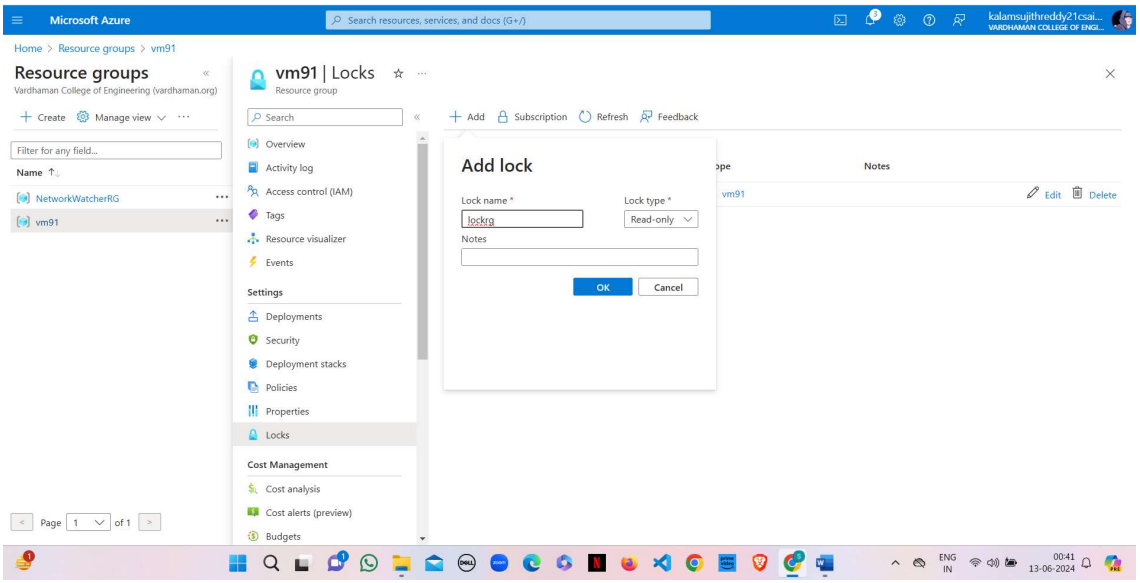


Step-2: On the left side there will be settings and click on locks, give lock name and select lock type.

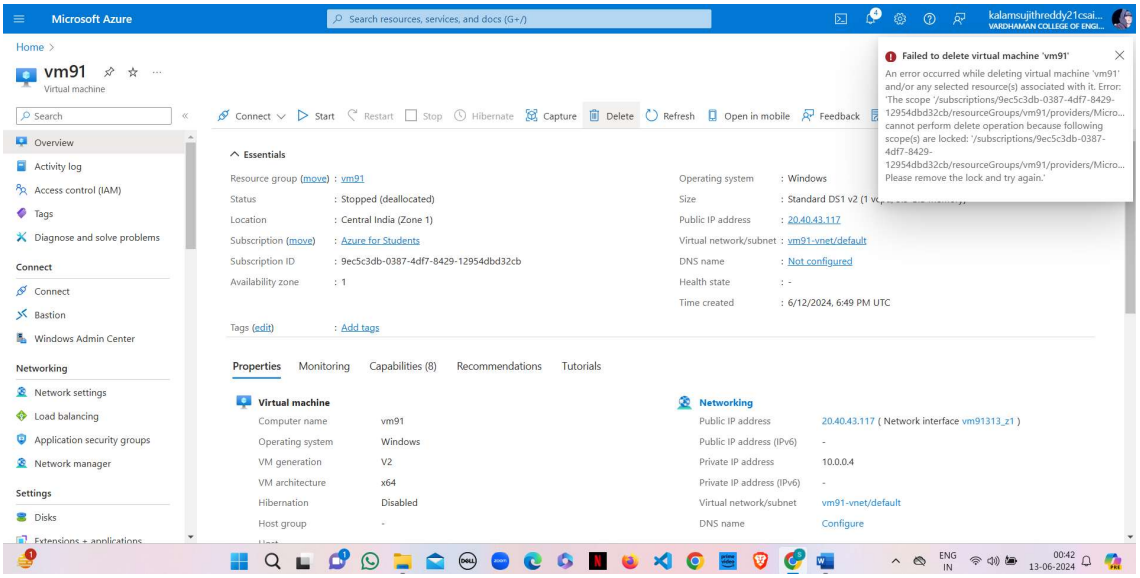


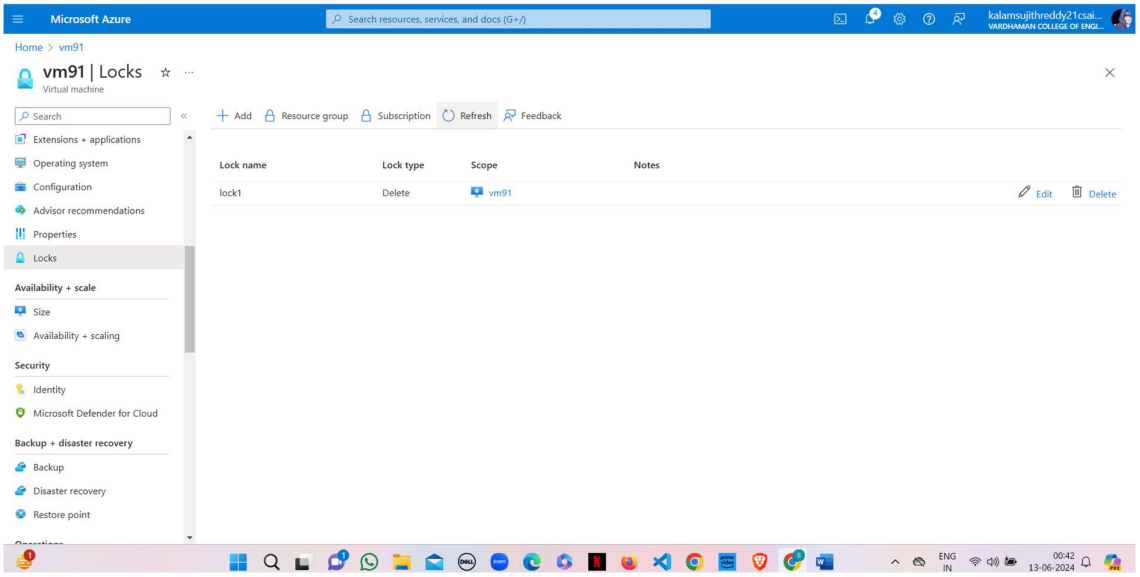
Step-3: Click on ok.

Similarly, you can do for Resource group and subscriptions.



Note: After creating the lock, you need to delete it for deleting VM.



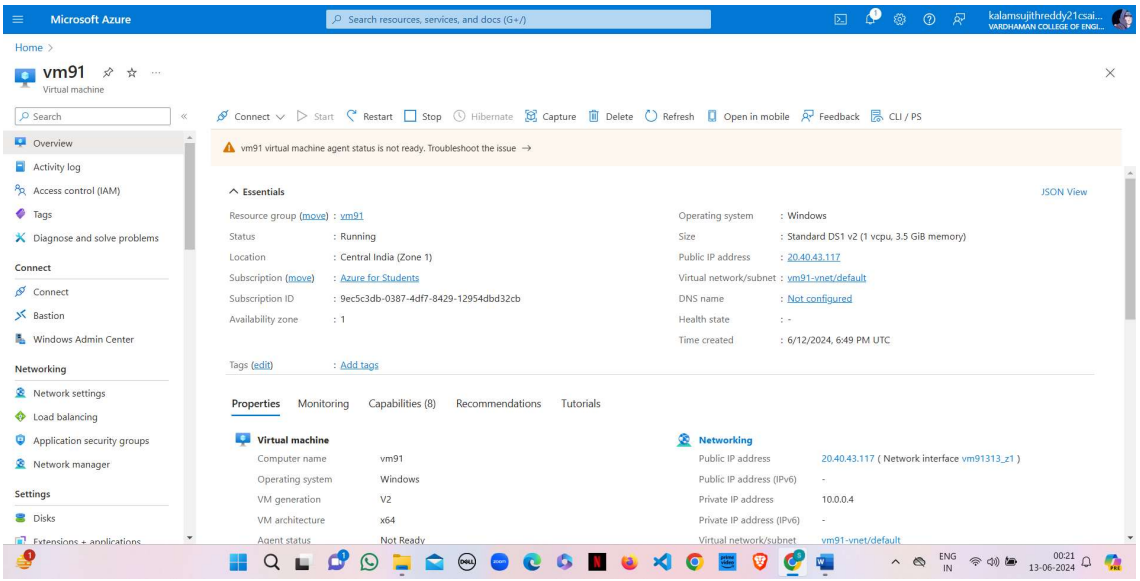


Result:

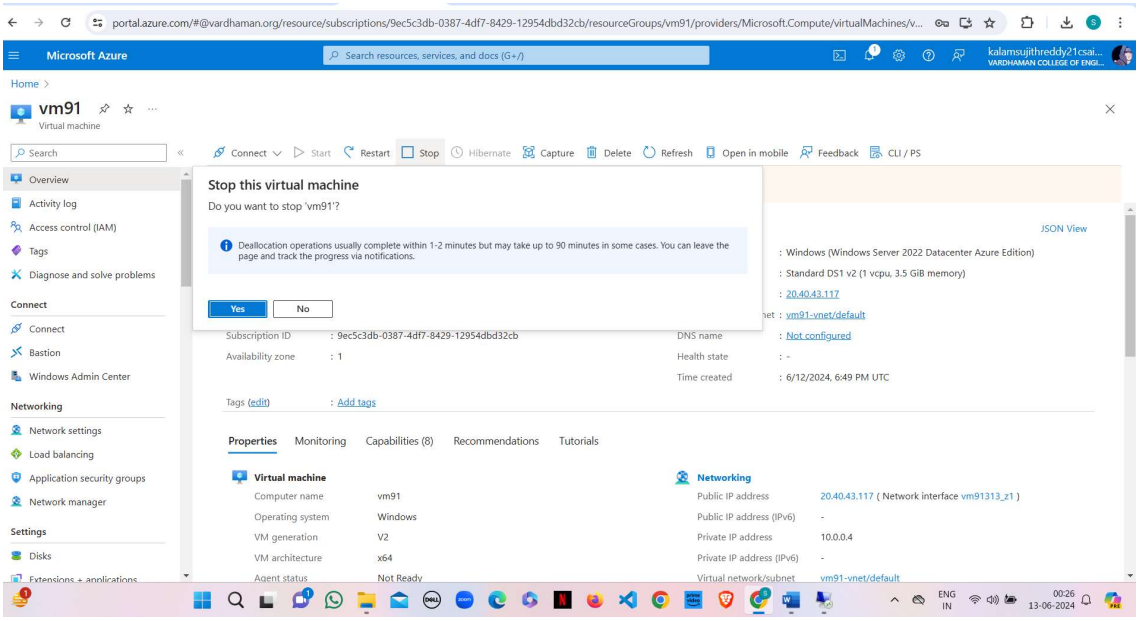
Implemented resource locks in the Azure portal to prevent accidental deletion or modification of critical resources. The locks were tested and effectively restricted changes, ensuring resource protection.

Q9) Perform scaling in Azure Portal.

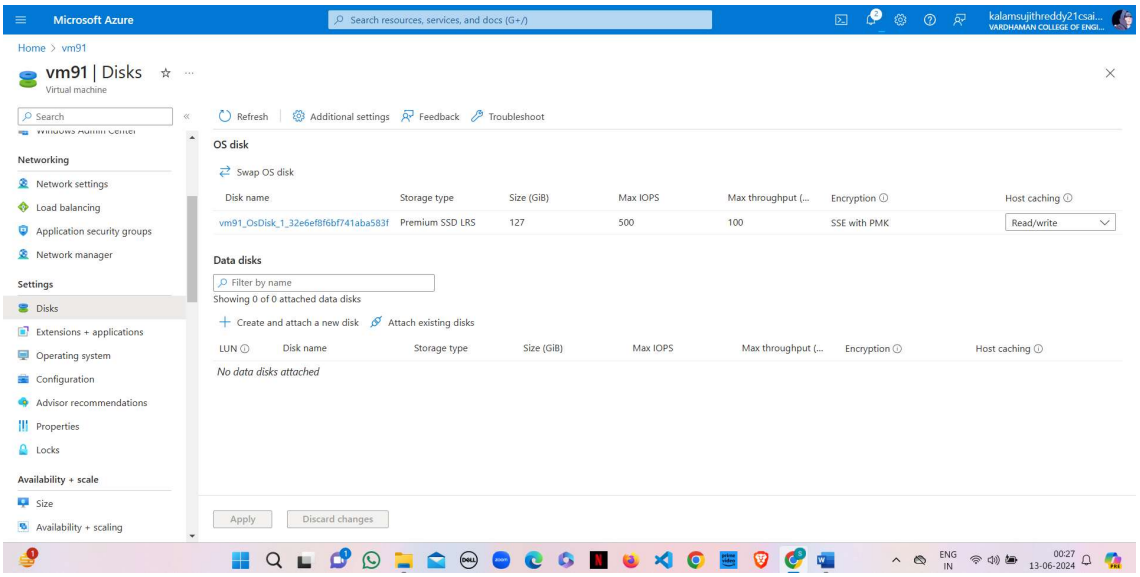
Step-1: Create a virtual machine (ubuntu or windows).



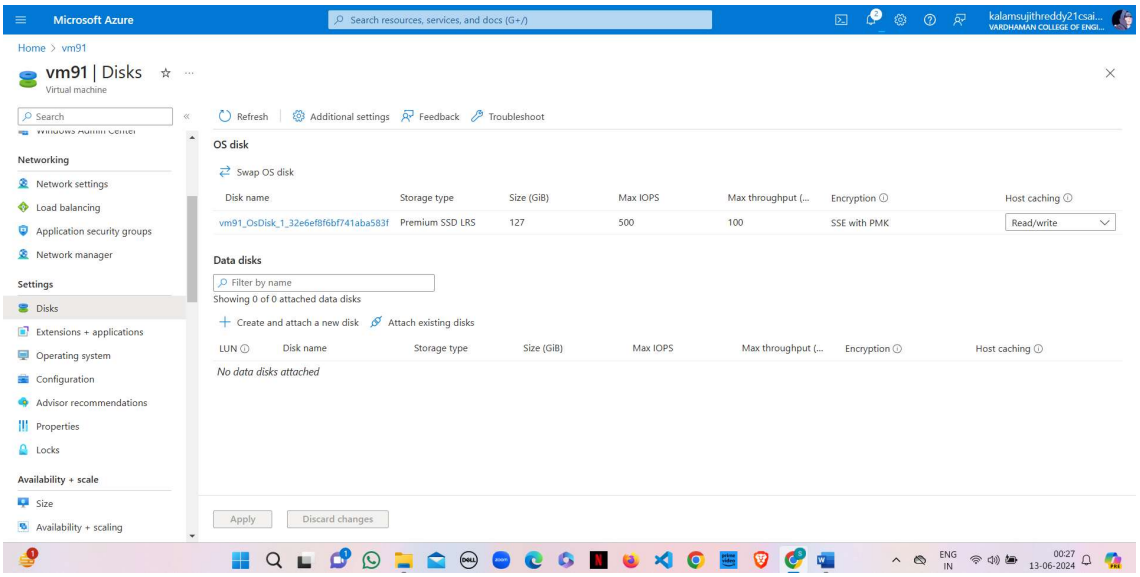
Step-2: After deployment of VM stop VM for scaling.



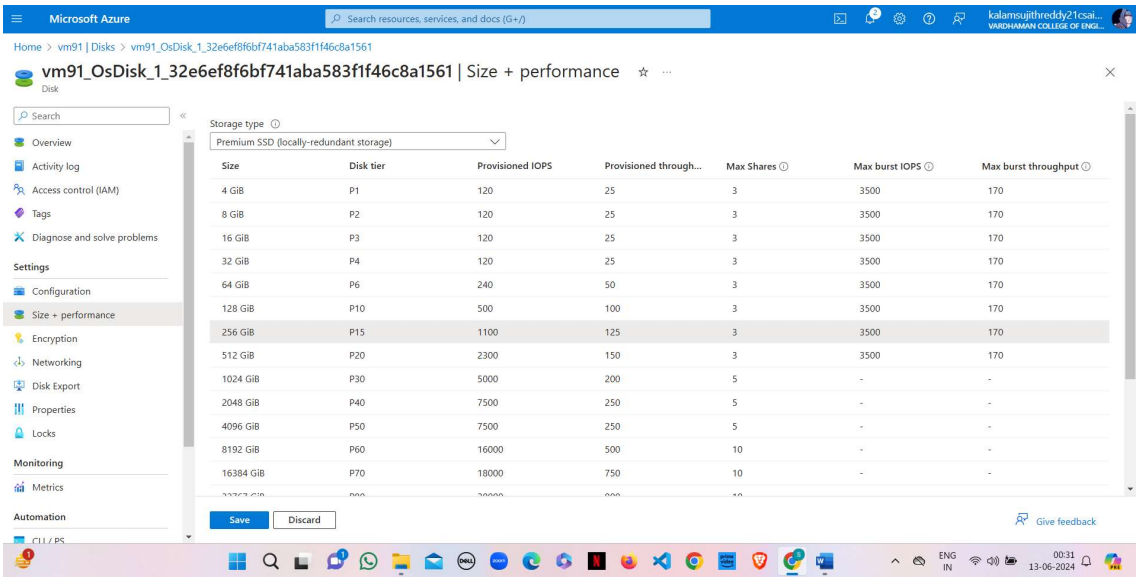
Step-3: On the left side there will be settings and click on disks.



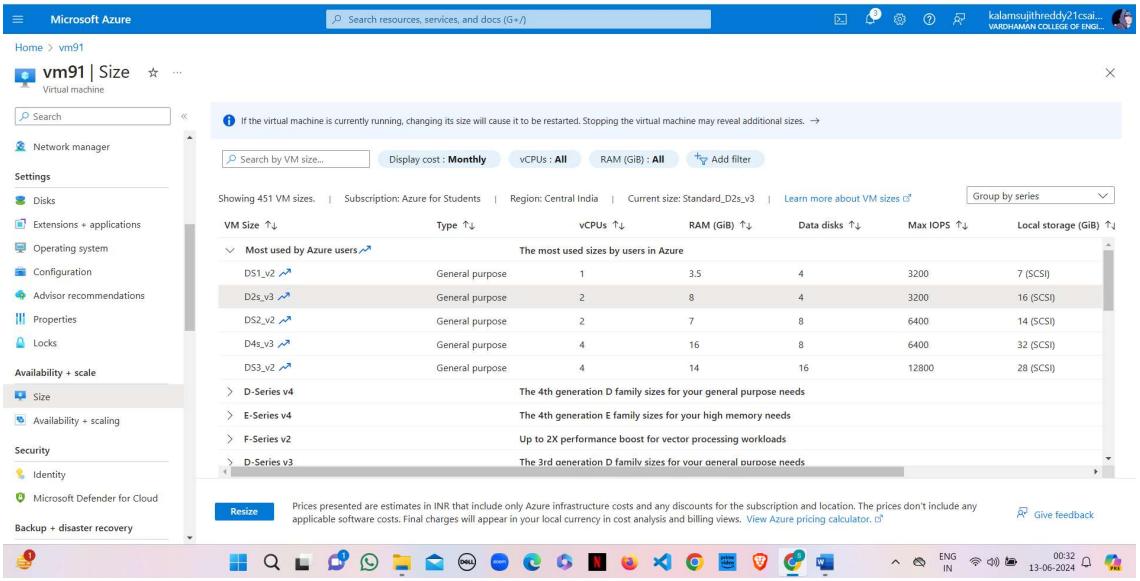
Step-4: Click on disk name and select your preferred size, save it.



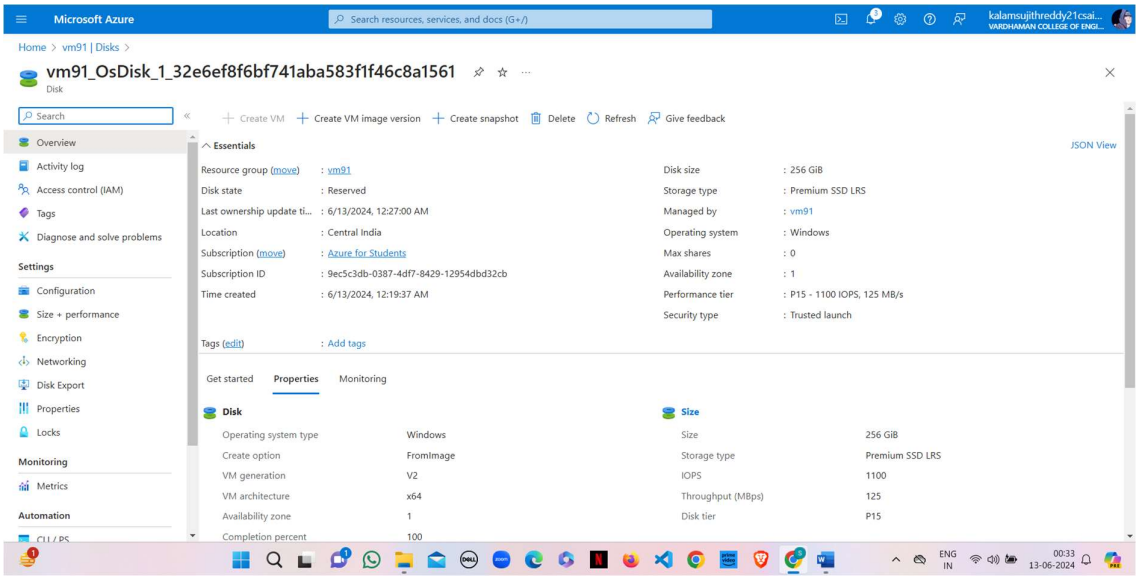
Step-5: On the left side there will be select + performance and click on size.



Step-6: click on disk name and select your preferred ram size, save it.



Step-7: Viewing VM after resizing the disk (Scale up).

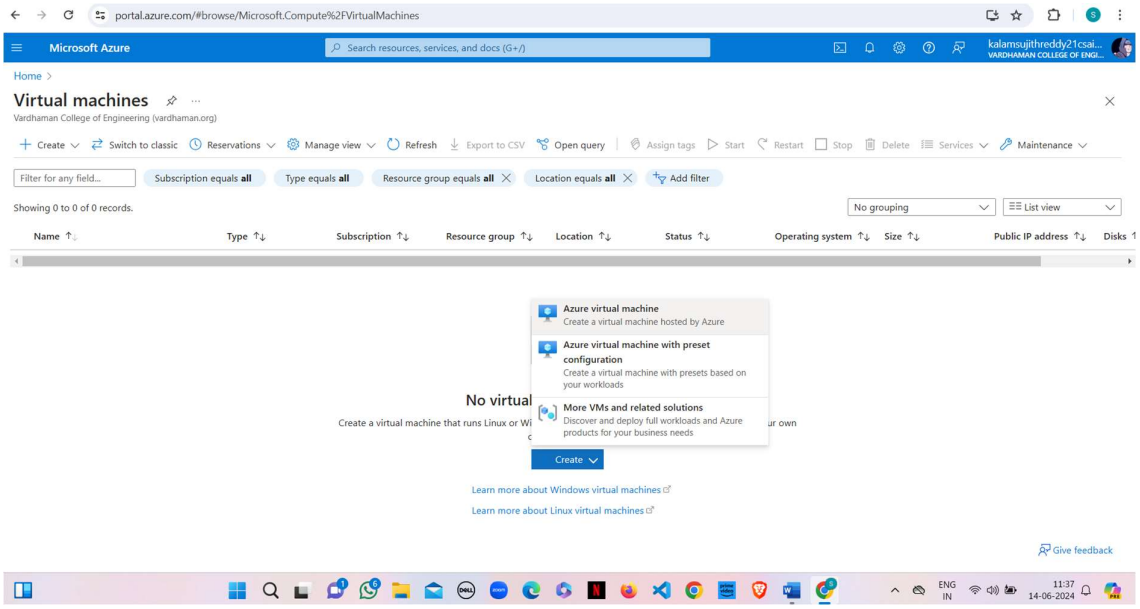


Result:

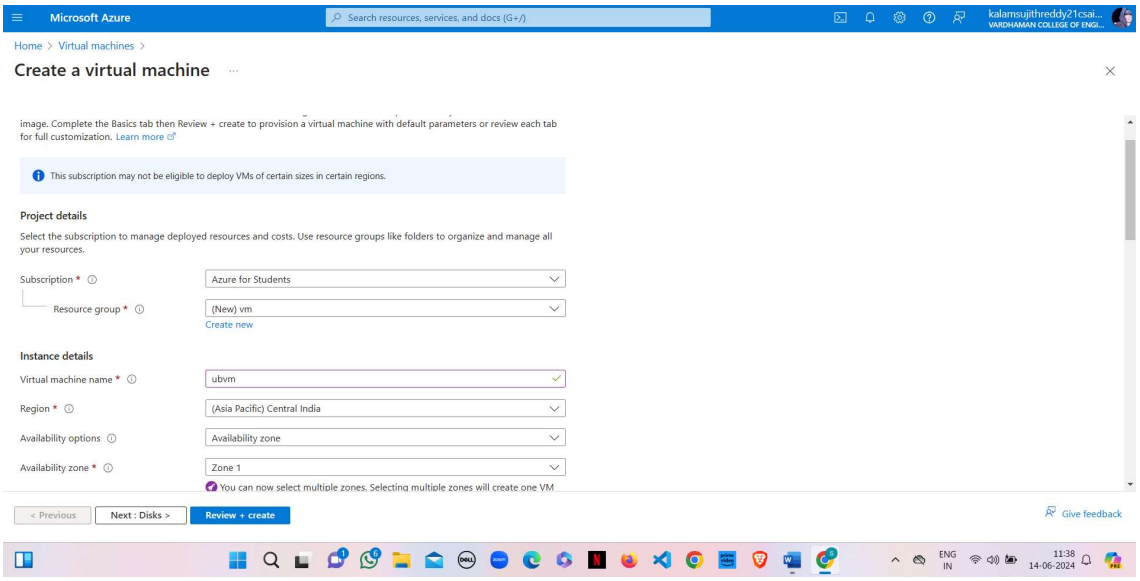
Conducted scaling operations in Azure Portal, successfully increasing and decreasing the number of virtual machine instances. The scaling process was seamless, with new instances provisioning correctly and load distribution verified.

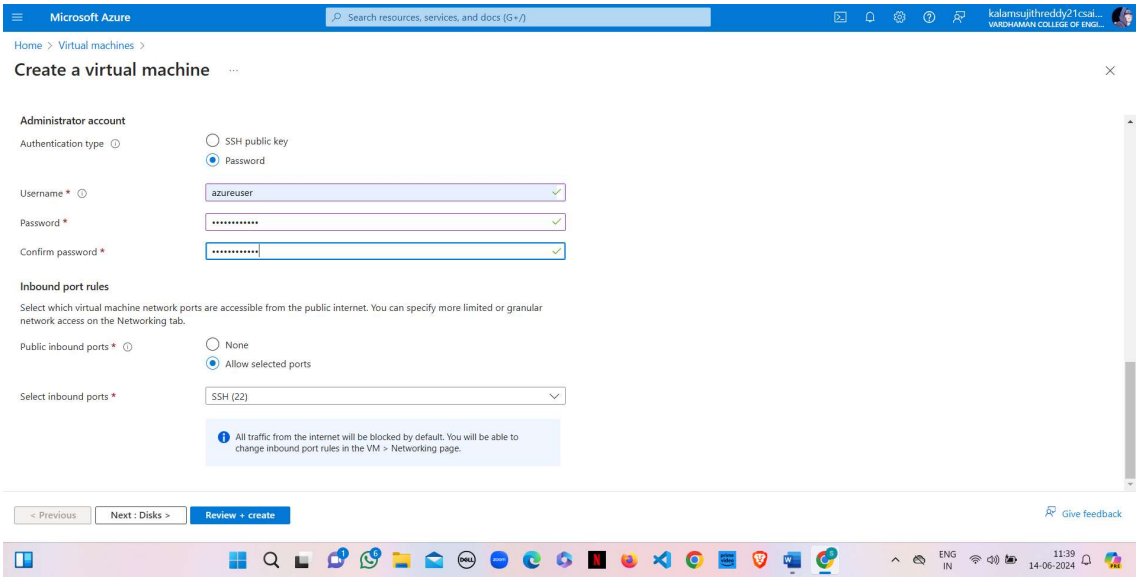
Q10) Perform attach and detach of data disk to Linux Server in Azure.

Step 1 : Create a Virtual Machine with username &password.



Step 2 : click on "Next:Disks>"



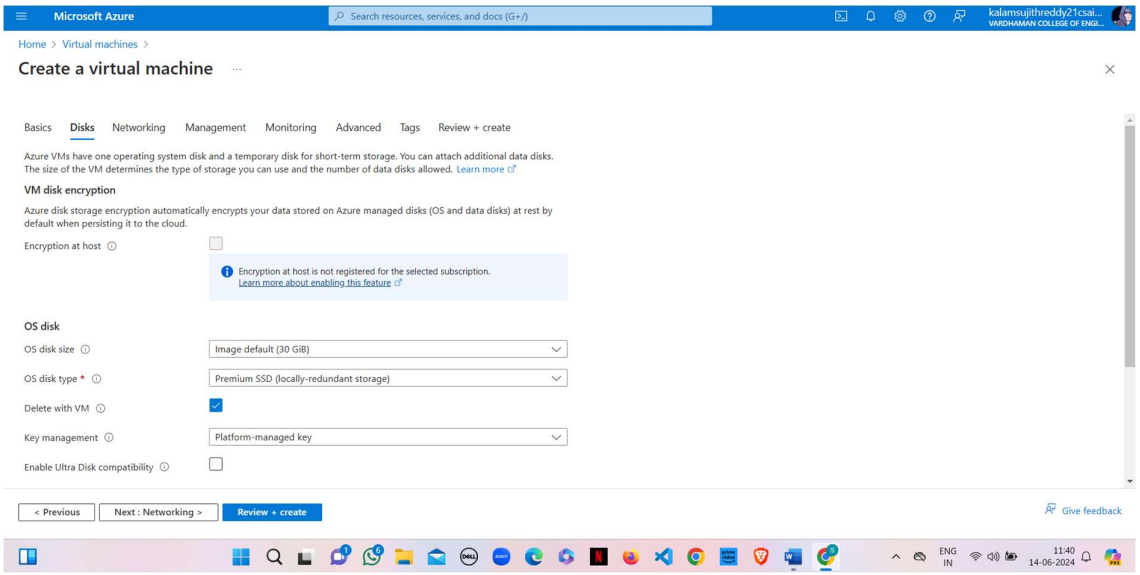


Step 3 : Select

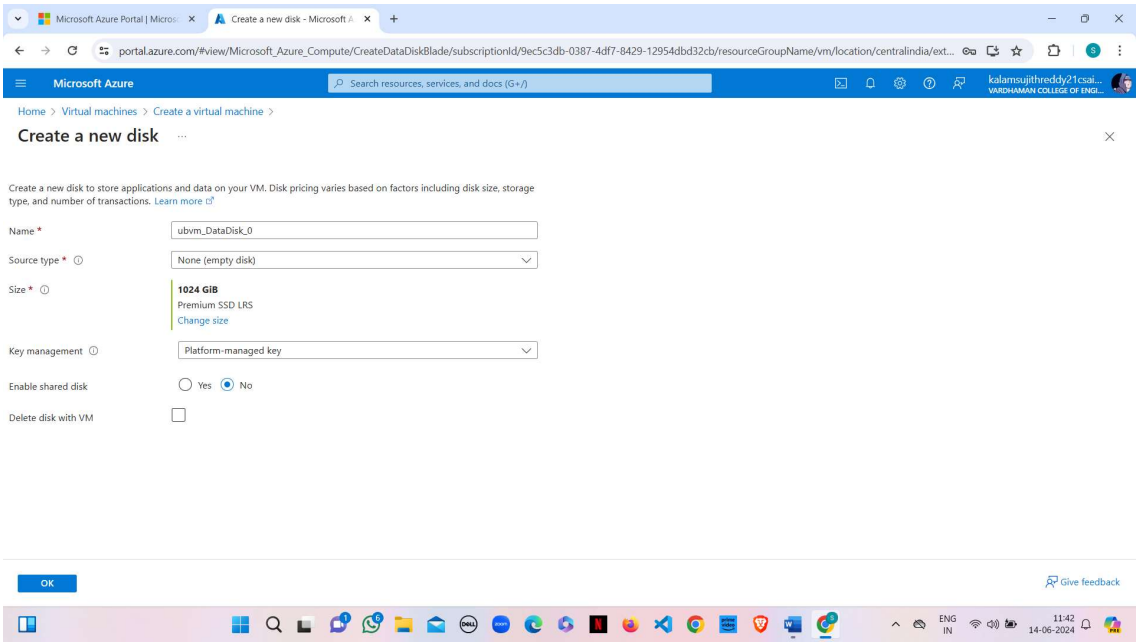
OS disk size -------30GB

OS disk type ------Premium SSD(LRS)

enable "Delete with VM"



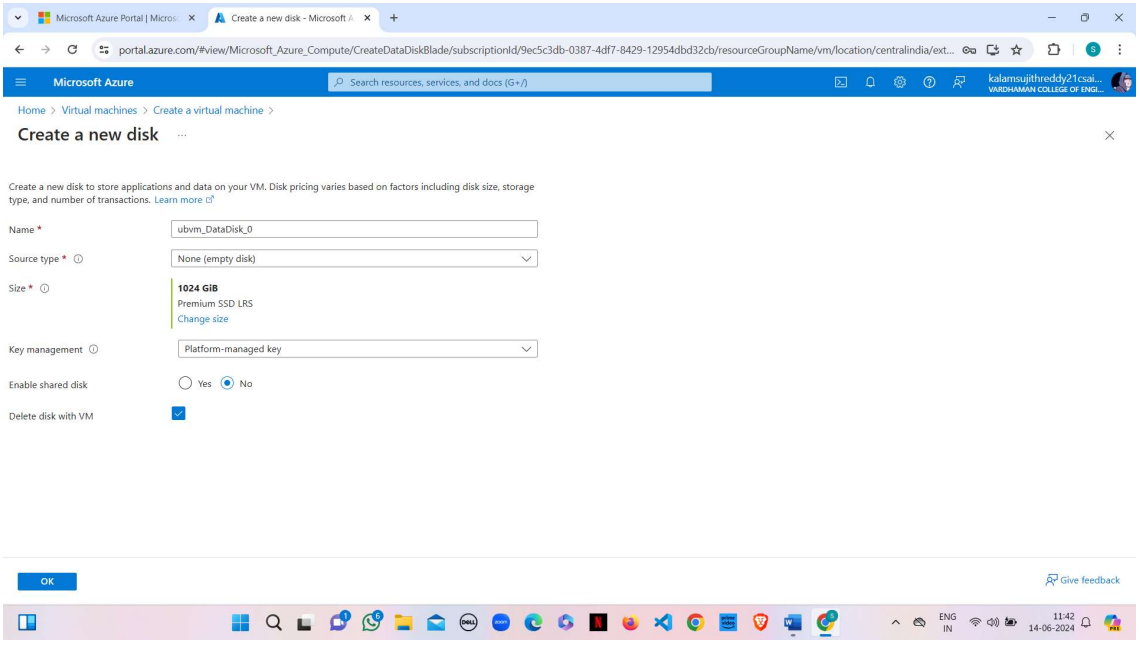
Step 4 : Click on "Create & attach a new disk"



Step 5 : Select

Source type -------None (empty disk), Size -------1024GB, Key manager ------- Platform managed key,

Enable shared disk -------NO and finally click on OK

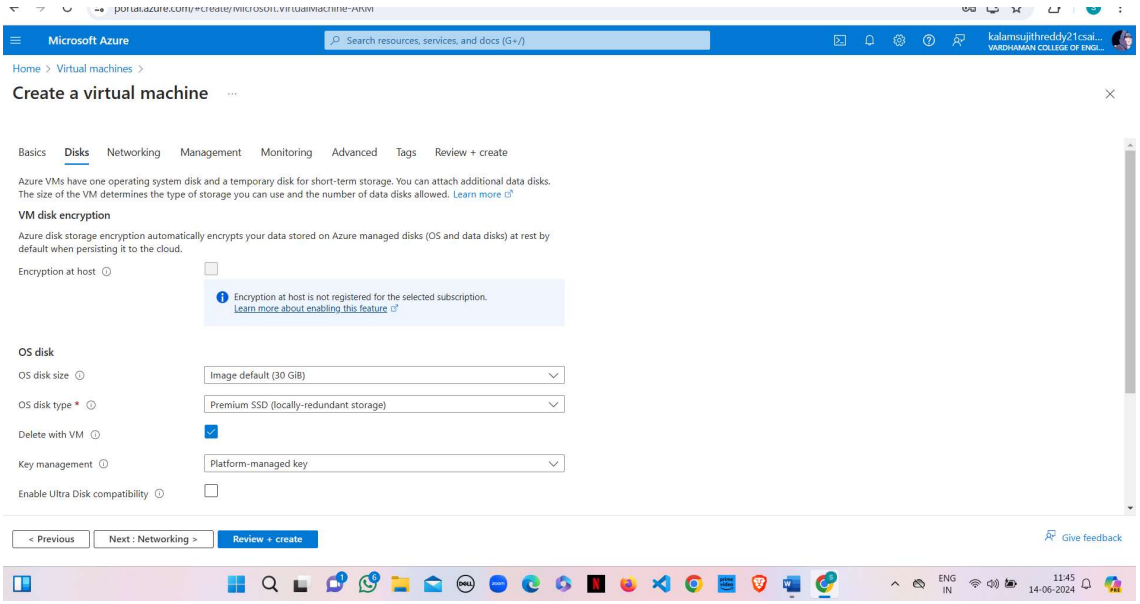


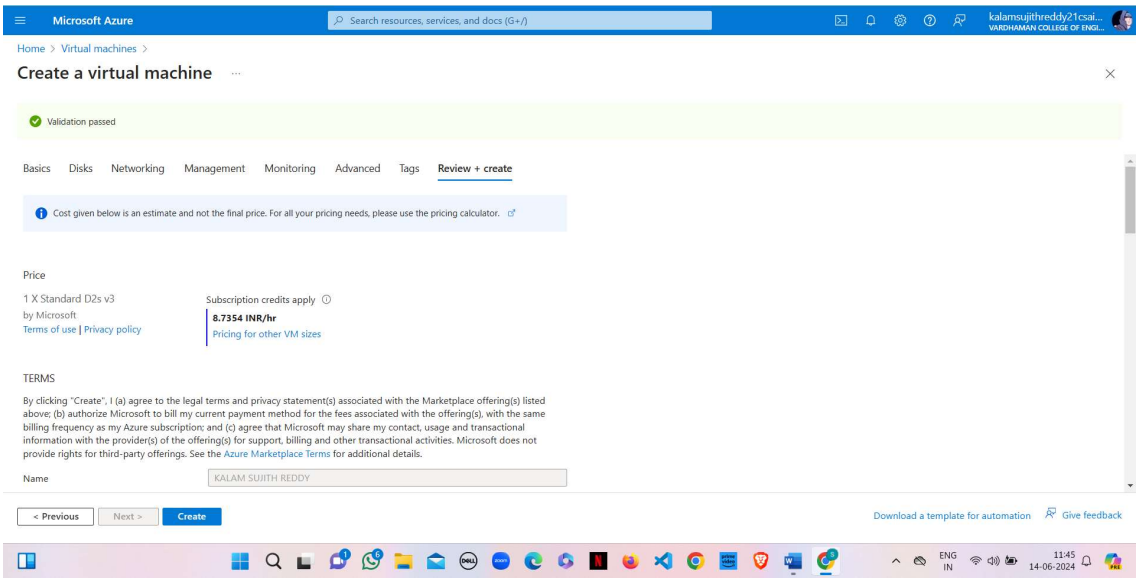
Step 6 : Select

Storage type -------Premium SSD(LRS), Custom disk size (GB) ------5

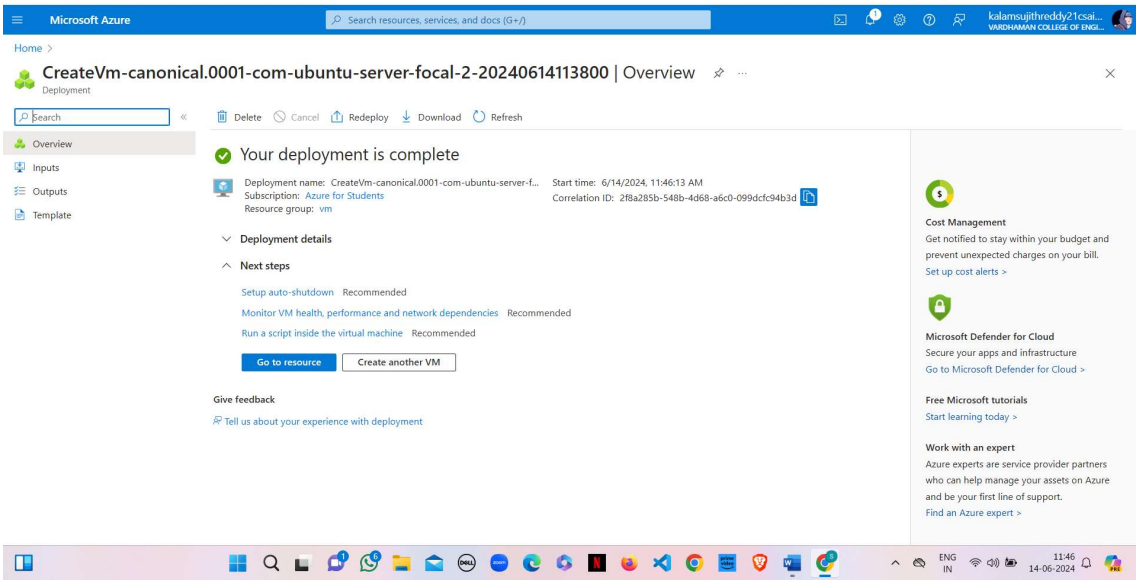
click on OK

Step 7 : Click on "Review + create" & click on create

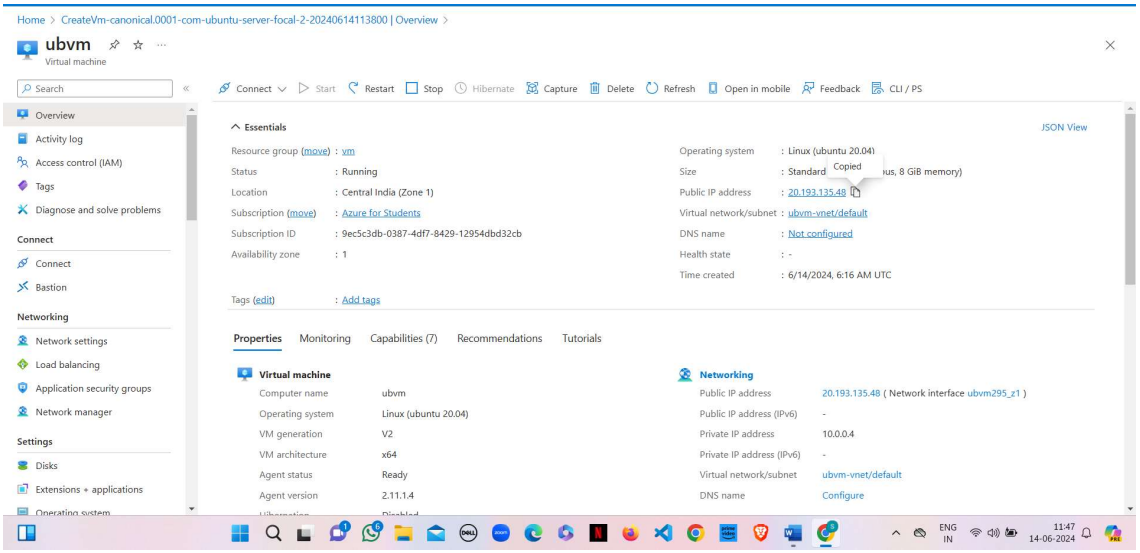




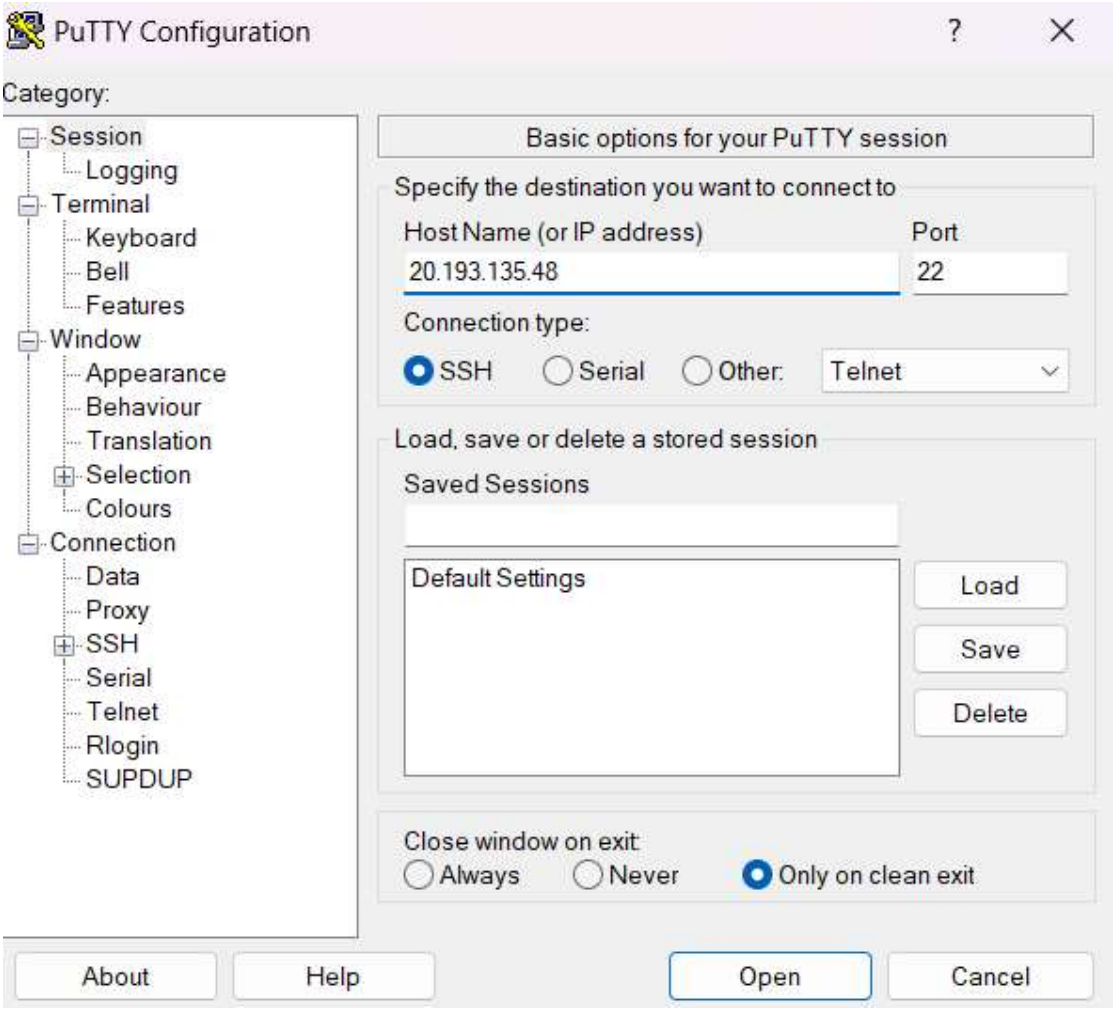
Step 8 : Click on "Go to resource group"



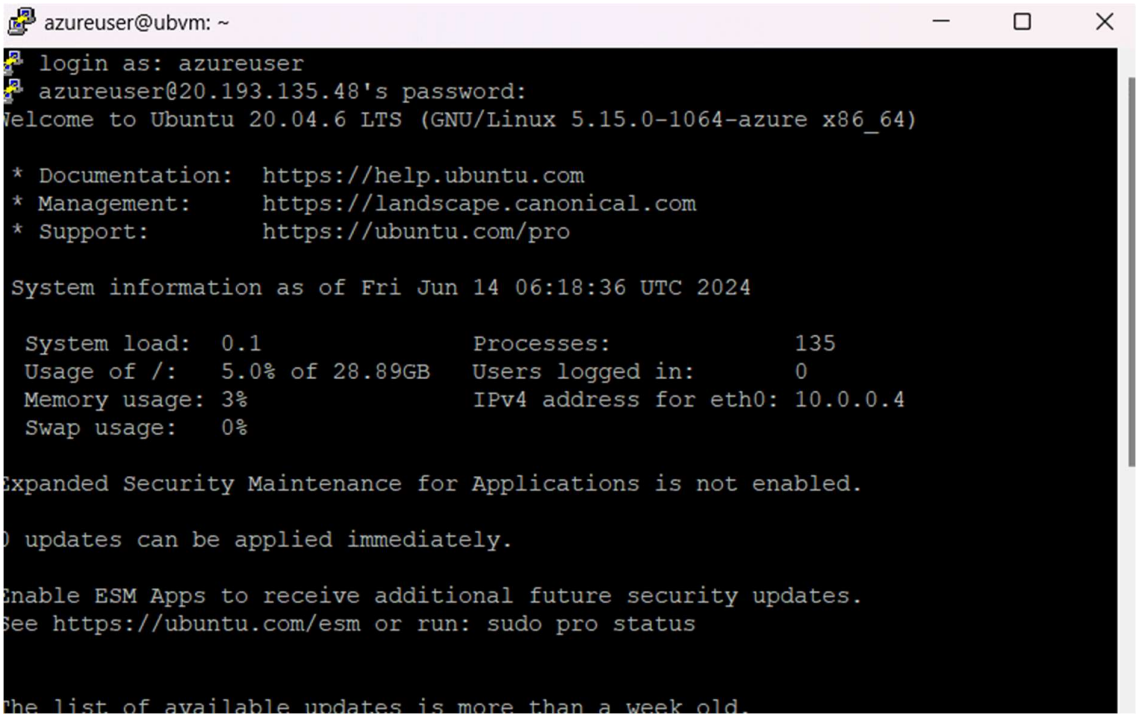
Step 9 : Copy public IP Address



Step 10 : Open "PUTTY" & paste the IP adress and click on "open"



Step 11 : Login into it with username and password



Step 12 : Type the below commands

$ df -hT

$ lsblk

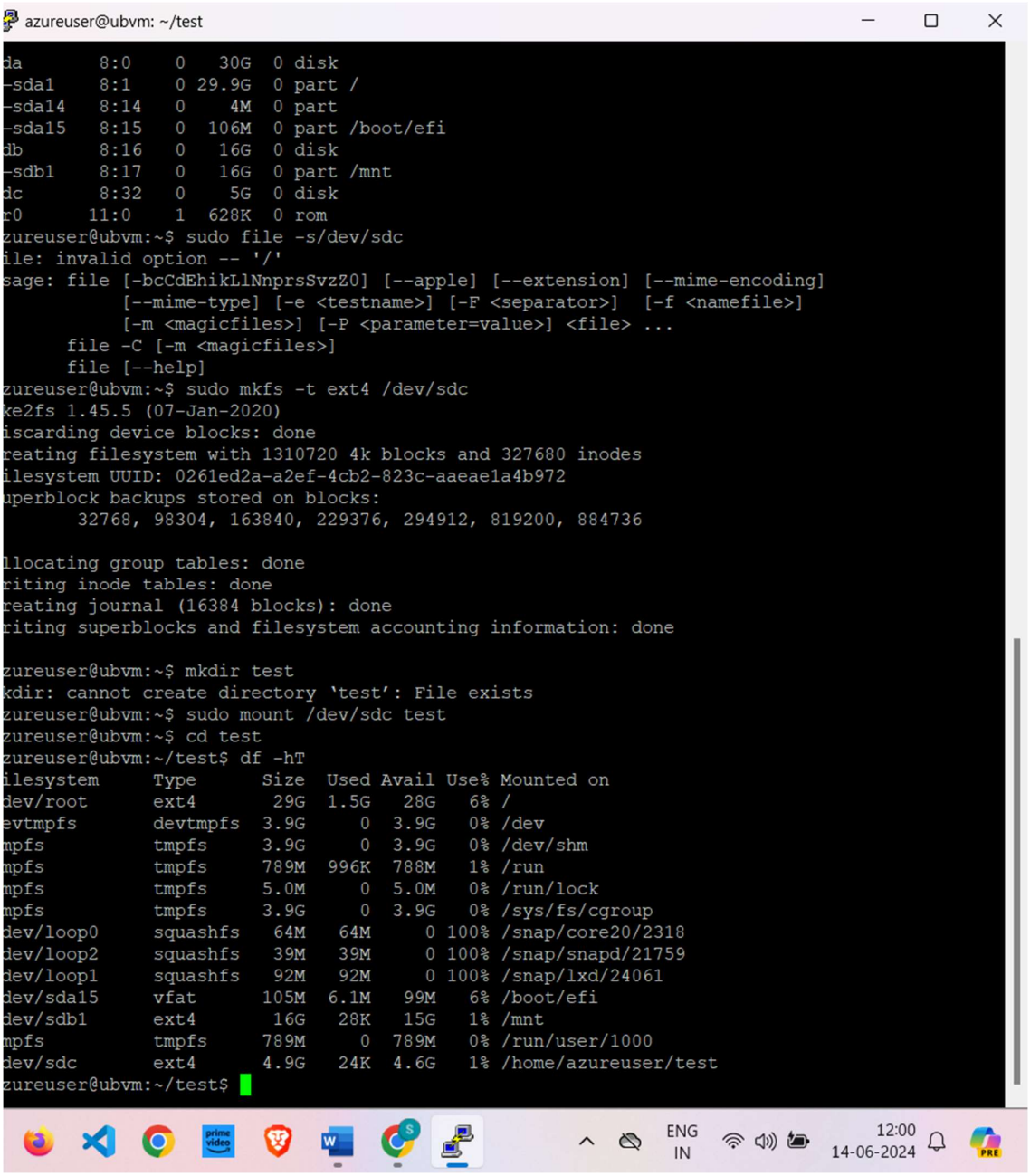
$ sudo filoe -s/dev/sdc

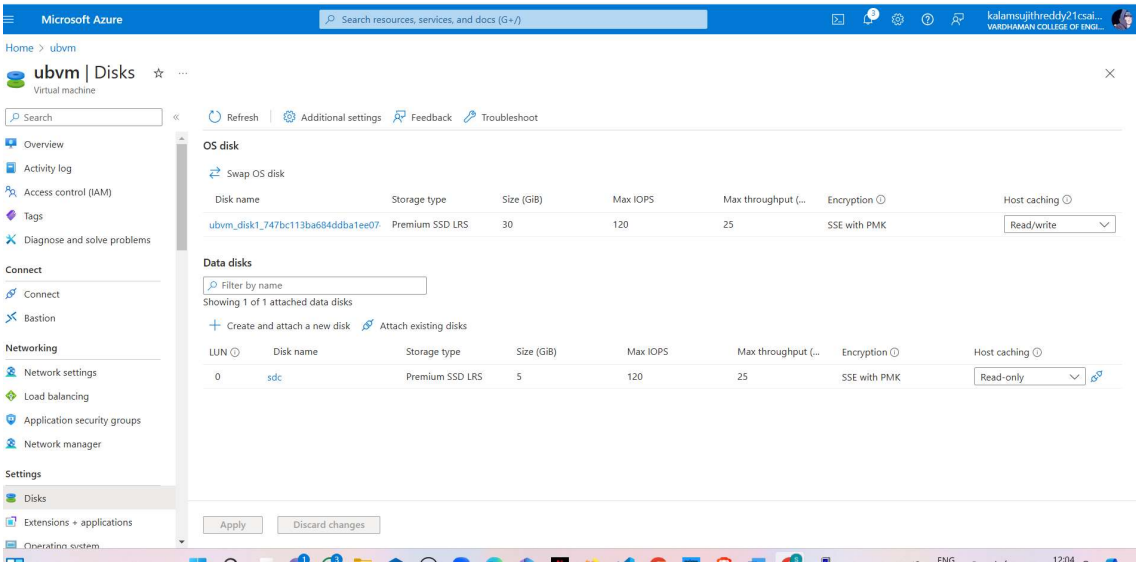
$ sudo mkfs -t ext4 /dev/sdc

$ mkdir test

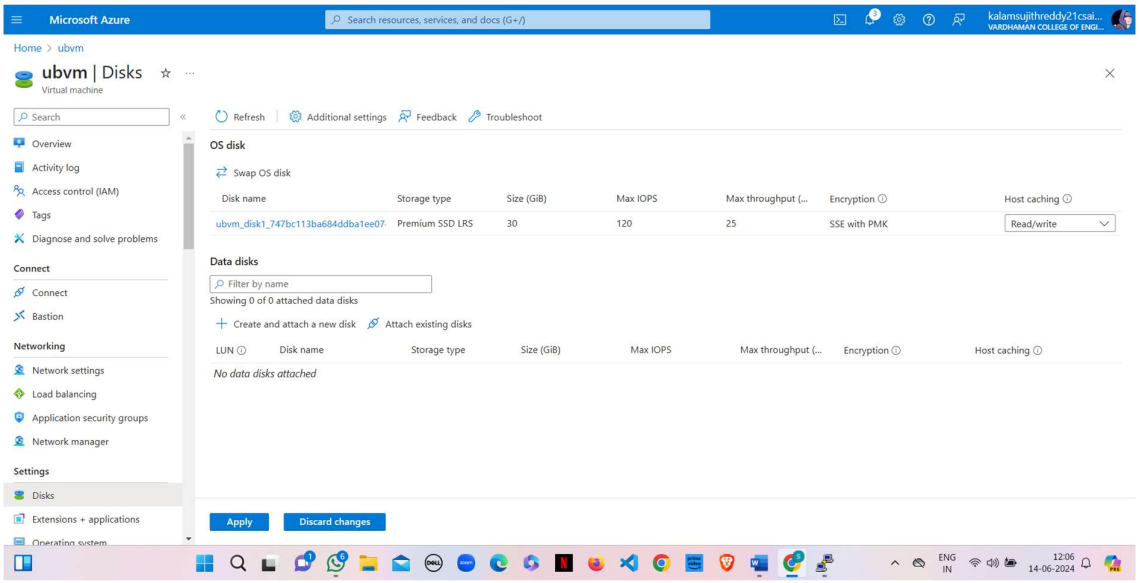
$ sudo mount /dev/sdc/ test

$ cd test


azureuser@ubvm: ~/test
da 8:0 0 30G 0 disk
-sda1 8:1 0 29.9G 0 part /
-sda14 8:14 0 4M 0 part
-sda15 8:15 0 106M 0 part /boot/efi
db 8:16 0 16G 0 disk
-sdb1 8:17 0 16G 0 part /mnt
dc 8:32 0 5G 0 disk
r0 11:0 1 628K 0 rom
zureuser@ubvm:~$ sudo file -s/dev/sdc
ile: invalid option -- '/'
sage: file [-bcCdEhikLlNnprsSvzZ0] [--apple] [--extension] [--mime-encoding]
[--mime-type] [-e <testname>] [-F <separator>] [-f <namefile>]
[-m <magicfiles>] [-P <parameter=value>] <file> ...
file -C [-m <magicfiles>]
file [--help]
zureuser@ubvm:~$ sudo mkfs -t ext4 /dev/sdc
ke2fs 1.45.5 (07-Jan-2020)
iscarding device blocks: done
reating filesystem with 1310720 4k blocks and 327680 inodes
ilesystem UUID: 0261ed2a-a2ef-4cb2-823c-aaeae1a4b972
uperblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736
llocating group tables: done
riting inode tables: done
reating journal (16384 blocks): done
riting superblocks and filesystem accounting information: done
zureuser@ubvm:~$ mkdir test
kdir: cannot create directory 'test': File exists
zureuser@ubvm:~$ sudo mount /dev/sdc test
zureuser@ubvm:~$ cd test
zureuser@ubvm:~/test$ df -hT
ilesystem Type Size Used Avail Use% Mounted on
dev/root ext4 29G 1.5G 28G 6% /
evtmpfs devtmpfs 3.9G 0 3.9G 0% /dev
mpfs tmpfs 3.9G 0 3.9G 0% /dev/shm
mpfs tmpfs 789M 996K 788M 1% /run
mpfs tmpfs 5.0M 0 5.0M 0% /run/lock
mpfs tmpfs 3.9G 0 3.9G 0% /sys/fs/cgroup
dev/loop0 squashfs 64M 64M 0 100% /snap/core20/2318
dev/loop2 squashfs 39M 39M 0 100% /snap/snapd/21759
dev/loop1 squashfs 92M 92M 0 100% /snap/lxd/24061
dev/sda15 vfat 105M 6.1M 99M 6% /boot/efi
dev/sdb1 ext4 16G 28K 15G 1% /mnt
mpfs tmpfs 789M 0 789M 0% /run/user/1000
dev/sdc ext4 4.9G 24K 4.6G 1% /home/azureuser/test
zureuser@ubvm:~/test$
ENG
IN
12:00
14-06-2024



Step 13 : Click on Apply



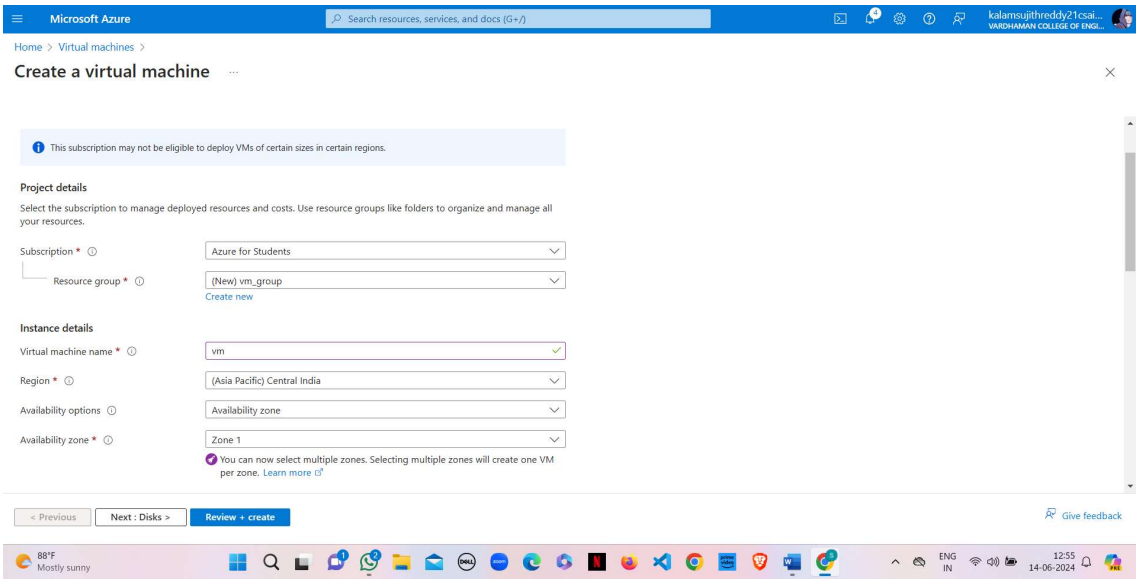
Result:

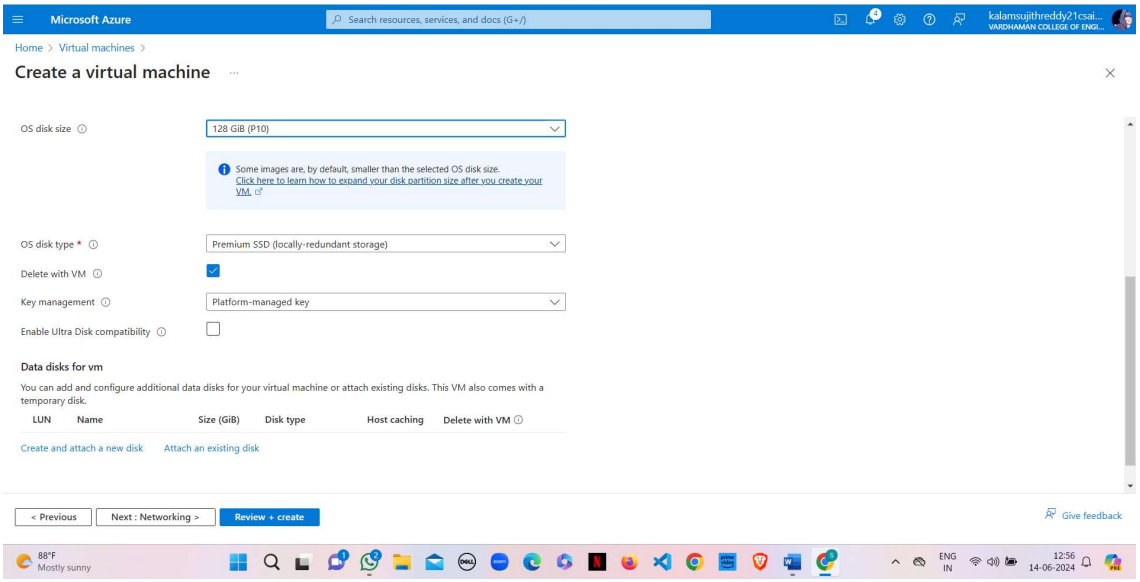
Attached and detached a data disk to a Linux server in Azure. The operations were performed without downtime, and the disk was recognized and accessible after attachment, then safely removed.

Q11) Perform attach and detach of data disk to Windows Server in Azure.

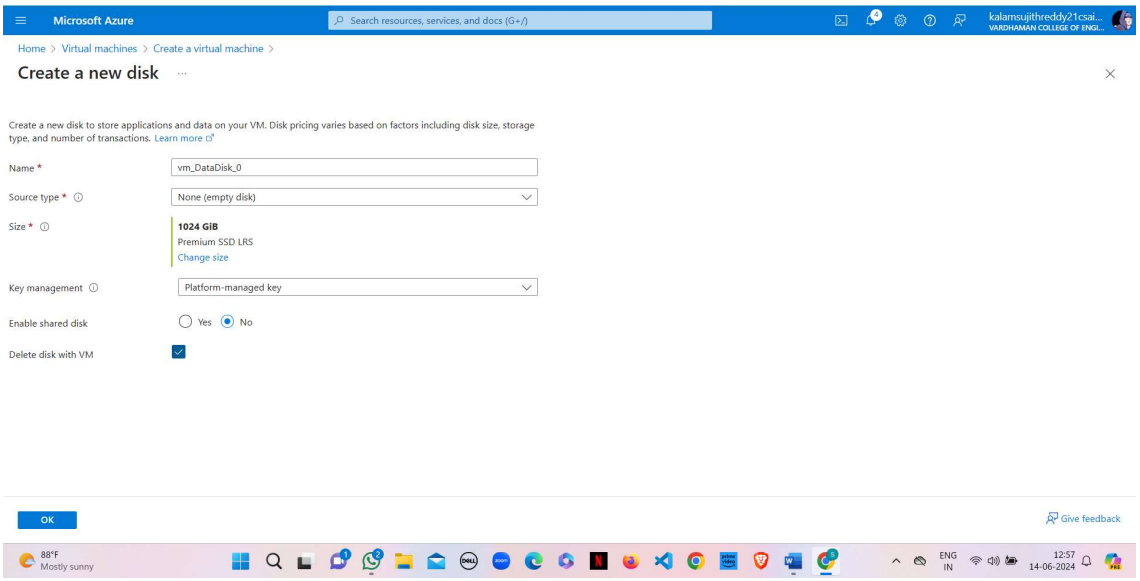
Steps:-

1) Create a Virtual name with username &password

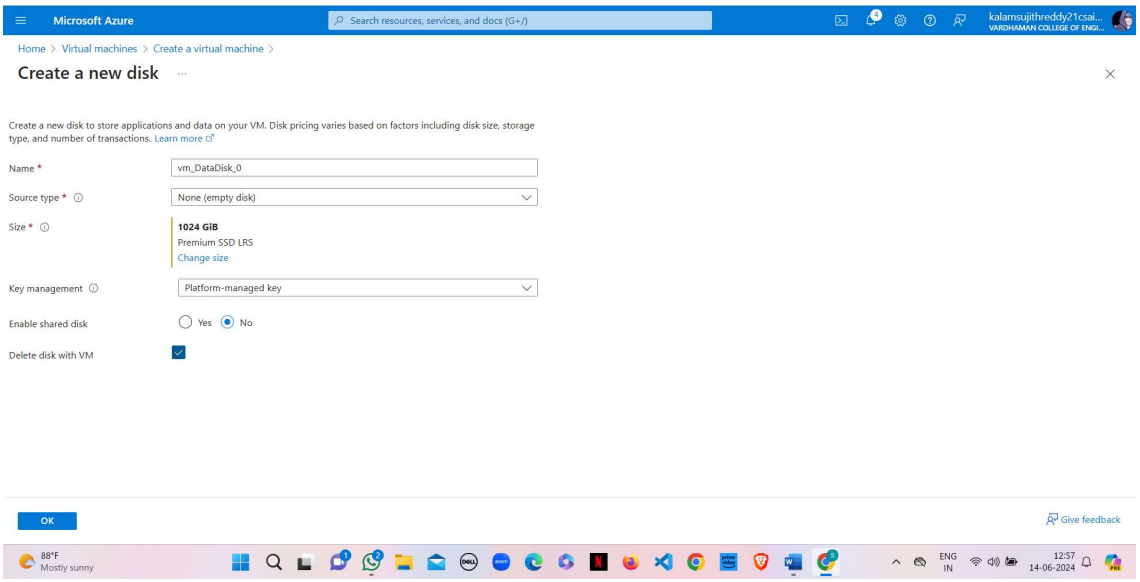




2) Click on "Next:Disks>"



3) Click on "Create & attach a new disk"



4) Click on “change size”

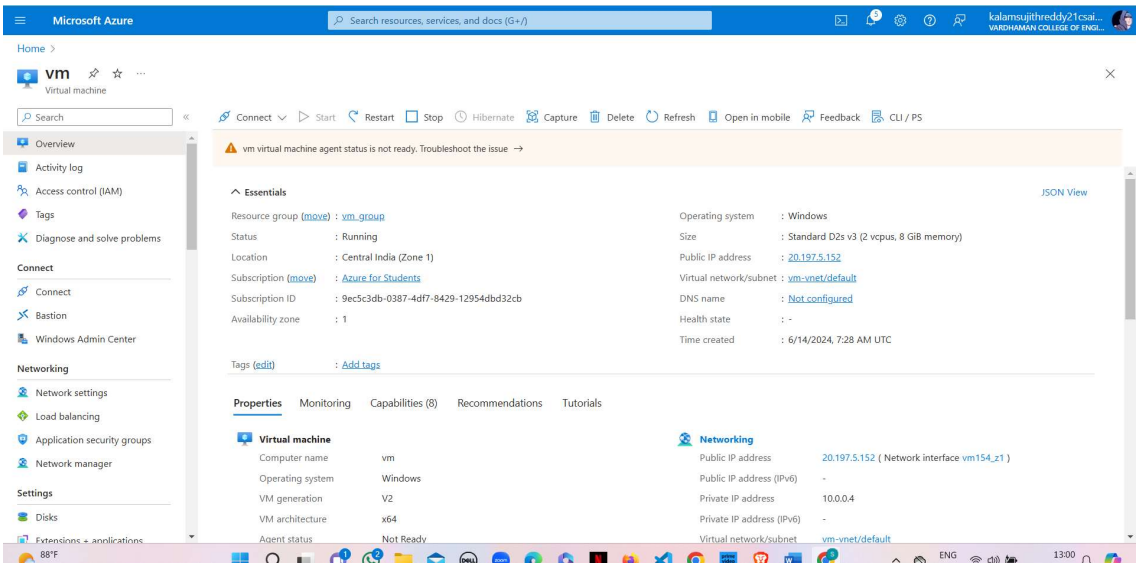
5) Customize data size to 10 GiB and click on OK

6) Enable delete with VM and click on OK

7) Click on "Review+create" & click on create

8) Click on "Go to resource group"

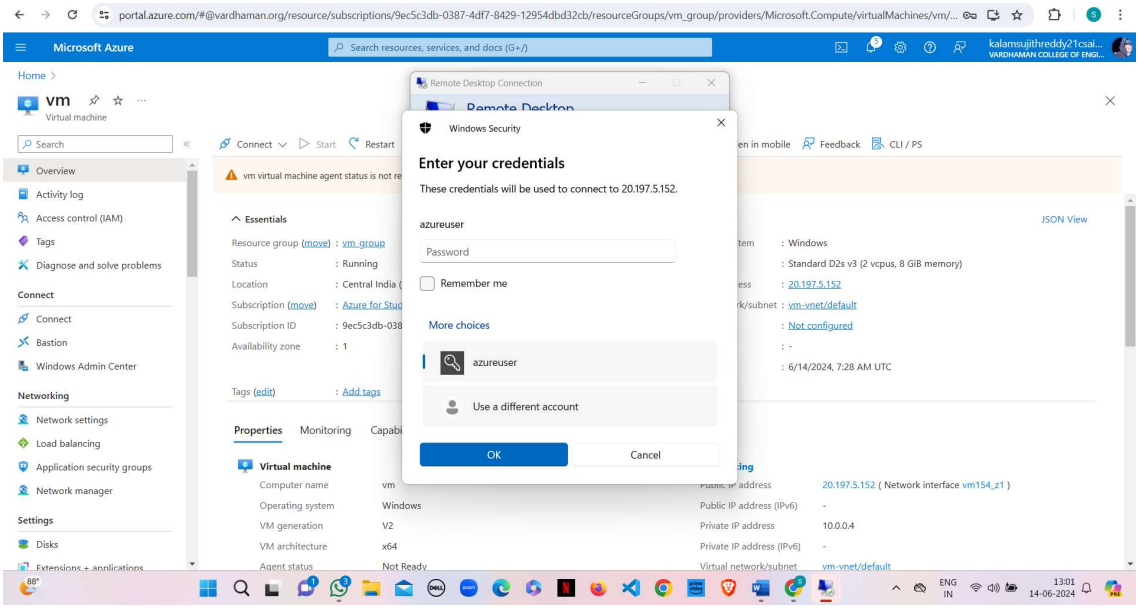
9) Copy public IP Address



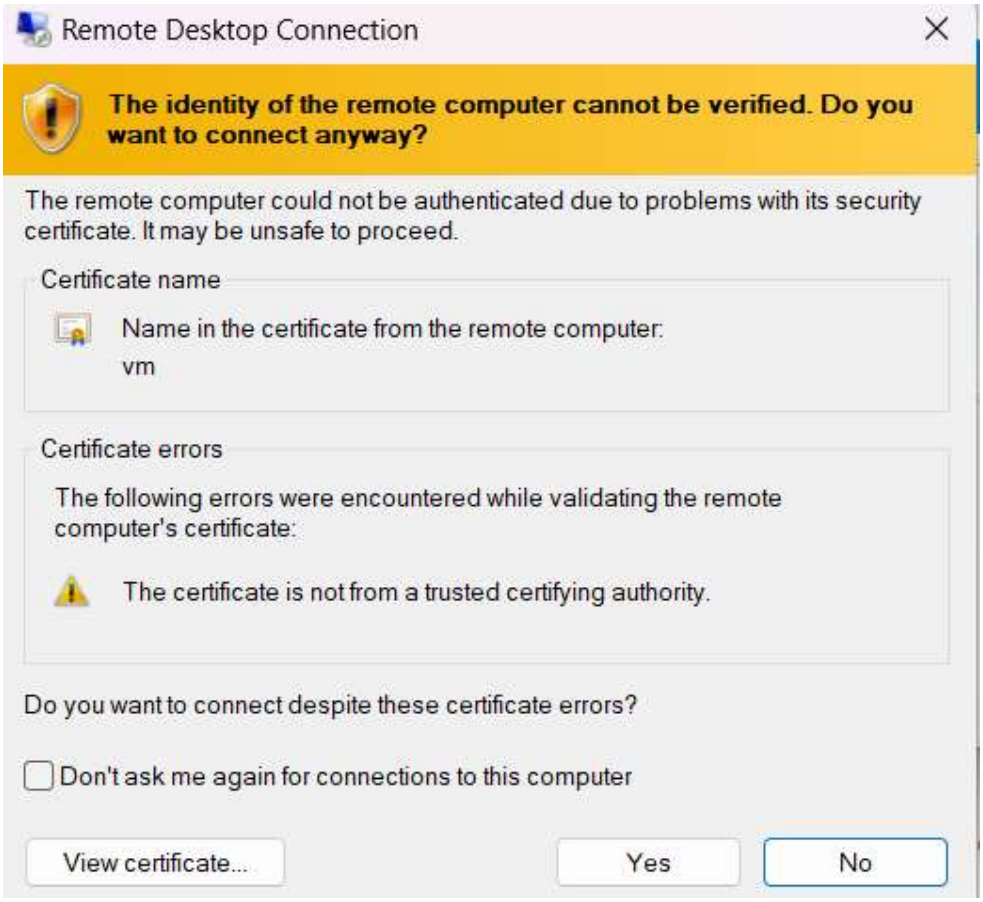
10) Open Remote Desktop Connection in your windows/system and paste the public IP Address

11) Click on “More choices”

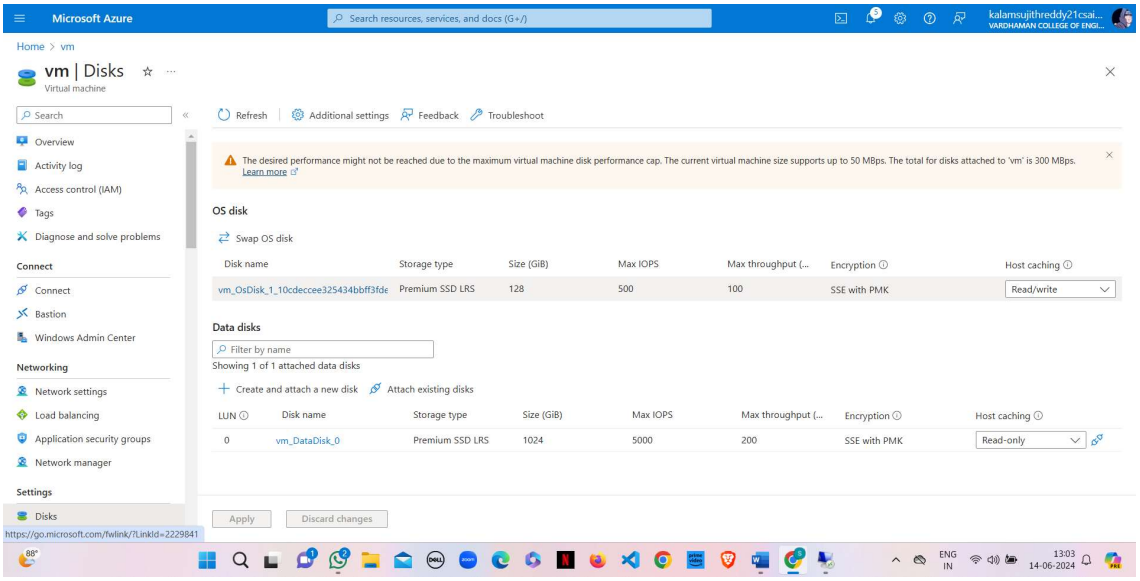
12) Click on “Use a different account”, enter the credentials and click on OK



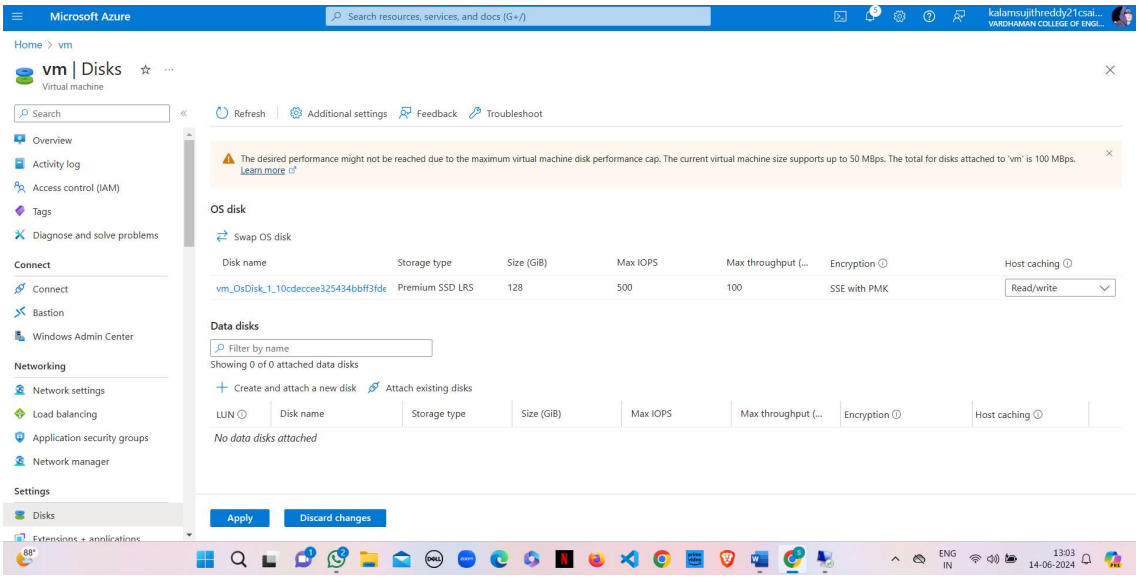
13) Click on yes and now the data disks are attached to the windows server



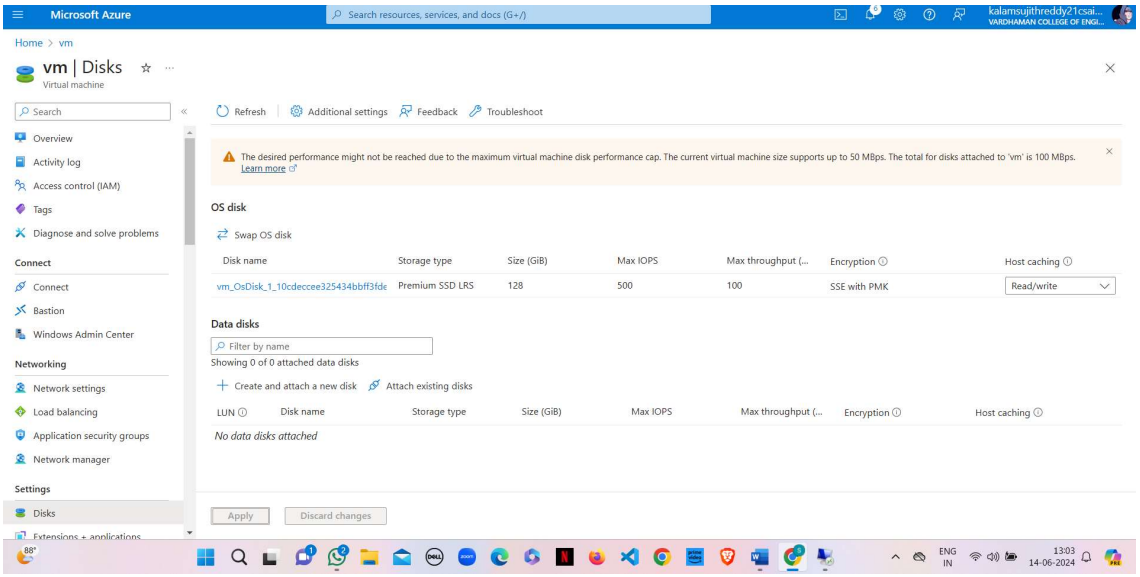
14) Click on “Disks” in your VM and you can see the attached data disks to the windows server



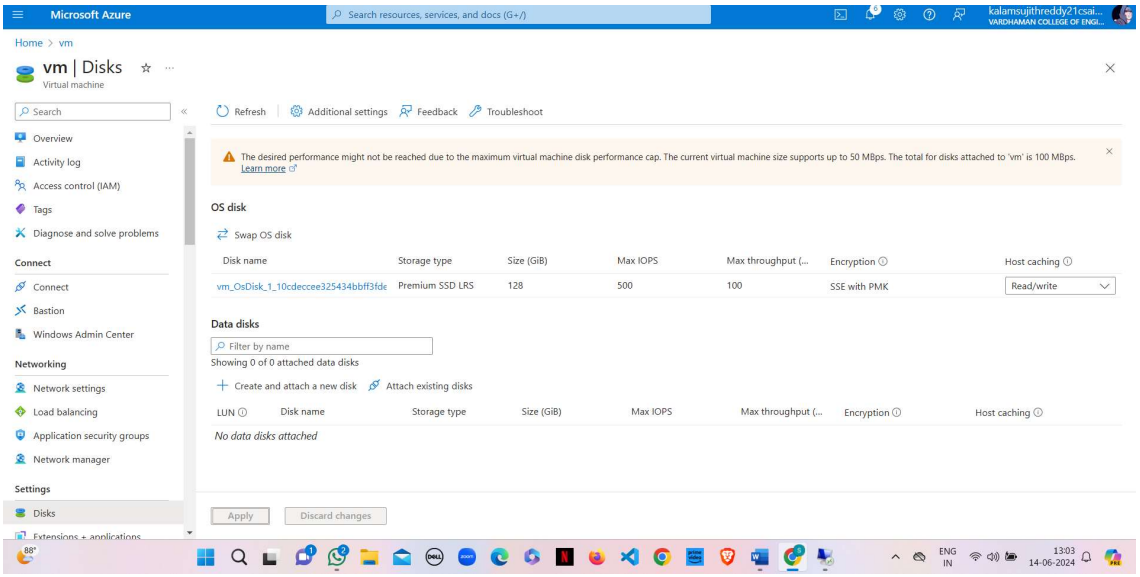
15) Detach the data disks from the windows server by clicking on the detach symbol



16) Click on “Apply”



17) Now the data disks are detached from the windows server

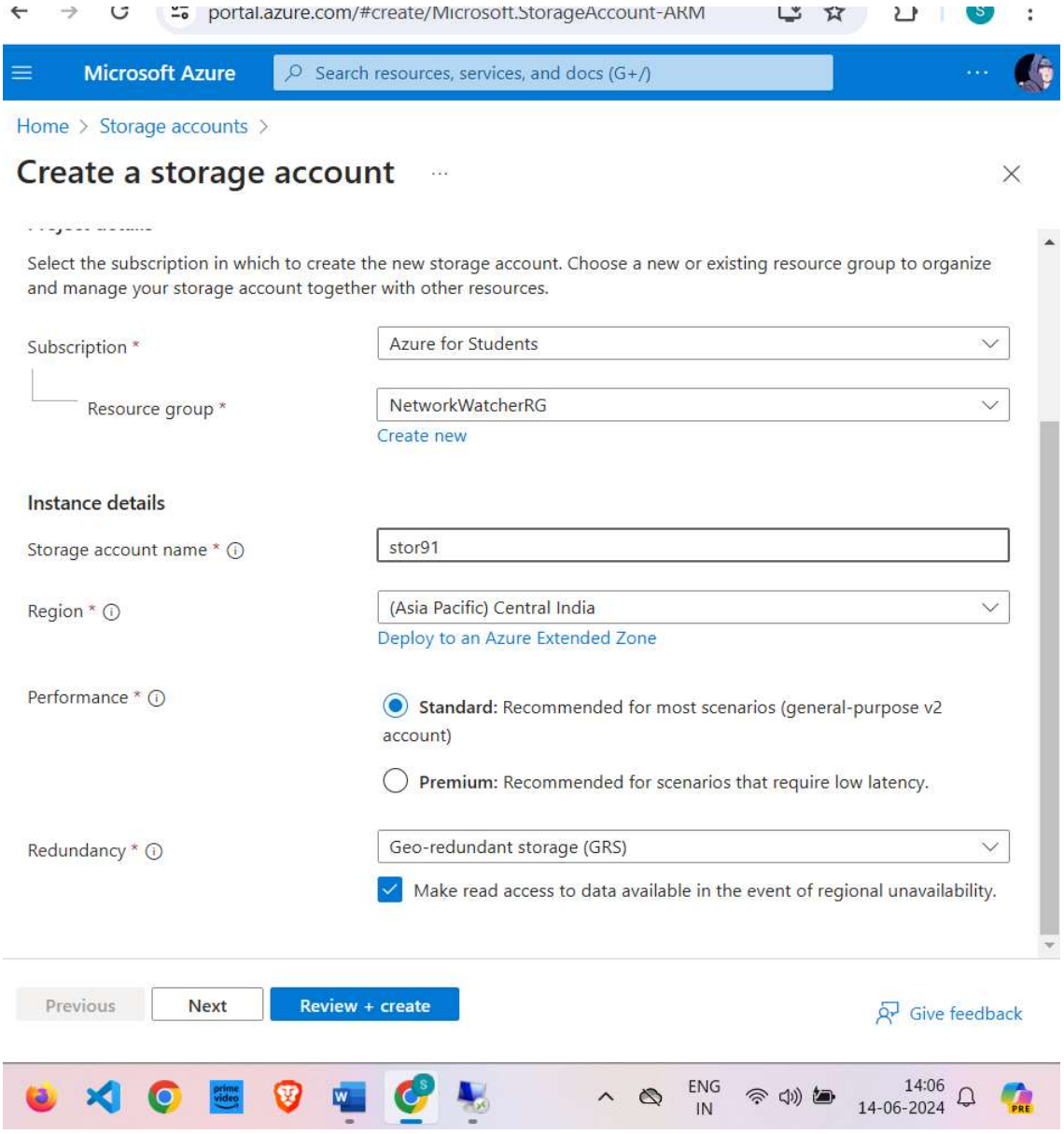


Result:

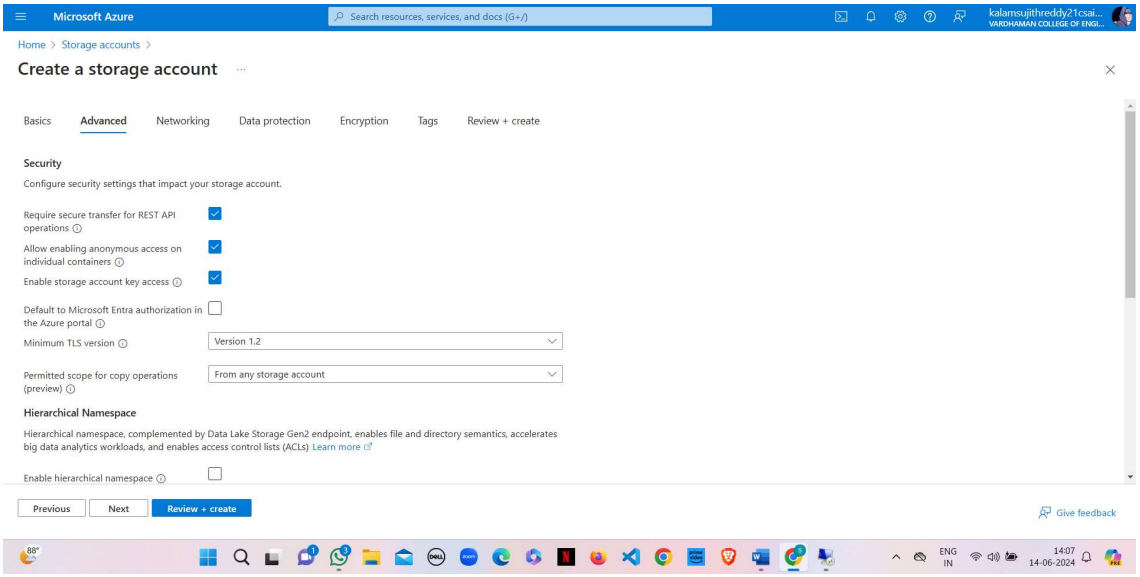
Successfully attached and detached a data disk to a Windows server in Azure. The disk was available for use upon attachment and removed cleanly without data loss.

Q12) Create Azure Storage Account, Container and upload and delete objects in it.

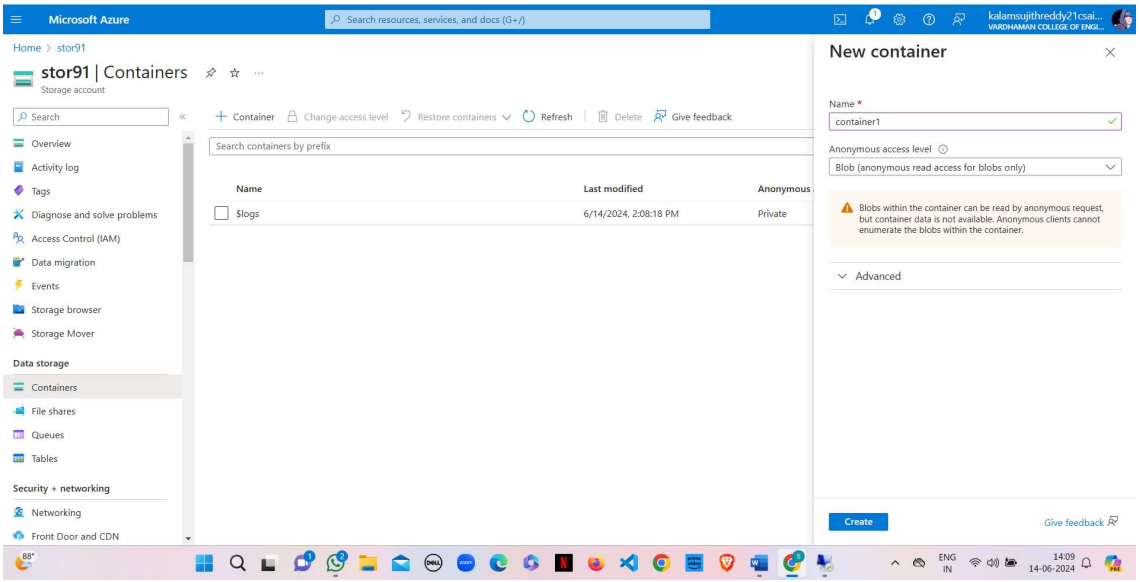
Step-1: Click On Storage Account and Create one and select redundancy as GRS/LRS.



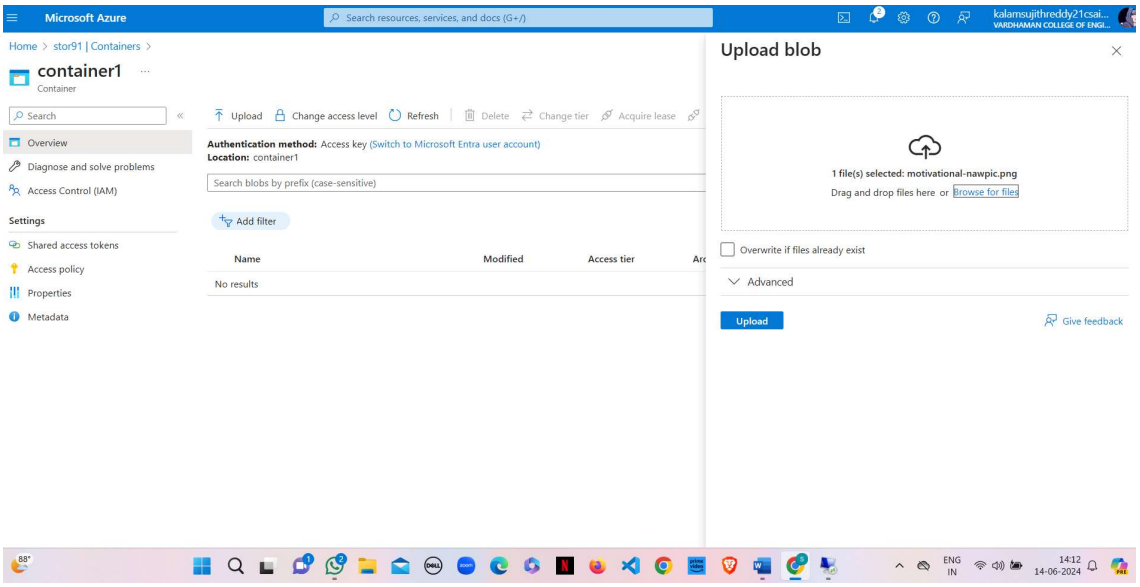
Step-2: Go to advance and Allow enabling anonymous access on individual containers.



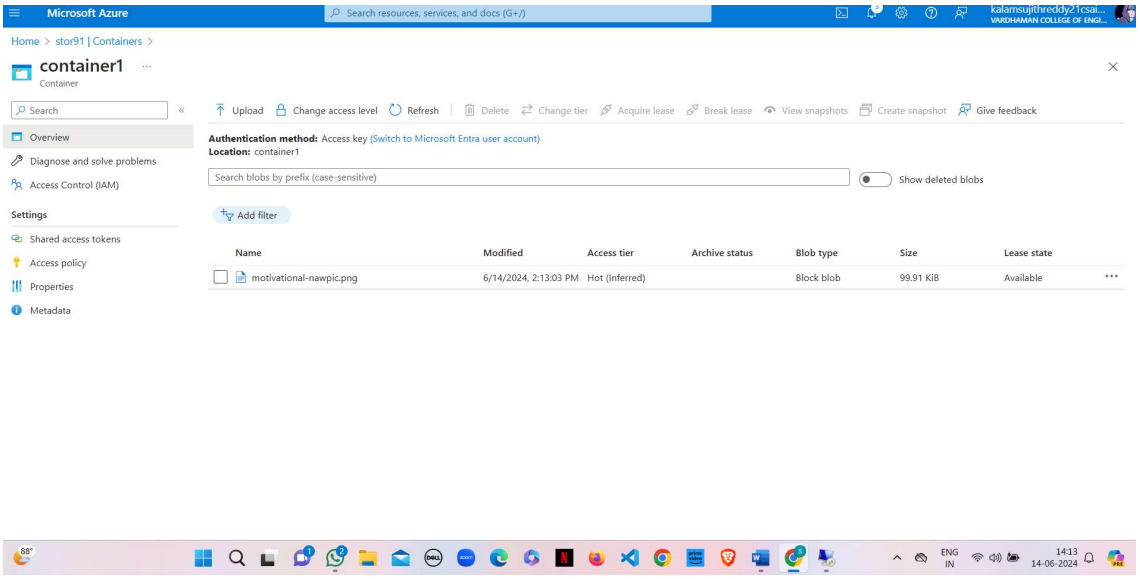
Step-3: After deployment Click on go to resource group and on Left Click on Containers and Create it with anonymous access level as blob (anonymous read access to blob only)

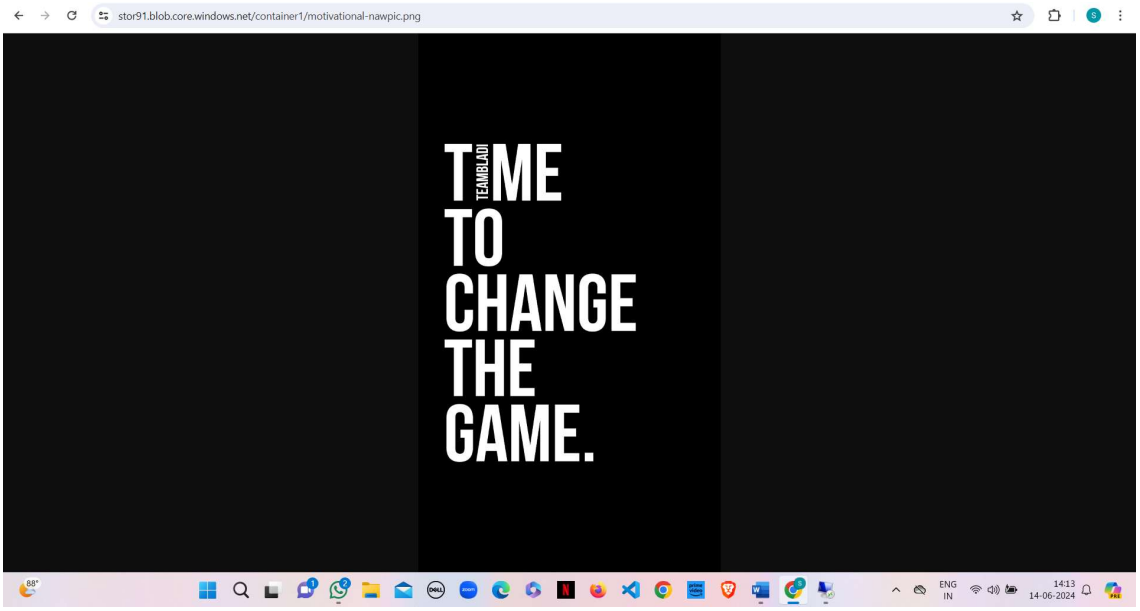


Step-4: Then open new container, click on upload and upload a file from desktop.

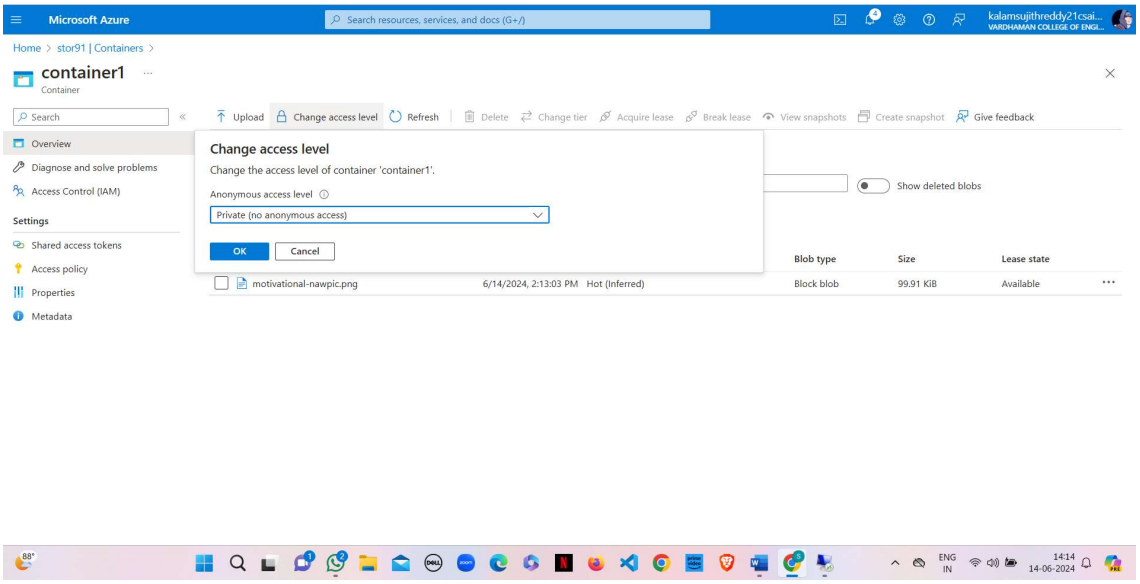


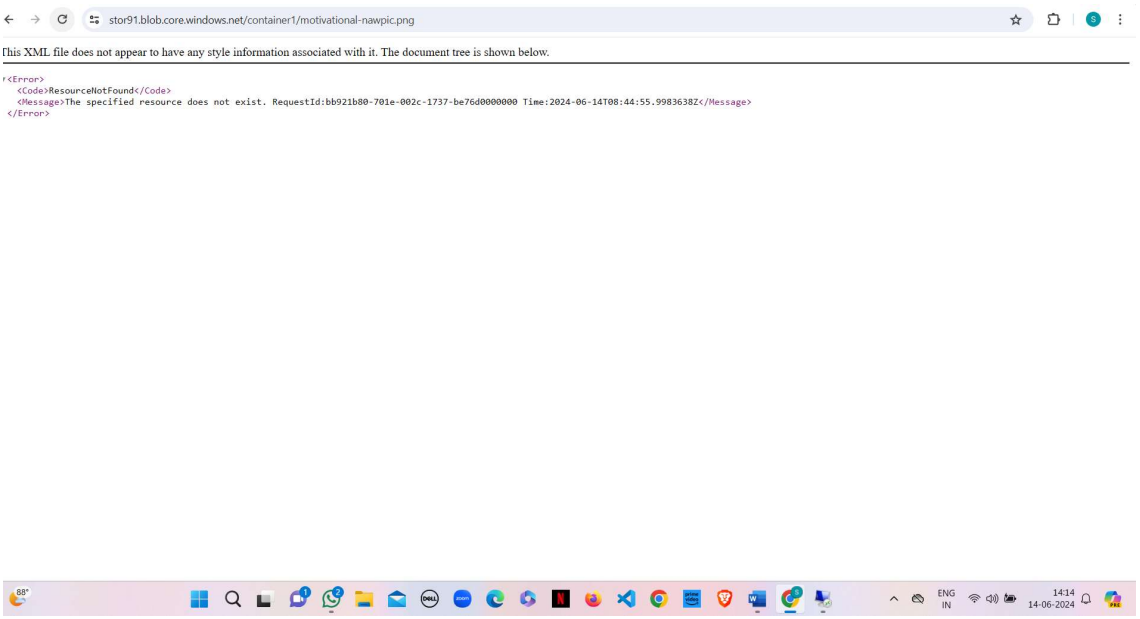
Step-5: Select the file and click on provided URL to open the file.



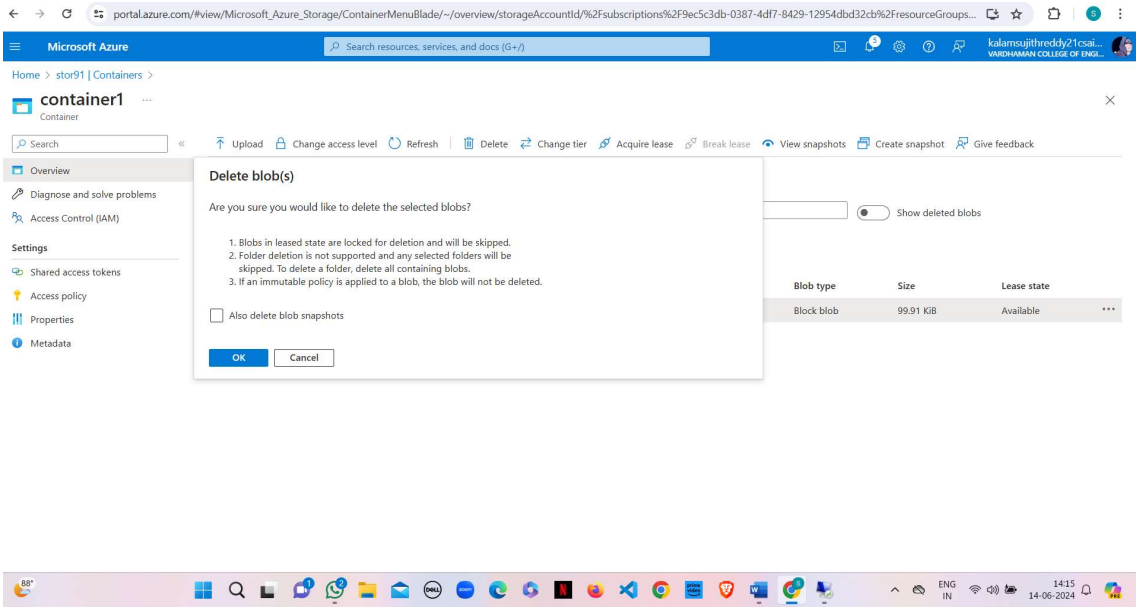


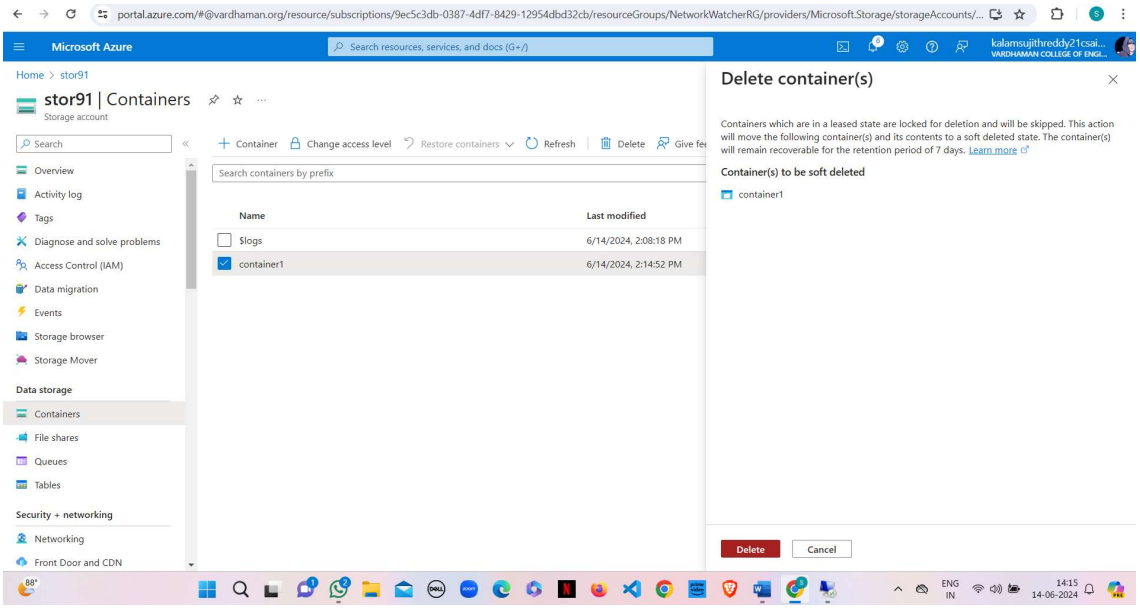
Step-6: On container click Change access level to Private (no anonymous access) and try to open the file in new tab it will show error.

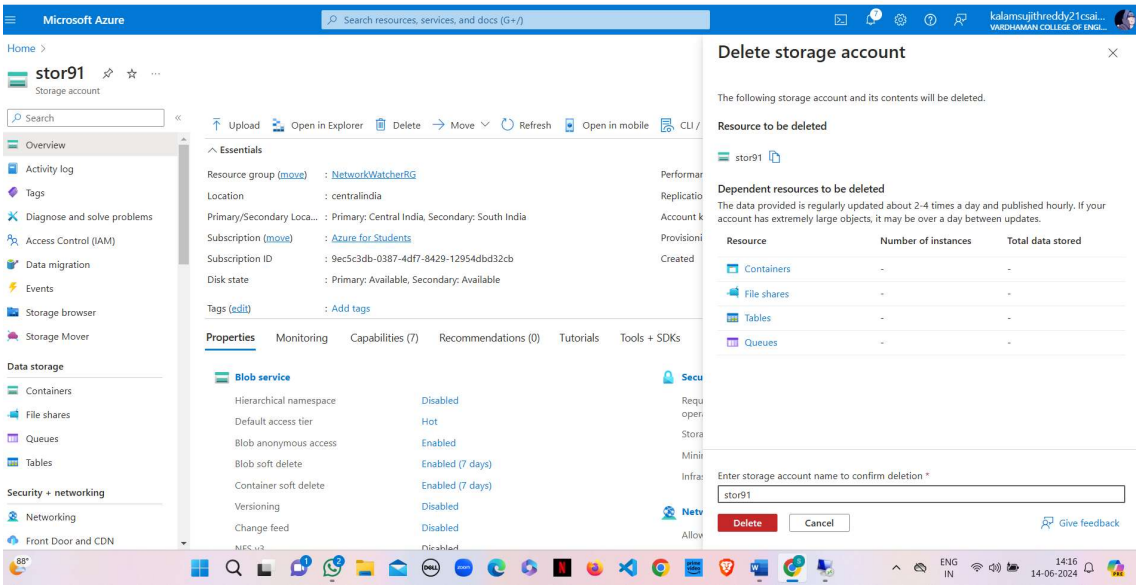




Step-7: Then delete blob container and storage account.







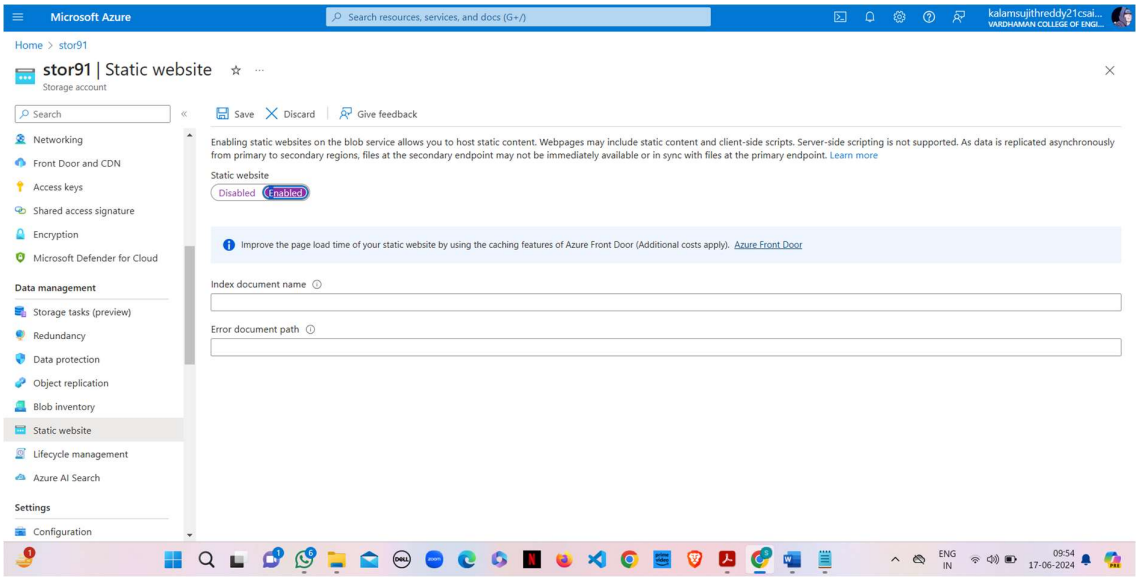
Result:

Created an Azure Storage Account and container, then uploaded and deleted objects within it. All operations were successfully performed, confirming the storage functionalities.

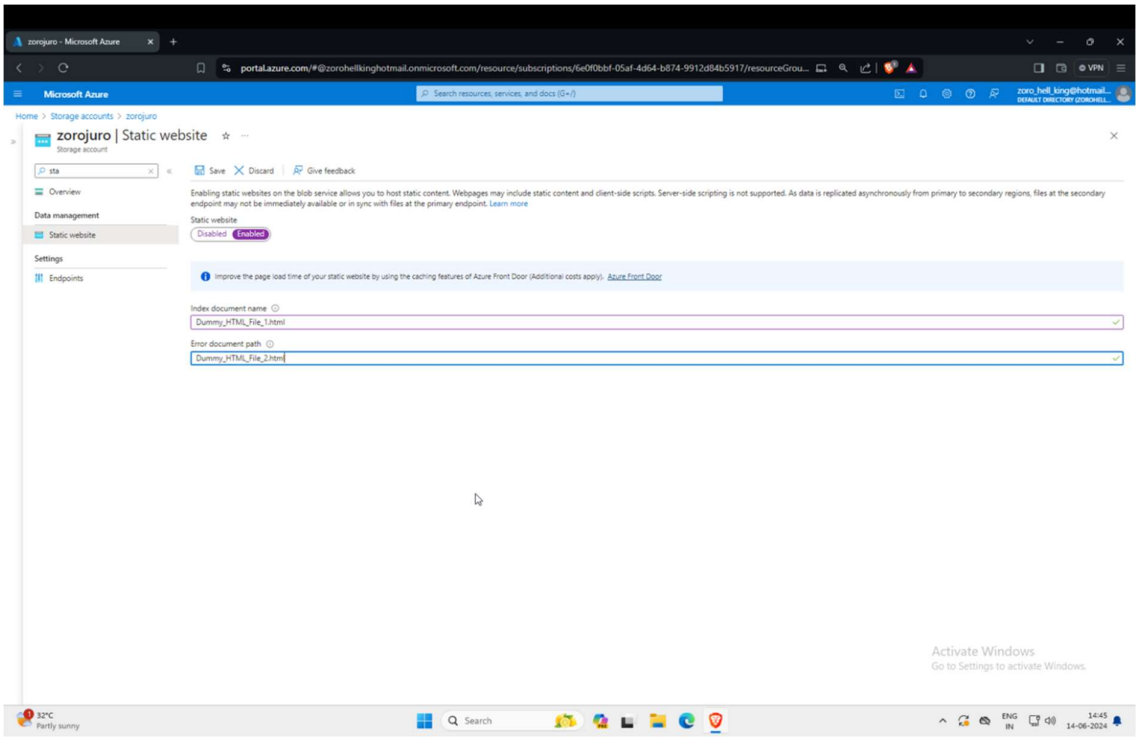
Q13) Implement static web hosting in Azure portal.

Step-1: As demonstrated in previous programs create a `Storage Account` and then create a `Container` with the required configurations.

Step-2: Navigate to the `Static website` section under `Settings` in the left-hand menu of your storage account. Click `Enabled` to turn on static website hosting.



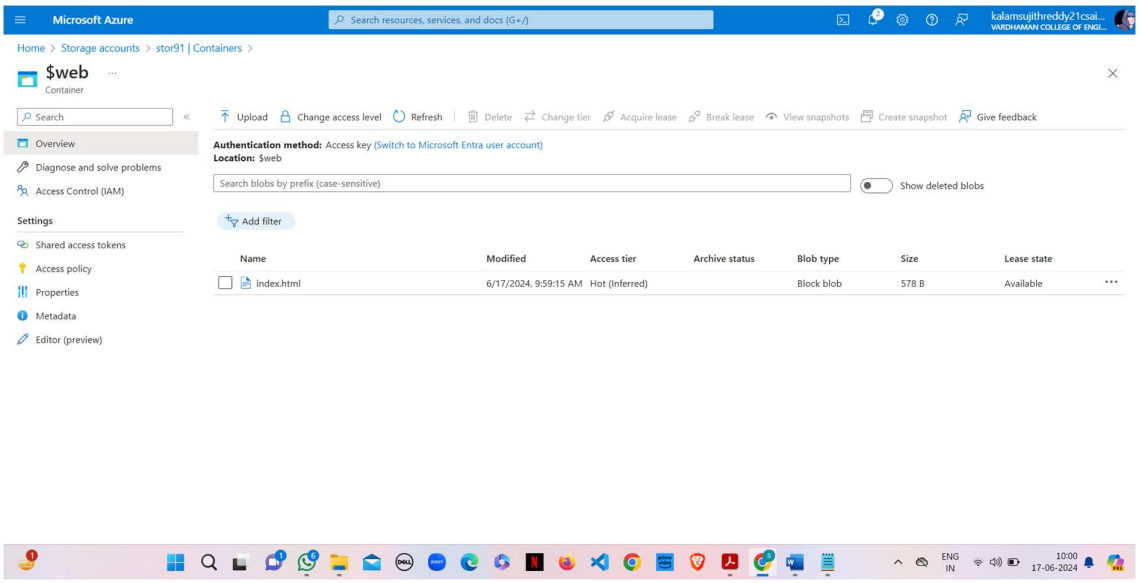
Step-3: Enter the name of your index document (e.g., index.html) in the `Index document name` field. Optionally, enter the name of your error document (e.g., 404.html) in the `Error document path` field. Click `Save` to apply the settings.



Step-4: Click on the name of the container you just created to open it and go to `$web` blob.

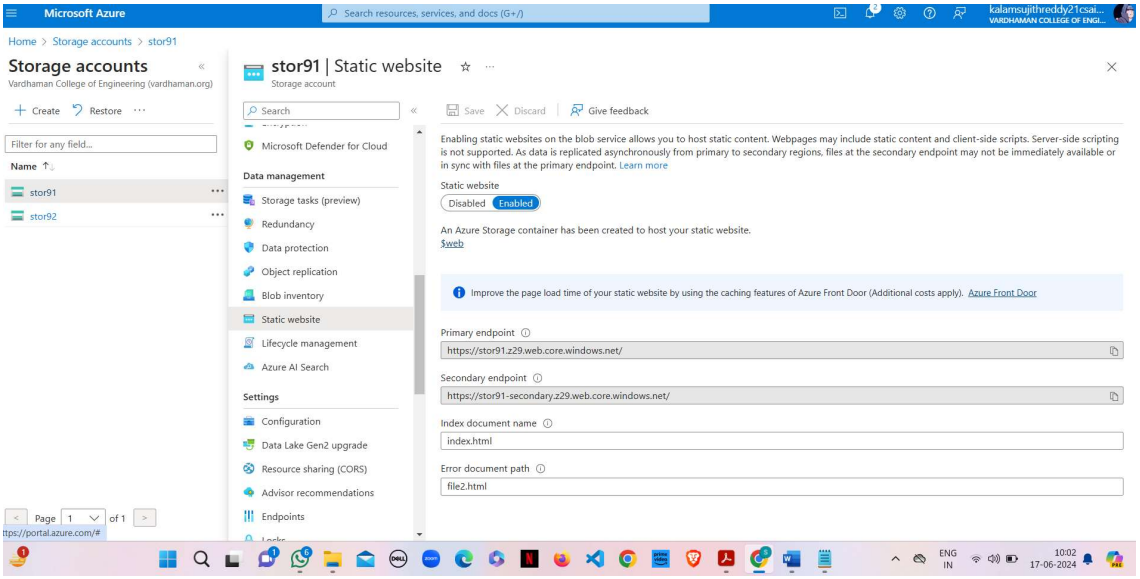
Step-5: Click on `Upload` to open the upload pane. Click `Browse` to choose the files you wish to upload from your local device (e.g., index.html, style.css, etc.). Click `Upload` to start uploading the files to the container.

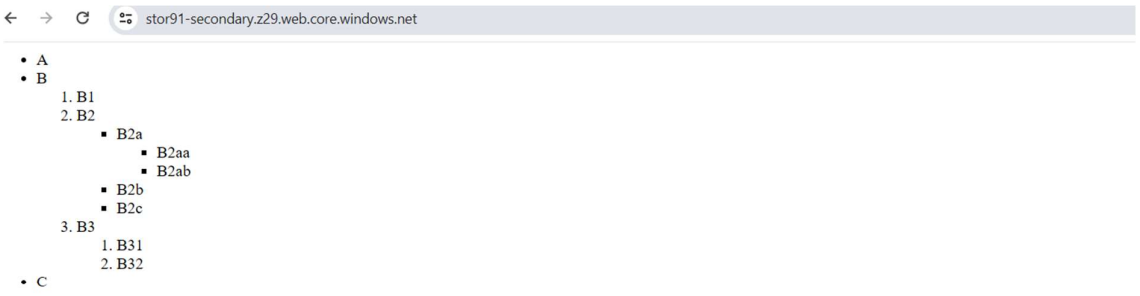
Step-6: After enabling static website hosting, you will see the primary endpoint URL for your static website at the top of the `Static website` page. Copy this URL.



Step-7: Paste the copied URL into your web browser to access your static website.

Step-8: Copy the URL listed under `Secondary endpoint` and paste it in the browser.





Result:

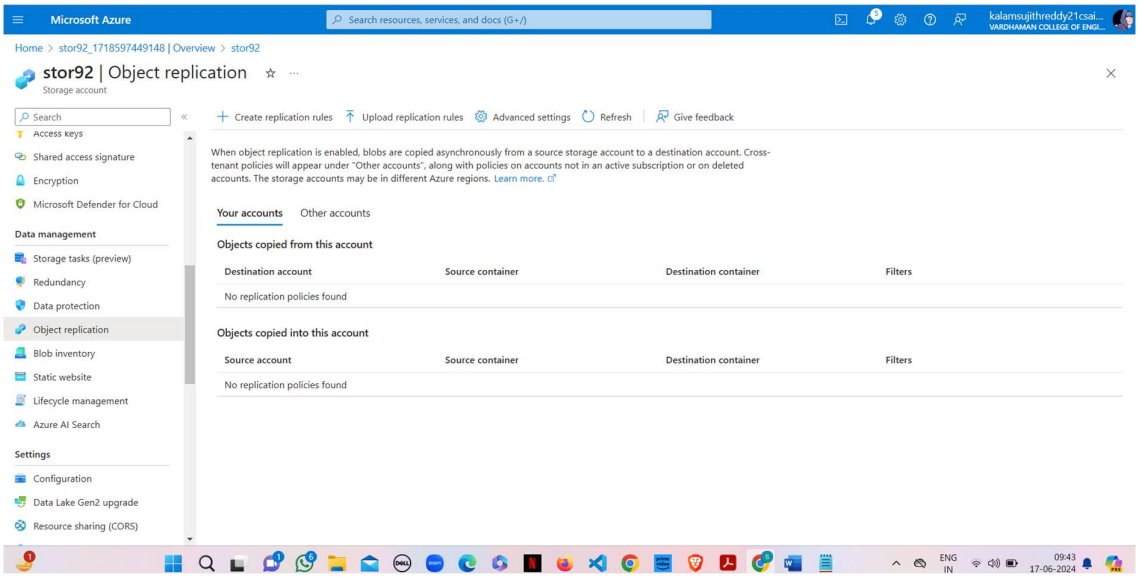
As you can observe both webpages accessed from primary and secondary endpoints are same. Seeing the same pages on both the primary and secondary endpoints is expected behaviour due to Azure's replication mechanisms. This setup ensures high availability and data redundancy, providing seamless access to your content even if one region goes down.

Q14) Implement object replication through Azure portal.

Step-1: As demonstrated in the previous program. Please create a Container each in two different Storage Accounts.

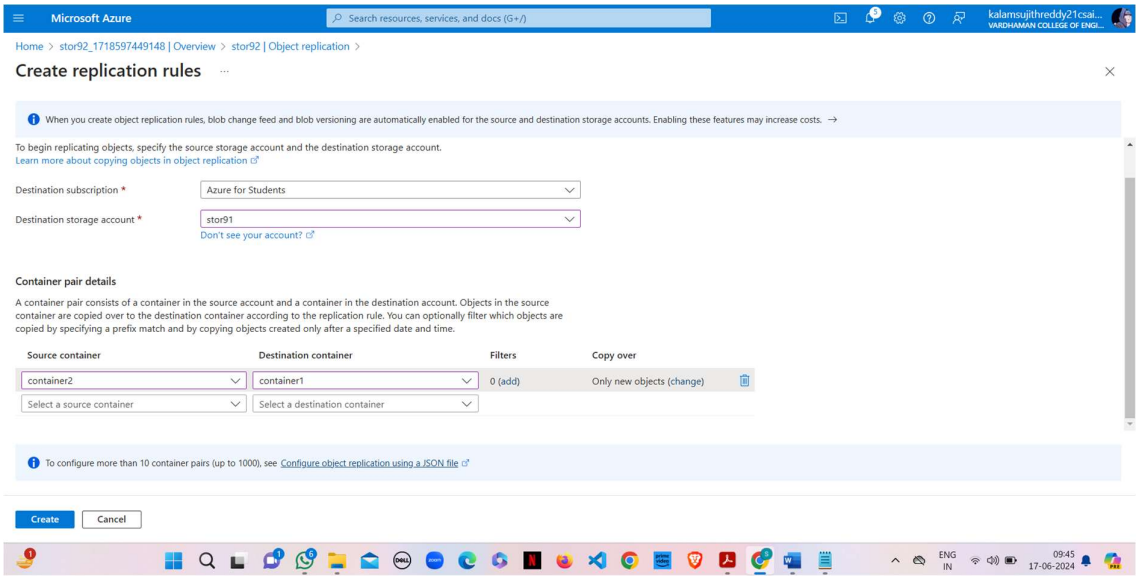
Step-2: Go to the resource page of the source storage account.

Step-3: Under the `Data management` section, click on `Object replication`. Click on `Add replication policy`.

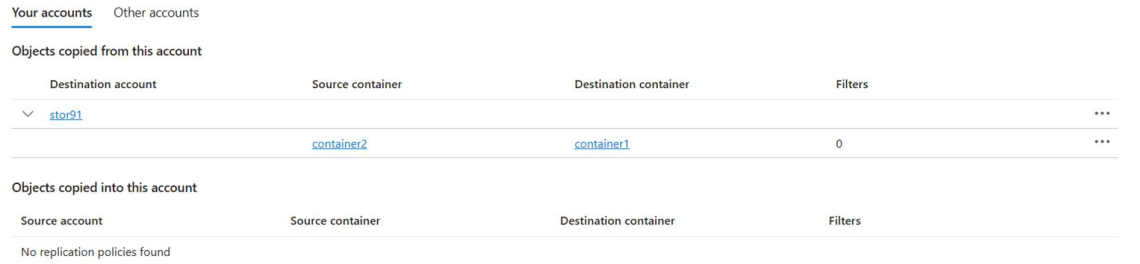


Step-4: Enter the destination storage account name or select it from the list. You might need to provide the destination storage account key. Obtain the key from the destination storage account under `Access keys`.

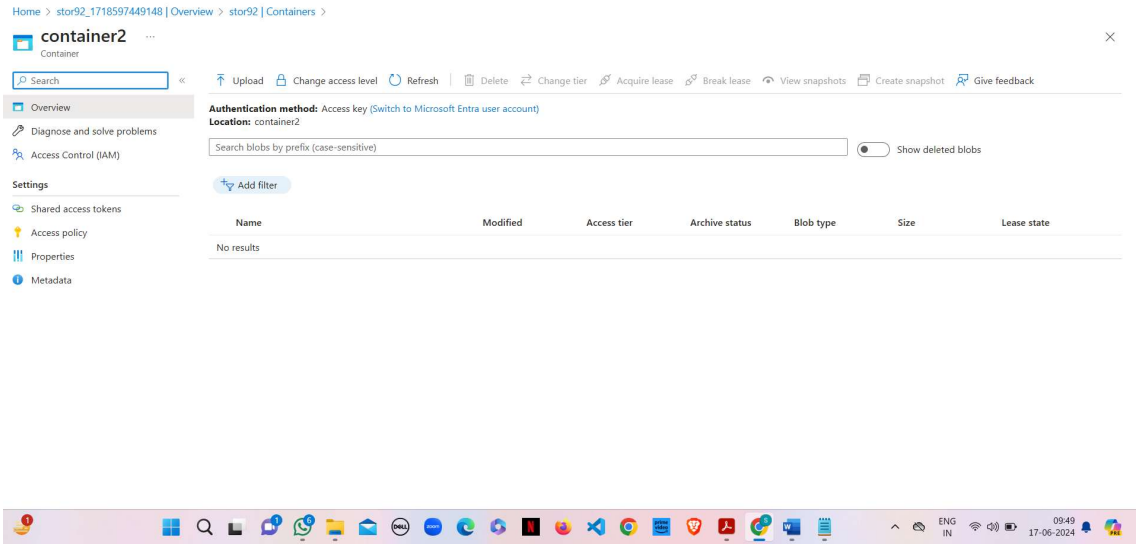
Step-5: Define the source and destination containers. Specify the replication rules, such as prefixes for which objects to replicate.

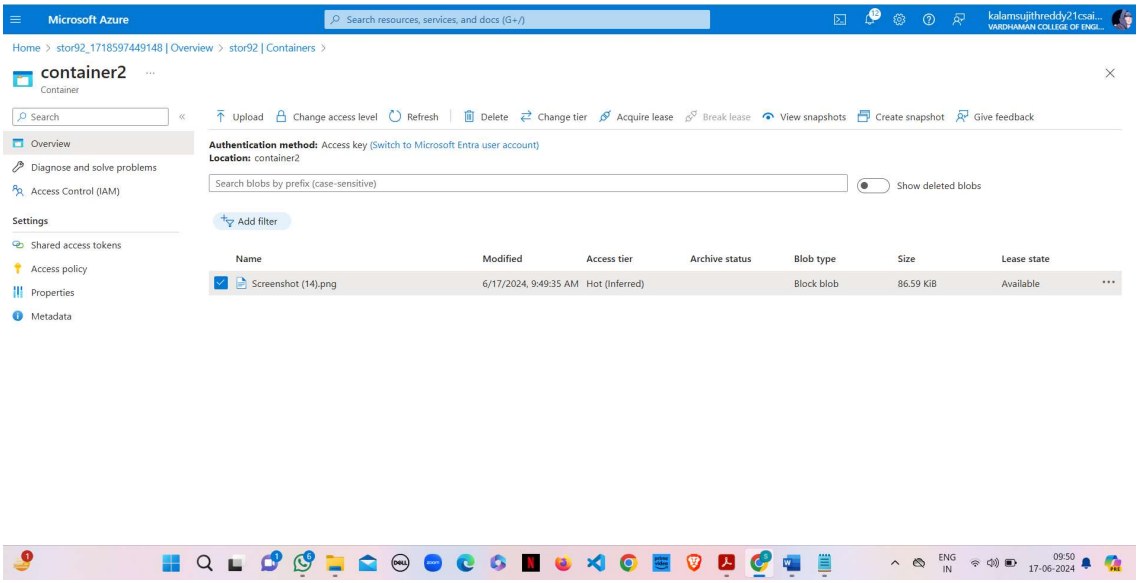


Step-6: Review the replication settings. Click `Save` or `Enable` to activate the replication policy.

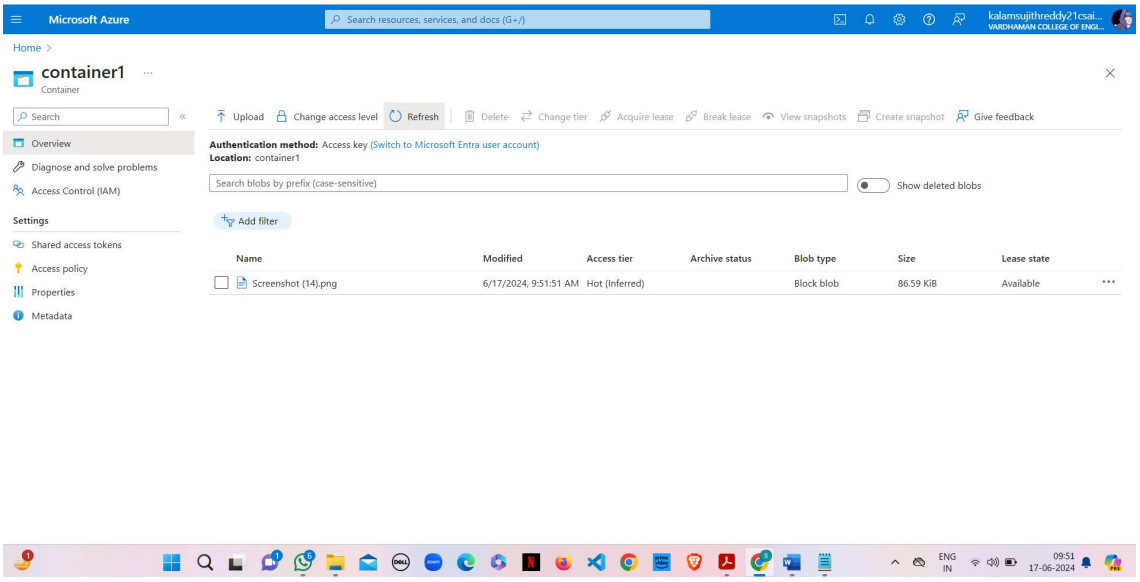


Step-7: Navigate to the source container and upload objects using the `Upload` button. Choose the files you want to upload from your local device and click `Upload`.





Step-8: After a short period, navigate to the destination container. Verify that the uploaded objects from the source container are replicated to the destination container.



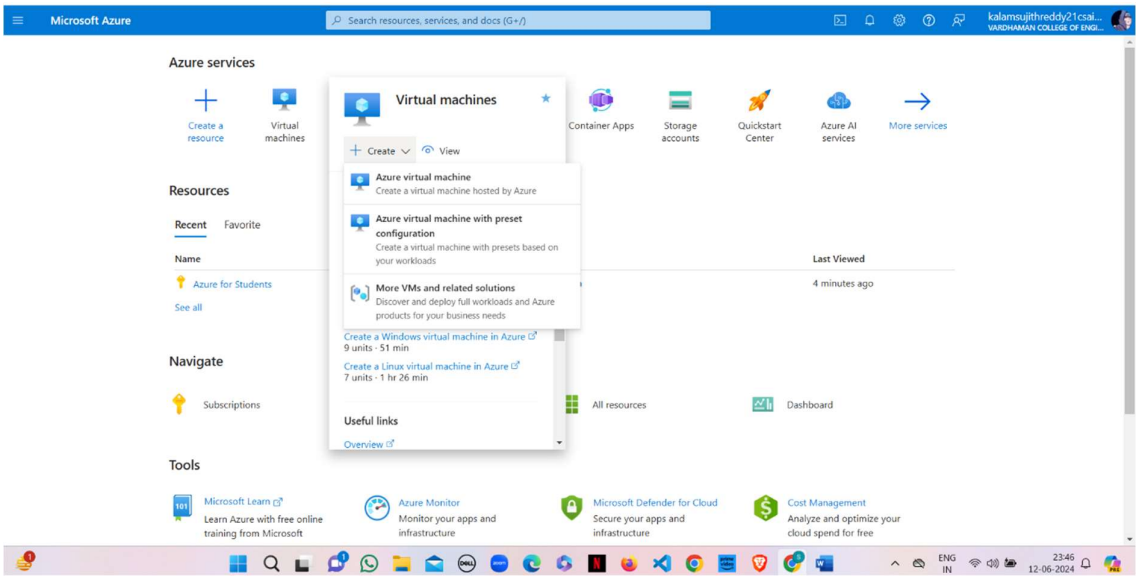
Result:

Configured object replication between two storage accounts in Azure. The replication was tested, and objects were successfully replicated across the accounts, ensuring data redundancy.

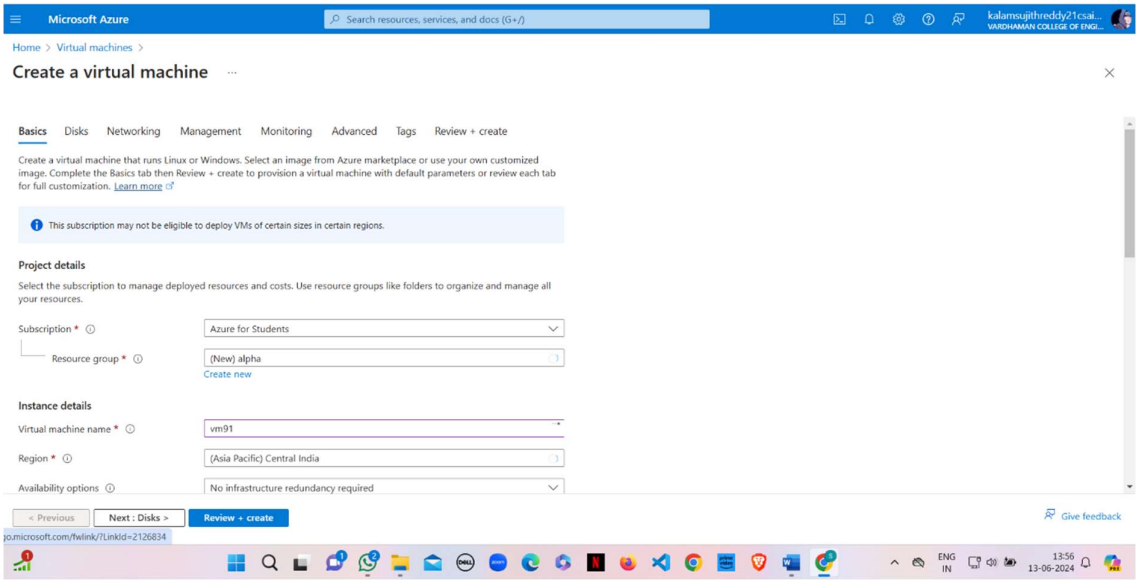
Q15) How we are adding new users, login credentials, changing owner, create authorized key files.

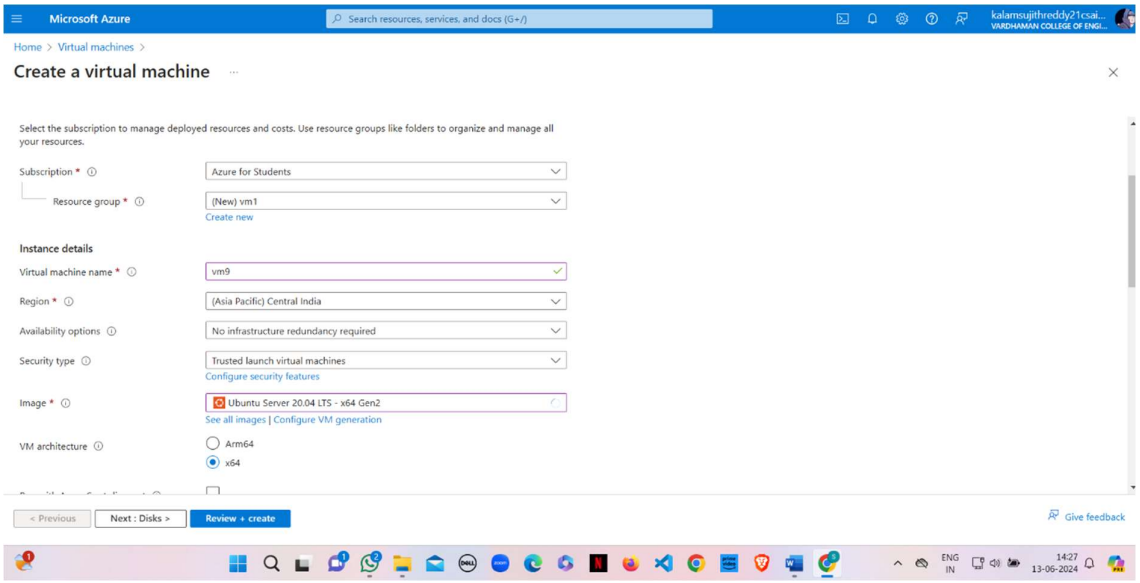
Step-1: Sign in to your Microsoft Azure account.

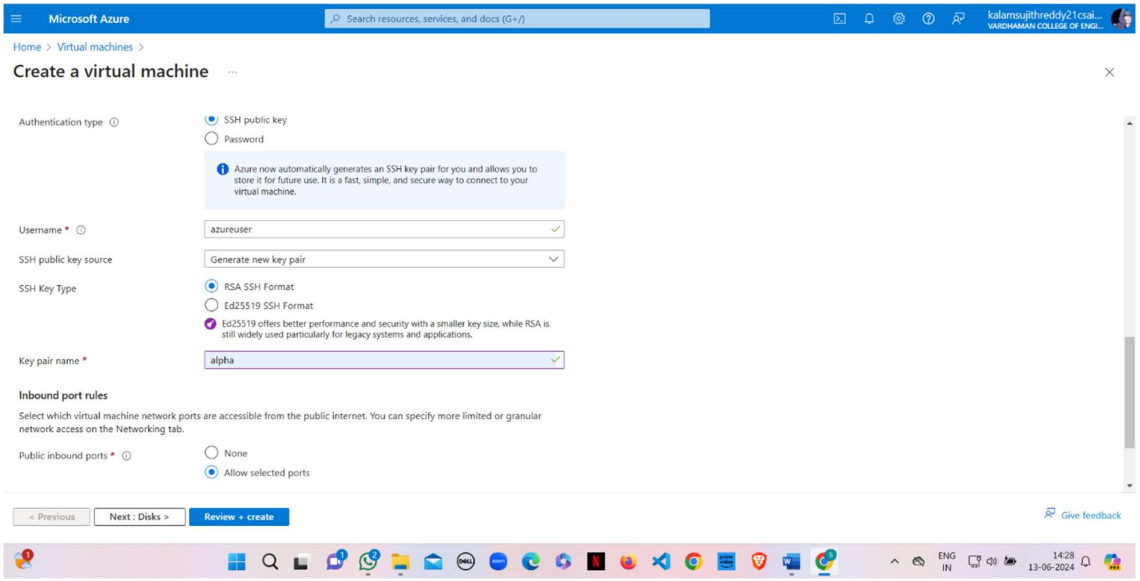
Step-2: Go To Virtual machine, and click on “Create” to create a window virtual machine.



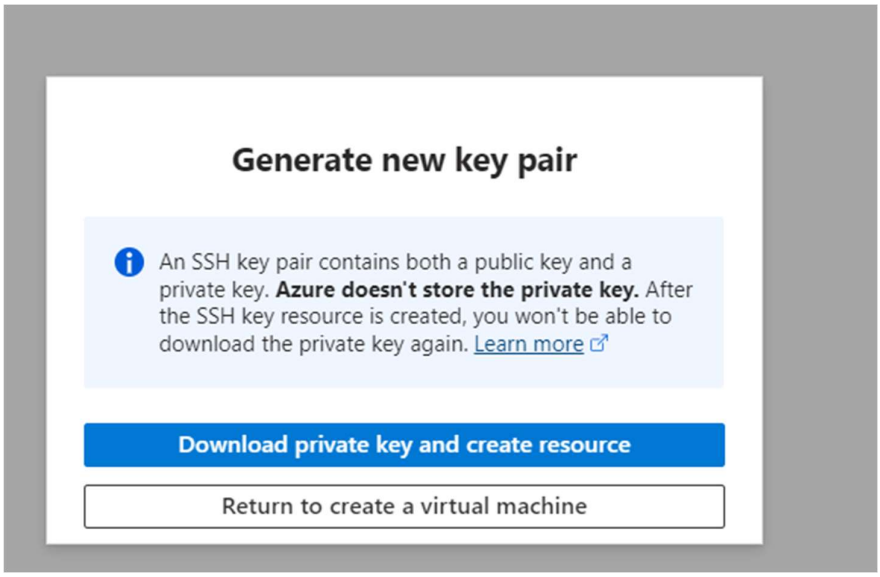
Step-3: Fill the details in that ubuntu by creating a “Resource Group”, Zone: Asia, Image: ubuntu, select “SSH”, Select the disk storage and so on. After that click on “Create + Review”. And finally click on “Create”.



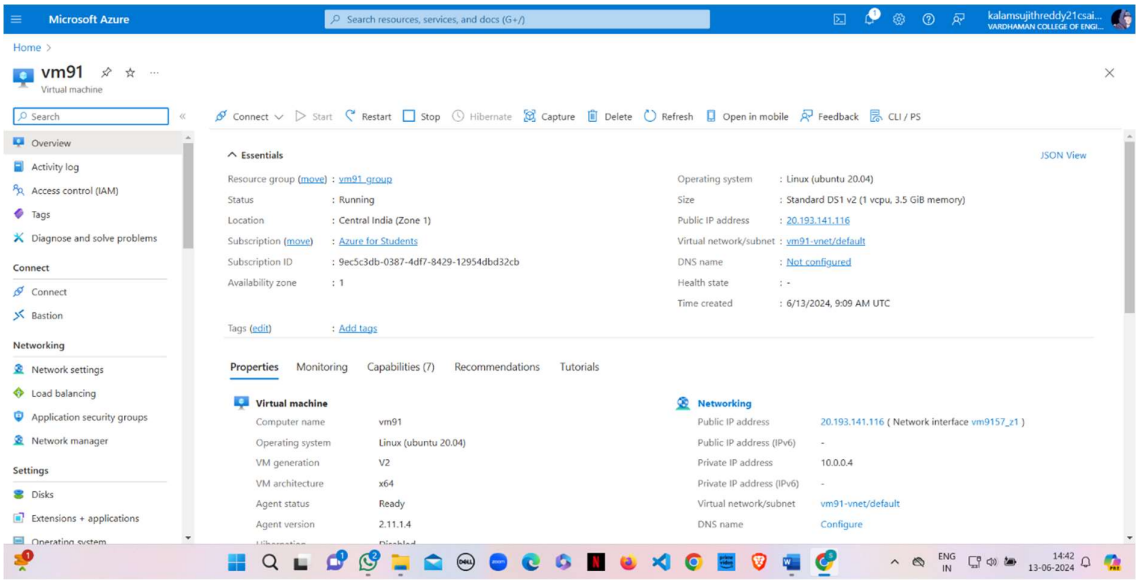




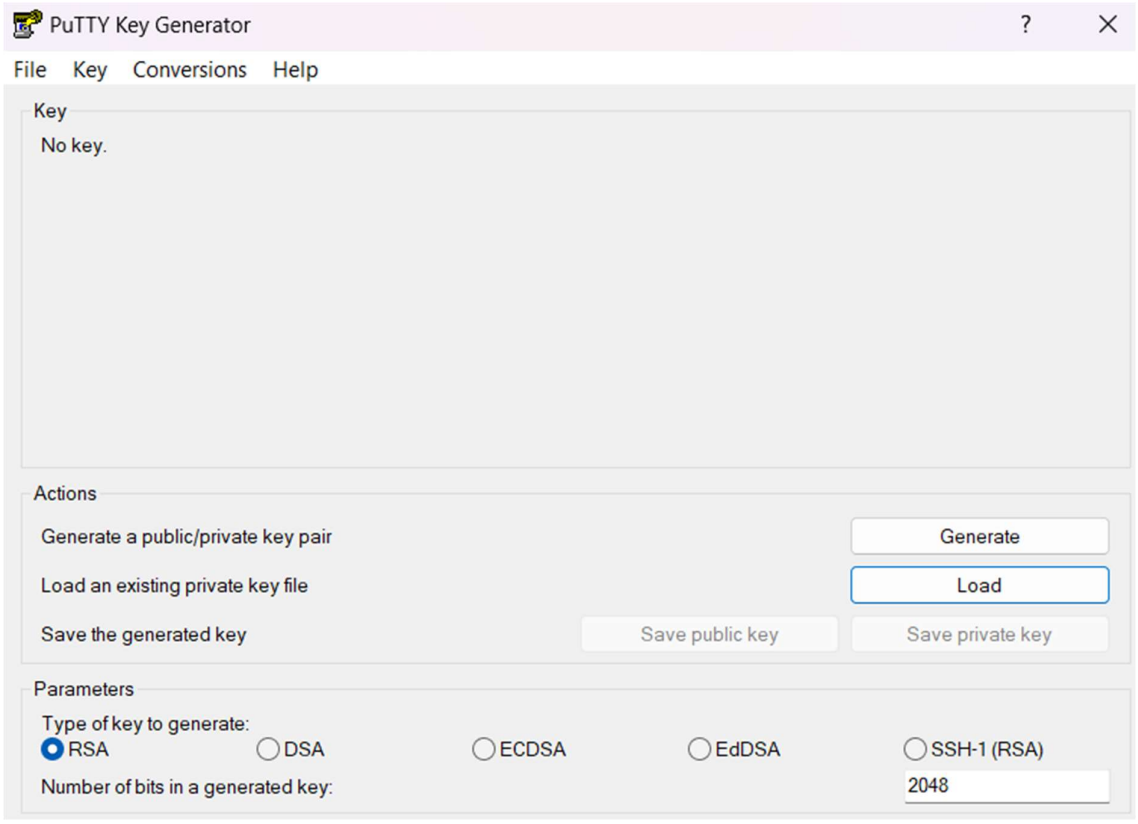
Step-4: After Deployment is over, Go to the remote desktop connection.

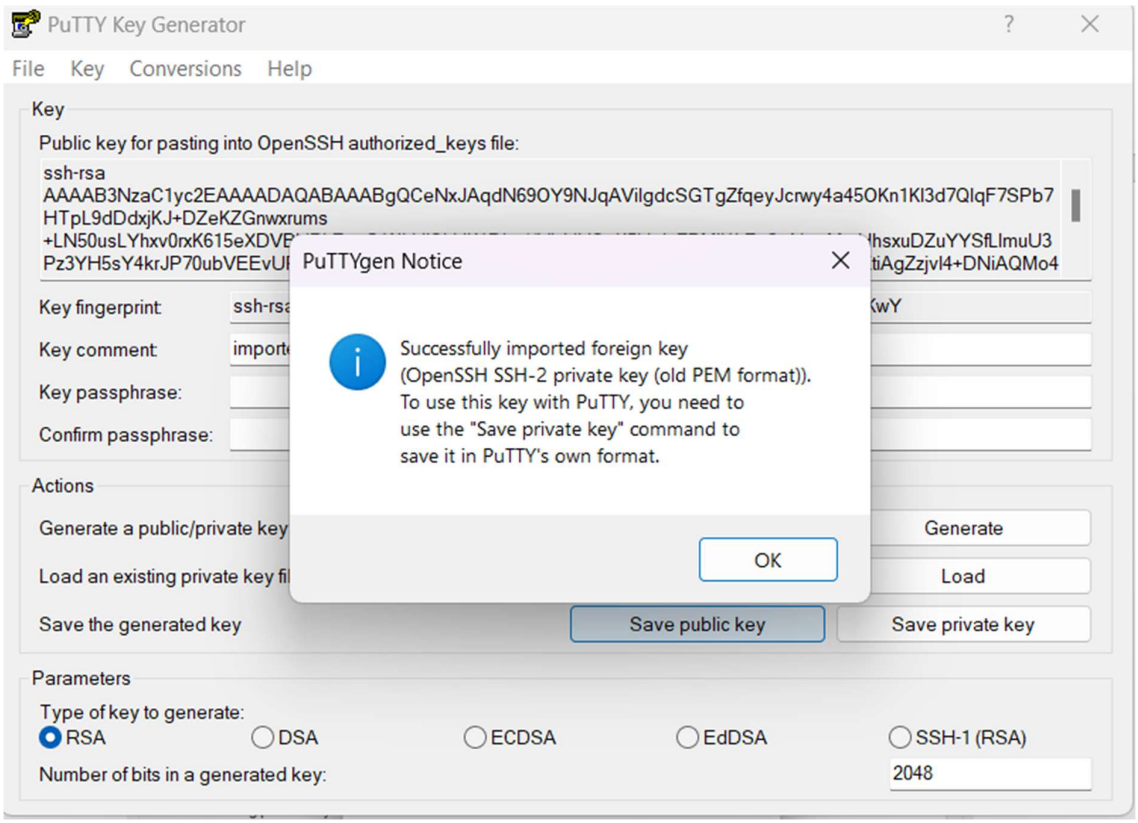


Step-5: Firstly, copy the public IP Address of that created virtual machine.

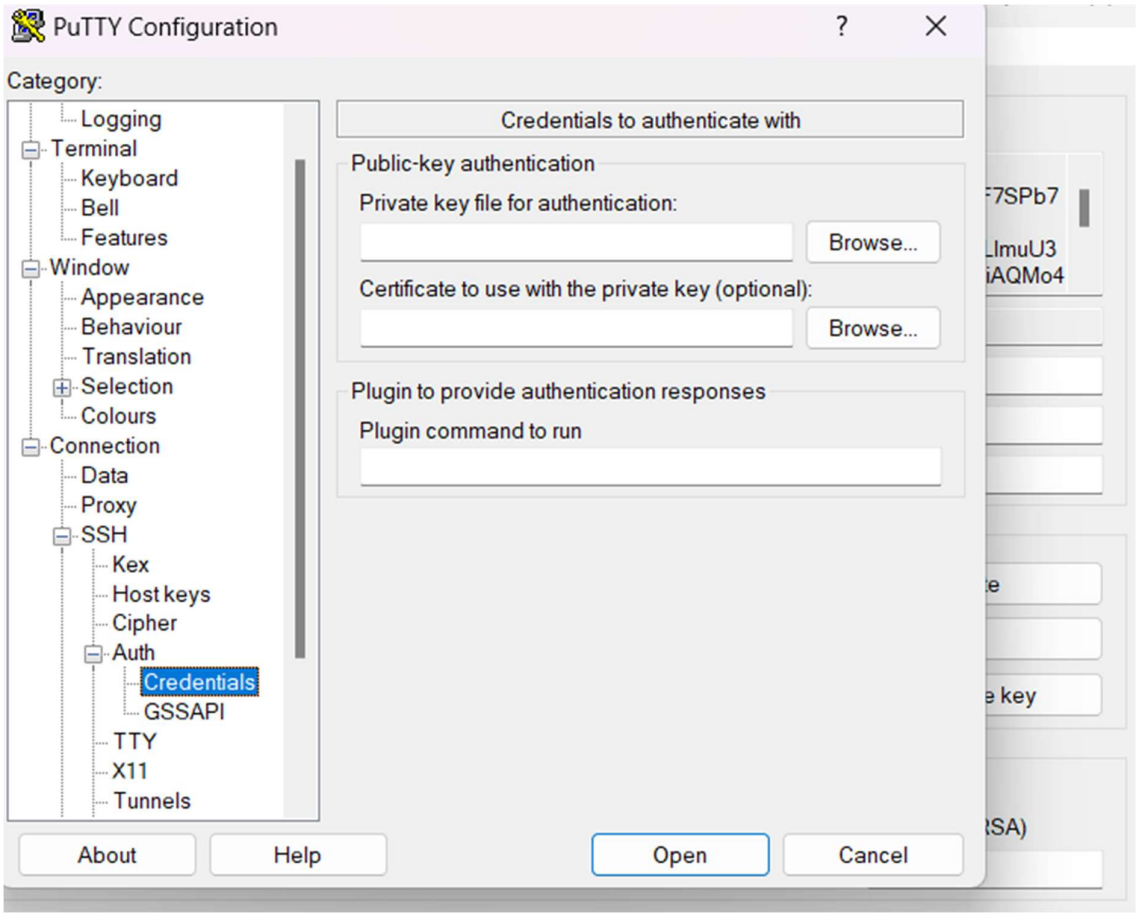


Step-6: Go to putty gen and click on load the key generator that you have downloaded.


PuTTY Key Generator
File Key Conversions Help
Key
No key.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Number of bits in a generated key:
2048


PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCeNxJAqdN69OY9NJqAVilgdcSGTgZfqeyJcrwy4a45OKn1KI3d7QIqF7SPb7
HTpL9dDdxjKJ+DZeKZGnwxrums
+LN50usLYhxv0rxK615eXDVP
Pz3YH5sY4krJP70ubVEEvUI
hsxuDZuYYSfLlmuU3
tiAgZzjvl4+DNiAQMo4
PuTTYgen Notice
Successfully imported foreign key
(OpenSSH SSH-2 private key (old PEM format)).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.
OK
Key fingerprint:
Key comment:
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key
Generate
Load an existing private key fi
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Number of bits in a generated key:
2048

Step-7: In putty, put the Copied IP Adress into it, and then go to ssh->auth->credentials and the put the generated private key.



Step-8: A login page will be opened in that type your username and you will be into the ubuntu.

Step-9: Login into your Ubuntu VM using your username and type the following commands.

To add new user in Linux server:

$sudo useradd -m Sujith

To set new password:

$sudo password Sujith

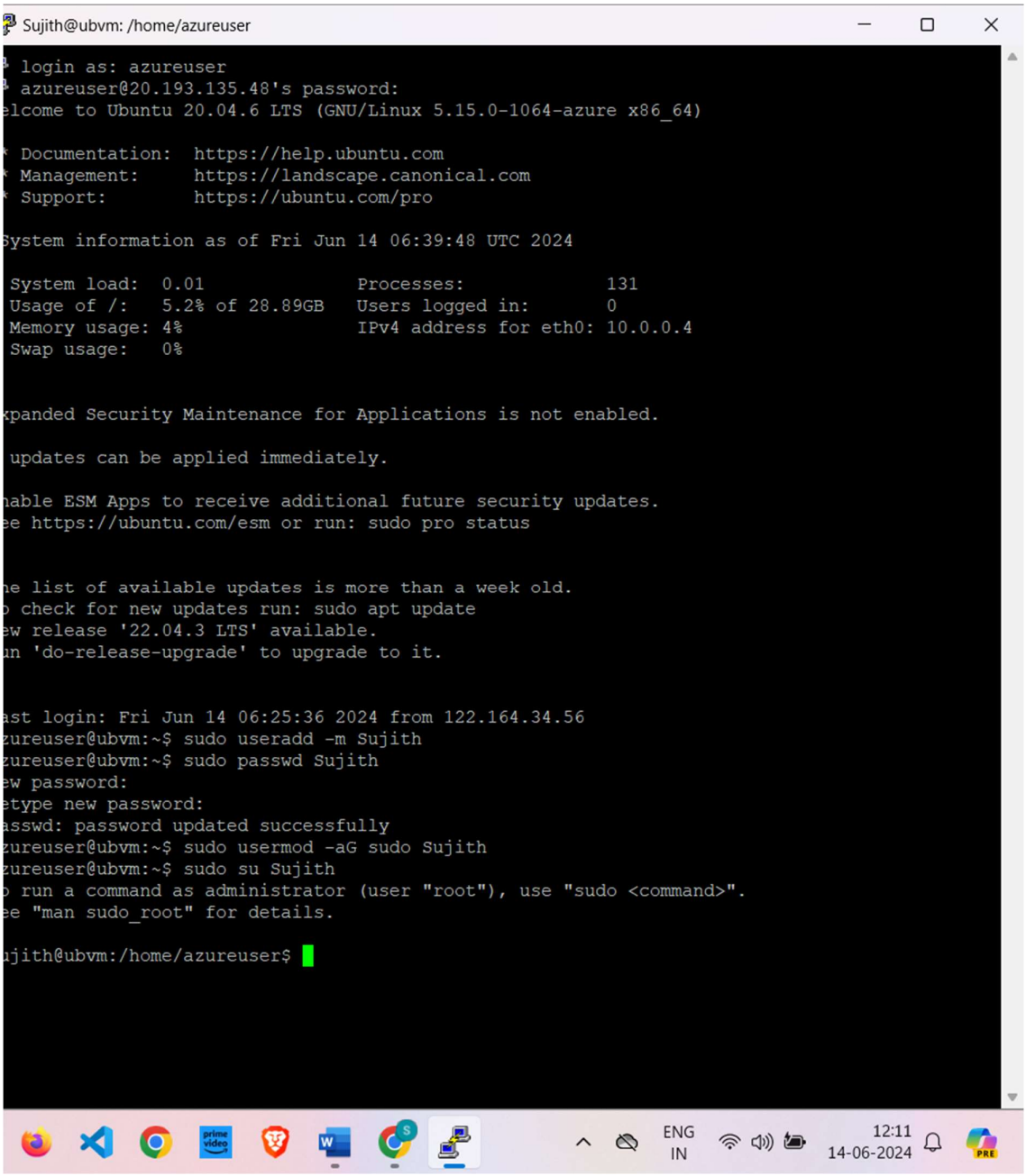
Enter new password and Retype password.

To modify login credentials:

$sudo usermod -aG sudo Sujith

To switch the user:

$sudo su Sujith



Result:

The Linux server has been setup and configured successfully. The new users were added and the credentials were updated successfully.