**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**

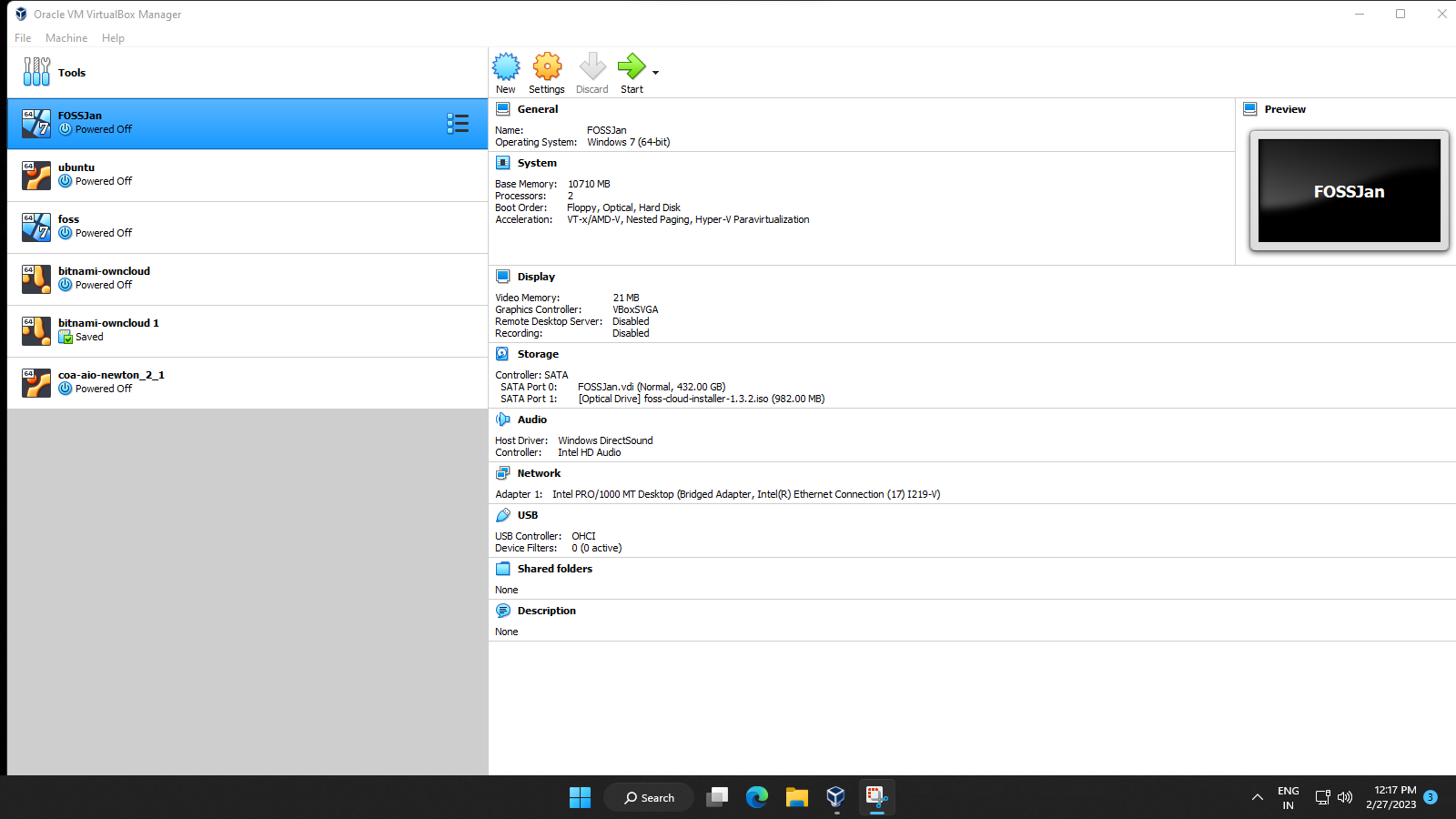
IaaS providers focus on the organization's core business rather than on IT infrastructure.

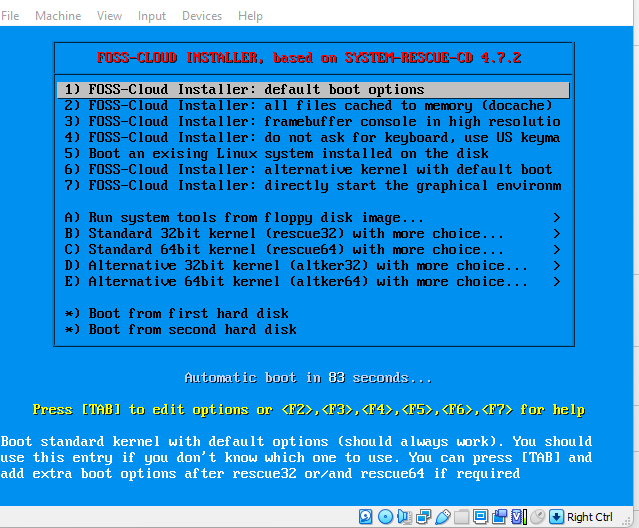
**5. On-demand scalability**

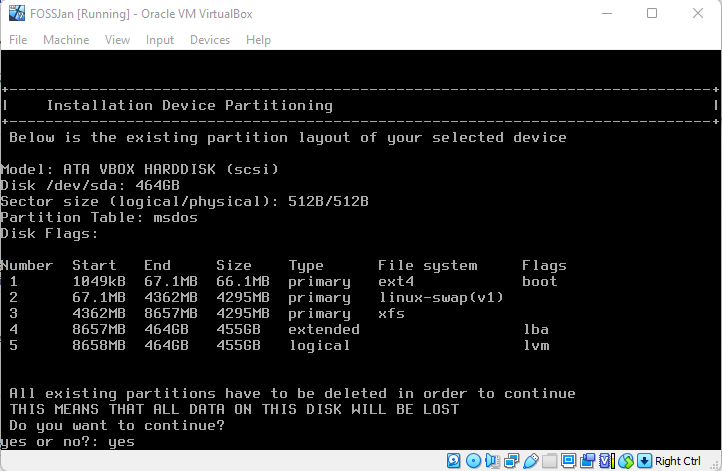
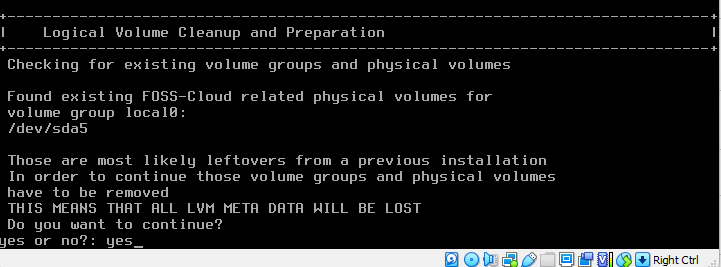
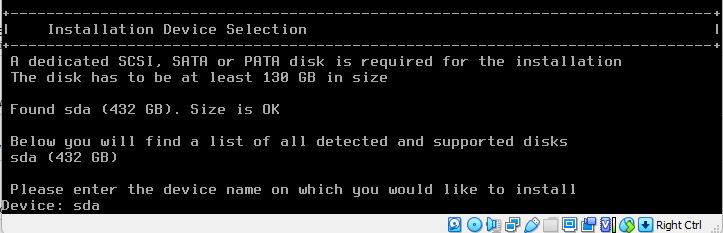
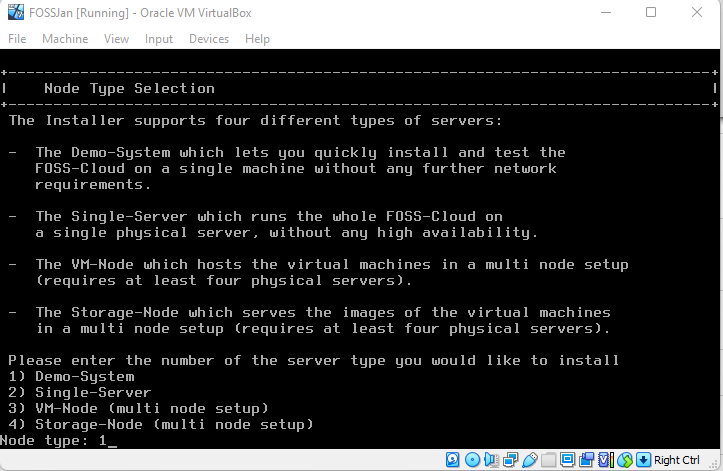
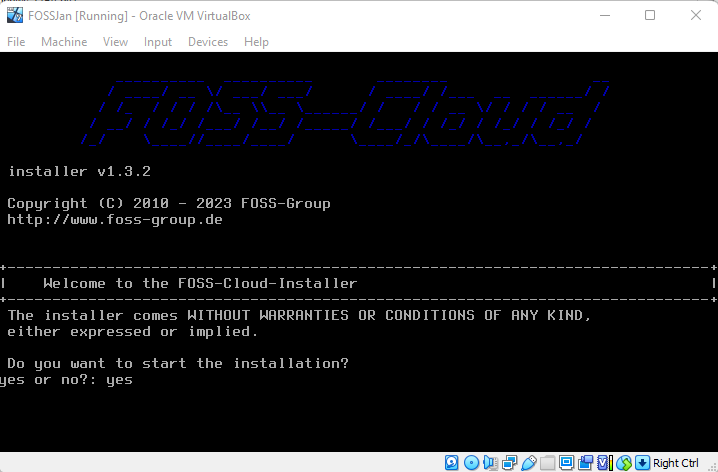
On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

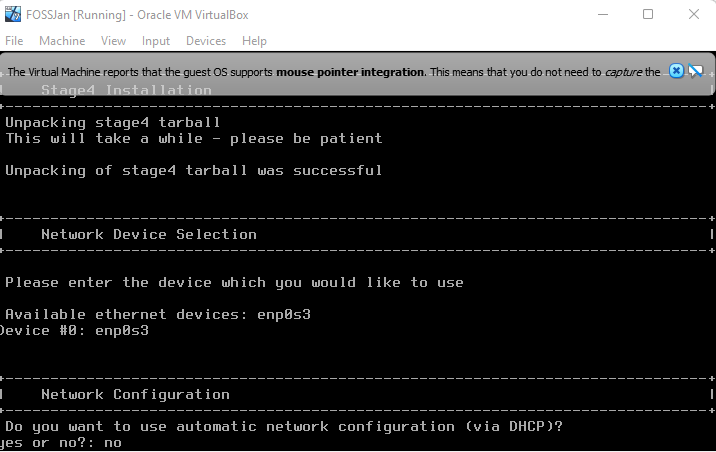
**Methods and Steps:**

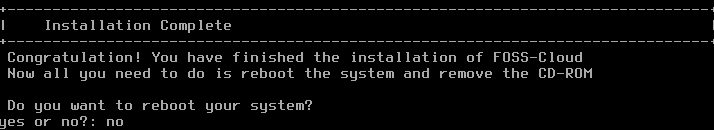
1. Using FOSS Demo / FOSS Server.

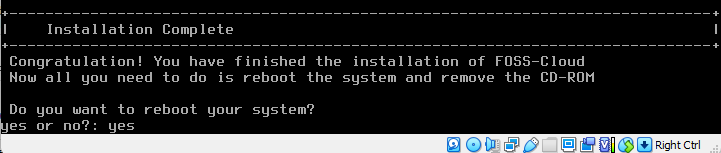
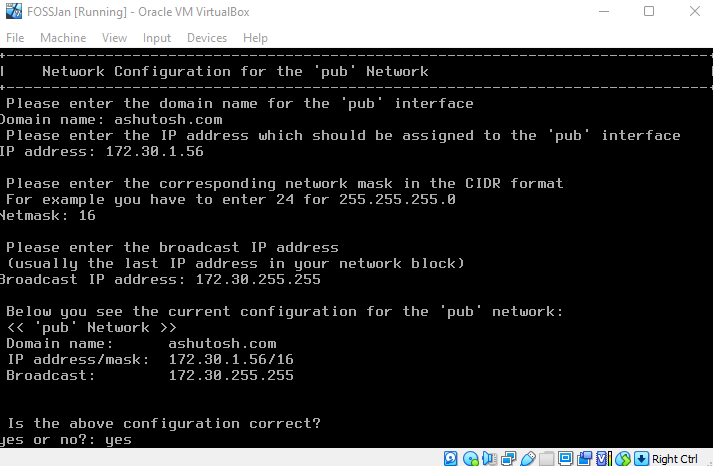
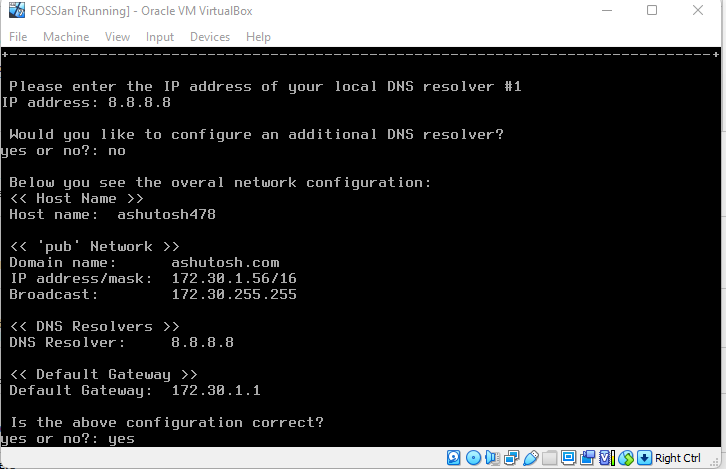
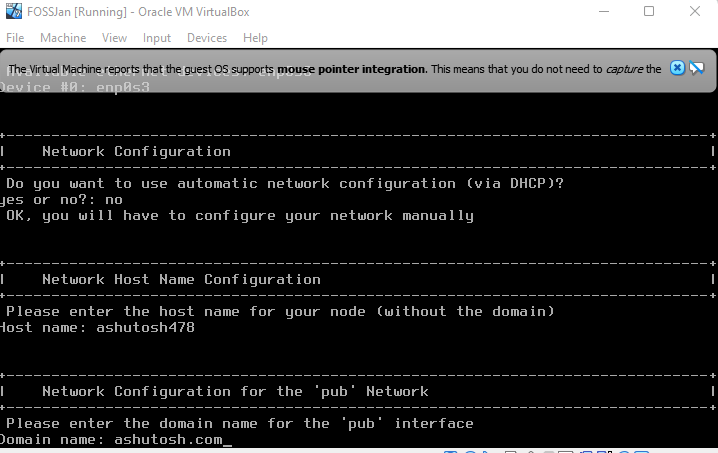
INSTALLATION:  








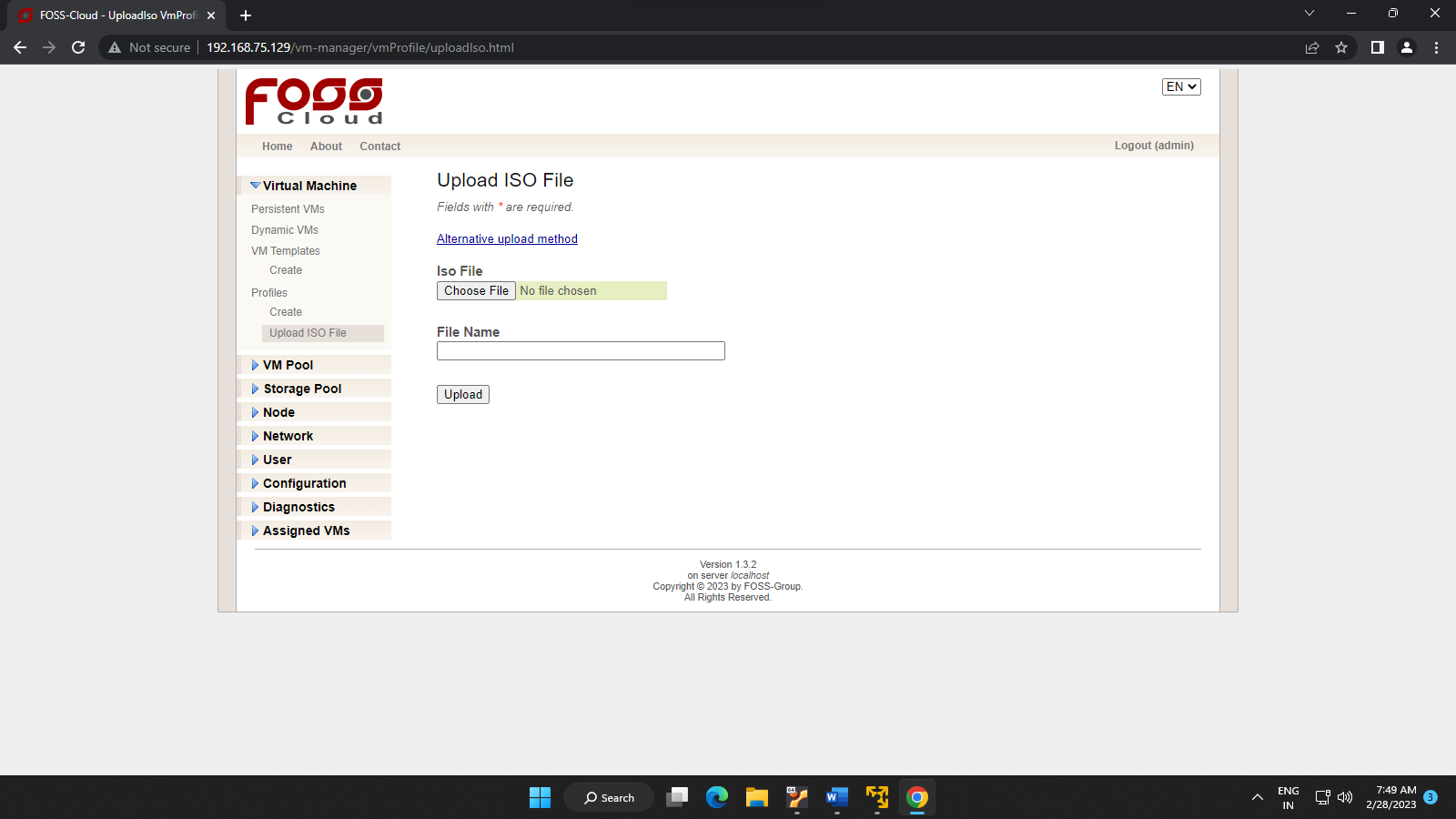




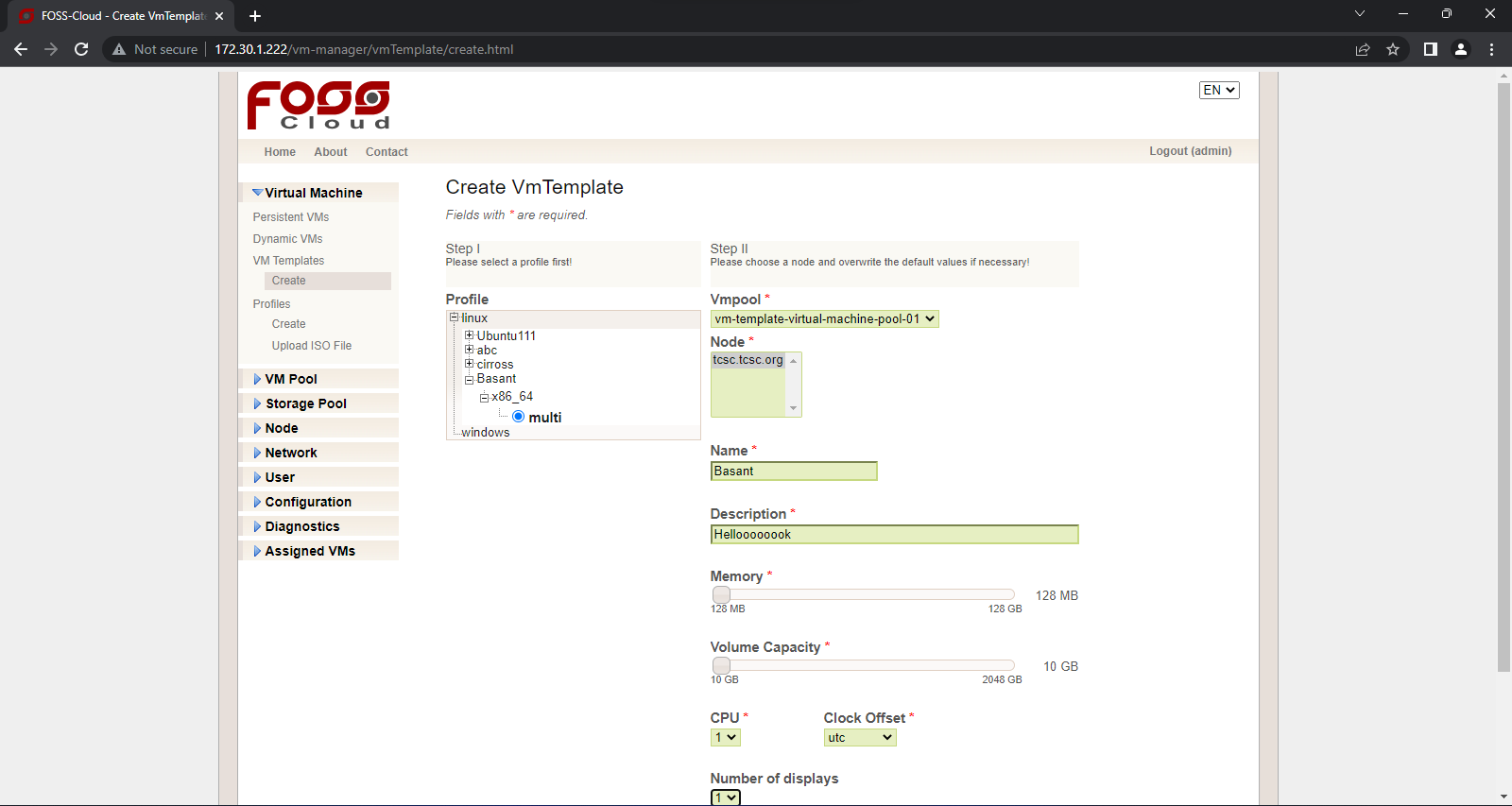
**Step 1:**After installation, it will show you  an IP Address. Put it in your browser to access your administrator page. The default user credentials are user: admin and password: admin. For root login – username- root and password – password.

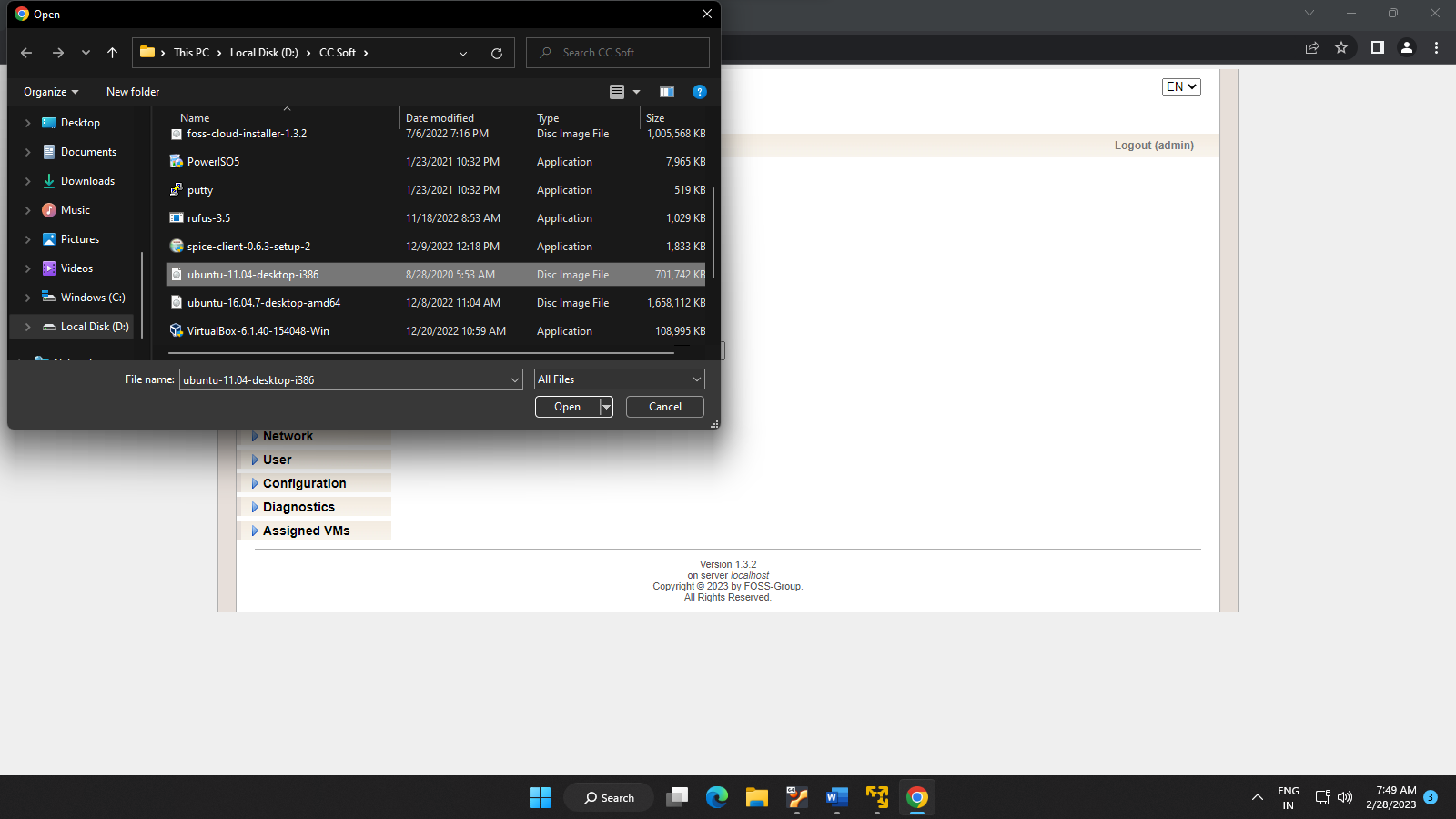
\

**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.

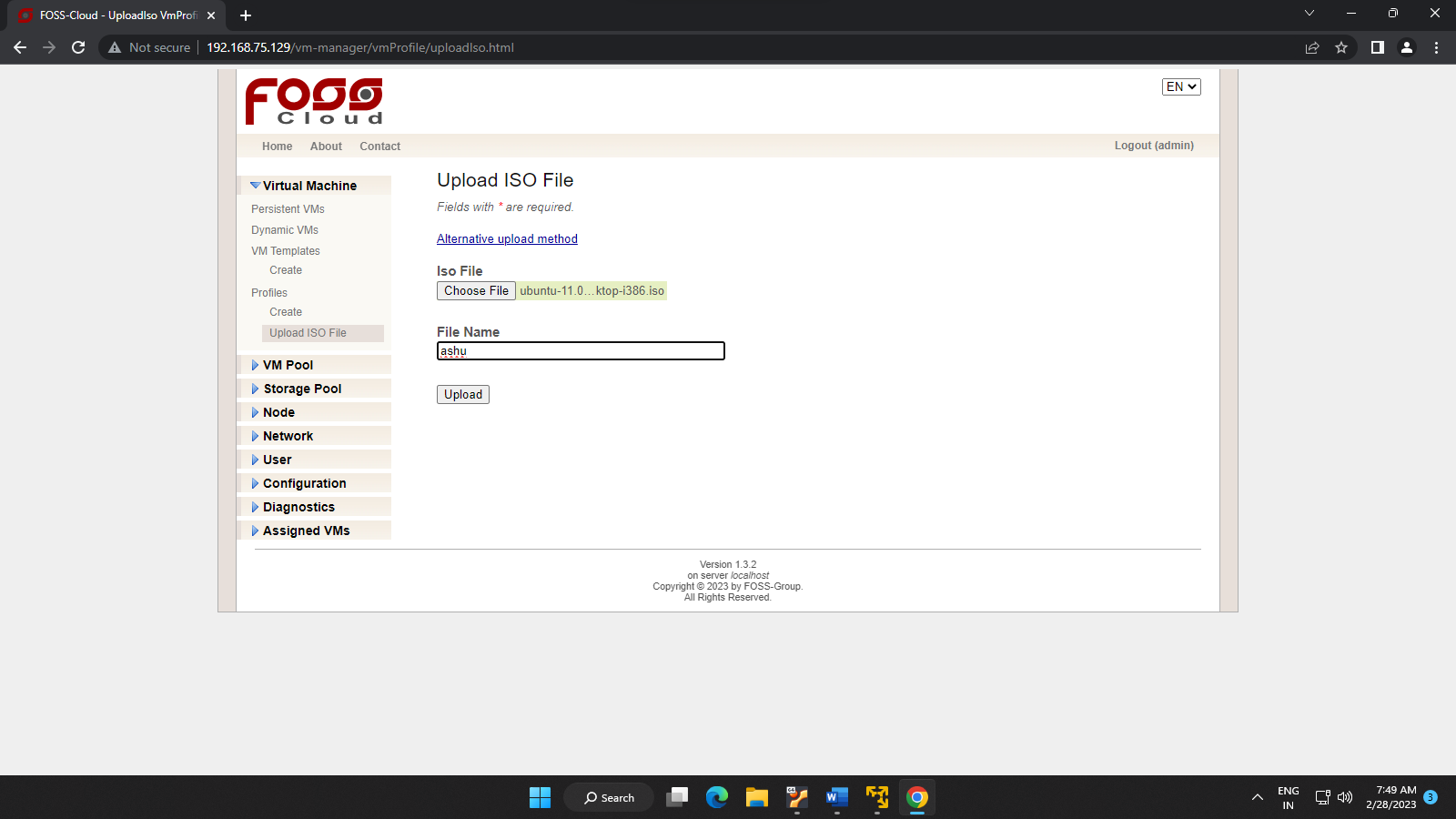


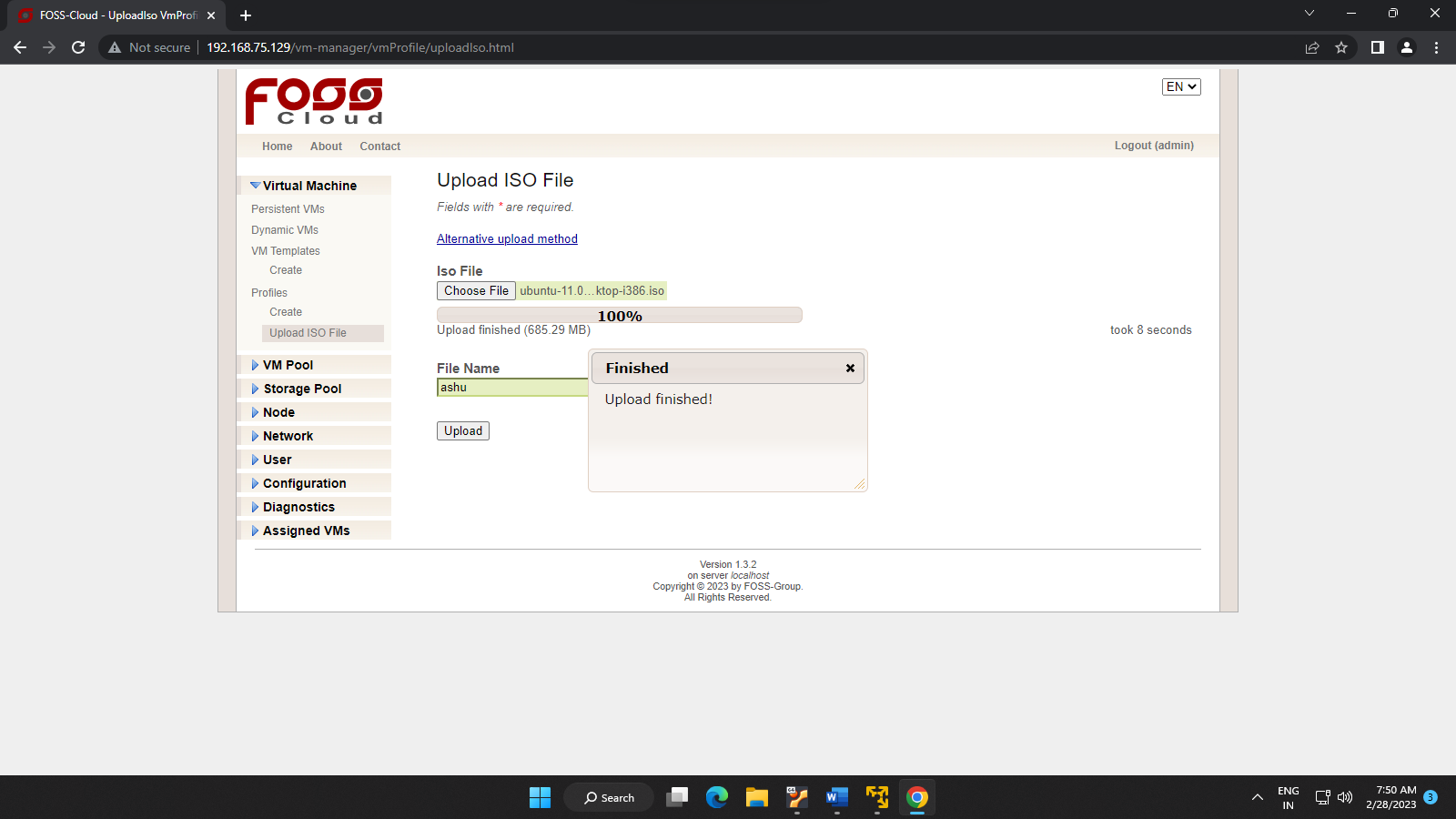
**Step 3:**Once you uploaded the file, create VmTemplate. In this option you are basically configuring your virtual machine’s storage location, CPU, Memory, Node etc. Here, you will find single nodes and VM pool in respective options because everything  was installed at the single server.

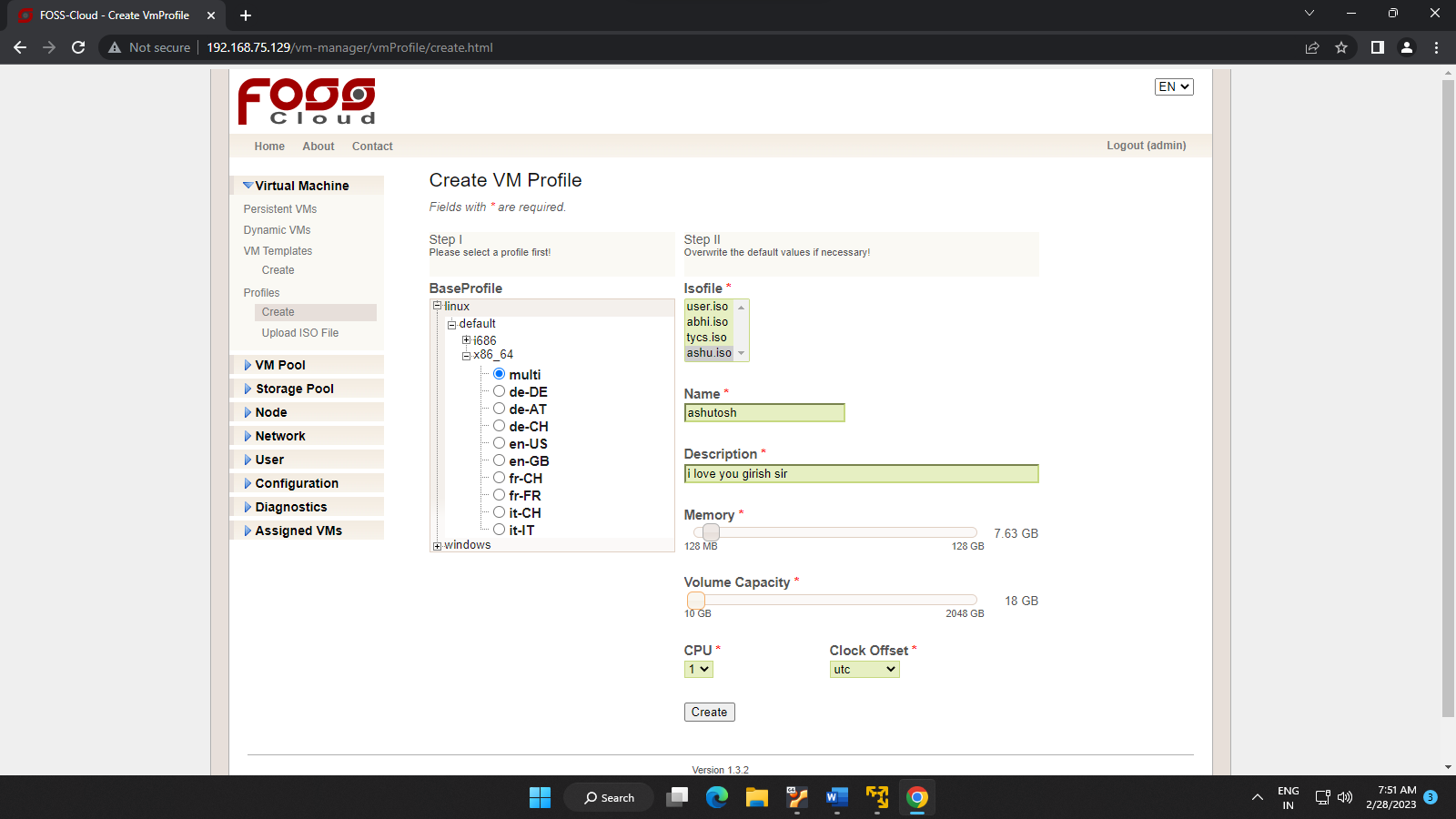


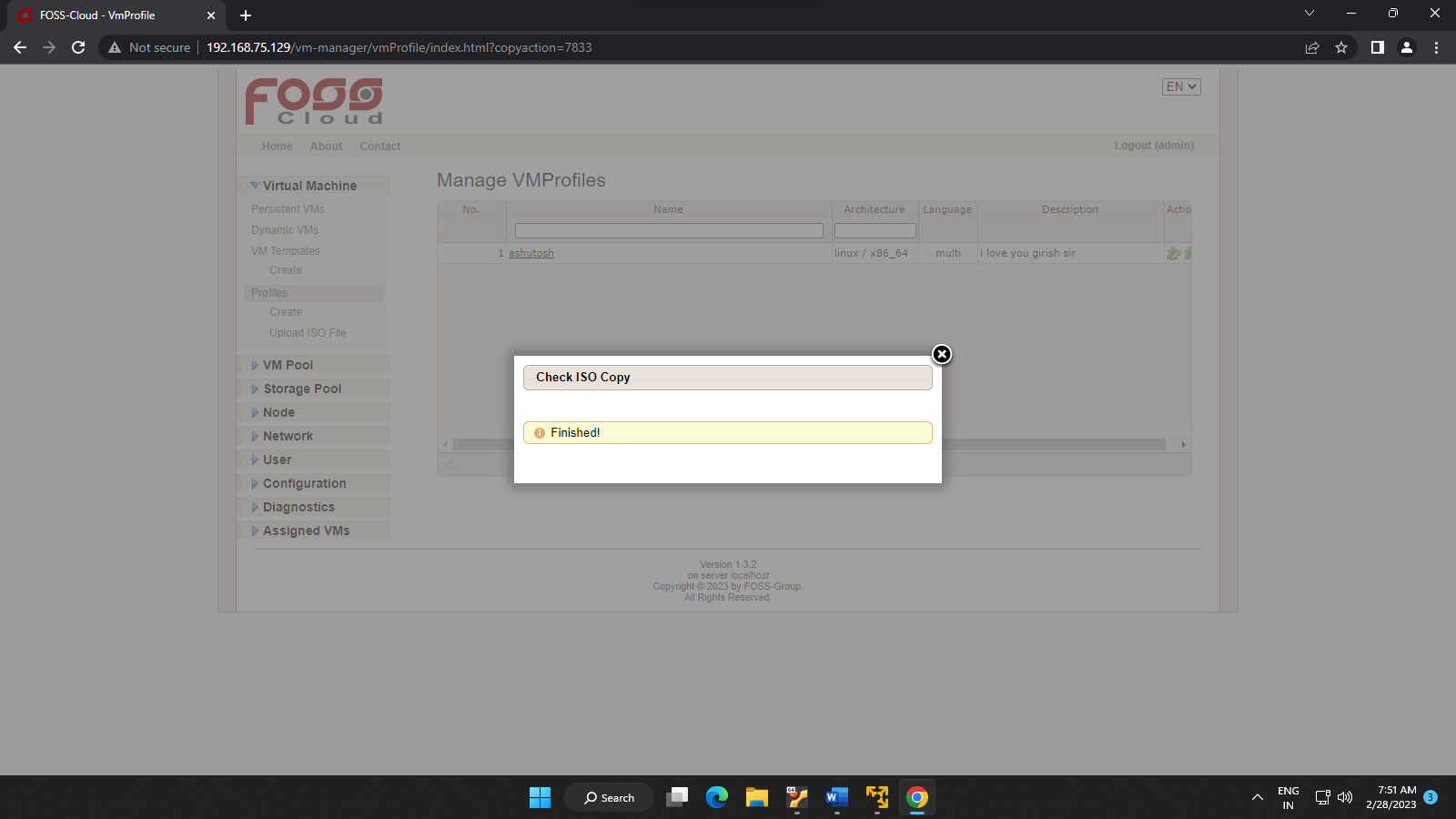


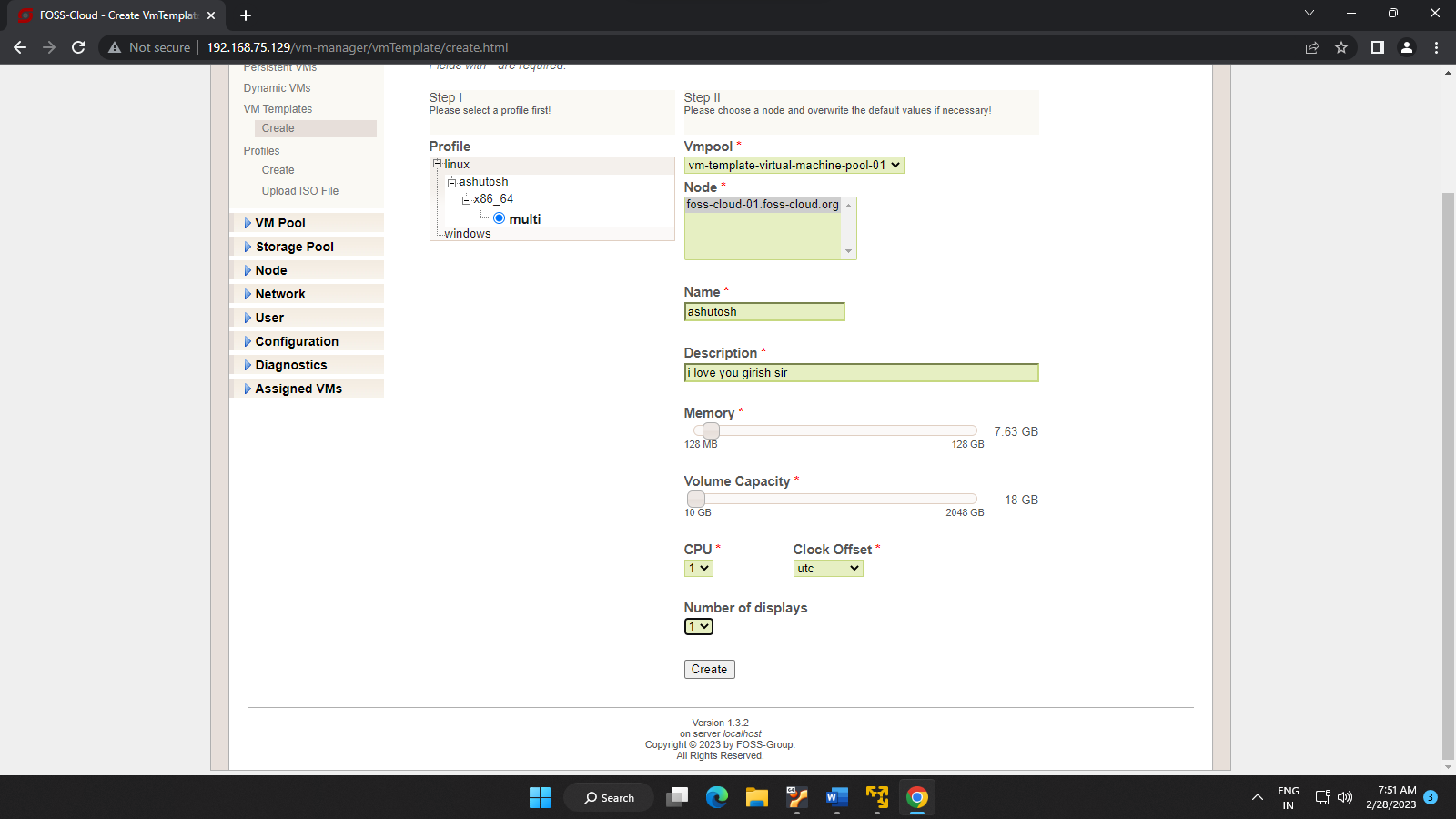
**Step 4:**Now, click on VMTemplates  and you will see a template which you have created in step 4. To start your machine go to Run action Tab and click on the green arrow. Under status tab, it shows the running text with the green circle which shows that your machine is running without any errors. To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

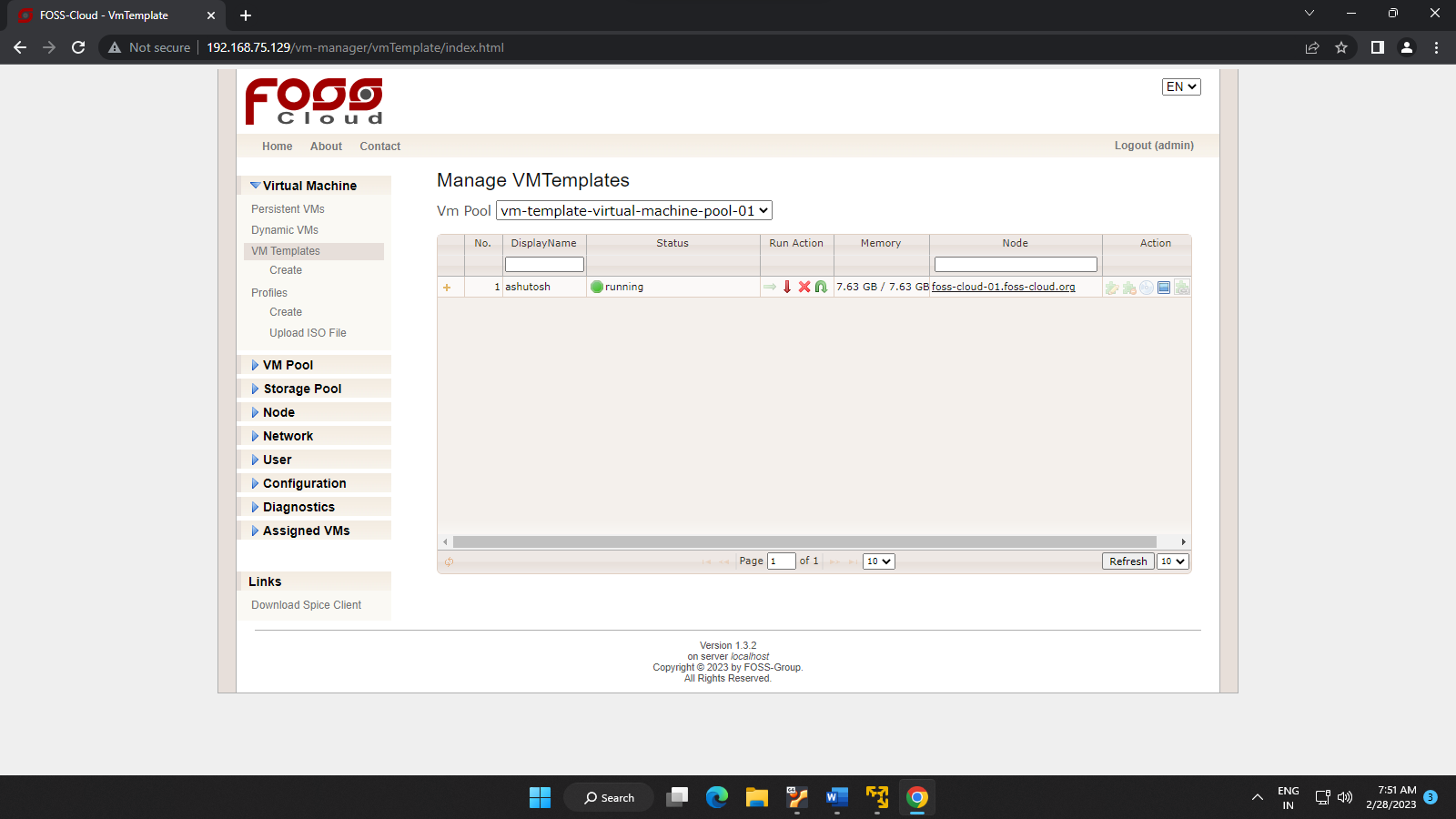


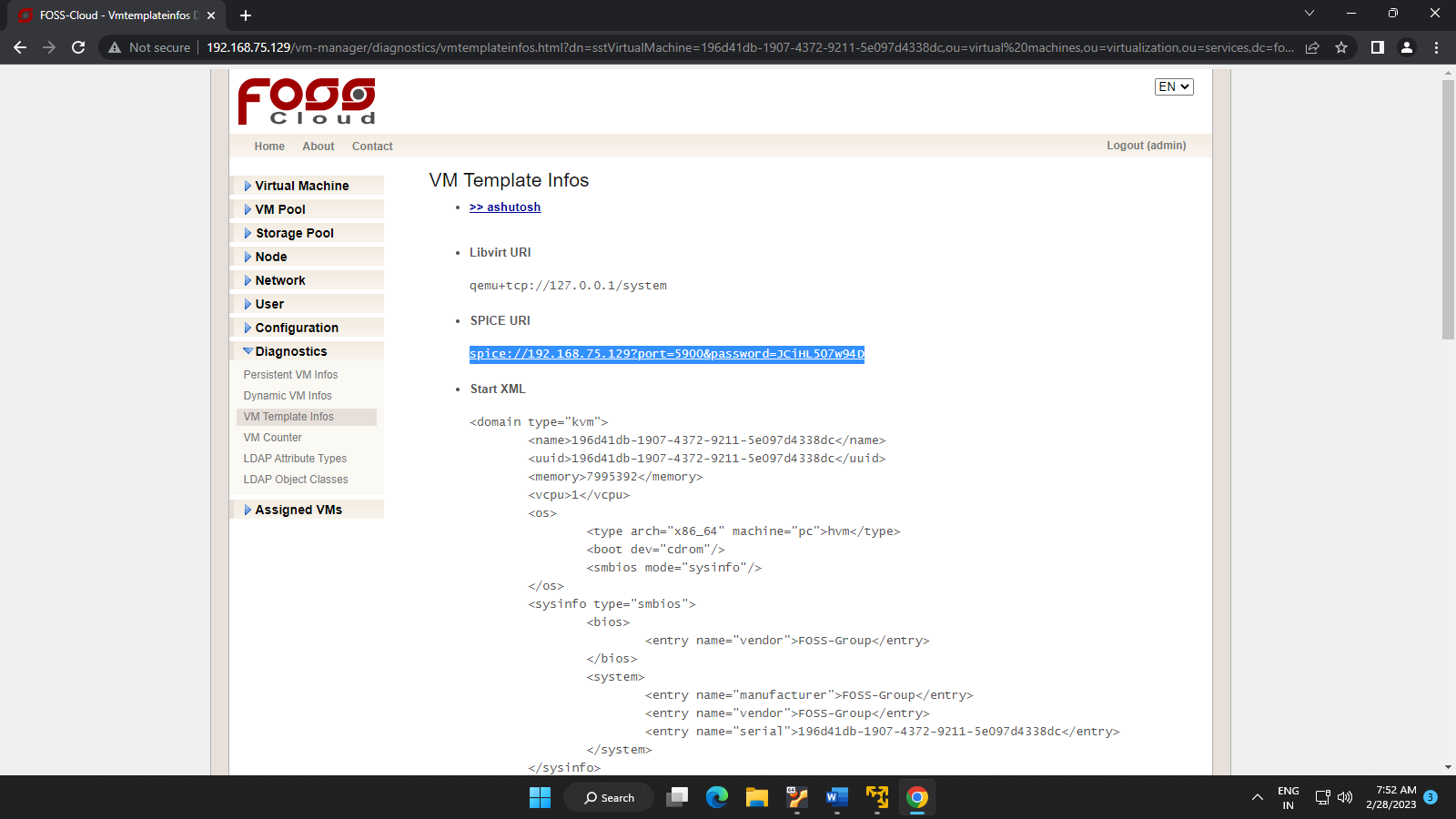


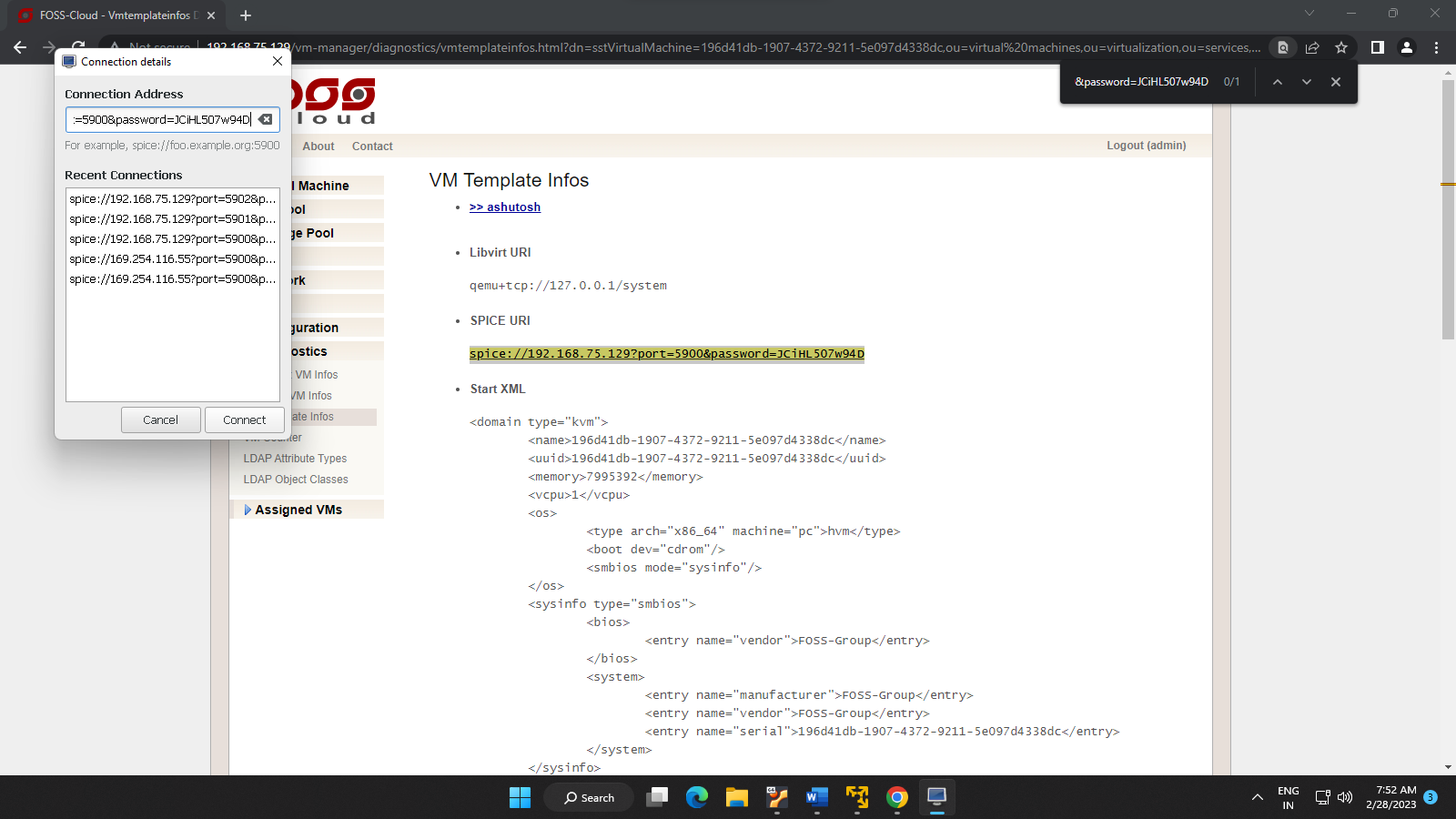


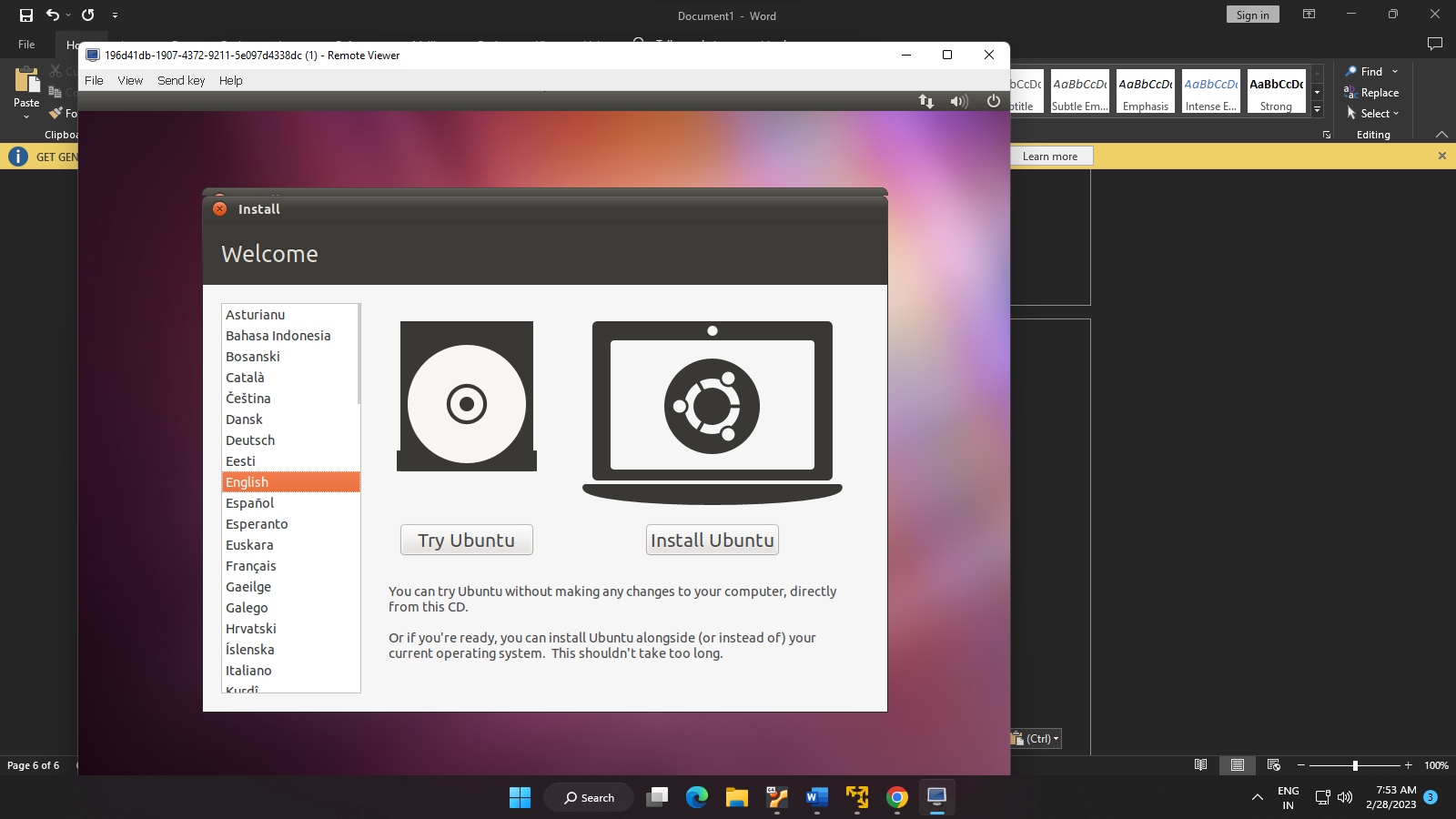




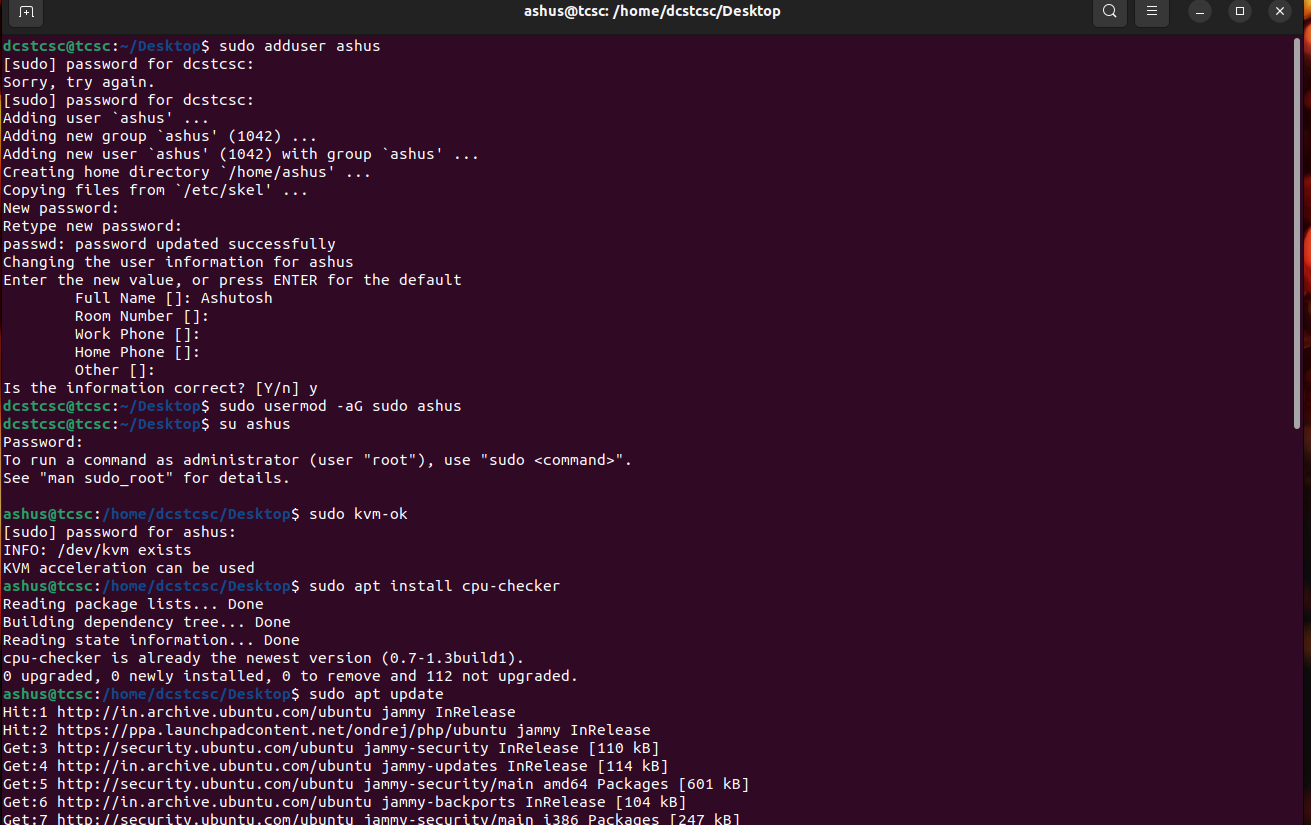


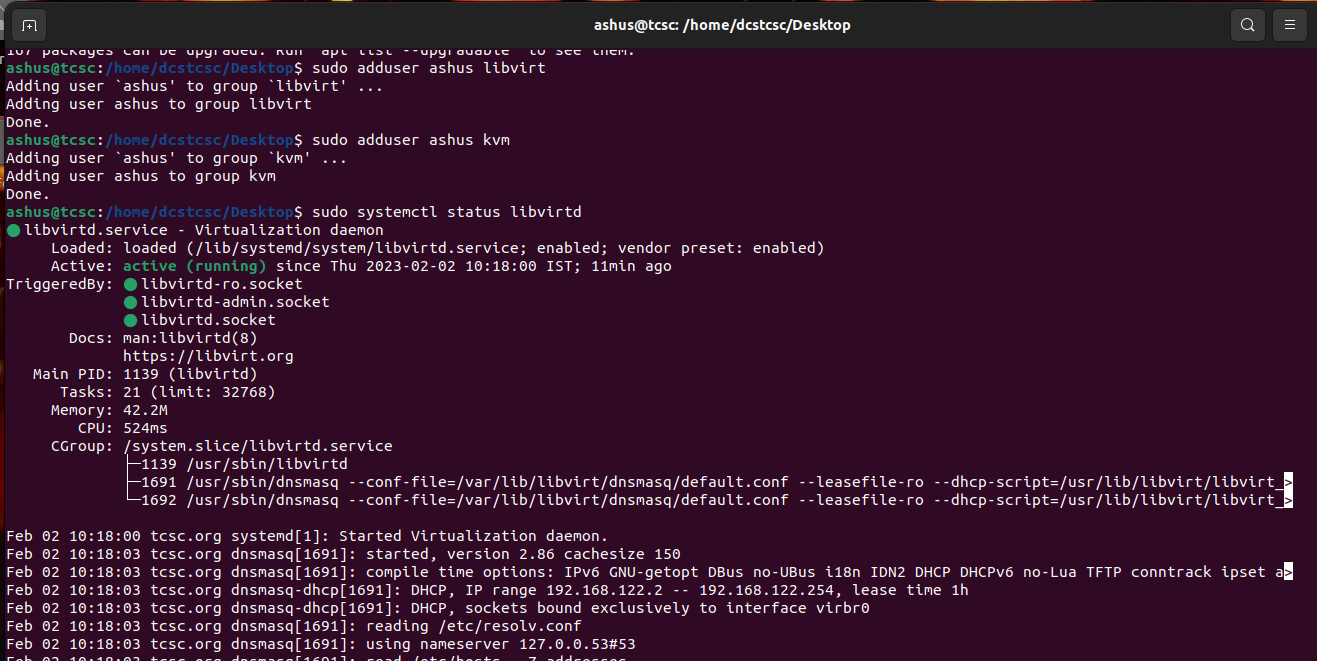


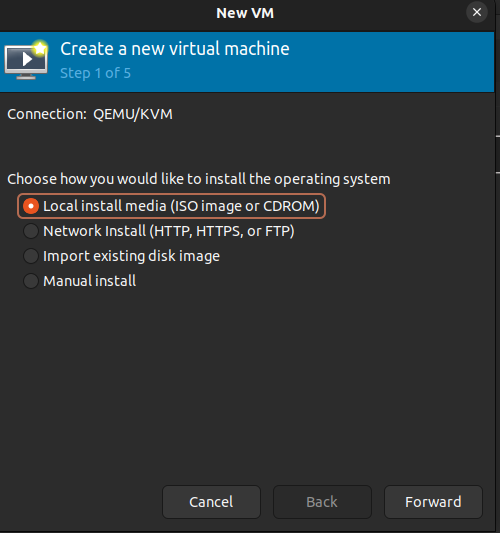


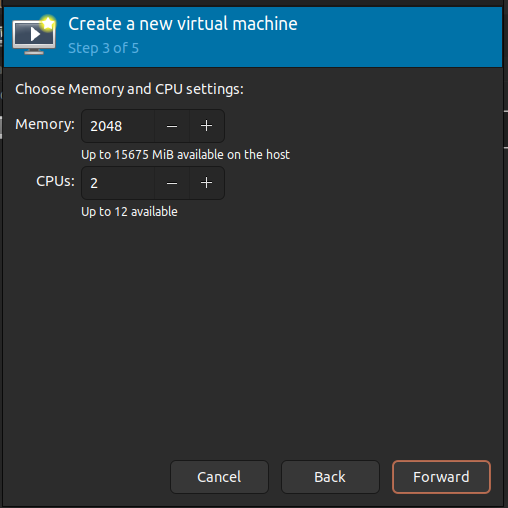
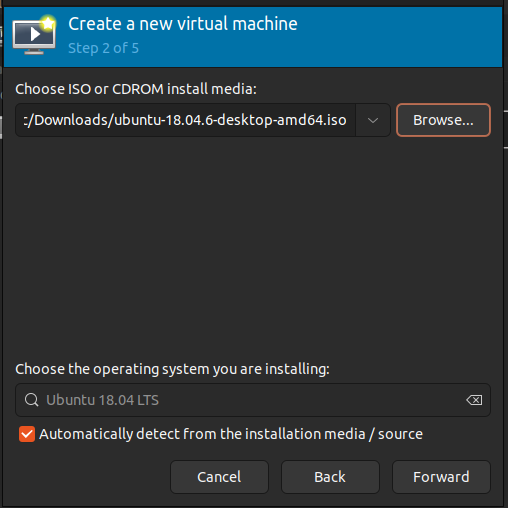


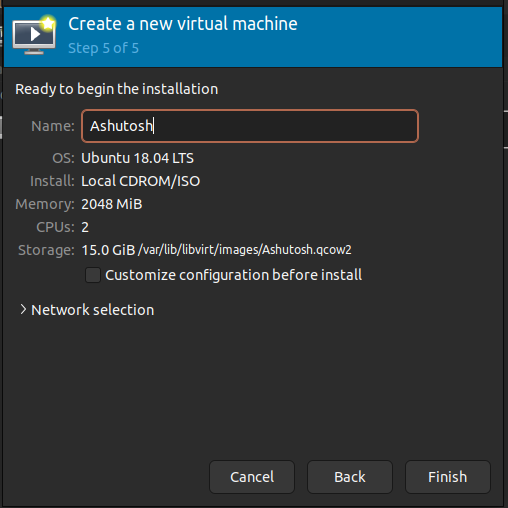
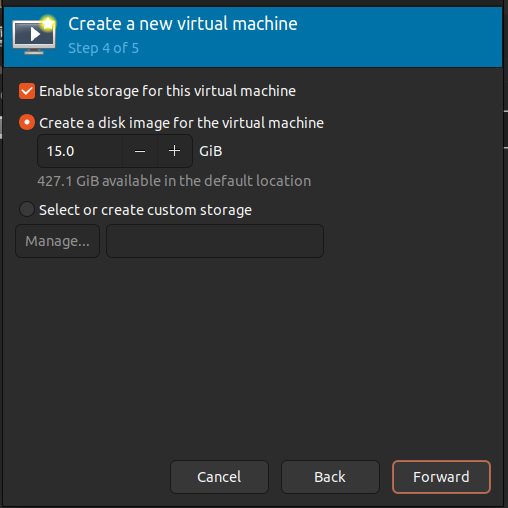
B. USING Ubuntu and KVM

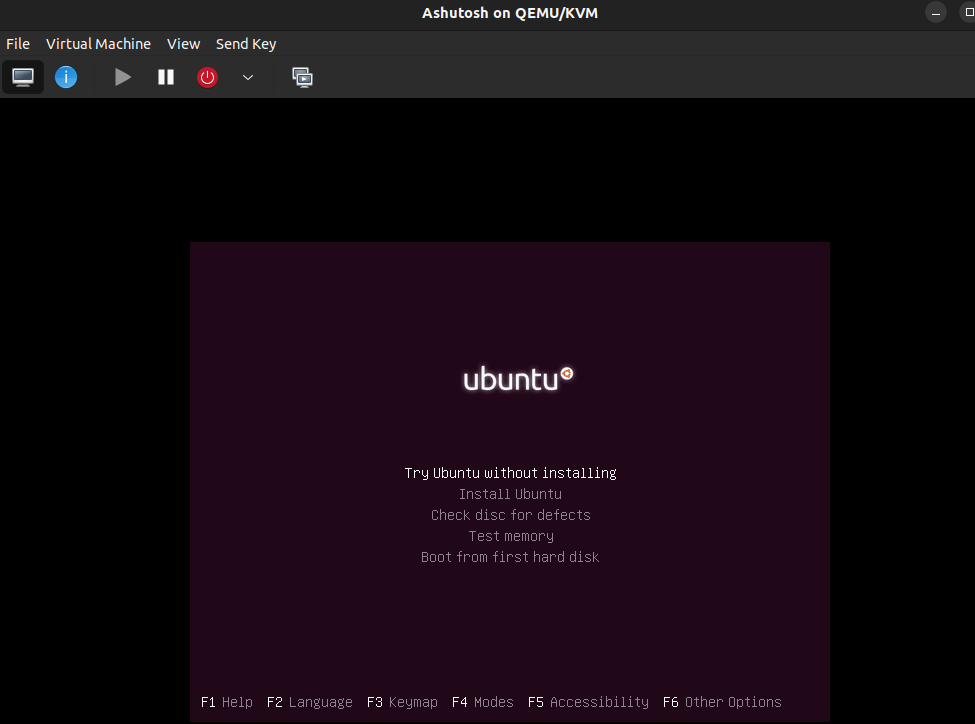
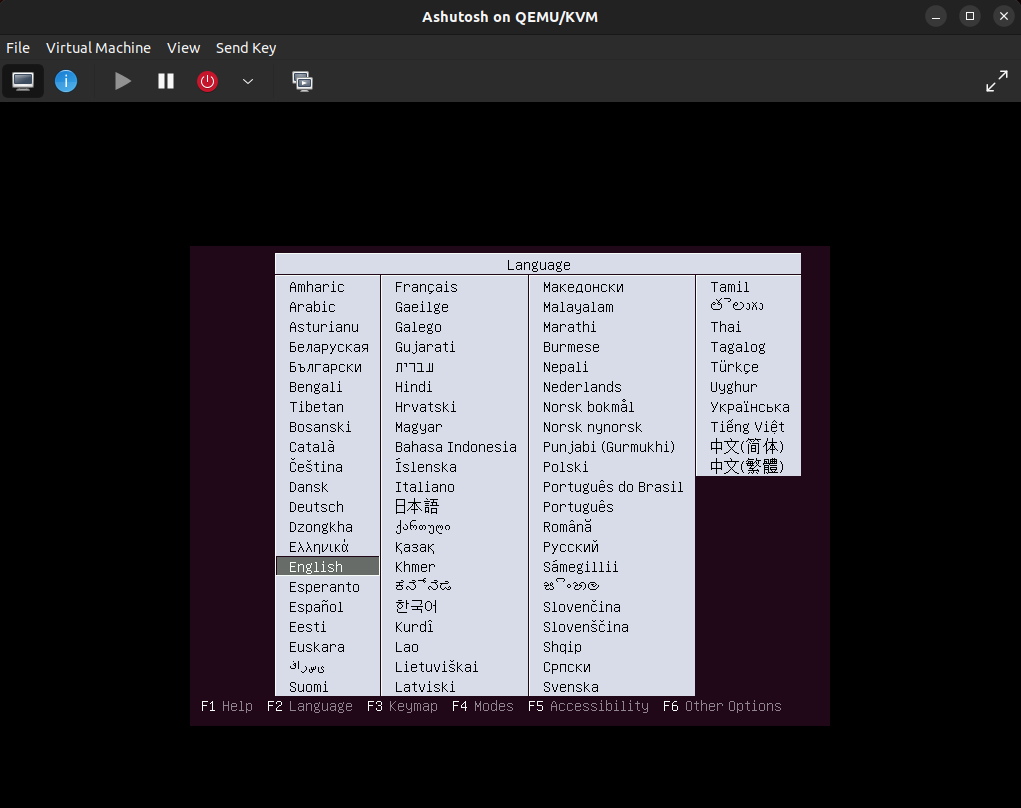


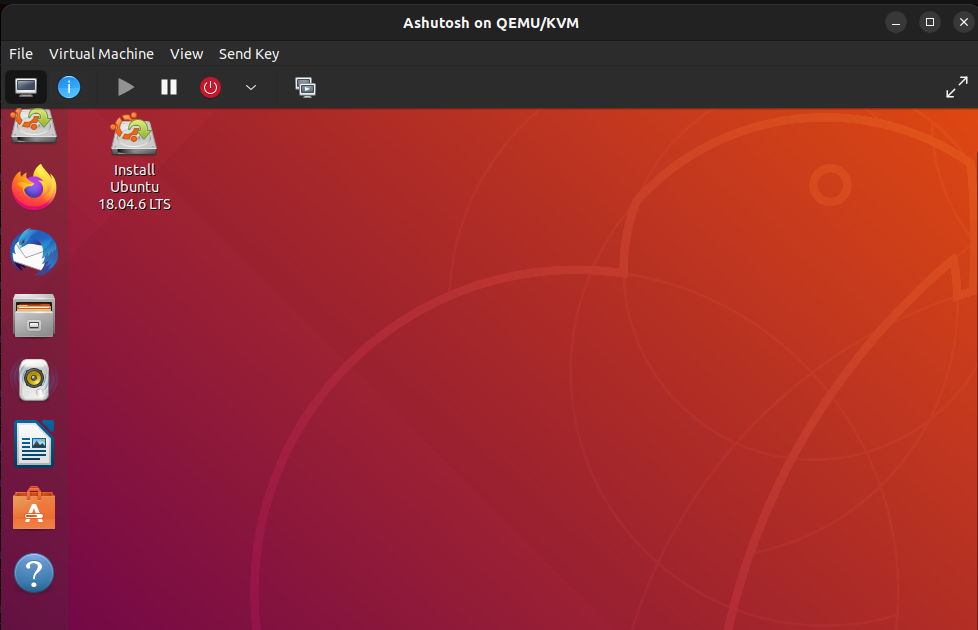






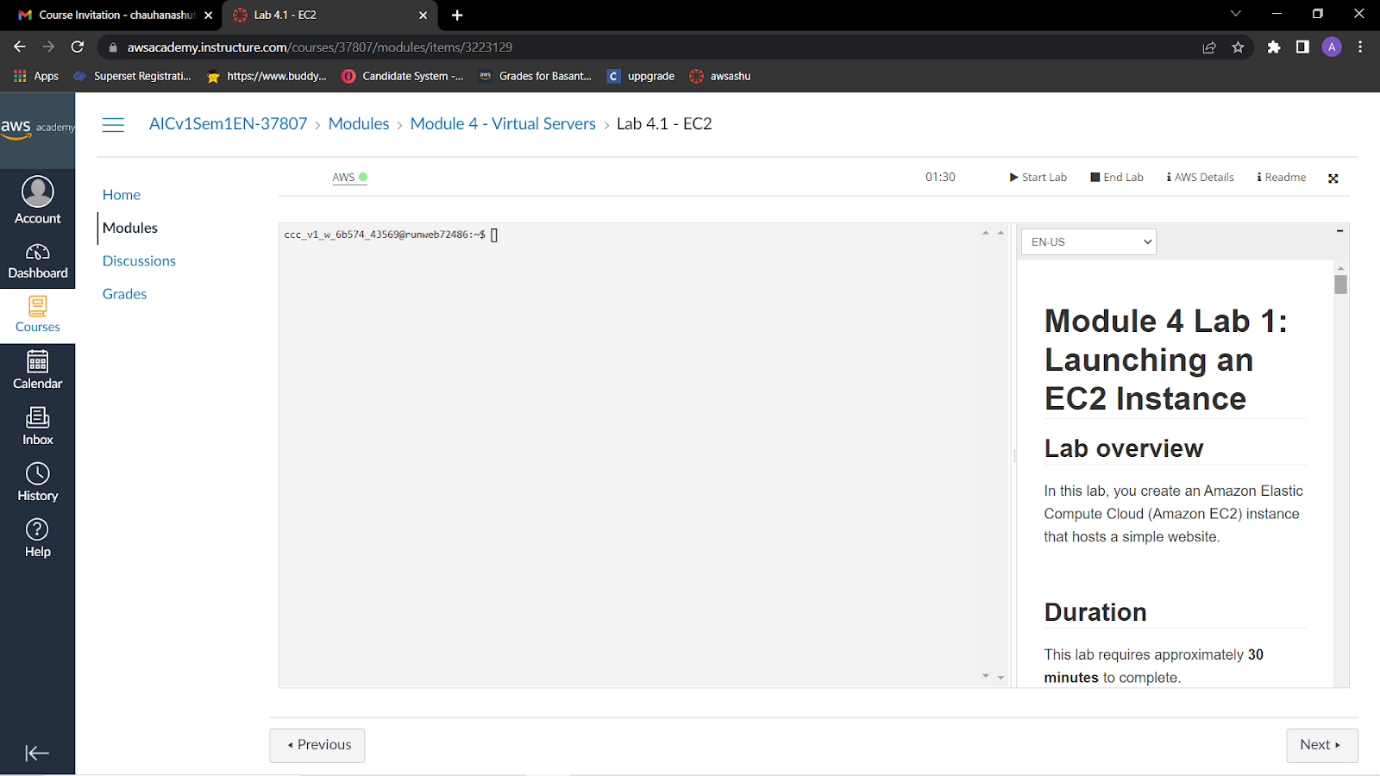






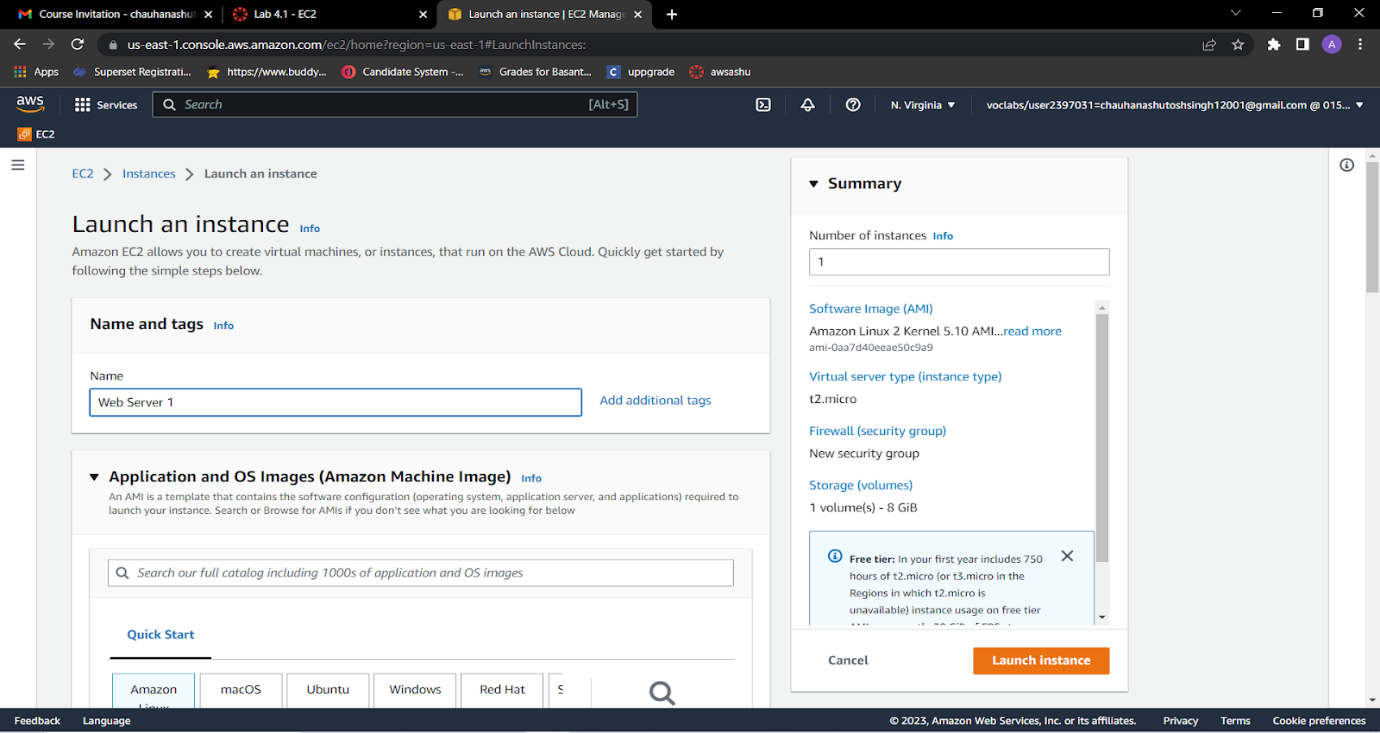
D. GCP/AWS/IBM/Azure/…

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

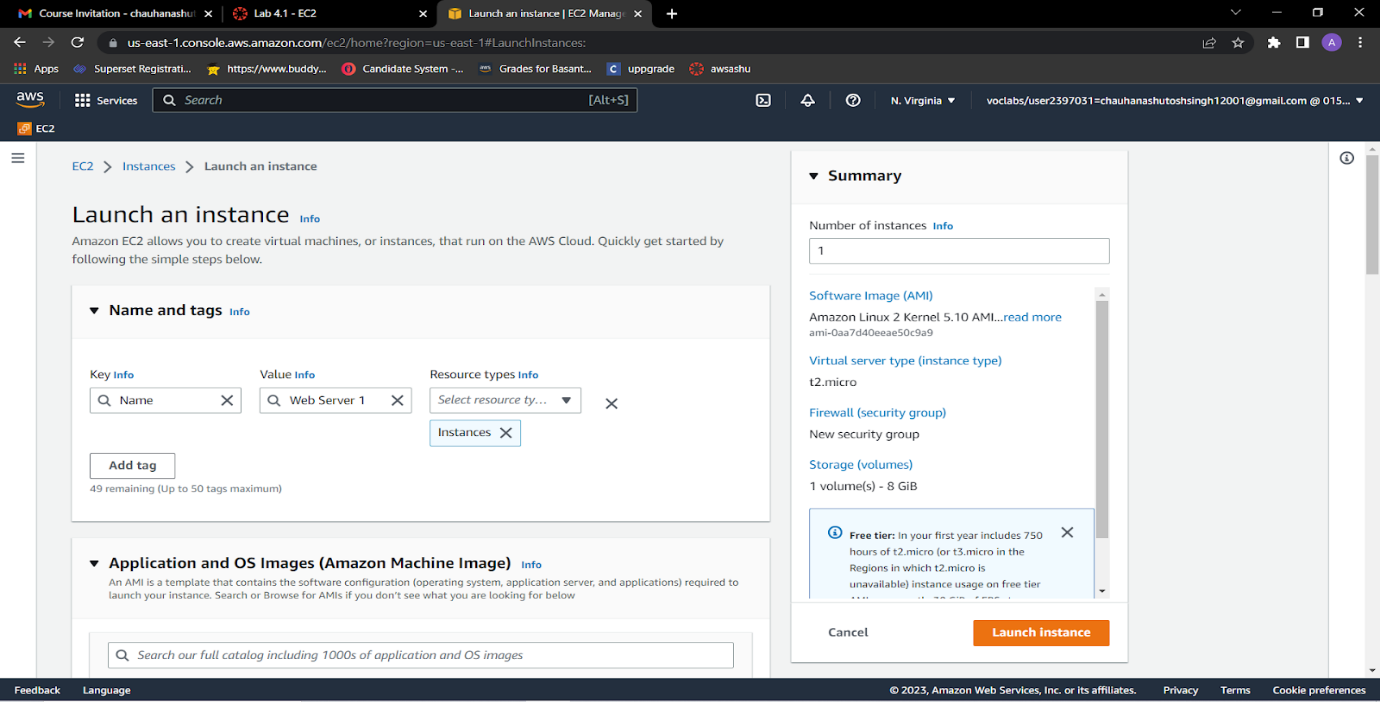


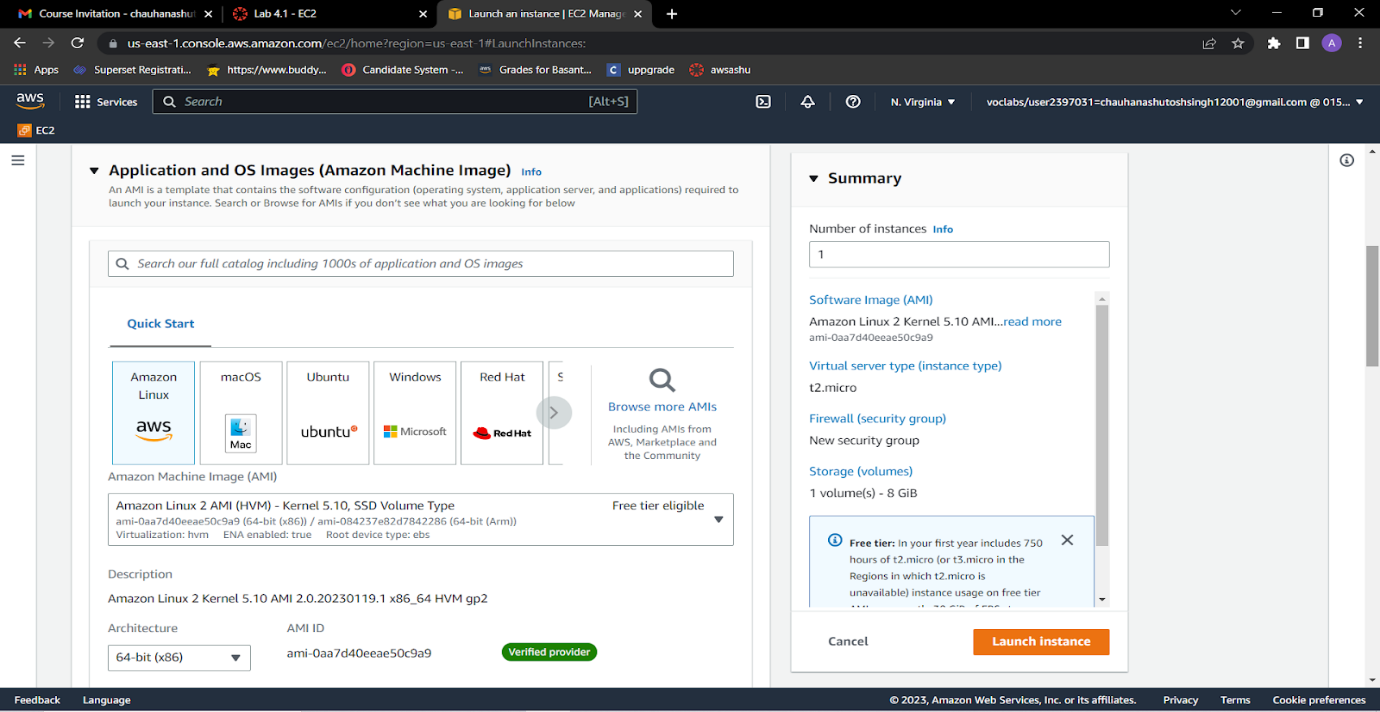
2.Choose the **Launch instance** button in the middle of the page, and then select **Launch instance** from the dropdown menu.

3.Give it the name Web Server 1



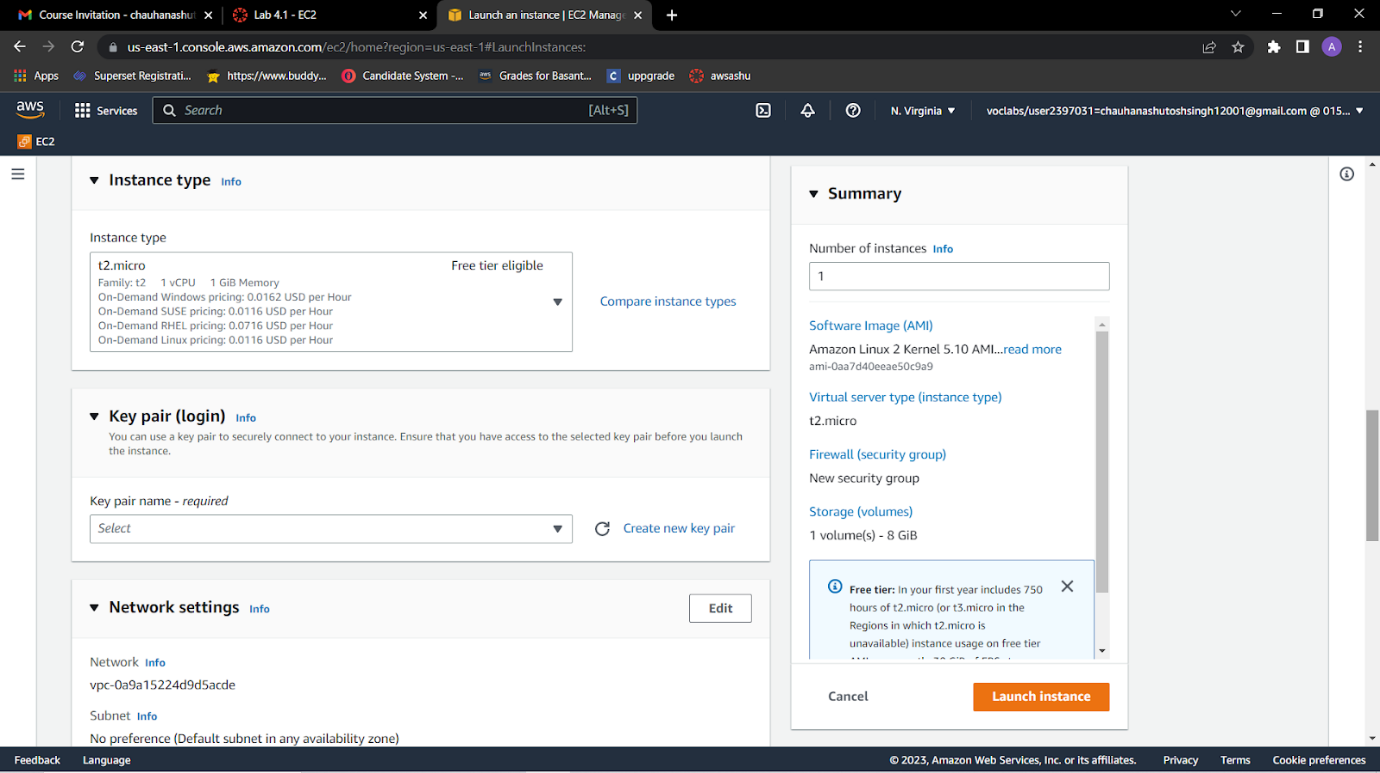
4.Choose an AMI from which to create the instance:

* 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.

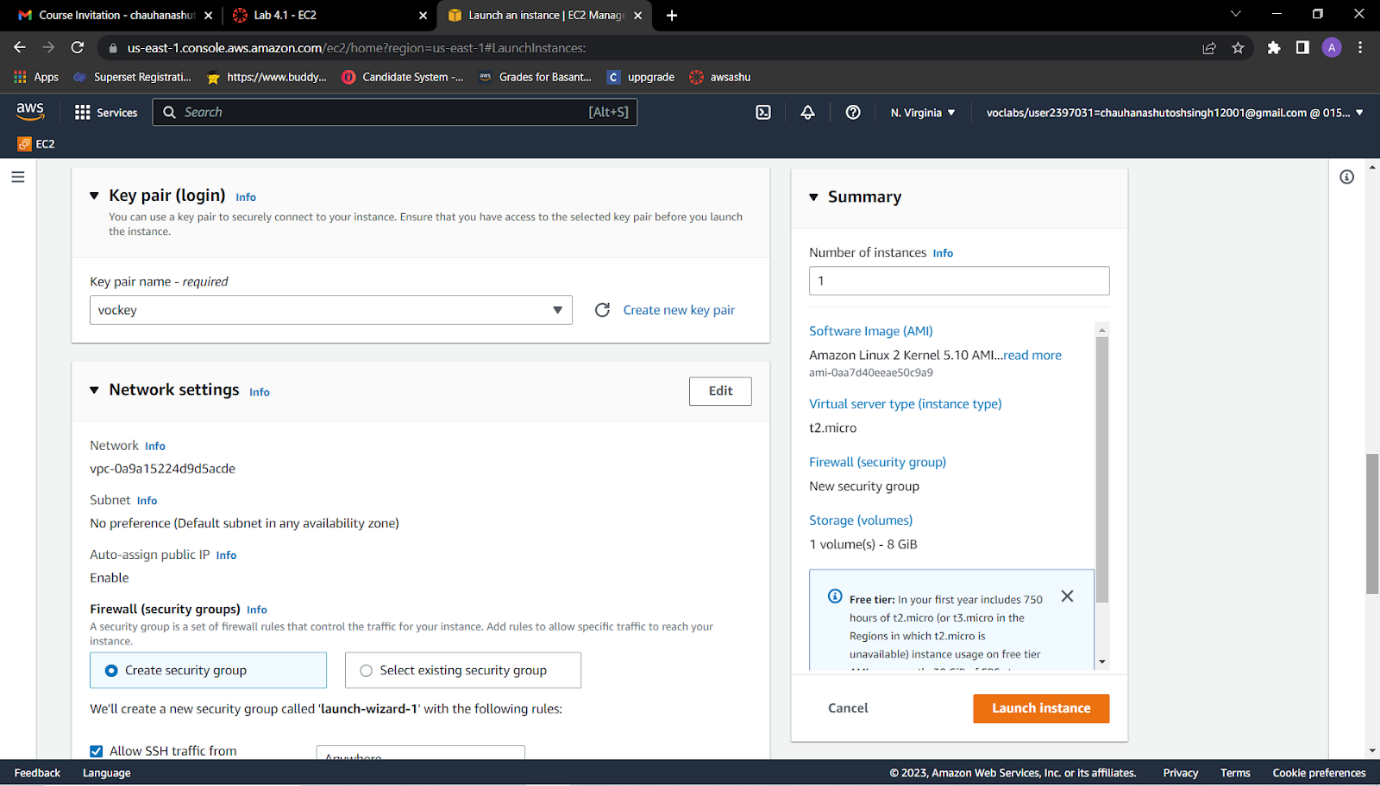
6.Select the key pair to associate with the instance From the Key pair name menu, select vockey.

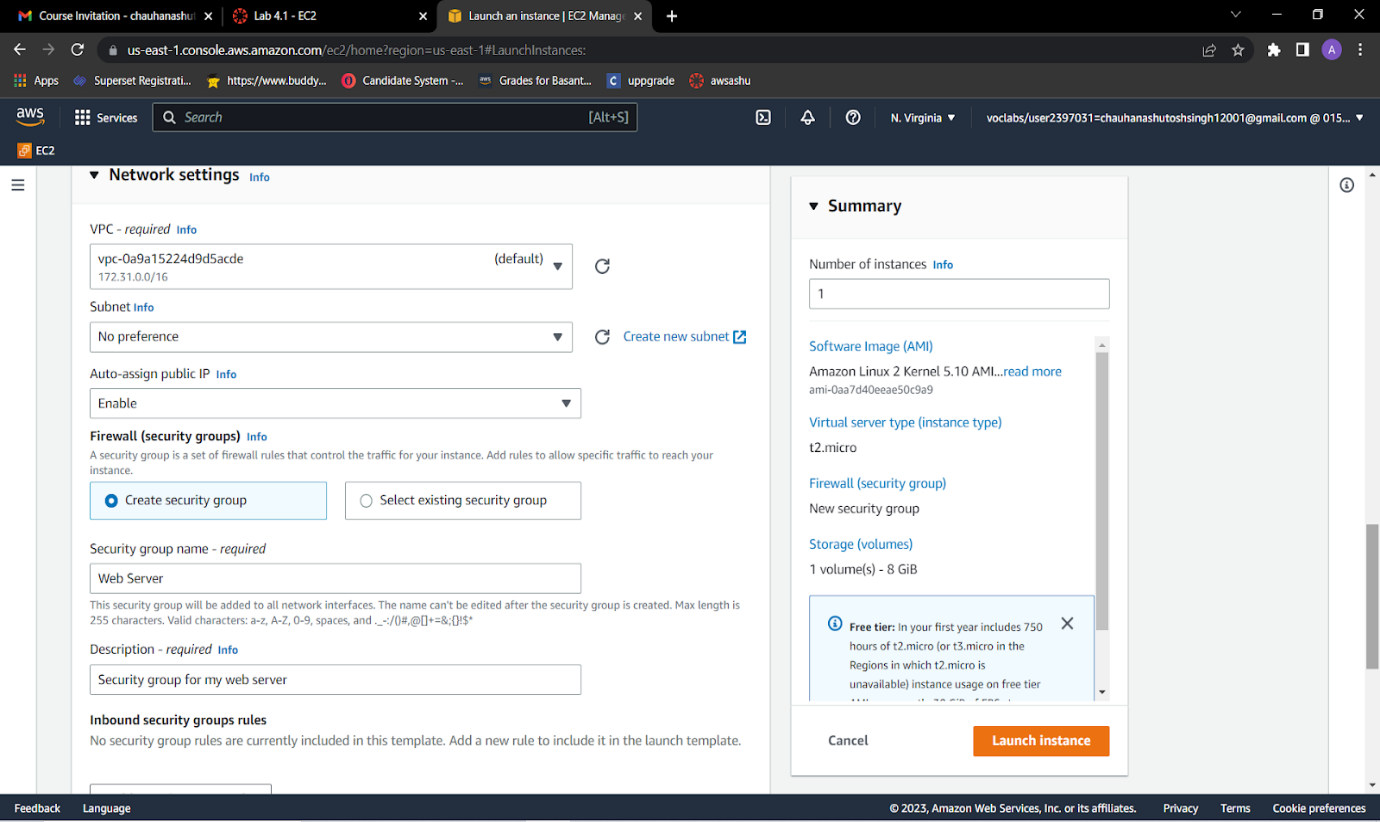


7.Next to Network settings, choose **Edit**.

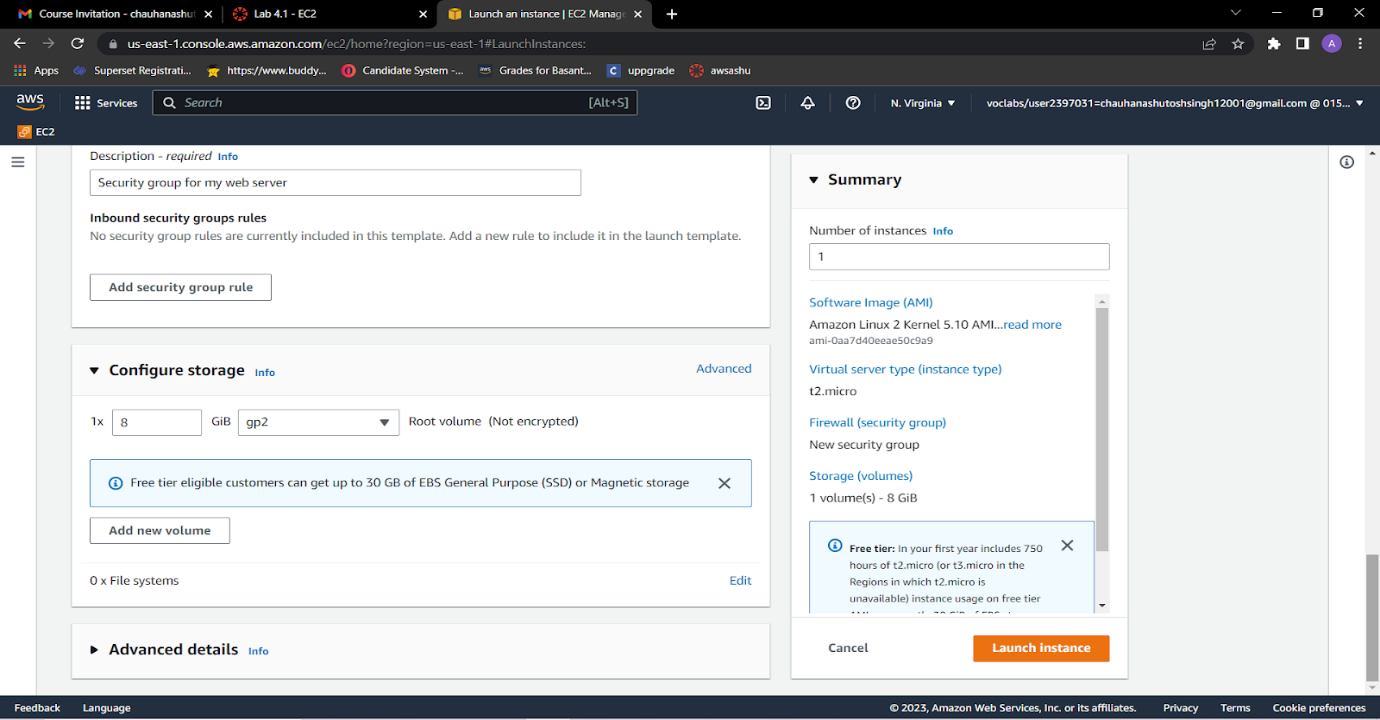
8.Keep the default *VPC* and *subnet* settings. Also keep the **Auto-assign public IP** setting set to **Enable**.

9.Under *Firewall (security groups)*, keep the default **Create security group** option chosen.



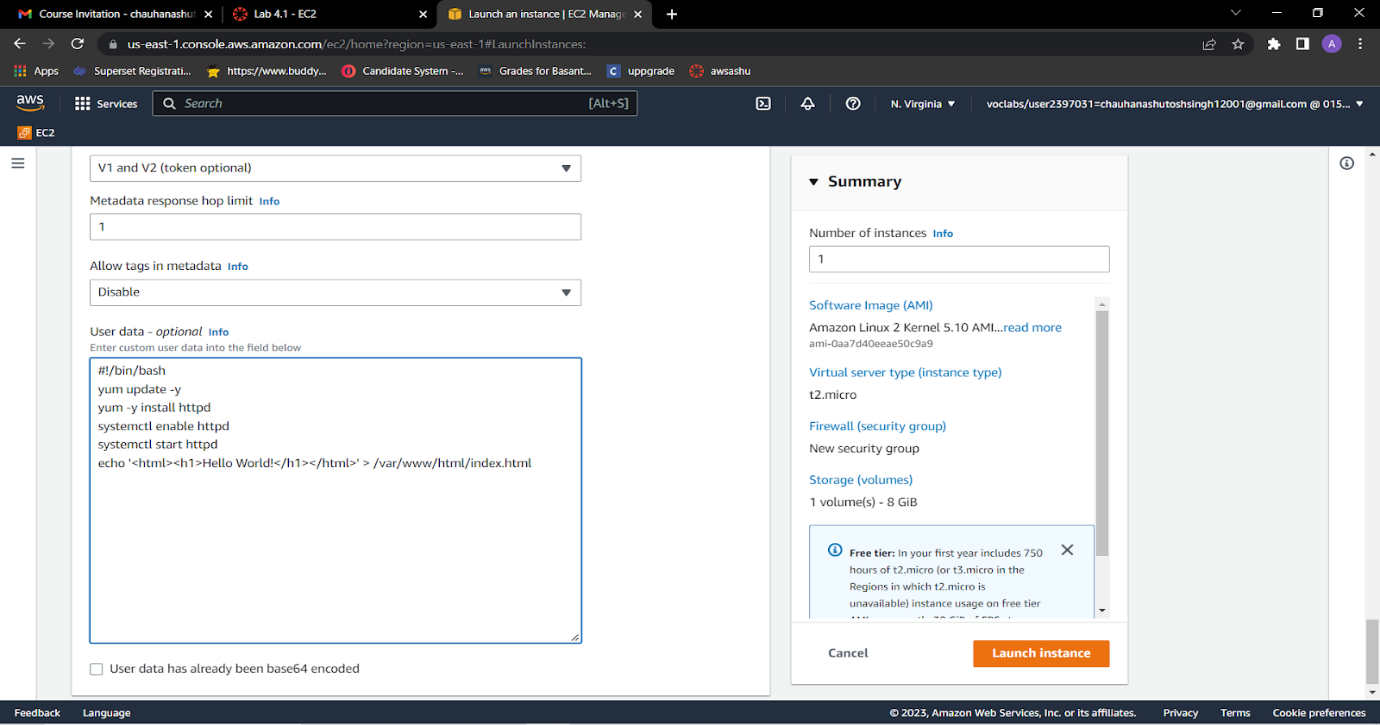


1. Configure a new security group:
   * Keep the default selection **Create a new security group**.
   * **Security group name:** Clear the text and enter Web Server
   * **Description:** Clear the text and enter Security group for my web server
   * Choose **Remove** to remove the default SSH inbound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

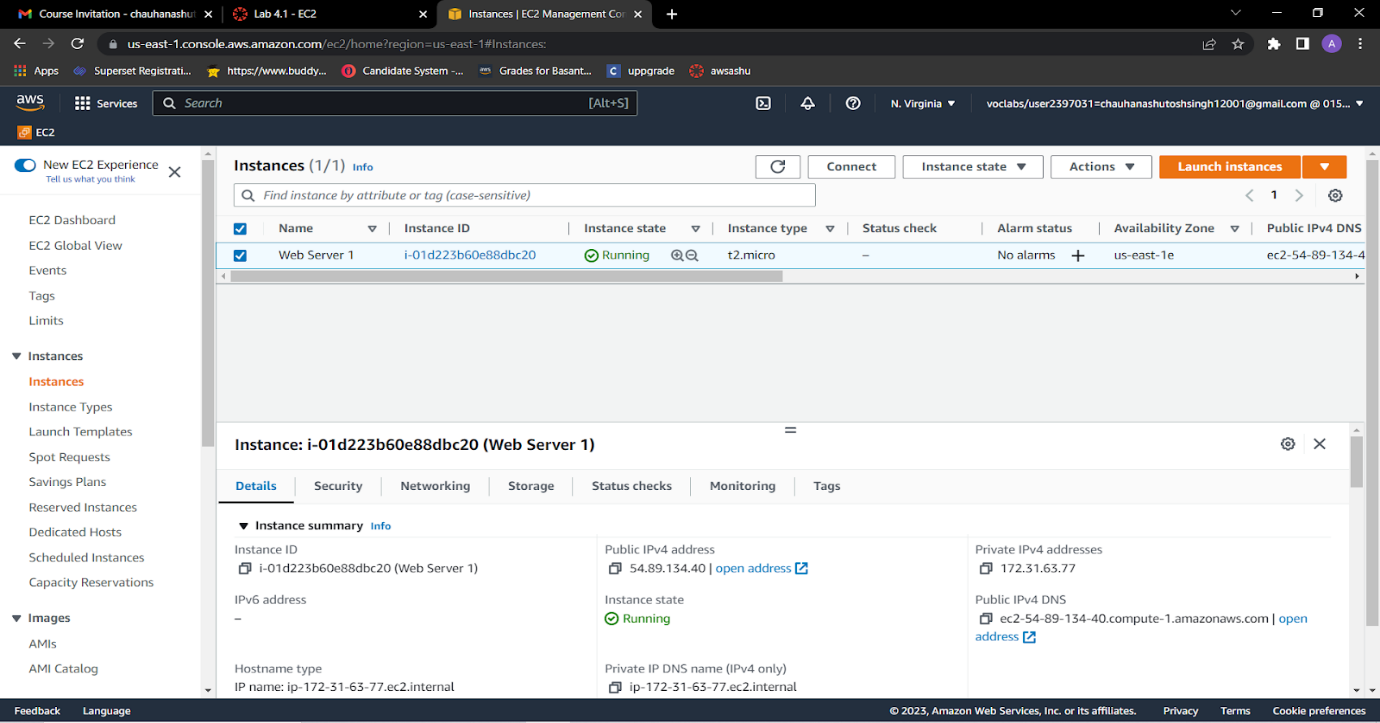
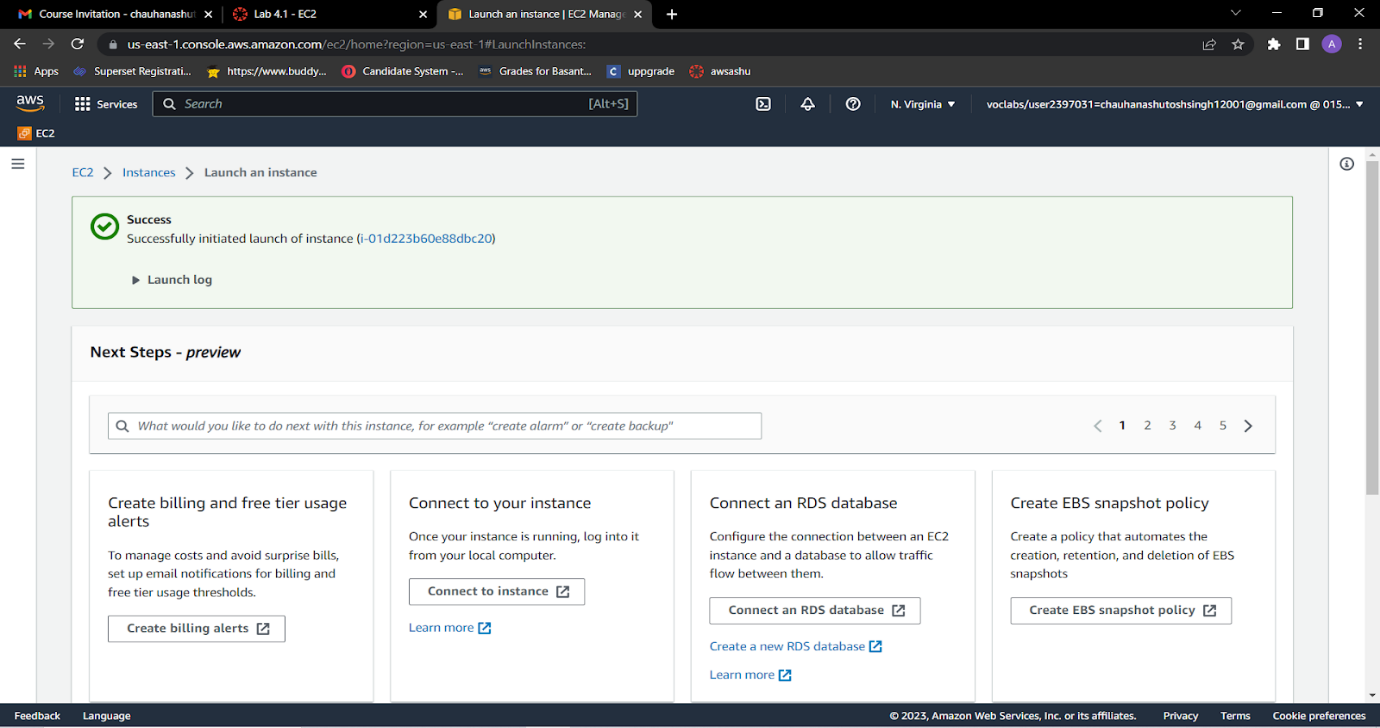


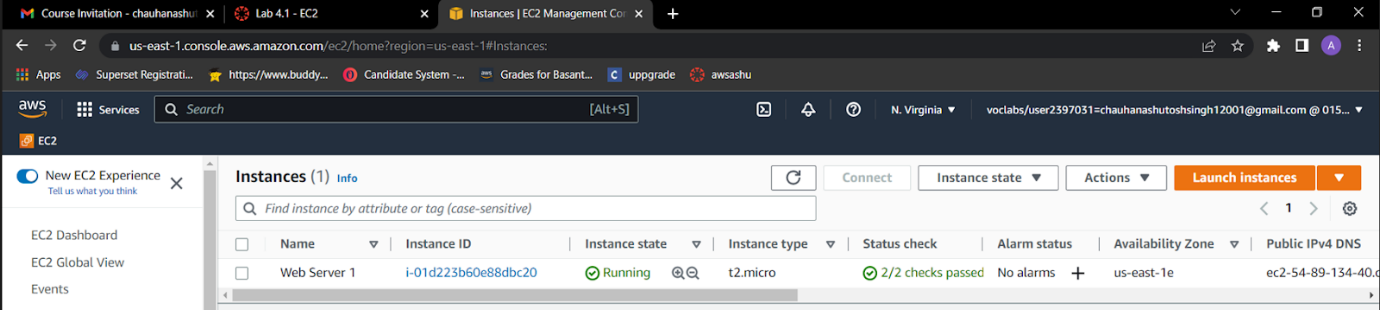
13. At the bottom of the **Summary** panel on the right side of the screen choose **Launch instance** You will see a Success message.

14. Go to  **View all instances**

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

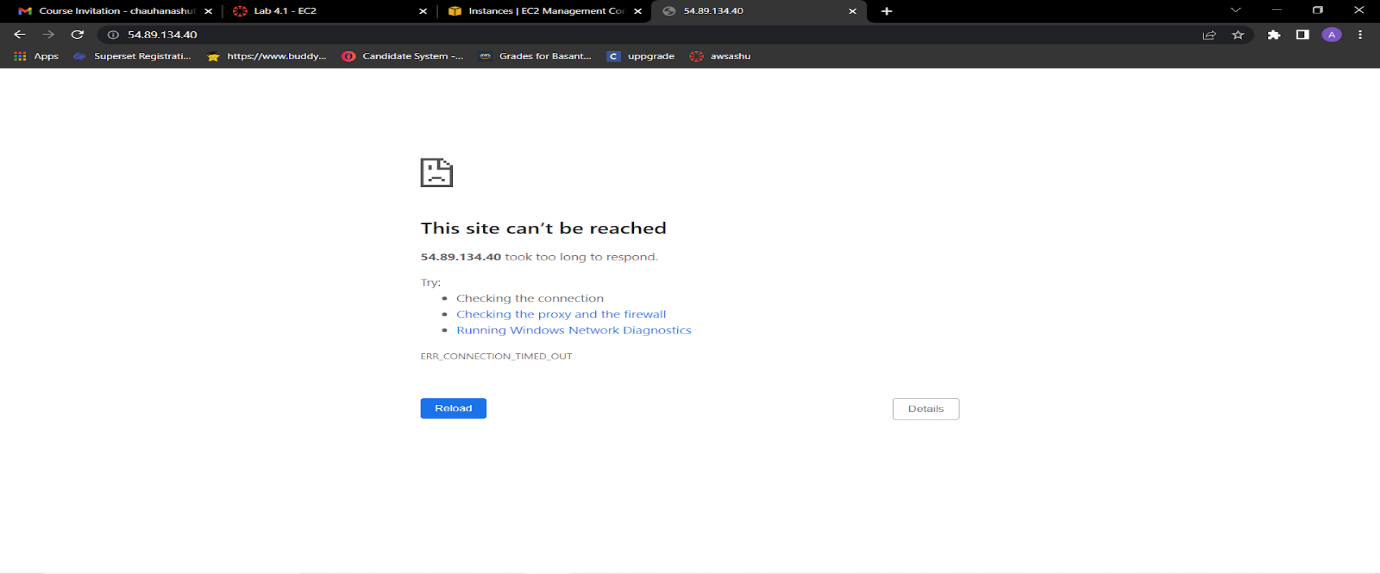
* **Instance state:** *Running*
* **Status check:** *2/2 checks passed*

**

**

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

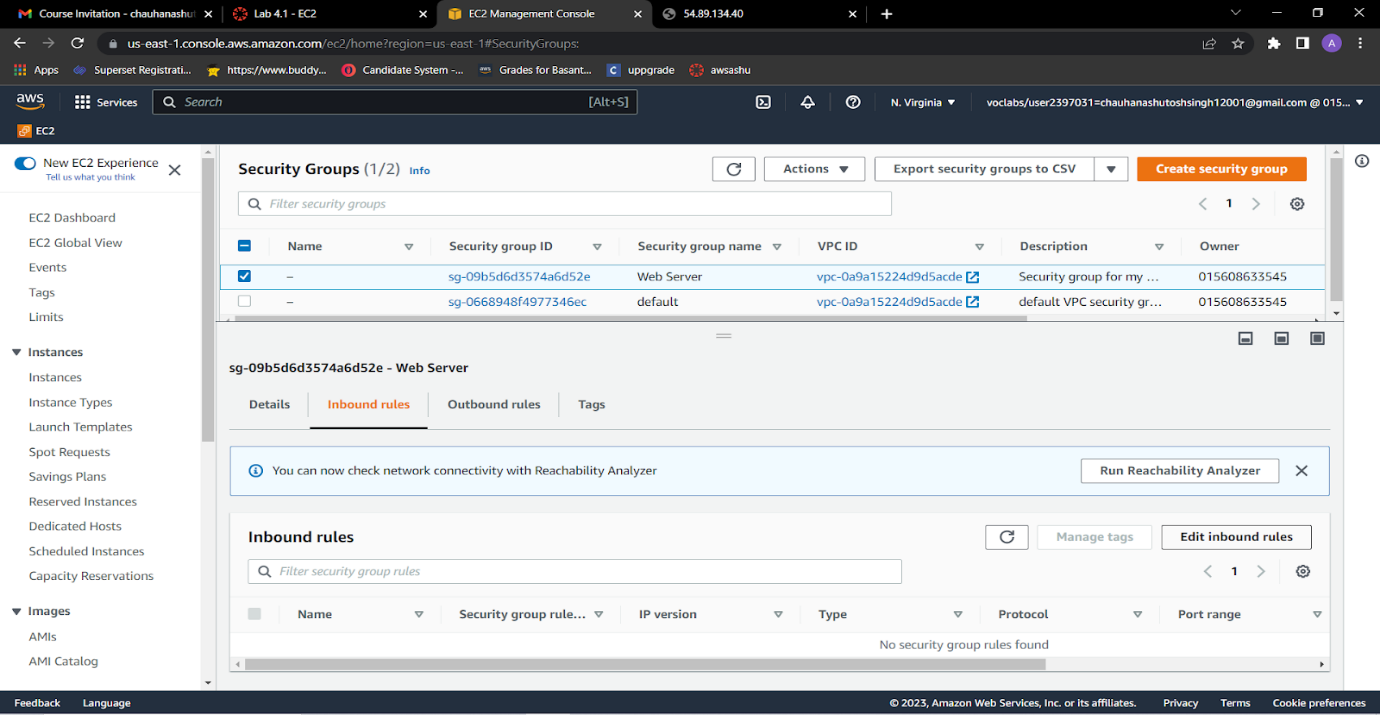
Open a new tab in your web browser, paste the public IP address you just copied, and press **Enter**.The webpage does not load. You must update the security group to be able to access the page.



15.Return to the **EC2 Management Console** browser tab.

16.In the left navigation pane, under **Network & Security**, choose **Security Groups**.

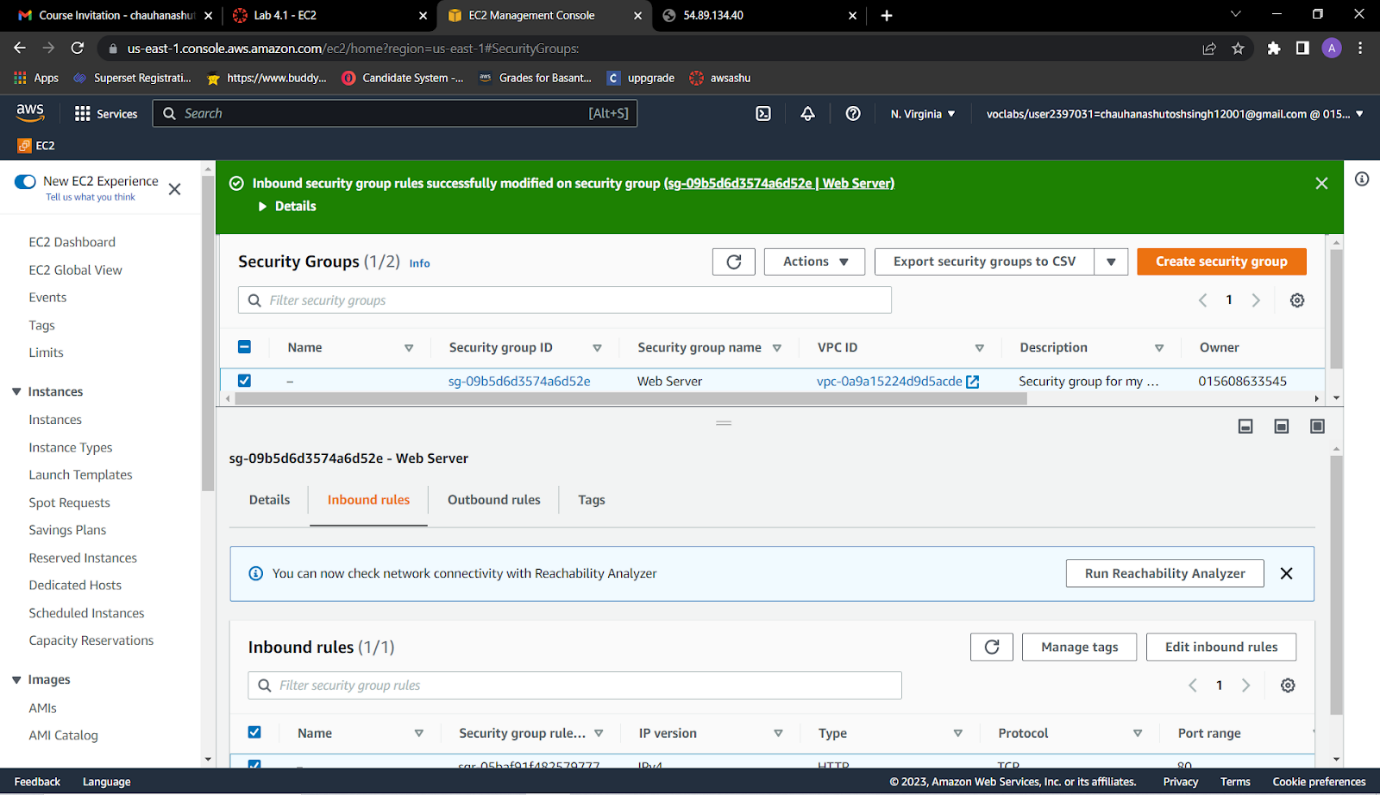
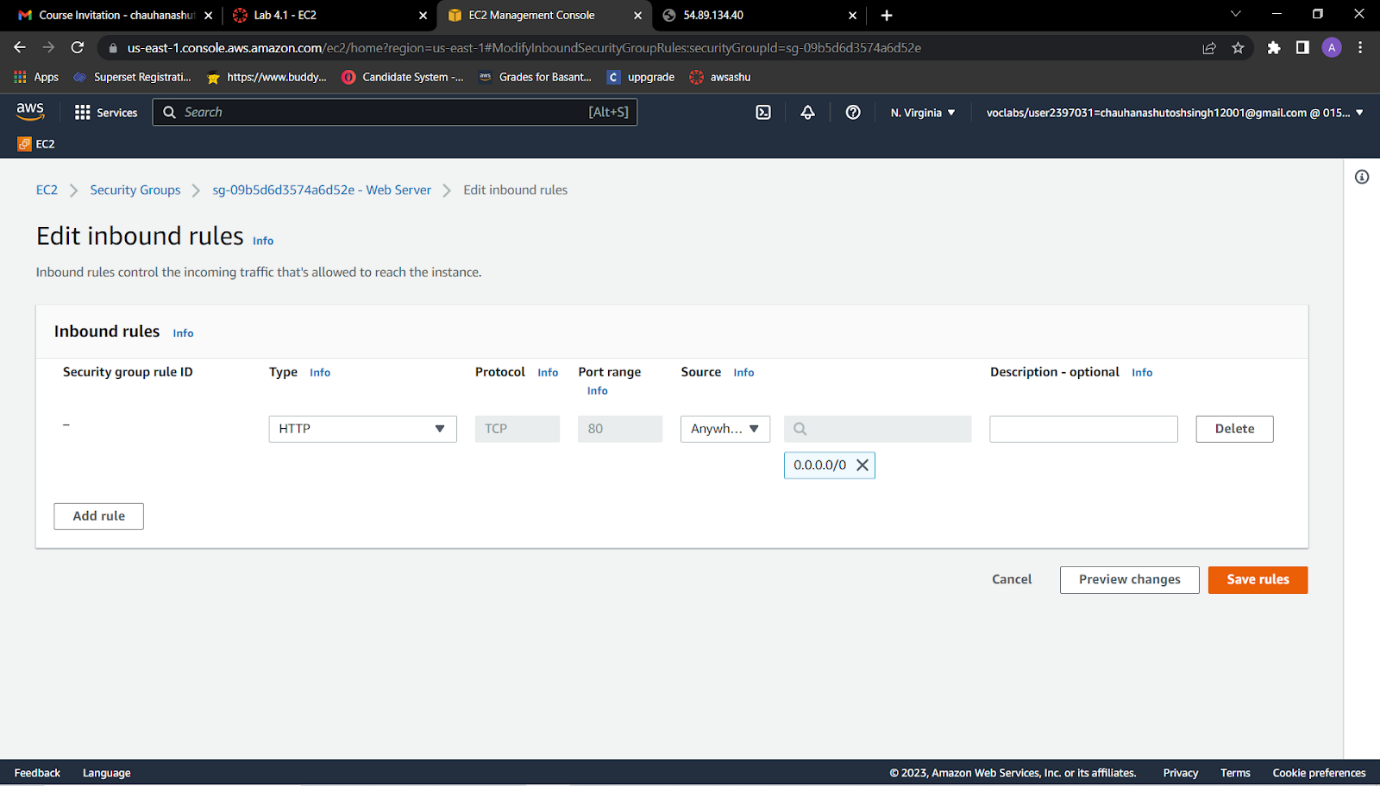
17.Select the **Web Server** security group, which you created when launching your EC2 instance.

18.In the lower pane, choose the **Inbound rules** tab.

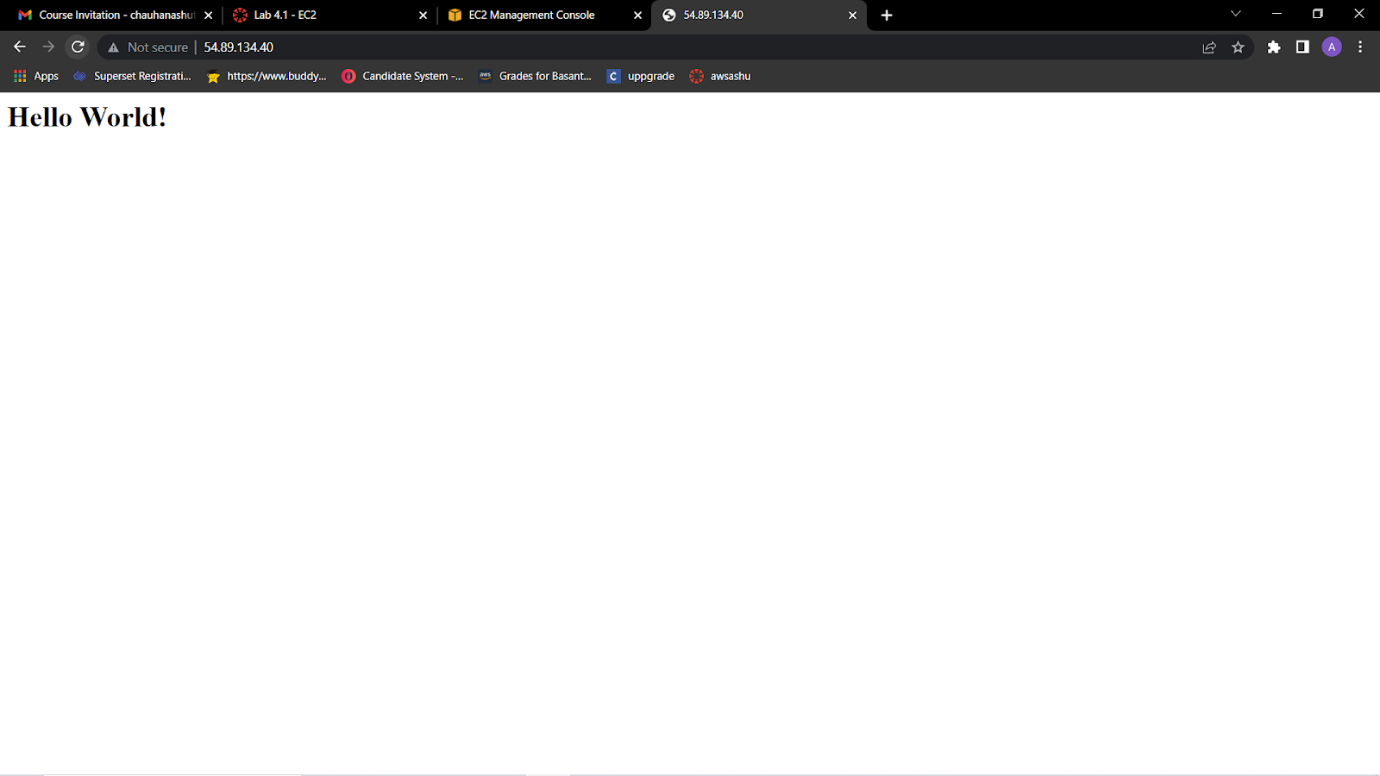
19.Choose **Edit inbound rules**, and then choose **Add rule**.Configure the following:

* **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!*

**

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