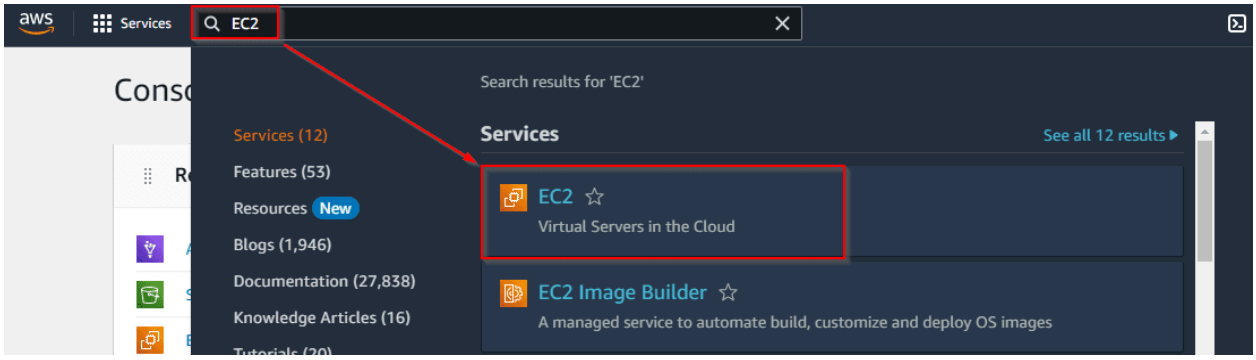
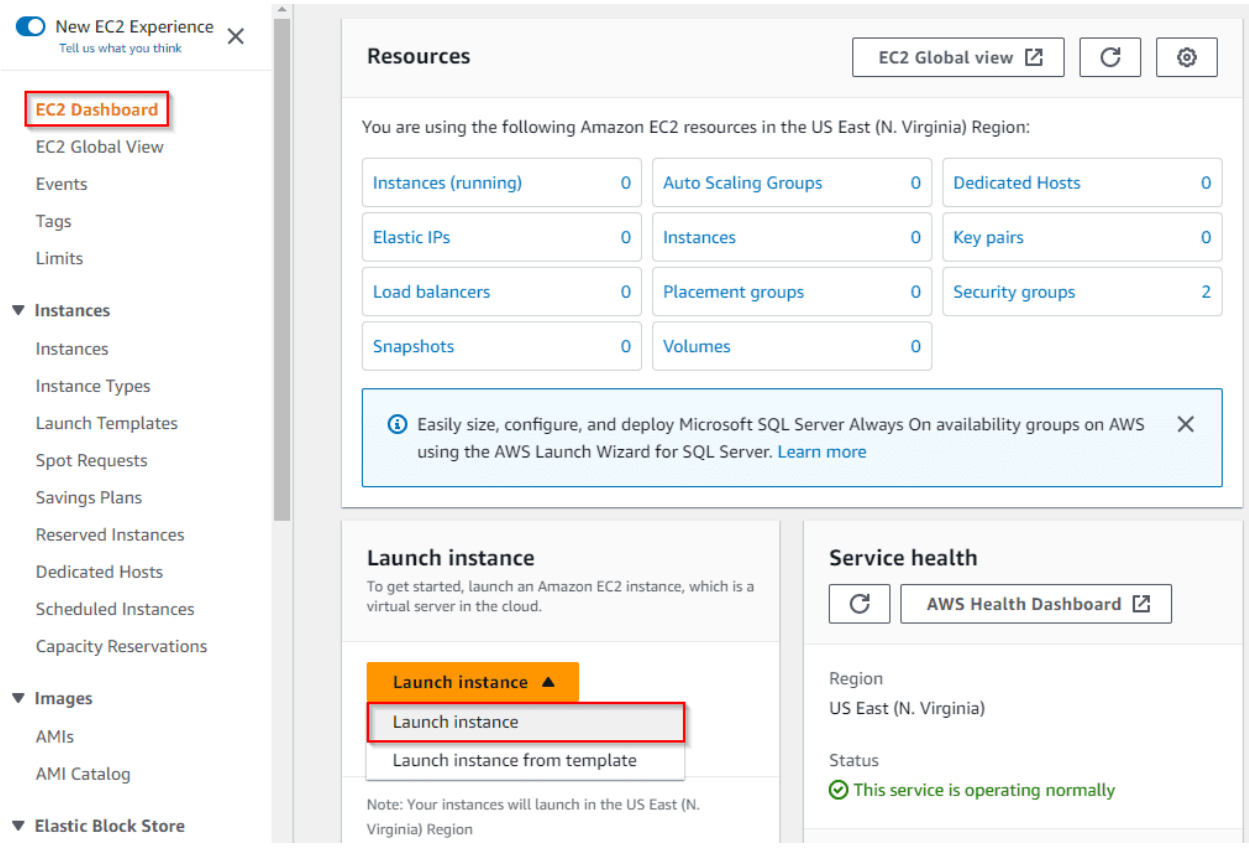
Creating A Linux EC2 Instance

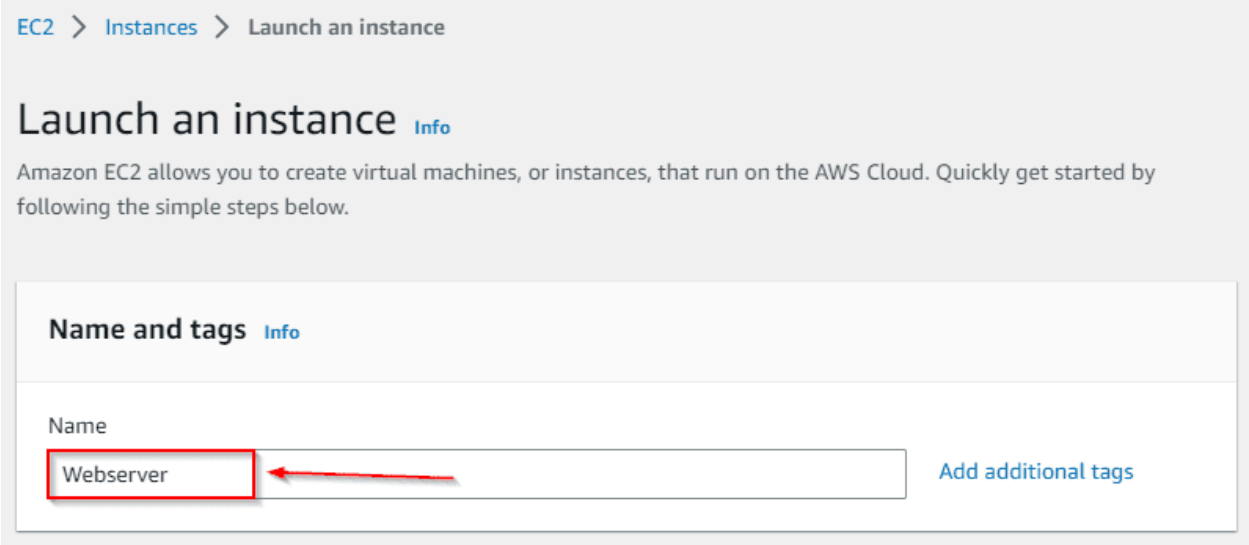
1. Open the AWS console and Search for **EC2** in the search bar and open it.



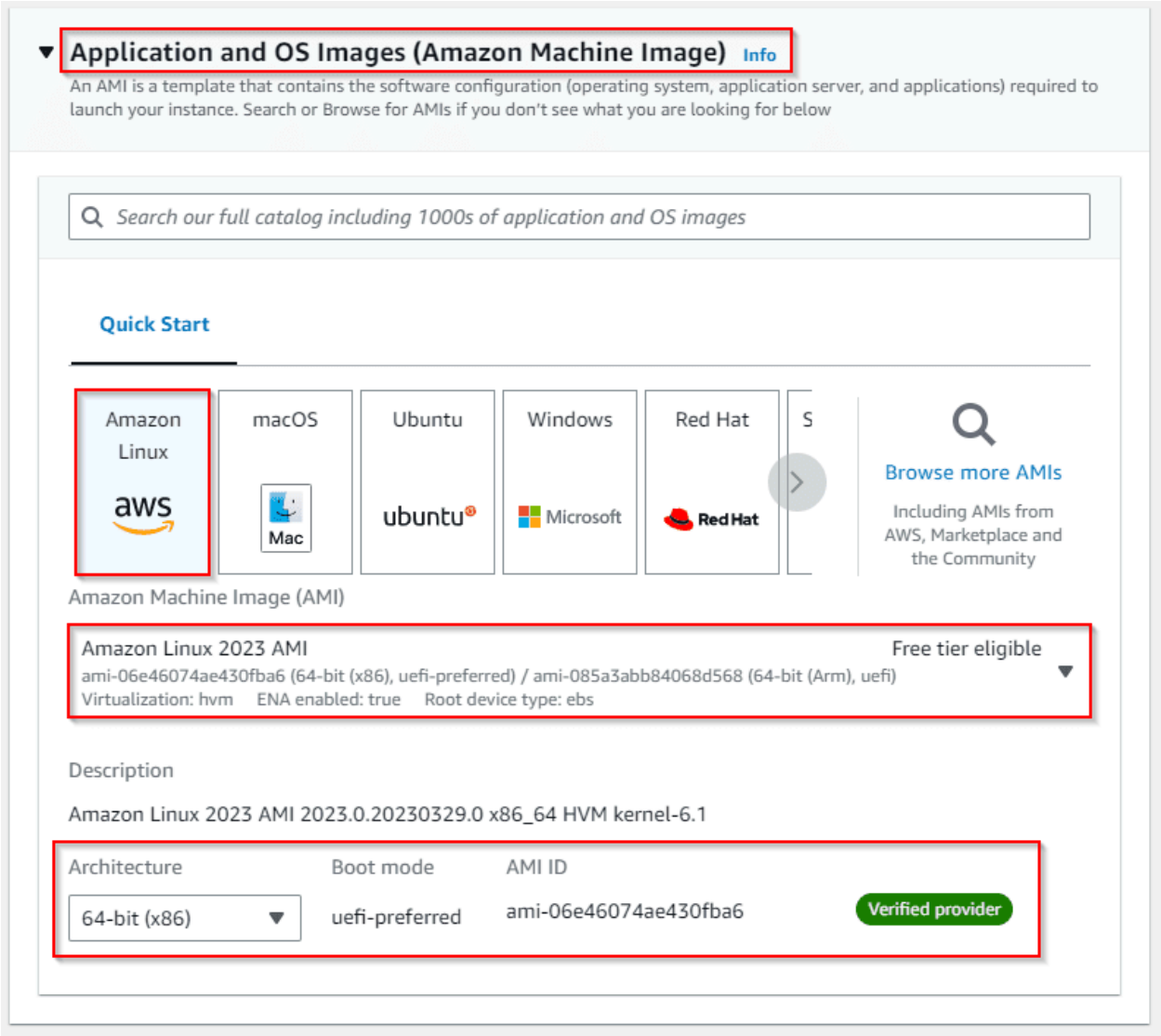
2. Once you are at the EC2 Dashboard, click on **Launch** to launch an instance.



3. Now under the Name, type Value as **Webserver** and Scroll Down. Tags are added just for specifying names in the key and value field.

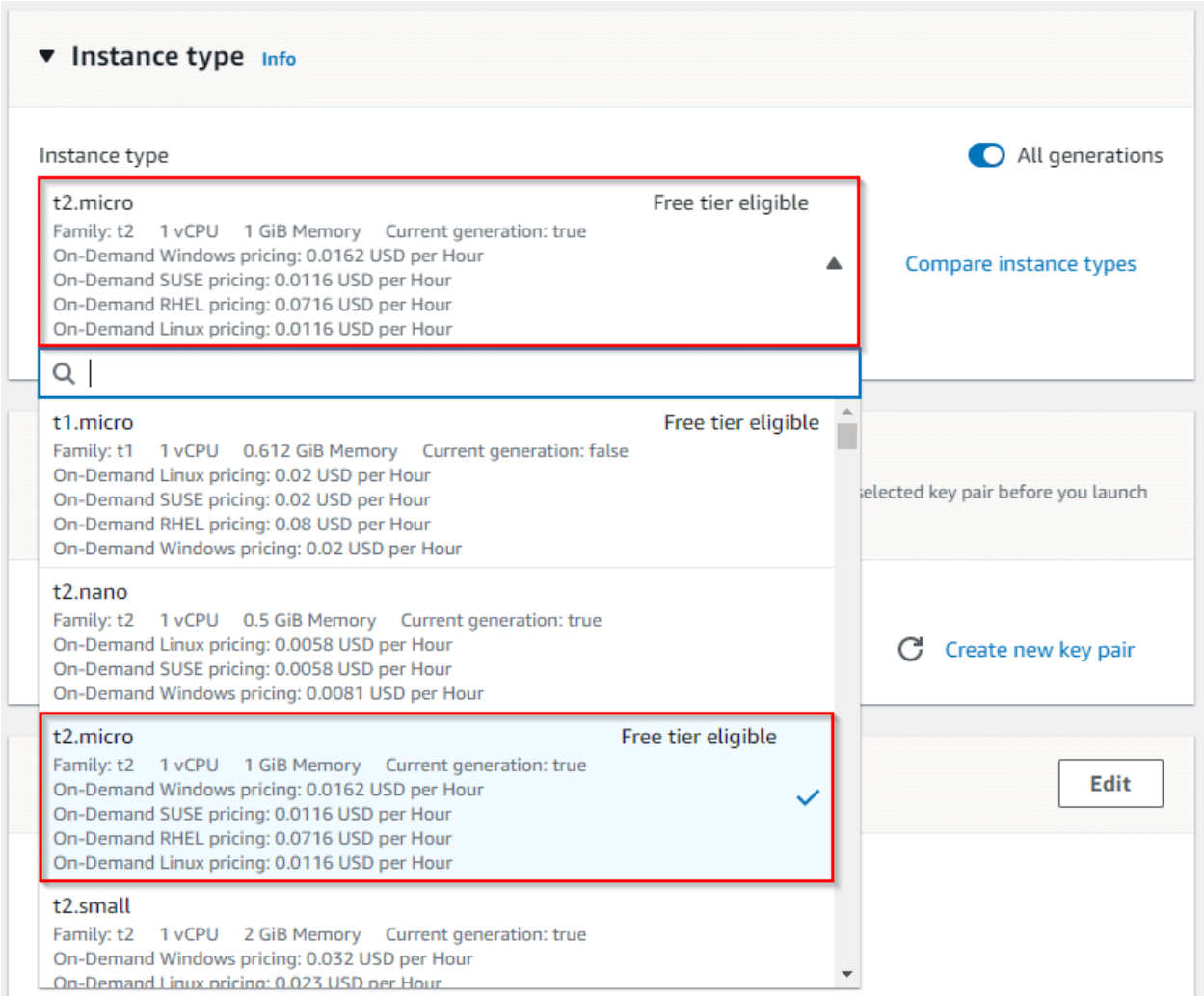


4. Choose **Amazon Linux 2023 AMI**, select 64-bit (x86) architecture, and Scroll Down.



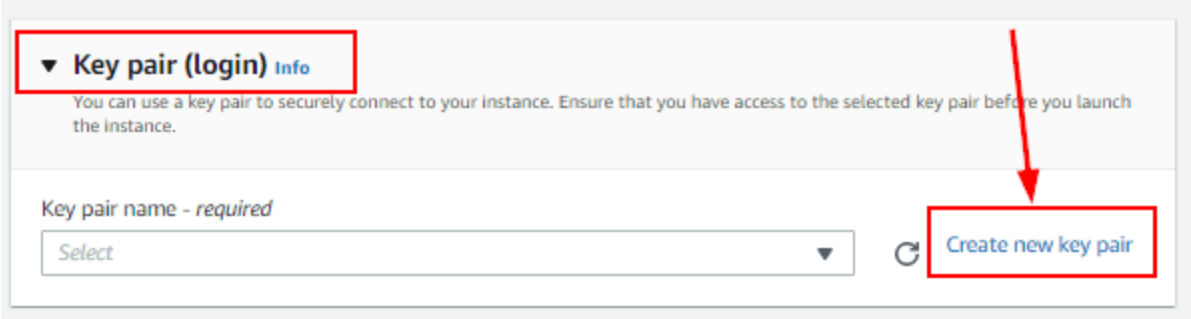
Note: Here, in the above step we are selecting the Amazon Linux 2023 AMI which is basically preconfigured with some tools installed on it as Amazon Linux 2023 AMI comes with AWS CLI pre-installed. AWS CLI is basically the Command Line Interface provided by AWS to access any of their services using CLI.

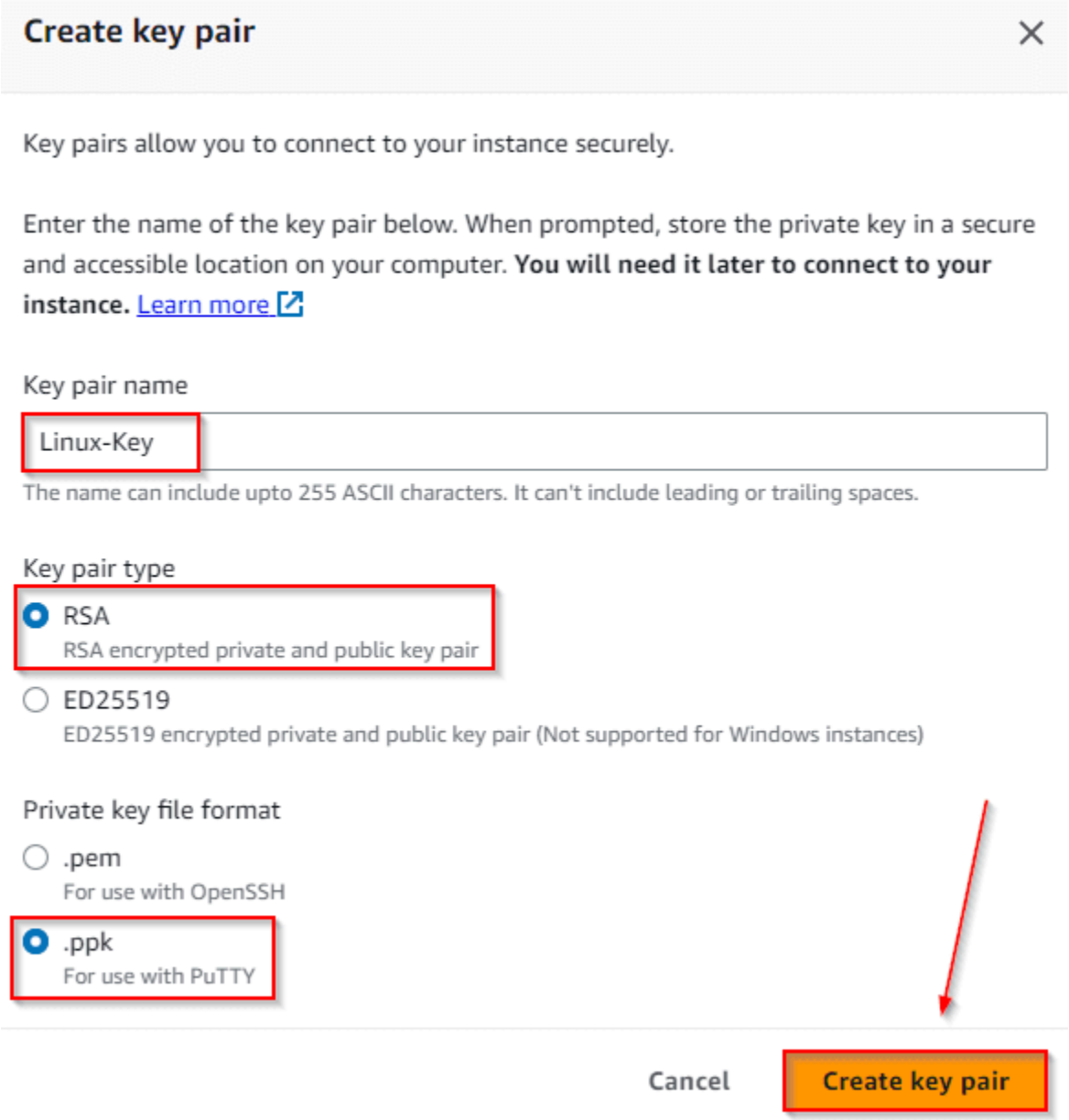
5. Select the **t2.micro** instance type which is eligible for the free tier.



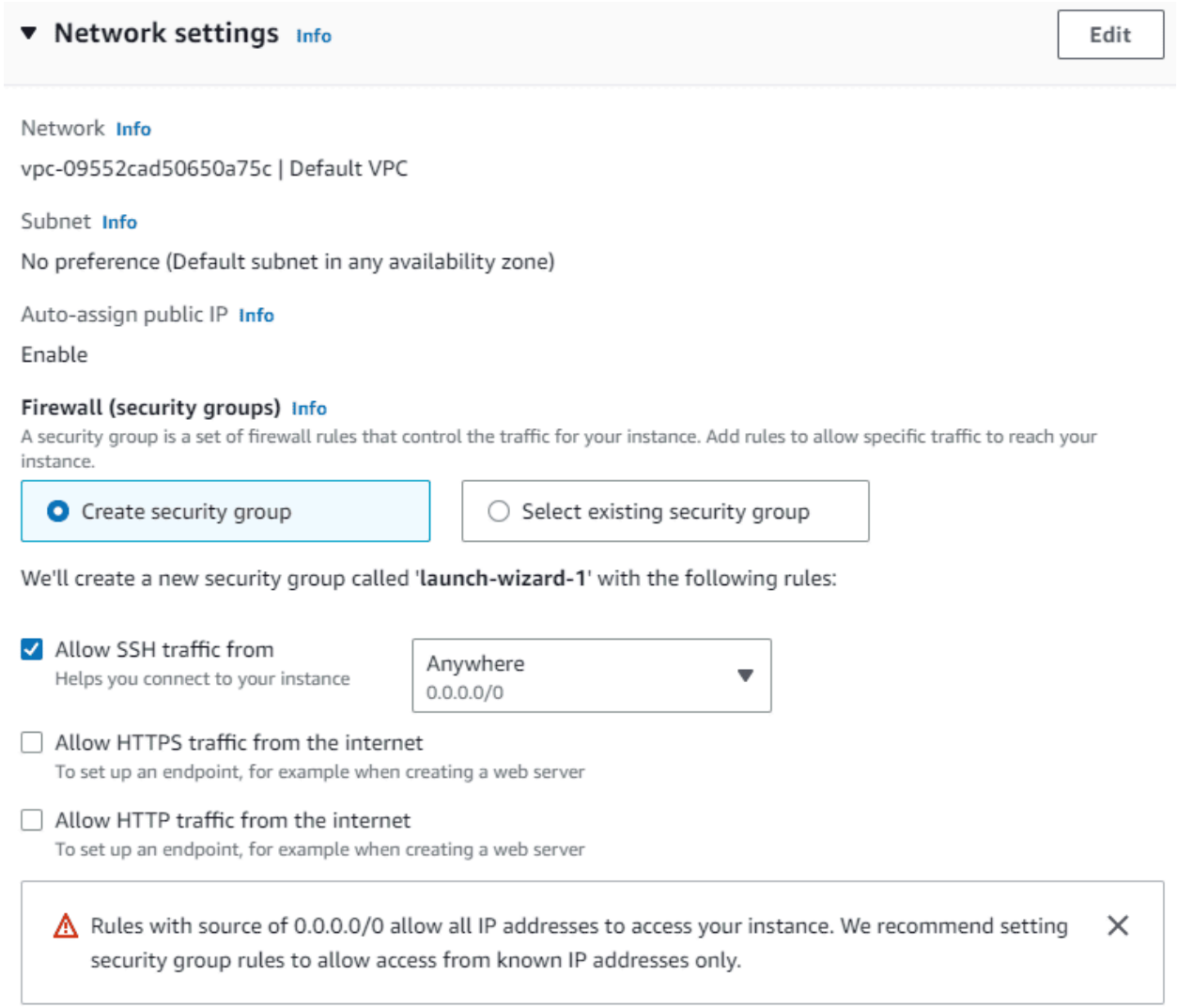
Note: Here we must choose the instance type as **t2.micro** because it is free tier eligible, i.e. you won't be charged for running the instance.

6. Select an existing key-pair or create a new one, we will **create a new one**, enter the name of the Key-pair as **Linux-Key** and rest **everything Default.**

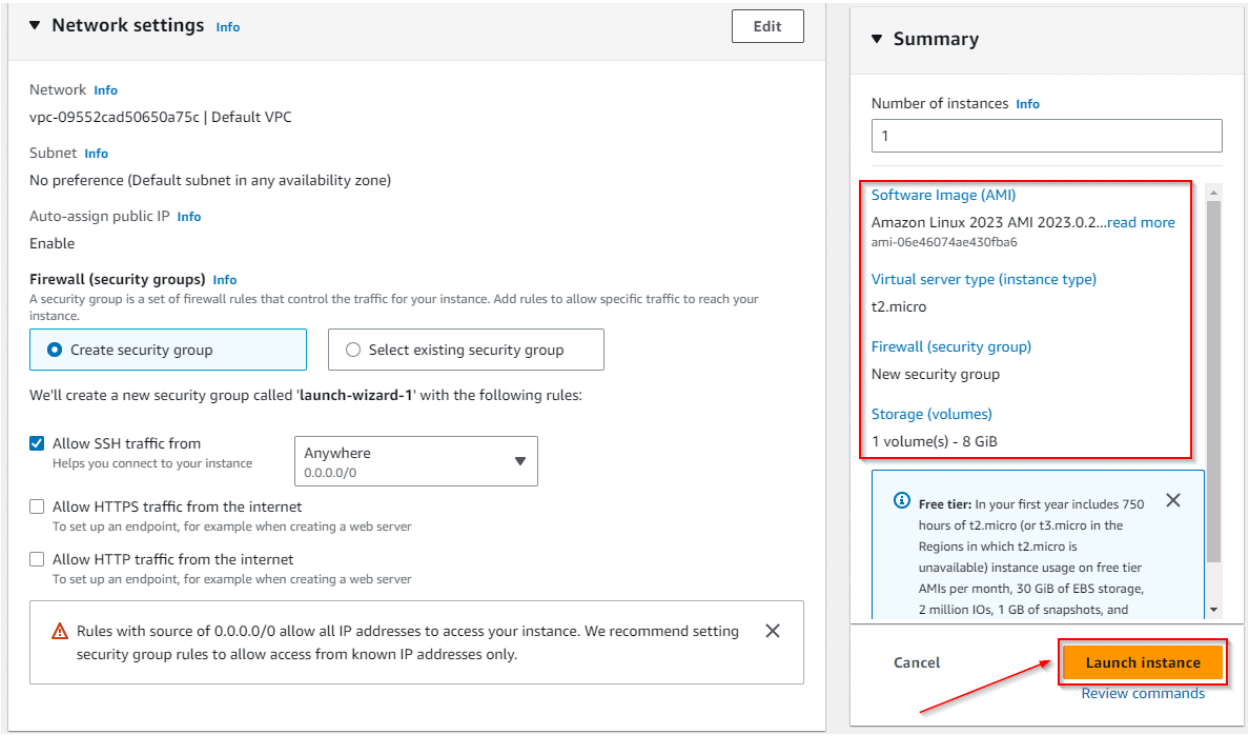

Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
Select
Create new key pair


Create key pair
Key pairs allow you to connect to your instance securely.
Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more
Key pair name
Linux-Key
The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
Cancel
Create key pair

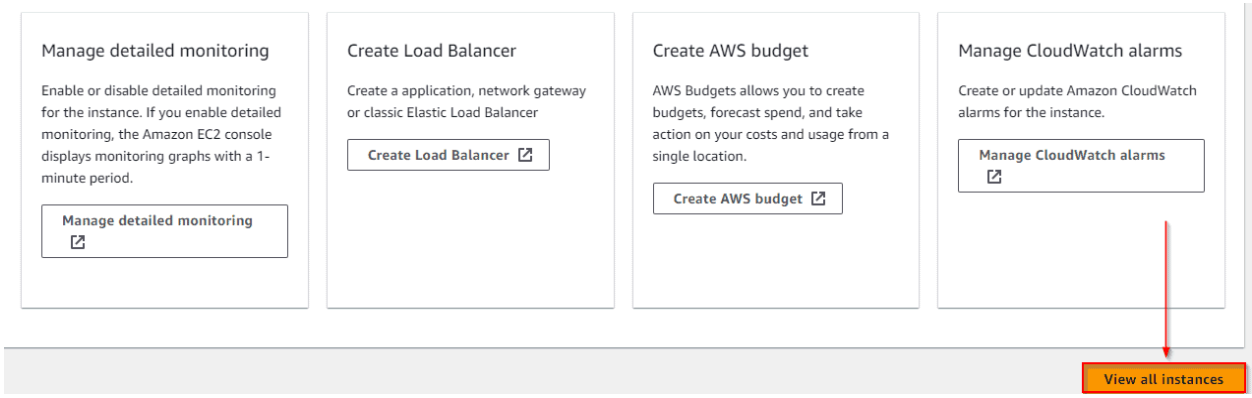
7. Here we can Configure Network Settings as per our needs. For now, we will keep **all the settings** as default.



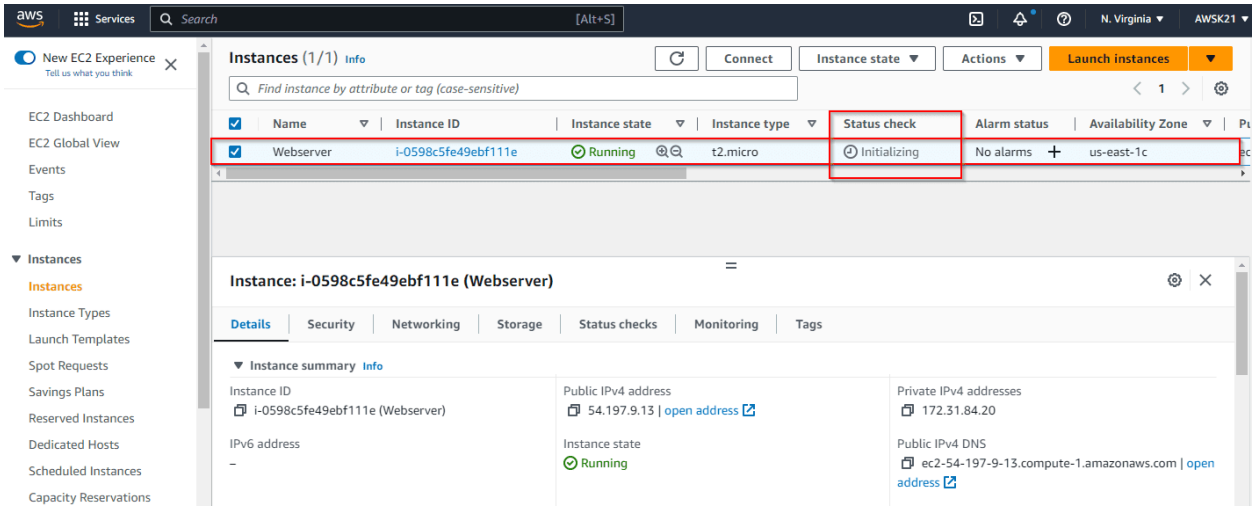
8. Now review all the things you have Configured and Click on **Launch Instance.**



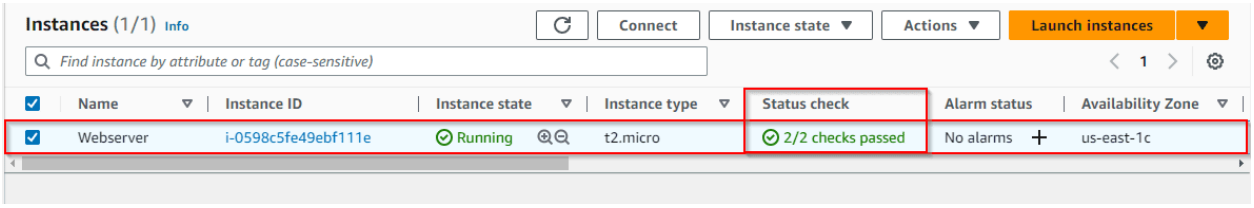
9. Now, scroll down and click on **View All Instances.**



10. Here, you shall see your instance is launching and the **Status check** is **Initializing**, wait for some time.



11. Refresh and you shall see your instance is **Up and Running**, and the Status check has changed to **2/2 checks.**



Note: Now, wait for the Status check of the instance to change to 2/2 checks pass as the instance is launching from an AMI and it needs time to install all the preconfigured things like AWS CLI and other tools. So, please wait till the Status check becomes 2/2 checks pass and then only proceed with further steps, and if the status check has not passed then you shall get an error in the further steps so please wait.

Thus, we have successfully created our first Linux Instance using EC2.

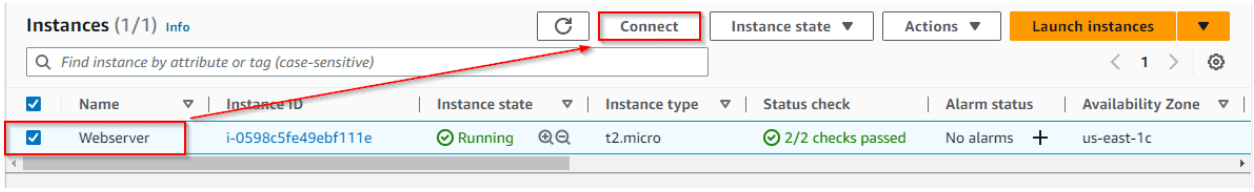
Note: Now we have launched the instance successfully, further we need to access the instance so, we have two ways of accessing an instance-

1. **Accessing via Browser using EC2 instance Connect.**
2. **Accessing using Putty (a Secure Shell SSH client).**

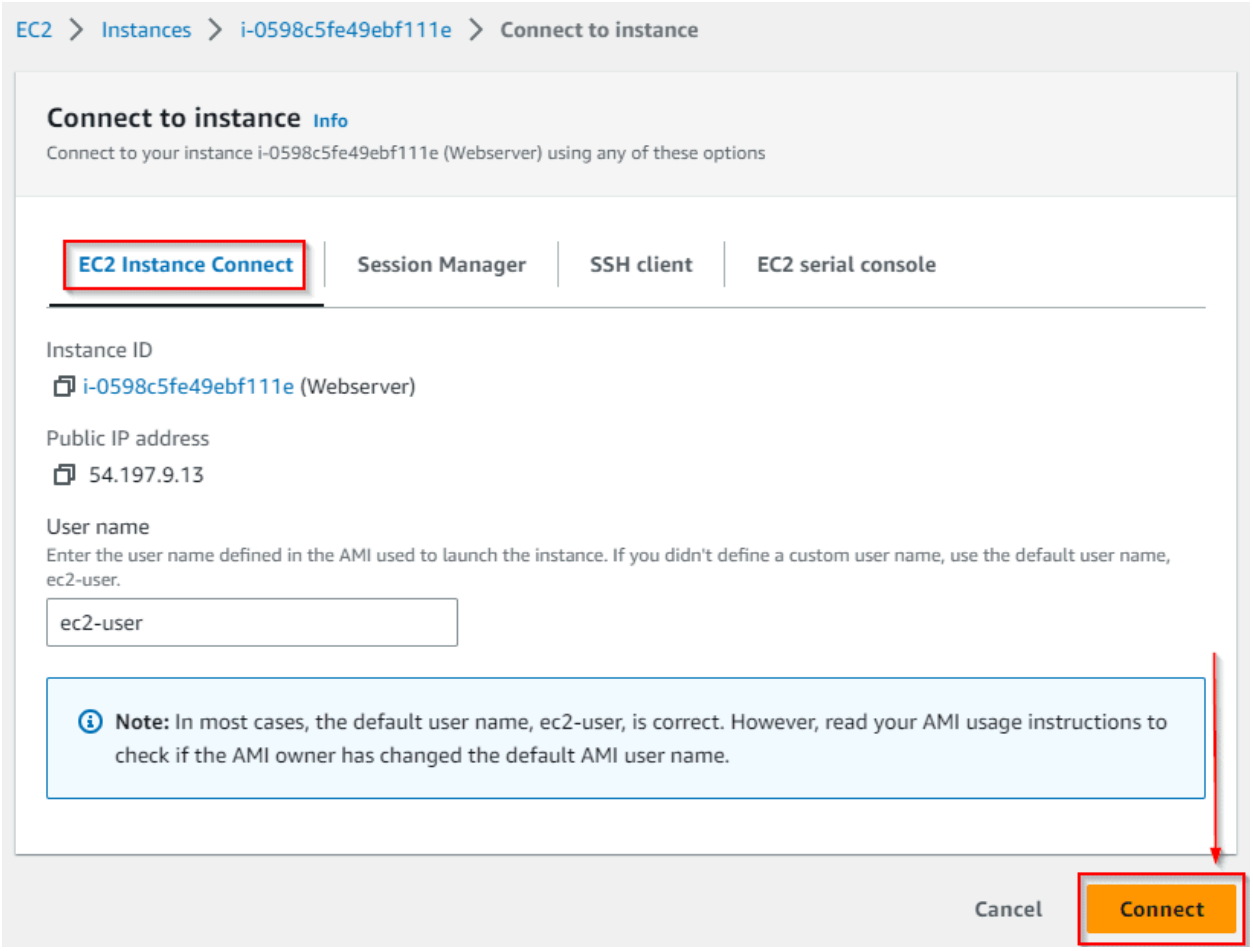
Accessing EC2 Instance Using EC2 Instance Connect

Note: Till now, we have launched an instance successfully, but we need to access it to run commands so for accessing our instance the easy way is you can access the CLI directly from the browser using the EC2 instance connect that we shall see in further steps.

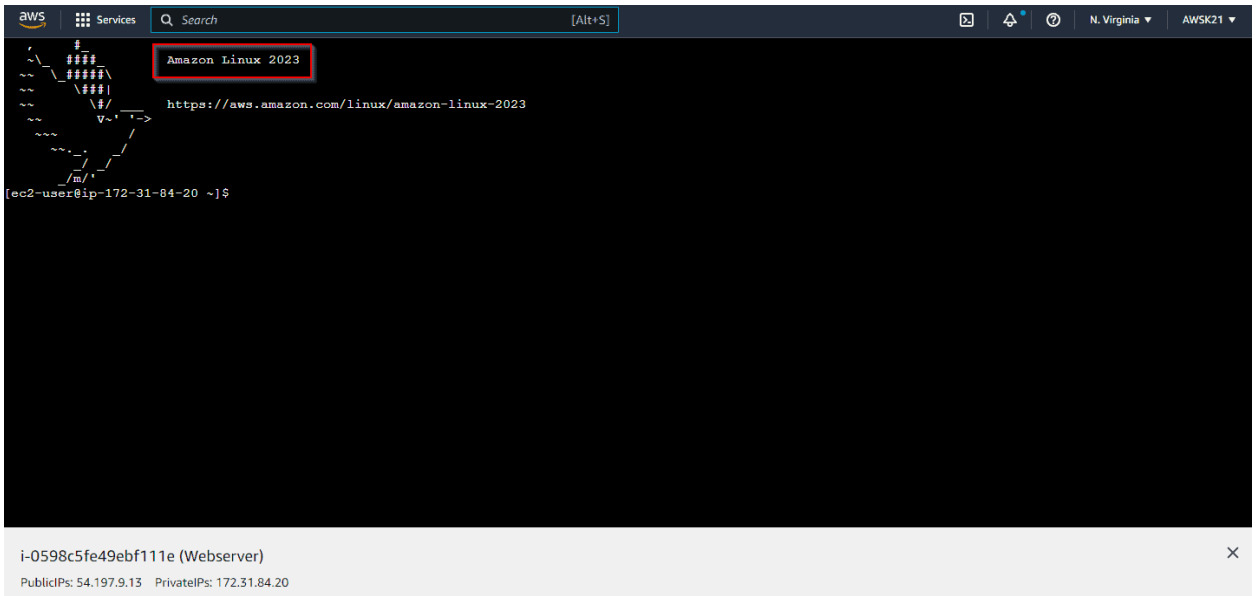
1. Select your Instance and Click on **Connect**.



2. Under EC2 Instance Connect, let everything default, and click on Connect.



3. Now you shall be redirected to a new window and you shall see the Linux CLI.

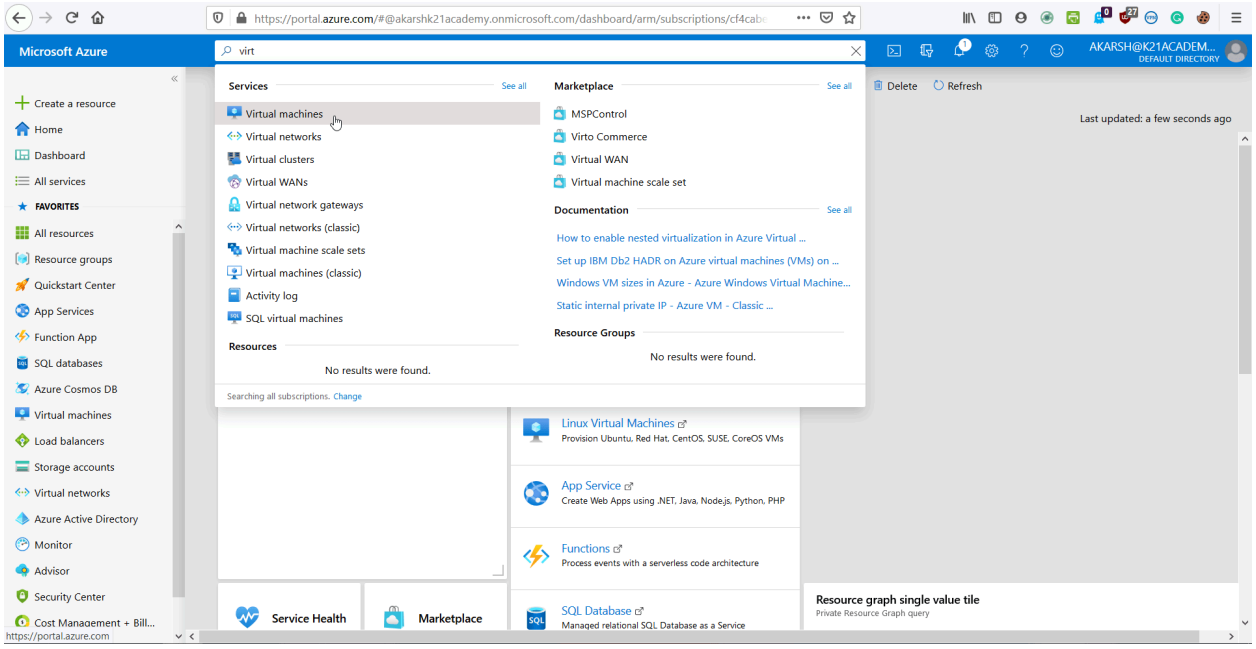


Thus, we have successfully connected to the AWS Linux EC2 Instance.

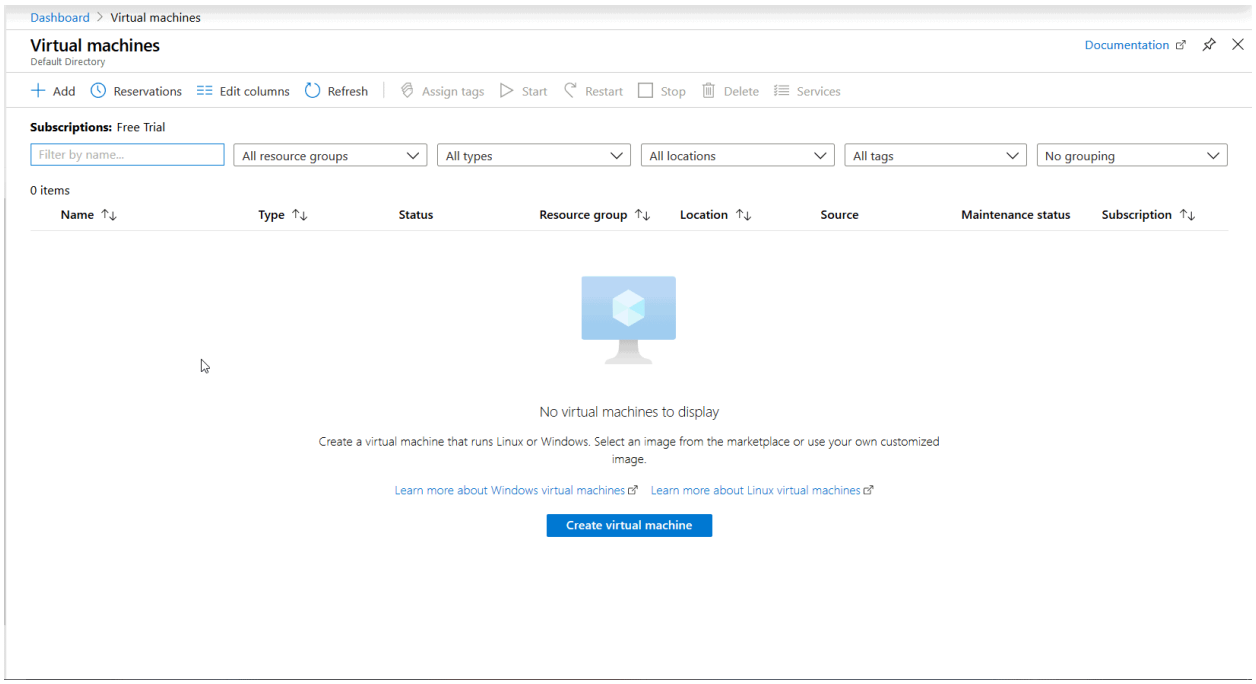
Creating An Ubuntu Virtual Machine on Azure

Step 1: In the **Azure portal**, search for Virtual Machine and select **Virtual Machine**.

Note: Please make sure you have a subscription before doing all this. If you created a free account for the first time, you'll already have a FREE TRIAL subscription for 1 month.



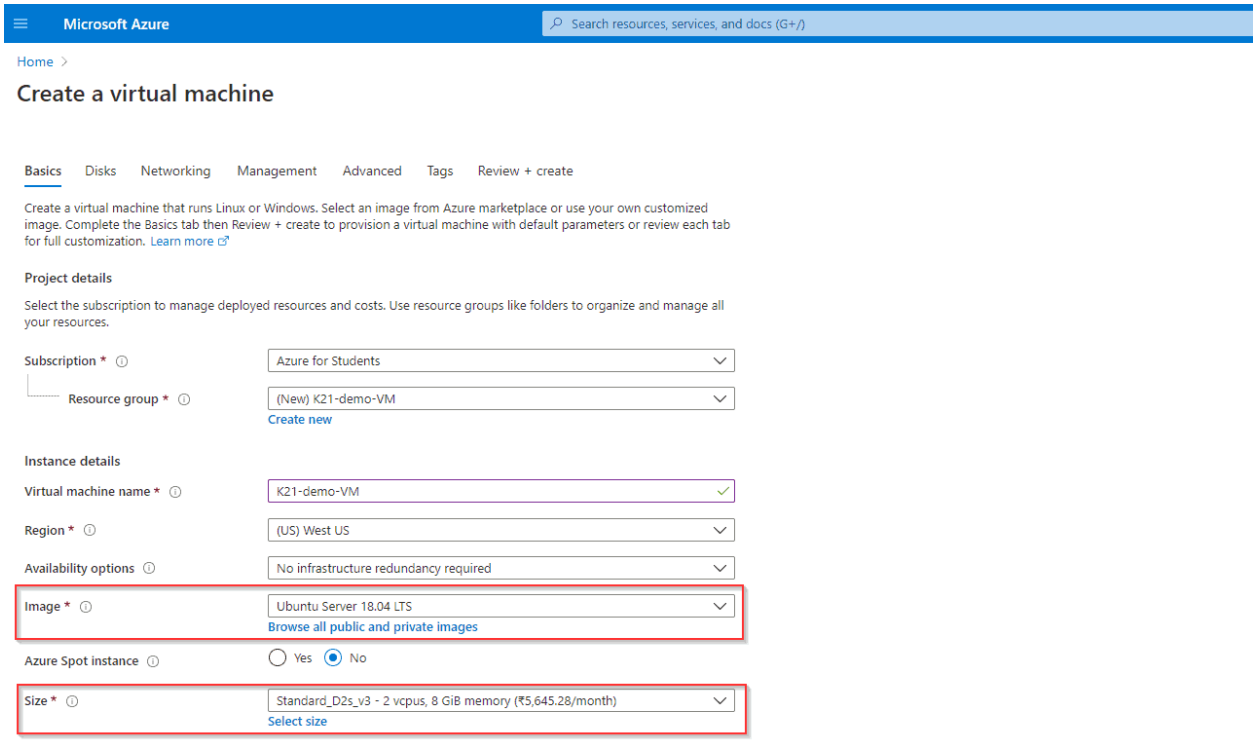
Step 2: Select **Add.**



Step 3: Enter the following values:

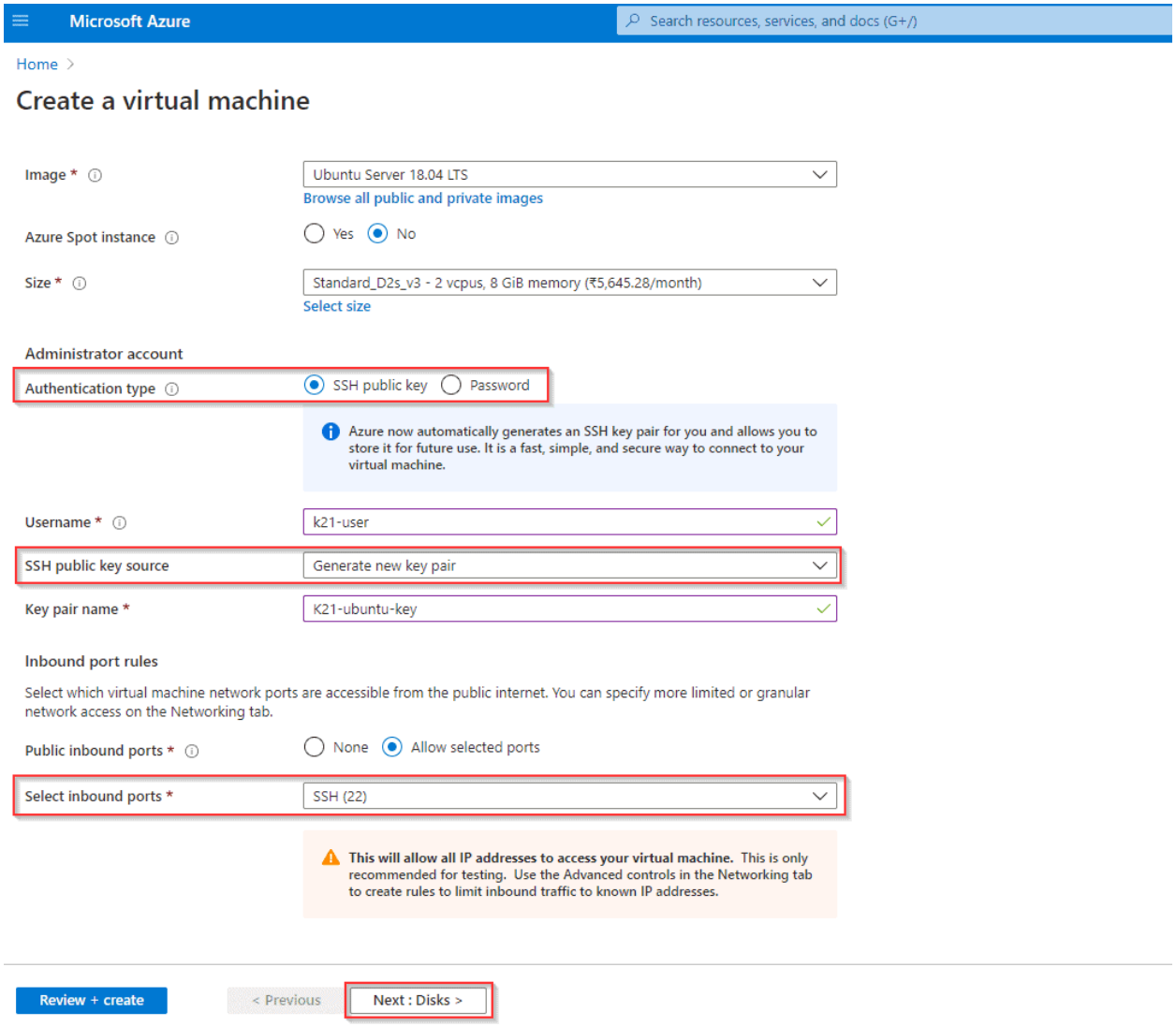
1. **Subscription**: Select your Azure subscription.
2. **Resource group**: Enter a new resource group name.

3. **Virtual Machine name**: It should be a **unique** name throughout the Azure network.
4. **Region**: Select an Azure location, such as **Western India, Central US, etc**.



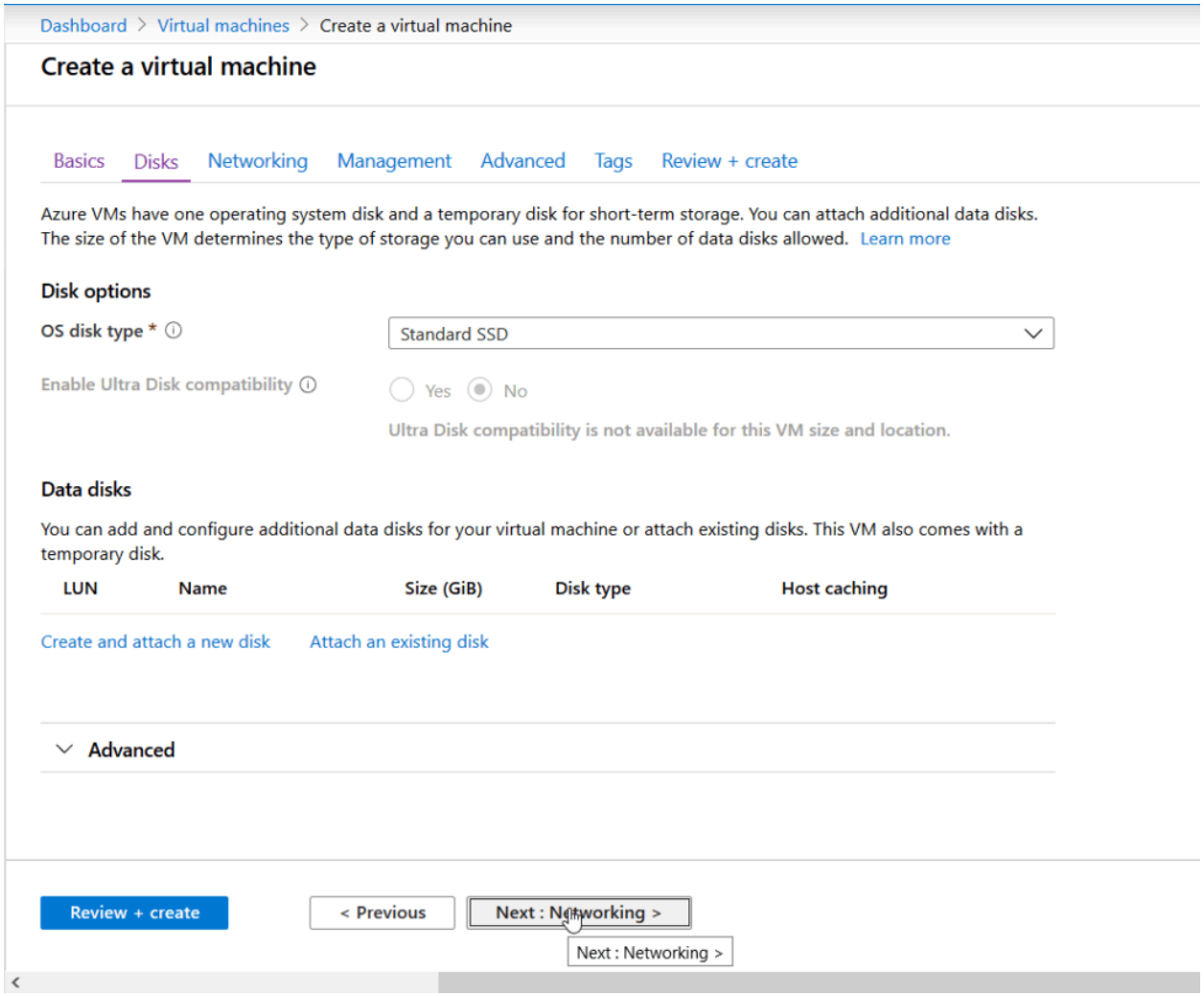
5. **Authentication Type:** SSH Public Key
6. **SSH Public Key Source:** Generate new key pair

7. **Select Inbound Ports:** SSH (**22**), this is the port that we will be using to connect to our Virtual Ubuntu Machine.



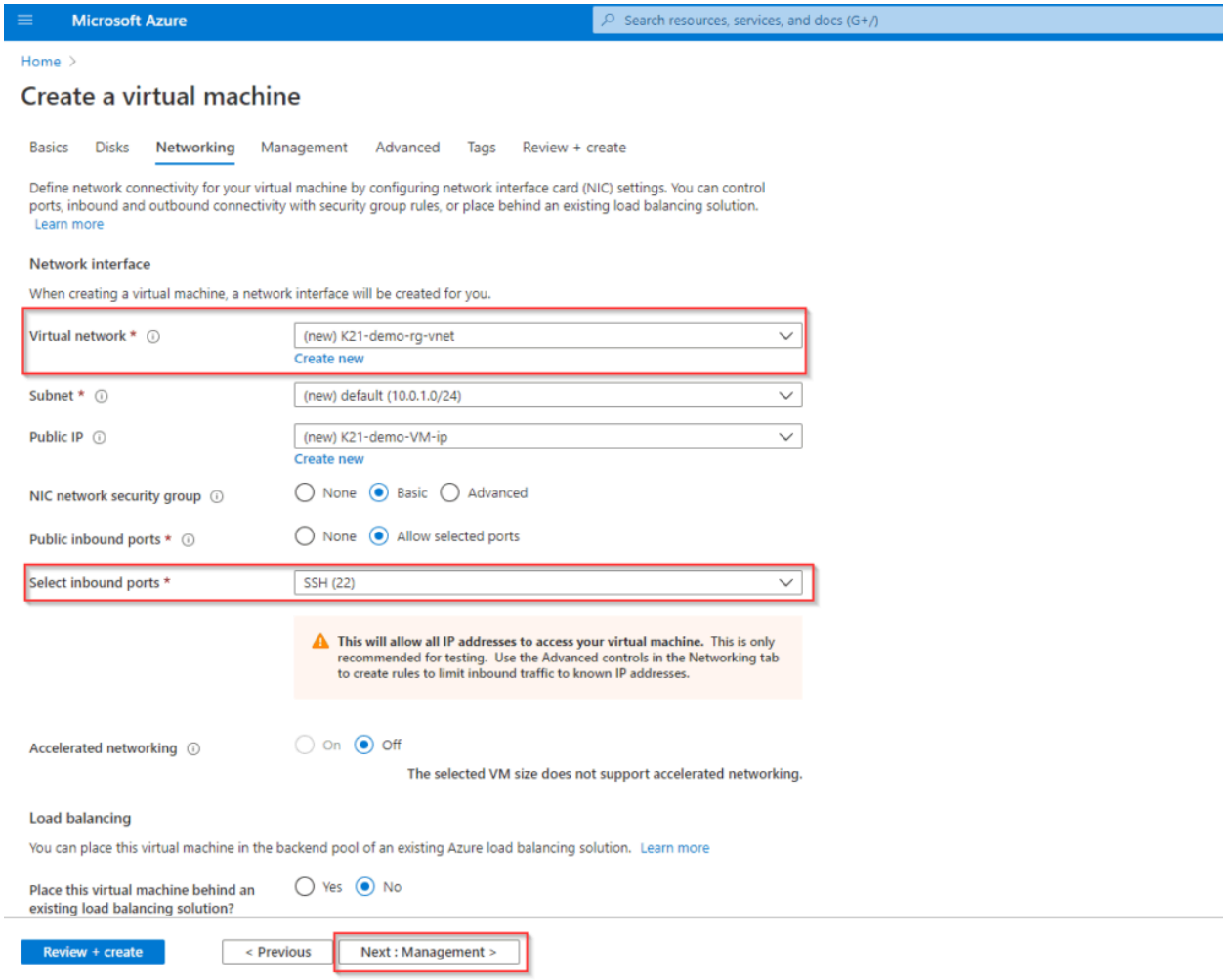
8. Select the Username and Key name as required and note them down as **we will need them later.**
9. Once done, click on Next: Disks >

Step 4: Select the type of disk you want to use. Click Next.



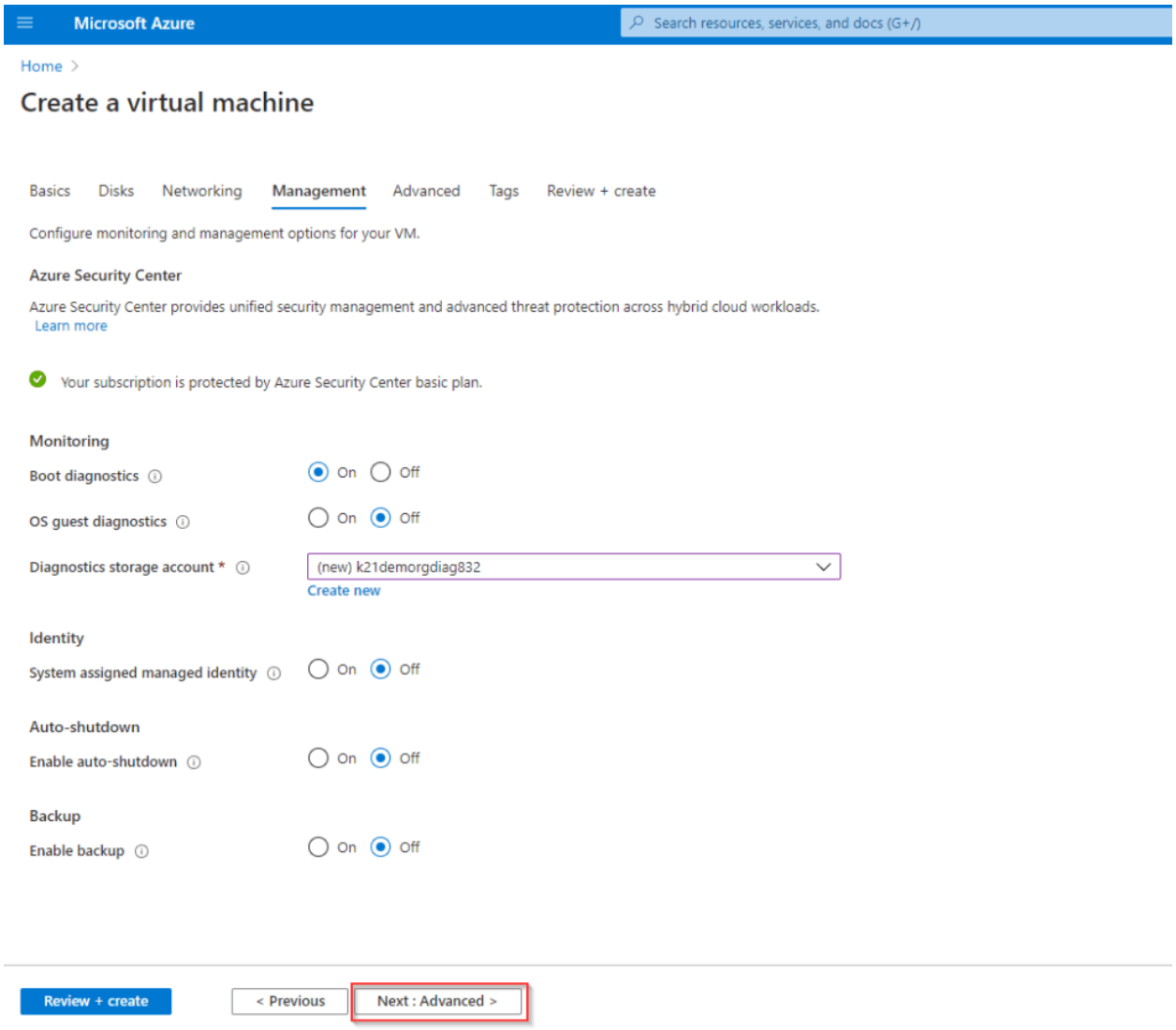
Step 5: Configure Networking

1. **Virtual Network:** Create a new one or use your existing Network.
2. **Select Inbound Ports:** SSH(22), This allows Port 22 to be opened in your Virtual Network for incoming traffic and will enable us to connect to our Virtual Machine inside our Virtual Network.
3. Leave everything else as default and click **next** to go to the Management Section.



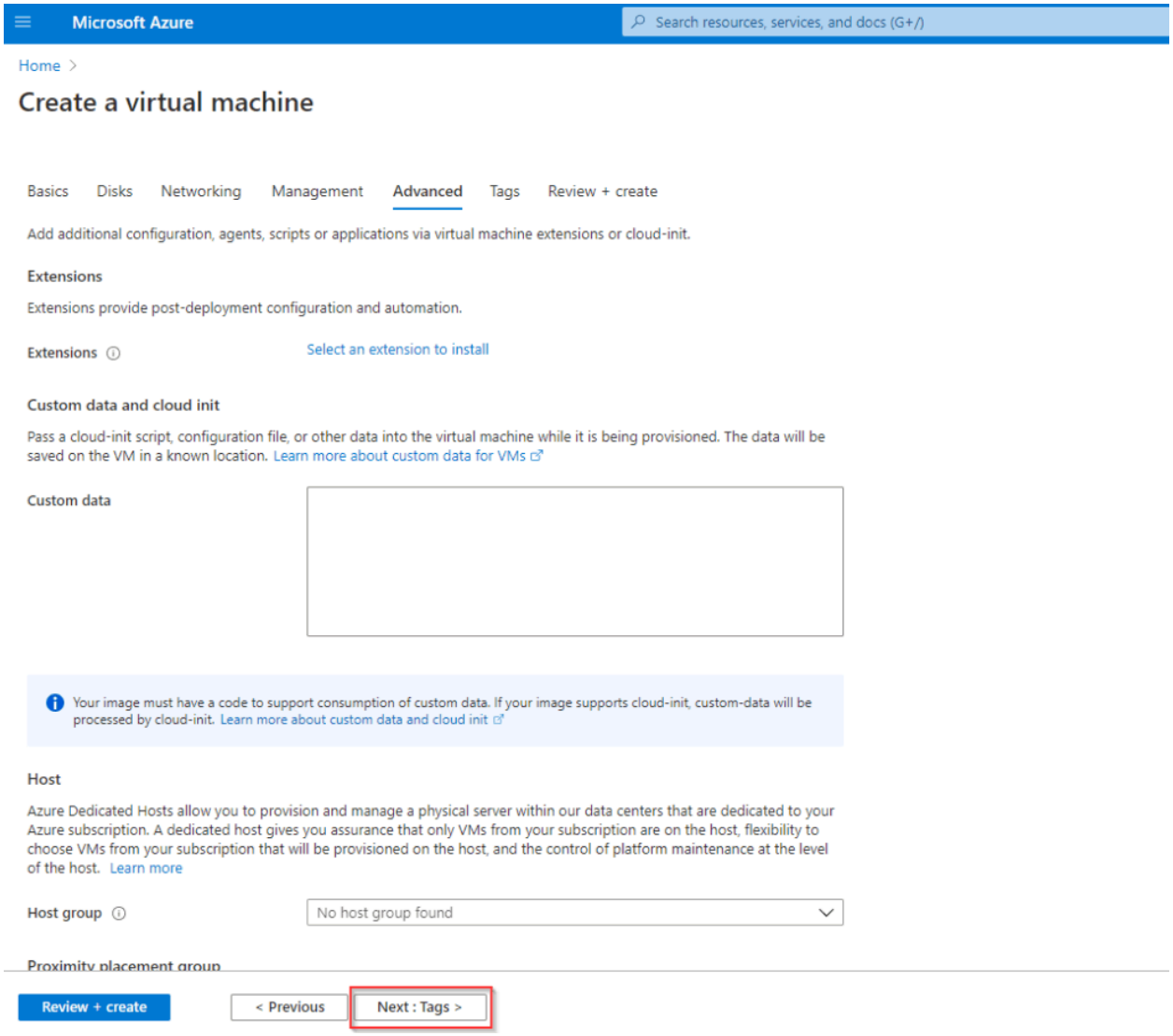
Step 6: Management

Leave all options as default and click on **next** to go to the Advanced Section.



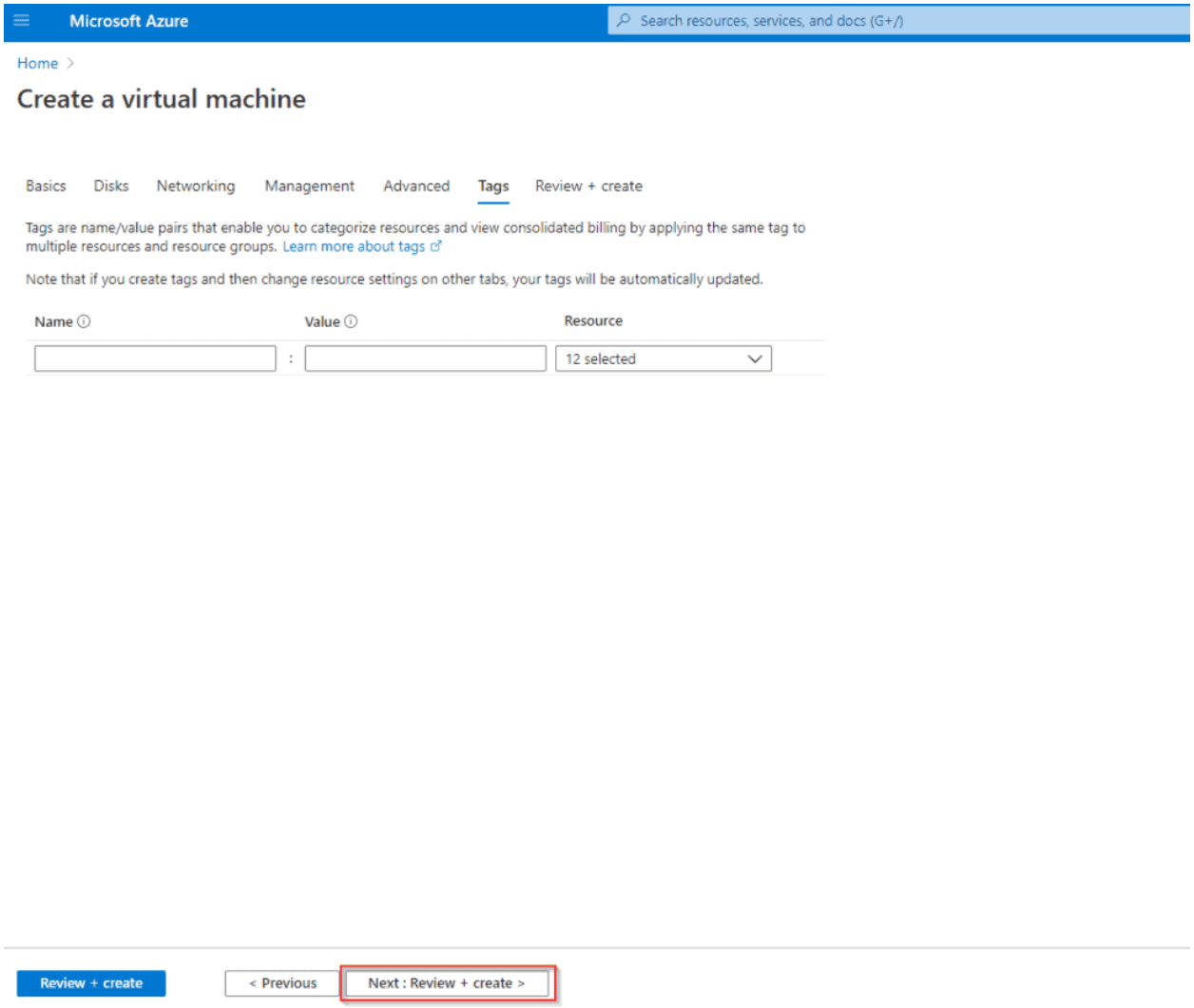
Step 7: Advanced Configuration

Add any custom data you want to run when the VM is being created or leave all options as default and click on **next** to go to the Tags Section.

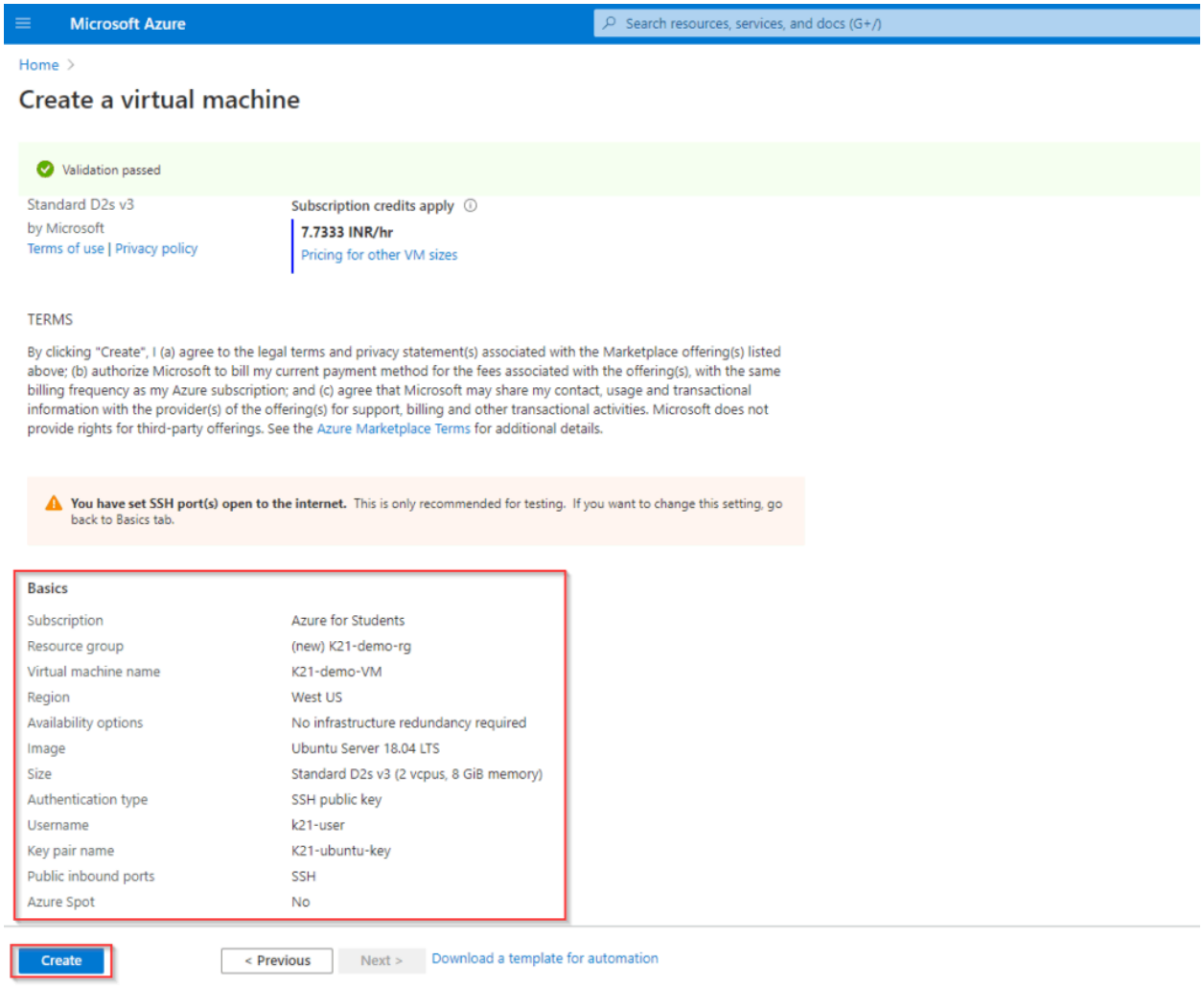


Step 8: Tags Configuration

Add any descriptive tags you would like to put to identify your VM at a later stage or leave Options at default and click on **next** to review and create your Virtual Machine.



Step 9: Review your settings and make any changes if required and select **Create**. It takes a few seconds to create a VM.



Step 10: SSH Keys

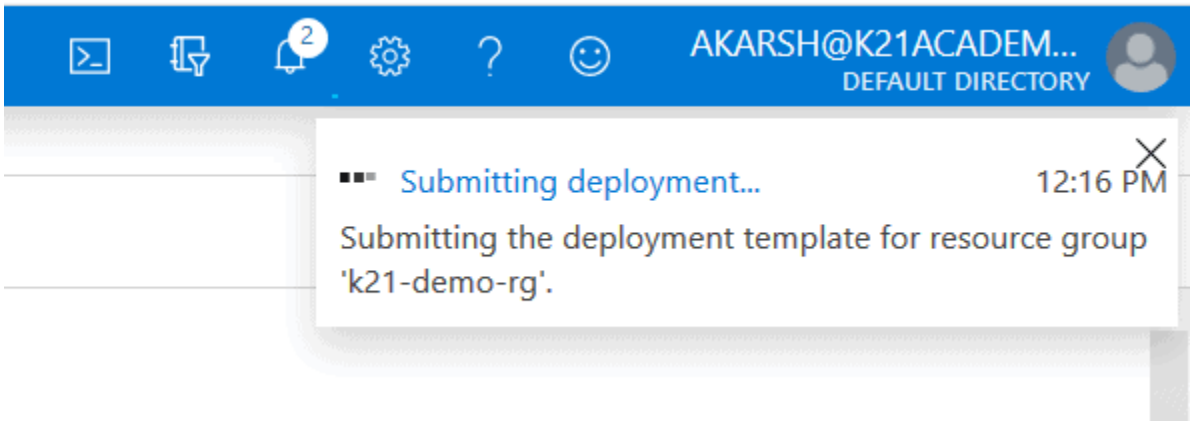
1. After you click on Create Azure will create an SSH Key Pair that we will be using to connect to our VM later. **Make sure to download the private key and keep it somewhere safe.**
2. Azure **does not** store your private key and this is the **only** instance when you will be able to access your private key from Azure.

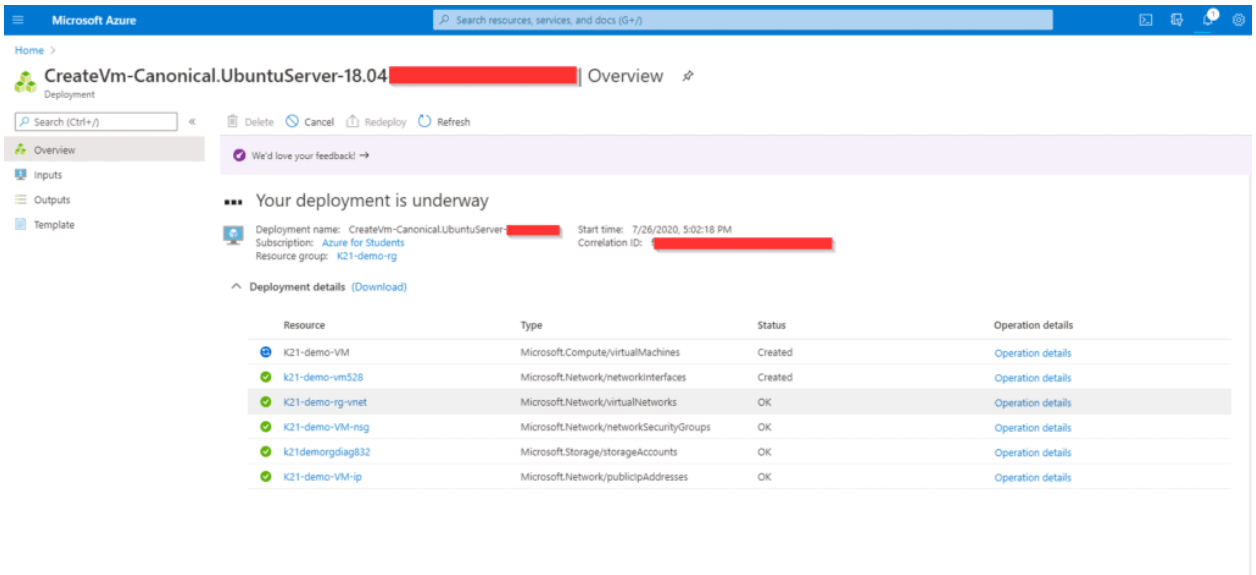
Generate new key pair

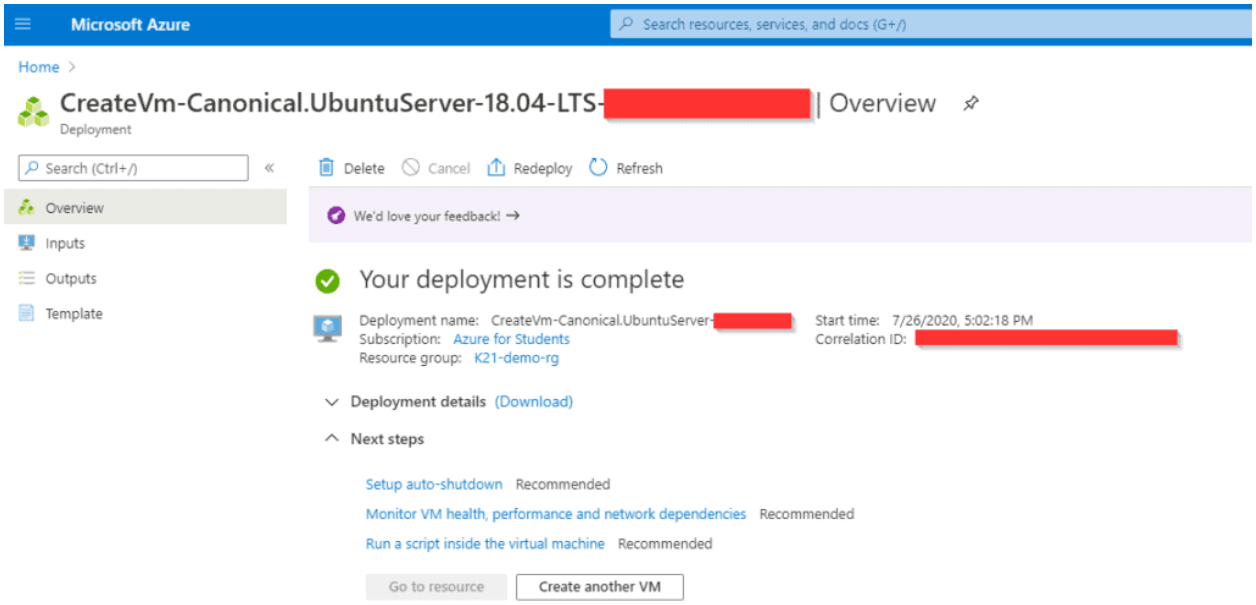
An SSH key pair contains both a public key and a private key. **Azure doesn't store the private key.** After the SSH key resource is created, you won't be able to download the private key again. Learn more

Download private key and create resource

Return to create a virtual machine







Connecting to Ubuntu Virtual Machine on Azure

As we have configured our VM to be accessible via SSH we will be using the PuTTY SSH client on our Windows machine.

You can download and install PuTTY from its **official** website. Simply select Download Putty and choose the appropriate installation file (32-bit or 64-bit as per your system) from the choices shown.

Package files

You probably want one of these. They include versions of all the PuTTY utilities.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

MSI ('Windows Installer')

32-bit:	putty-0.74-installer.msi	(or by FTP)	(signature)
64-bit:	putty-64bit-0.74-installer.msi	(or by FTP)	(signature)

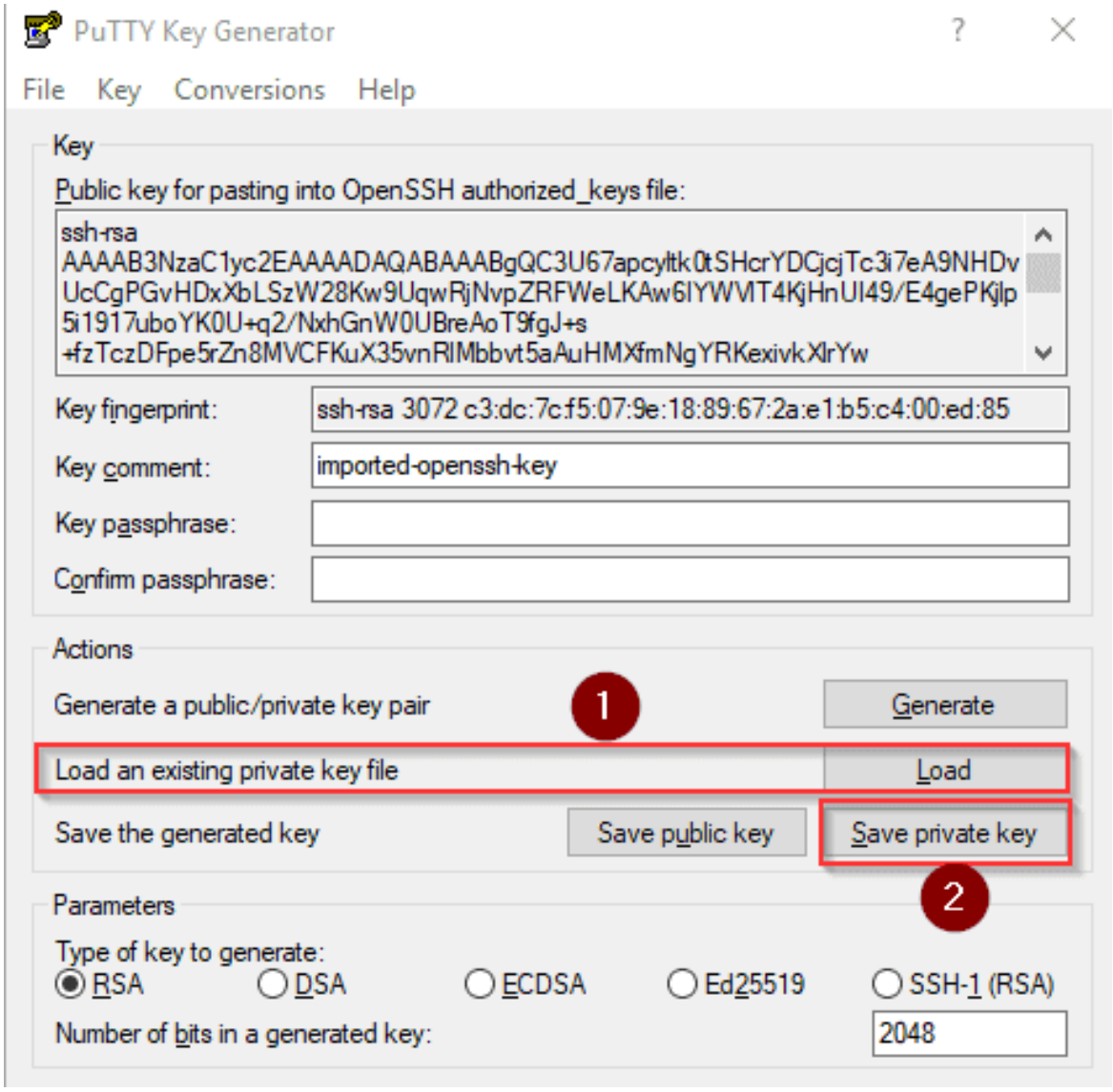
Unix source archive

.tar.gz:	putty-0.74.tar.gz	(or by FTP)	(signature)

Step 1: Converting our Private key into the proper extension.

The Azure private key we downloaded is in the (**.pem**) format, for using it with PuTTY we need to convert it into the (**.ppk)** format.

1. Open PuTTYgen, an application automatically installed alongside PuTTY.
2. Select load an **existing** private key. (make sure to select **All files** option while browsing to your **Azure Key**)
3. You will get an Operation successful message if the key was imported correctly.
4. Click on **Save Private Key** to save the key in a PuTTY usable format.
5. you can optionally set a password to be used with this key for further security but for this tutorial, we will be skipping that.

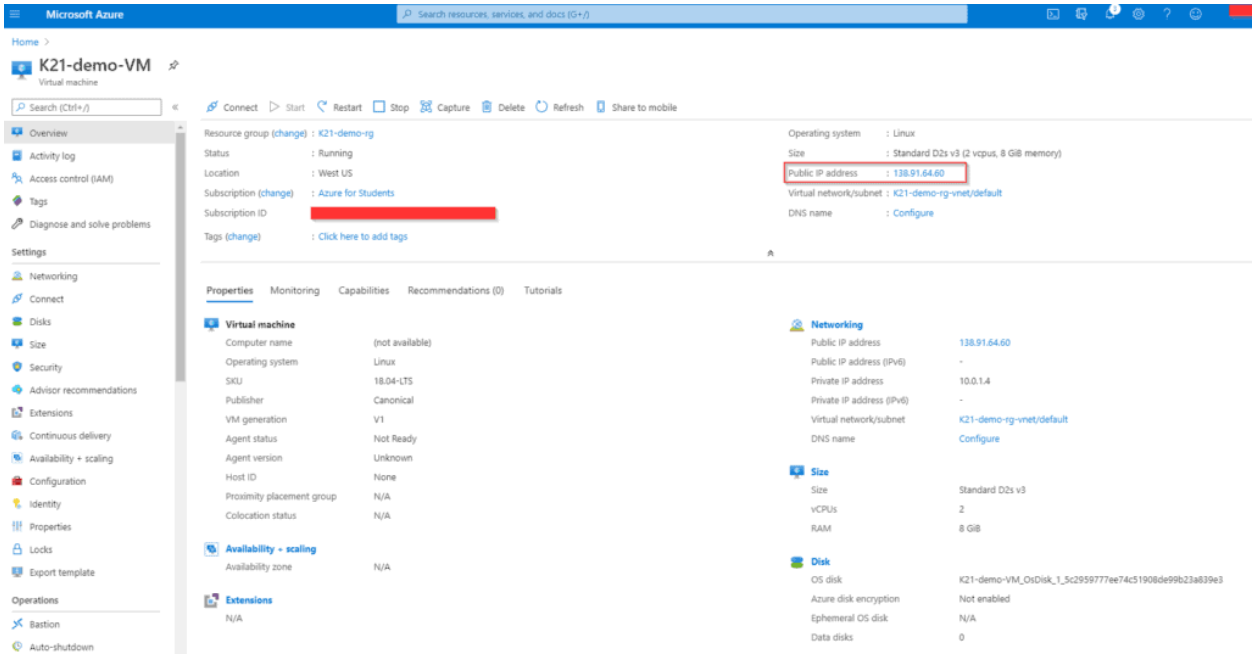


Also Check: Az 104 Microsoft Azure Administrator: PDF Documentation & Tutorial. Click here

Step 2: Getting the SSH connection information.

1. Go to the VM dashboard
2. Select your VM
3. Note the **public IP address.**

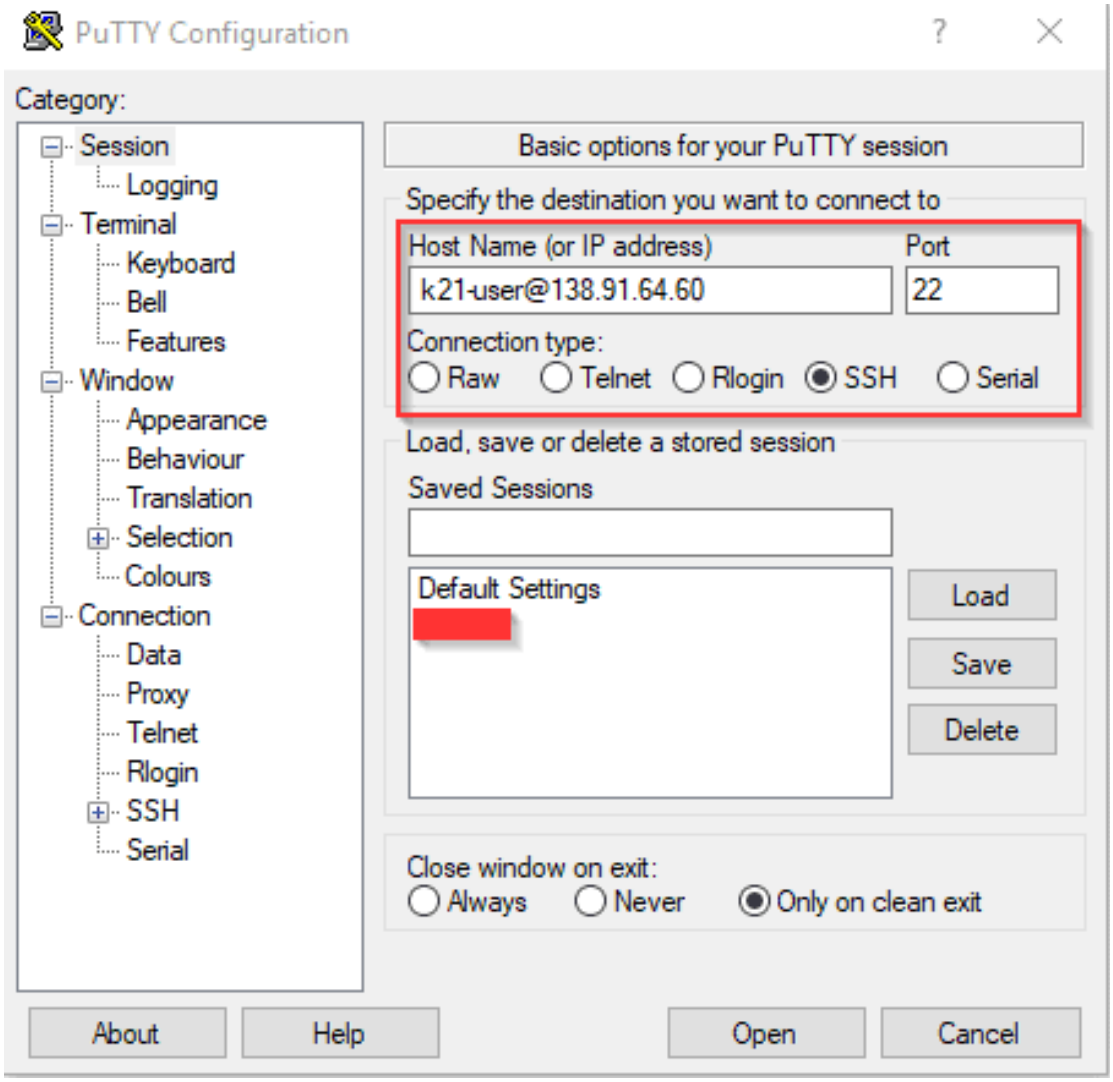
Note: every time the VM is restarted, this IP will be **Different,** unless you have an **Elastic IP** configured for your VM.



Also Read: Our blog post on Vnet Peering Azure. Click here

Step 3: Open the PuTTY installation on your Windows Machine.

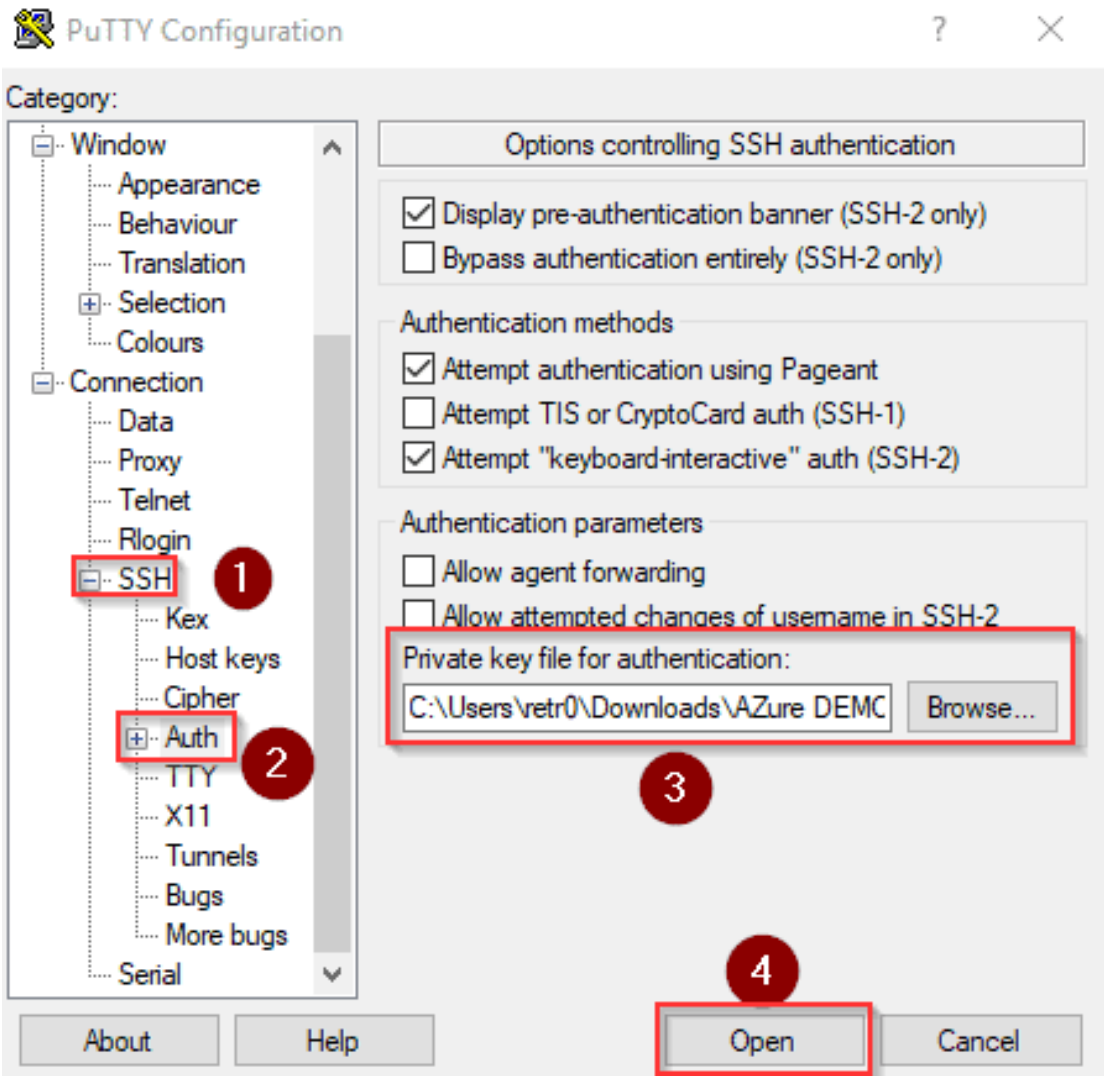
1. Enter the Host Name details in the following format: <**Username of VM**>@<**Public IP of VM**>
2. Make sure Port is **22.**
3. The connection type is **SSH.**



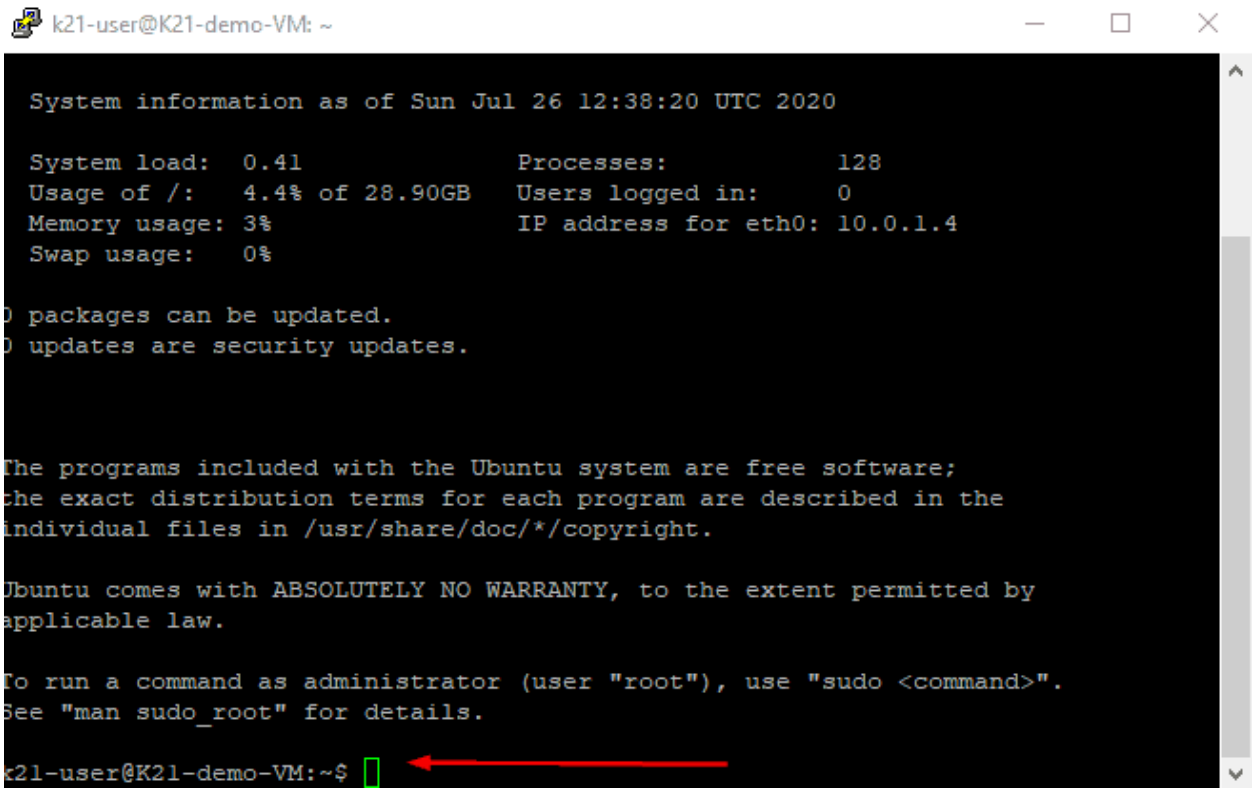
Also Check az 104 vs az 103: to know the major differences between them.

Step 4: Inserting our SSH key for authentication.

1. Expand the **SSH** option under Connection in the sidebar.
2. Select **Auth, Do not expand it.**
3. Leave all options at default settings and under private key file for authentication, browse to the **Private Key** we had **created from PuTTYgen** earlier.
4. Click Open.
5. Click yes in the security alert box to allow the remote connection.



If all the steps were done correctly then the connection will be successful and you will be logged into your Ubuntu Virtual Machine.



(Optional) Creating a VM on Google Cloud Compute

Watch [this video]() to learn the step-by-step instructions of Google Cloud Compute, or explore the framework yourself.