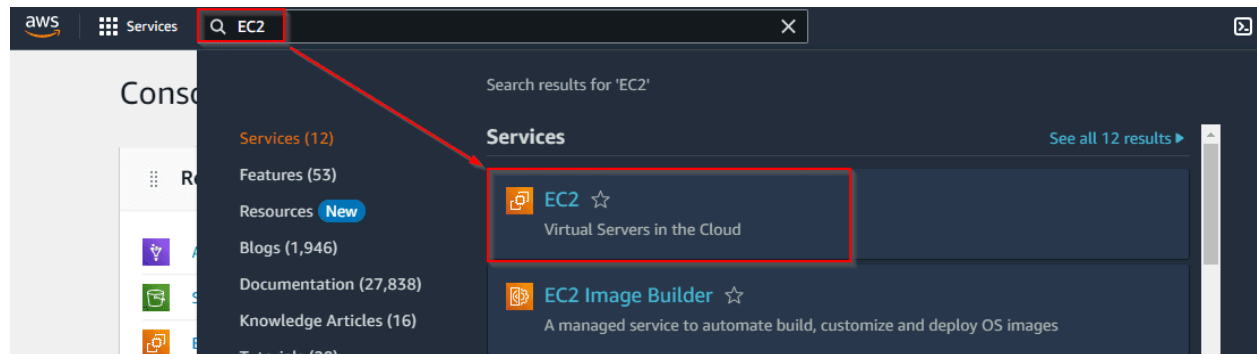
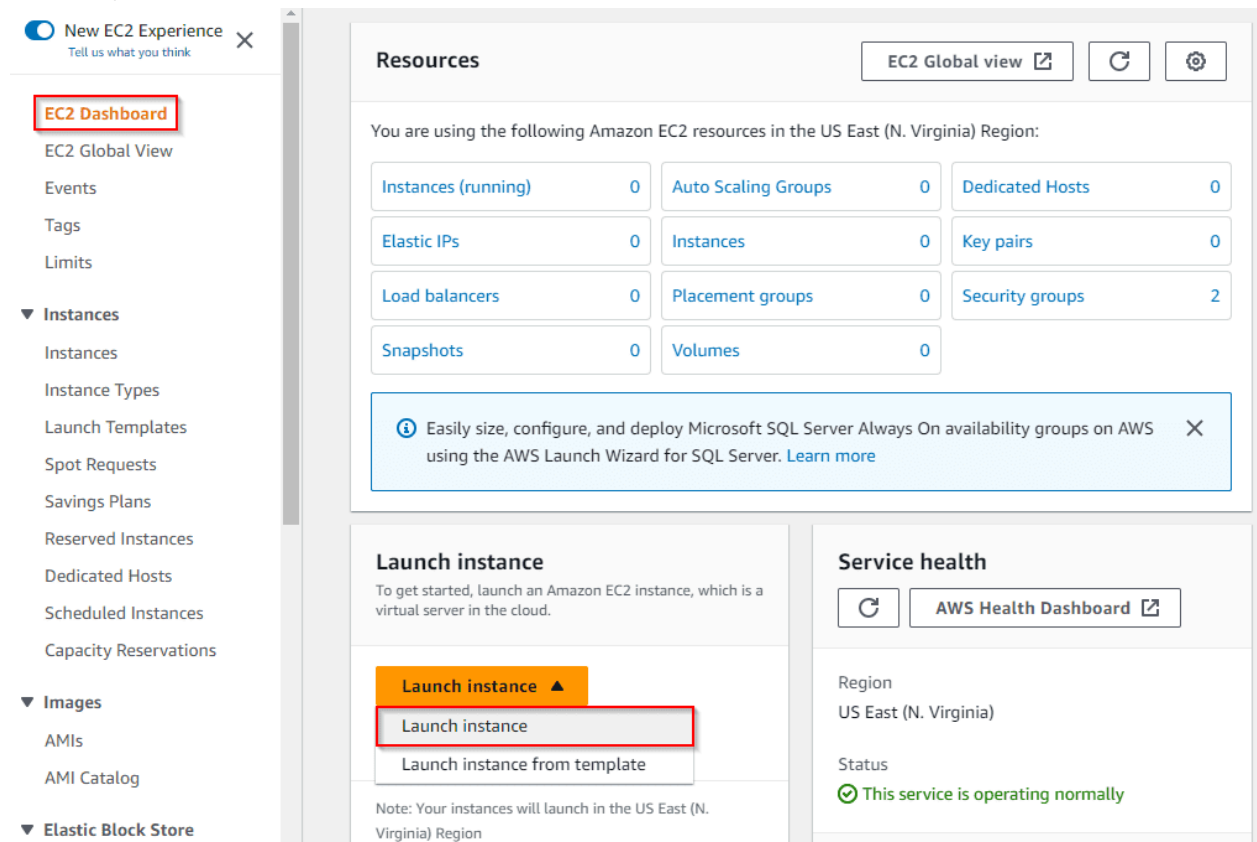


Creating A Linux EC2 Instance

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.

[EC2](#) > [Instances](#) > Launch an instance

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

Webserver

[Add additional tags](#)

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

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

S

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

Free tier eligible ▼

ami-06e46074ae430fba6 (64-bit (x86), uefi-preferred) / ami-085a3abb84068d568 (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.0.20230329.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	
64-bit (x86) ▼	uefi-preferred	ami-06e46074ae430fba6	Verified provider

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.

▼ Instance type [Info](#)

Instance type ☑ All generations

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

Q |

t1.micro Free tier eligible
Family: t1 1 vCPU 0.612 GiB Memory Current generation: false
On-Demand Linux pricing: 0.02 USD per Hour
On-Demand SUSE pricing: 0.02 USD per Hour
On-Demand RHEL pricing: 0.08 USD per Hour
On-Demand Windows pricing: 0.02 USD per Hour

t2.nano
Family: t2 1 vCPU 0.5 GiB Memory Current generation: true
On-Demand Linux pricing: 0.0058 USD per Hour
On-Demand SUSE pricing: 0.0058 USD per Hour
On-Demand Windows pricing: 0.0081 USD per Hour

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

t2.small
Family: t2 1 vCPU 2 GiB Memory Current generation: true
On-Demand Windows pricing: 0.032 USD per Hour
On-Demand Linux pricing: 0.023 USD per Hour

[Compare instance types](#)

selected key pair before you launch

[Create new key pair](#)

[Edit](#)

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.

▼ **Network settings** [Info](#)

Edit

Network [Info](#)

vpc-09552cad50650a75c | Default VPC

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called '**launch-wizard-1**' with the following rules:



☒ Allow SSH traffic from
Helps you connect to your instance

Anywhere

0.0.0.0/0

☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

 Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. 

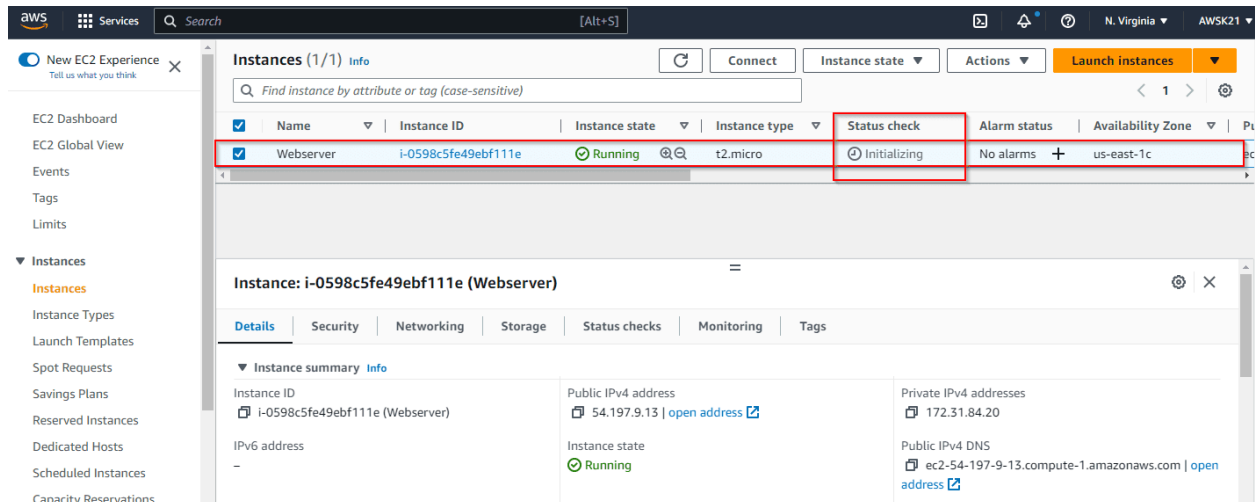
8. Now review all the things you have Configured and Click on **Launch Instance**.

The screenshot shows the 'Launch Instance' wizard in the AWS Management Console. The 'Network settings' tab is active on the left, showing configuration for a new VPC (vpc-09552cad50650a75c) and subnet (No preference). The 'Firewall (security groups)' section has 'Create security group' selected, and a new group named 'launch-wizard-1' is being created with rules for SSH, HTTPS, and HTTP traffic. A warning message states: 'Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.' The 'Summary' tab on the right shows the instance configuration: 1 instance, Amazon Linux 2023 AMI (ami-06e46074ae430fba6), t2.micro instance type, new security group, and 1 volume (8 GiB). A 'Free tier' notification is visible. At the bottom right, the 'Launch instance' button is highlighted with a red arrow, and the 'Cancel' button is also visible.

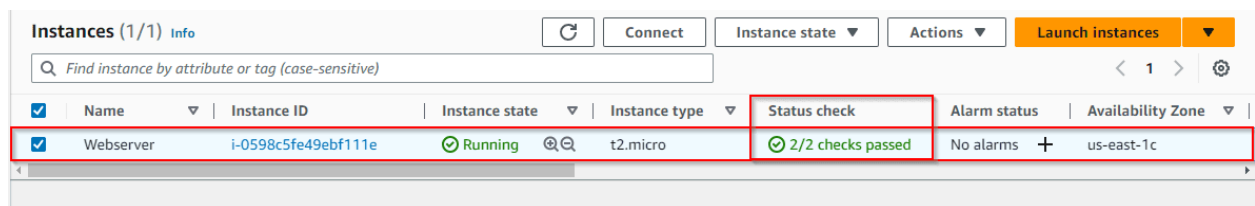
9. Now, scroll down and click on **View All Instances**.

The screenshot shows the 'View All Instances' page in the AWS Management Console. It features four main sections: 'Manage detailed monitoring', 'Create Load Balancer', 'Create AWS budget', and 'Manage CloudWatch alarms'. Each section has a brief description and a button to manage or create the respective resource. At the bottom right, the 'View all instances' button is highlighted with a red arrow.

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.

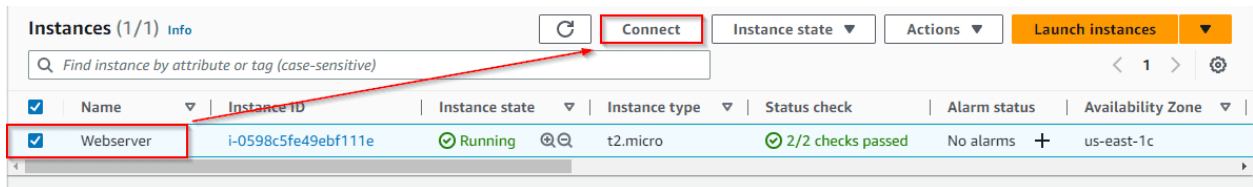
Note: Now we have launched the instance successfully, further we need to access the instance so, we have two ways of accessing an instance-

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**.

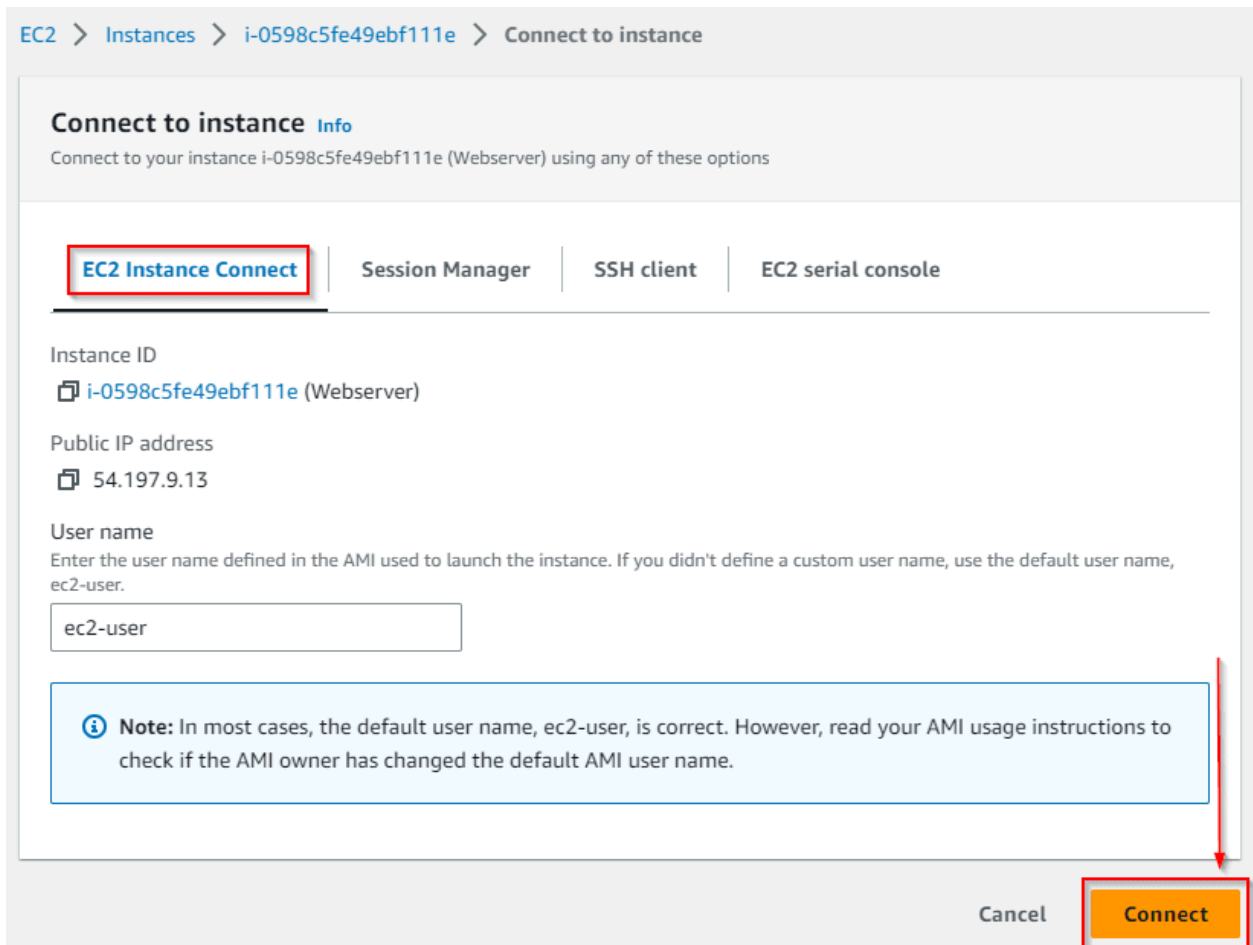


Instances (1/1) Info

Find instance by attribute or tag (case-sensitive)

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	Webserver	i-0598c5fe49ebf111e	Running	t2.micro	2/2 checks passed	No alarms	us-east-1c

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



EC2 > Instances > i-0598c5fe49ebf111e > Connect to instance

Connect to instance Info

Connect to your instance i-0598c5fe49ebf111e (Webserver) using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID
i-0598c5fe49ebf111e (Webserver)

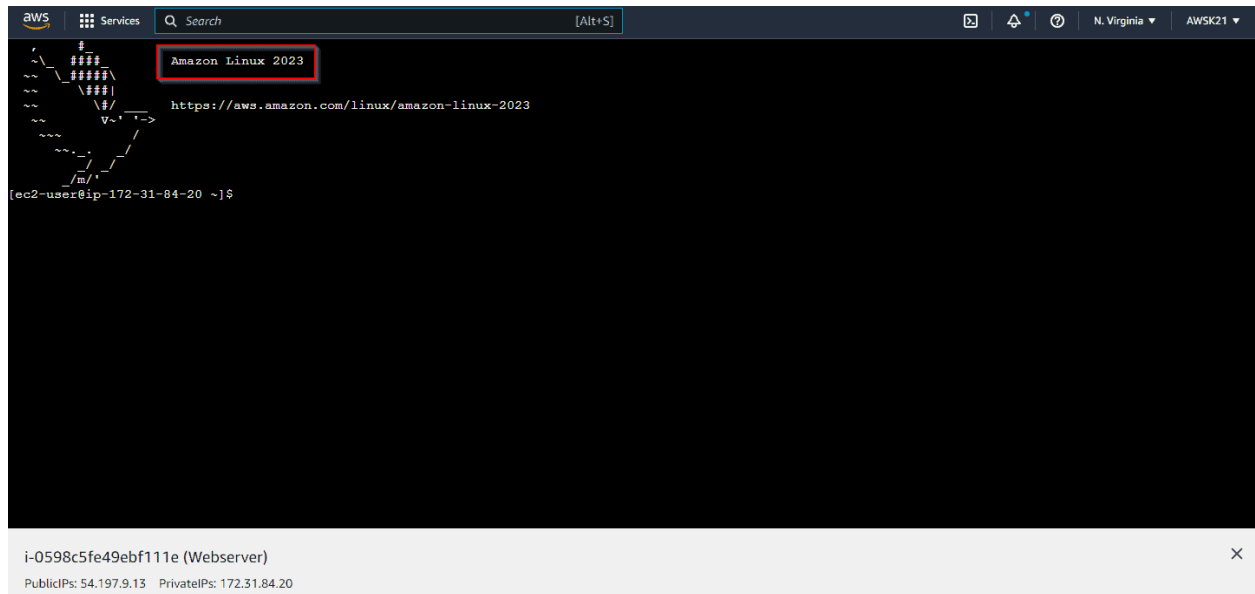
Public IP address
54.197.9.13

User name
Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.
ec2-user

Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel **Connect**

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

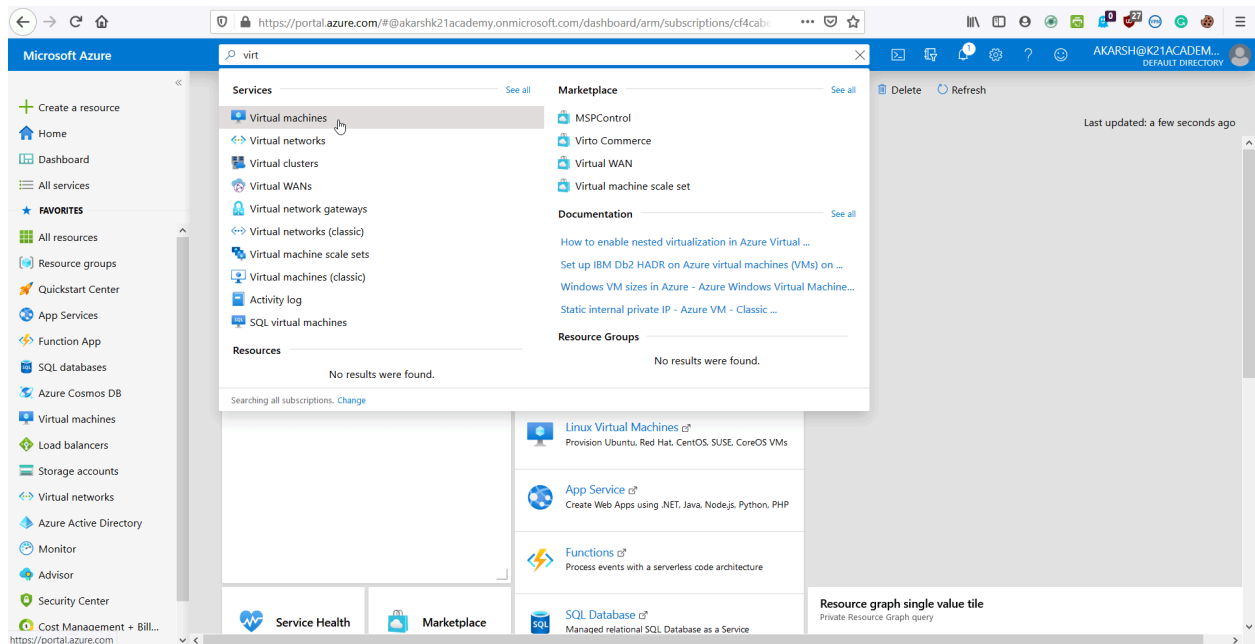


Thus, we have successfully connected to the AWS Linux EC2 Instance.

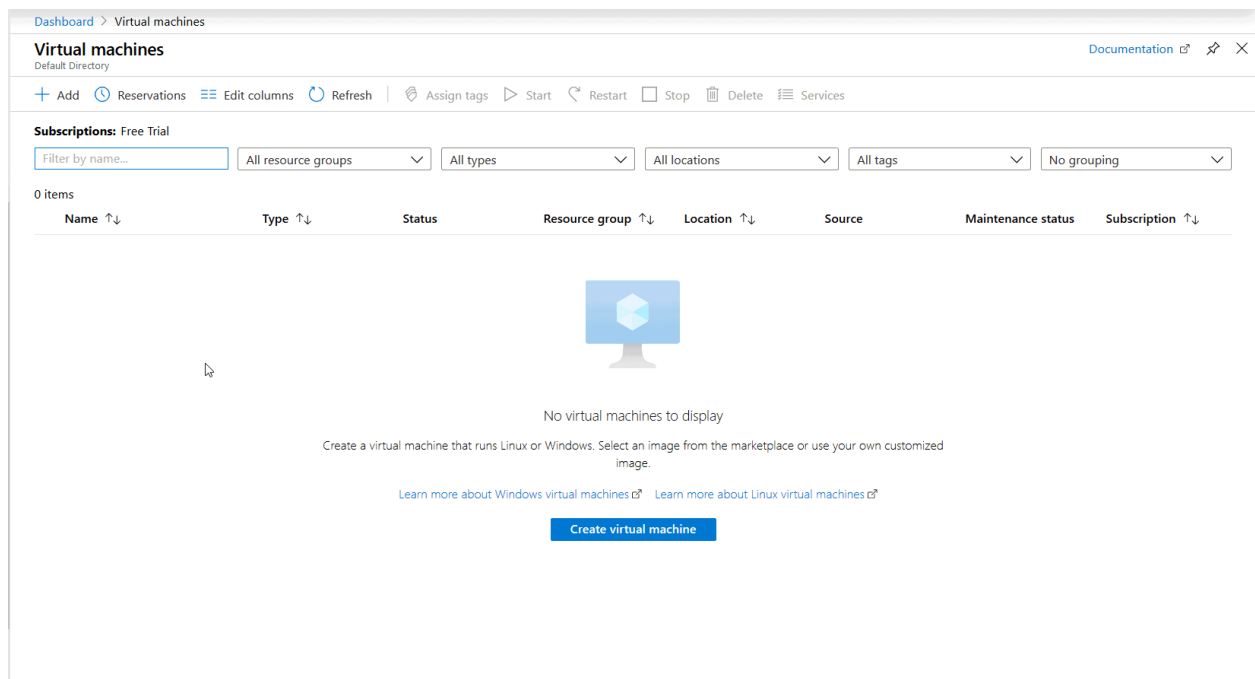
Creating An Ubuntu Virtual Machine on Azure

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.**

Microsoft Azure Search resources, services, and docs (G+)

Home >

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

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) K21-demo-VM [Create new](#)

Instance details

Virtual machine name * ⓘ K21-demo-VM ✓

Region * ⓘ (US) West US

Availability options ⓘ No infrastructure redundancy required

Image * ⓘ Ubuntu Server 18.04 LTS [Browse all public and private images](#)

Azure Spot instance ⓘ ☐ Yes ☒ No

Size * ⓘ Standard_D2s_v3 - 2 vcpus, 8 GiB memory (₹5,645.28/month) [Select size](#)

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.

Microsoft Azure

Home >

Create a virtual machine

Image * ⓘ Ubuntu Server 18.04 LTS
[Browse all public and private images](#)

Azure Spot instance ⓘ ☐ Yes ☒ No

Size * ⓘ Standard_D2s_v3 - 2 vcpus, 8 GiB memory (₹5,645.28/month)
[Select size](#)

Administrator account

Authentication type ⓘ ☒ SSH public key ☐ Password

ℹ 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 * ⓘ k21-user ✓

SSH public key source Generate new key pair ✓

Key pair name * K21-ubuntu-key ✓

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

Select inbound ports * SSH (22) ✓

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

[Review + create](#) [< Previous](#) [Next : Disks >](#)

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.

Dashboard > Virtual machines > Create a virtual machine

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type * ⓘ Standard SSD

Enable Ultra Disk compatibility ⓘ ☐ Yes ☒ No

Ultra Disk compatibility is not available for this VM size and location.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
-----	------	------------	-----------	--------------

[Create and attach a new disk](#) [Attach an existing disk](#)

Advanced

Review + create

< Previous

Next : Networking >

Next : Networking >

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.

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) >

Create a virtual machine

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ

(new) K21-demo-rg-vnet

Create new

Subnet * ⓘ

(new) default (10.0.1.0/24)

Public IP ⓘ

(new) K21-demo-VM-ip

Create new

NIC network security group ⓘ

☐ None ☒ Basic ☐ Advanced

Public inbound ports * ⓘ

☐ None ☒ Allow selected ports

Select inbound ports *

SSH (22)

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Accelerated networking ⓘ

☐ On ☒ Off

The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution?

☐ Yes ☒ No

Review + create

< Previous

Next : Management >

Step 6: Management

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

Microsoft Azure

Search resources, services, and docs (G+/)

[Home](#) >

Create a virtual machine

BasicsDisksNetworkingManagementAdvancedTagsReview + create

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
[Learn more](#)

✔ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ ☒ On ☐ Off

OS guest diagnostics ⓘ ☐ On ☒ Off

Diagnostics storage account * ⓘ

(new) k21demorgdiag832

[Create new](#)

Identity

System assigned managed identity ⓘ ☐ On ☒ Off

Auto-shutdown

Enable auto-shutdown ⓘ ☐ On ☒ Off

Backup

Enable backup ⓘ ☐ On ☒ Off

Review + create

< Previous

Next : Advanced >

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.

Microsoft Azure

Search resources, services, and docs (G+/)

Home >

Create a virtual machine

BasicsDisksNetworkingManagementAdvancedTagsReview + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ[Select an extension to install](#)

Custom data and cloud init

Pass a cloud-init script, configuration file, or other data into the virtual machine while it is being provisioned. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#)

Custom data

Your image must have a code to support consumption of custom data. If your image supports cloud-init, custom-data will be processed by cloud-init. [Learn more about custom data and cloud init](#)

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

Host group ⓘ

No host group found

Proximity placement group

Review + create

< Previous

Next : Tags >

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.

Microsoft Azure

Search resources, services, and docs (G+/I)

[Home](#) >

Create a virtual machine

Basics Disks Networking Management Advanced **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ	Value ⓘ	Resource
<input type="text"/>	:	<input type="text" value="12 selected"/> ▼

Review + create

< Previous

Next : Review + create >

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

Microsoft Azure

Search resources, services, and docs (G+)

Home >

Create a virtual machine

✓ Validation passed

Standard D2s v3
by Microsoft
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ

7.7333 INR/hr
[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

⚠ You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Subscription	Azure for Students
Resource group	(new) K21-demo-rg
Virtual machine name	K21-demo-VM
Region	West US
Availability options	No infrastructure redundancy required
Image	Ubuntu Server 18.04 LTS
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Authentication type	SSH public key
Username	k21-user
Key pair name	K21-ubuntu-key
Public inbound ports	SSH
Azure Spot	No

Create

< Previous

Next >

[Download a template for automation](#)

Step 10: SSH Keys

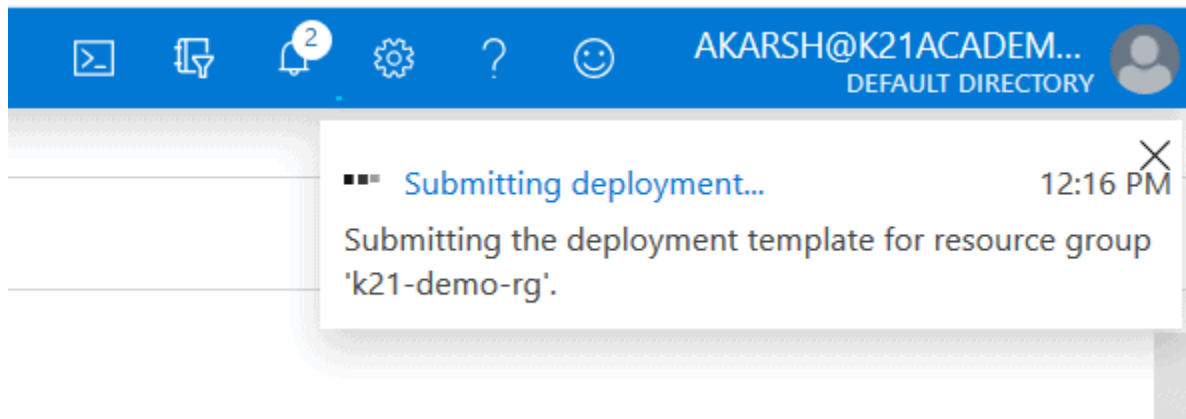
1. After you click on Create Azure will create an SSH Key Pair that we will be using to connect to our VM later. **Make sure to download the private key and keep it somewhere safe.**
2. Azure **does not** store your private key and this is the **only** instance when you will be able to access your private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

Generate new key pair

i 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](#)



Microsoft Azure

Search resources, services, and docs (G+)

Home > CreateVm-Canonical.UbuntuServer-18.04 Overview

Deployment

Search (Ctrl+F) < Delete Cancel Redeploy Refresh

We'd love your feedback! →

... Your deployment is underway

Deployment name: CreateVm-Canonical.UbuntuServer- Start time: 7/26/2020, 5:02:18 PM
Subscription: Azure for Students Correlation ID:
Resource group: K21-demo-rg

Deployment details (Download)

Resource	Type	Status	Operation details
K21-demo-VM	Microsoft.Compute/virtualMachines	Created	Operation details
k21-demo-vm528	Microsoft.Network/networkInterfaces	Created	Operation details
K21-demo-rg-vnet	Microsoft.Network/virtualNetworks	OK	Operation details
K21-demo-VM-nsg	Microsoft.Network/networkSecurityGroups	OK	Operation details
k21demorgdiag32	Microsoft.Storage/storageAccounts	OK	Operation details
K21-demo-VM-ip	Microsoft.Network/publicIPAddresses	OK	Operation details

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header with the Microsoft Azure logo and a search bar. Below the header, the breadcrumb 'Home >' is visible. The main content area displays the deployment 'CreateVm-Canonical.UbuntuServer-18.04-LTS' with a redacted ID. The deployment is in a 'Complete' state, indicated by a green checkmark and the message 'Your deployment is complete'. The deployment details show the name, subscription ('Azure for Students'), resource group ('K21-demo-rg'), start time ('7/26/2020, 5:02:18 PM'), and correlation ID (redacted). A sidebar on the left contains navigation links for Overview, Inputs, Outputs, and Template. Below the deployment status, there are recommended next steps: 'Setup auto-shutdown', 'Monitor VM health, performance and network dependencies', and 'Run a script inside the virtual machine'. At the bottom, there are two buttons: 'Go to resource' and 'Create another VM'.

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](#) [\(or by FTP\)](#) [\(signature\)](#)

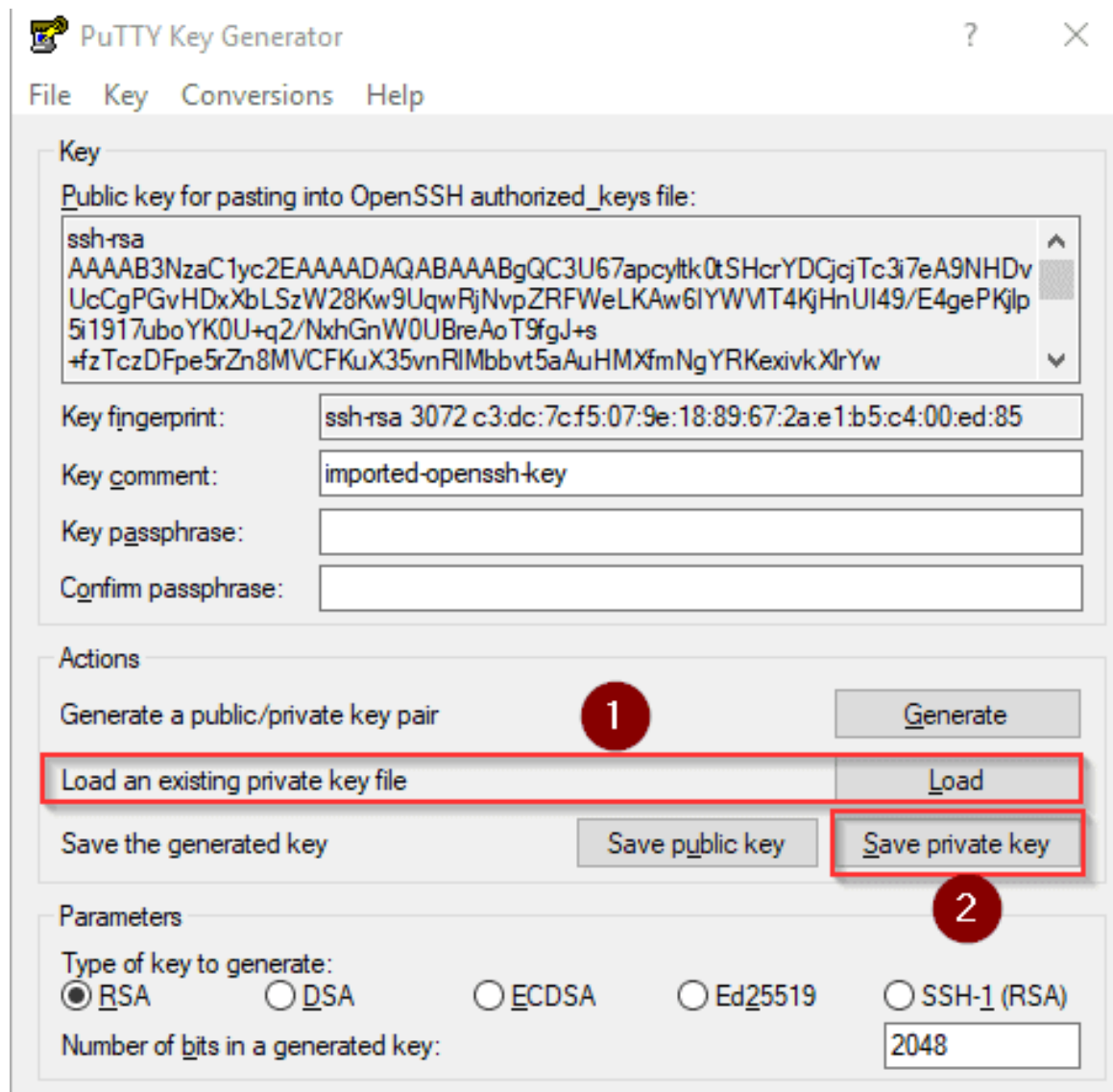
Unix source archive

.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**.

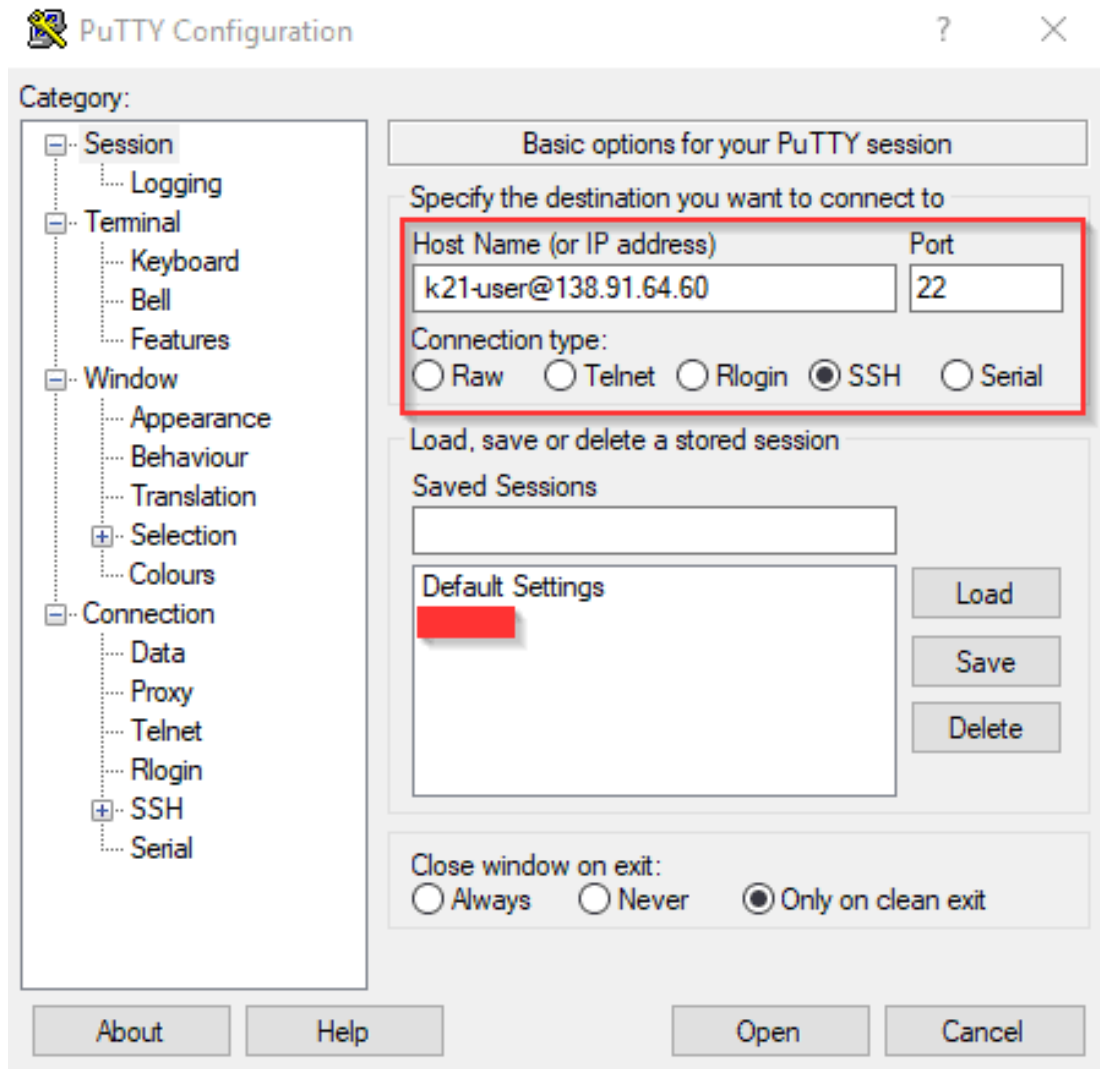
Note: every time the VM is restarted, this IP will be **Different**, unless you have an **Elastic IP** configured for your VM.

The screenshot displays the Microsoft Azure portal interface for a virtual machine named 'K21-demo-VM'. The left sidebar contains navigation options such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Disks, Size, Security, Advisor recommendations, Extensions, Continuous delivery, Availability + scaling, Configuration, Identity, Properties, Locks, Export template, Operations, Bastion, and Auto-shutdown. The main content area shows the VM's overview, including its resource group (K21-demo-rg), status (Running), location (West US), and subscription (Azure for Students). A red box highlights the public IP address, 138.91.64.60. Below this, the 'Properties' tab is selected, showing details like computer name, operating system (Linux), SKU (18.04-LTS), publisher (Canonical), VM generation (V1), agent status (Not Ready), agent version (Unknown), host ID, proximity placement group (N/A), and colocation status (N/A). The 'Availability + scaling' section shows the availability zone (N/A). The 'Extensions' section is also visible. On the right, the 'Networking' section shows the public IP address (138.91.64.60), private IP address (10.0.1.4), and virtual network/subnet (K21-demo-rg-vnet/default). The 'Size' section shows the VM size (Standard D2s v3) with 2 vCPUs and 8 GiB of RAM. The 'Disk' section shows the OS disk (K21-demo-VM_OsDisk_1_5c2959777ee74c51908de99b23a839e3) and its properties.

Also Read: Our blog post on [Vnet Peering Azure](#). Click here

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

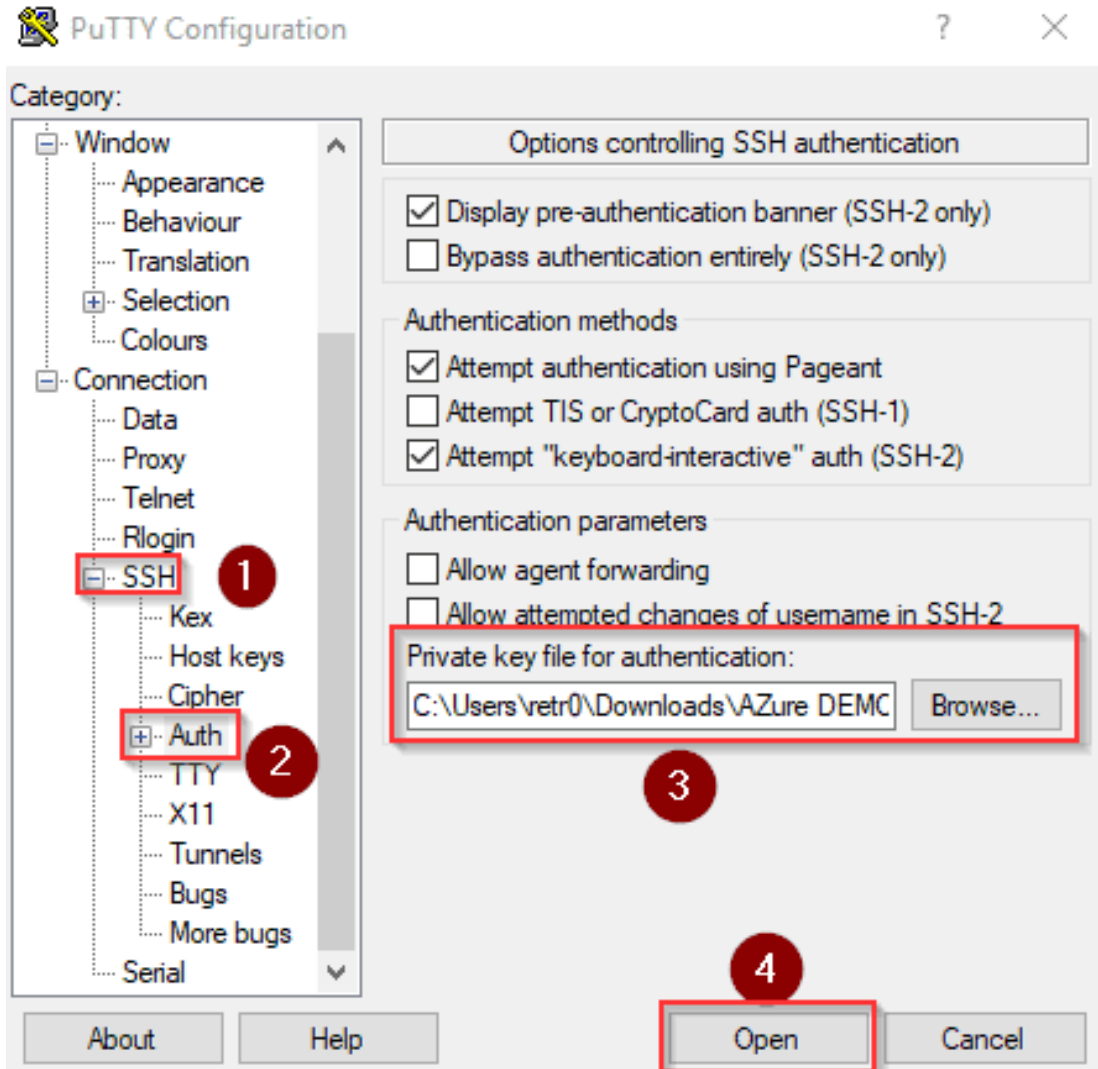
1. Enter the Host Name details in the following format: **<Username of VM>@<Public IP of VM>**
2. Make sure Port is **22**.
3. The connection type is **SSH**.



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.

```
k21-user@K21-demo-VM: ~  
  
System information as of Sun Jul 26 12:38:20 UTC 2020  
  
System load: 0.41      Processes:           128  
Usage of /: 4.4% of 28.90GB  Users logged in:    0  
Memory usage: 3%      IP address for eth0: 10.0.1.4  
Swap usage: 0%  
  
0 packages can be updated.  
0 updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
k21-user@K21-demo-VM:~$
```

(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.