

Deploying webserver in Ubuntu

instance (AWS platform)

Go to <https://aws.amazon.com/> site and sign in to console

Open EC2(Amazon Elastic Compute Cloud) Dashboard

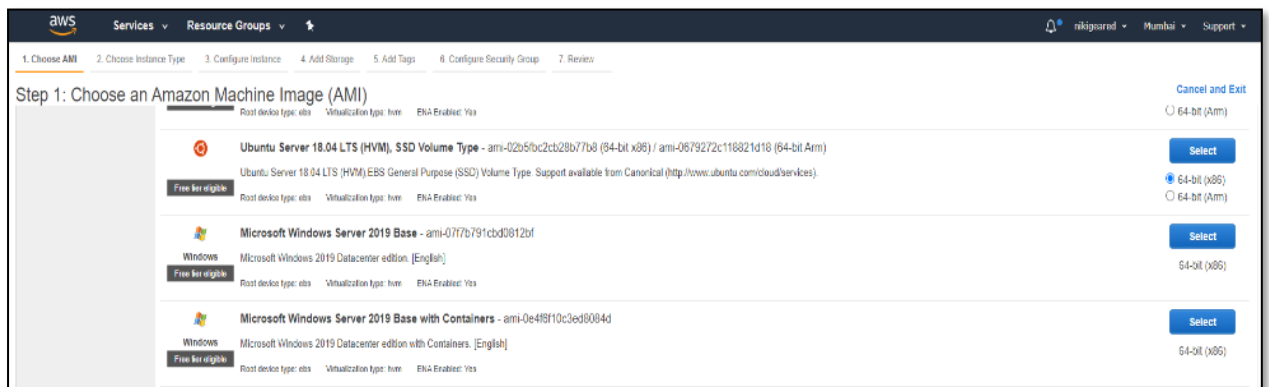
The screenshot shows the AWS EC2 Dashboard for the Asia Pacific (Mumbai) Region. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Limits, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, and Elastic IPs. The main content area is divided into several sections: Resources, Launch instance, Scheduled events, Service health, and Zone status. The Resources section shows a summary of EC2 resources in the Asia Pacific (Mumbai) Region, including Running instances, Elastic IPs, Dedicated Hosts, Snapshots, Volumes, Load balancers, Key pairs, Security groups, and Placement groups. The Launch instance section provides instructions on how to get started and includes a 'Launch instance' button. The Scheduled events section shows no scheduled events for the Asia Pacific (Mumbai) Region. The Service health section indicates that the service is operating normally. The Zone status section shows the status of three availability zones: ap-south-1a (aps1-az1), ap-south-1b (aps1-az3), and ap-south-1c (aps1-az2), all of which are operating normally.

Resource	Count
Running instances	0
Elastic IPs	0
Dedicated Hosts	0
Snapshots	0
Volumes	0
Load balancers	0
Key pairs	0
Security groups	1
Placement groups	0

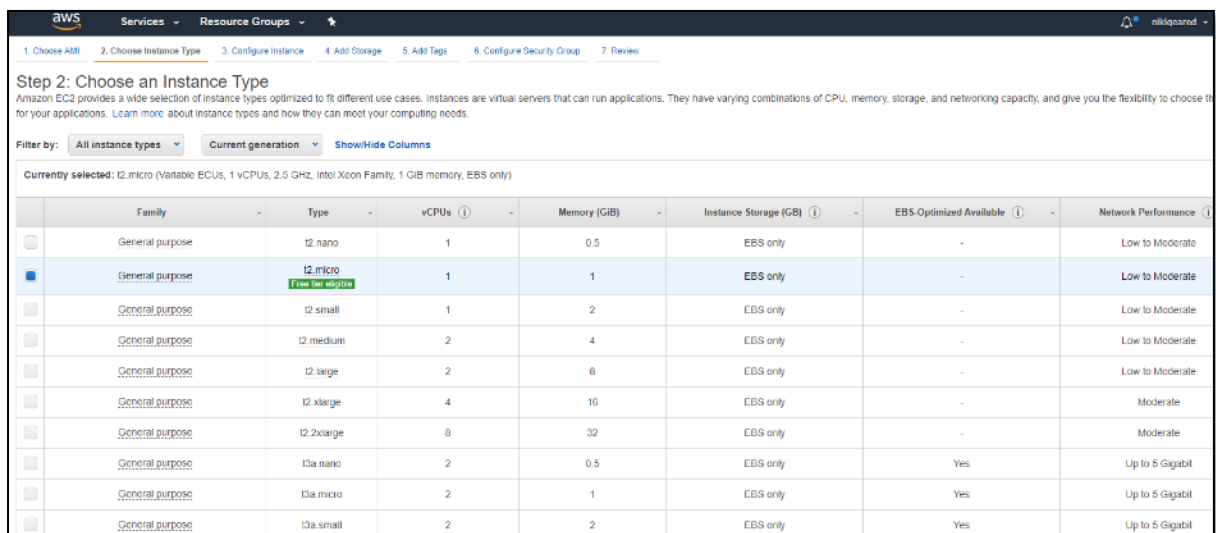
Zone	Status
ap-south-1a (aps1-az1)	Zone is operating normally
ap-south-1b (aps1-az3)	Zone is operating normally
ap-south-1c (aps1-az2)	Zone is operating normally

Choose Amazon Machine Image

Select Server 18.04 LTS server



Choose instanced type



Configure instance Detail

Nikhil Thiruvanthari
nikigear@gmail.com

Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing.

Number of instances ⓘ [Launch into Auto Scaling Group](#) ⓘ

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ [Create new VPC](#)

Subnet ⓘ [Create new subnet](#)

Auto-assign Public IP ⓘ

Placement group ⓘ ☐ Add instance to placement group

Capacity Reservation ⓘ

IAM role ⓘ [Create new IAM role](#)

Shutdown behavior ⓘ

Stop - Hibernate behavior ⓘ ☐ Enable hibernation as an additional stop behavior

Enable termination protection ⓘ ☐ Protect against accidental termination

Monitoring ⓘ ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy ⓘ [Additional charges will apply for dedicated tenancy.](#)

T2/T3 Unlimited ⓘ ☐ Enable
[Additional charges may apply](#)

File systems ⓘ [Add file system](#) [Create new file system](#)

Add Storage

Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ
Root	/dev/sda1	snap-01c49bd5fe5f144e2	<input type="text" value="8"/>	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Add Tag if any

Configure Security Group

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	Custom 0.0.0.0/0

[Add Rule](#)

Warning
 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.

Review Instance Launch

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Warning
 Improve your instances' security. Your security group, launch-wizard-2, is open to the world.
 Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
 You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-02b5fbc2cb28b77b8
 Free tier eligible
 Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).
 Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups

Security group name: launch-wizard-2
Description: launch-wizard-2 created 2020-08-21T14:41:49.301+05:30

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

Instance Details

Storage

Select Keypair

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair
Select a key pair
No key pairs found

No key pairs found

You don't have any key pairs. Please create a new key pair by selecting the **Create a new key pair** option above to continue.

Cancel Launch Instances

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair
Key pair name
nikhils_key

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel Launch Instances

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair
Select a key pair
nikhils_key

☐ I acknowledge that I have access to the selected private key file (nikhils_key.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Finalise and Launch

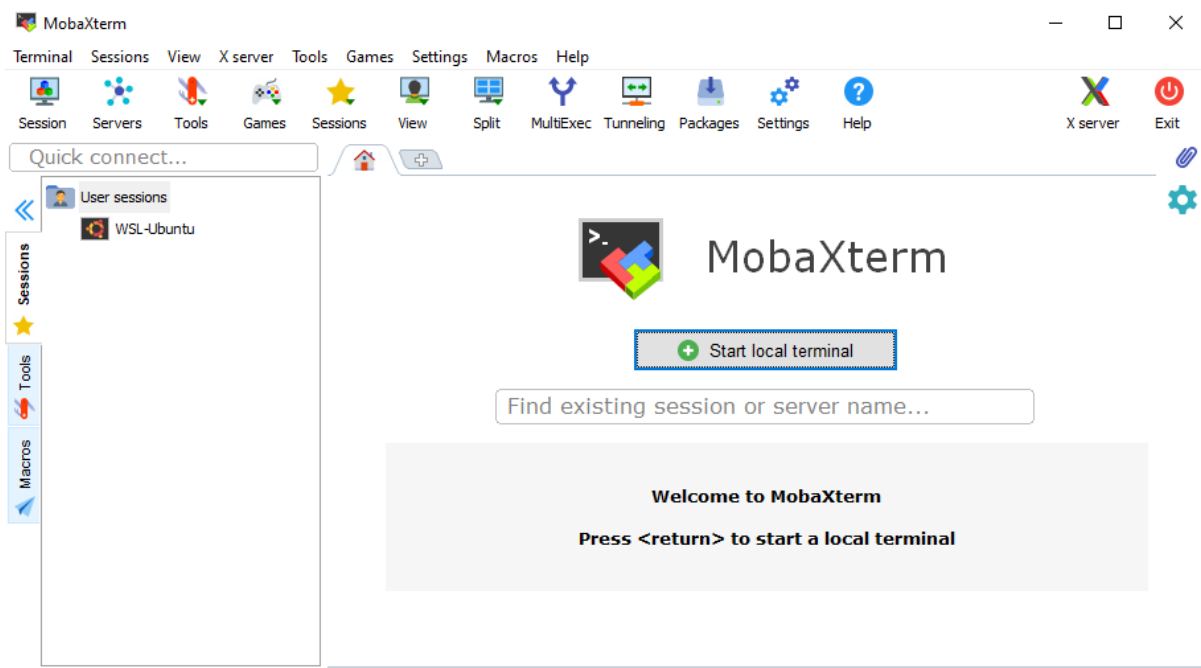
Resource Groups ✕									
Launch Instance ✕									
Filter by tags and attributes or search by keyword									
	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	Key Name
<input checked="" type="checkbox"/>	ubuntu	i-04fd68d2cd5911f6b	t2.micro	ap-south-1b	running	2/2 checks ...	None	ec2-13-126-249-171.ap...	nikhils_key
<input type="checkbox"/>		i-0d3ee34fa7bfc0a	t2.micro	ap-south-1b	terminated		None		nikhils_key

Instance: i-04fd68d2cd5911f6b (ubuntu) Public DNS: ec2-13-126-249-171.ap-south-1.compute.amazonaws.com

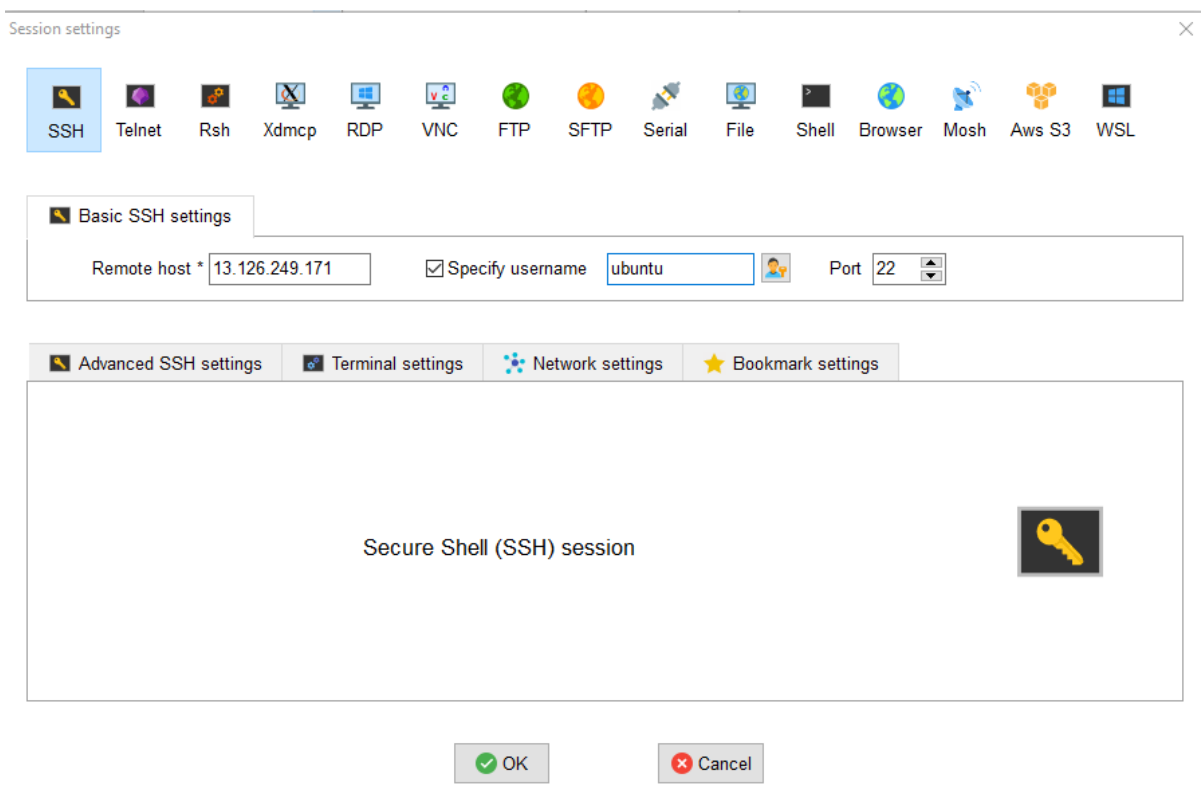
Description	Status Checks	Monitoring	Tags
Instance ID	i-04fd68d2cd5911f6b	Public DNS (IPv4)	ec2-13-126-249-171.ap-south-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	13.126.249.171
Instance type	t2.micro	IPv6 IPs	-

Open MobaXterm_Personal

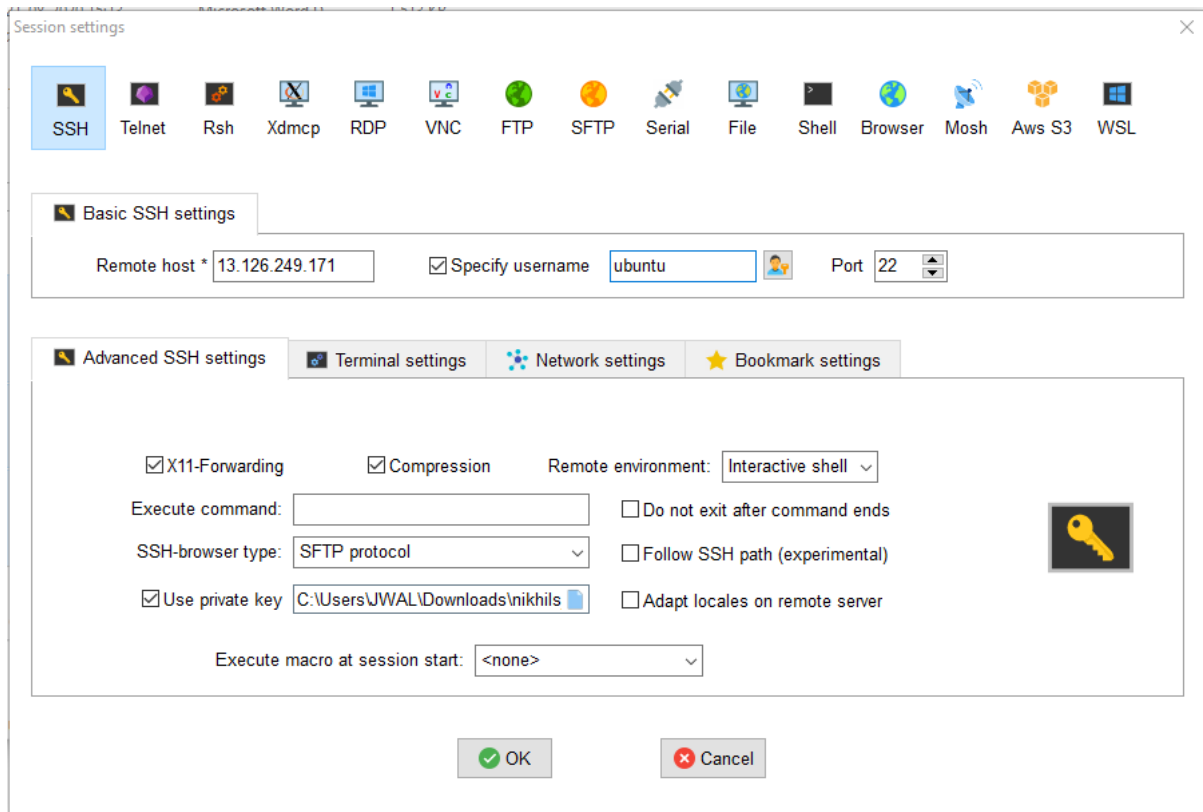
Nikhil Thiruvanthari
nikigear@gmail.com



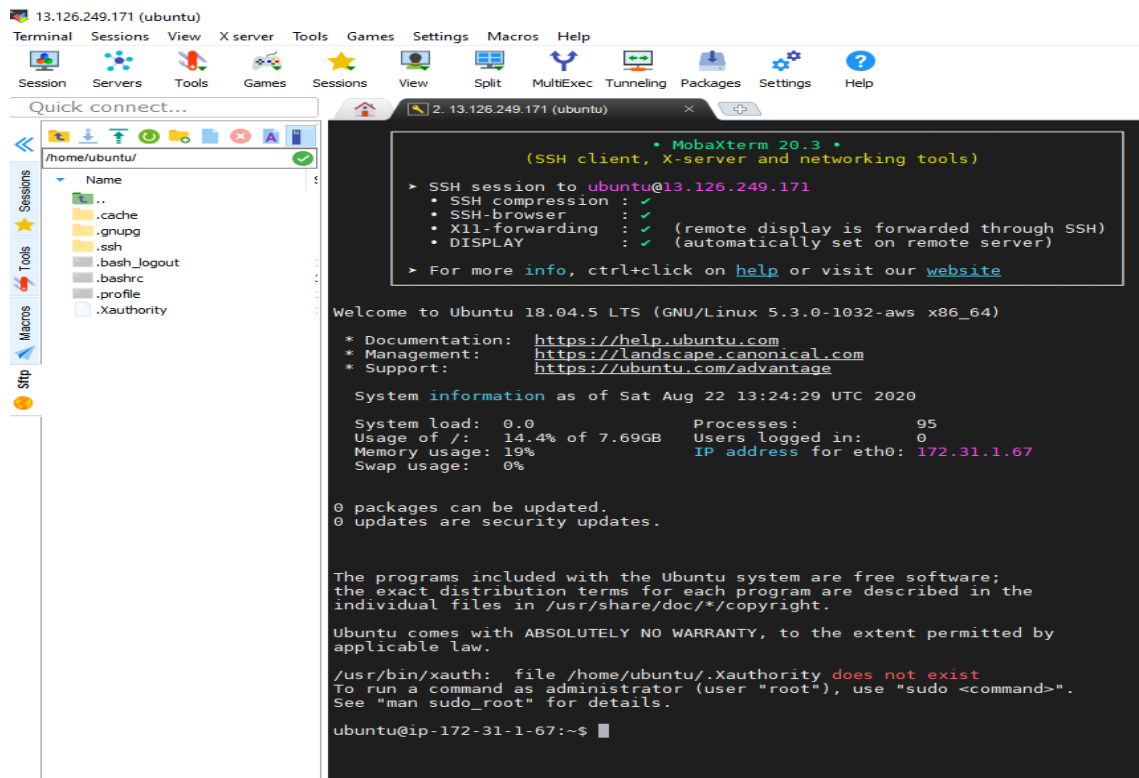
Click Session SSH and Add public ip from ec2 instance dashboard



Click advance SSH Settings and insert private (previously created)



Click Ok and Launch the remote window



Install nginx web server using bash

Note: Simply copy the command below and paste in the bash to install the nginx web server.

Nikhil Thiruvanthari
nikigear@gmail.com

```
sudo apt-get -y update  
sudo apt-get -y install nginx
```

Not secure 13.126.249.171

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.