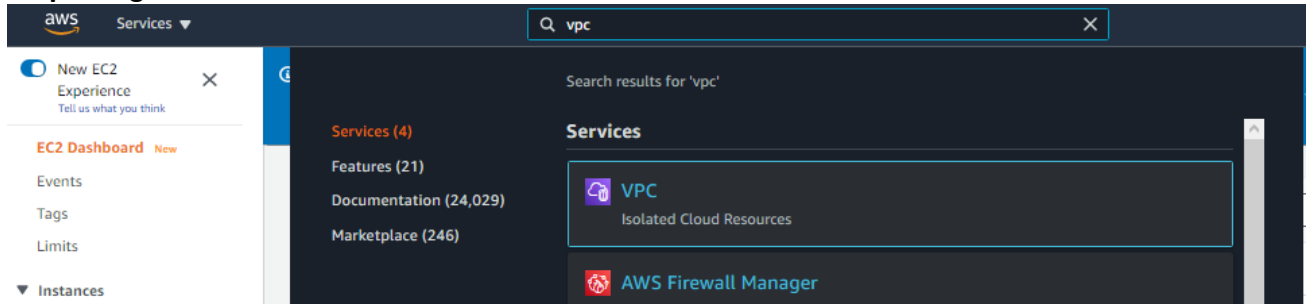


## Lab 1

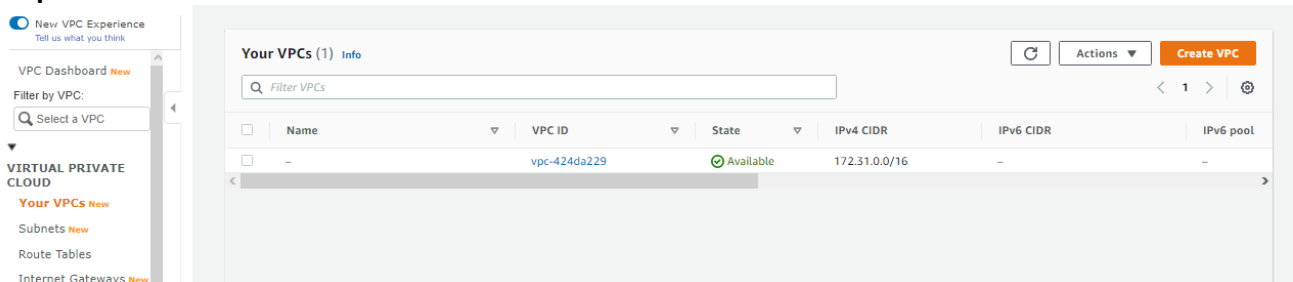
### Launch a Linux or Window Server by creating VPC, Route Table in a cloud.

A virtual private cloud(VPC) is the logical division of service provider's public cloud multi-tenant architecture to support private cloud computing. This model enables an enterprise to achieve the benefits of private cloud to enable more granular control over virtual networks and an isolated environment for sensitive workloads while still taking advantages of public cloud resources.

#### Step1: Log in to AWS Console and Select the VPC

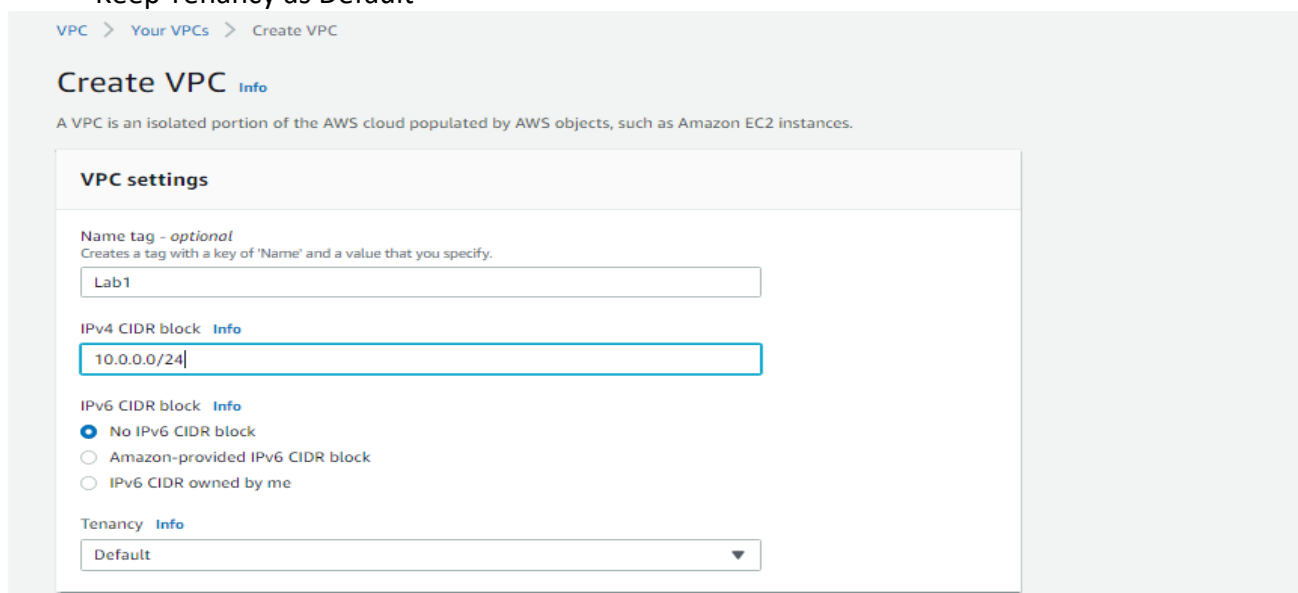


#### Step 2: Click on Create a Your VPC from Left Side Menu.Now Click on Create VPC button



#### Step 3:

- Now Enter the name for VPC
- Enter the CIDR Block as 10.0.0.0/24
- Keep Tenancy as Default



## Step 4: Click on create VPC

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key:  Value - optional:

You can add 49 more tags.

## Step 5: VPC Created Successfully

**New VPC Experience**  
Tell us what you think

VPC Dashboard [New](#)

Filter by VPC:

**VIRTUAL PRIVATE CLOUD**

**Your VPCs** [New](#)

- [Subnets](#) [New](#)
- [Route Tables](#)
- [Internet Gateways](#) [New](#)
- [Egress Only Internet Gateways](#) [New](#)
- [DHCP Options Sets](#) [New](#)
- [Elastic IPs](#) [New](#)
- [Managed Prefix Lists](#) [New](#)
- [Endpoints](#)
- [Endpoint Services](#)
- [NAT Gateways](#) [New](#)
- [Peering Connections](#)

**SECURITY**

- [Network ACLs](#) [New](#)

**You successfully created vpc-0a6313870ef522392 / Lab1**

VPC > Your VPCs > vpc-0a6313870ef522392

**vpc-0a6313870ef522392 / Lab1**

**Details** [Info](#)

VPC ID <a href="#">vpc-0a6313870ef522392</a>	State <span>Available</span>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set <a href="#">dopt-bc79b3d7</a>	Route table <a href="#">rtb-0d29b1b89a0af37e</a>	Network ACL <a href="#">acl-0150b3953303b6815</a>
Default VPC No	IPv4 CIDR 10.0.0.0/24	IPv6 pool -	IPv6 CIDR -
Owner ID <a href="#">165068001243</a>			

[CIDRs](#) [Flow logs](#) [Tags](#)

**IPv4 CIDRs** [Info](#)

CIDR	Status
10.0.0.0/24	<span>Available</span>

## Step 6: Create the subnet once after creating the VPC

**Subnets (3)** [Info](#)

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	-	<a href="#">subnet-79430635</a>	<span>Available</span>	<a href="#">vpc-424da229</a>	172.31.0.0/20	-
<input type="checkbox"/>	-	<a href="#">subnet-d5f5e1bd</a>	<span>Available</span>	<a href="#">vpc-424da229</a>	172.31.32.0/20	-
<input type="checkbox"/>	-	<a href="#">subnet-8fdf50f4</a>	<span>Available</span>	<a href="#">vpc-424da229</a>	172.31.16.0/20	-

## Step 7:

- Enter the name for subnet
  - Select the availability zone
  - Enter the CIDR Block
- Then click on create Subnet

## Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

### Subnet 1 of 1

#### Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Lab1-Subnet

The name can be up to 256 characters long.

#### Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference

#### IPv4 CIDR block [Info](#)

10.0.0.0/24

#### ▼ Tags - optional

##### Key

Name

##### Value - optional

Lab1-Subnet

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel

Create subnet

## Step 8: Next create the internet gateway creation

- Enter the name for Internet Gateway

New VPC Experience  
Tell us what you think

VPC Dashboard [New](#)

Filter by VPC:  
Select a VPC

**VIRTUAL PRIVATE CLOUD**

- Your VPCs [New](#)
- Subnets [New](#)
- Route Tables
- Internet Gateways** [New](#)
- Egress Only Internet Gateways [New](#)
- DHCP Options Sets [New](#)
- Elastic IPs [New](#)

### Internet gateways (1) [Info](#)

Filter internet gateways

Actions [Create Internet gateway](#)

	Name	Internet gateway ID	State	VPC ID	Owner
<input type="checkbox"/>	-	igw-94d068fc	Attached	vpc-424da229	165068001243

🟢 The following internet gateway was created: igw-06d4846d46120cbd5 . You can now attach to a VPC to enable the VPC to communicate with the internet. Attach to a VPC ✕

VPC > Internet gateways > igw-06d4846d46120cbd5

### igw-06d4846d46120cbd5 / Lab1 Internet Gateway Actions

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-06d4846d46120cbd5	Detached	-	165068001243

Tags

Manage tags

Key	Value
Name	Lab1 Internet Gateway

**Step 9:** Now Attach the created internet gateway to the VPC by right click and click on attach to VPC

Internet gateways (1/2) Info Refresh Actions Create internet gateway

	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	Lab1 Intern...	igw-06d4846d46120cbd5	Detached	-	165068001243
<input type="checkbox"/>	-	igw-94d068fc	Attached	vpc-424da229	165068001243

Create internet gateway

View details

Attach to VPC

Detach from VPC

Manage tags

Delete internet gateway

**Step 10:** Now attach internet gateway to VPC

VPC > Internet gateways > Attach to VPC (igw-06d4846d46120cbd5)

### Attach to VPC (igw-06d4846d46120cbd5) Info

**VPC**  
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs  
Attach the internet gateway to this VPC.

vpc-0a6313870ef522392 - Lab1

**AWS Command Line Interface command**

Cancel Attach internet gateway

🟢 Internet gateway igw-06d4846d46120cbd5 successfully attached to vpc-0a6313870ef522392 ✕

Internet gateways (2) Info Refresh Actions Create internet gateway

	Name	Internet gateway ID	State	VPC ID	Owner
<input type="checkbox"/>	Lab1 Internet Gate...	igw-06d4846d46120cbd5	Attached	vpc-0a6313870ef522392   Lab1	165068001243
<input type="checkbox"/>	-	igw-94d068fc	Attached	vpc-424da229	165068001243

New VPC Experience

Tell us what you think

VPC Dashboard New

Filter by VPC:

VIRTUAL PRIVATE CLOUD

Your VPCs New

Subnets New

## Step 11: Now Click on Create route table button to create Route Tables

The screenshot shows the AWS VPC console interface. On the left, there's a sidebar with 'VIRTUAL PRIVATE CLOUD' and 'Route Tables' highlighted. The main area has a 'Create route table' button and an 'Actions' dropdown. Below this is a table of existing route tables.

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
	rtb-0d29bf1b89a0af37e	-	-	Yes	vpc-0a6313870ef522392  ...	165068001243
	rtb-59c86432	-	-	Yes	vpc-424da229	165068001243

## Step 12:

- Enter the Name for Route Table
- Now Select the VPC From the Drop down list(Already created VPC)

[Route Tables](#) > [Create route table](#)

### Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag

VPC\*

Key (128 characters maximum)

Value (256 characters maximum)

*This resource currently has no tags*

[Add Tag](#) 50 remaining (Up to 50 tags maximum)

\* Required

[Cancel](#) [Create](#)

## Step 13: Route Table Created

[Route Tables](#) > [Create route table](#)

### Create route table

✓ The following Route Table was created:

Route Table ID **rtb-005db07f1f6fdf263**

[Close](#)

## Step 14:

- Add subnet associations for route table
- Select the subnet ID that you have created Associate it with the table

The screenshot shows the AWS VPC console interface. On the left, there's a sidebar with 'VIRTUAL PRIVATE CLOUD' and 'Route Tables' highlighted. The main area has a 'Create route table' button and an 'Actions' dropdown. Below this is a table of existing route tables. A context menu is open over the first row, showing options like 'Set Main Route Table', 'Delete Route Table', 'Edit subnet associations', etc.

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
Lab1 R	263	-	-	No	vpc-0a6313870ef522392  ...	165068001243
	37e	-	-	Yes	vpc-0a6313870ef522392  ...	165068001243
		-	-	Yes	vpc-424da229	165068001243

[Route Tables](#) > Edit subnet associations

## Edit subnet associations

Route table rtb-005db07f1f6fd263 (Lab1 Routing Table)

Associated subnets subnet-07062a945791b7a20

Filter by attributes or search by keyword			
<input type="checkbox"/>	Subnet ID	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	subnet-07062a945791b7a20   Lab1-Sub...	10.0.0.0/24	-
		Current Route Table	
		Main	

\* Required

[Cancel](#) [Save](#)

## Step 15: Edit routes in route table then set the destination as 0.0.0.0

[Route Tables](#) > Edit routes

## Edit routes

Destination	Target	Status	Propagated
10.0.0.0/24	local	active	No
0.0.0.0/0	igw-06d4846d46120cbd5		No

[Add route](#)

\* Required

[Cancel](#) [Save routes](#)

## Step 16: Go to EC2 and click on launch instance

New EC2 Experience

EC2 Dashboard

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Welcome to the new EC2 console!

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running) 0

Instances (all states) 0

Placement groups 0

Volumes 0

Dedicated Hosts 0

Key pairs 14

Security groups 17

Elastic IPs 0

Load balancers 0

Snapshots 0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Service health

Service Health Dashboard

Region Asia Pacific (Mumbai)

Status This service is operating

Account attributes

Supported platforms

Default VPC

Settings

EBS encryption

Zones

Default credit specification

Console experiments

Explore AWS

Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in a single EC2 ASG.

Enable Best Price-Performance with

## Step 17: Now choose any Linux instance from free tier

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

[Cancel and Exit](#)

### Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

Search by Systems Manager parameter

Quick Start

My AMIs

AWS Marketplace

Community AMIs

☒ Free tier only

Amazon Linux 2 AMI (HVM), SSD Volume Type

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

ami-04b1ddd35fd71475a (64-bit x86) / ami-0d5c7546de7618191 (64-bit Arm)

Free tier eligible

Select

64-bit (x86)

64-bit (Arm)

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type

Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

ami-0a9d27a9f4f5c0efc (64-bit x86) / ami-0d46b0a8ba9a483af (64-bit Arm)

Free tier eligible

Select

64-bit (x86)

64-bit (Arm)

## Step 18: Select t2.micro free tire eligible and click on launch instance

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECU, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	i3	i3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	i3	i3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	i3	i3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### 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, assign an access management role to the instance, and more.

Number of instances 1 Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network vpc-0a6313870ef522392 | Lab1 Create new VPC

Subnet subnet-07062a945791b7a20 | Lab1-Subnet | ap-sou 251 IP Addresses available Create new subnet

Auto-assign Public IP Enable

Placement group ☐ Add instance to placement group

Capacity Reservation Open

Domain join directory No directory Create new directory

IAM role None Create new IAM role

CPU options ☐ Specify CPU options

Shutdown behavior Stop

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

Cancel Previous Review and Launch Next: Add Storage

## Step 19: Now add the storage for Linux Instance

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### 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	Encryption
Root	/dev/xvda	snap-06f54b142aaa48c61	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

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.

## Step 20: Assign the tags

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	Lab1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

## Step 21 : Add the HTTP,SSH rule in Configure security group

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### 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 your instance, add rules that allow unrestricted access to the 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: launch-wizard-14

Description: launch-wizard-14 created 2021-01-02T18:39:12.611+05:30

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0, ::0	e.g. SSH for Admin Desktop
MYSQ/Auror	TCP	3306	My IP 1.22.149.227/32	e.g. SSH for Admin Desktop

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.

## Step 22: Create new Key Pair and then download the key pair in your local machine

### 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

Lab1

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

## Step 23: Now our Linux Instance is running

Instances (1/1) Info

Filter instances

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
<input checked="" type="checkbox"/>	Lab1	i-01a85977fd88b2704	Running	t2.micro	Initializing	No alarms	ap-south-1a	-	65.0.18.186

VPC > Your VPCs > vpc-0a6313870ef522392 > Edit DNS resolution

### Edit DNS resolution

DNS resolution

Indicates whether the DNS resolution is supported.

VPC ID

vpc-0a6313870ef522392

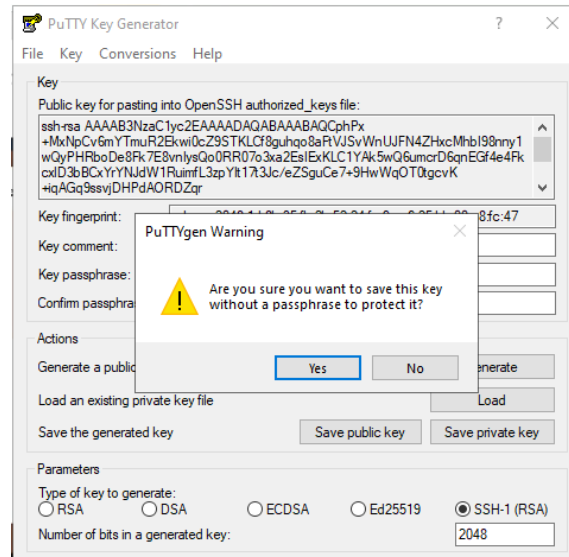
DNS resolution

☒ Enable

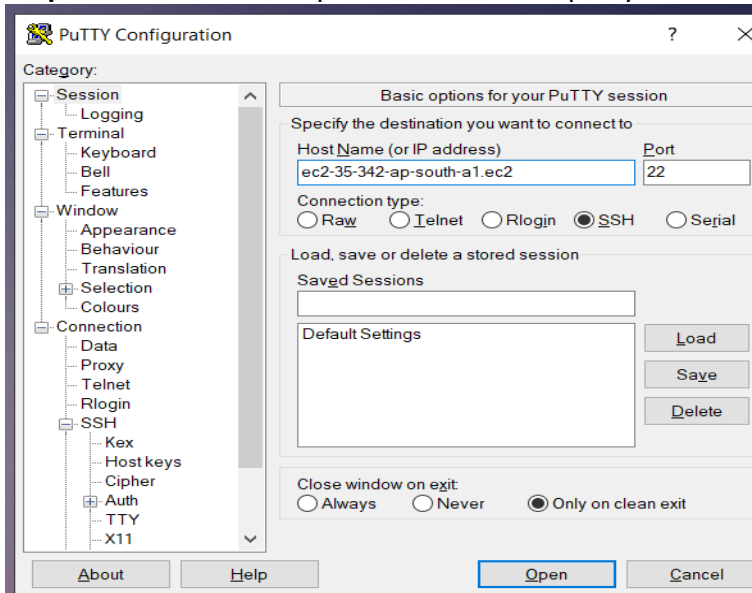
Cancel Save changes

## Step 24: Download the Putty Client application to connect Linux Instance. Open putty key generator and load the downloaded .pem file and convert and save the file

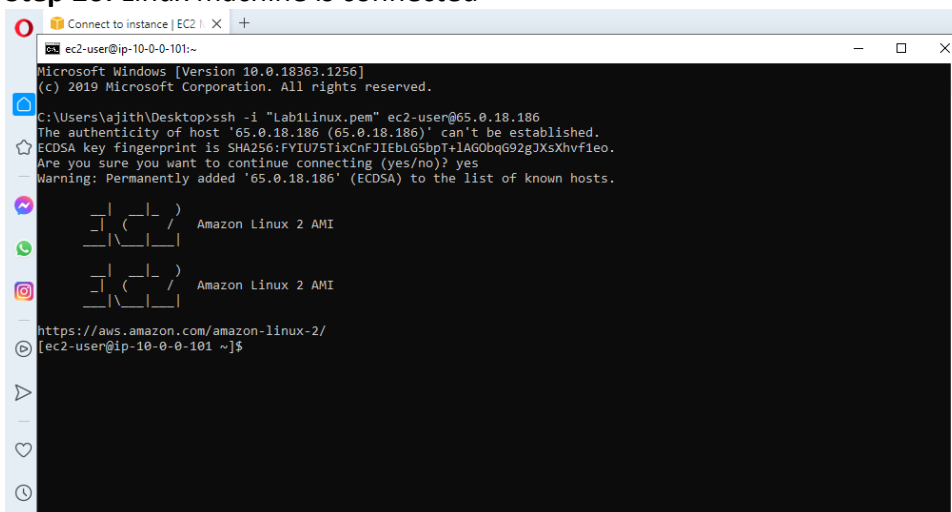




**Step 25:** Now enter the public dns name in putty software and click on open



**Step 26:** Linux machine is connected



# FOR WINDOWS INSTANCE

## Step 1: Go to EC2 and click on launch instance and select Windows server VM

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

[Cancel and Exit](#)

### Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

My AMIs

AWS Marketplace

Community AMIs

☒ Free tier only 1

Amazon Linux

Free tier eligible

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-04b1dd35fd71475a (64-bit x86) / ami-0d5c7546de7618191 (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Red Hat

Free tier eligible

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0a9d27a9f4f5c0efc (64-bit x86) / ami-0d46b0a8ba9a483af (64-bit Arm)

Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

SUSE Linux

Free tier eligible

SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type - ami-0b3ac3edf2397475 (64-bit x86) / ami-0ab71076ab9b53b0d (64-bit Arm)

SUSE Linux Enterprise Server 15 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Amazon EC2 AMI Tools preinstalled: Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Ubuntu

Free tier eligible

Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-0a4a70bd98c6d6441 (64-bit x86) / ami-00e24e2d9b2d70f5c (64-bit Arm)

Ubuntu Server 20.04 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 ENA Enabled: Yes

Select

64-bit (x86)  
64-bit (Arm)

Select

64-bit (x86)  
64-bit (Arm)

Select

64-bit (x86)  
64-bit (Arm)

Select

64-bit (x86)  
64-bit (Arm)

## Step 2: Select the free tier eligible t2.micro

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, ~, 1 GiB memory, EBS only)								
	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes

## Step 3: Configure the instance details according your needs

### 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, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: ☐ Request Spot instances

Network: vpc-94b6b6b9 (default) Create new VPC

Subnet: No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: ☐ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory Create new directory

IAM role: None Create new IAM role

CPU options: ☐ Specify CPU options

Shutdown behavior: Stop

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

Enable termination protection: ☐ Protect against accidental termination

Monitor: ☐ Enable CloudWatch detailed monitoring

Cancel

Previous

Review and Launch

Next: Add Storage

## Step 4: Now add the storage for Windows instance

### 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	Encryption
Root	/dev/sda1	snap-0ff00d622acb42e95	30	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[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.

## Step 5: In Configure Security group add the necessary rules

### 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 your instance, add rules that allow unrestricted access to the 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

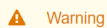
☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

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.

## Step 6: Create a new key pair and download the key pair

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

lab1

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

## Step 7: Now got to ec2 dashboard and select instance click on connect button

Instances (1/1) Info

Connect Instance state Actions Launch instances

Filter instances

search: i-053c9779d486d6790 Clear filters

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/>	-	i-053c9779d486d6790	Running	t2.micro	Initializing	No alarms	us-east-1d	ec2-3-80-61-9.compute-1.amazonaws.com

## Step 8: Now upload the generated .pem file and upload here. Now click on generate password and copy username and the password

EC2 > Instances > i-053c9779d486d6790 > Connect to instance

Connect to instance Info

Connect to your instance i-053c9779d486d6790 using any of these options

Session Manager

RDP client

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

Download remote desktop file

When prompted, connect to your instance using the following details:

Public DNS

ec2-3-80-61-9.compute-1.amazonaws.com

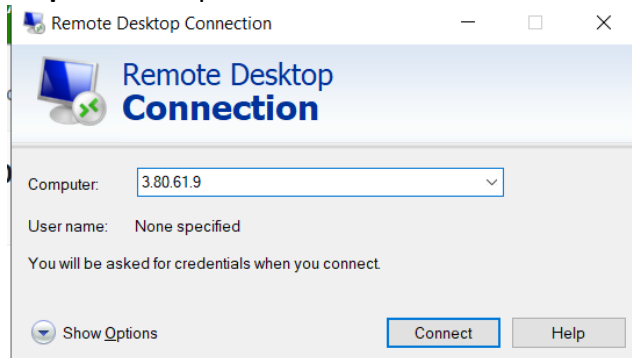
User name

Administrator

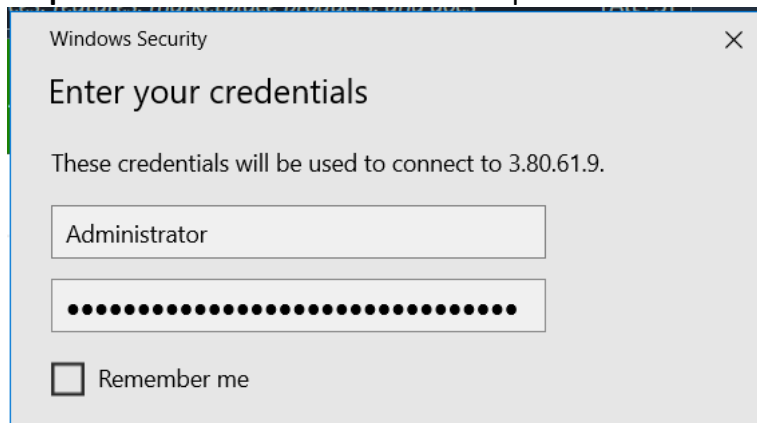
Password Get password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

**Step 9 :** Now open the RDP client in host machine and enter the public ip of Windows instance



**Step 10:** Now enter the username and password for windows VM



**Step 11:** Now we successfully login to Windows Virtual Machine

