PCET's
Pimpri
Chinchwad
University, Pune

Learn | Grow | Achieve

Checked By	Dr. Avinash Golande
Name	
Sign	
Date	
Grade	

EXPERIMENT NO . 11

- **Title:-** Launch and Configure a Virtual Machine using Amazon EC2

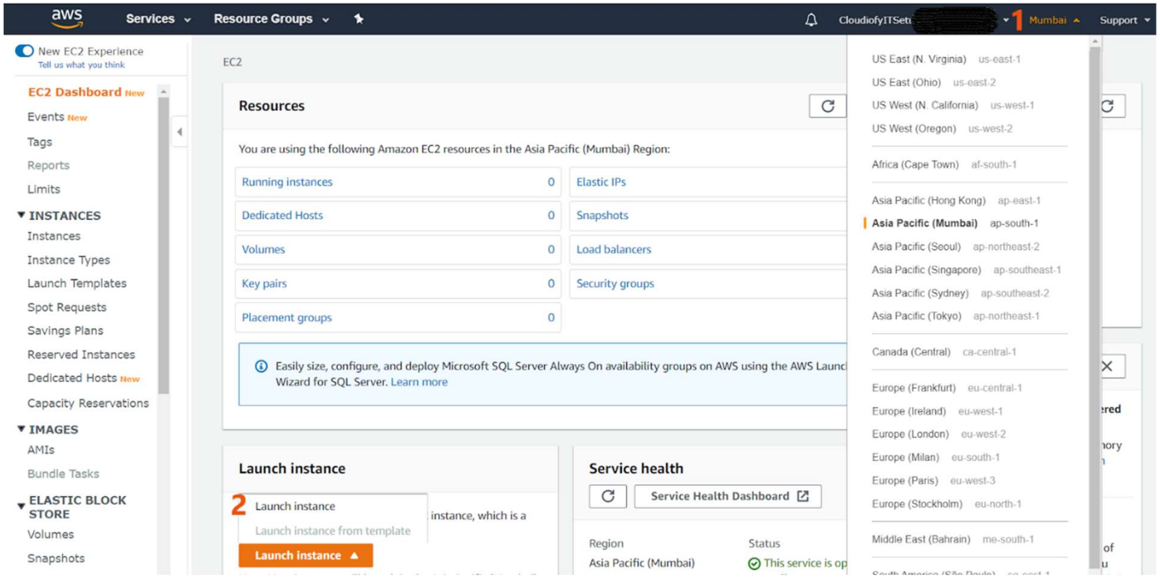
- **Objective :-**

To learn how to provision and manage Amazon EC2 instances using both the AWS Management Console and the AWS Command Line Interface (CLI), and to establish secure remote connections to Linux EC2 instances from a Windows machine.

Resources used :- AWS Account (Free Tier), AWS Management Console, AWS CLI, PuTTY & PuTTYgen (for SSH), Key Pair (.pem/.ppk), Security Group (port 22), VPC & Subnet ID, PC/Laptop with Internet connection.

- **Theory :-**

1.Log in to AWS Console and go to EC2 Service


aws
Services
Resource Groups
CloudiofyITSet[redacted]
1
Mumbai
Support
New EC2 Experience
Tell us what you think
EC2 Dashboard New
Events New
Tags
Reports
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts New
Capacity Reservations
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
EC2
Resources
Launch instance
2
Launch instance
Launch instance from template
Launch instance
Service health
Service Health Dashboard
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2
Africa (Cape Town) af-south-1
Asia Pacific (Hong Kong) ap-east-1
Asia Pacific (Mumbai) ap-south-1
Asia Pacific (Seoul) ap-northeast-2
Asia Pacific (Singapore) ap-southeast-1
Asia Pacific (Sydney) ap-southeast-2
Asia Pacific (Tokyo) ap-northeast-1
Canada (Central) ca-central-1
Europe (Frankfurt) eu-central-1
Europe (Ireland) eu-west-1
Europe (London) eu-west-2
Europe (Milan) eu-south-1
Europe (Paris) eu-west-3
Europe (Stockholm) eu-north-1
Middle East (Bahrain) me-south-1

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

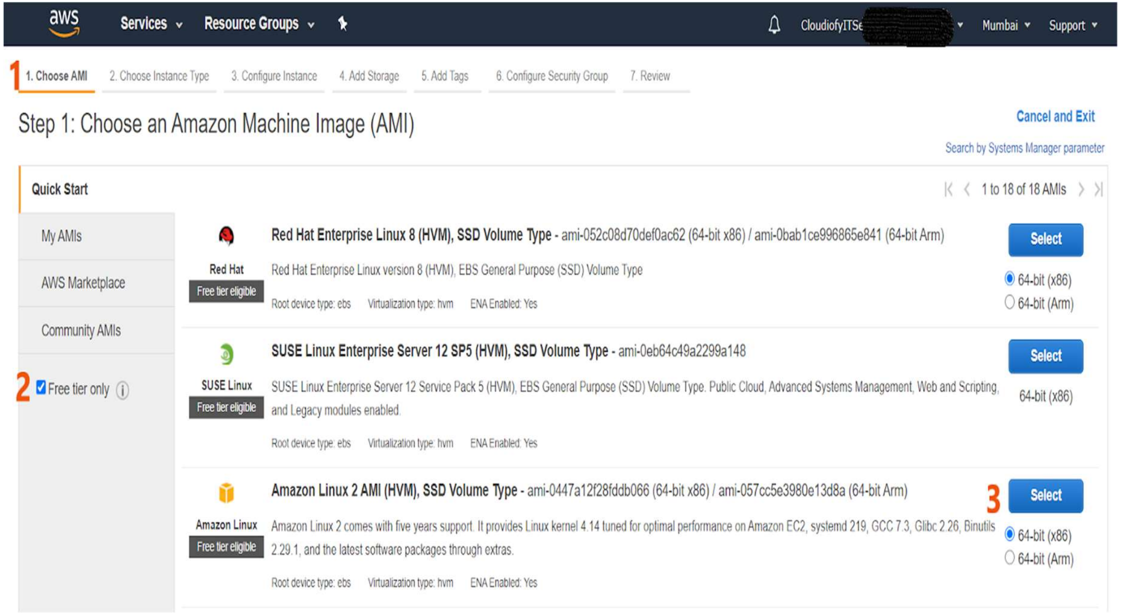
Running instances	0	Elastic IPs
Dedicated Hosts	0	Snapshots
Volumes	0	Load balancers
Key pairs	0	Security groups
Placement groups	0	

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launc Wizard for SQL Server. Learn more

instance, which is a

Region	Status
Asia Pacific (Mumbai)	This service is op

1. Choose an Amazon Machine Image (AMI)



Step 1: Choose an Amazon Machine Image (AMI)

☑ Free tier only

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-052c08d70def0ac62 (64-bit x86) / ami-0bab1ce996865e841 (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

● 64-bit (x86)
○ 64-bit (Arm)

SUSE Linux Enterprise Server 12 SP5 (HVM), SSD Volume Type - ami-0eb64c49a2299a148

SUSE Linux Enterprise Server 12 Service Pack 5 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.

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

64-bit (x86)

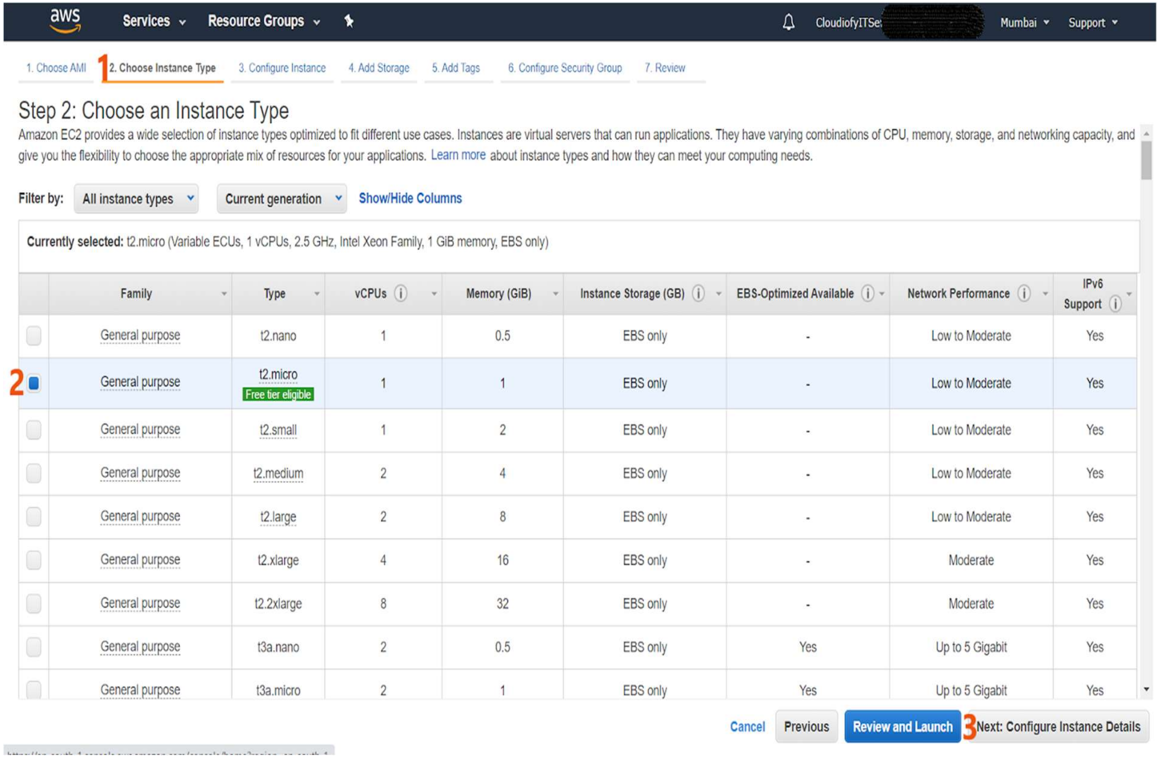
Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0447a12f28fddb066 (64-bit x86) / ami-057cc5e3980e13d8a (64-bit Arm)

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.

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

● 64-bit (x86)
○ 64-bit (Arm)

2. Choose an Instance Type



Step 2: Choose an Instance Type

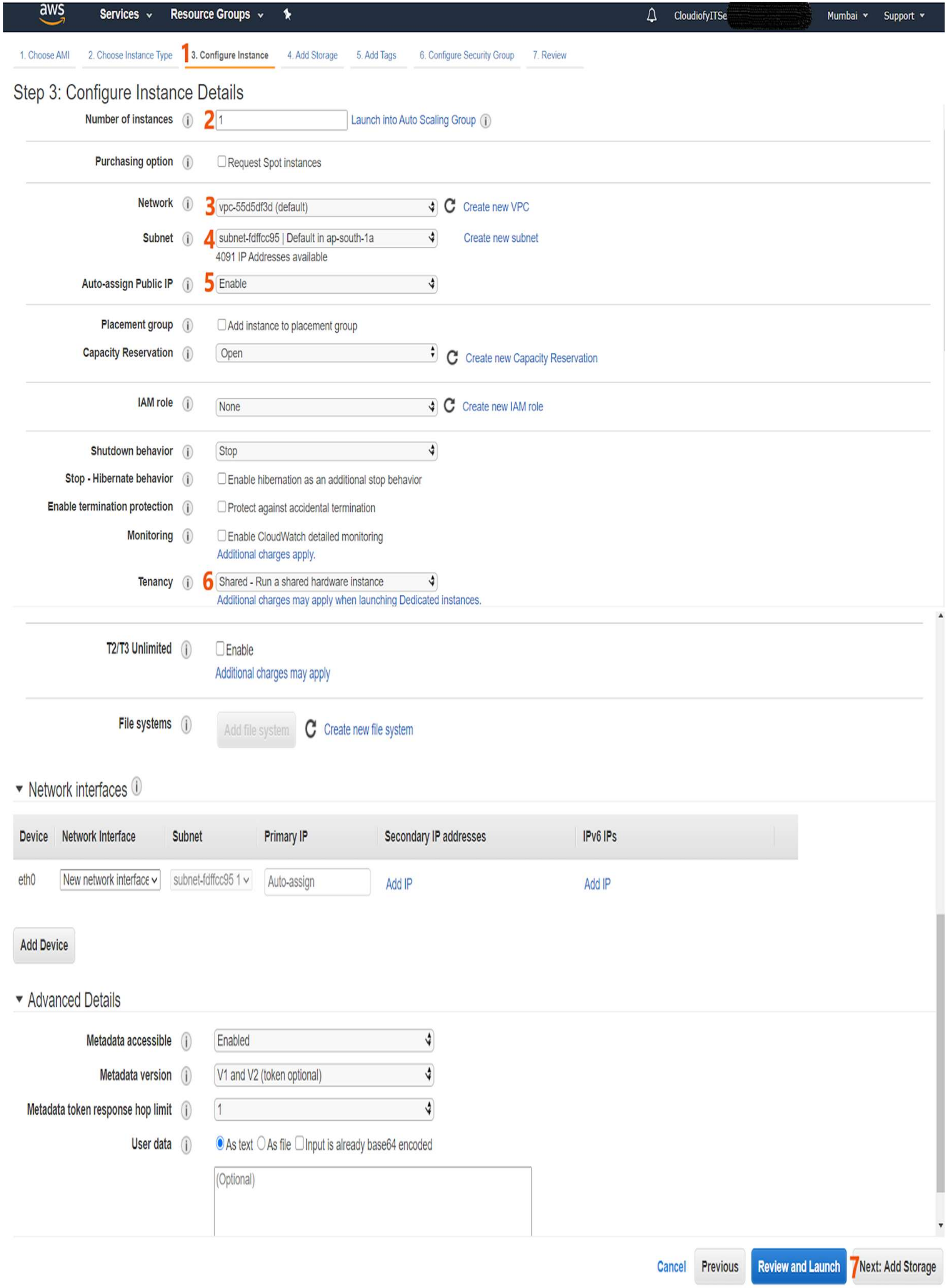
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources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

Filter by: All instance types | Current generation

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
■	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
□	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
□	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

3. Configure Instance Details



Step 3: Configure Instance Details

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-55d5df3d (default) — Create new VPC

Subnet: subnet-fdffcc95 | Default in ap-south-1a — Create new subnet
4091 IP Addresses available

Auto-assign Public IP: Enable

Placement group: □ Add instance to placement group

Capacity Reservation: Open — Create new Capacity Reservation

IAM role: None — Create new IAM role

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.

Tenancy: Shared - Run a shared hardware instance
Additional charges may apply when launching Dedicated instances.

T2/T3 Unlimited: □ Enable
Additional charges may apply

File systems: Add file system — Create new file system

▾ Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-fdffcc95 1	Auto-assign	Add IP	Add IP

Add Device

▾ Advanced Details

Metadata accessible: Enabled

Metadata version: V1 and V2 (token optional)

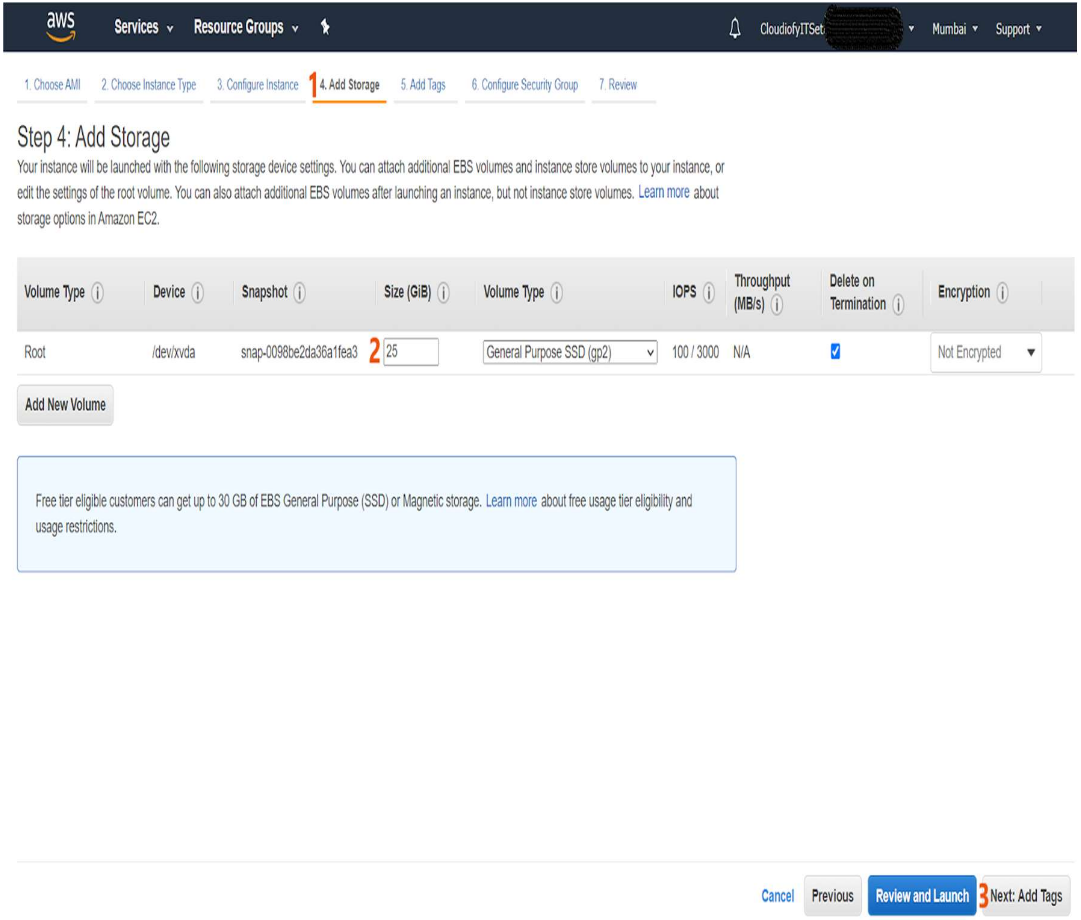
Metadata token response hop limit: 1

User data: ● As text ○ As file □ Input is already base64 encoded

(Optional)

Cancel | Previous | Review and Launch | Next: Add Storage

4. Add Storage



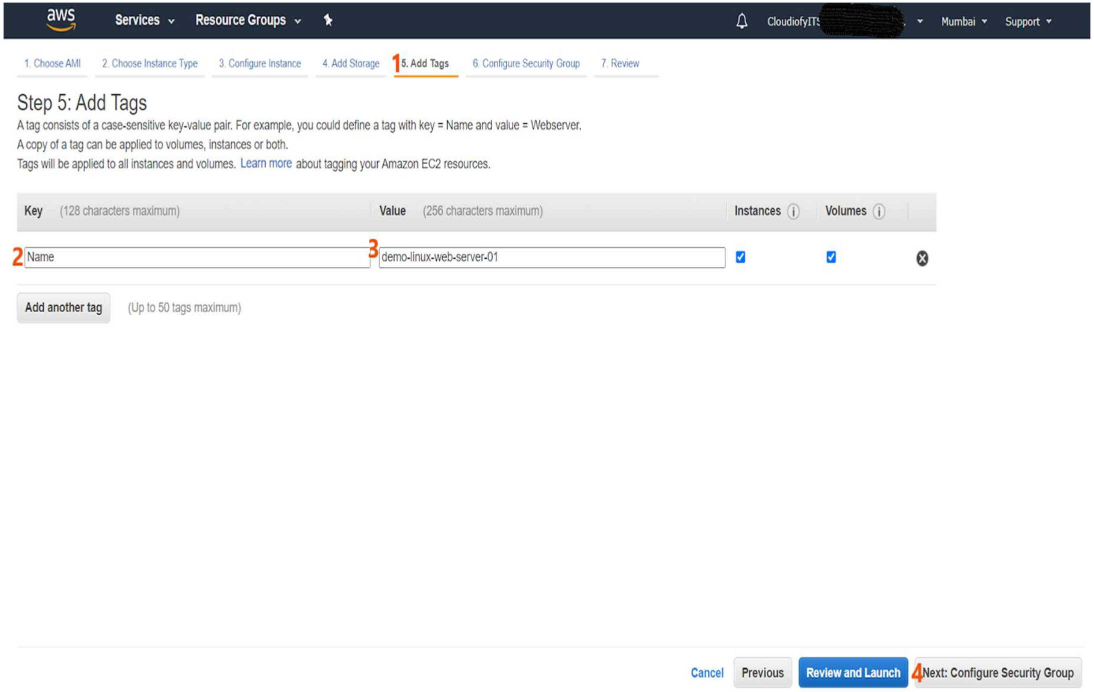
Step 4: Add Storage

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	Encryption
Root	/dev/xvda	snap-0098be2da36a1fea3	25	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

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.

5. Add Tags

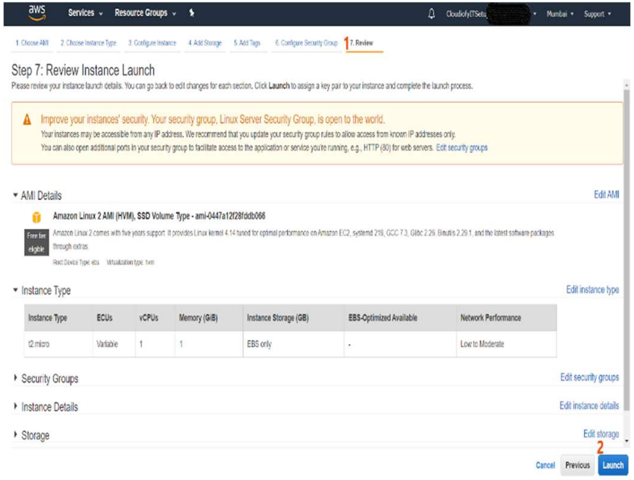


Step 5: Add Tags

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	demo-linux-web-server-01	☑	☑

6. Configure Security Group



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.

Improve your instances' security. Your security group, Linux Server Security Group, 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 — Edit AMI

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0447a12f28fddb066

Free tier eligible

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.

Root Device Type: ebs   Virtualization type: hvm

▾ Instance Type — Edit instance type

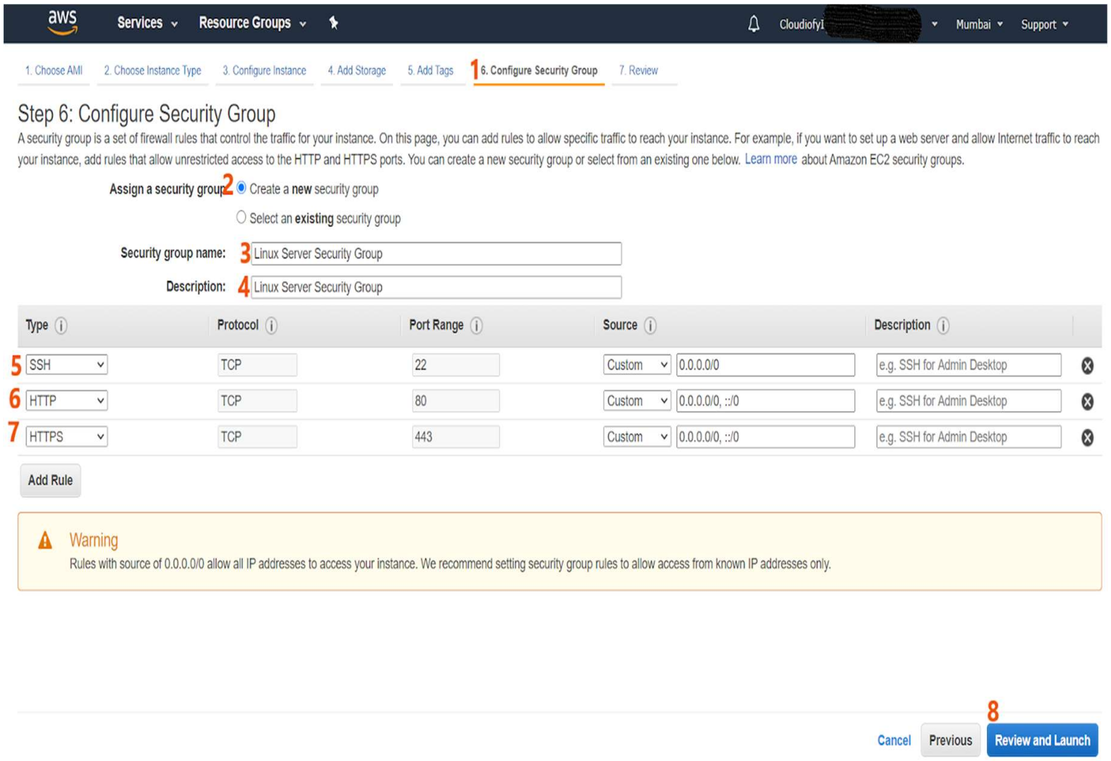
Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

▸ Security Groups — Edit security groups

▸ Instance Details — Edit instance details

▸ Storage — Edit storage

7. Review Instance, Launch and Select or Create Key Pair



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.

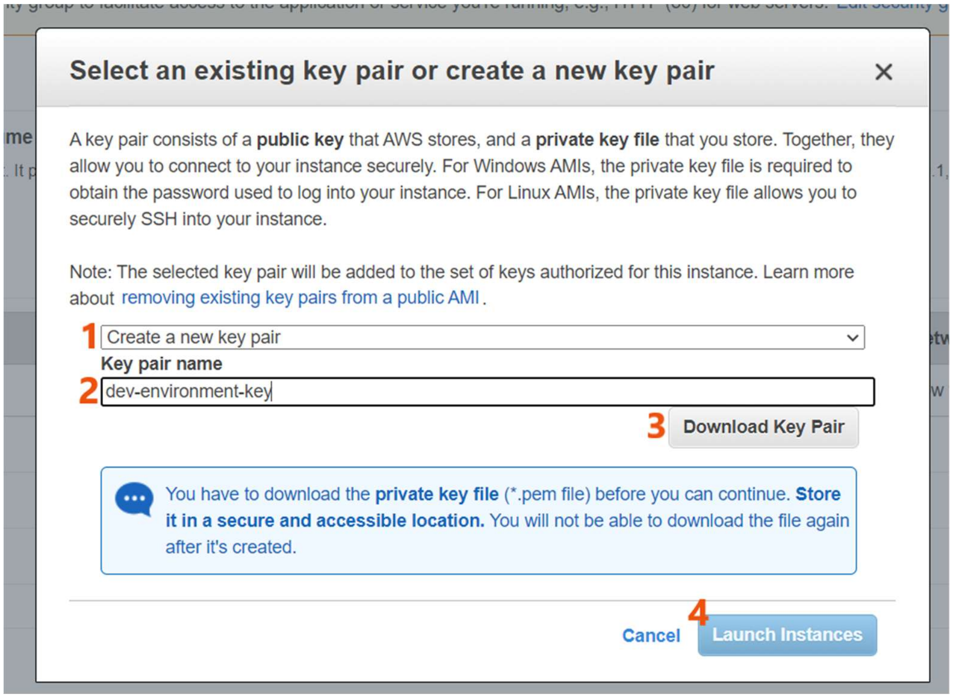
Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: Linux Server Security Group

Description: Linux Server Security Group

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, ::/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

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.



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 .

1 Create a new key pair

Key pair name

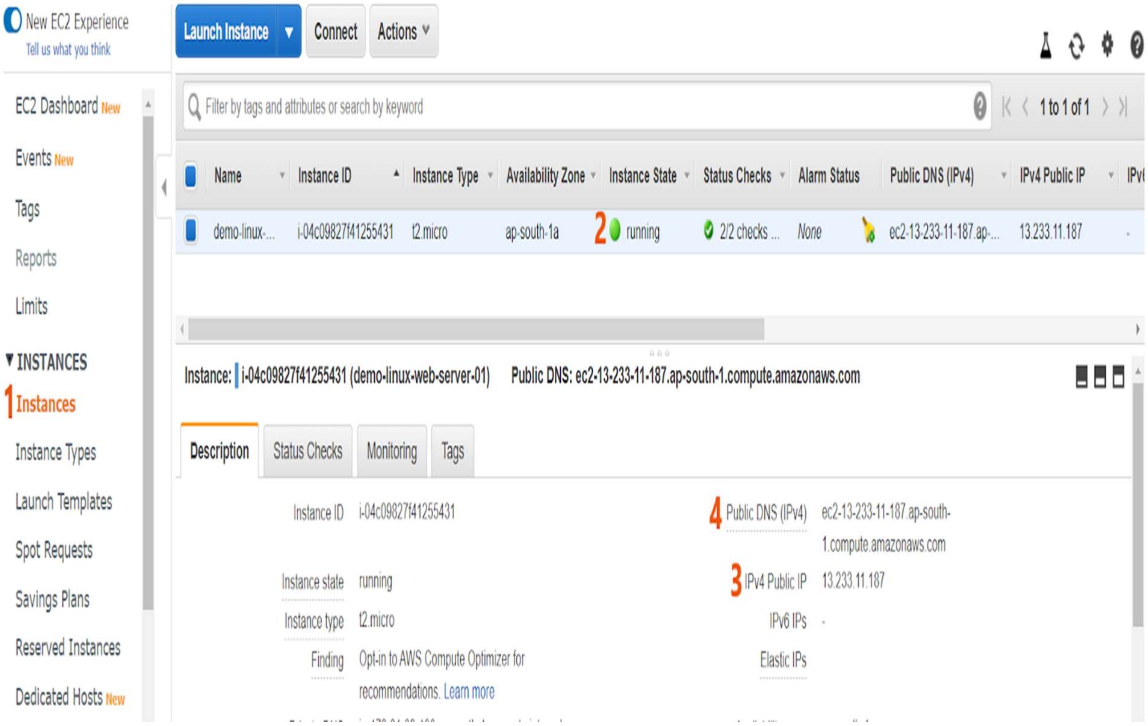
2 dev-environment-key

3 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.

4 Cancel Launch Instances

8. Done! Verify created instance is ready



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv
demo-linux-...	i-04c09827f41255431	t2.micro	ap-south-1a	2 running	2/2 checks ...	None	ec2-13-233-11-187.ap-...	13.233.11.187	-

Instance: i-04c09827f41255431 (demo-linux-web-server-01) Public DNS: ec2-13-233-11-187.ap-south-1.compute.amazonaws.com

Instance ID i-04c09827f41255431

Instance state running

Instance type t2.micro

Finding Opt-in to AWS Compute Optimizer for recommendations. Learn more

4 Public DNS (IPv4) ec2-13-233-11-187.ap-south-1.compute.amazonaws.com

3 IPv4 Public IP 13.233.11.187

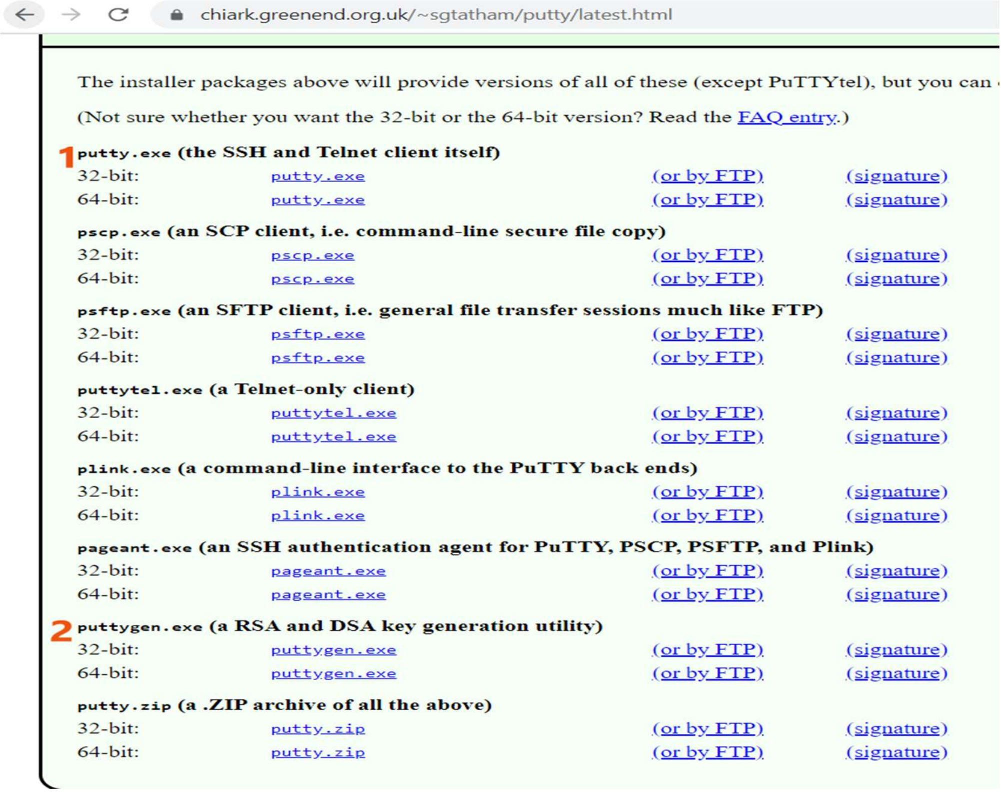
IPv6 IPs -

Elastic IPs

How to connect EC2 Linux instance from Windows using PuTTY

1. Install PuTTY on your local computer
   - Download and install PuTTY from the PuTTY download page

Download the putty.exe and puttygen.exe file



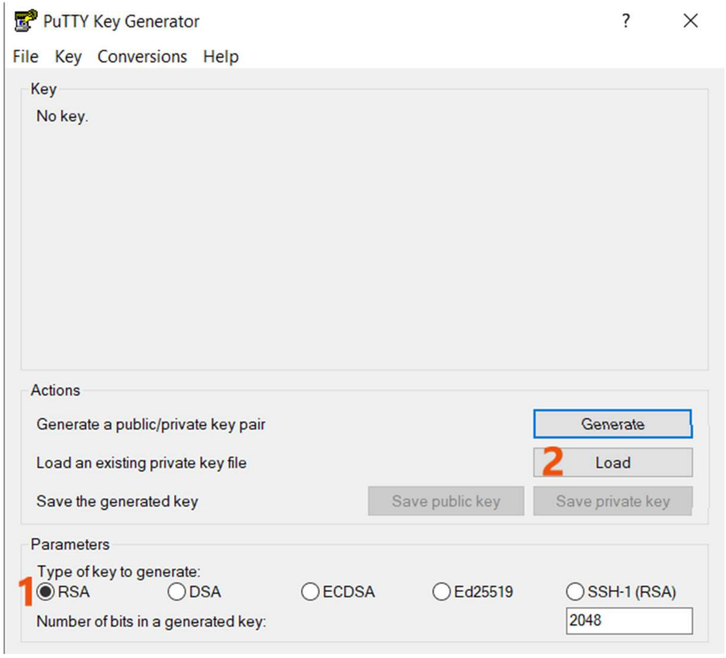
chiark.greenend.org.uk/~sgtatham/putty/latest.html

The installer packages above will provide versions of all of these (except PuTTYtel), but you can

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

putty.exe (the SSH and Telnet client itself)			
32-bit:	putty.exe	(or by FTP)	(signature)
64-bit:	putty.exe	(or by FTP)	(signature)
pscp.exe (an SCP client, i.e. command-line secure file copy)			
32-bit:	pscp.exe	(or by FTP)	(signature)
64-bit:	pscp.exe	(or by FTP)	(signature)
psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTP)			
32-bit:	psftp.exe	(or by FTP)	(signature)
64-bit:	psftp.exe	(or by FTP)	(signature)
puttytel.exe (a Telnet-only client)			
32-bit:	puttytel.exe	(or by FTP)	(signature)
64-bit:	puttytel.exe	(or by FTP)	(signature)
plink.exe (a command-line interface to the PuTTY back ends)			
32-bit:	plink.exe	(or by FTP)	(signature)
64-bit:	plink.exe	(or by FTP)	(signature)
pageant.exe (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)			
32-bit:	pageant.exe	(or by FTP)	(signature)
64-bit:	pageant.exe	(or by FTP)	(signature)
puttygen.exe (a RSA and DSA key generation utility)			
32-bit:	puttygen.exe	(or by FTP)	(signature)
64-bit:	puttygen.exe	(or by FTP)	(signature)
putty.zip (a .ZIP archive of all the above)			
32-bit:	putty.zip	(or by FTP)	(signature)
64-bit:	putty.zip	(or by FTP)	(signature)

2. Convert your private key using PuTTYgen
    - Open puttygen.exe, select RSA, and click on Load



No key.

Generate a public/private key pair

Load an existing private key file

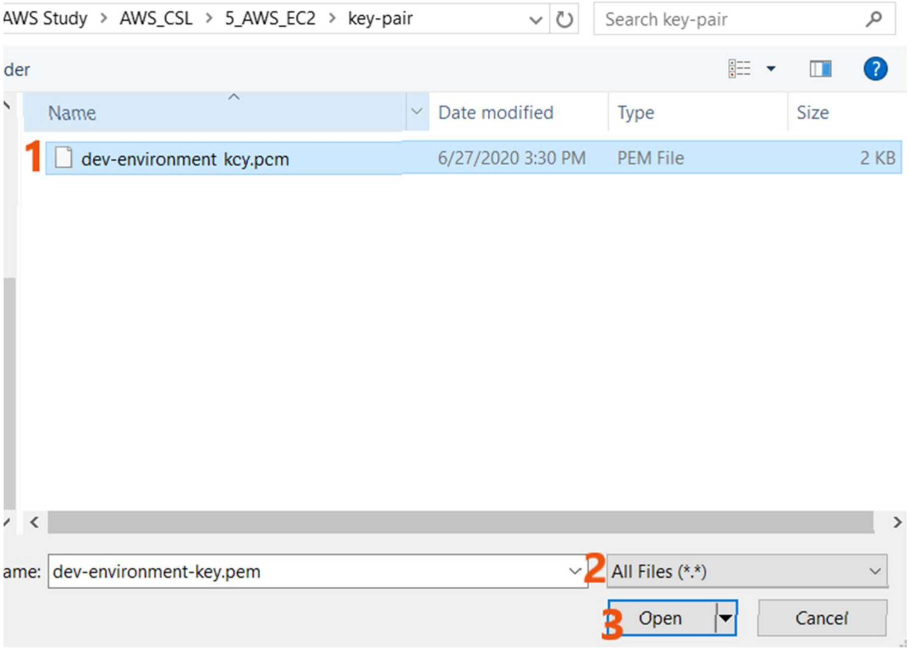
Save the generated key

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

- By default, PuTTYgen displays only files with the extension .ppk. To locate your .pem file, select the option to display files of all types. Select your .pem file for the key pair that you specified when you launched your instance and click to Open. PuTTYgen displays a notice that the .pem file was successfully imported.



AWS Study > AWS_CSL > 5_AWS_EC2 > key-pair

Search key-pair

Name	Date modified	Type	Size
1 dev-environment key.pem	6/27/2020 3:30 PM	PEM File	2 KB

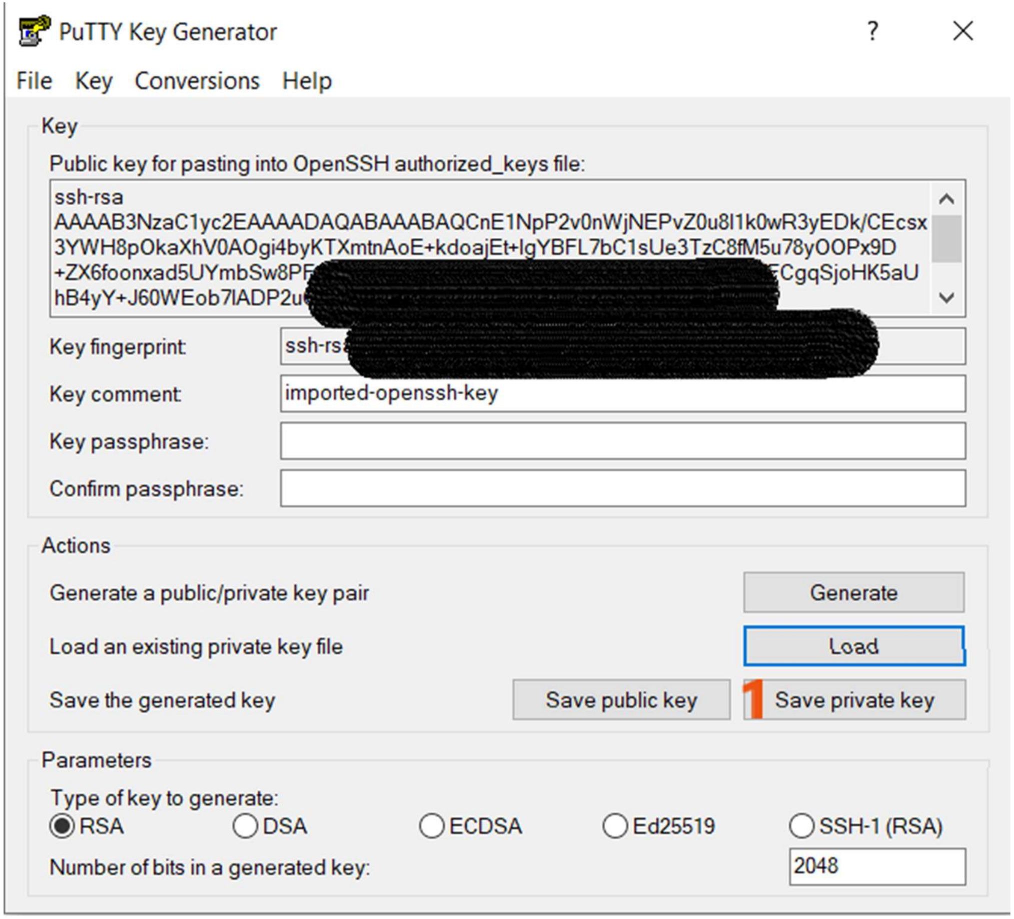
ame: dev-environment-key.pem

2 All Files (*.*)

3 Open

Cancel

- To save the key in the format that PuTTY can use, click Save private key. PuTTYgen displays a warning about saving the key without a passphrase. Click on Yes.



PuTTY Key Generator

Key

Public key for pasting into OpenSSH authorized_keys file:

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCnE1NpP2v0nWjNEPvZ0u8l1k0wR3yEDk/CEcsx
3YWH8pOkaXhV0AOgi4byKTXmtnAoE+kdoajEt+lgYBFL7bC1sUe3TzC8fM5u78yOOPx9D
+ZX6foonxad5UYmbSw8PF[redacted]ECgqSjoHK5aU
hB4yY+J60WEob7lADP2u

Key fingerprint: ssh-rs[redacted]

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair — Generate

Load an existing private key file — Load

Save the generated key — Save public key — 1 Save private key

Parameters

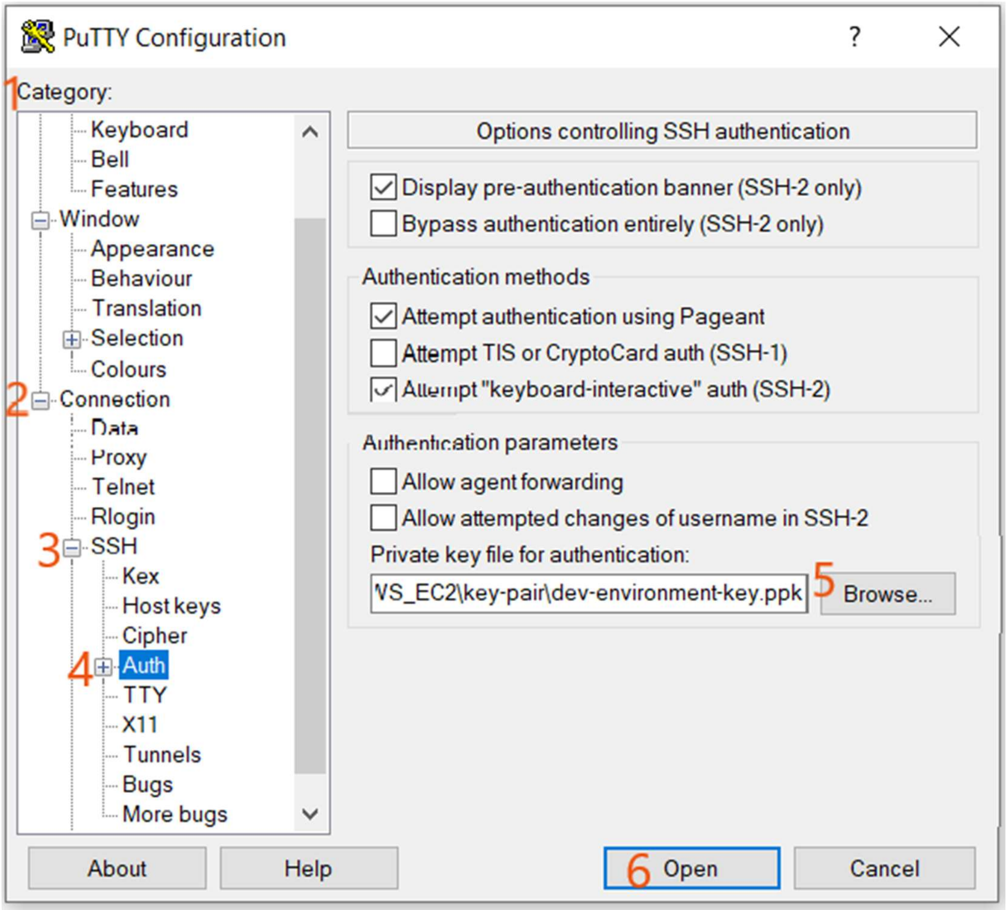
Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

- In the Category, expand Connection type, expand SSH, and then select Auth

- Click on Browse. Select the .ppk file that you generated for your key pair and Select Open



PuTTY Configuration

Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
□ Bypass authentication entirely (SSH-2 only)

Authentication methods

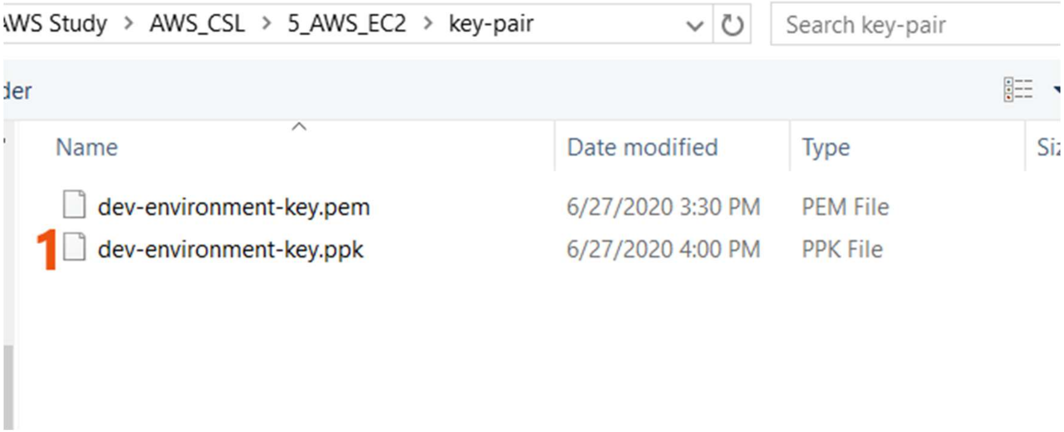
☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

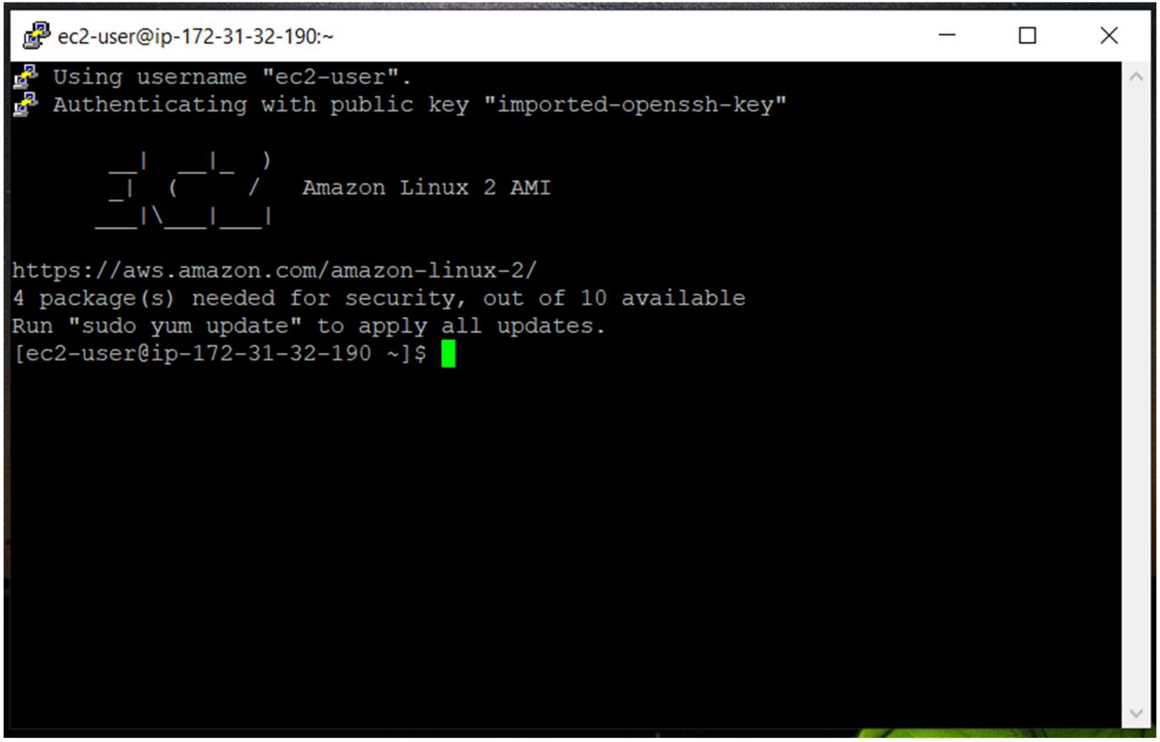
Private key file for authentication:
VS_EC2\key-pair\dev-environment-key.ppk

- Provide the name for the key that you used for the key pair (for example, dev-environment-key) and click on Save.
PuTTY automatically adds the .ppk file extension.



Name	Date modified	Type
dev-environment-key.pem	6/27/2020 3:30 PM	PEM File
dev-environment-key.ppk	6/27/2020 4:00 PM	PPK File

- For first time connection, PuTTY displays a security alert dialog box that asks whether you trust the host to which you are connecting, Click on Yes. A window opens and you are connected to your instance



```
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
4 package(s) needed for security, out of 10 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-32-190 ~]$
```

Part B:

Launch your instance

To launch an Amazon EC2 instance using the AMI you selected, use the aws ec2 run-instances command. You can launch the instance into a virtual private cloud (VPC).

Initially, your instance appears in the pending state, but changes to the running state after a few minutes.

The following example shows how to launch a t2.micro instance in the specified subnet of a VPC. Replace the *italicized* parameter values with your own

aws ec2 run-instances --image-id ami-xxxxxxxx --count 1 --instance-type t2.micro --key-name MyKeyPair --security-group-ids sg-903004f8 --subnet-id subnet-6e7f829e

Add a tag to your instance

A tag is a label that you assign to an AWS resource. It enables you to add metadata to your resources that you can use for a variety of purposes. For more information, see Tagging Your Resources in the *Amazon EC2 User Guide for Linux Instances*.

The following example shows how to add a tag with the key name "Name" and the value "MyInstance" to the specified instance, by using the aws ec2 create-tags command.

aws ec2 create-tags --resources i-5203422c --tags Key=Name,Value=MyInstance

You can use the AWS CLI to list your instances and view information about them. You can list all your instances, or filter the results based on the instances that you're interested in.

The following examples show how to use the aws ec2 describe-instances command.

The following command lists all your instances.

$ **aws ec2 describe-instances**

The following command filters the list to only your t2.micro instances and outputs only the InstanceId values for each match.

```
$aws ec2 describe-instances --filters "Name=instance-type,Values=t2.micro" --query
"Reservations[].Instances[].InstanceId"
```

Terminate your instance

Terminating an instance deletes it. You can't reconnect to an instance after you've terminated it. As soon as the state of the instance changes to shutting-down or terminated, you stop incurring charges for that instance. If you want to reconnect to an instance later, use stop-instances instead of terminate-instances. For more information, see Terminate Your Instance in the *Amazon EC2 User Guide for Linux Instances*.

To delete an instance, you use the command aws ec2 terminate-instances to delete it.

```
aws ec2 terminate-instances --instance-ids i-5203422c
```

To create an ec2 instance using CLI, you need the following.

1. Security group ID
2. Key pair name
3. AMI Id
4. Subnet ID

We will create each resource using the CLI. If you have existing resources, you can directly use the respective resource IDs instead of creating them.

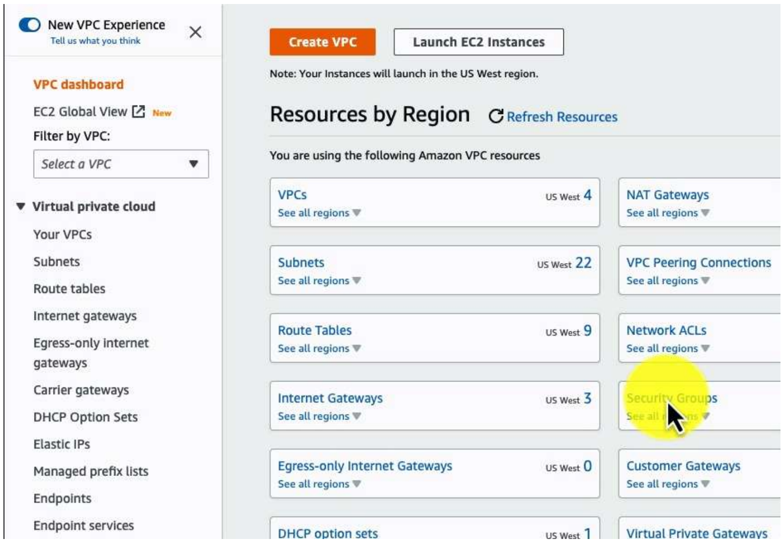
Get VPC ID and Subnet ID

To create a security group, you need the following two IDs

1. **VPC ID:** To create a security group
2. **One Subnet ID:** To launch ec2 instance.

You can get these details from the AWS Management console.

Go to the VPC dashboard and click on the VPC. You will get the VPC ID, click on the subnets, and search with the VPC ID to list all the subnets associated with that VPC, as shown below.


New VPC Experience
Tell us what you think
VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP Option Sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
Create VPC
Launch EC2 Instances

Note: Your Instances will launch in the US West region.

Resources by Region ⟳ Refresh Resources

You are using the following Amazon VPC resources

VPCs See all regions US West 4
NAT Gateways See all regions
Subnets See all regions US West 22
VPC Peering Connections See all regions
Route Tables See all regions US West 9
Network ACLs See all regions
Internet Gateways See all regions US West 3
Security Groups See all regions
Egress-only Internet Gateways See all regions US West 0
Customer Gateways See all regions
DHCP option sets US West 1
Virtual Private Gateways

I’m going to use the following VPC and subnet IDs for this guide. You need to replace these IDs with your VPC and subnet ID.

To launch Instance command:

```
$aws ec2 run-instances --image-id ami-0dfcb1ef8550277af --count 1 --instance-type t2.micro --key-name RSCOE --security-group-ids sg-0c00bc9fa987e28c8 --subnet-id subnet-03591a615a626ead5
```

Conclusion:-

In this practical, we successfully launched and connected Amazon EC2 instances using both the AWS Management Console and the AWS Command Line Interface (CLI). We learned how to configure instance details, create and use key pairs, manage security groups, and establish a secure SSH connection using PuTTY. This experiment provided hands-on experience in deploying and managing virtual machines on the AWS cloud platform, enhancing our understanding of cloud infrastructure, automation, and remote connectivity.