Lab 3 – EC2

Today's tasks:

1. Create an EC2 instance in public subnet
2. SSH into it and run a web app
3. Create an EC2 instance in private subnet and ssh from the public instance via private IP
4. Check whether the private instance has internet connection
5. Delete the entire VPC with its resources then recreate everything again.

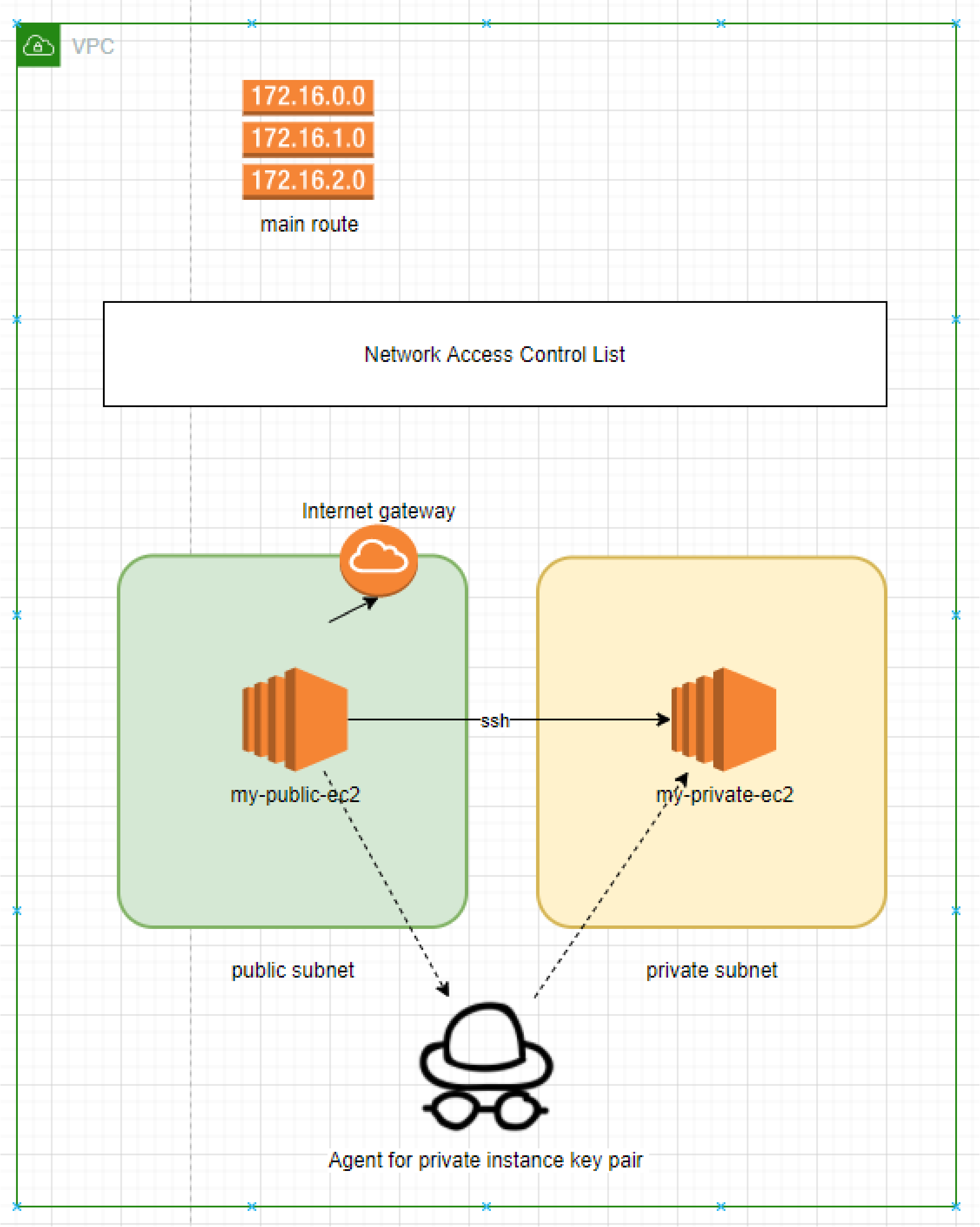
Bonus tasks:

- Create a NAT gateway (Elastic IP will get allocated with it) in public subnet then check the internet connection in private instance by pinging google.
  - Create a RouteTable for private subnets
  - Associate private subnets with the Route table for private subnets
  - Create the NAT gateway
  - Add a route to the Route table for private subnets pointing to the NAT
- Draw its architecture diagram.

Submit items below in one pdf file:

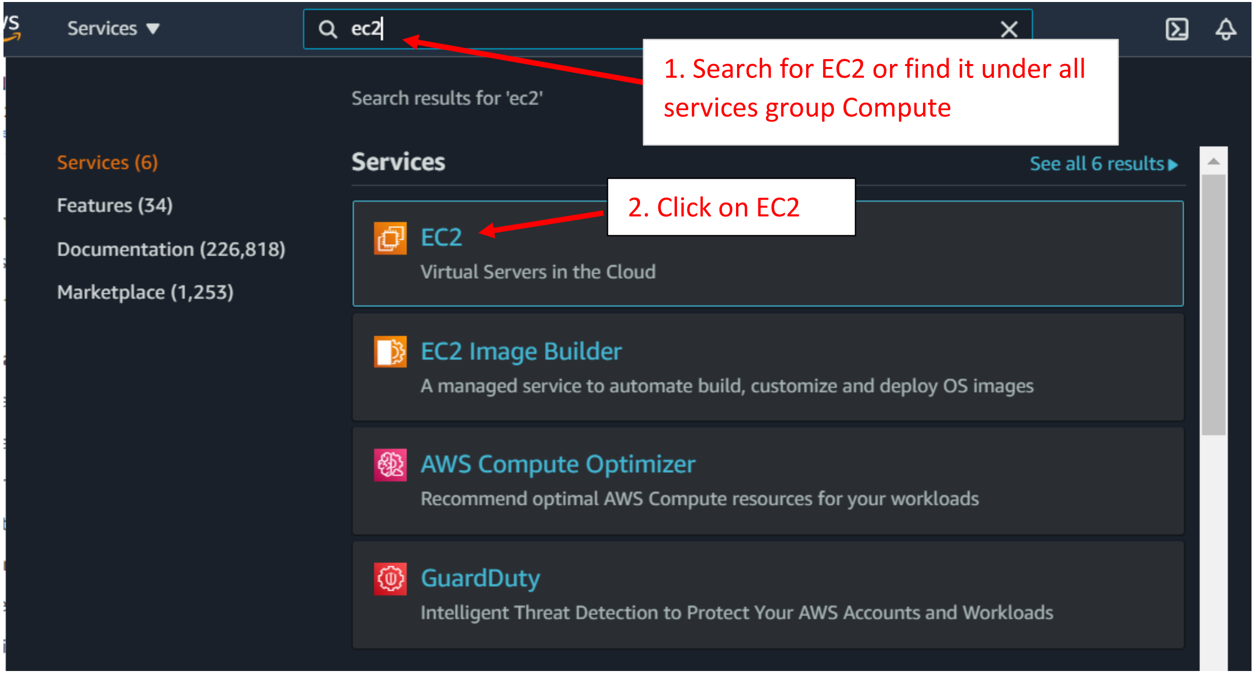
1. Screenshot of a web app that shows your name.
2. Submit the IP address of the web app that must work.
3. Screenshot of ssh-ing from public to private instance via private IP.
4. Screenshot of the result when pinging google in private instance.
5. Screenshot of what came up when you hit delete button on VPC.

Arcihtecture diagram of what we will build out on the cloud today.



Instruction 1. Create an EC2 in public subnet

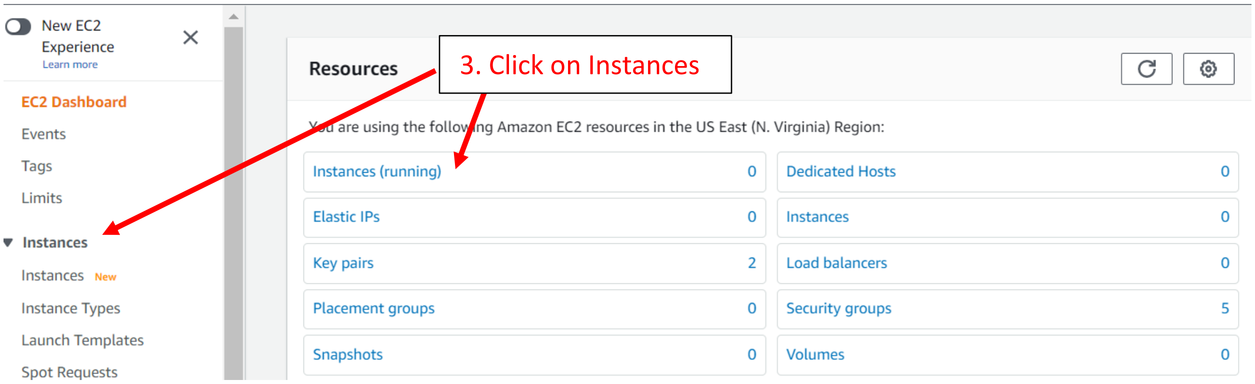
Go to the EC2 Instances Display


Services ▼
ec2
Search results for 'ec2'
Services (6)
Features (34)
Documentation (226,818)
Marketplace (1,253)
Services
See all 6 results ▶
EC2
Virtual Servers in the Cloud
EC2 Image Builder
A managed service to automate build, customize and deploy OS images
AWS Compute Optimizer
Recommend optimal AWS Compute resources for your workloads
GuardDuty
Intelligent Threat Detection to Protect Your AWS Accounts and Workloads

1. Search for EC2 or find it under all services group Compute

2. Click on EC2

…

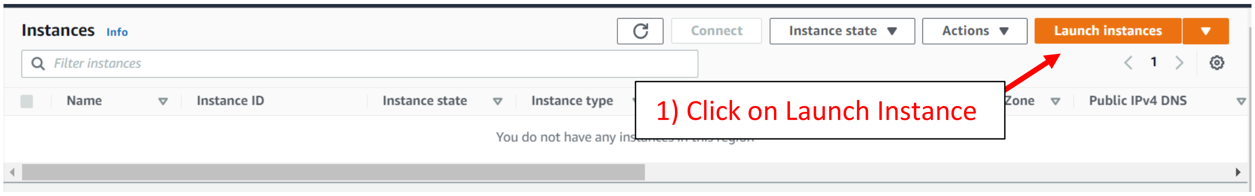


3. Click on Instances

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	2	Load balancers	0
Placement groups	0	Security groups	5
Snapshots	0	Volumes	0

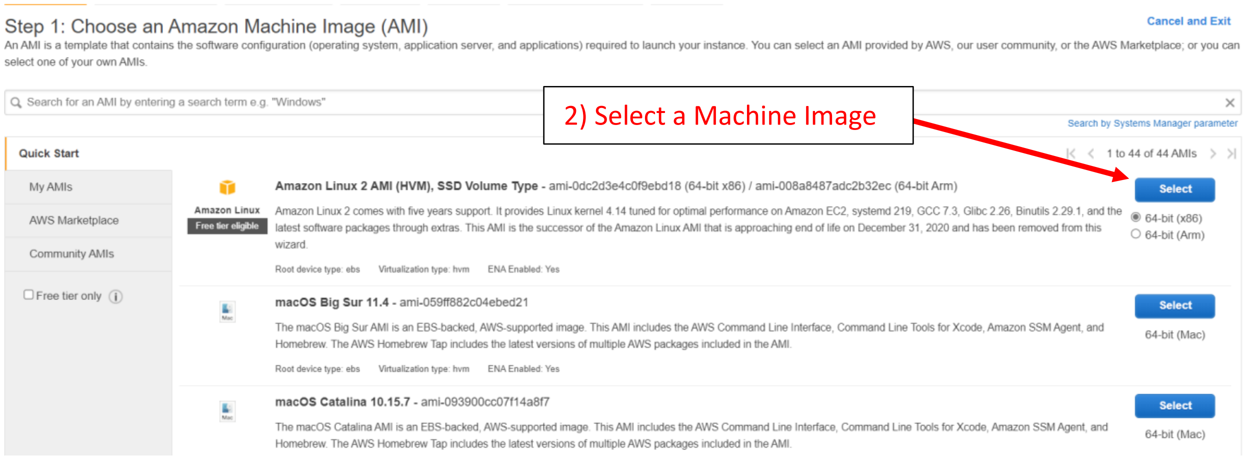
Start an EC2 Instance



You do not have any instances in this region

1) Click on Launch Instance

…



Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

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

2) Select a Machine Image

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0dc2d3e4c0f9ebd18 (64-bit x86) / ami-008a8487adc2b32ec (64-bit Arm)

Amazon Linux — 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. 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

Select ● 64-bit (x86) ○ 64-bit (Arm)

macOS Big Sur 11.4 - ami-059ff882c04ebed21

The macOS Big Sur AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

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

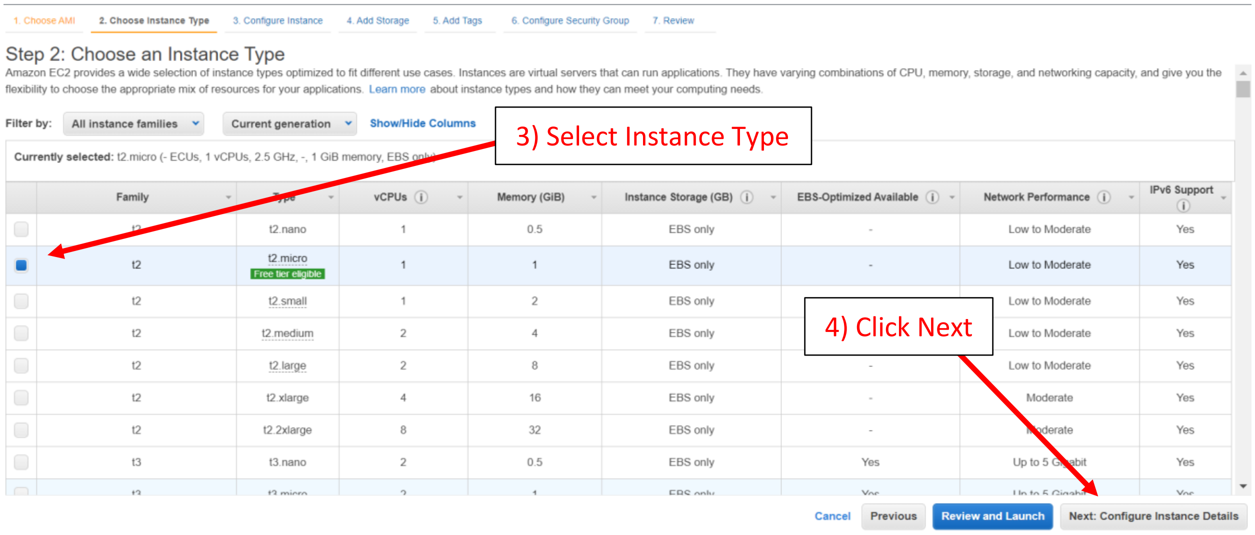
Select 64-bit (Mac)

macOS Catalina 10.15.7 - ami-093900cc07f14a8f7

The macOS Catalina AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

Select 64-bit (Mac)

...



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

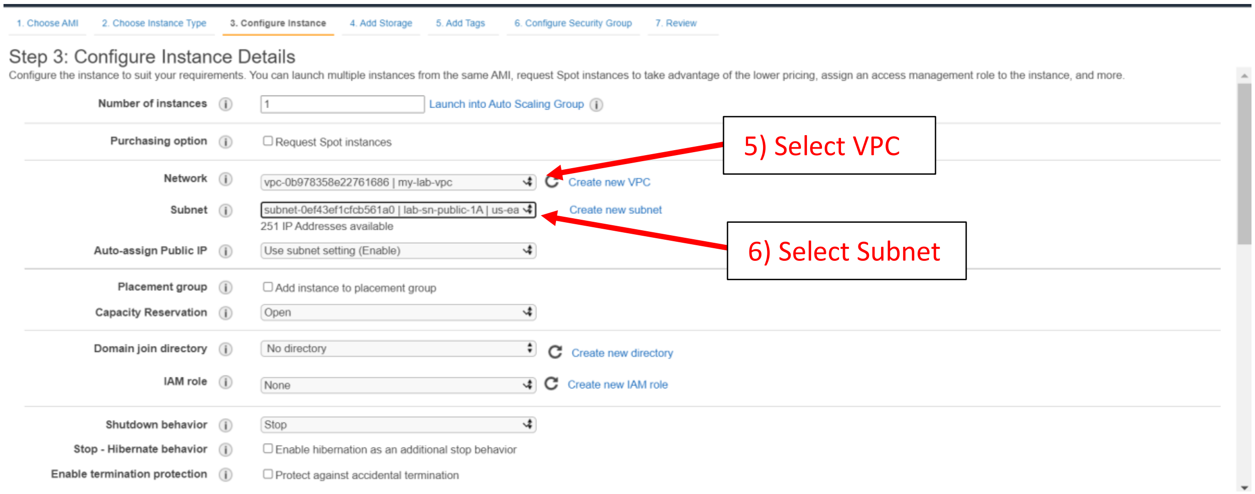
3) Select Instance Type

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
□	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
■	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
□	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
□	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

4) Click Next

...



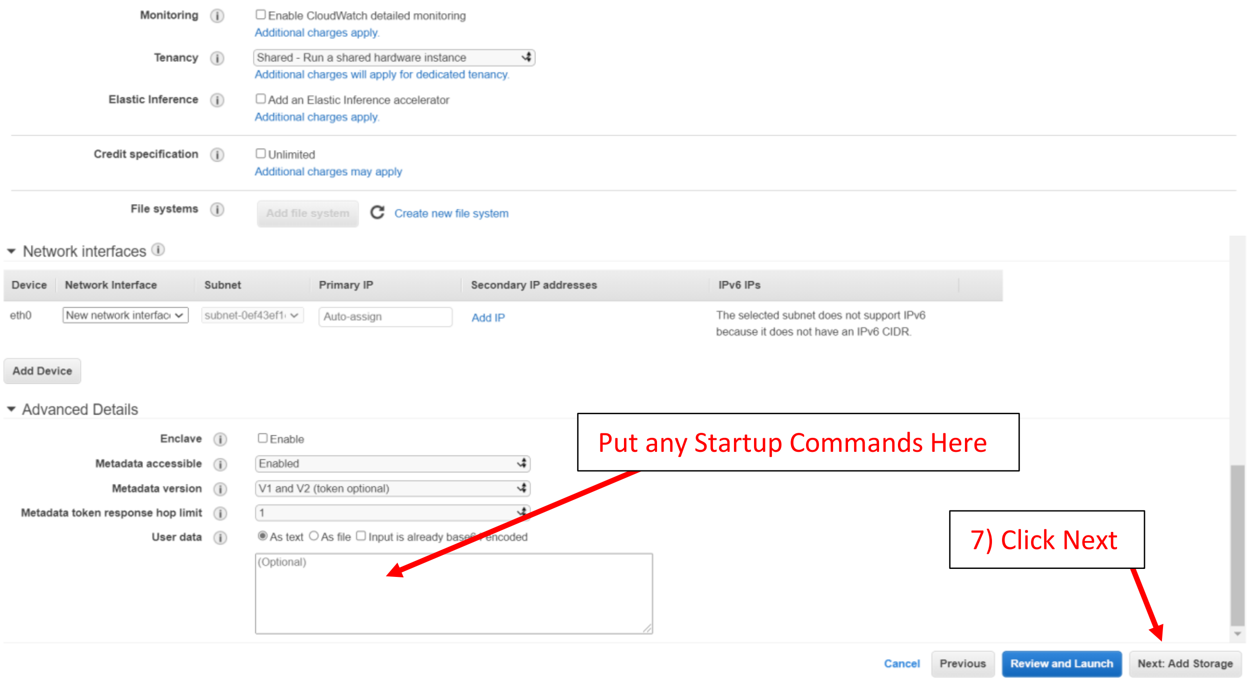
Step 3: Configure Instance Details

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-0b978358e22761686 | my-lab-vpc Create new VPC
Subnet	subnet-0ef43ef1cfcb561a0 | lab-sn-public-1A | us-ea Create new subnet 251 IP Addresses available
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
Shutdown behavior	Stop
Stop - Hibernate behavior	□ Enable hibernation as an additional stop behavior
Enable termination protection	□ Protect against accidental termination

5) Select VPC

6) Select Subnet



Monitoring ⓘ □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy ⓘ Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

Elastic Inference ⓘ □ Add an Elastic Inference accelerator
Additional charges apply.

Credit specification ⓘ □ Unlimited
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 interfac	subnet-0ef43ef1	Auto-assign	Add IP	The selected subnet does not support IPv6 because it does not have an IPv6 CIDR.

Add Device

▾ Advanced Details

Enclave ⓘ □ Enable

Metadata accessible ⓘ Enabled

Metadata version ⓘ V1 and V2 (token optional)

Metadata token response hop limit ⓘ 1

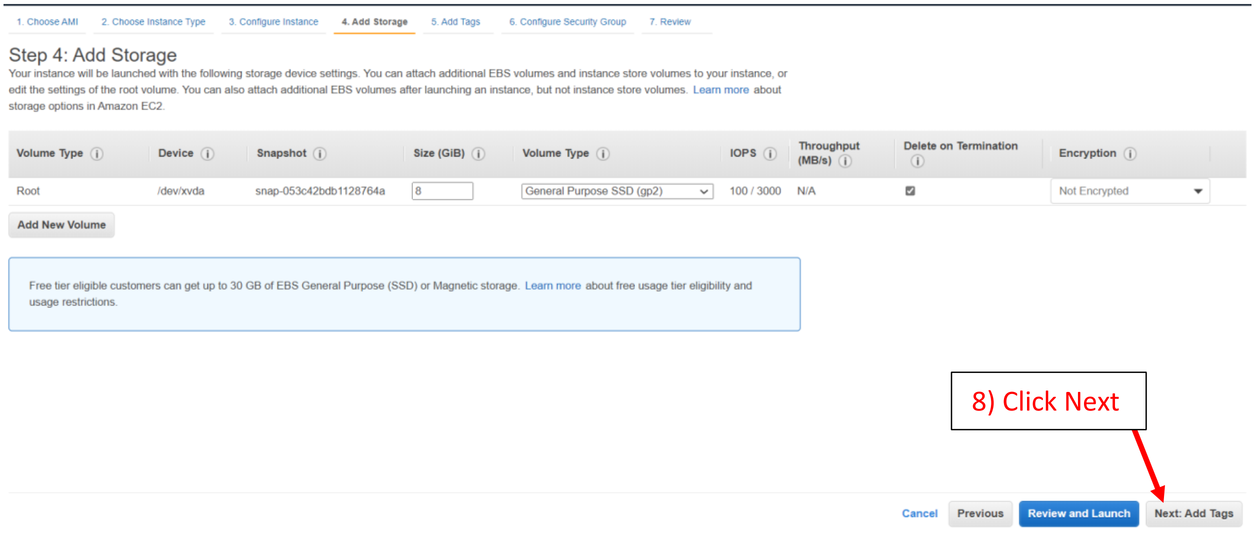
User data ⓘ ● As text ○ As file □ Input is already base64 encoded

(Optional)

Put any Startup Commands Here

7) Click Next

…



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.

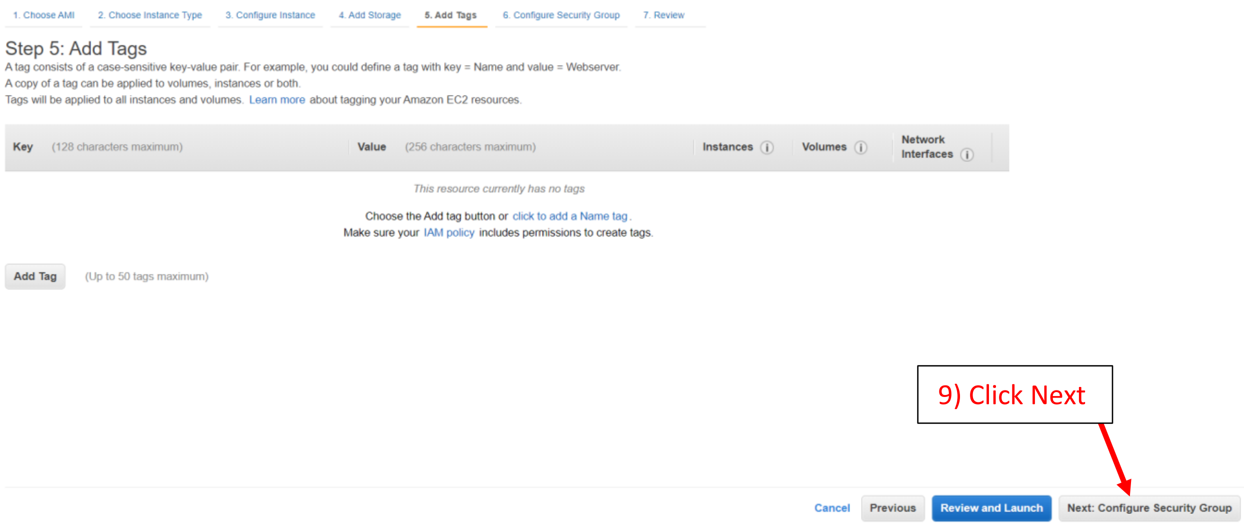
Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption ⓘ
Root	/dev/xvda	snap-053c42bdb1128764a	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

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.

8) Click Next

…



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.

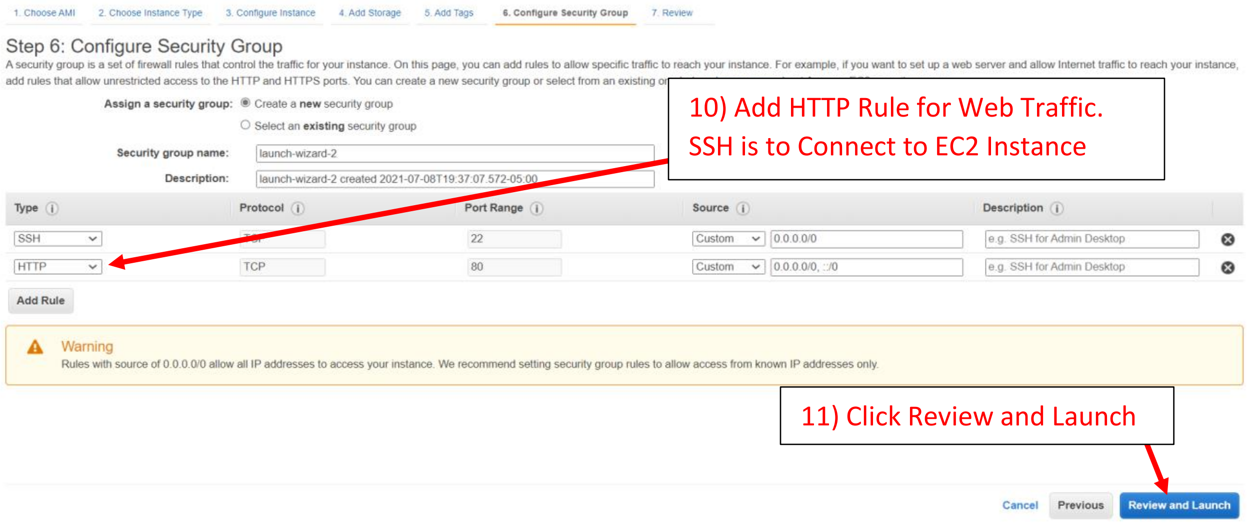
Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ	Network Interfaces ⓘ

This resource currently has no tags

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

9) Click Next

…



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 o

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

Security group name: launch-wizard-2

Description: launch-wizard-2 created 2021-07-08T19:37:07.572-05:00

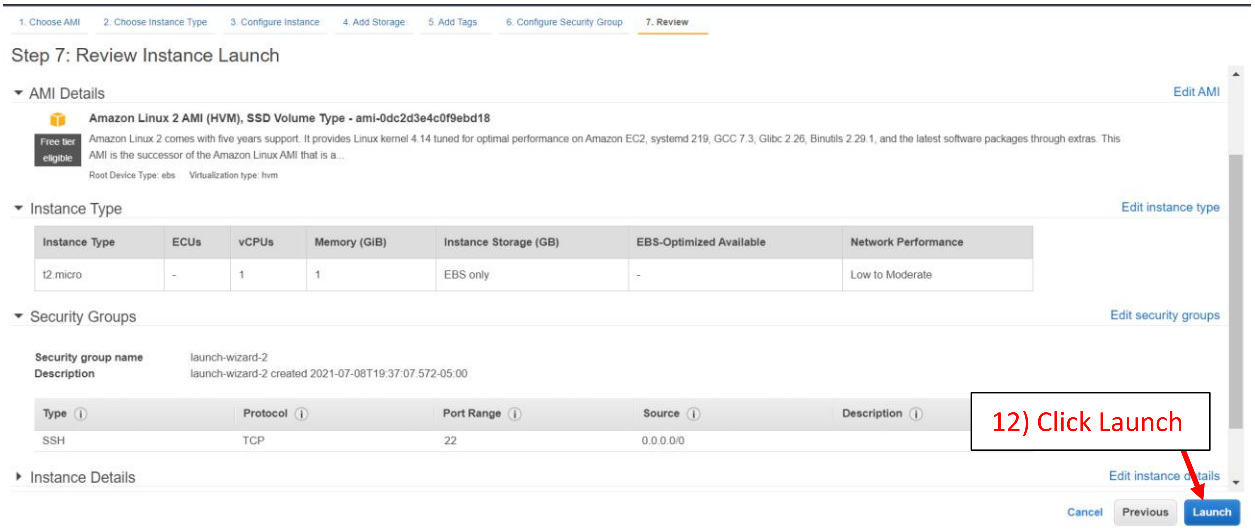
Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ		Description ⓘ
SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

⚠ 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.

10) Add HTTP Rule for Web Traffic.
SSH is to Connect to EC2 Instance

11) Click Review and Launch

…



Step 7: Review Instance Launch

▾ AMI Details

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0dc2d3e4c0f9ebd18

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. This AMI is the successor of the Amazon Linux AMI that is a ...

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	-	1	1	EBS only	-	Low to Moderate

▾ Security Groups

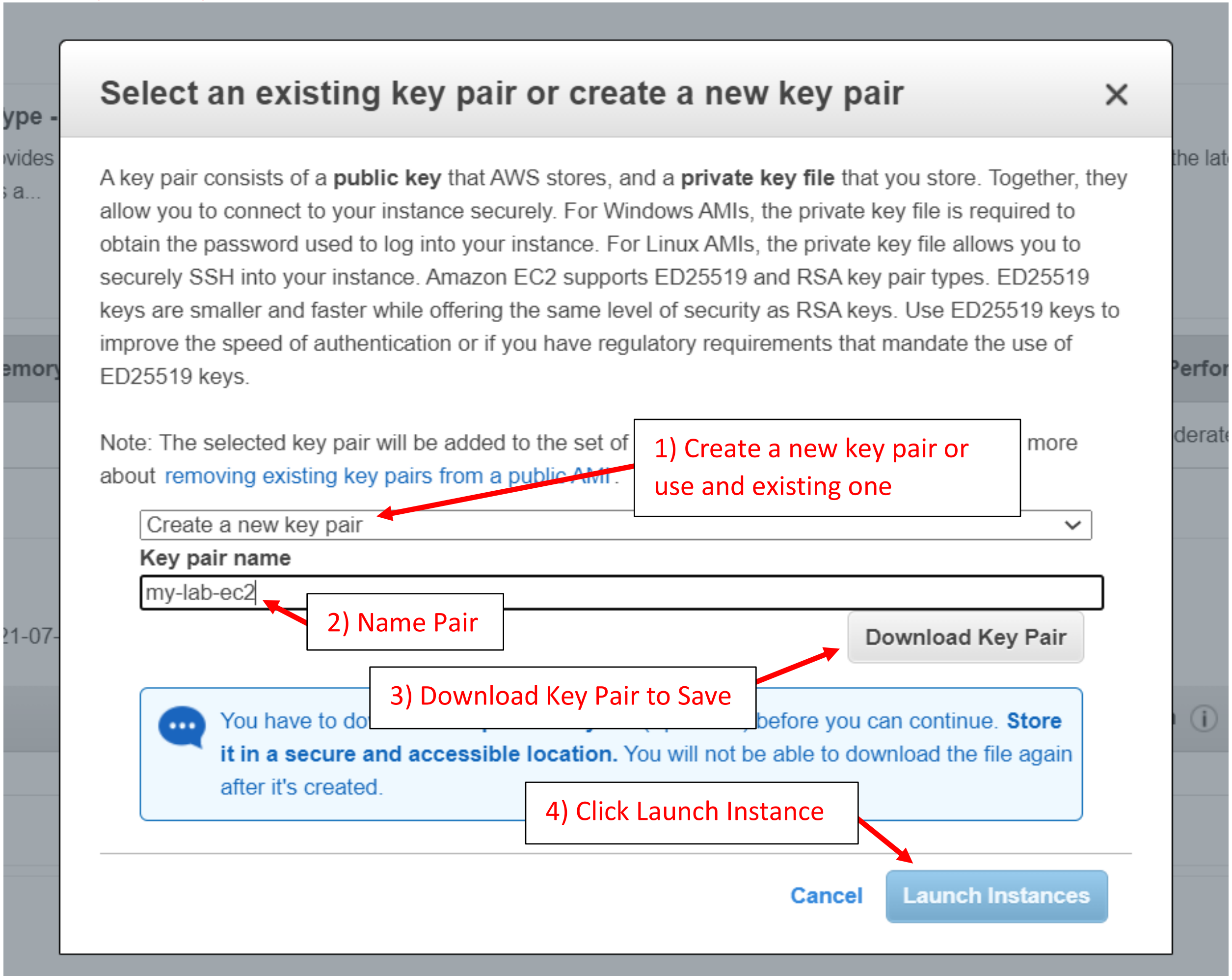
Security group name launch-wizard-2
Description launch-wizard-2 created 2021-07-08T19:37:07.572-05:00

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

▸ Instance Details

12) Click Launch

Save Key Pair so you can Access the Instance



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. Amazon EC2 supports ED25519 and RSA key pair types. ED25519 keys are smaller and faster while offering the same level of security as RSA keys. Use ED25519 keys to improve the speed of authentication or if you have regulatory requirements that mandate the use of ED25519 keys.

Note: The selected key pair will be added to the set of more about removing existing key pairs from a public AMI.

Create a new key pair

Key pair name

my-lab-ec2

You have to do 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.

1) Create a new key pair or use and existing one

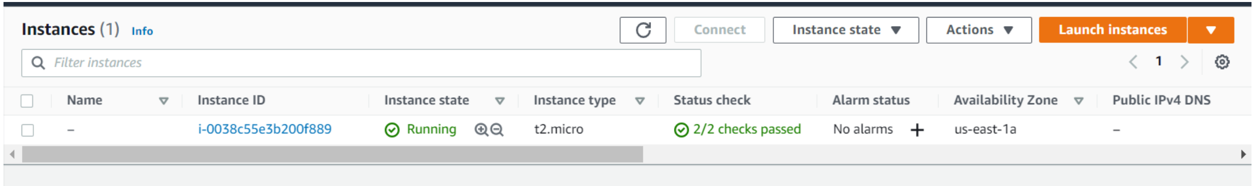
2) Name Pair

3) Download Key Pair to Save

4) Click Launch Instance

...

Check the Status in the Instances Display. After a Few Minutes Instance State should be Running and Status Check should show 2/2 checks passed



Instances (1)

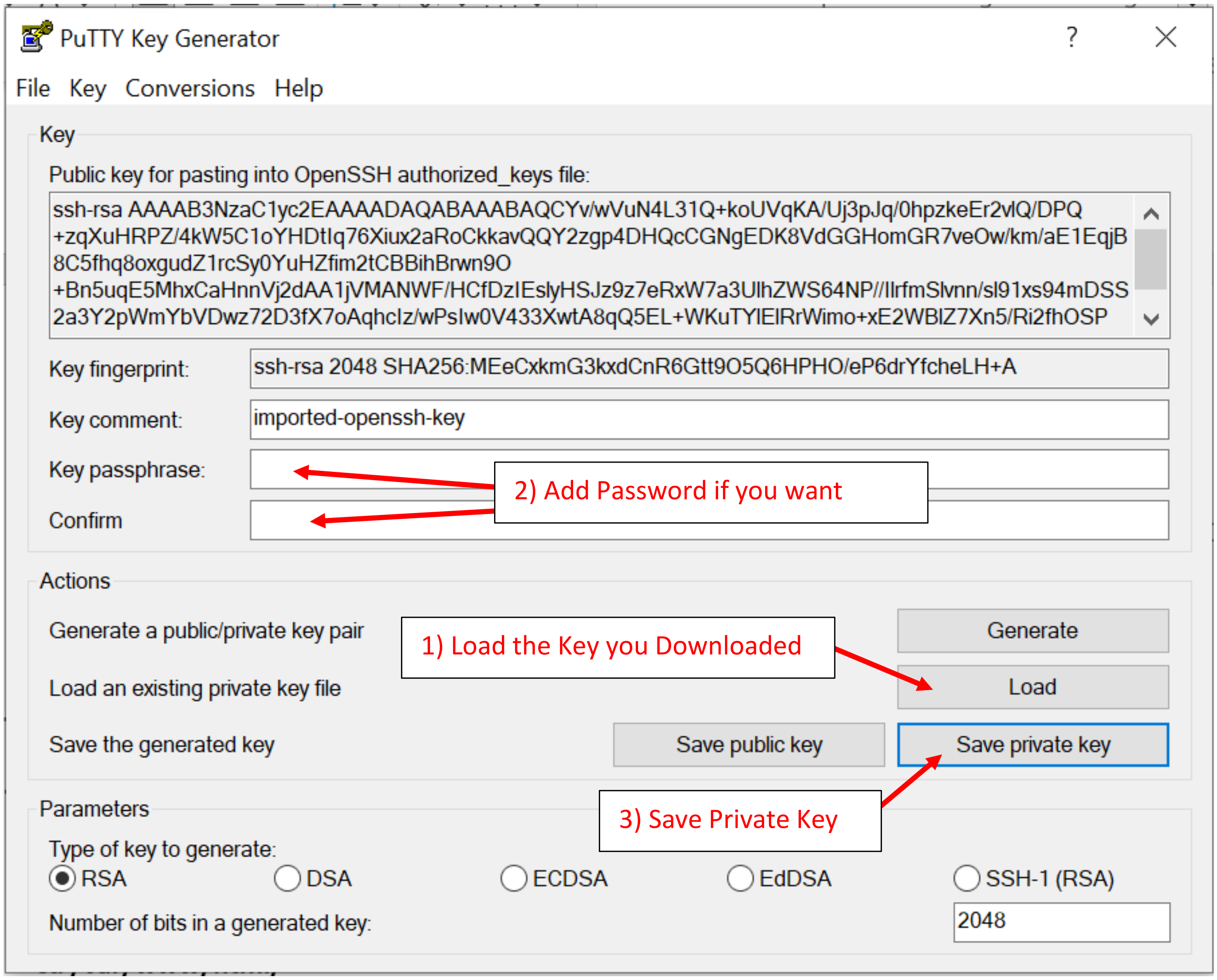
□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
□	–	i-0038c55e3b200f889	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms +	us-east-1a	–

Instruction 2. SSH into the EC2 and create a web app

1. SSH into the EC2 (https://docs.aws.amazon.com/quickstarts/latest/vmlaunch/step-2-connect-to-instance.html)

   SSH through PuTTY if windows. Mac is much easier. Select EC2, click on connect, click on SSH Client tab. And follow that.

PuTTYGen – Generate pem to PuTTY private keyCreate



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCYv/wVuN4L31Q+koUVqKA/Uj3pJq/0hpzkeEr2vlQ/DPQ
+zqXuHRPZ/4kW5C1oYHDtIq76Xiux2aRoCkkavQQY2zgp4DHQcCGNgEDK8VdGGHomGR7veOw/km/aE1EqjB
8C5fhq8oxgudZ1rcSy0YuHZfim2tCBBihBrwn9O
+Bn5uqE5MhxCaHnnVj2dAA1jVMANWF/HCfDzIEslyHSJz9z7eRxW7a3UlhZWS64NP//IlrfmSlvnn/sl91xs94mDSS
2a3Y2pWmYbVDwz72D3fX7oAqhclz/wPslw0V433XwtA8qQ5EL+WKuTYlElRrWimo+xE2WBlZ7Xn5/Ri2fhOSP
```

Key fingerprint: ssh-rsa 2048 SHA256:MEeCxkmG3kxdCnR6Gtt9O5Q6HPHO/eP6drYfcheLH+A

Key comment: imported-openssh-key

Key passphrase:

Confirm

2) Add Password if you want

Generate a public/private key pair

Load an existing private key file

1) Load the Key you Downloaded

Save the generated key

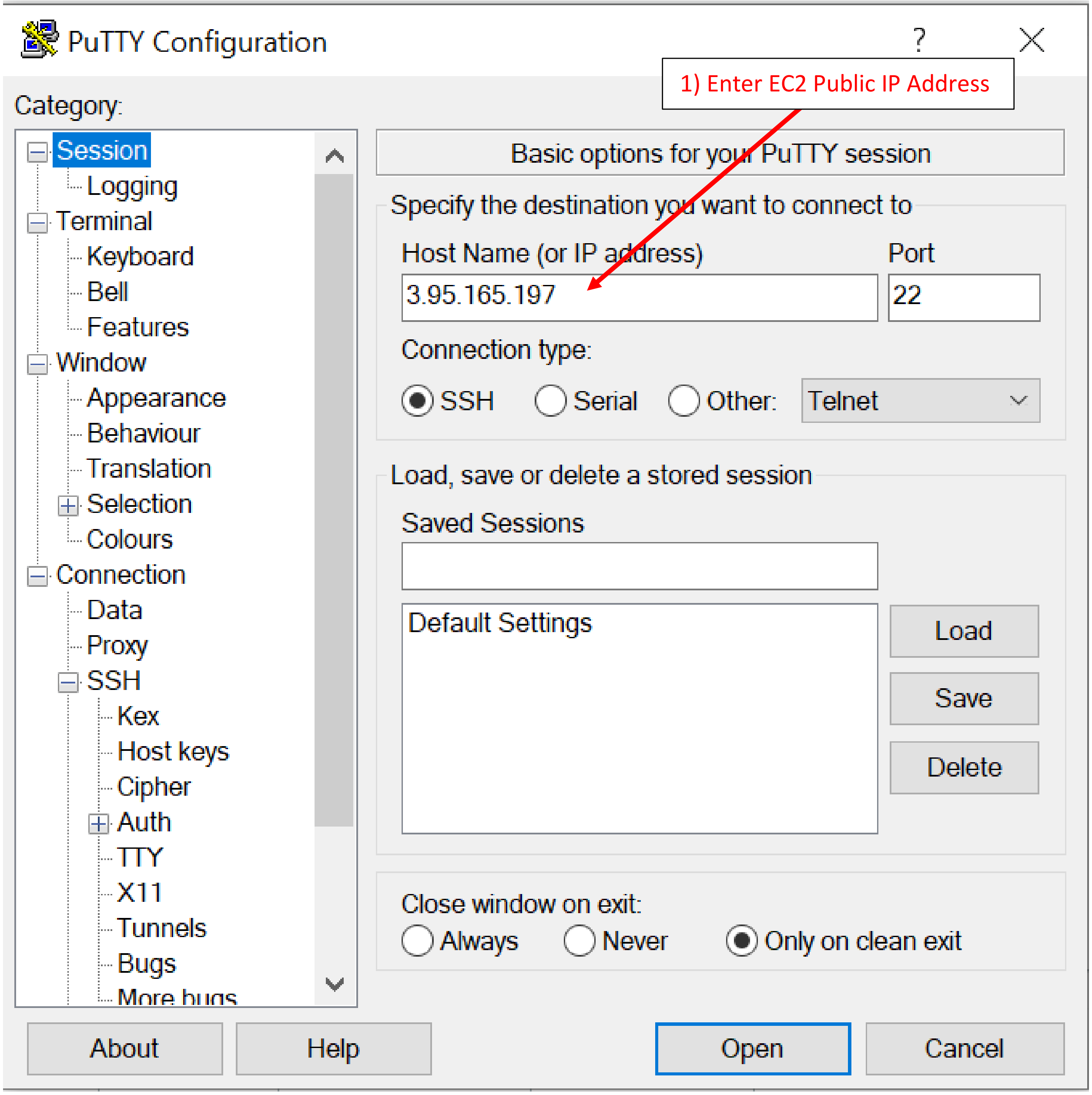
3) Save Private Key

Type of key to generate:

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

Number of bits in a generated key: 2048

Connect to EC2 Instance via Putty



1) Enter EC2 Public IP Address

PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 3.95.165.197

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

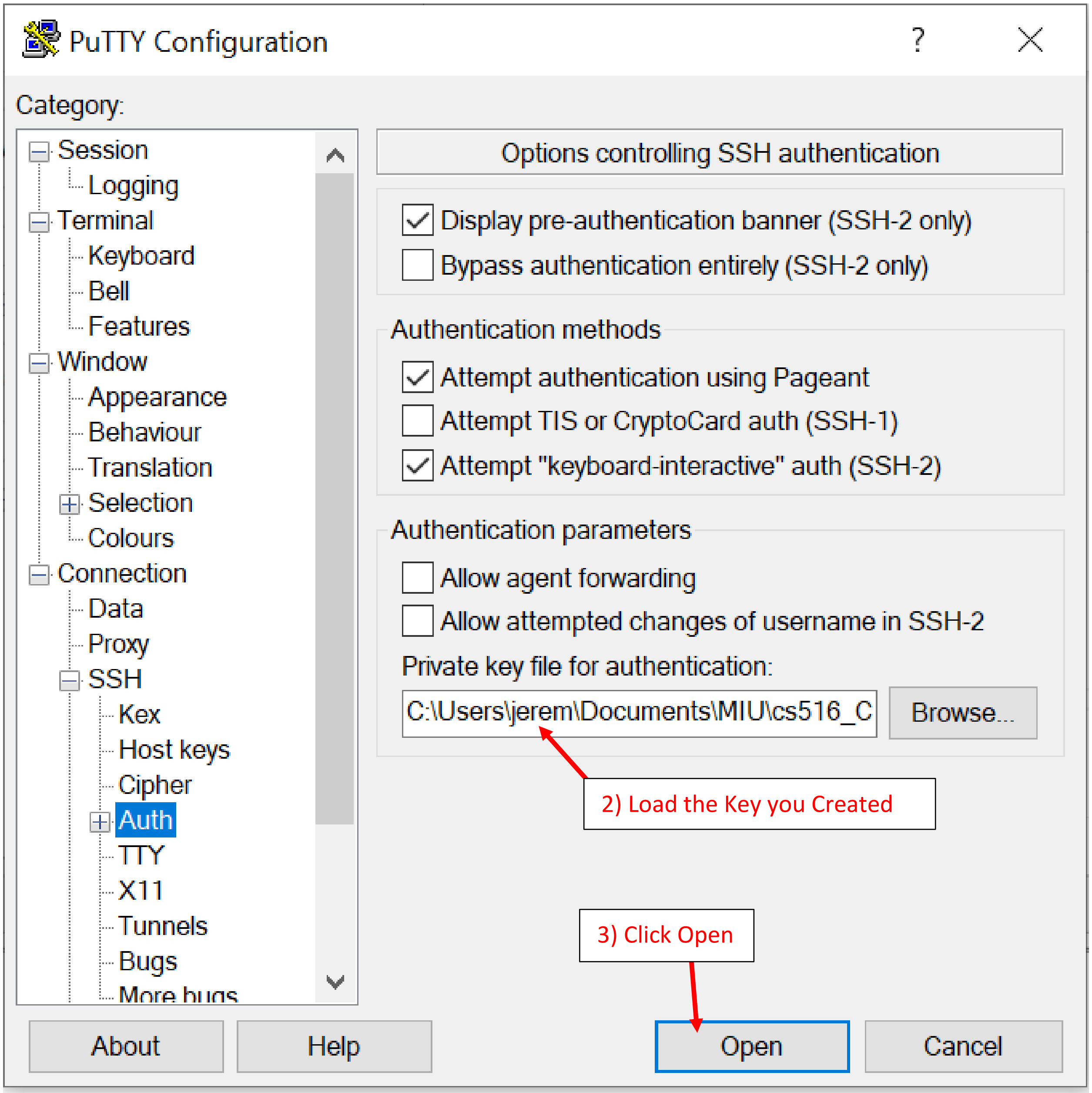
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

...



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

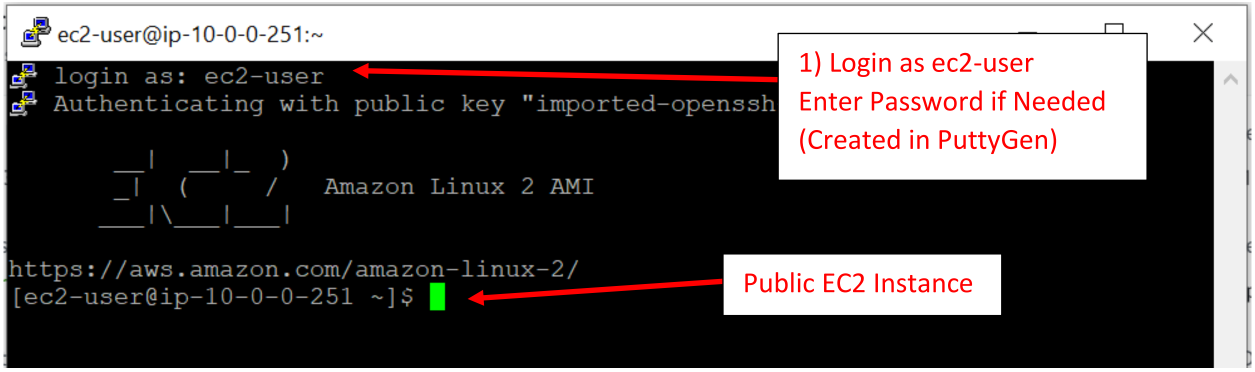
□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication: C:\Users\jerem\Documents\MIU\cs516_C

2) Load the Key you Created

3) Click Open

Log Into EC2 Instance



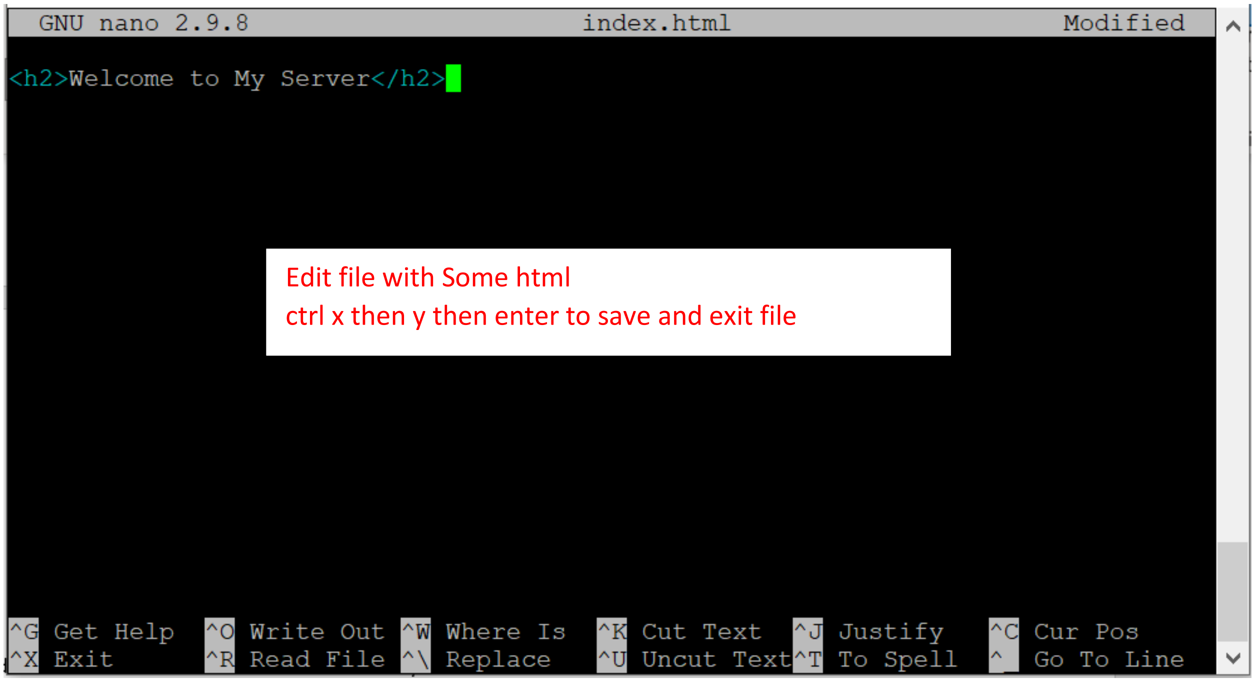
```
login as: ec2-user
Authenticating with public key "imported-openssh

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-251 ~]$
```

1) Login as ec2-user
Enter Password if Needed
(Created in PuttyGen)

Public EC2 Instance

Start Static Web Service

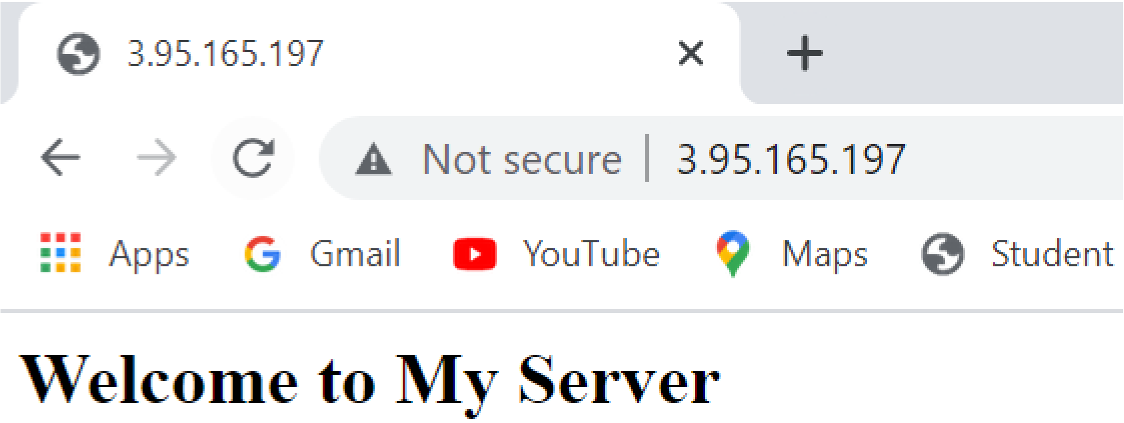
sudo -s (Change to Root User)
yum update –y (Update if Needed)
yum install –y httpd (Install Server)
service httpd start (Start Server)
cd /var/www/html/ (Change Directory)
touch index.html (Create File for Server to Serve)
nano index.html (Edit File to Serve)



```
  GNU nano 2.9.8                    index.html                    Modified

<h2>Welcome to My Server</h2>











^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text^T To Spell    ^_ Go To Line
```

Edit file with Some html
ctrl x then y then enter to save and exit file

Test Website with EC2 Instance Public IP



Welcome to My Server

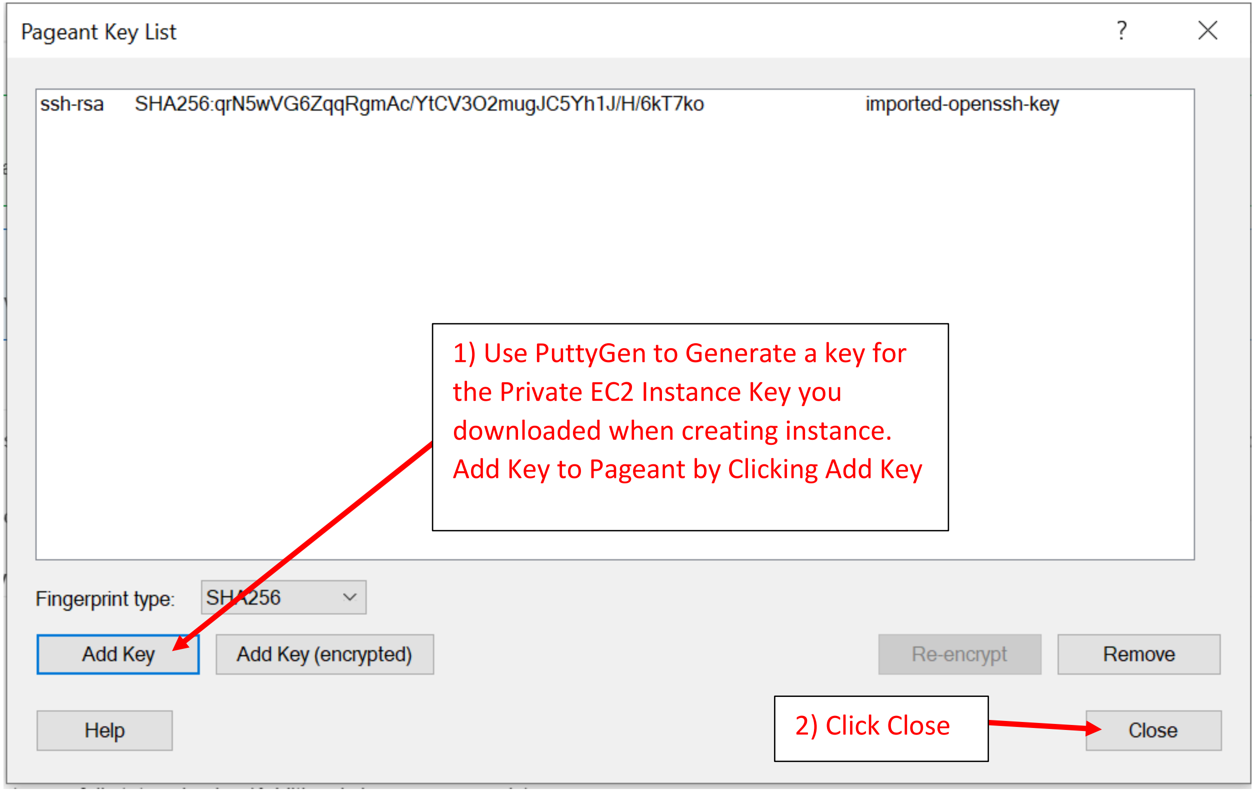
Instruction 3. Create an EC2 in private subnet. SSH into it from public EC2 using the private IP.

Repeat the same steps of create an EC2 in public subnet. But **select one of the private subnets!**

Connect from the bastion (EC2 in public subnet) to the EC2 in private subnet. Detailed instructions for Windows below. Both Mac (Linux) and Windows users refer this full article https://aws.amazon.com/blogs/security/securely-connect-to-linux-instances-running-in-a-private-amazon-vpc/

Use **PAgent** (download https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html) and load ppk in PAgent. - The reason we are using the PAgent is that, we can't store the private key for the private instance in the public instance. Because if a hacker takes over the public instance, who can easily take over the private instance as well. So the best practice is to store the private key of the private instance in an agent. Use that when ssh-ing. Another best practice is to use System Manager by giving the required IAM role to the EC2 instance that is what AWS recommends.

Add Private EC2 Instance Key to Pageant



Pageant Key List

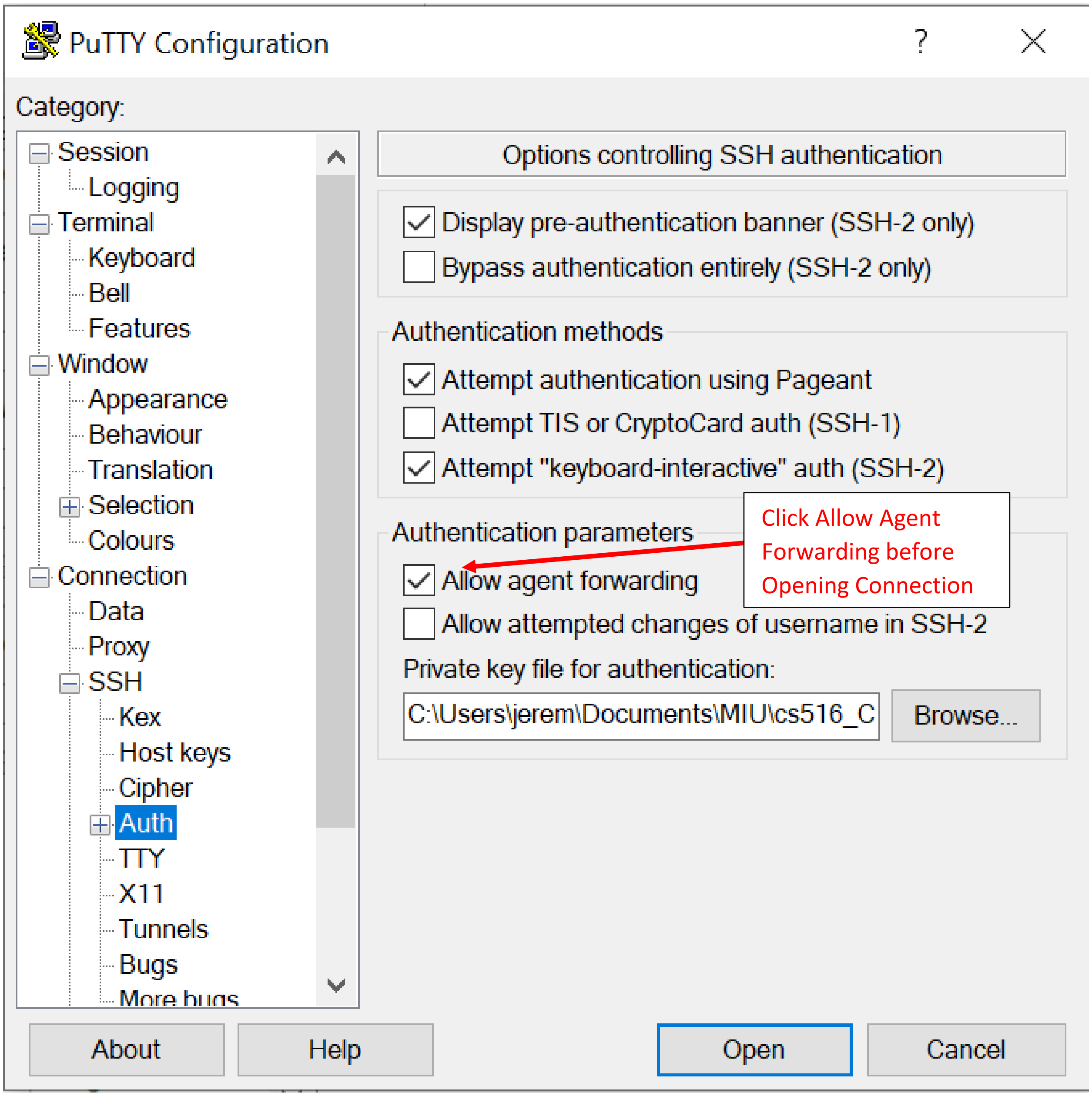
ssh-rsa SHA256:qrN5wVG6ZqqRgmAc/YtCV3O2mugJC5Yh1J/H/6kT7ko imported-openssh-key

Fingerprint type: SHA256

1) Use PuttyGen to Generate a key for the Private EC2 Instance Key you downloaded when creating instance. Add Key to Pageant by Clicking Add Key

2) Click Close

Connect to Public EC2 Instance. Same as above execpt select **allow agent forwarding,** which will forward the private instance key you attached.



PuTTY Configuration

Category:

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

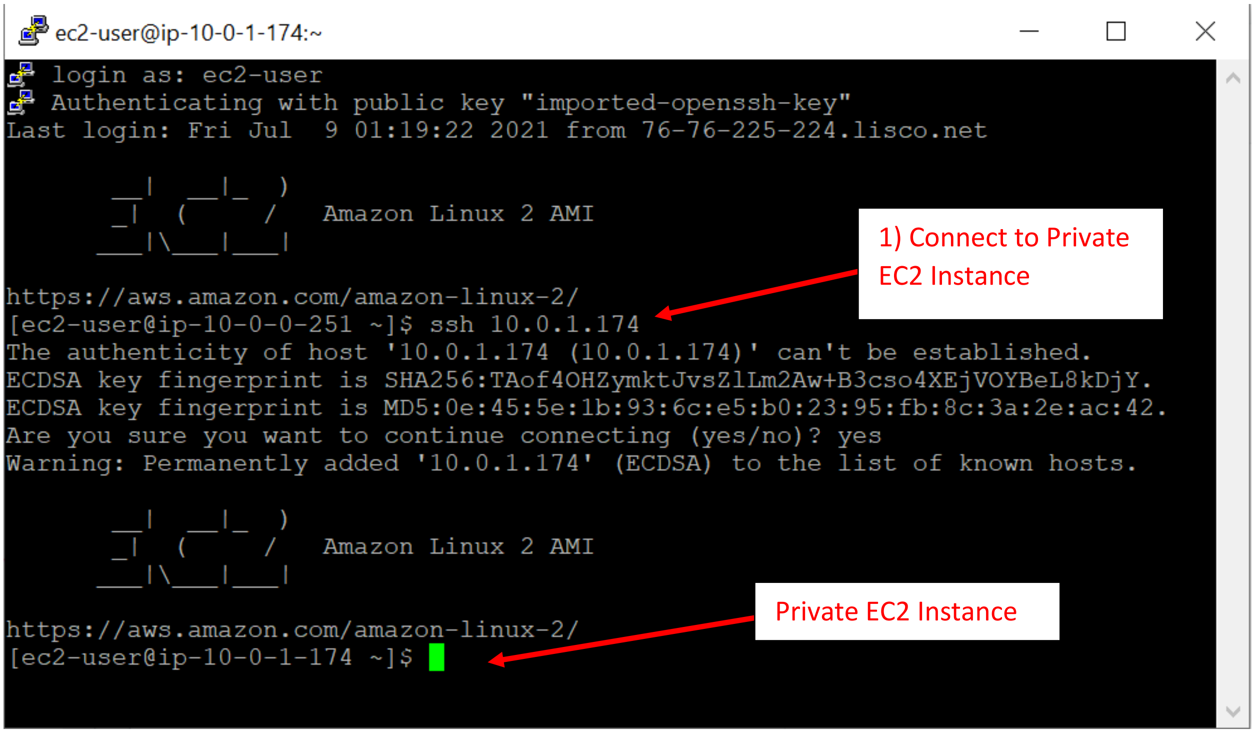
□ Allow attempted changes of username in SSH-2

Private key file for authentication:

C:\Users\jerem\Documents\MIU\cs516_C

Click Allow Agent Forwarding before Opening Connection

SSH from public instance (bastion or jump) to web server in private subnet using **ssh 'private-ip-of-the-instance'**



```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Fri Jul  9 01:19:22 2021 from 76-76-225-224.lisco.net

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-251 ~]$ ssh 10.0.1.174
The authenticity of host '10.0.1.174 (10.0.1.174)' can't be established.
ECDSA key fingerprint is SHA256:TAof4OHZymktJvsZlLm2Aw+B3cso4XEjVOYBeL8kDjY.
ECDSA key fingerprint is MD5:0e:45:5e:1b:93:6c:e5:b0:23:95:fb:8c:3a:2e:ac:42.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.174' (ECDSA) to the list of known hosts.

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-174 ~]$
```

1) Connect to Private EC2 Instance

Private EC2 Instance