Project 1.a Create an AWS Instance, setup restriction of web access

For this specialization, I have created an AMI image with LAMP package installed for you to clone an instance and use it for learning the cybersecurity concepts, security policy and related enforcement procedures. If you intend to use your own AWS paid account, you can still use the Coursera-CS5910-ami2 image in the Community AMIs to clone an instance with LAMP server package in about 2 minutes.

However, if you decide not to use your credit card but still enjoy the free available service offered by AWS for education purpose, you are lucky that, after 12/31/2021, even though AWS stopped their old AWS Educate free service, they will offer new AWS Academy free service for our learners. The only bad news now is that they currently restricts the use of non-AWS owned images. Therefore you cannot use the Coursera-CS5910-ami2 image in the Community AMIs with AWS Academy account, you will need to clone an Amazon AWS instance (virtual machine) from the Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type image in the Quick Start category and then install LAMP server package for your exercises. The server patches and LAMP installation will take about 30 minutes. The upside is you learn how to install LAMP server package on a Linux platform.

In either case, you will need an AWS account to login to the AWS management console and use their EC2 GUI control to create the instance for our class projects.

Your first task is to apply for your free AWS Academy account or a regular AWS regular basic account. Follow the instruction in Section 1. The AWS regular account provides full access to AWS services with all privileges for learning public cloud computing/security. The AWS academy account allows you to work on the creation of AWS EC2 instances for the exercises of this specialization. However, it restricts the usage of AWS service only in us-east-1 (North Virginia) region.

Warning: Use your AWS regular account wisely, then you will not be charged for running instances for the exercises in learning our specialization. Make sure you stop the instance each time after you finish your exercise! You may be charge small fees for the storage. Please make sure you set up a billing alarm and follow all the guidelines in the lessons, otherwise you might incur costs. We do not take any responsibility for any costs incurred. See http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/free-tier-alarms.html for setting up billing alarm. Note that with your free AWS Academy account, you also need to use your $100 free credit wisely. Make sure to stop your instances after your session. Developing good public cloud hygiene habit is important.

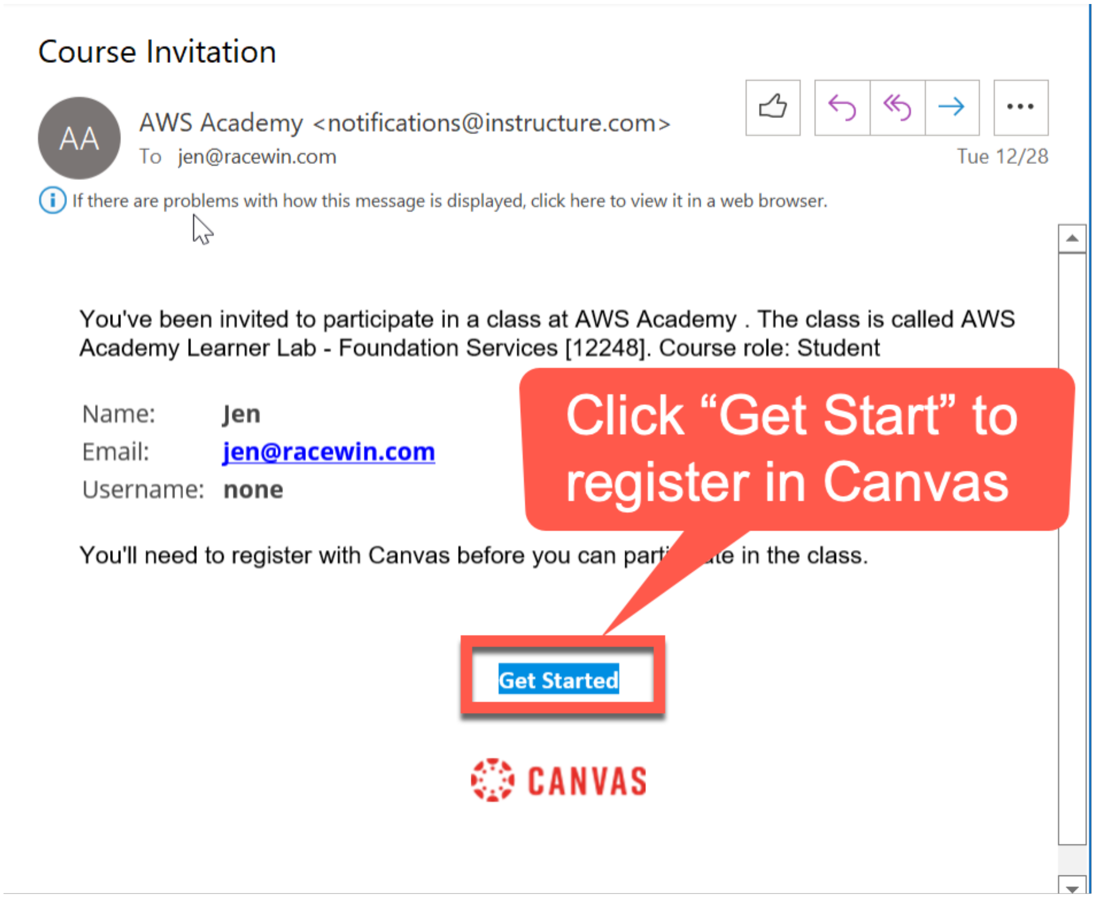
In this project, you will learn how to set up a default project web page. You will learn **the availability support by the AWS EC2 service** and how to **restrict access to the web service** of the instance only to you at home by specifying the sources that allow SSH/HTTP/HTTPS access with Security Group Interface. You will also learn how use the private key to access the AWS Linux instance without needing to provide login or password.

1. Create AWS Account

1.1 Option 1. Create free AWS Academy Account with Basic Support.

For this specialization and certificate, I have worked with AWS Academy to provide an AWS Academy Student Account with $100 free credit for you to conduct the exercises in this specialization. You will not need to show your credit card for the accessing this AWS Academy account. I will need you to email cchow@uccs.edu with subject titled “request AWS Academy account for xxxxxx Coursera course” and include the browser image or the official email from Coursera which proves your enrollment of our Coursera courses. Make sure you indicate clearly the registered email address, which I should use as Username for you to access the AWS Academy portal.

When I added you to the AWS Academy Learner Lab, you will receive an email similar to the one below:



Course Invitation

AWS Academy <notifications@instructure.com>
To jen@racewin.com
Tue 12/28

If there are problems with how this message is displayed, click here to view it in a web browser.

You've been invited to participate in a class at AWS Academy . The class is called AWS Academy Learner Lab - Foundation Services [12248]. Course role: Student

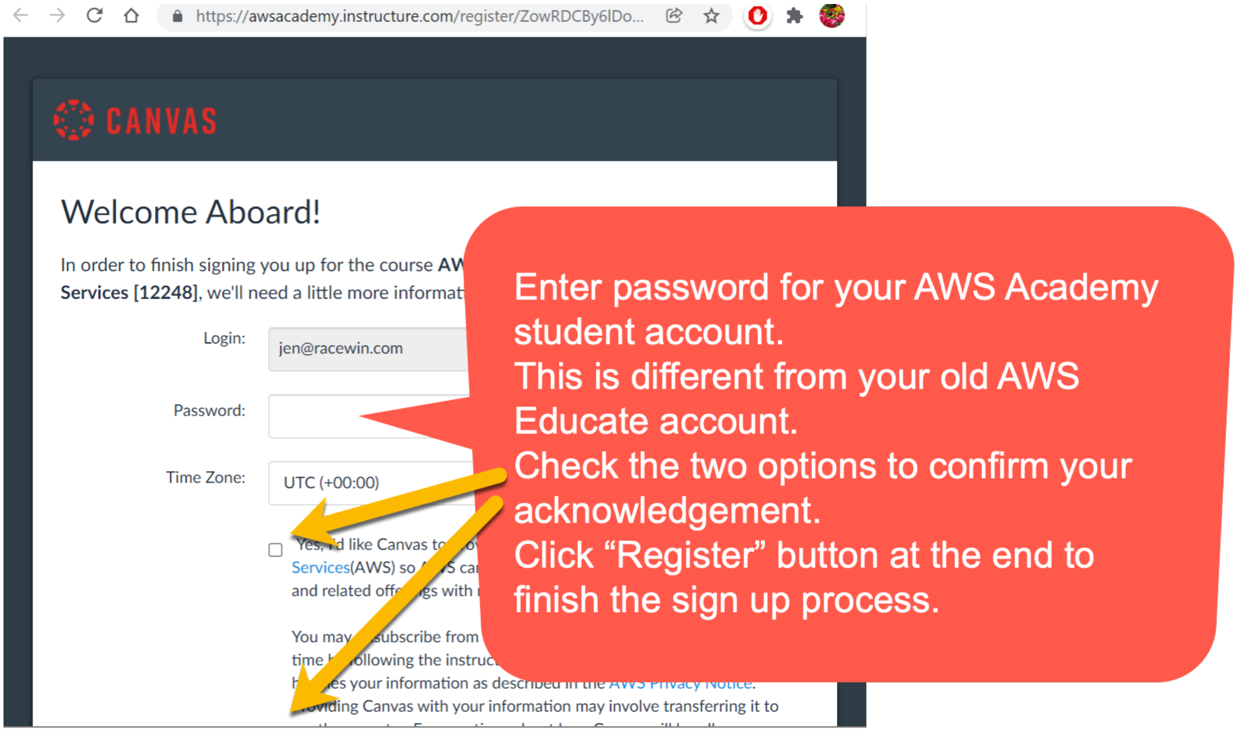
Name:	Jen
Email:	jen@racewin.com
Username:	none

You'll need to register with Canvas before you can part te in the class.

Click “Get Start” to register in Canvas

Click the "Get Started" button. You will be directed to a web site with url similar to

https://awsacademy.instructure.com/courses/12xxx8?invitation=tuuJ6s3gcaYt92sxycafaXXX



Welcome Aboard!

In order to finish signing you up for the course AW... Services [12248], we'll need a little more informat...

Login: jen@racewin.com

Password:

Time Zone: UTC (+00:00)

Enter password for your AWS Academy student account.
This is different from your old AWS Educate account.
Check the two options to confirm your acknowledgement.
Click "Register" button at the end to finish the sign up process.

Enter the password for your AWS Academy student account. This is different from your old AWS Educate account. Check the two options to confirm your acknowledgement. Click "Register" button at the end to finish the sign up process.

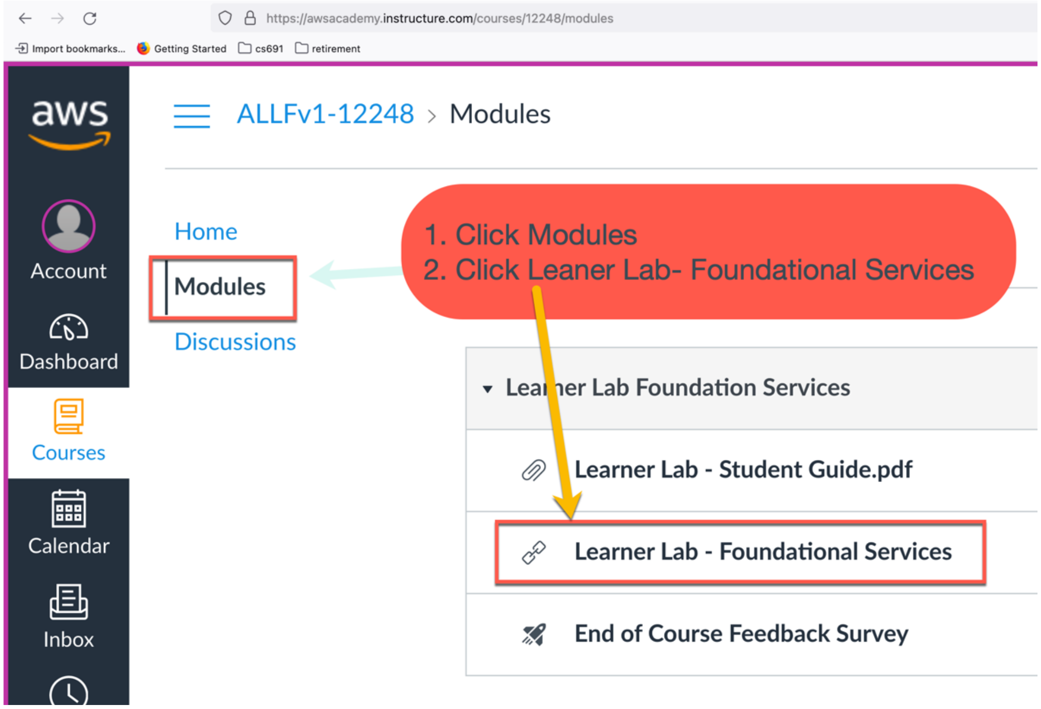
Follow the above steps to register with Canvas, which is a Learning Management System (LMS) for AWS Academy.

Note that with your AWS Academy account, you will not be asked for credit card and set up a regular AWS account with billing. Your access will go through AWS Academy web site and then through vocareum.com 3rd party web site to access free AWS services. Please do not go directly to https://aws.com/ then click the management console on the right side. In that case you will ask to setup regular account with your credit card.

Here are the six steps where you can access the AWS Management Console with free credits for creating AWS EC2 instance to be used for our class projects:

1. Login to your AWS Academy account. https://www.awsacademy.com/SiteLogin
2. Click "Modules"

3. Click “Learner Lab – Foundational Services”



https://awsacademy.instructure.com/courses/12248/modules

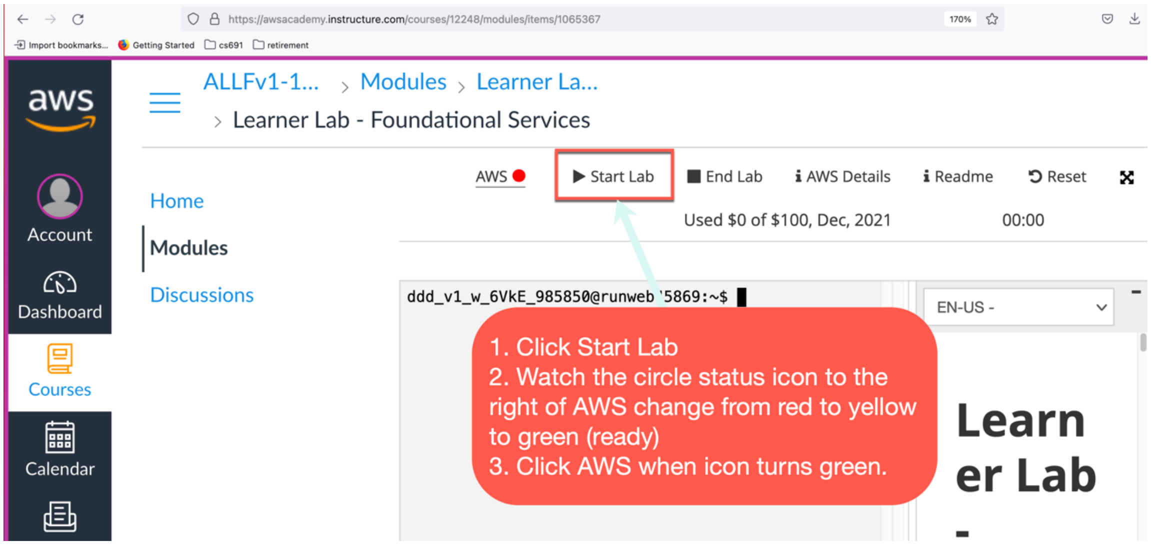
ALLFv1-12248 > Modules

1. Click Modules
2. Click Leaner Lab- Foundational Services

▾ Learner Lab Foundation Services

- Learner Lab - Student Guide.pdf
- Learner Lab - Foundational Services
- End of Course Feedback Survey

4. Click “Start Lab”. Watch the circle status icon to the right of AWS change from red to yellow to green (ready). Click AWS when its right icon turns green.



https://awsacademy.instructure.com/courses/12248/modules/items/1065367

ALLFv1-1... > Modules > Learner La... > Learner Lab - Foundational Services

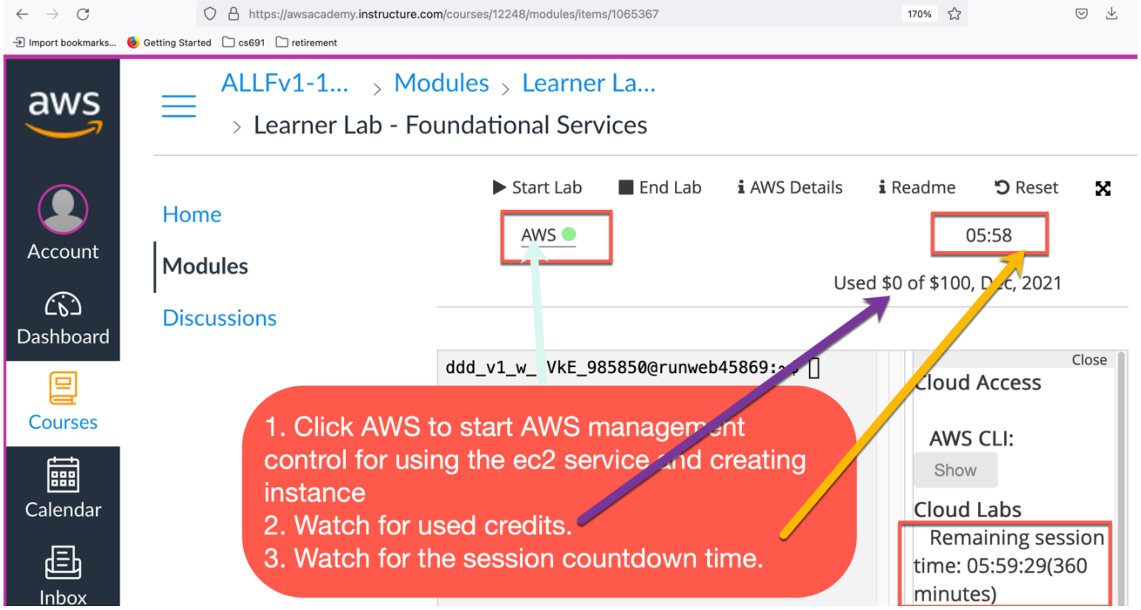
AWS ● ▶ Start Lab ■ End Lab ℹ AWS Details ℹ Readme ⟲ Reset

Used $0 of $100, Dec, 2021 00:00

```
ddd_v1_w_6VkE_985850@runweb'5869:~$ █
```

1. Click Start Lab
2. Watch the circle status icon to the right of AWS change from red to yellow to green (ready)
3. Click AWS when icon turns green.

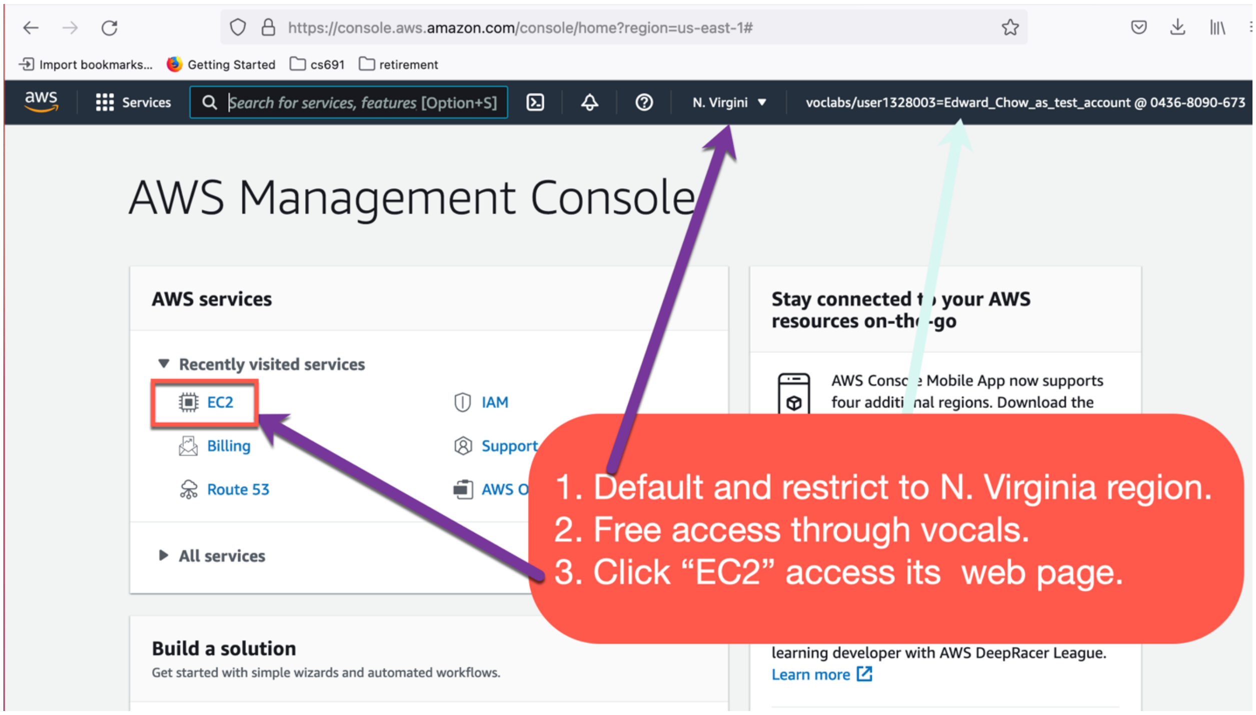
5. Click AWS to start AWS management control for using the ec2 service and creating instance. Watch for used credits and the session countdown time.



1. Click AWS to start AWS management control for using the ec2 service and creating instance
2. Watch for used credits.
3. Watch for the session countdown time.

https://awsacademy.instructure.com/courses/12248/modules/items/1065367
ALLFv1-1...
Modules
Learner La...
Learner Lab - Foundational Services
Account
Dashboard
Courses
Calendar
Inbox
Home
Modules
Discussions
Start Lab
End Lab
AWS Details
Readme
Reset
AWS
05:58
Used $0 of $100, Dec, 2021
Close
Cloud Access
AWS CLI:
Show
Cloud Labs
Remaining session time: 05:59:29(360 minutes)

6. You are now access AWS services through an account under vocstartsoft with an ID and your email. It also shows that you are accessing the default and only region, N. Virginia. Select EC2 AWS service



1. Default and restrict to N. Virginia region.
2. Free access through vocals.
3. Click “EC2” access its web page.

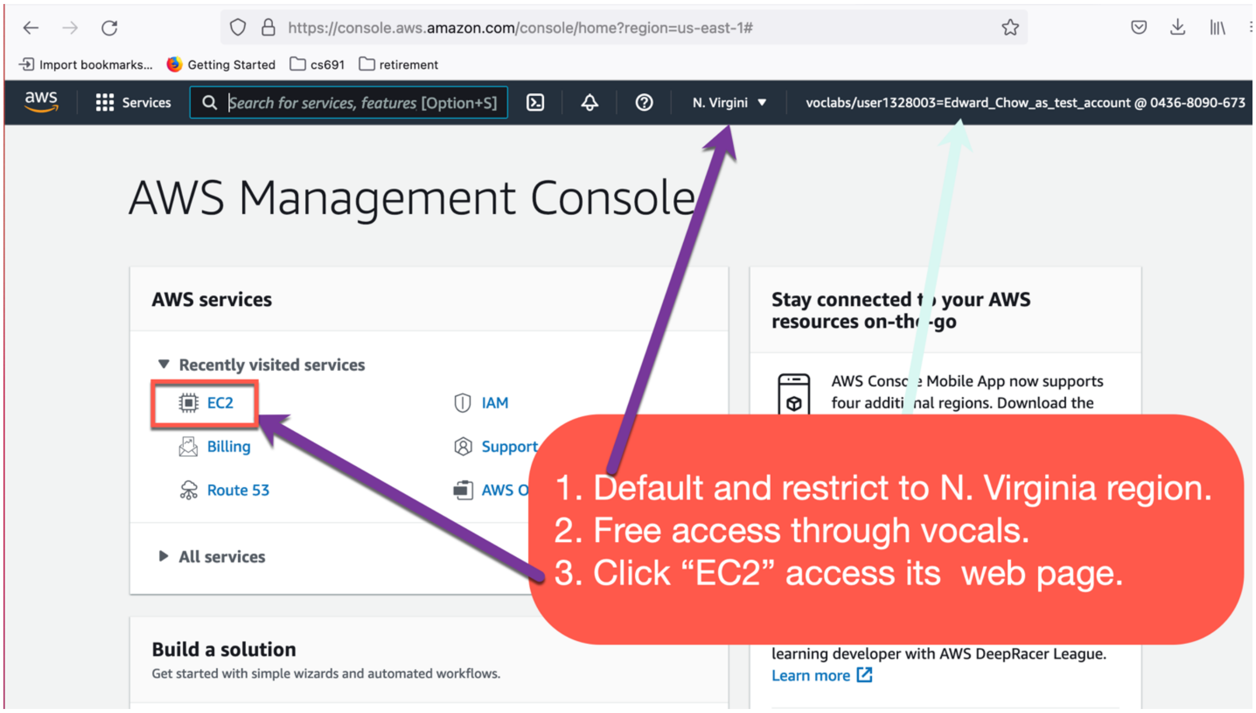
https://console.aws.amazon.com/console/home?region=us-east-1#
Services
Search for services, features [Option+S]
N. Virgini
voclabs/user1328003=Edward_Chow_as_test_account @ 0436-8090-673
AWS Management Console
AWS services
Recently visited services
EC2
IAM
Billing
Support
Route 53
All services
Build a solution
Get started with simple wizards and automated workflows.
Stay connected to your AWS resources on-the-go
Learn more

1.2 Option 2. Create AWS Regular Account with Basic Support.

Follow the link, http://ciast.uccs.edu/coursera/pub/CreateAWSBasicAccount.pdf to register for AWS regular account. This basic account will give privileges to use/learn other AWS cloud services such as Route53 Advanced DNS server for creating your own domain names.

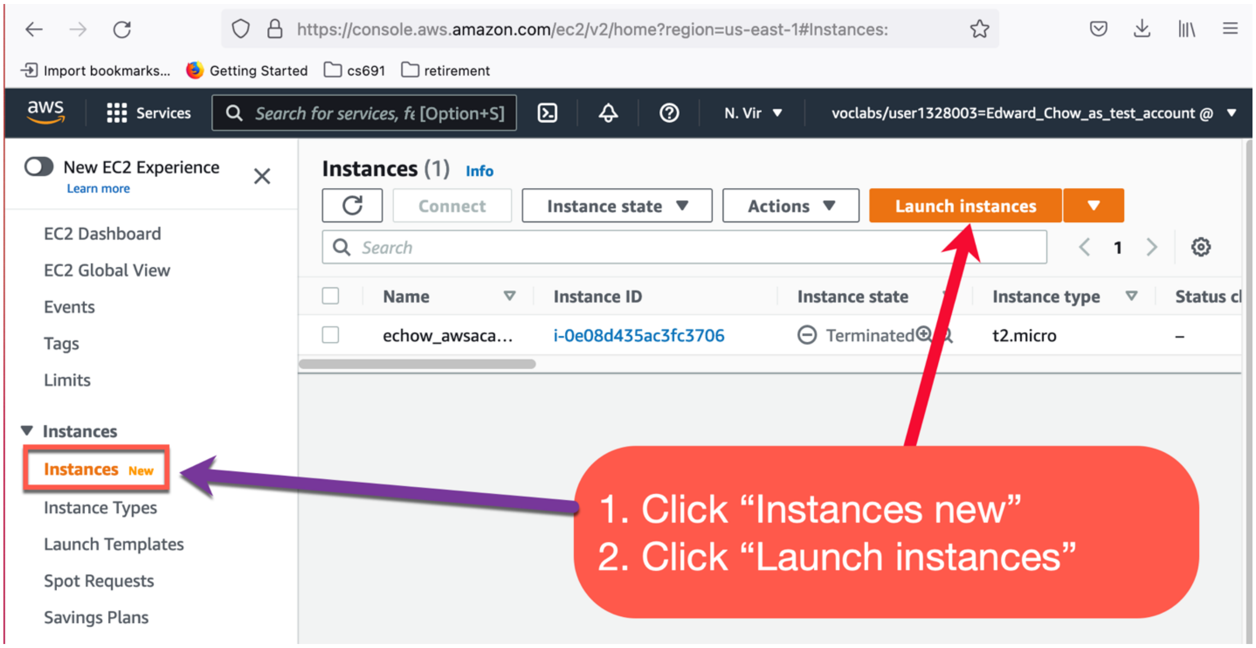
2. Create AMI instance and Install LAMP for CS5910 exercises.

Once setup an AWS account, use the AWS management console
to create an AWS EC2 instance. Click on EC2 service. Note that for those with AWS Academy account, you region will be automatically set to N. Virginia and you will not be able to use services outsides of that region.


https://console.aws.amazon.com/console/home?region=us-east-1#
Import bookmarks...
Getting Started
cs691
retirement
aws
Services
Search for services, features [Option+S]
N. Virgini
voclabs/user1328003=Edward_Chow_as_test_account @ 0436-8090-673
AWS Management Console
AWS services
Recently visited services
EC2
IAM
Billing
Support
Route 53
AWS O
All services
Build a solution
Get started with simple wizards and automated workflows.
Stay connected t your AWS resources on-th -go
AWS Conso e Mobile App now supports four additi nal regions. Download the
learning developer with AWS DeepRacer League.
Learn more

1. Default and restrict to N. Virginia region.
2. Free access through vocals.
3. Click “EC2” access its web page.

Then click Click “Instances new” menuitem on the left panel of EC2 dashboard.
Click “Launch instances”button on the upper right.



Name	Instance ID	Instance state	Instance type	Status cl
echow_awsaca...	i-0e08d435ac3fc3706	Terminated	t2.micro	–

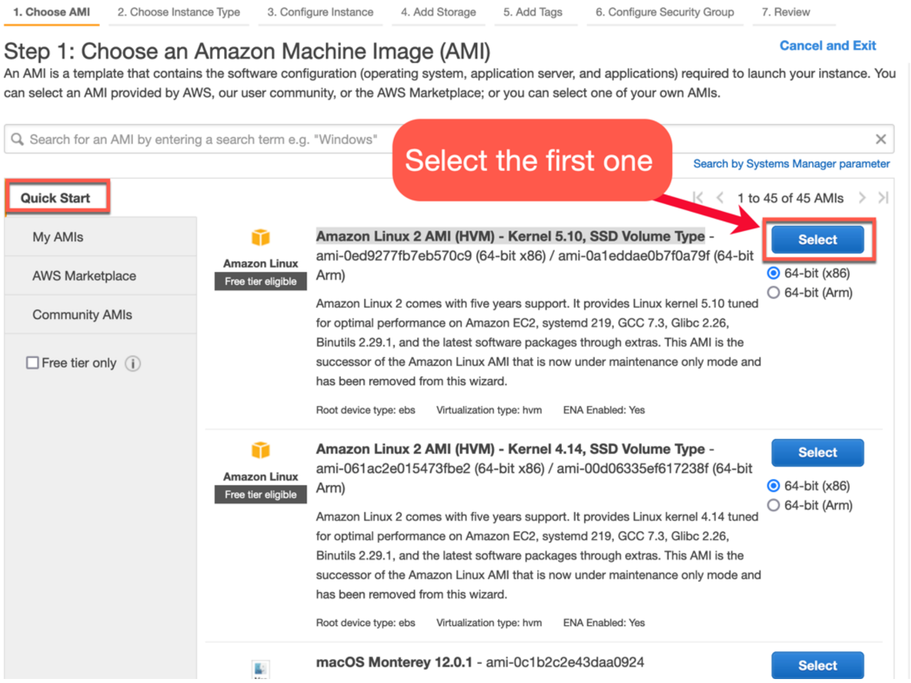
1. Click “Instances new”
2. Click “Launch instances”

We will then be guided through 7-step process to clone an EC2 instance.

2.1. Seven step process to create an Amazon Linux 2 based instance.
2.1.1. Step 1. Choose an Amazon Machine Image (AMI)

2.1.1.1 For those with AWS Academy free access account.
Here with the restriction currently imposed by AWS Academy, we can only choose those AMI image owned by Amazon in Quick Start category. Select the first entry “Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type”.

Warning!! If you choose to use my Coursera-CS5910-ami2 AMI image in Community AMIs to clone the instance, you will find out painfully at the end of Step 7 of this cloning process, your instance launch will fail!



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.

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-0ed9277fb7eb570c9 (64-bit x86) / ami-0a1eddae0b7f0a79f (64-bit Arm)

● 64-bit (x86)
○ 64-bit (Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 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 now under maintenance only mode and has been removed from this wizard.

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

Amazon Linux 2 AMI (HVM) - Kernel 4.14, SSD Volume Type - ami-061ac2e015473fbe2 (64-bit x86) / ami-00d06335ef617238f (64-bit Arm)

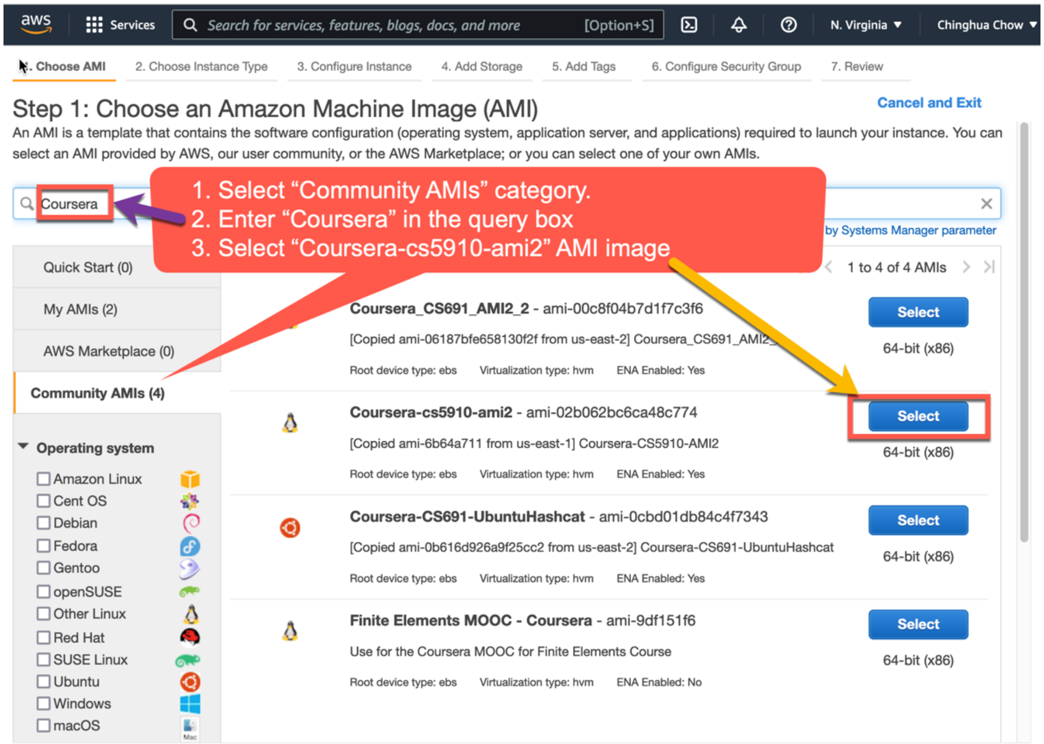
● 64-bit (x86)
○ 64-bit (Arm)

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 now under maintenance only mode and has been removed from this wizard.

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

macOS Monterey 12.0.1 - ami-0c1b2c2e43daa0924

2.1.1.2. For those intend to use their own AWS paid regular account.
Click Community AMIs on the left panel and enter “Coursera” in the query box, then choose Coursera-CS5910-ami2 AMI image that show up. Note that there are other AMI for other Coursera classes.



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.

1. Select “Community AMIs” category.
2. Enter “Coursera” in the query box
3. Select “Coursera-cs5910-ami2” AMI image

Coursera_CS691_AMI2_2 - ami-00c8f04b7d1f7c3f6

[Copied ami-06187bfe658130f2f from us-east-2] Coursera_CS691_AMI2_

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

64-bit (x86)

Coursera-cs5910-ami2 - ami-02b062bc6ca48c774

[Copied ami-6b64a711 from us-east-1] Coursera-CS5910-AMI2

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

64-bit (x86)

Coursera-CS691-UbuntuHashcat - ami-0cbd01db84c4f7343

[Copied ami-0b616d926a9f25cc2 from us-east-2] Coursera-CS691-UbuntuHashcat

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

64-bit (x86)

Finite Elements MOOC - Coursera - ami-9df151f6

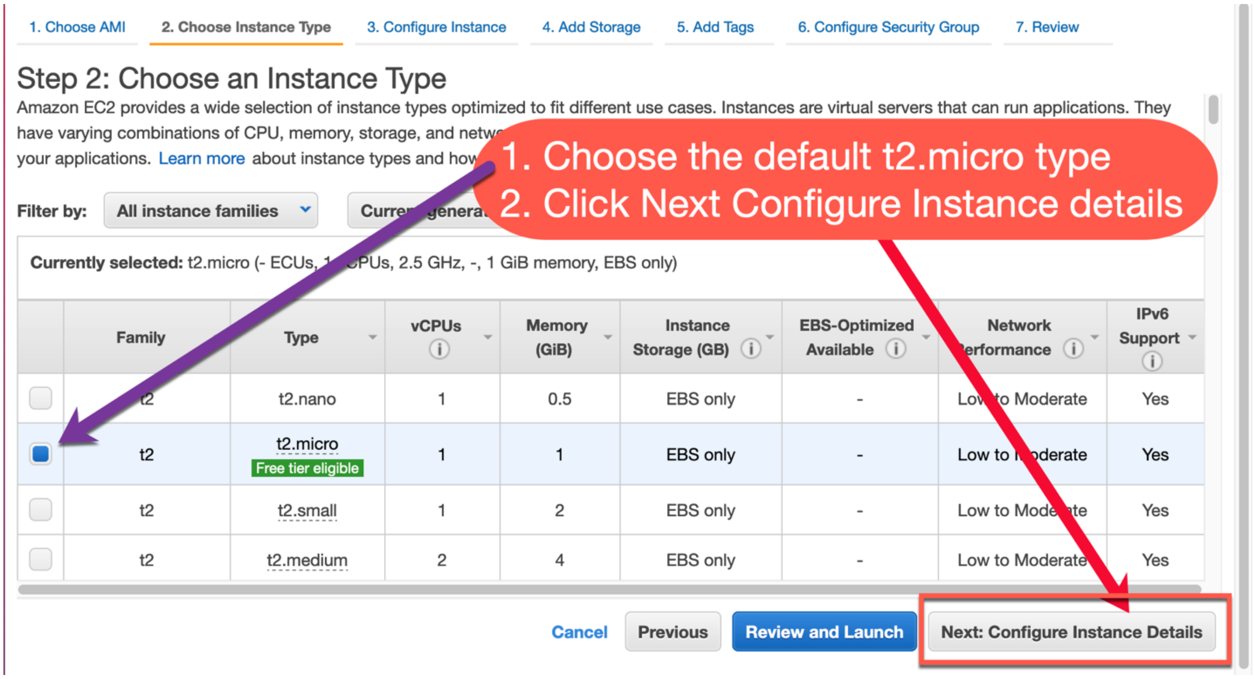
Use for the Coursera MOOC for Finite Elements Course

Root device type: ebs   Virtualization type: hvm   ENA Enabled: No

64-bit (x86)

2.1.2. Step 2. Choose an Instance Type

Choose the default t2.micro type. Then click “Next Configure Instance details”. Donot select “Review and Launch” since we still need to specify the instance name in Step 5 Add tags.



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 netw your applications. Learn more about instance types and how

Filter by: All instance families | Current generation

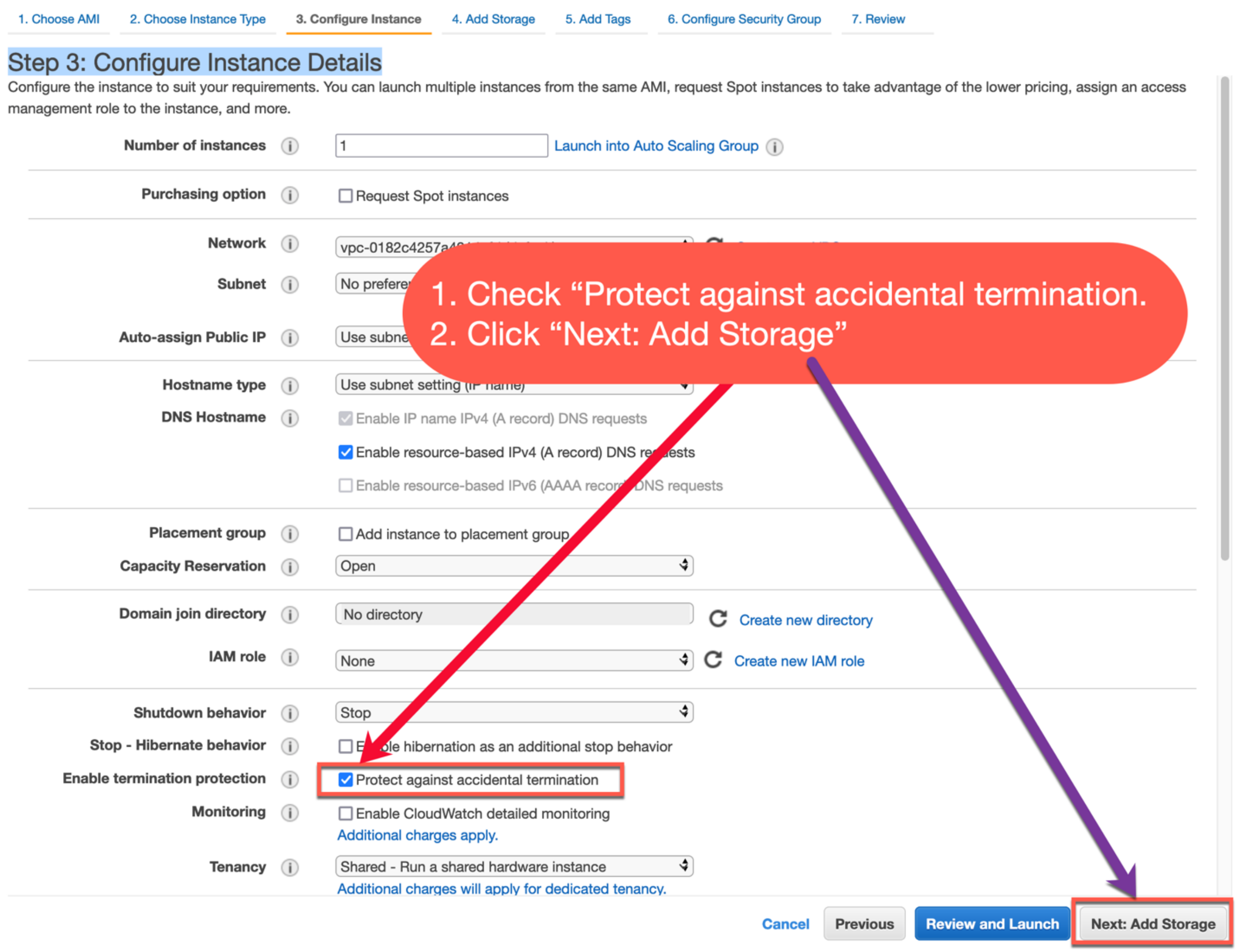
Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	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

1. Choose the default t2.micro type
2. Click Next Configure Instance details

2.1.3. Step 3: Configure Instance Details

Check “Enable termination protection”. Then click “Next: Add Storage”.



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-0182c4257a

Subnet: No prefere

Auto-assign Public IP: Use subne

Hostname type: Use subnet setting

DNS Hostname: ☑ Enable IP name IPv4 (A record) DNS requests
☑ Enable resource-based IPv4 (A record) DNS requests
□ Enable resource-based IPv6 (AAAA record) DNS requests

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

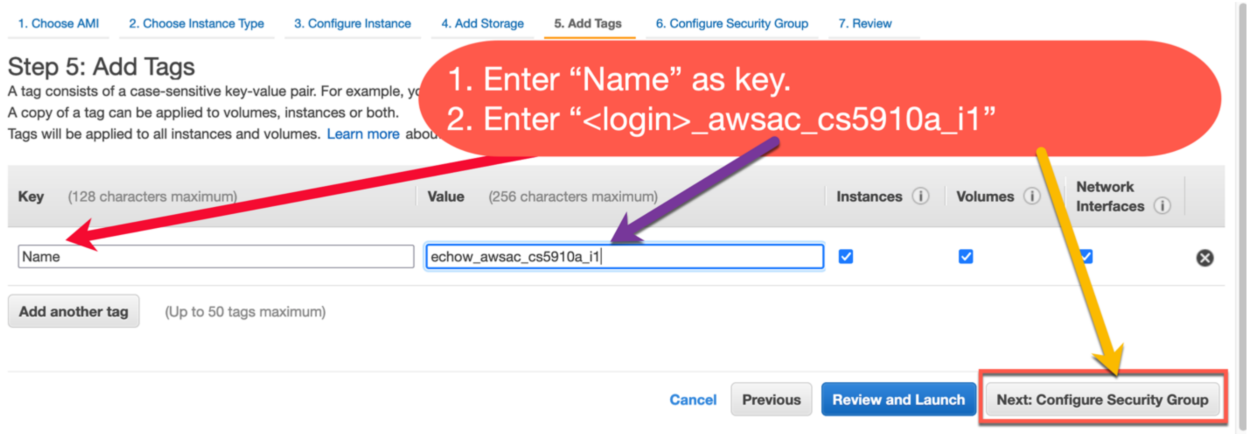
Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

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

1. Check “Protect against accidental termination.
2. Click “Next: Add Storage”

2.1.4. Step 4. Add Storage.
Choose the default 8 GB General purpose SSD (gp2). Click “Next: Add Tags”.

2.1.5. Step 5. Add Tags.
Click “Add Tag” button. Then enter “Name” as Key and “<login>_awsac_cs5910a_i1” as Value. where <login> is your login name in the email address. The string specified in the Name value will be used as the name for the instance showing in the EC2 dashboard for management. Make sure to use the unique name. Here I propose to use your login (so that it is unique for the teacher or group to tell your instance apart), the cs5910a (for the class specific), and i<n> where n could specific instance from the same image. It is useful to use such naming scheme to manage a large group of instances.
Click “Next: Configure Security Group” to reach Step 6.



Step 5: Add Tags

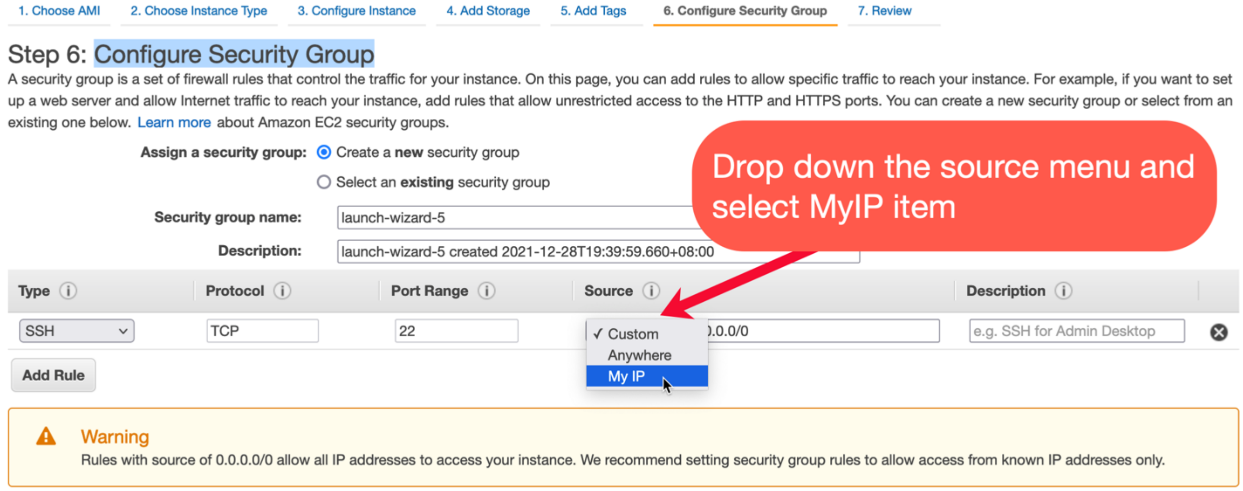
A tag consists of a case-sensitive key-value pair. For example, yo
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more abou

1. Enter "Name" as key.
2. Enter "<login>_awsac_cs5910a_i1"

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces	
Name	echow_awsac_cs5910a_i1	☑	☑	☑	⊗

2.1.6. Step 6. Configure Security Group

Since this is a Linux instance, by default we use SSH connection to manage/configure it. The windows instance will typically use Desktop Connection. As indicate in the warning, rule with 0.0.0.0/0 as source will allow any one including hackers to access the instance. It is dangerous especially when our instance is not yet being patched or properly configured! Let us change the source to MyIP (your current client IP address), so that only you can configure and patch it through the SSH secure connection.



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-5

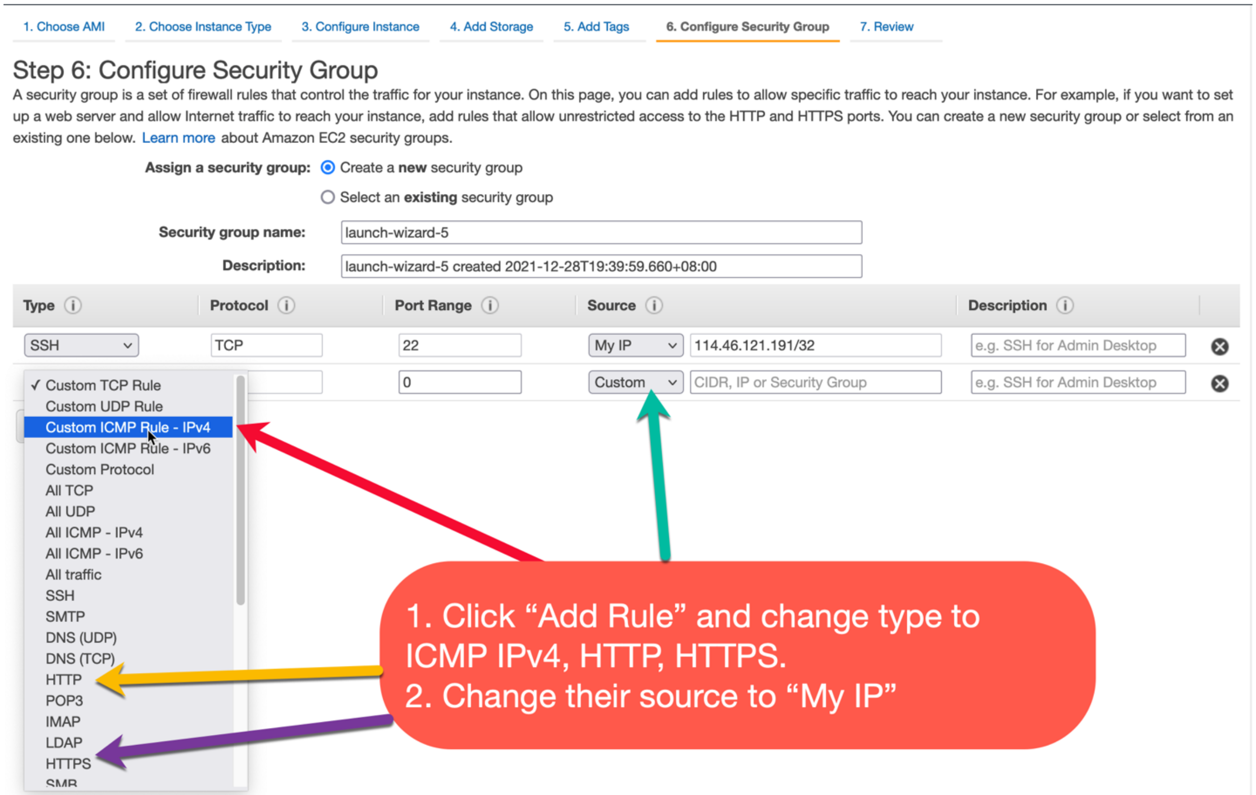
Description: launch-wizard-5 created 2021-12-28T19:39:59.660+08:00

Drop down the source menu and select MyIP item

Type	Protocol	Port Range	Source	Description	
SSH	TCP	22	✓ Custom Anywhere My IP).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.

Once selected, the 0.0.0.0/0 source value will be replaced with your local client IP address. Next, click "Add Rule". Then select one of ICMPv4, HTTP, HTTPS from the "Custom TCP" drop down menu, as incoming traffic type to the firewall, or AWS security group. Make sure you change the source of those rules to "MyIP" setting also.



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

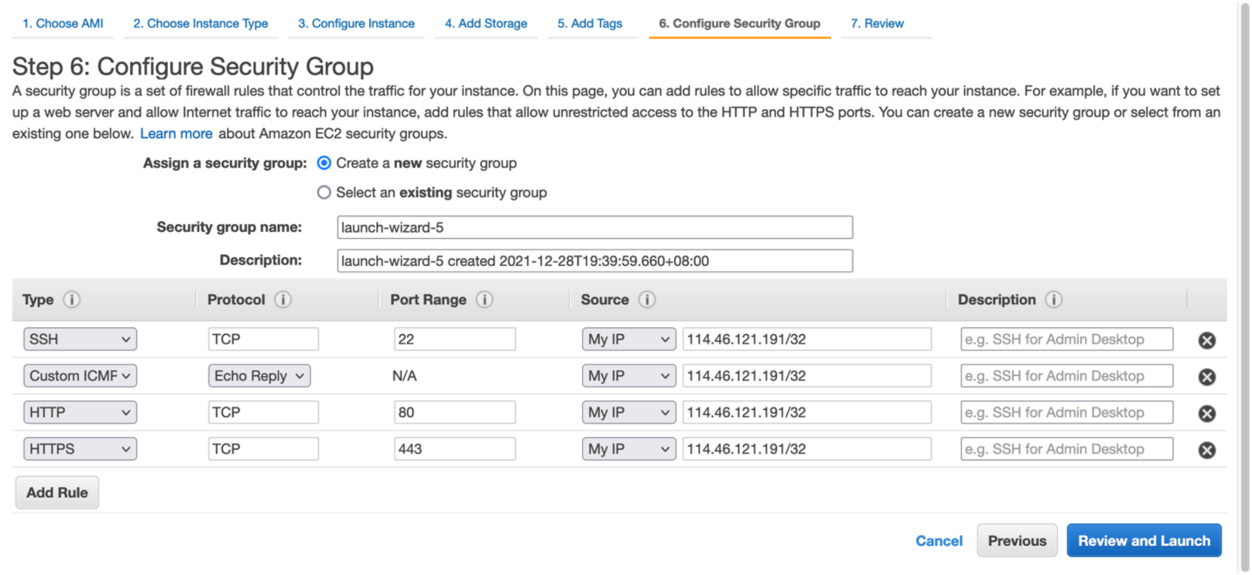
Security group name: launch-wizard-5

Description: launch-wizard-5 created 2021-12-28T19:39:59.660+08:00

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	My IP	114.46.121.191/32	e.g. SSH for Admin Desktop
		0	Custom	CIDR, IP or Security Group	e.g. SSH for Admin Desktop

1. Click "Add Rule" and change type to ICMP IPv4, HTTP, HTTPS.
2. Change their source to "My IP"

The security group specification should look like the diagram below. Click "Review and Launch"



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

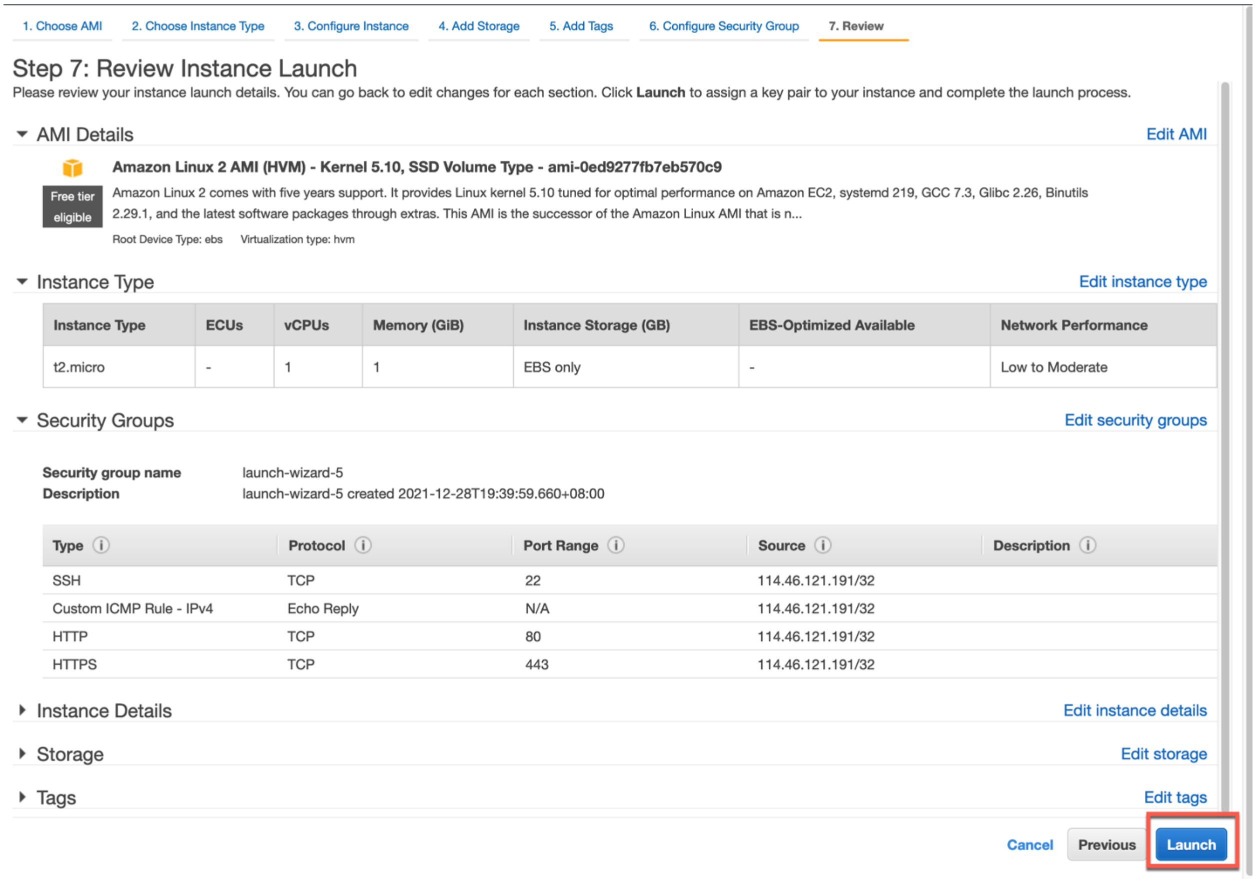
Security group name: launch-wizard-5

Description: launch-wizard-5 created 2021-12-28T19:39:59.660+08:00

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	My IP	114.46.121.191/32	e.g. SSH for Admin Desktop
Custom ICMF	Echo Reply	N/A	My IP	114.46.121.191/32	e.g. SSH for Admin Desktop
HTTP	TCP	80	My IP	114.46.121.191/32	e.g. SSH for Admin Desktop
HTTPS	TCP	443	My IP	114.46.121.191/32	e.g. SSH for Admin Desktop

2.1.7. Step 7: Review Instance Launch

Click “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.

AMI Details

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-0ed9277fb7eb570c9

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 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 n...

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-5
Description	launch-wizard-5 created 2021-12-28T19:39:59.660+08:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	114.46.121.191/32	
Custom ICMP Rule - IPv4	Echo Reply	N/A	114.46.121.191/32	
HTTP	TCP	80	114.46.121.191/32	
HTTPS	TCP	443	114.46.121.191/32	

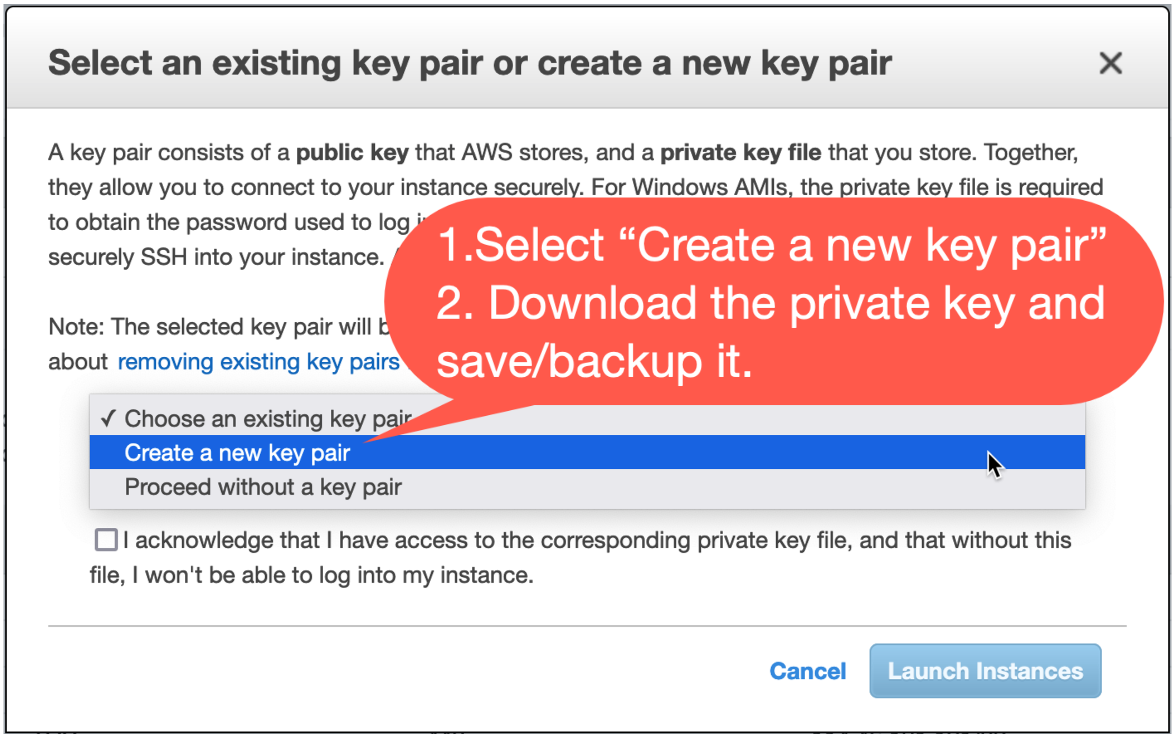
Instance Details

Storage

Tags

You will then be prompted to use an exist key pair or generate a new key pair for access the instance. Here we will ask AWS to generate a new key pair for us and allow us to download the private key part of the key pair. Once you have the private key, you can select “existing key par” later to reuse the same key pair. AWS keeps a copy of your public key in its ec2 management system and also append it to the .ssh/authorized_keys file of the instance for verification purpose. When we use a SSH client to connect to the sshd server of the instance, the SSH client will send a token encrypted with the private key to the sshd server, the sshd server will then use the related pubic key in .ssh/authorized_keys to decrypt the token and decide whether to allow secure access or not.

For those interested in exploring further, you can check the content of .ssh/authorized_keys file in the instance for the saved public key.



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 i

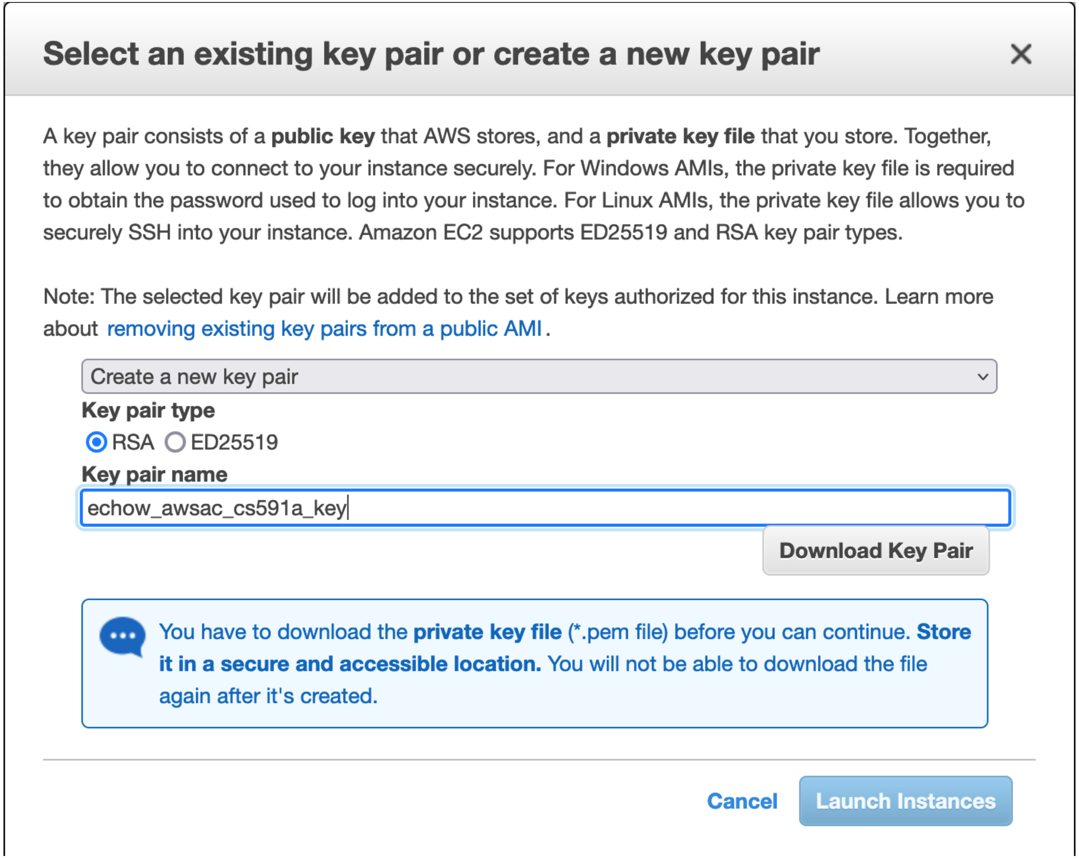
securely SSH into your instance.

Note: The selected key pair will b

about removing existing key pairs

1.Select "Create a new key pair"
2. Download the private key and save/backup it.

□ I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my 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.

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 type

● RSA ○ ED25519

Key pair name

echow_awsac_cs591a_key

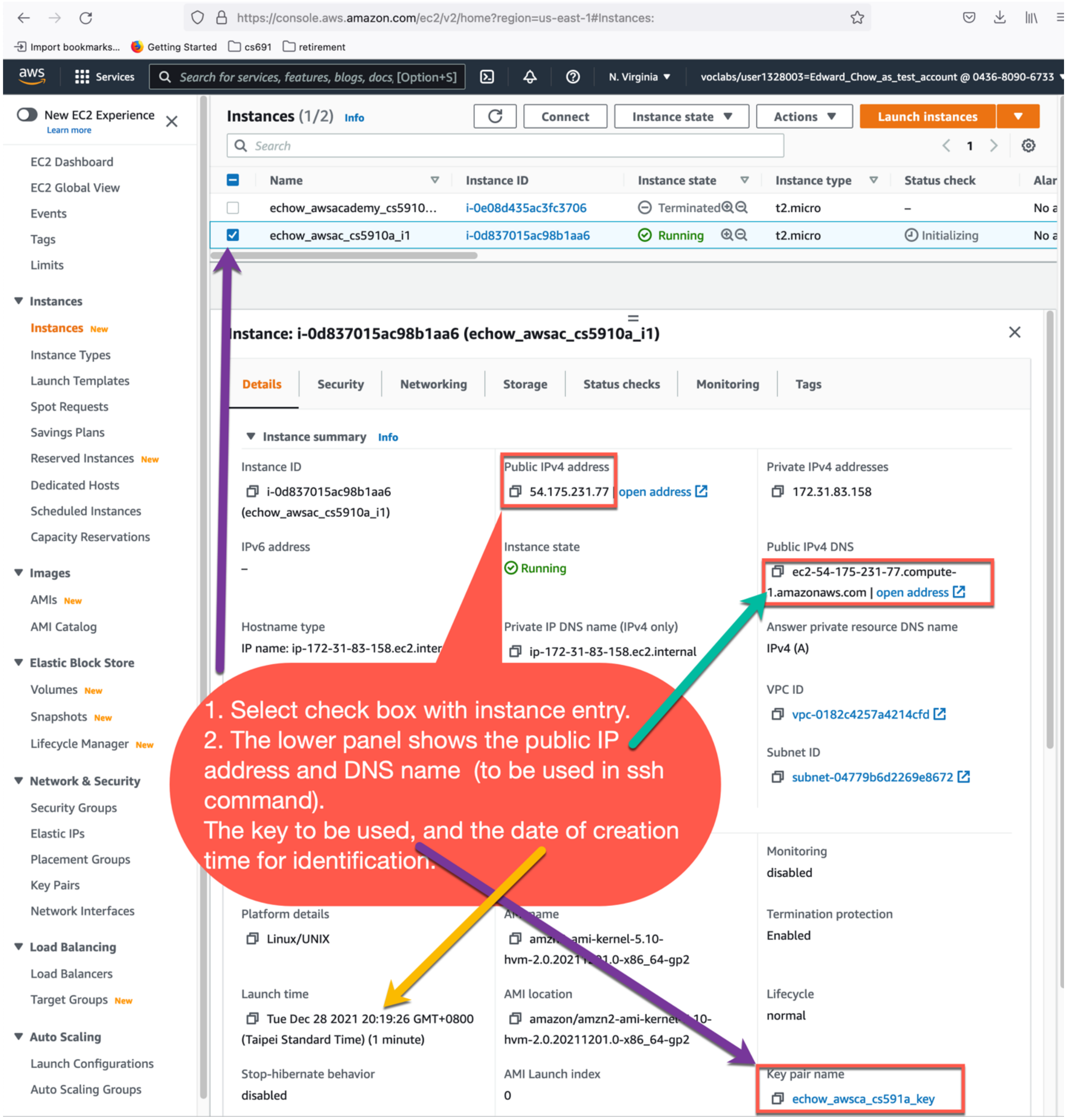
You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Here for the Key pair name entry, I would suggest entering <login>_awsac_cs591a_key as the key name. Here I replace <login> with my login echow. Therefore my key pair name is echow_awsac_cs591a_key.

Click “Download Key Pair”. Here the button label is misleading. We only download the private key not the key pair. You will remind to save the file. Make sure you move it from the download area and save it in a secure directory or even back it up to a flash drive. Once you lost the private key, you lost access to the instance. Note that the actual file name for the private key will have .pem as file extension. Therefore in my directory I see an echow_awsac_cs591a_key.pem file.

Then click the Launch Instances. Click again in the “View Instances” in the Launch Status page.

From the instance list, you can check the box in front of the instance entry of your interest. We can identify here “echow_awsac_cs591a_key” is the Name key value we entered in Step 5 of the instance creation process.



	Name	Instance ID	Instance state	Instance type	Status check	Alar
□	echow_awsacademy_cs5910...	i-0e08d435ac3fc3706	Terminated	t2.micro	–	No a
☑	echow_awsac_cs5910a_i1	i-0d837015ac98b1aa6	Running	t2.micro	Initializing	No a

Instance: i-0d837015ac98b1aa6 (echow_awsac_cs5910a_i1)

Instance ID
i-0d837015ac98b1aa6 (echow_awsac_cs5910a_i1)

Public IPv4 address
54.175.231.77 | open address

Private IPv4 addresses
172.31.83.158

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-54-175-231-77.compute-1.amazonaws.com | open address

Hostname type
IP name: ip-172-31-83-158.ec2.inter

Private IP DNS name (IPv4 only)
ip-172-31-83-158.ec2.internal

Answer private resource DNS name
IPv4 (A)

VPC ID
vpc-0182c4257a4214cfd

Subnet ID
subnet-04779b6d2269e8672

Monitoring
disabled

Platform details
Linux/UNIX

AMI name
amzn2-ami-kernel-5.10-hvm-2.0.20211201.0-x86_64-gp2

Termination protection
Enabled

Launch time
Tue Dec 28 2021 20:19:26 GMT+0800 (Taipei Standard Time) (1 minute)

AMI location
amazon/amzn2-ami-kernel-5.10-hvm-2.0.20211201.0-x86_64-gp2

Lifecycle
normal

Stop-hibernate behavior
disabled

AMI Launch index
0

Key pair name
echow_awsca_cs591a_key

1. Select check box with instance entry.
2. The lower panel shows the public IP address and DNS name (to be used in ssh command).
The key to be used, and the date of creation time for identification.

Make sure you back up your private key in a safe place such as a flash drive. You may want to encrypt it.

Once the instance is initialized and running, click it on the dashboard or hit the Instances of the EC2 main window. Find the public IP address assigned to this instance. We will reference this as <InstancePublicIPAddress> to be used in setting up the access.

2.2. Associate Elastic IP Address with the Instance

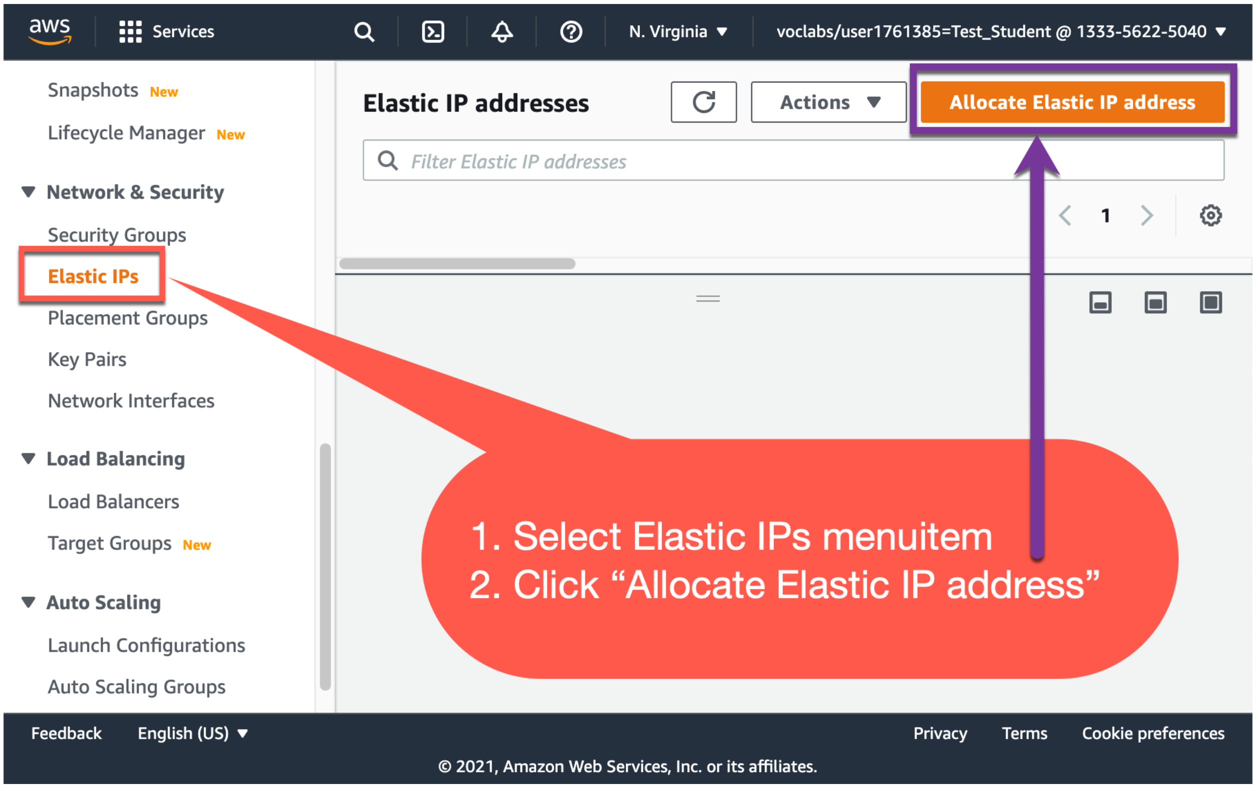
To save IP address space, AWS will reclaim the public IP address of the instance once it is “stopped” or “suspended”. Next time when we restart or resume the instance, AWS will assign a new public IP address for the instance. This often confuses the new users since they forget to check the new public IP public IP address in the detailed info panel for the instance. They thought the instance is not reachable for some other reasons.

To avoid such an inconvenience, AWS provides “Elastic IP Address” to be associated with the instance so that when the instance is resumed, it will have the same Elastic IP Address for accessing the instance. Note that when you are not using an instance with Elastic IP address (not intuitive), you will incur some charge, but normally it is much less than the suspension of the instance for a long period of time.

Follow the steps below to request an Elastic IP address and associate with the instance we just cloned:

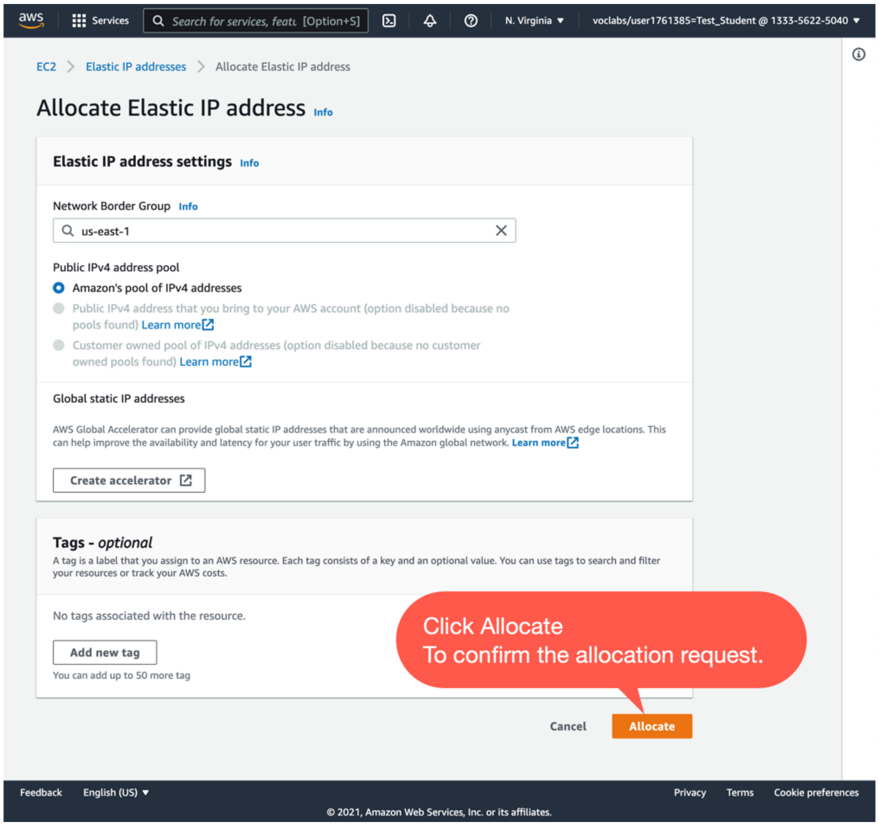
2.2.1. Request An Elastic IP address.

Select Elastic IPs menu-item on the left panel of AWS EC2 dashboard. Click “Allocate Elastic IP address.



1. Select Elastic IPs menuitem
2. Click “Allocate Elastic IP address”

2.2.2. Confirm its allocation by clicking on the Allocate button on the lower right.


aws
Services
Search for services, featu [Option+S]
N. Virginia ▼
voclabs/user1761385=Test_Student @ 1333-5622-5040 ▼
EC2 > Elastic IP addresses > Allocate Elastic IP address
Info
Create accelerator
Add new tag
Cancel
Allocate
Feedback
English (US) ▼
Privacy
Terms
Cookie preferences
© 2021, Amazon Web Services, Inc. or its affiliates.

Allocate Elastic IP address

Elastic IP address settings

Network Border Group: us-east-1

Public IPv4 address pool

● Amazon's pool of IPv4 addresses

○ Public IPv4 address that you bring to your AWS account (option disabled because no pools found) Learn more

○ Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) Learn more

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

Tags - *optional*

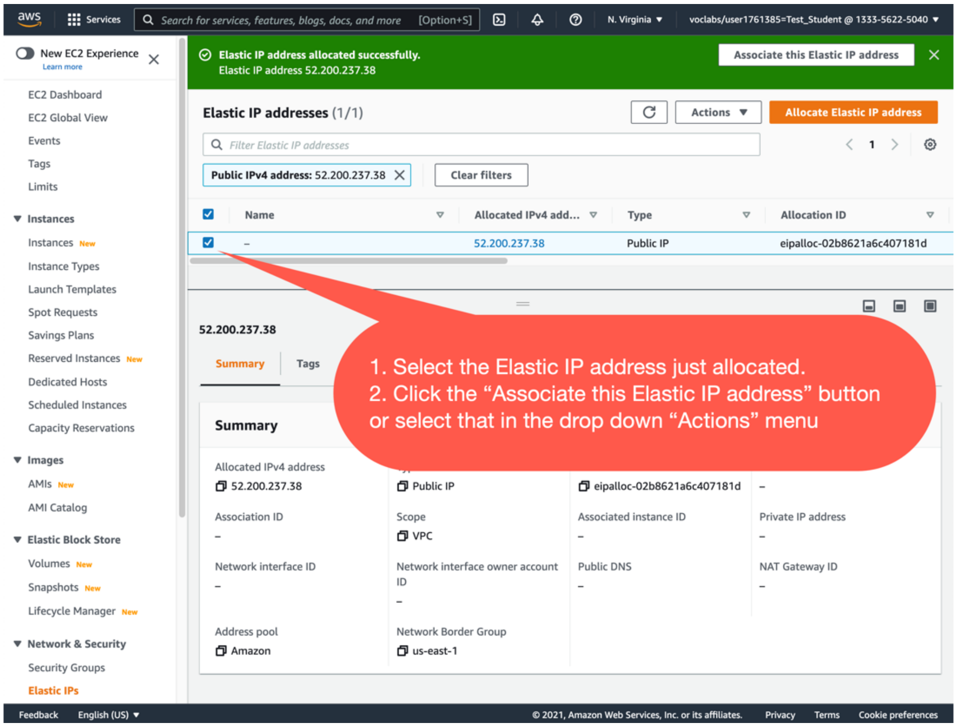
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add up to 50 more tag

Click Allocate
To confirm the allocation request.

2.2.3. Select the Elastic IP address just allocated. Click the "Associate this Elastic IP address" button or select that in the drop down "Actions" menu



Elastic IP address allocated successfully.
Elastic IP address 52.200.237.38

Elastic IP addresses (1/1)

Public IPv4 address: 52.200.237.38

☑	Name	Allocated IPv4 add...	Type	Allocation ID
☑	–	52.200.237.38	Public IP	eipalloc-02b8621a6c407181d

52.200.237.38

Summary

Allocated IPv4 address: 52.200.237.38

Public IP

eipalloc-02b8621a6c407181d

–

Association ID: –

Scope: VPC

Associated instance ID: –

Private IP address: –

Network interface ID: –

Network interface owner account ID: –

Public DNS: –

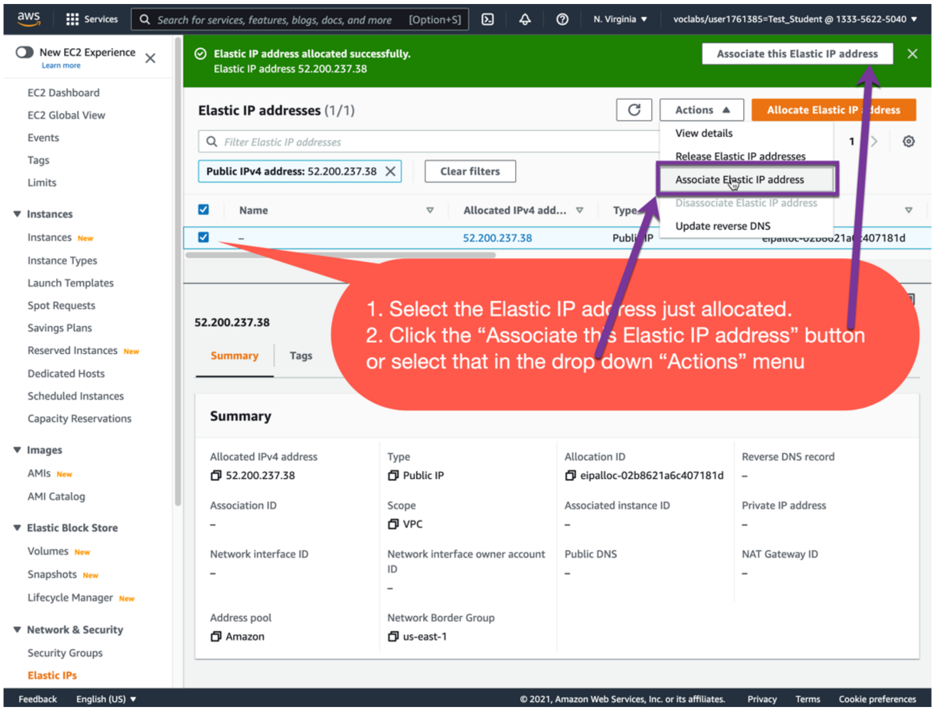
NAT Gateway ID: –

Address pool: Amazon

Network Border Group: us-east-1

1. Select the Elastic IP address just allocated.
2. Click the "Associate this Elastic IP address" button or select that in the drop down "Actions" menu

2.2.4. Select the Elastic IP address just allocated. Click the “Associate this Elastic IP address” button or select that in the drop down “Actions” menu



Elastic IP address allocated successfully.
Elastic IP address 52.200.237.38

Elastic IP addresses (1/1)

Public IPv4 address: 52.200.237.38

☑	Name	Allocated IPv4 add...	Type	
☑	–	52.200.237.38	Public IP	eipalloc-02b8621a6c407181d

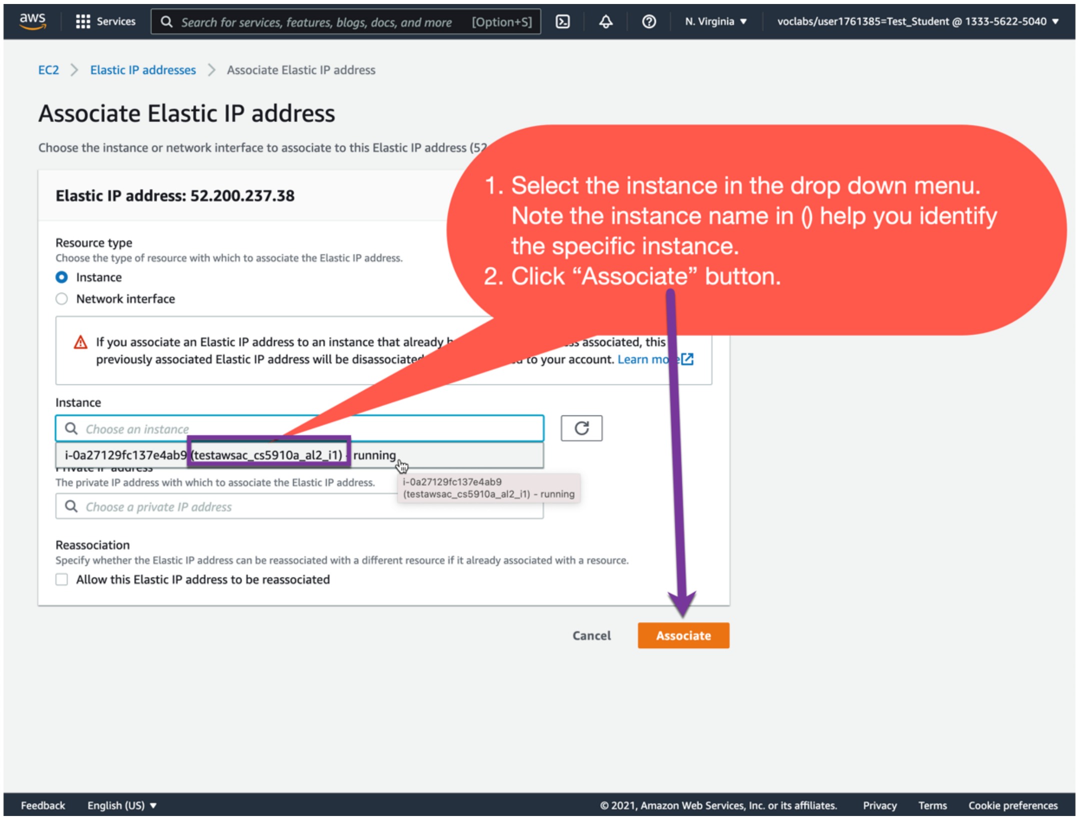
52.200.237.38

Summary

Allocated IPv4 address 52.200.237.38	Type Public IP	Allocation ID eipalloc-02b8621a6c407181d	Reverse DNS record –
Association ID –	Scope VPC	Associated instance ID –	Private IP address –
Network interface ID –	Network interface owner account ID –	Public DNS –	NAT Gateway ID –
Address pool Amazon	Network Border Group us-east-1		

1. Select the Elastic IP address just allocated.
2. Click the “Associate this Elastic IP address” button or select that in the drop down “Actions” menu

2.2.5.


aws
Services
Search for services, features, blogs, docs, and more [Option+S]
N. Virginia
voclabs/user1761385=Test_Student @ 1333-5622-5040
EC2 > Elastic IP addresses > Associate Elastic IP address
Cancel
Associate
Feedback
English (US)
© 2021, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (52

Elastic IP address: 52.200.237.38

Resource type
Choose the type of resource with which to associate the Elastic IP address.
● Instance
○ Network interface

If you associate an Elastic IP address to an instance that already h... ...ss associated, this previously associated Elastic IP address will be disassociated ... to your account. Learn more

Instance
Choose an instance
i-0a27129fc137e4ab9 (testawsac_cs5910a_al2_i1) - running

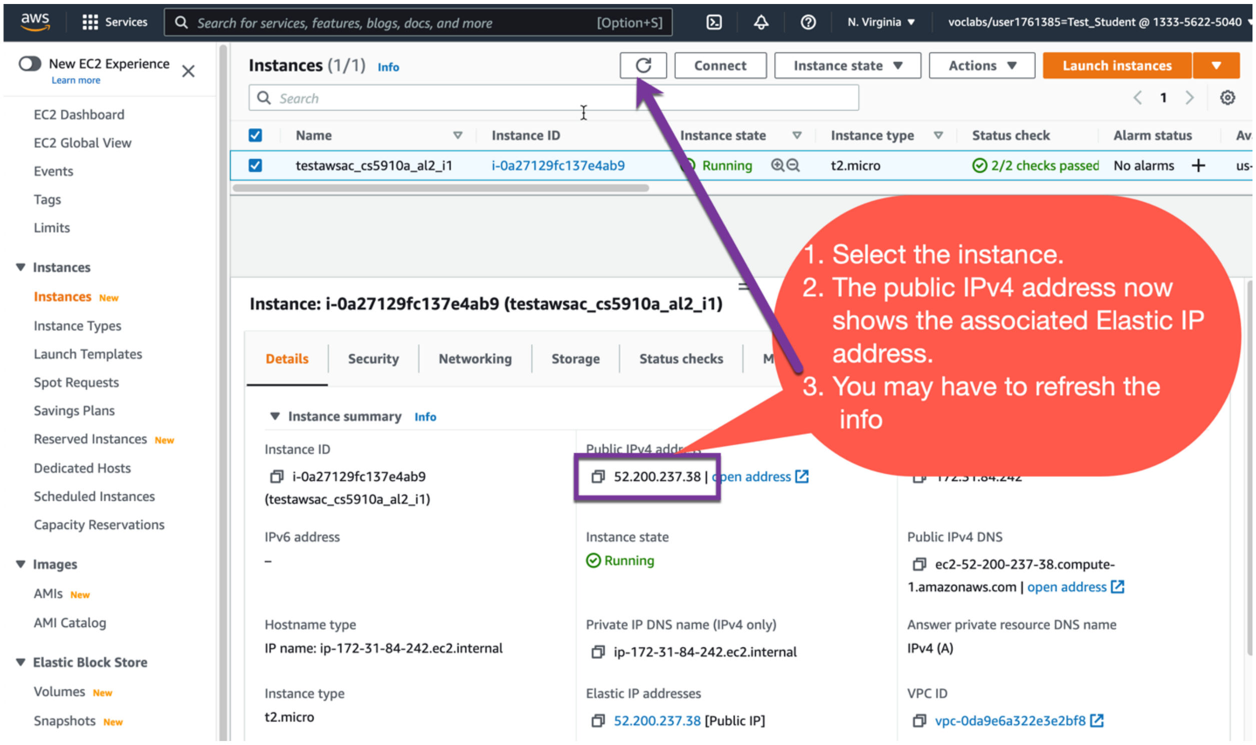
Private IP address
The private IP address with which to associate the Elastic IP address.
Choose a private IP address

i-0a27129fc137e4ab9
(testawsac_cs5910a_al2_i1) - running

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
□ Allow this Elastic IP address to be reassociated

1. Select the instance in the drop down menu. Note the instance name in () help you identify the specific instance.
2. Click “Associate” button.

2.2.6 Select the instance. The public IPv4 address now shows the associated Elastic IP address. You may have to refresh the info



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Av
☑	testawsac_cs5910a_al2_i1	i-0a27129fc137e4ab9	Running	t2.micro	2/2 checks passed	No alarms	us-

1. Select the instance.
2. The public IPv4 address now shows the associated Elastic IP address.
3. You may have to refresh the info

Instance: i-0a27129fc137e4ab9 (testawsac_cs5910a_al2_i1)

Instance summary Info

Instance ID
i-0a27129fc137e4ab9 (testawsac_cs5910a_al2_i1)

Public IPv4 addr
52.200.237.38 | open address

172.31.84.242

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-52-200-237-38.compute-1.amazonaws.com | open address

Hostname type
IP name: ip-172-31-84-242.ec2.internal

Private IP DNS name (IPv4 only)
ip-172-31-84-242.ec2.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t2.micro

Elastic IP addresses
52.200.237.38 [Public IP]

VPC ID
vpc-0da9e6a322e3e2bf8

3. Access your AMI instance.

3.1 For mac or Linux users,

You can use ssh command in the directory containing your instance's private key.

```
ssh –i <privateKey>.pem ec2-user@<InstancePublicIPAddress>
```

```
Here <privateKey>.pem is the keypair name in the last prompt window of the instance
creation process;
<InstancePublicIPAddress> is the instance public IP address showing in the previous
diagram of the instance's info window;
–i indicates to the ssh client command we are using the specific private key file for
accessing the server.
```

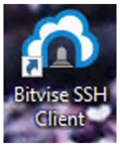
Here the parameter right after -i option is the private key file name. Make sure the file access mode need to be change to 600 or rw only by the owner, i.e., can only be accessed by you. You can use "chmod go-rw `<login>_awsac_cs5910a_key.pem`" to remove group and other user access to your private key file. Without such change, the ssh will refuse to make connection. SSH client follows the new standard for security practice implementation.

Note that this SSH client command try to access the home directory of a user called "ec2-user" on a server or instance running SSH server daemon. In the AWS Amazon Linux 2 image, there is only one user ec2-user created as the first user. As a first user, ec2-user can use "sudo" precedes any privileged command to run typical system configuration operations like a root user.

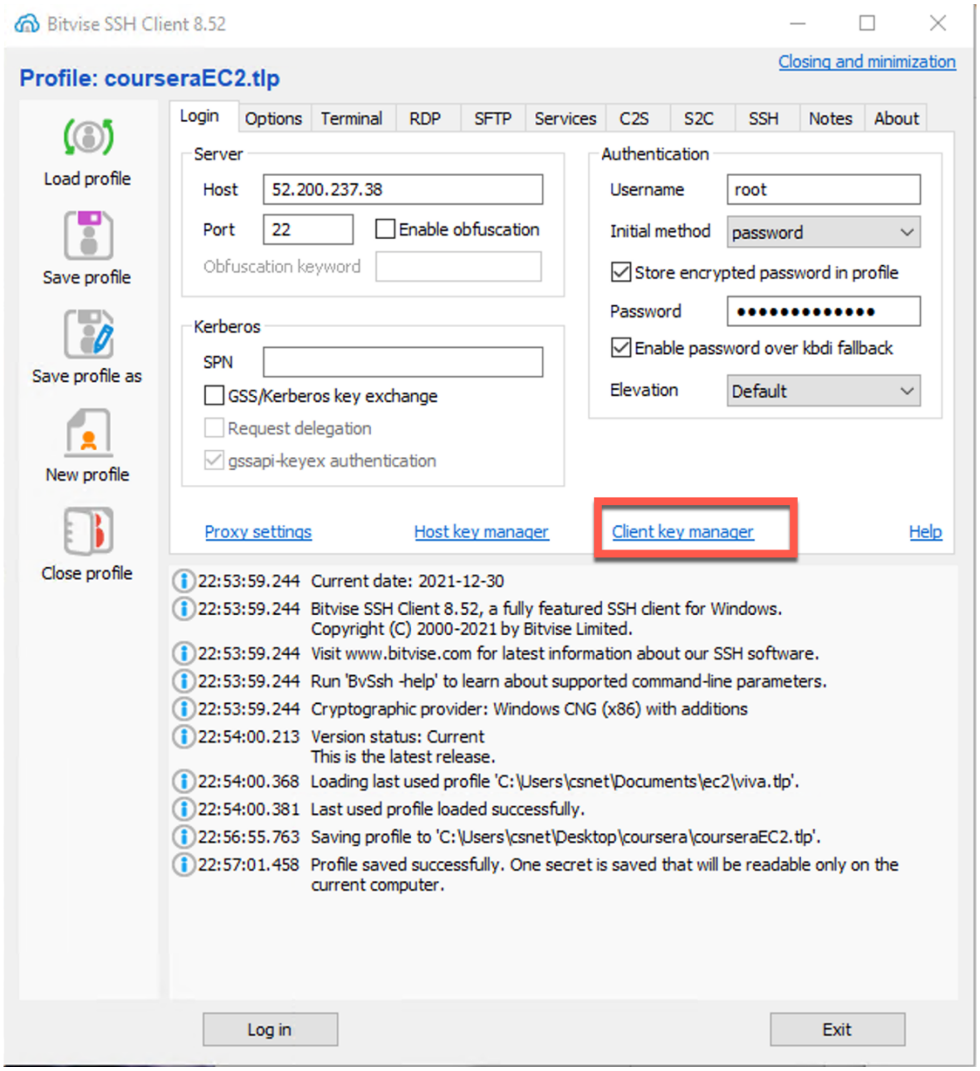
3.2 For Windows users,

you can download the bitvise SSH Client app installer and install bitvise app. It is available at https://www.bitvise.com/ssh-client-download. It provides a nice SFTP gui for drag and drop files between remote server and your local client. It also does not require to go through the .pem to .ppk file conversion which is required by putty app. The putty is also a popular command line interface app and can be downloaded at https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html (choose the proper msi file). I recommend using bitvise for accessing our instance. It also saves your configuration time.

3.2.1 Install bitvise SSH Client

After download and install the bitvise app, you should see the following app installed on the upper left corn or the desktop. 

Step 1. First import the private key into the bitvise app using its Client key manager.



Profile: courseraEC2.tlp

Host: 52.200.237.38

Port: 22 □ Enable obfuscation

Obfuscation keyword:

SPN:

□ GSS/Kerberos key exchange

□ Request delegation

☑ gssapi-keyex authentication

Username: root

Initial method: password

☑ Store encrypted password in profile

Password: ••••••••••••••

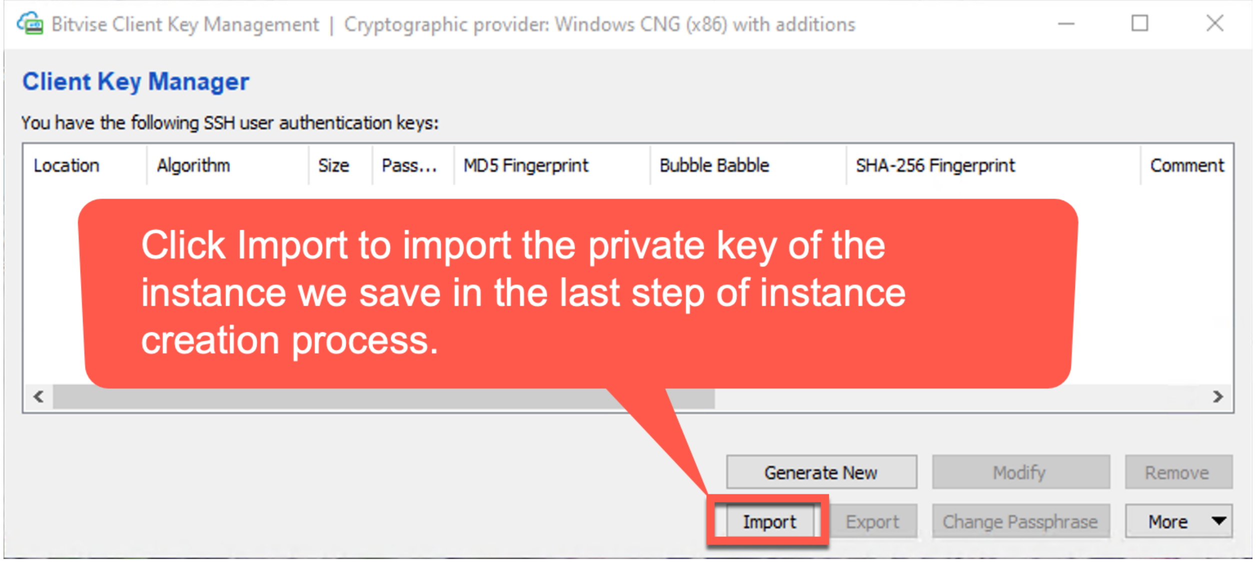
☑ Enable password over kbdi fallback

Elevation: Default

```
22:53:59.244  Current date: 2021-12-30
22:53:59.244  Bitvise SSH Client 8.52, a fully featured SSH client for Windows.
              Copyright (C) 2000-2021 by Bitvise Limited.
22:53:59.244  Visit www.bitvise.com for latest information about our SSH software.
22:53:59.244  Run 'BvSsh -help' to learn about supported command-line parameters.
22:53:59.244  Cryptographic provider: Windows CNG (x86) with additions
22:54:00.213  Version status: Current
              This is the latest release.
22:54:00.368  Loading last used profile 'C:\Users\csnet\Documents\ec2\viva.tlp'.
22:54:00.381  Last used profile loaded successfully.
22:56:55.763  Saving profile to 'C:\Users\csnet\Desktop\coursera\courseraEC2.tlp'.
22:57:01.458  Profile saved successfully. One secret is saved that will be readable only on the
              current computer.
```

Figure 1. First import the private key into the bitvise app using its Client key manager.

Step 2. Click Import button.



Bitvise Client Key Management | Cryptographic provider: Windows CNG (x86) with additions
Generate New
Modify
Remove
Import
Export
Change Passphrase
More

Client Key Manager

You have the following SSH user authentication keys:

Location	Algorithm	Size	Pass...	MD5 Fingerprint	Bubble Babble	SHA-256 Fingerprint	Comment

Click Import to import the private key of the instance we save in the last step of instance creation process.

Figure 2. Click Import button to import the private key.

Step 3. Change the file type to all file (*.*) in order to reveal our private key in .pem file format. Note that the Bitvise Kepair Files (*.bkp) type will not show the .pem file type which is used to generate the private key during the last step of instance creation process.

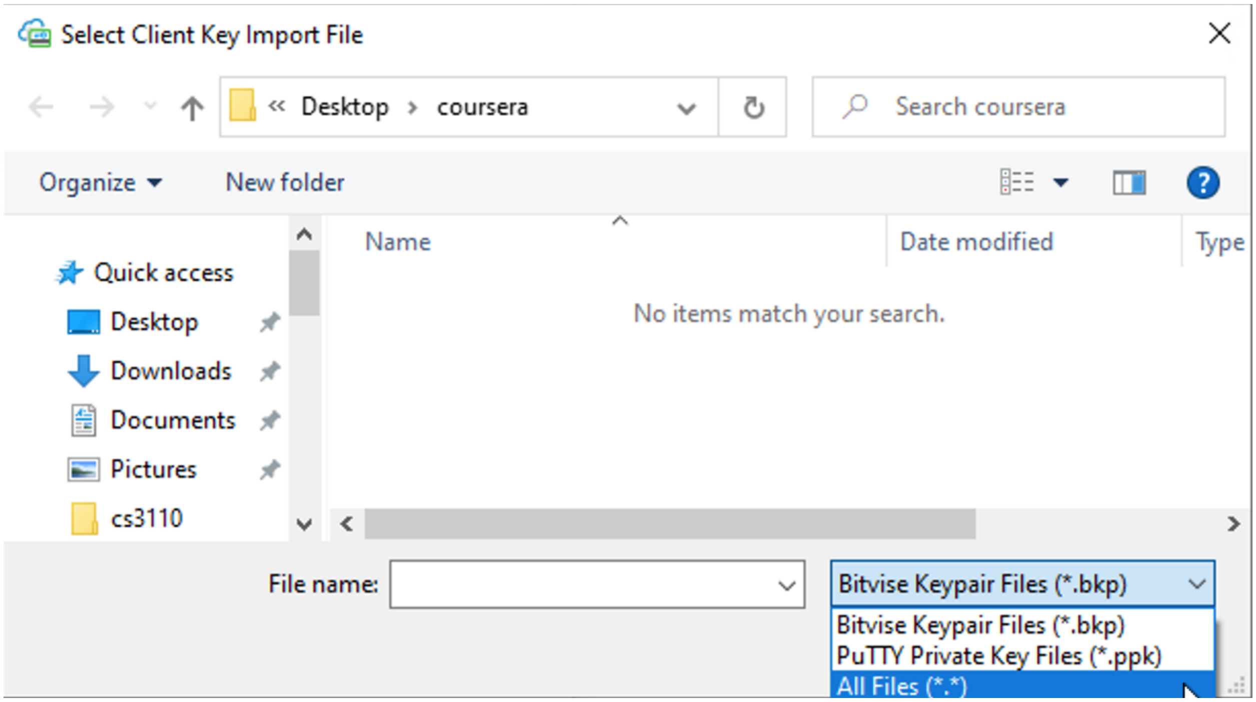
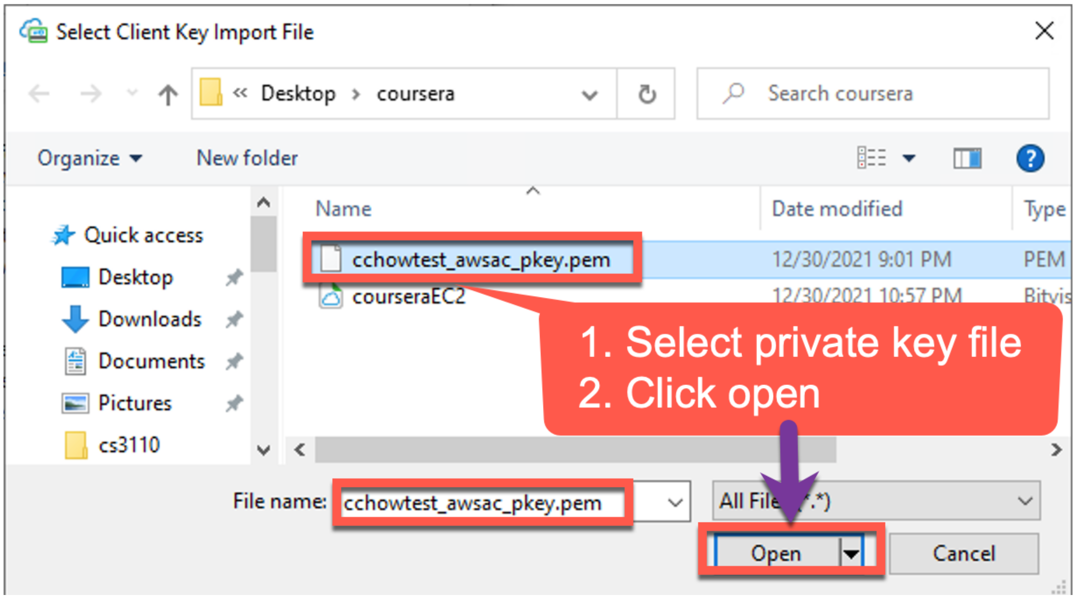


Figure 3. Change file type to All Files (*.*) to reveal our private key in .pem file format.

Step 4. Select our private key and Click Open.



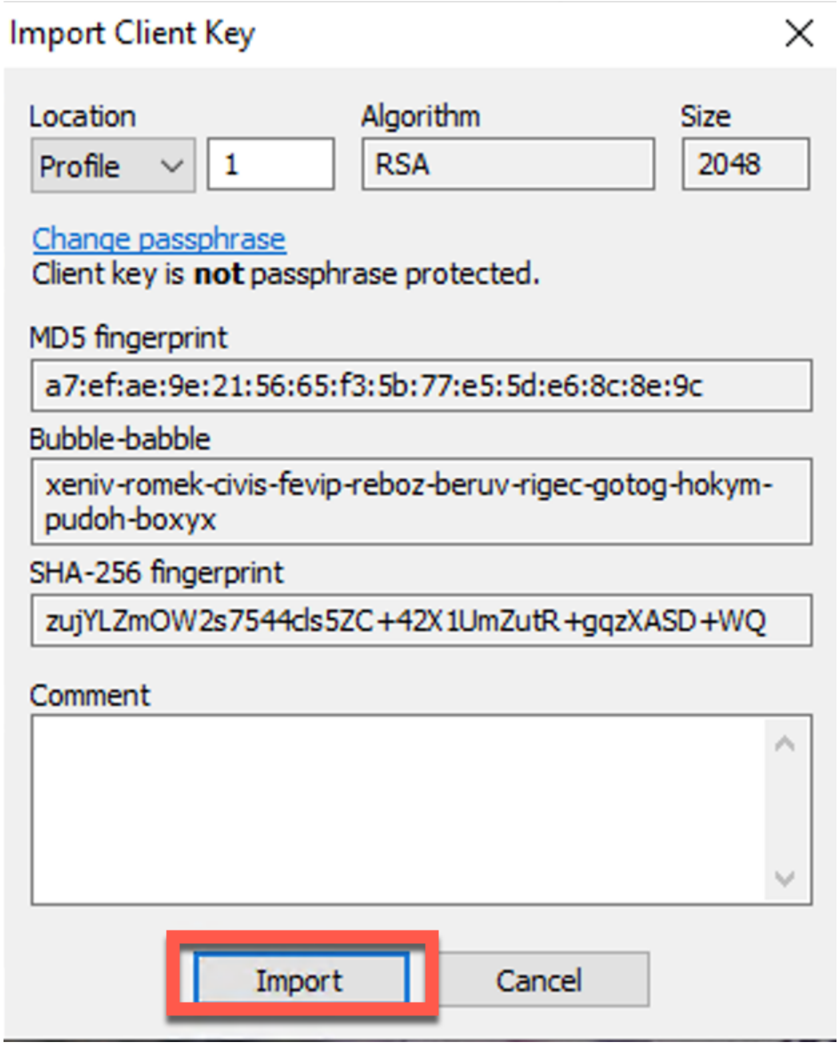
File name: cchowtest_awsac_pkey.pem

1. Select private key file
2. Click open

Figure 4. Select private key in .pem file and click Open.

Note that in Figure 4, we use cchowtest_awsac_pkey.pem as an example.

Step 5. Import the private key and save as Profile Location key #1



Import Client Key

Location: Profile 1

Algorithm: RSA

Size: 2048

Client key is **not** passphrase protected.

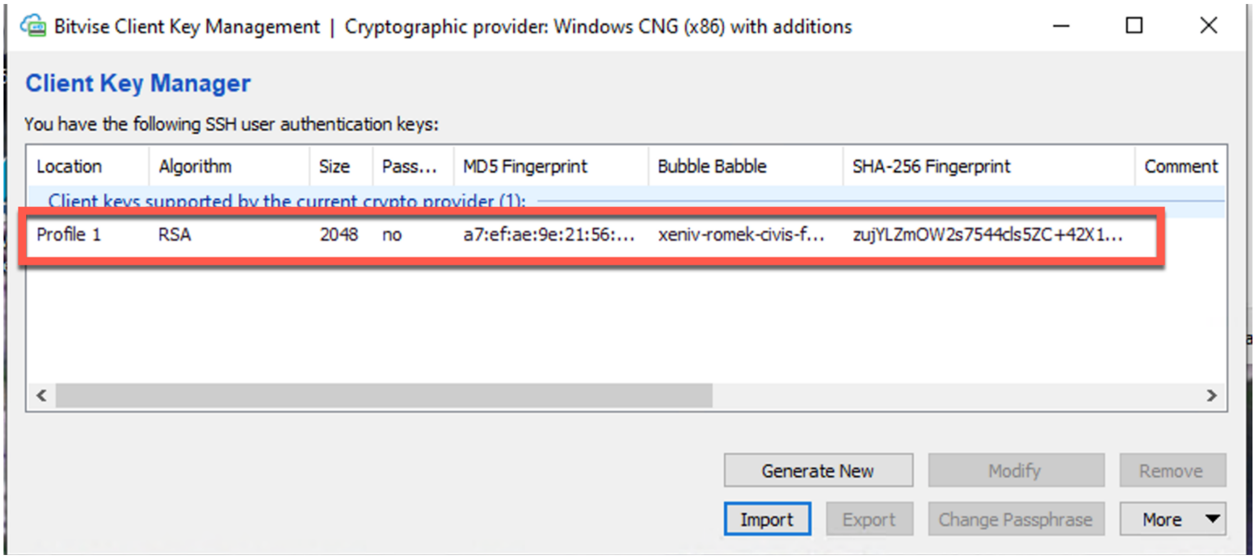
MD5 fingerprint: a7:ef:ae:9e:21:56:65:f3:5b:77:e5:5d:e6:8c:8e:9c

Bubble-babble: xeniv-romek-civis-fevip-reboz-beruv-rigec-gotog-hokym-pudoh-boxyx

SHA-256 fingerprint: zujYLZmOW2s7544cls5ZC+42X1UmZutR+gqzXASD+WQ

Comment:

Figure 5. Save it in Profile Location key #1 by default and Click “Import”.



Bitvise Client Key Management | Cryptographic provider: Windows CNG (x86) with additions

Client Key Manager

You have the following SSH user authentication keys:

Location	Algorithm	Size	Pass...	MD5 Fingerprint	Bubble Babble	SHA-256 Fingerprint	Comment
Client keys supported by the current crypto provider (1):							
Profile 1	RSA	2048	no	a7:ef:ae:9e:21:56:...	xeniv-romek-civis-f...	zujYLZmOW2s7544dls5ZC+42X1...	

Figure 6. Client Key Manager display the imported Global 1 key, our private key.

Step 6. Specify the instance IP address, username, access method, the private key used for accessing the instance.

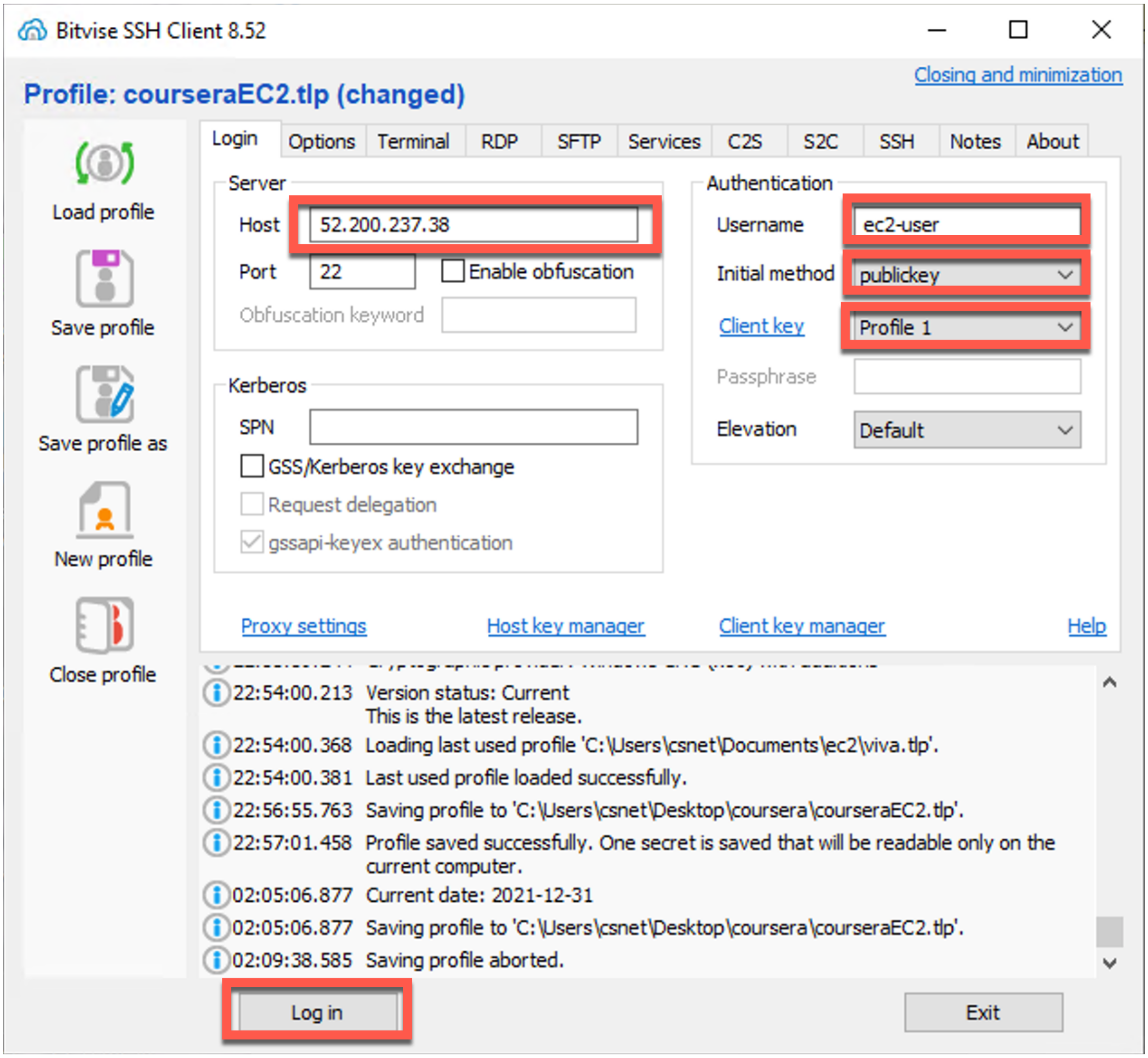
1. Specify public IP address of the instance
Make sure you use the current elastic IP address of the instance.

2. Specify ec2-user as Username
Use "ec2-user", not the "root" for accessing the AWS EC2 instance, since its sshd is configured to be refusing root direct login and there is initially only this single "first" user created.

3. Choose publickey as Initial method
Here we are telling the bitvise SSH client that in this SSH authentication protocol, the SSH Server will use the public key saved in the /home/ec2-user/.ssh/authorized_keys file for verifying the security token generated by the SSH client where a known string is encrypted by the private key and the public key crypto algorithm.

4. Choose Profile key #1 saved in the bitvise SSH Client as private key for this authentication.

5. Click Log in



Profile: courseraEC2.tlp (changed)

Server

Host: 52.200.237.38

Port: 22

□ Enable obfuscation

Obfuscation keyword:

Kerberos

SPN:

□ GSS/Kerberos key exchange

□ Request delegation

☑ gssapi-keyex authentication

Authentication

Username: ec2-user

Initial method: publickey

Client key: Profile 1

Passphrase:

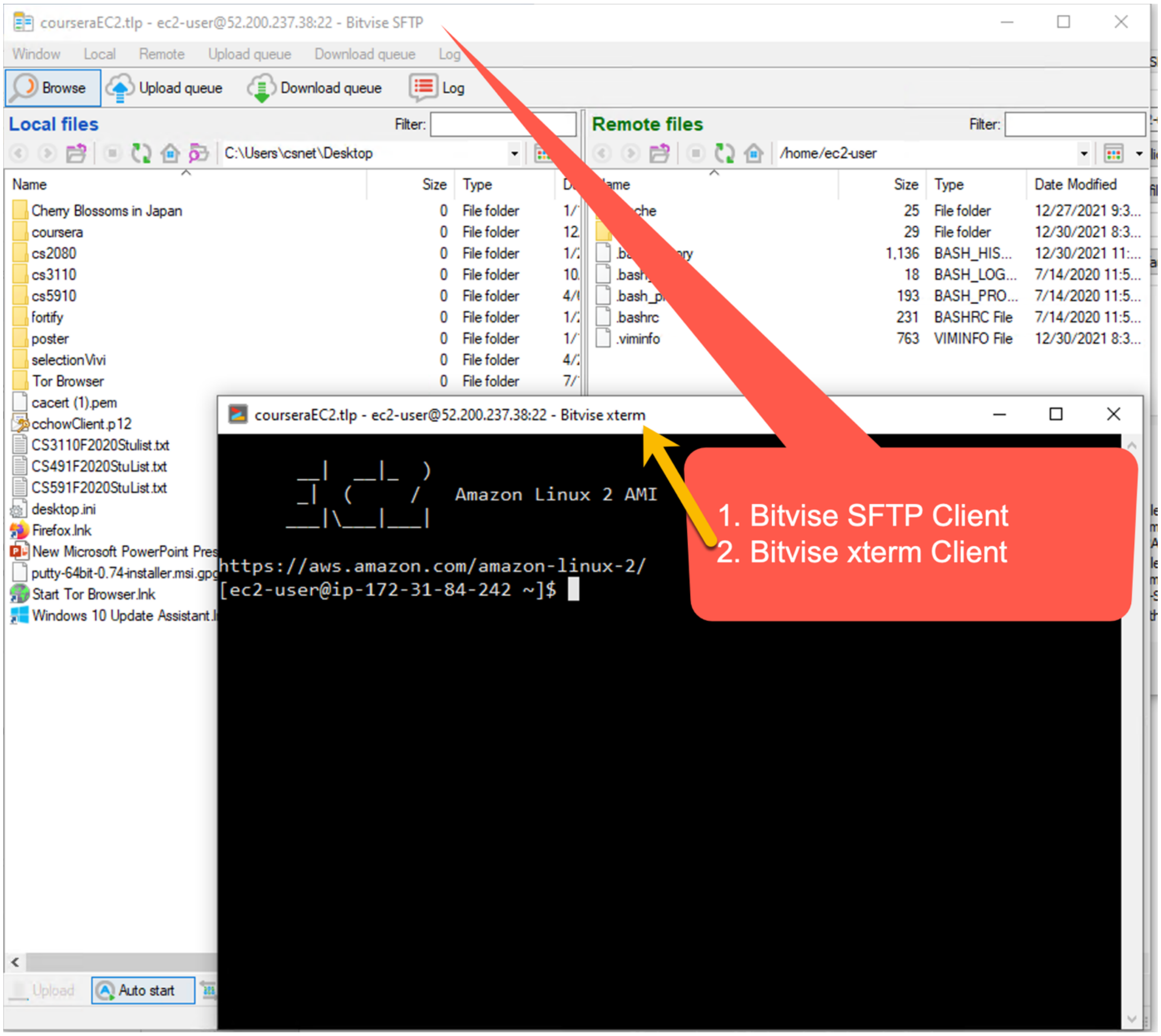
Elevation: Default

```
22:54:00.213  Version status: Current
              This is the latest release.
22:54:00.368  Loading last used profile 'C:\Users\csnet\Documents\ec2\viva.tlp'.
22:54:00.381  Last used profile loaded successfully.
22:56:55.763  Saving profile to 'C:\Users\csnet\Desktop\coursera\courseraEC2.tlp'.
22:57:01.458  Profile saved successfully. One secret is saved that will be readable only on the
              current computer.
02:05:06.877  Current date: 2021-12-31
02:05:06.877  Saving profile to 'C:\Users\csnet\Desktop\coursera\courseraEC2.tlp'.
02:09:38.585  Saving profile aborted.
```

Figure 7. Specify parameters for accessing the SSH daemon on the instance server.

Step 7. The bitvise SSH client app and SFTP app are launched,

Finally the bitvise app launches two tools: Bitvise SFTP Client and Bitvise xterm Client. We use Bitvise SFTP Client for dragging and droping files between SSH client and SSH server and use Bitvise xterm Client for entering/executing commands on a remote terminal session on the instance.



C:\Users\csnet\Desktop

Name	Size	Type	D
Cherry Blossoms in Japan	0	File folder	1/
coursera	0	File folder	12
cs2080	0	File folder	1/
cs3110	0	File folder	10
cs5910	0	File folder	4/
fortify	0	File folder	1/
poster	0	File folder	1/
selectionVivi	0	File folder	4/
Tor Browser	0	File folder	7/
cacert (1).pem			
cchowClient.p12			
CS3110F2020Stulist.txt			
CS491F2020StuList.txt			
CS591F2020StuList.txt			
desktop.ini			
Firefox.lnk			
New Microsoft PowerPoint Pres			
putty-64bit-0.74-installer.msi.gpg			
Start Tor Browser.lnk			
Windows 10 Update Assistant.l			

/home/ec2-user

Name	Size	Type	Date Modified
che	25	File folder	12/27/2021 9:3...
	29	File folder	12/30/2021 8:3...
.ba ry	1,136	BASH_HIS...	12/30/2021 11:...
.bash	18	BASH_LOG...	7/14/2020 11:5...
.bash_p	193	BASH_PRO...	7/14/2020 11:5...
.bashrc	231	BASHRC File	7/14/2020 11:5...
.viminfo	763	VIMINFO File	12/30/2021 8:3...

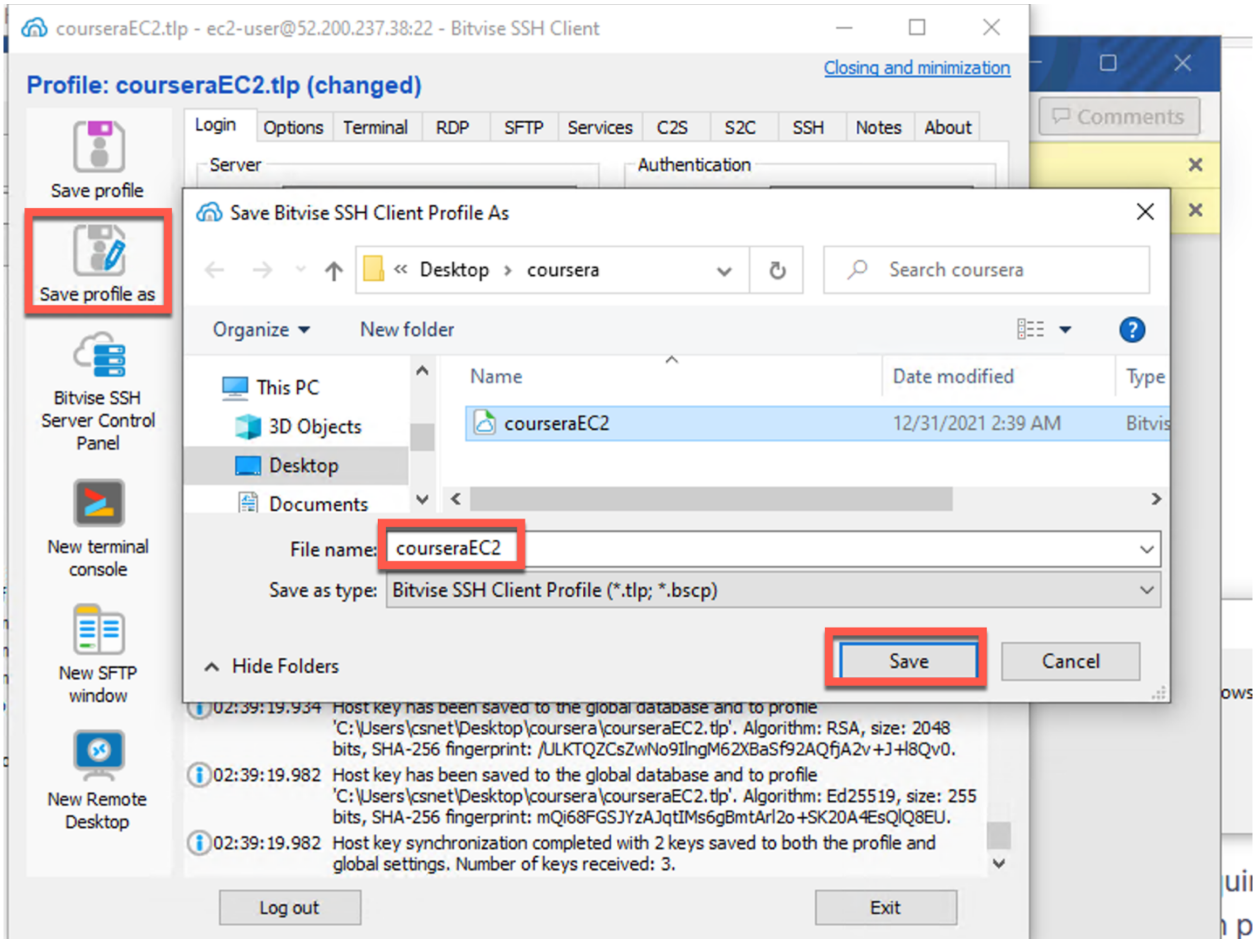
```
       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-84-242 ~]$ 
```

1. Bitvise SFTP Client
2. Bitvise xterm Client

Figure 8. Bitvise SFTP Client and Bitvise xterm Client

Step 8. Save the SSH configuration as a profile for future reference.

Click "Save profile" and enter CourseraEC2 as profile name. Next time we start bitvise, it will remember the current profile. In we have switched to different profile, we can also click Open profile to bring back the SSH settings for accessing the instance. Click Login to verify if it works.



File name: courseraEC2

Save as type: Bitvise SSH Client Profile (*.tlp; *.bscp)

```
02:39:19.934  Host key has been saved to the global database and to profile
              'C:\Users\csnet\Desktop\coursera\courseraEC2.tlp'. Algorithm: RSA, size: 2048
              bits, SHA-256 fingerprint: /ULKTQZCsZwNo9IlngM62XBaSf92AQfjA2v+J+l8Qv0.
02:39:19.982  Host key has been saved to the global database and to profile
              'C:\Users\csnet\Desktop\coursera\courseraEC2.tlp'. Algorithm: Ed25519, size: 255
              bits, SHA-256 fingerprint: mQi68FGSJYzAJqtIMs6gBmtArl2o+SK20A4EsQlQ8EU.
02:39:19.982  Host key synchronization completed with 2 keys saved to both the profile and
              global settings. Number of keys received: 3.
```

Figure 9. Save profile for future reference.

3.2.2 Option: Install putty SSH Client

3.2.3 Install putty SSH Client

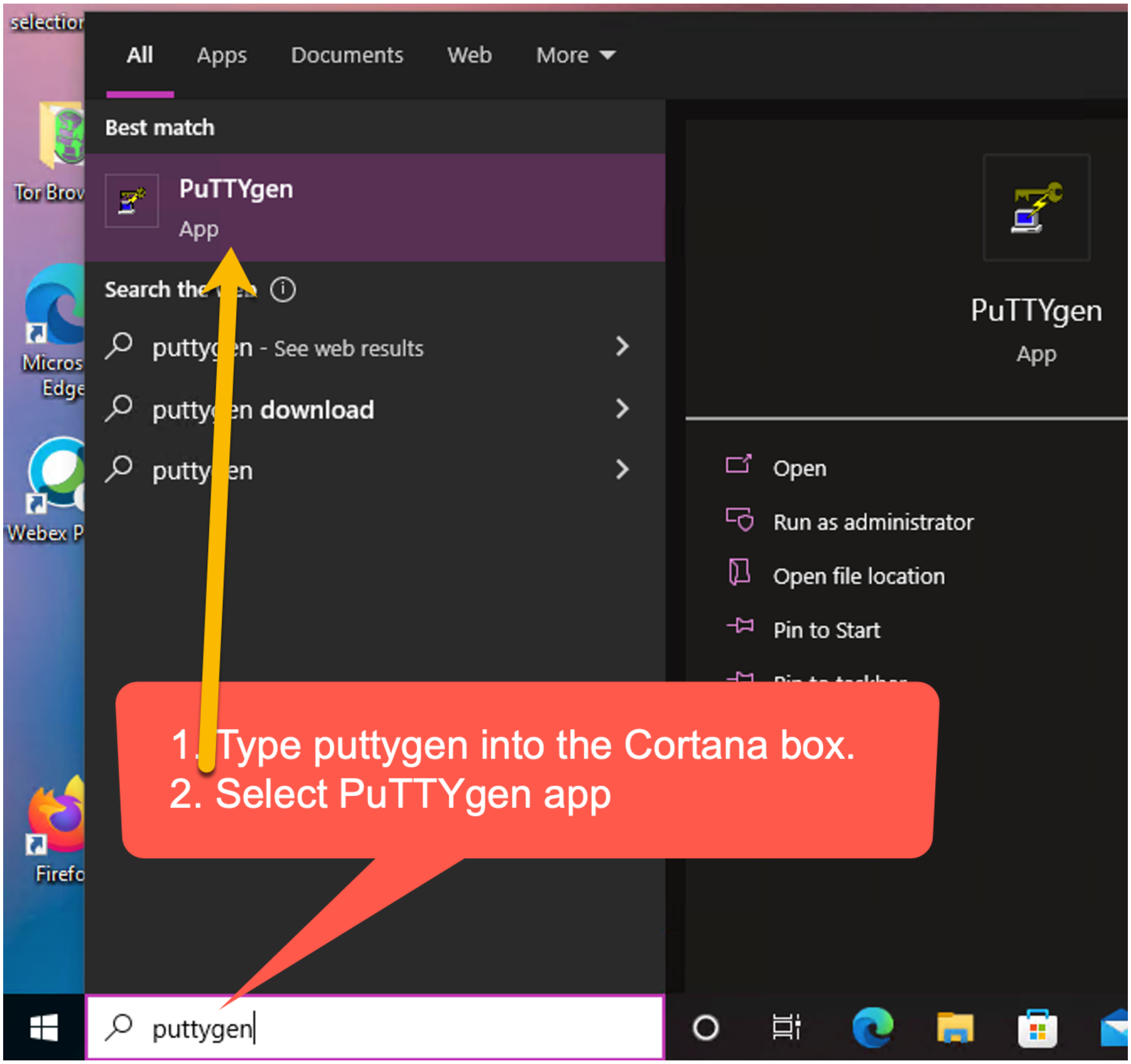
The putty is also a popular command line interface app and can be downloaded at https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html (choose the proper msi file). The current version is 0.76 *as of 12/31/2021.*

After download and install the putty app, you should see the following app installed on the upper left corn or the desktop.

3.2.4. Follow the steps below to setup the private key for accessing your instance using putty.

Step 1. Use PuTTYgen app to convert the .pem file to .ppk private key format

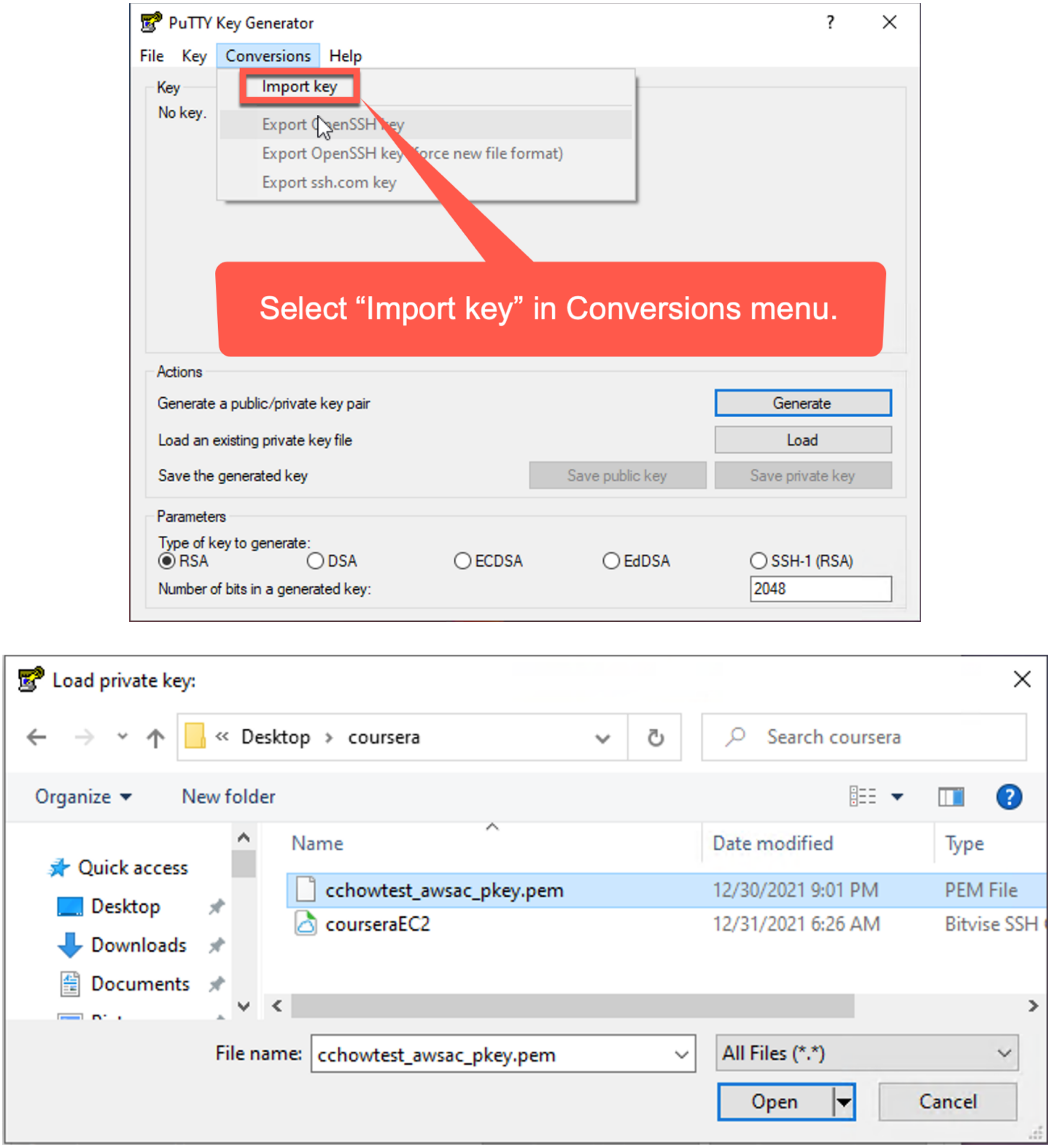
The current putty version does not accept the .pem file format. Type puttygen into the Cortana box. Select PuTTYgen app.



1. Type puttygen into the Cortana box.
2. Select PuTTYgen app

Figure 10. Open PuttyGen app.

Select Import key menuitem in Convert menu to conver the .pem file format to .ppk file format.



Select “Import key” in Conversions menu.

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Name	Date modified	Type
cchowtest_awsac_pkey.pem	12/30/2021 9:01 PM	PEM File
courseraEC2	12/31/2021 6:26 AM	Bitvise SSH

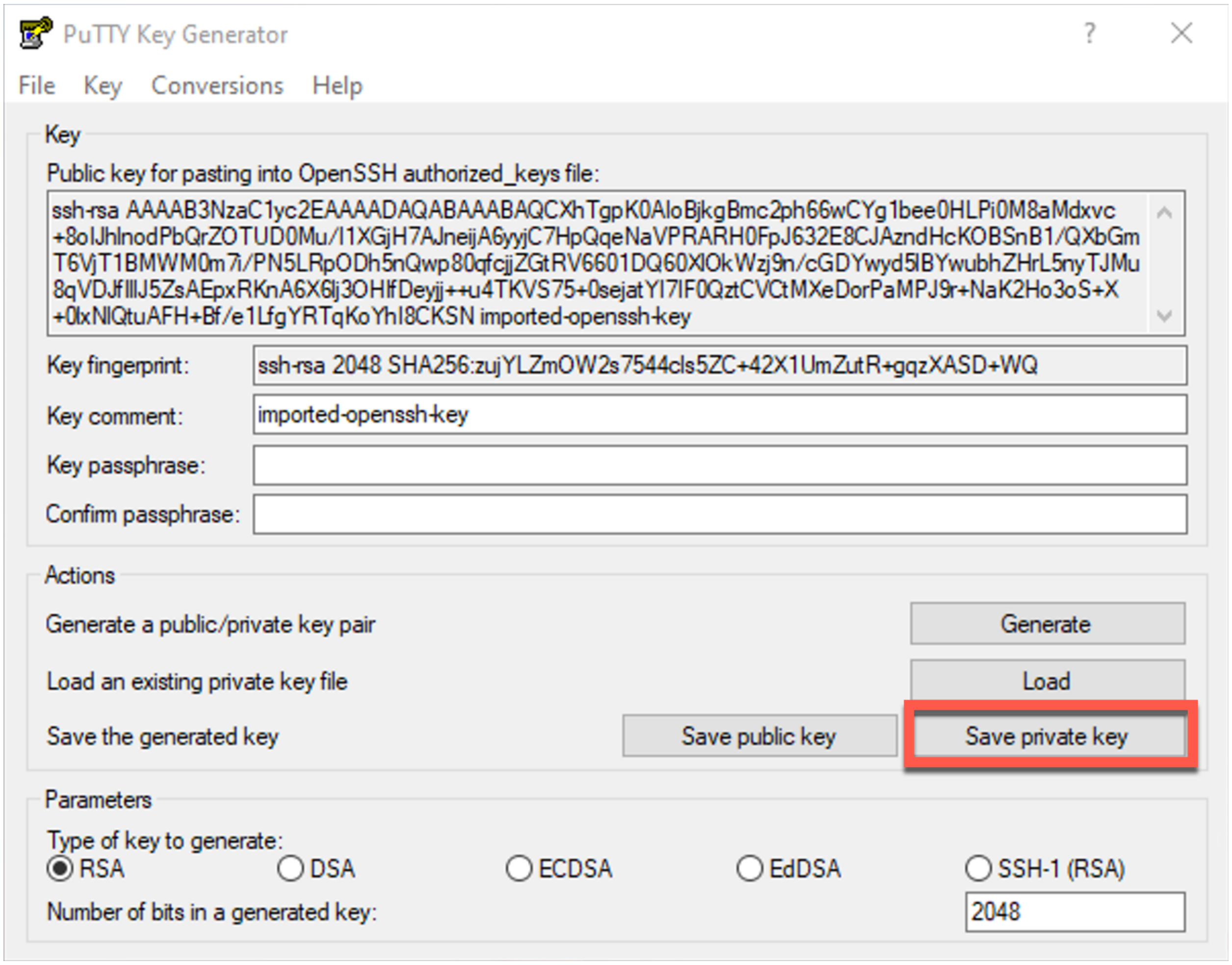
File name: cchowtest_awsac_pkey.pem

All Files (*.*)

Figure 11. Choose Import key in Conversions menu.

After selecting the private key, the app converted the .pem file into .ppk file format.

We can click on the “Save Private Key” button to save the file.



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCXhTgpK0AloBjkgBmc2ph66wCYg1bee0HLPi0M8aMdxvc
+8olJhlnodPbQrZOTUD0Mu/I1XGjH7AJneijA6yyjC7HpQqeNaVPRARH0FpJ632E8CJAzndHcKOBSnB1/QXbGm
T6VjT1BMWM0m7i/PN5LRpODh5nQwp80qfcjjZGtRV6601DQ60XlOkWzj9n/cGDYwyd5lBYwubhZHrL5nyTJMu
8qVDJfIIlJ5ZsAEpxRKnA6X6lj3OHlfDeyjj++u4TKVS75+0sejatYI7IF0QztCVCtMXeDorPaMPJ9r+NaK2Ho3oS+X
+0lxNIQtuAFH+Bf/e1LfgYRTqKoYhI8CKSN imported-openssh-key
```

Key fingerprint: ssh-rsa 2048 SHA256:zujYLZmOW2s7544cls5ZC+42X1UmZutR+gqzXASD+WQ

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

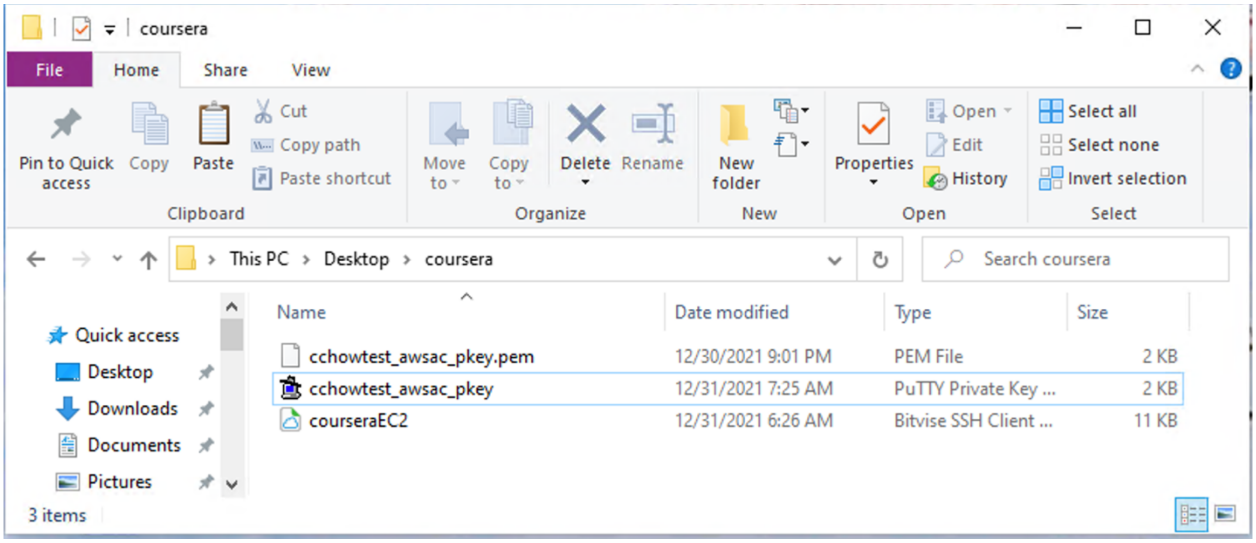
Save the generated key

Parameters

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

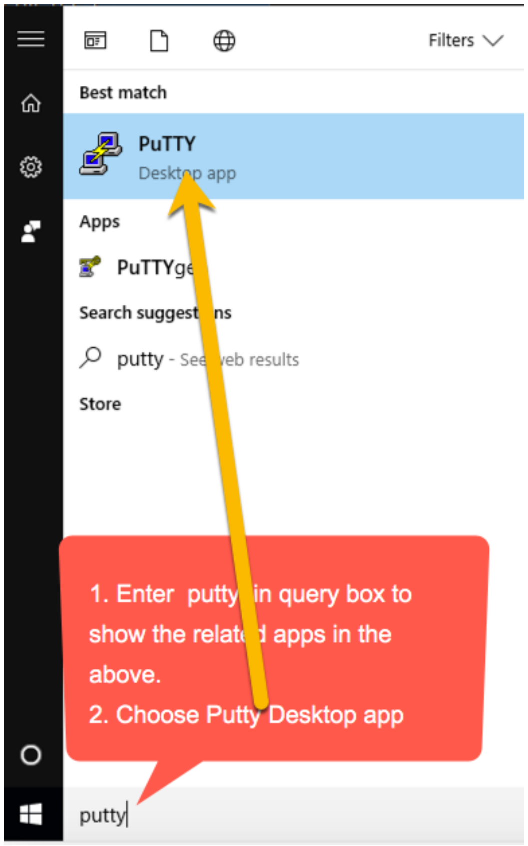
Number of bits in a generated key: 2048

Make sure you remove .pem in the filename. The result file name in our example is cchowtest_awsac_pkey.ppk



Name	Date modified	Type	Size
cchowtest_awsac_pkey.pem	12/30/2021 9:01 PM	PEM File	2 KB
cchowtest_awsac_pkey	12/31/2021 7:25 AM	PuTTY Private Key ...	2 KB
courseraEC2	12/31/2021 6:26 AM	Bitvise SSH Client ...	11 KB

Step 2. Start putty app.

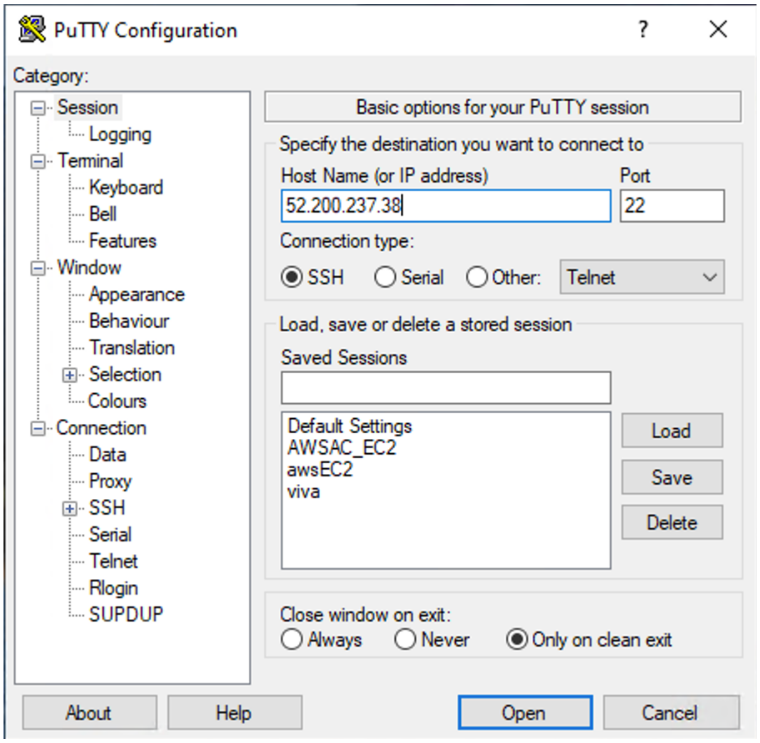


1. Enter putty in query box to show the related apps in the above.
2. Choose Putty Desktop app

putty

Figure 12. Launch putty app.

Step 3. Enter the public IP address in the Hostname or IP address field.



Host Name (or IP address): 52.200.237.38

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

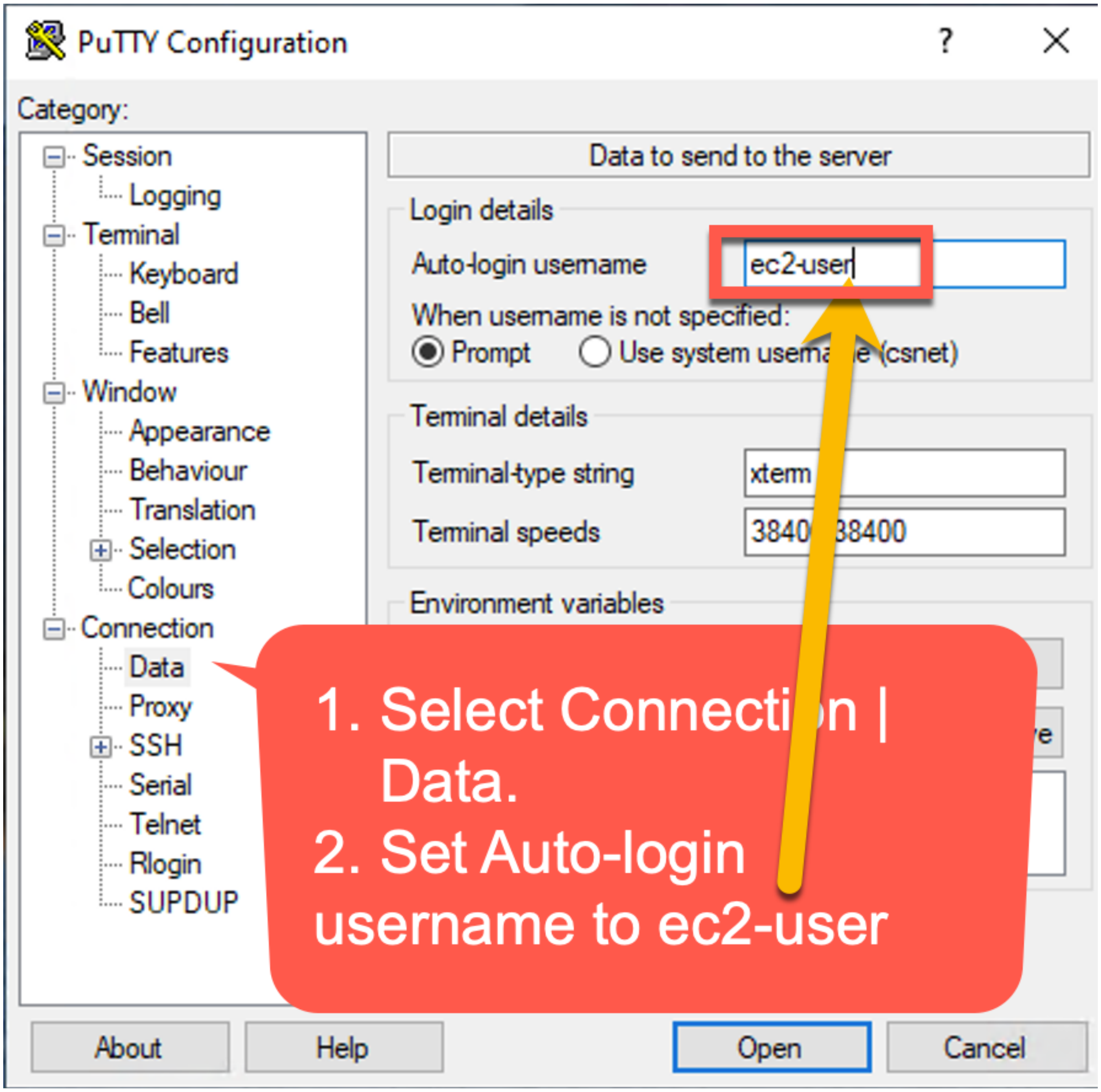
Saved Sessions:

Default Settings
AWSAC_EC2
awsEC2
viva

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

Figure 13. Specify Instance IP address and Clock Connection Data.

Step 4. Click **Connection > Data** in the left-hand navigation pane and set the Auto-login username to ec2-user.   It is critical we set the username to ec2-user instead of root which shows in my putty set up tutorial.



Auto-login username: ec2-user

When username is not specified:
● Prompt ○ Use system username (csnet)

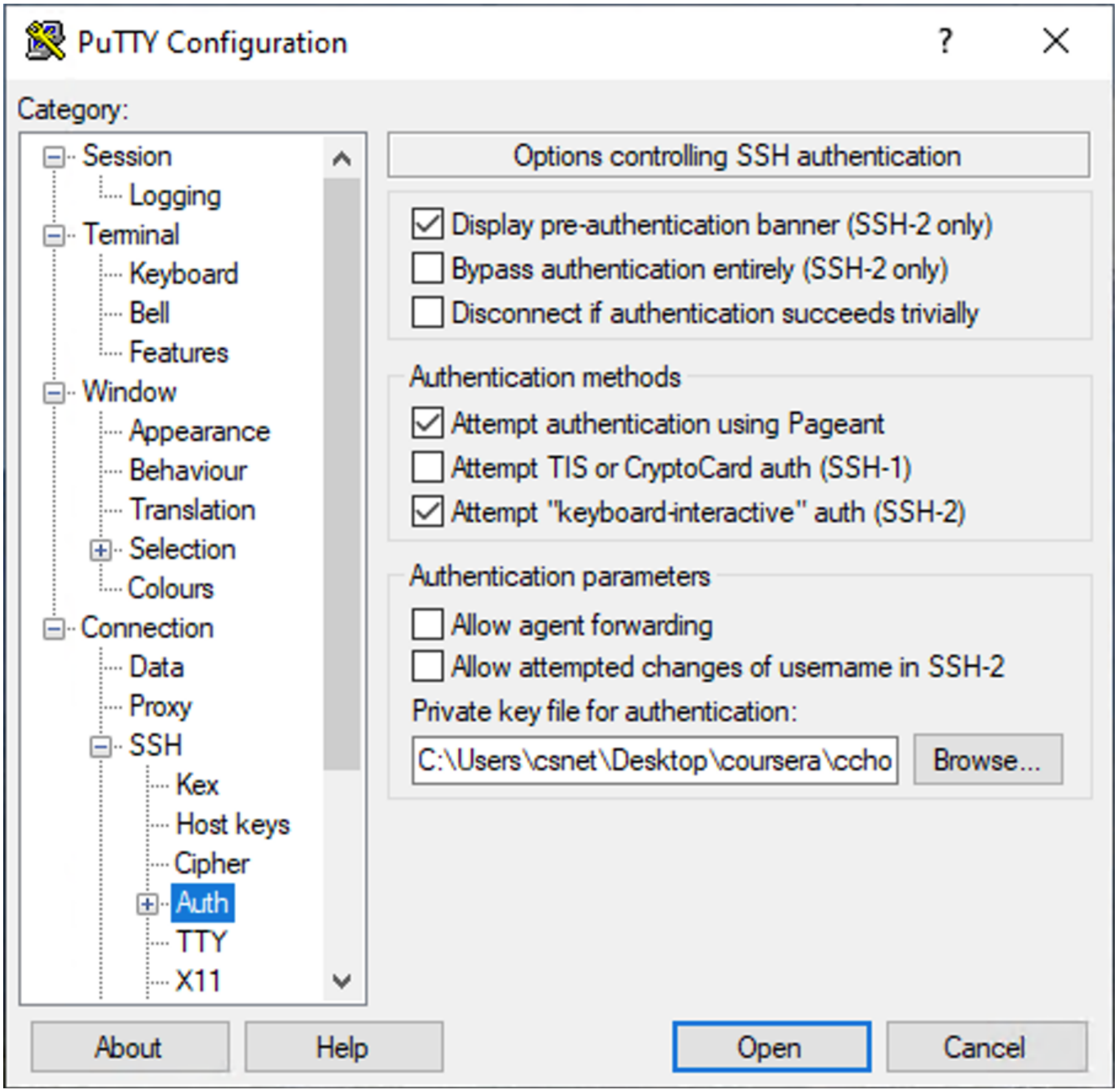
Terminal-type string: xterm

Terminal speeds: 38400,38400

1. Select Connection | Data.
2. Set Auto-login username to ec2-user

Figure 14. Set Autologin username to ec2-user.

Step 5. Click **Connection > SSH > Auth** in the left-hand navigation pane and configure the private key to use by clicking **Browse** under Private key file for authentication.



☑ Display pre-authentication banner (SSH-2 only)
□ Bypass authentication entirely (SSH-2 only)
□ Disconnect if authentication succeeds trivially

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

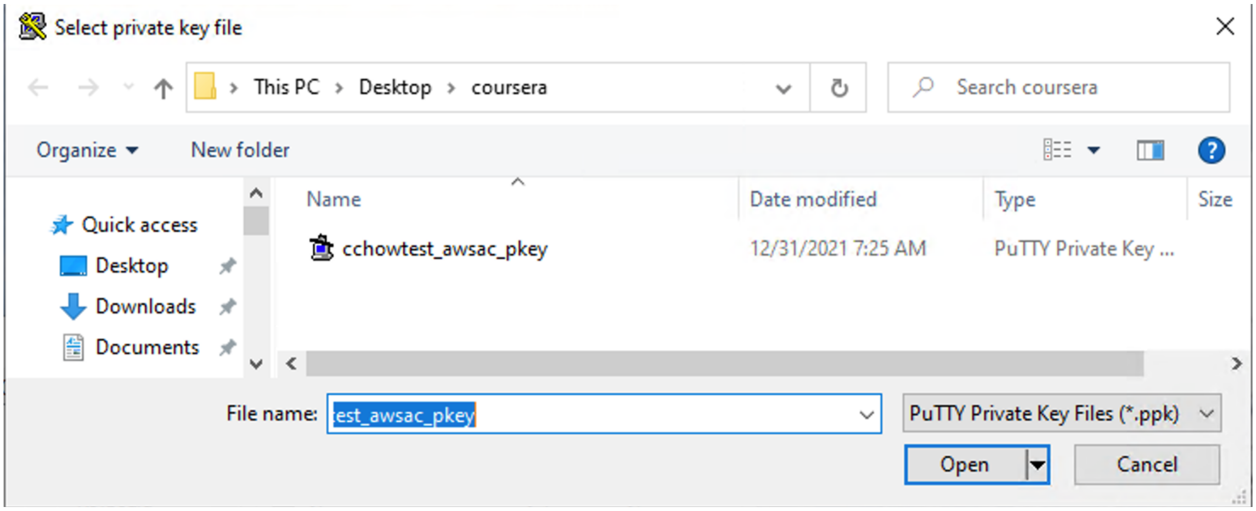
□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication: C:\Users\csnet\Desktop\coursera\ccho

Figure 15. Set private key for the session.

When browsing to select the private key file, make sure you select the private key file in .ppk format which PuTTYgen generates for us.

See Figure 16.



cchowtest_awsac_pkey 12/31/2021 7:25 AM PuTTY Private Key ...

File name: est_awsac_pkey

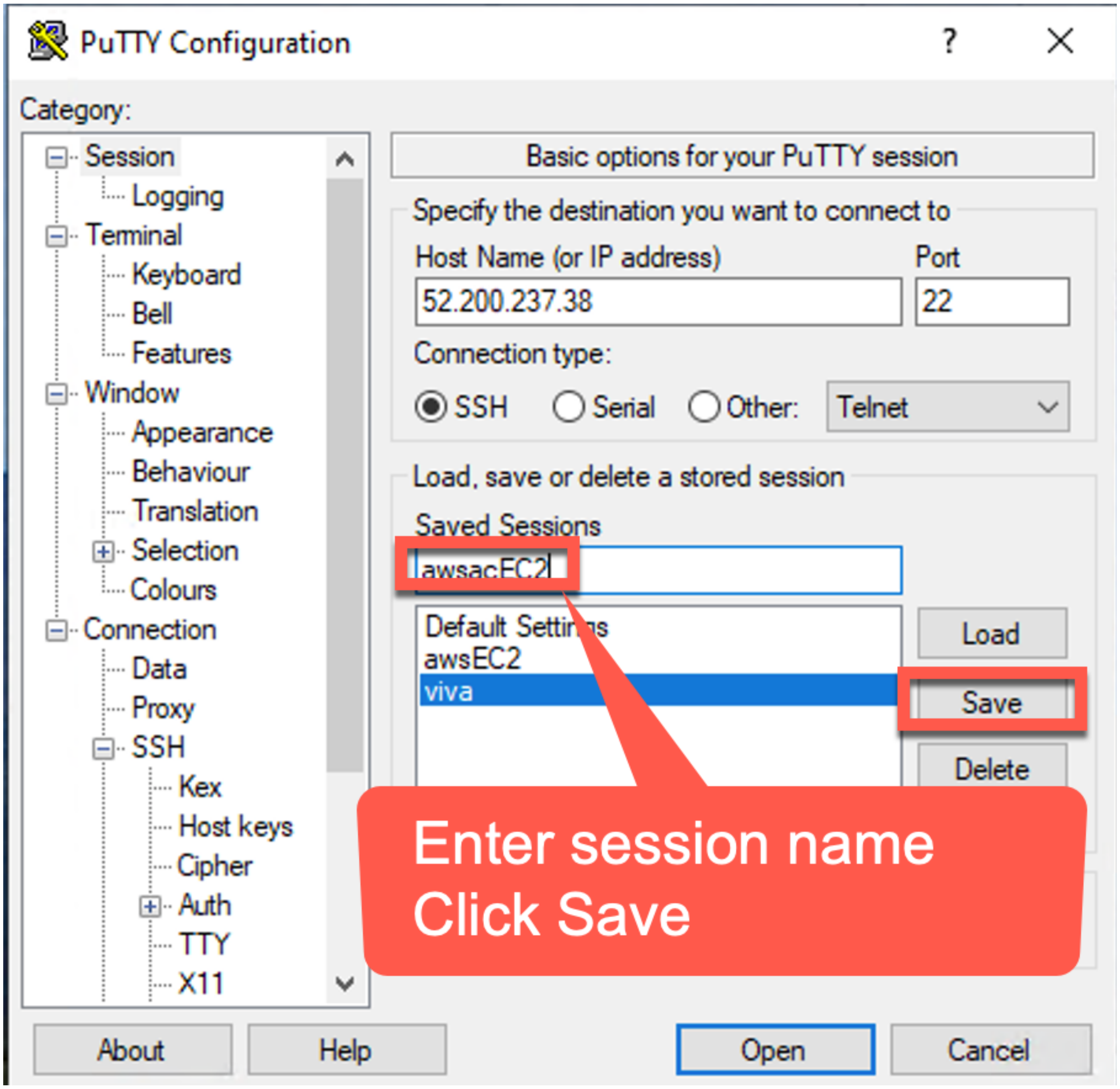
PuTTY Private Key Files (*.ppk)

Figure 16. Select the private key file in .ppk file format.

Navigate to the location where you saved your private key earlier, select the file, and click **Open**.

The private key path is now displayed in the **Private key file for authentication** field.

Step 6. Click **Session** in the left-hand navigation pane and click **Save** in the Load, save or delete a stored session section.



Host Name (or IP address): 52.200.237.38

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

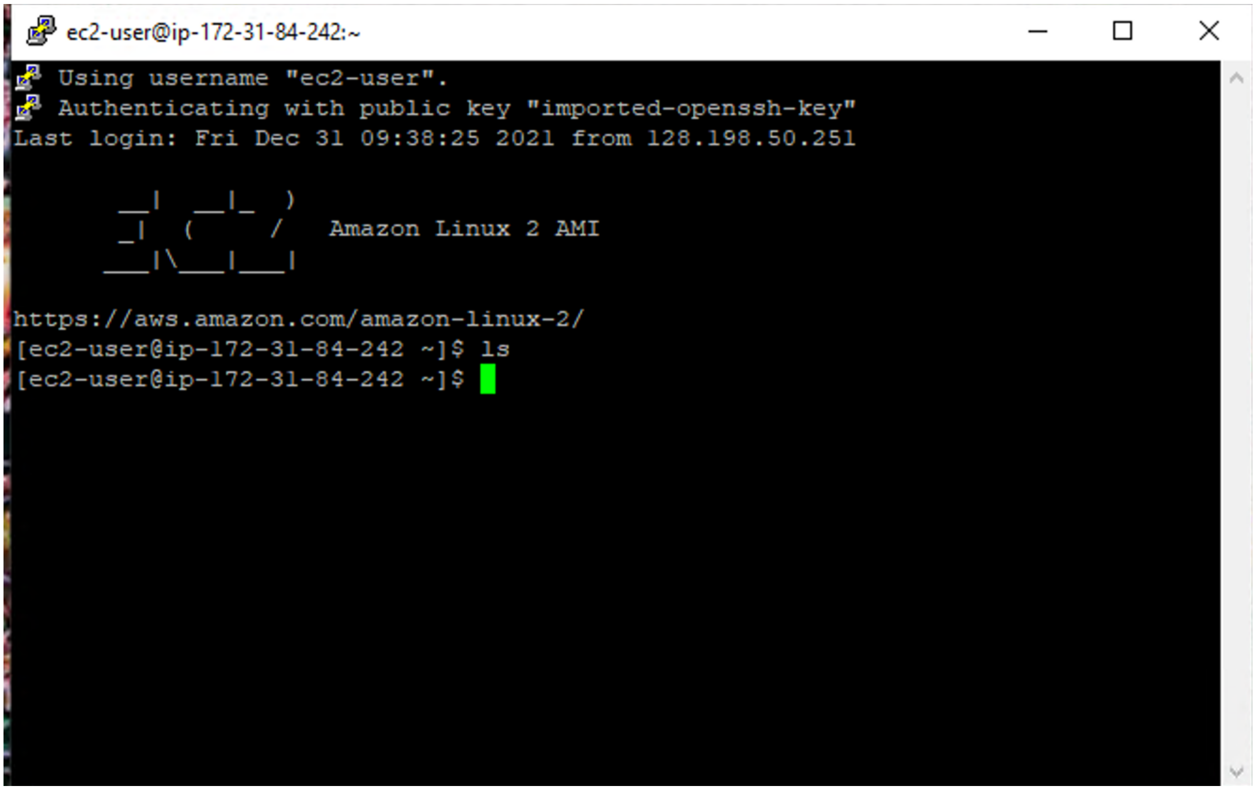
Saved Sessions: awsacEC2

Default Settings
awsEC2
viva

Enter session name
Click Save

Figure 17. Save Session with awsacEC2 as session name for future usage.

Step 7. Click **Open** to begin your session with the server. See Figure 18 for a successful login to our instance.



```
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Fri Dec 31 09:38:25 2021 from 128.198.50.251

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-84-242 ~]$ ls
[ec2-user@ip-172-31-84-242 ~]$
```

Figure 18. Putty Terminal session to AMI Linux instance without login password.

3.3. What you do when you get "failed to connect" message?

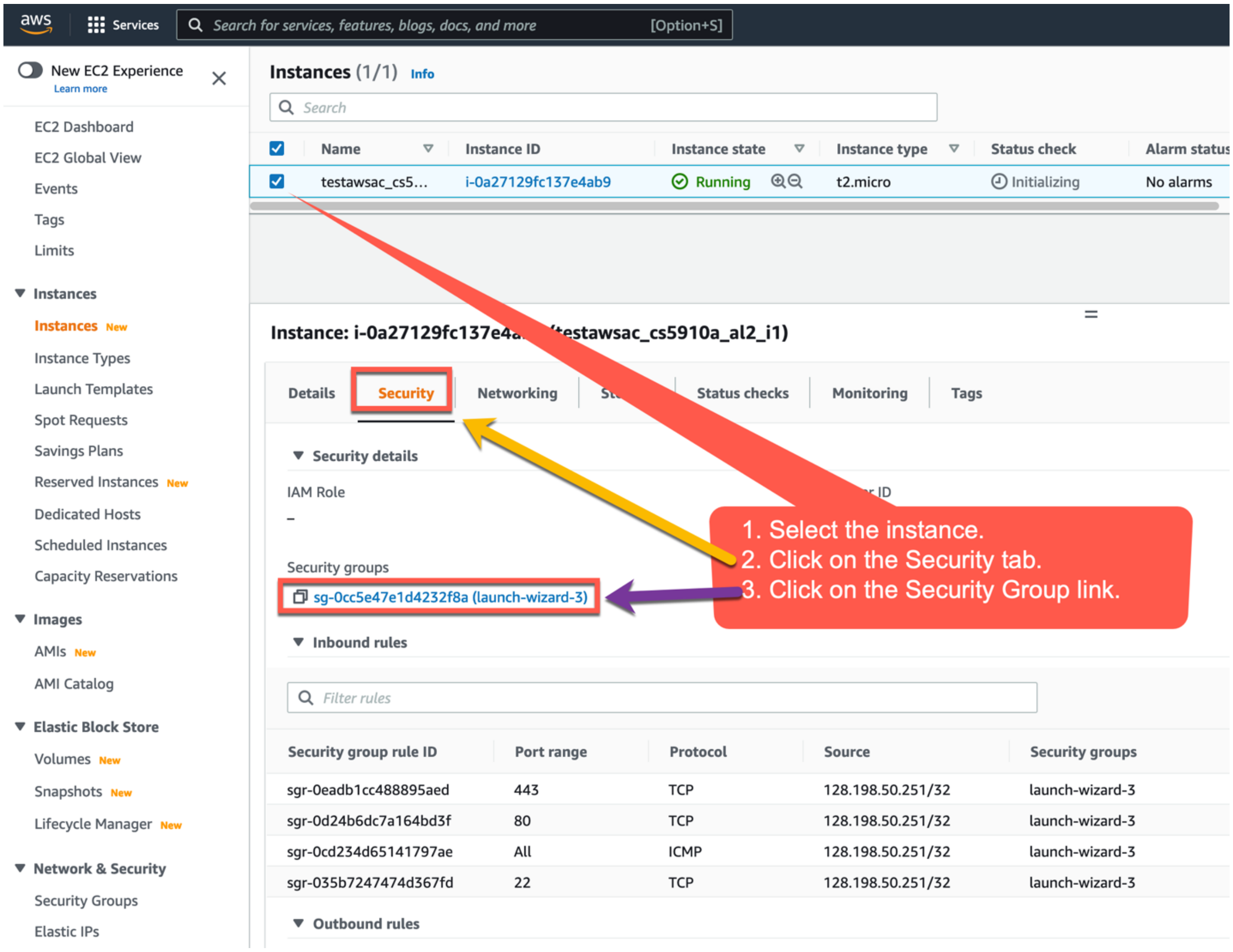
When your SSL terminal client failed to make connection to your AMI Linux server instance, there could be several reasons and some can be easily solved, others may take systematic diagnoses:

Possible Reason 1: You may not set the Source List of the security group of your instance properly.

The common situation is that we moved our client machine to a different subnet or location and was assigned with a different public IP address. In that case we need to reselect the "My IP" in the source column of all the related security group rules, so that the instance will accept the new connections coming from that new client location.

The security group specifies the firewall rules that govern the incoming or outgoing connection. The source list of the incoming firewall rules is particularly important and need to be configured correctly. It should include the current assigned IP address of your client machine. Without that, any connection from the client will be rejected. In Page 11 of Section 2.1.6. Step 6. Configure Security Group, we show how to add the current IP address of your client to the allowed connected Source List. Perhaps you missed the step. Here is how to add it after the instance is already created and running:

Step a. Select the instance and choose its security groups.



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	testawsac_cs5…	i-0a27129fc137e4ab9	Running	t2.micro	Initializing	No alarms

Instance: i-0a27129fc137e4a /testawsac_cs5910a_al2_i1)

Security details

IAM Role

–

Security groups

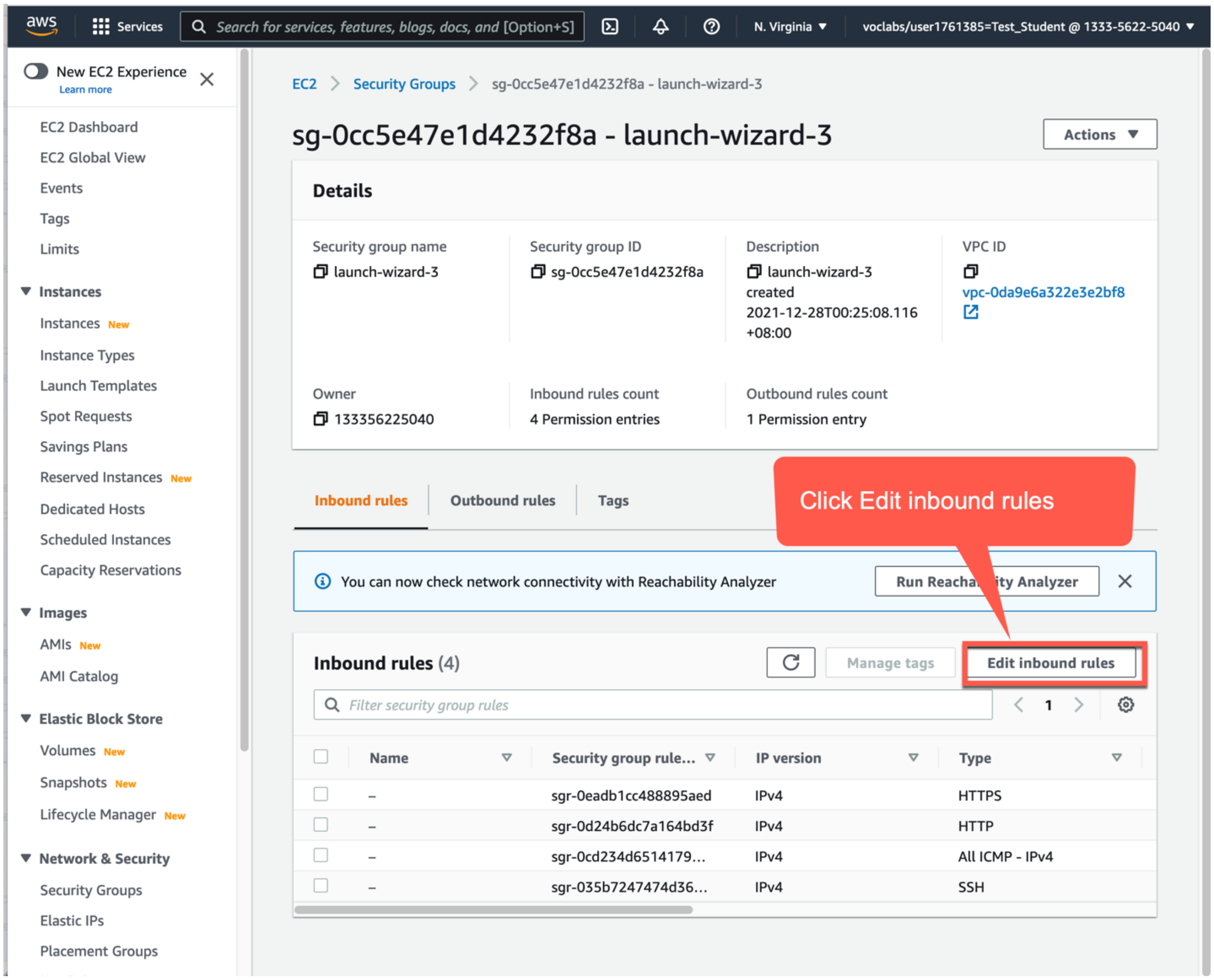
sg-0cc5e47e1d4232f8a (launch-wizard-3)

Inbound rules

Security group rule ID	Port range	Protocol	Source	Security groups
sgr-0eadb1cc488895aed	443	TCP	128.198.50.251/32	launch-wizard-3
sgr-0d24b6dc7a164bd3f	80	TCP	128.198.50.251/32	launch-wizard-3
sgr-0cd234d65141797ae	All	ICMP	128.198.50.251/32	launch-wizard-3
sgr-035b7247474d367fd	22	TCP	128.198.50.251/32	launch-wizard-3

1. Select the instance.
2. Click on the Security tab.
3. Click on the Security Group link.

Step b. Edit inbound rules.



sg-0cc5e47e1d4232f8a - launch-wizard-3

Details

Security group name	Security group ID	Description	VPC ID
launch-wizard-3	sg-0cc5e47e1d4232f8a	launch-wizard-3 created 2021-12-28T00:25:08.116 +08:00	vpc-0da9e6a322e3e2bf8

Owner	Inbound rules count	Outbound rules count
133356225040	4 Permission entries	1 Permission entry

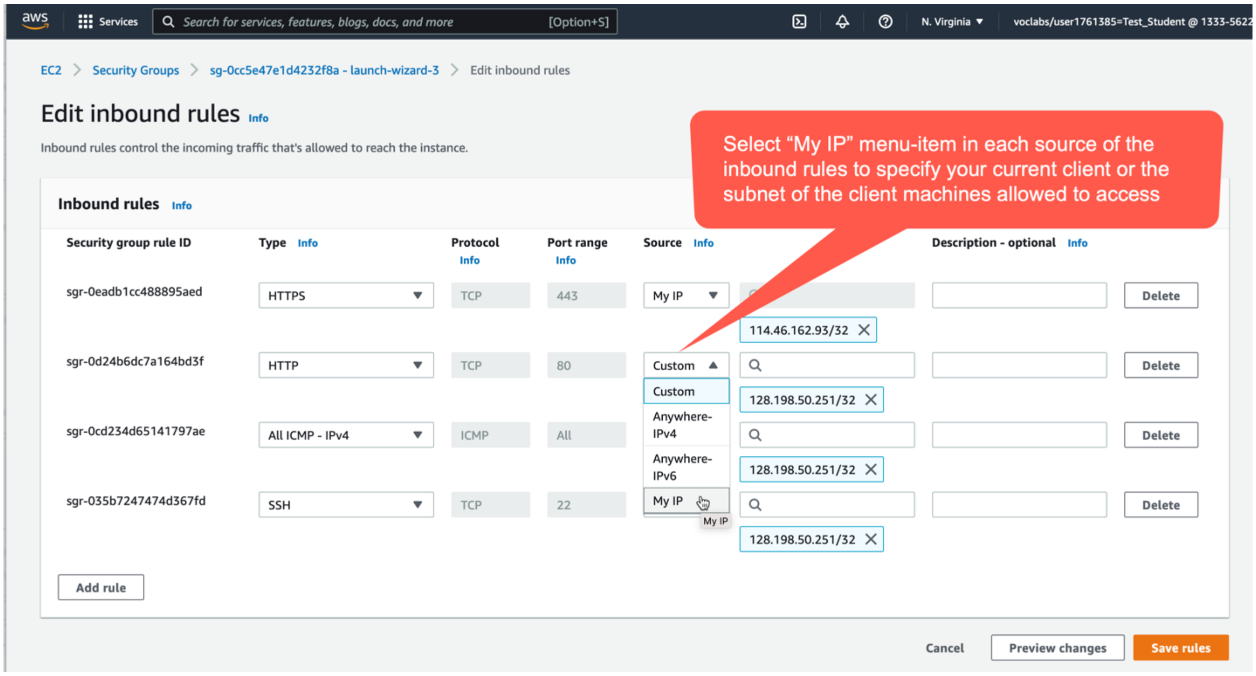
You can now check network connectivity with Reachability Analyzer

Inbound rules (4)

□	Name	Security group rule...	IP version	Type
□	–	sgr-0eadb1cc488895aed	IPv4	HTTPS
□	–	sgr-0d24b6dc7a164bd3f	IPv4	HTTP
□	–	sgr-0cd234d6514179...	IPv4	All ICMP - IPv4
□	–	sgr-035b7247474d36...	IPv4	SSH

Click Edit inbound rules

Step c. Set new My IP



EC2 > Security Groups > sg-0cc5e47e1d4232f8a - launch-wizard-3 > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional	
sgr-0eadb1cc488895aed	HTTPS	TCP	443	My IP	114.46.162.93/32		Delete
sgr-0d24b6dc7a164bd3f	HTTP	TCP	80	Custom	128.198.50.251/32		Delete
sgr-0cd234d65141797ae	All ICMP - IPv4	ICMP	All		128.198.50.251/32		Delete
sgr-035b7247474d367fd	SSH	TCP	22		128.198.50.251/32		Delete

Select "My IP" menu-item in each source of the inbound rules to specify your current client or the subnet of the client machines allowed to access

aws
Services
Search for services, features, blogs, docs, and more [Option+S]
N. Virginia
voclabs/user1761385=Test_Student @ 1333-5622
Custom
Anywhere-IPv4
Anywhere-IPv6
My IP
My IP
Add rule
Cancel
Preview changes
Save rules

Possible Reason 2. Use wrong private key or the app can not find the right private key. Check if the private key you configured is associated with the creation of the related instance. Often we found a wrong private key is used, when there are multiple private keys for multiple instances. For Mac or Linux client, when you use ssh command with -i option, make sure you are in the right directory that contains the related private key.

Possible Reason 3. There is potential Internet outage between you and the AWS region. Make sure you get response from a server in the same AWS region of your instance.
In our case, for learners using AWS Academy free service, they can use command "ping -c 2 rds.us-east-1.amazonaws.com" or access web page https://rds.us-east-1.amazonaws.com and see if you get response. If not, you can systematically check if it is the network problem between your machine and the AWS region. Starting from ping your local residential gateway such as 192.168.0.1, and see if you can reach a known internet site you often visit.

4. Install LAMP Server Package

Many of our cybersecurity exploit examples can be illustrated with a server system installed with Linux Apache MySQL PHP (LAMP) server package. Follow the following steps in this web page to set up LAMP servers on our new instance. We remote login to our AWS instance to run the related system configuration commands. It will take about 25 minutes to complete the whole process, including the installation of phpMyAdmin to manage the MySQL server through php web pages.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-lamp-amazon-linux-2.html

Note that in the above web page, it does not provide detailed info in setting up and running a httpd server that supports for HTTPS (HTTP Secure) which protect your data with SSL/TLS encryption. To add that support, please follow the instruction in the web page
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/SSL-on-amazon-linux-2.html

Use the following yum command to install the mod_ssl package for HTTPS.

```
[ec2-user@ip-172-31-84-242 ~]$  yum install mod_ssl.x86_64
…
```

Here we run the four commands in the instance to create and set up certificate and private key for the web server.

```
[ec2-user@ip-172-31-84-242 ~]$  cd /etc/pki/tls/certs
[ec2-user@ip-172-31-84-242 certs]$ sudo ./make-dummy-cert localhost.crt
[ec2-user@ip-172-31-84-242 certs]$ sudo vi /etc/httpd/conf.d/ssl.conf
```

Using the editor we comment out Line 107 by adding # as the first character in that line, similar to the one below.

```
#SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

The reason we do that is the localhost.crt combines the certificate and private key created using the make-dummy-cert. In this simple set up, they are combined in a single file. Normally we separate certificate and private key into two separate files and also saved in different directories for better protection.

```
[ec2-user@ip-172-31-84-242 certs]$ sudo systemctl restart httpd
```

A related LAMP installation session was captured and saved in
http://ciast.uccs.edu/coursera/pub/LAMPInstallationSession.pdf
for your reference.

5. Create Project Web Page and Verify Access

The AMI Linux instance is installed with Apache web server and the default web site is located in /var/www/html.

Task 1. Create default web page.

For this project and to test the access control of web access to instances, we like to uniquely identify the web server by creating a default web page with the following simple content as /var/www/html/index.html.

<h1>This is the Apache web server created by <your email address> for CS5910 Coursera Specialization</h1>

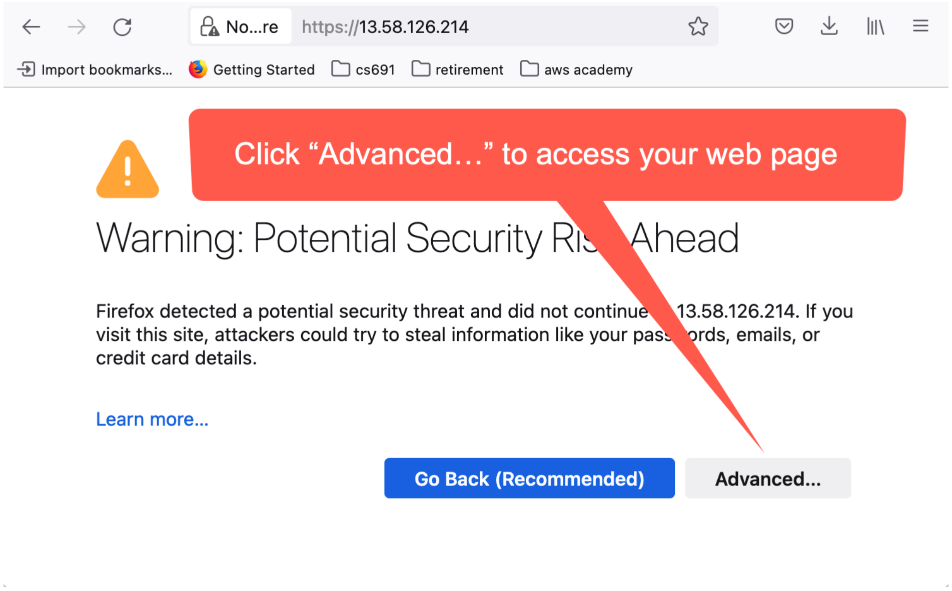
where <your email address> is the one you used for your Coursera account. Note that you have control over the access to this web server. Only you and your peer reviewers will have accessed to this web page.

Verify Web Access

Type https://<your instance IP address>/ in the firefox browser of your local machine to verify if the default web page is up. Here replace the <your instance IP address> with the IP address of the instance you set up. In my case, it is.
Capture the browser image of your default web page as myWebSite.png similar to Figure 19c below.

Deliverable of Project 1a: Submit the above captured firefox browser image of the default web site of the instance as deliverable for Project 1a.

Note that the web browser will warn the web access is not secure, since the certificate presented by the web server is self-signed, not signed by a public Certificate Authority (CA). On firefox browser, click “Advanced” and then “Add Exception…” followed by “Confirmed Security Exception”.

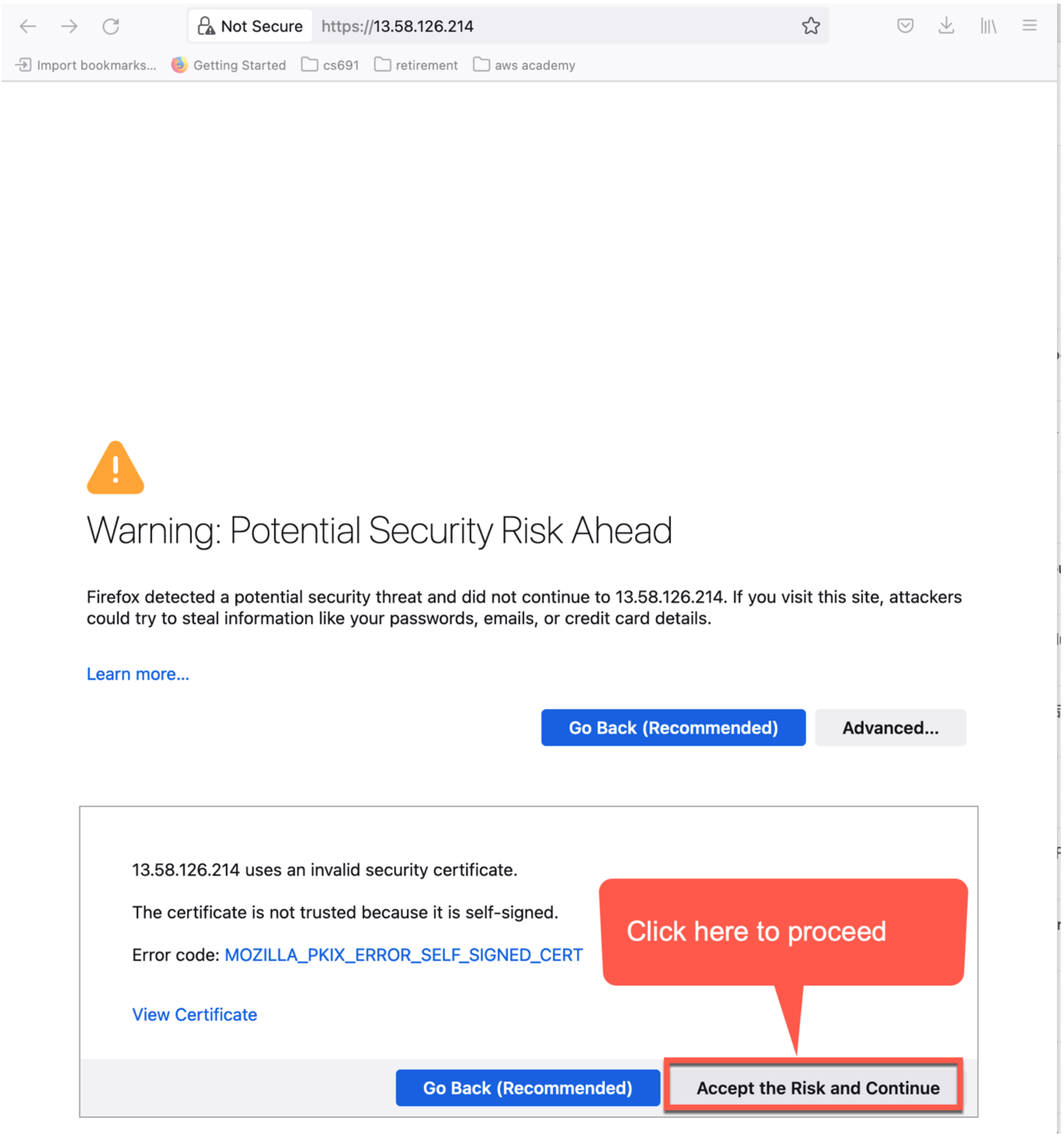


Click “Advanced…” to access your web page

Warning: Potential Security Ris Ahead

Firefox detected a potential security threat and did not continue 13.58.126.214. If you visit this site, attackers could try to steal information like your pass ords, emails, or credit card details.

Figure 19a. Brower warns the potential man-in-the middle attack.



Warning: Potential Security Risk Ahead

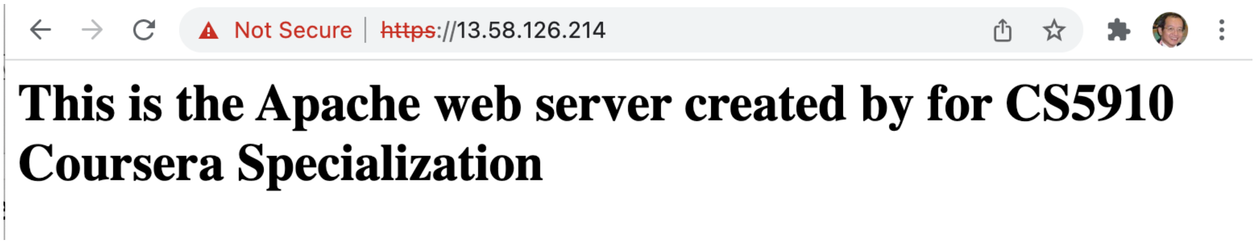
Firefox detected a potential security threat and did not continue to 13.58.126.214. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

13.58.126.214 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

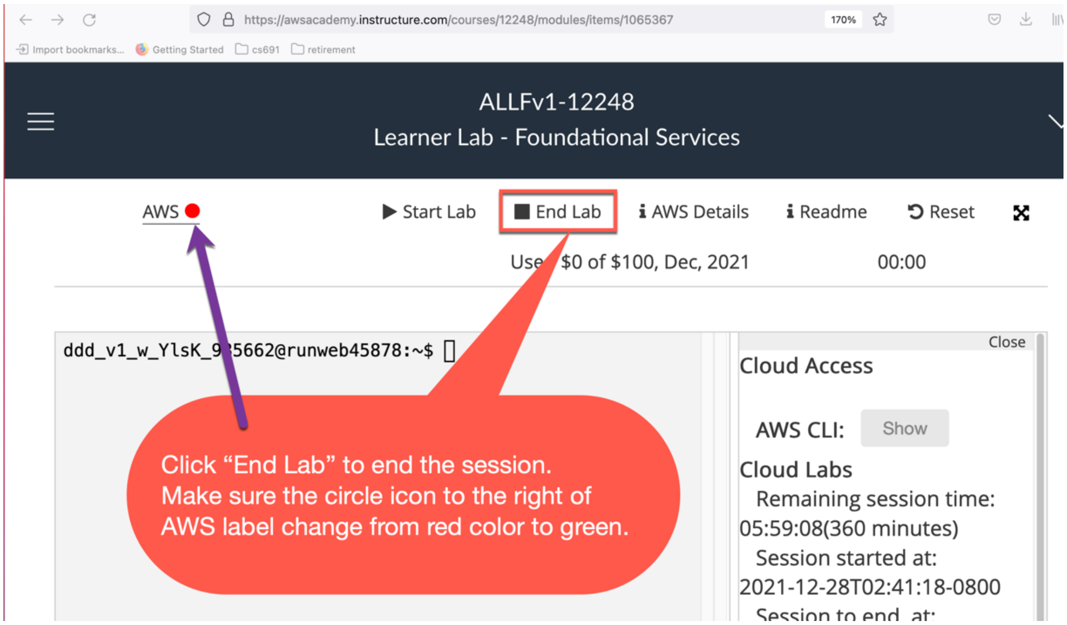
Figure 19b. Choose to access the default web page even with warning.



This is the Apache web server created by for CS5910 Coursera Specialization

Figure 19c. Https access to the default web page with warning.

Make sure you finish your session by clicking the “End Lab”. The results is to shutdown the AWS session. The green icon to the right of “AWS” button will be changed to red color.



Used $0 of $100, Dec, 2021 00:00

```
ddd_v1_w_YlsK_9 5662@runweb45878:~$ 
```

Click “End Lab” to end the session.
Make sure the circle icon to the right of AWS label change from red color to green.

Cloud Access

AWS CLI:

Cloud Labs

Remaining session time: 05:59:08(360 minutes)

Session started at: 2021-12-28T02:41:18-0800

Session to end at: