

First open Instance menu and then press on Launch Instances button

The screenshot shows the AWS Management Console for the us-east-2 region. The left sidebar contains the navigation menu, with 'Instances' highlighted. The top right corner features the 'Launch Instances' button. The main area displays a table of five existing EC2 instances, all in a 'Running' state.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
Public#1	i-01c0aa9aca86f5ae7	Running	t2.micro	2/2 checks passed	No alarms	us-east
Public#2	i-03538ce039e629028	Running	t2.micro	2/2 checks passed	No alarms	us-east
-	i-098199124938054d1	Running	t2.micro	2/2 checks passed	No alarms	us-east
PrivateEC2	i-0a1aba039f4a7610a	Running	t2.micro	2/2 checks passed	No alarms	us-east
Private#1	i-0434a323ee871096c	Running	t2.micro	2/2 checks passed	No alarms	us-east

Search for linux and then choose Amazon Linux 2 AMI option (For Free Accounts). Then press Select Button

The screenshot shows the 'Step 1: Choose an Amazon Machine Image (AMI)' wizard. The search bar contains 'linux'. The 'Amazon Linux 2 AMI (HVM), SSD Volume Type' is selected, and the 'Select' button is highlighted. The 'macOS Big Sur 11.5.2' is also visible as an option.

Step 1: Choose an Amazon Machine Image (AMI)

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

Search by Systems Manager parameter

Quick Start

- My AMIs
- AWS Marketplace
- Community AMIs
- ☐ Free tier only

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-00dfe2c7ce89a450b (64-bit x86) / ami-031dea1a744251b51 (64-bit Arm)

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

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

macOS Big Sur 11.5.2 - ami-0b1674fbc9847f6d

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 second option (t2.micro) which is for free tier. Then press Next Configure Instance Details

Step 2: Choose an Instance Type

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

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

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

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes

Micro instances are eligible for the AWS free usage tier. For the first 12 months following your AWS sign-up date, you get up to 750 hours of micro instances each month. When your free usage tier expires or if your usage exceeds the free tier restrictions, you pay standard, pay-as-you-go service rates. [Learn more](#) about free usage tier eligibility and restrictions.

Buttons: Cancel | Previous | Review and Launch | Next: Configure Instance Details

In this menu we can select vps & subnet. But in this assignment will leave them with default options

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-2b99f140 (default) | Create new VPC

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

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

Placement group: ☐ Add instance to placement group

Capacity Reservation: Open

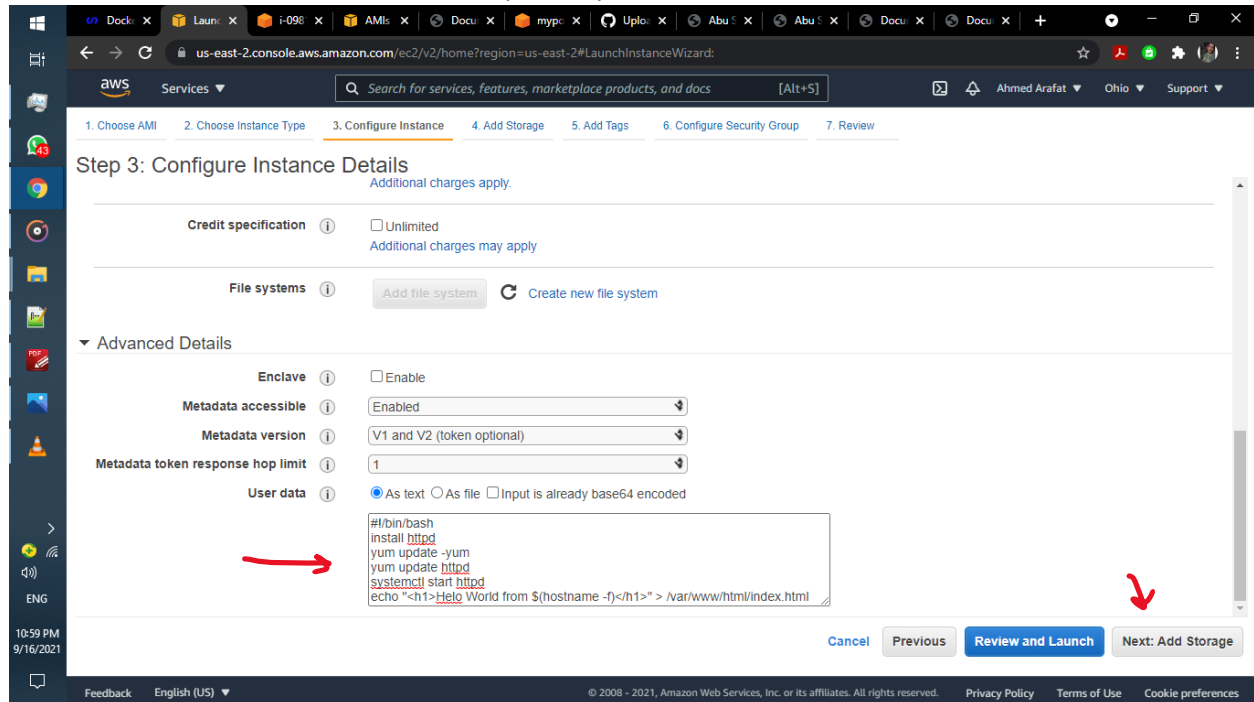
Domain join directory: No directory | Create new directory

IAM role: None | Create new IAM role

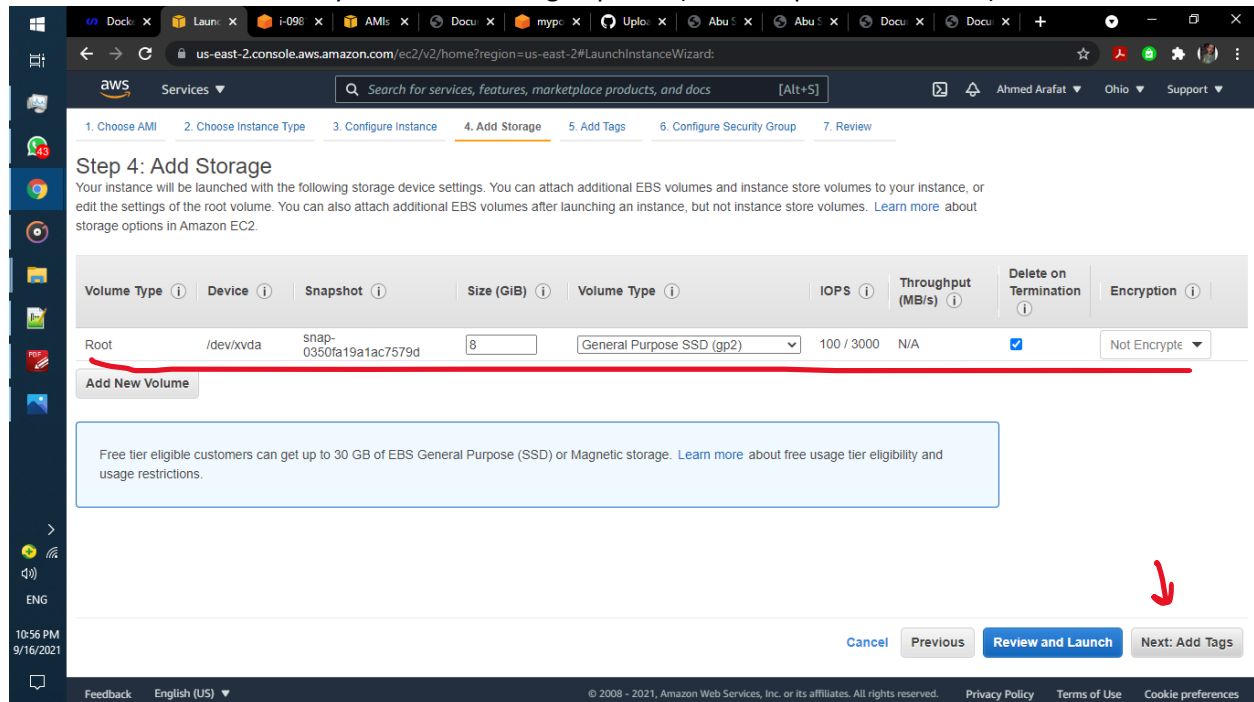
Shutdown behavior: Stop

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

Press down button until user data is shown and paste in textfield code that will be executed when EC2 is created. First to install apache and then update OS software then update apache and then start apache service .Then redirect standard output (<h1></h1>) and save it in index.html {which will be executed automatically when public IP address is used in browser}



Here you can edit storage options (default option is selected)



Add a tag to make EC2 more descriptive

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	Value	Instances	Volumes	Network Interfaces
MyWebsite	Testing My First Hosted Website	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

In Security Group you add http and make it public (0.0.0.0/0), so people can access your website. Then press Review and Launch button

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-6

Description: launch-wizard-6 created 2021-09-16T22:56:45.344+02:00

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

[Add Rule](#)

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

Make sure that options are correct and then hit Launch button

Step 7: Review Instance Launch

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

Improve your instances' security. Your security group, launch-wizard-6, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details [Edit AMI](#)

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-00dfe2c7ce89a450b

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 [Edit 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 [Edit security groups](#)

[Cancel](#) [Previous](#) [Launch](#)

Choose (Create a new pair) option then select RSA radio option and give it a name

Step 7: Review Instance Launch

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

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

AMI Details [Edit AMI](#)

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-00dfe2c7ce89a450b

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 [Edit 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 [Edit security groups](#)

[Cancel](#) [Previous](#) [Launch](#)

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

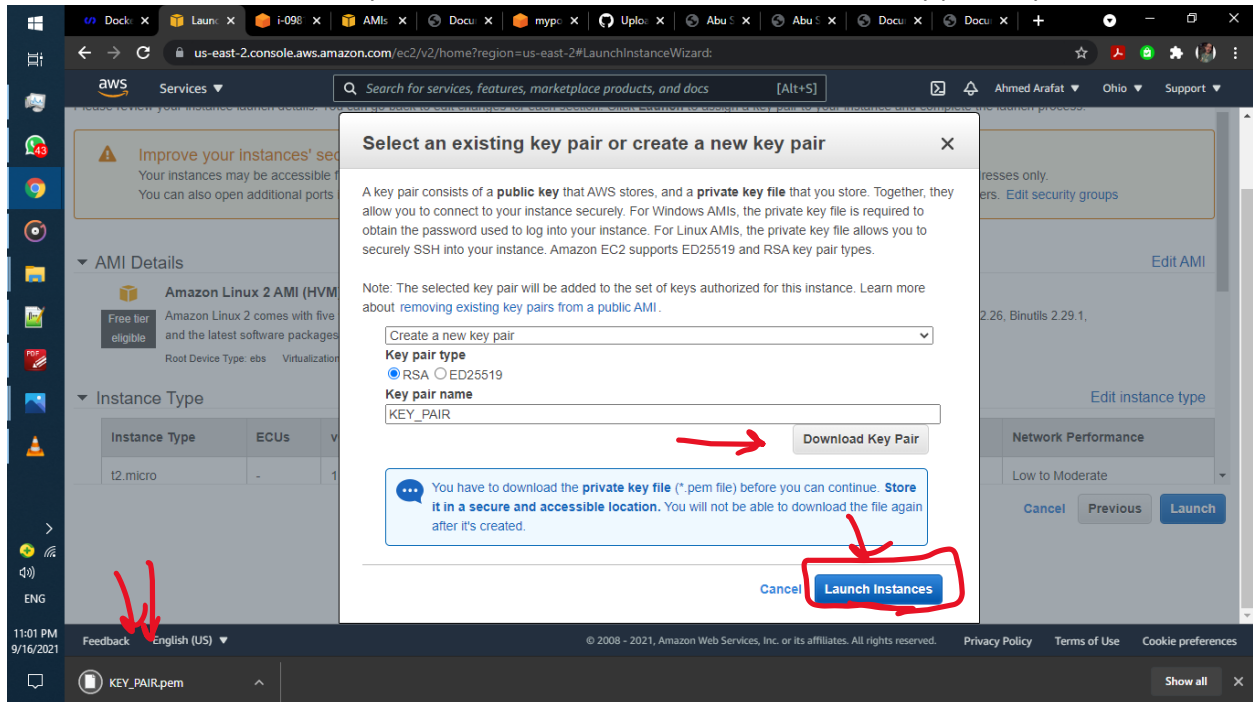
KEY_PAIR

[Download Key Pair](#)

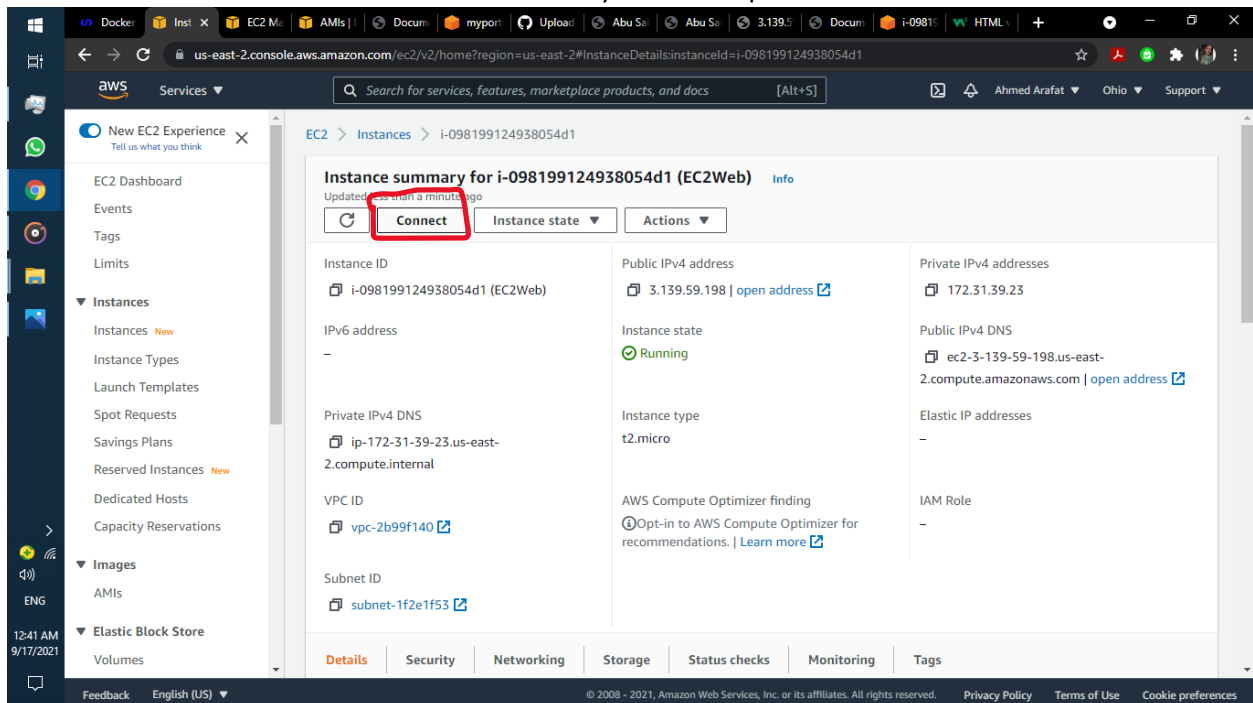
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.

[Cancel](#) [Launch Instances](#)

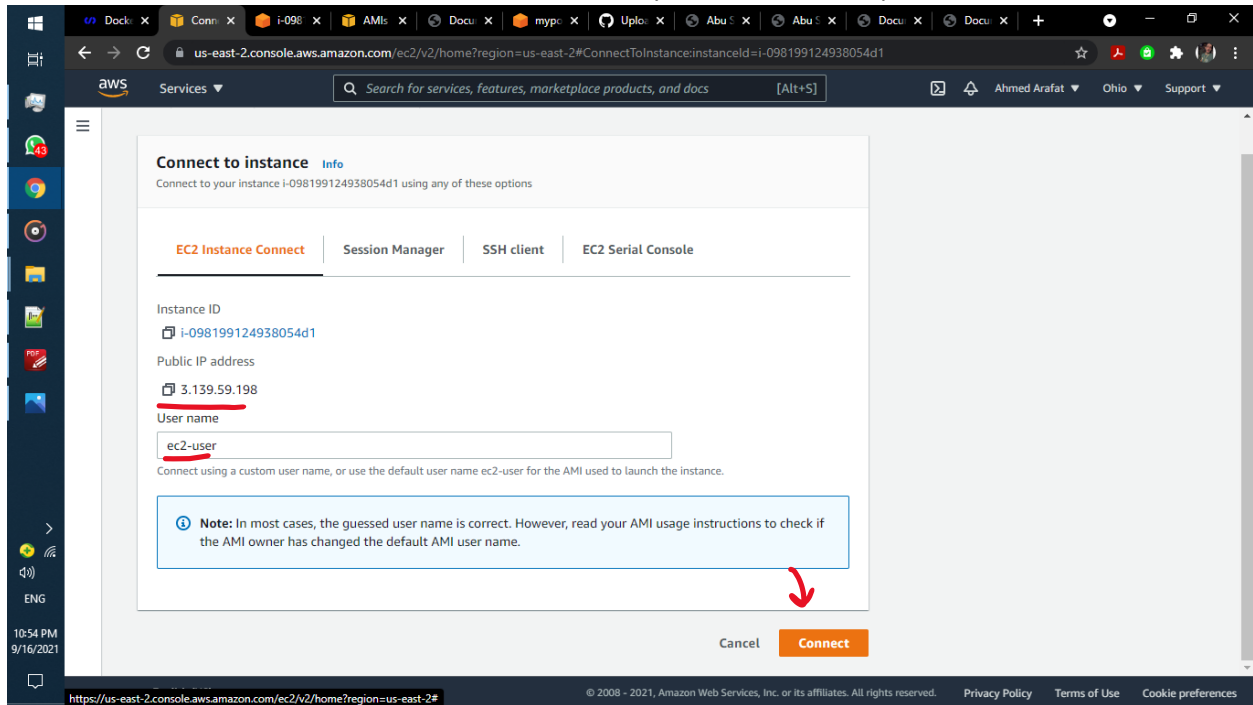
Press Download Key Pair Button to download file that contains key pair on your PC



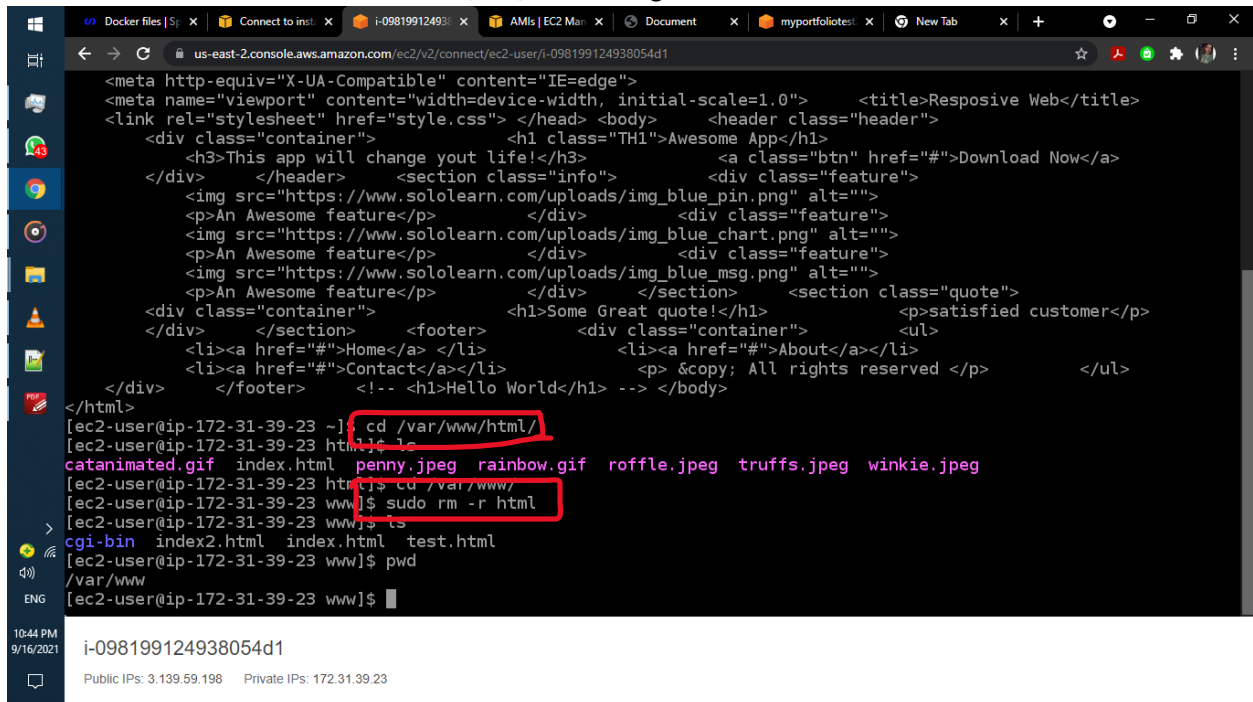
Wait for seconds until instance is ready and then open it. Then hit Connect button



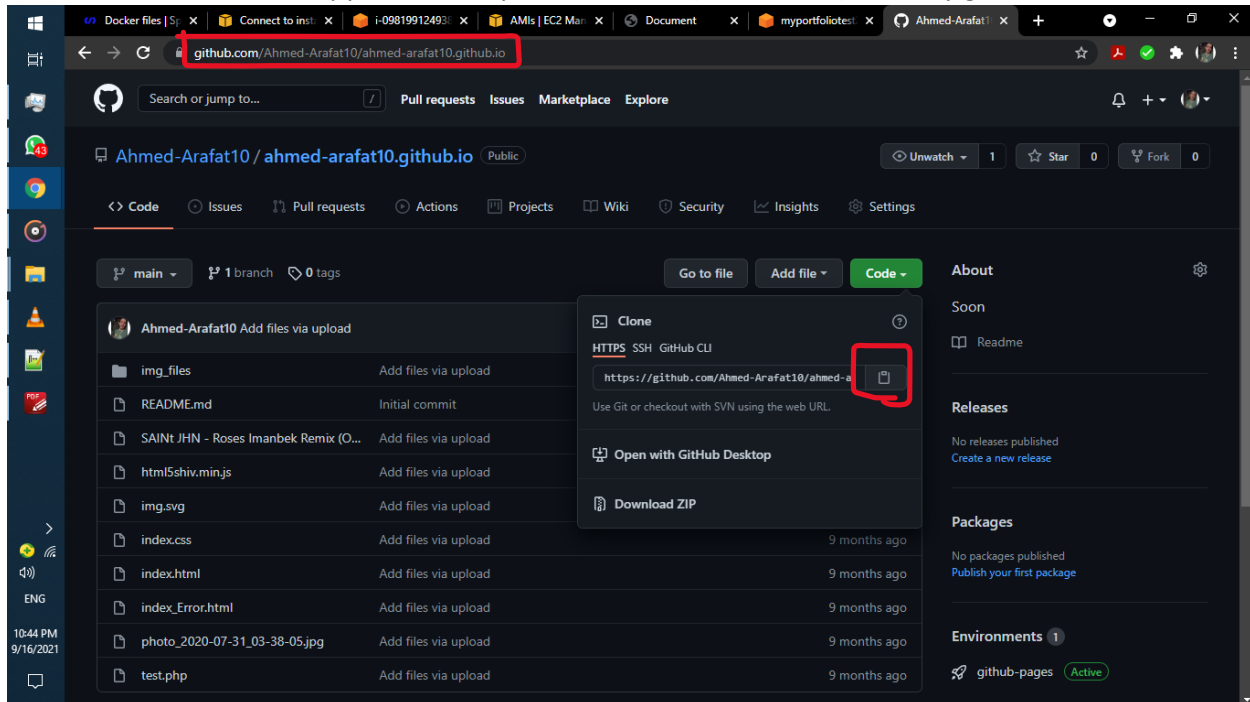
Public IP Address is used as a URL of your website. Then press connect



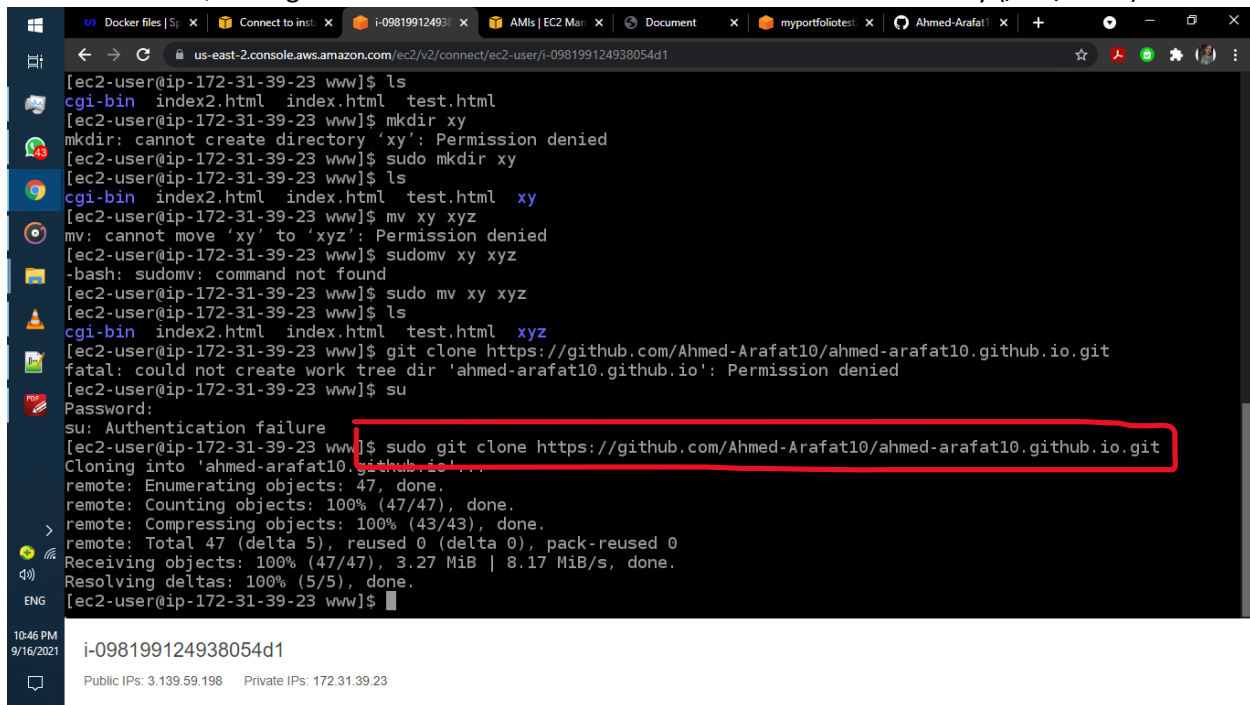
You are now accessing linux server using terminal remotely. What I did here is that I changed directory to /var/www using cd command



Then I copied link of my static website (HTML + CSS) from my github



I used `$ sudo git clone <GithubLink>` to make a clone in current Directory (/var/www)



Then I deleted html Dir. Using (\$ sudo rm -r html/)

```
us-east-2.console.aws.amazon.com/ec2/v2/connect/ec2-user/i-098199124938054d1
[ec2-user@ip-172-31-39-23 www]$ mkdir xy
mkdir: cannot create directory 'xy': Permission denied
[ec2-user@ip-172-31-39-23 www]$ sudo mkdir xy
[ec2-user@ip-172-31-39-23 www]$ ls
cgi-bin  index2.html  index.html  test.html  xy
[ec2-user@ip-172-31-39-23 www]$ mv xy xyz
mv: cannot move 'xy' to 'xyz': Permission denied
[ec2-user@ip-172-31-39-23 www]$ sudo mv xy xyz
-bash: sudo mv: command not found
[ec2-user@ip-172-31-39-23 www]$ sudo mv xy xyz
[ec2-user@ip-172-31-39-23 www]$ ls
cgi-bin  index2.html  index.html  test.html  xyz
[ec2-user@ip-172-31-39-23 www]$ git clone https://github.com/Ahmed-Arafat10/ahmed-arafat10.github.io.git
fatal: could not create work tree dir 'ahmed-arafat10.github.io': Permission denied
[ec2-user@ip-172-31-39-23 www]$ su
Password:
su: Authentication failure
[ec2-user@ip-172-31-39-23 www]$ sudo git clone https://github.com/Ahmed-Arafat10/ahmed-arafat10.github.io.git
Cloning into 'ahmed-arafat10.github.io'...
remote: Enumerating objects: 47, done.
remote: Counting objects: 100% (47/47), done.
remote: Compressing objects: 100% (43/43), done.
remote: Total 47 (delta 5), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (47/47), 3.27 MiB | 8.17 MiB/s, done.
Resolving deltas: 100% (5/5), done.
[ec2-user@ip-172-31-39-23 www]$ ls
ahmed-arafat10.github.io  cgi-bin  index2.html  index.html  test.html  xyz
[ec2-user@ip-172-31-39-23 www]$
```

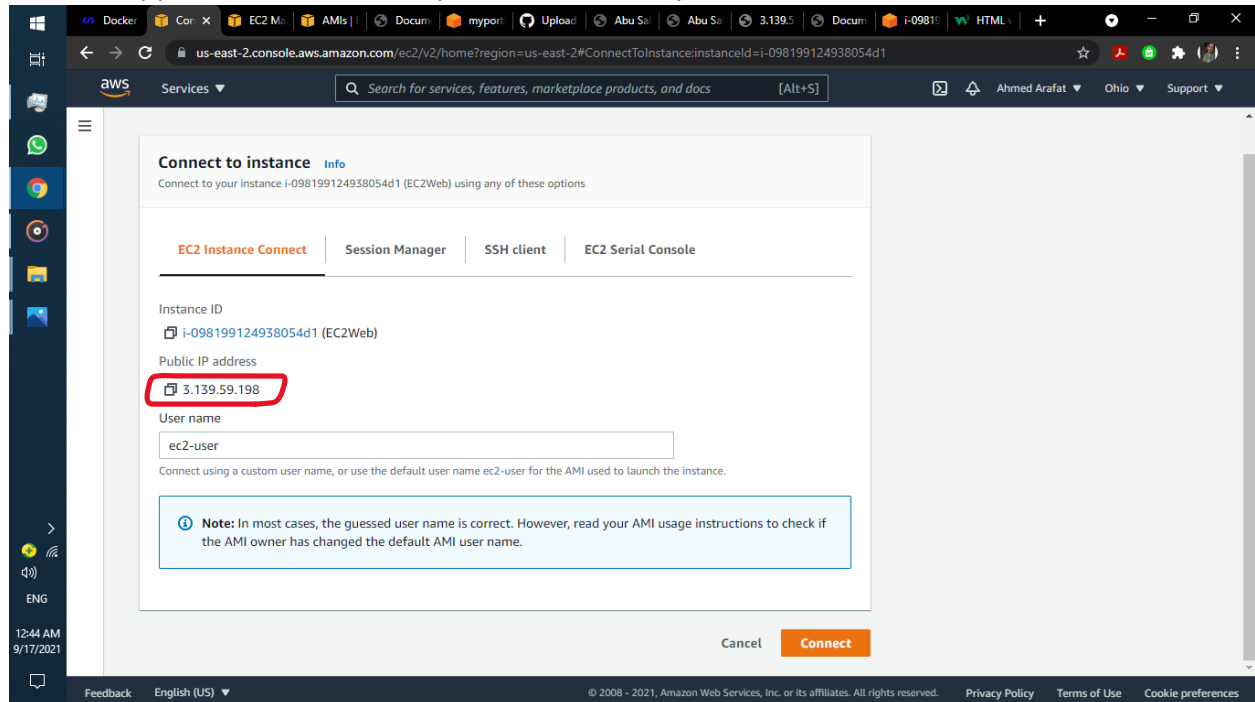
i-098199124938054d1
Public IPs: 3.139.59.198 Private IPs: 172.31.39.23

Then I renamed my gihub repo to html using (\$ sudo mv OldName NewName), So now I have a Directory called html that contains all files of my static website

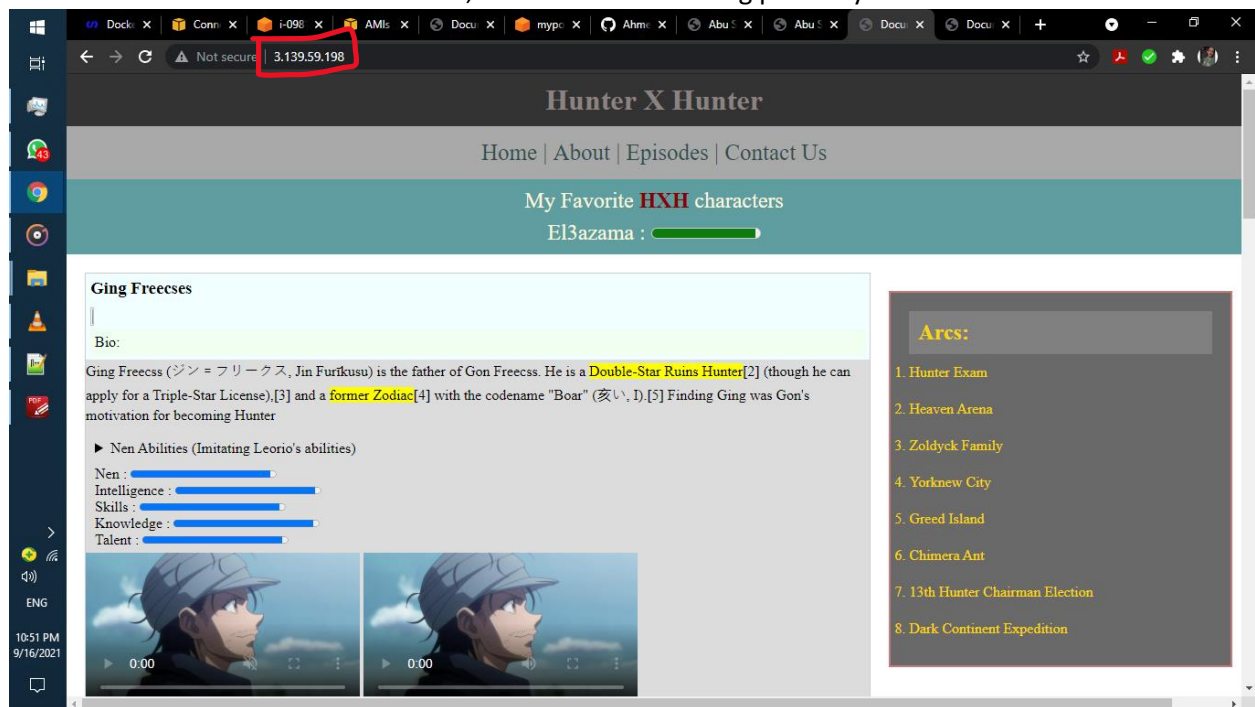
```
us-east-2.console.aws.amazon.com/ec2/v2/connect/ec2-user/i-098199124938054d1
[ec2-user@ip-172-31-39-23 www]$ ls
cgi-bin  index2.html  index.html  test.html  xyz
[ec2-user@ip-172-31-39-23 www]$ git clone https://github.com/Ahmed-Arafat10/ahmed-arafat10.github.io.git
fatal: could not create work tree dir 'ahmed-arafat10.github.io': Permission denied
[ec2-user@ip-172-31-39-23 www]$ su
Password:
su: Authentication failure
[ec2-user@ip-172-31-39-23 www]$ sudo git clone https://github.com/Ahmed-Arafat10/ahmed-arafat10.github.io.git
Cloning into 'ahmed-arafat10.github.io'...
remote: Enumerating objects: 47, done.
remote: Counting objects: 100% (47/47), done.
remote: Compressing objects: 100% (43/43), done.
remote: Total 47 (delta 5), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (47/47), 3.27 MiB | 8.17 MiB/s, done.
Resolving deltas: 100% (5/5), done.
[ec2-user@ip-172-31-39-23 www]$ ls
ahmed-arafat10.github.io  cgi-bin  index2.html  index.html  test.html  xyz
[ec2-user@ip-172-31-39-23 www]$ mv ahmed-arafat10.github.io/ html
mv: cannot move 'ahmed-arafat10.github.io/' to 'html': Permission denied
[ec2-user@ip-172-31-39-23 www]$ sudo mv ahmed-arafat10.github.io/ html
[ec2-user@ip-172-31-39-23 www]$ ls
cgi-bin  html  index2.html  index.html  test.html  xyz
[ec2-user@ip-172-31-39-23 www]$ cd html
[ec2-user@ip-172-31-39-23 html]$ ls
html5shiv.min.js  index.css  photo_2020-07-31_03-38-05.jpg  test.php
img_files         index_Error.html  README.md
img.svg           index.html        SAINT JHN - Roses Imanbek Remix (Official Audio).mp3
[ec2-user@ip-172-31-39-23 html]$
```

i-098199124938054d1
Public IPs: 3.139.59.198 Private IPs: 172.31.39.23

Copy Public IP Address and paste it in browser (you can also add :80 to end of IP Address)



Booom, The website is working perfectly <3



Extra: If you want to change security configuration for an instance later go to Network & Security > Security Groups. Then press on Security group ID you want to edit

The screenshot shows the AWS Management Console interface. On the left sidebar, the 'Network & Security' menu item is highlighted with a red box, and the 'Security Groups' sub-item is also highlighted. The main content area displays a table of Security Groups. A red arrow points to the 'sg-050c67fec52ec92b9' security group ID in the table.

Name	Security group ID	Security group name	VPC ID	Description
-	sg-050c67fec52ec92b9	launch-wizard-1	vpc-2b99f140	launch-wizard-1
-	sg-07e5ed739ebe2f803	default	vpc-05ce3d5ab6c0b3608	default VPC secu
-	sg-0ad52aaeb87f9cdcc	launch-wizard-2	vpc-05ce3d5ab6c0b3608	launch-wizard-2
-	sg-0baaa089ec896be43	launch-wizard-4	vpc-05ce3d5ab6c0b3608	launch-wizard-4
-	sg-0baf6811c578c9220	launch-wizard-3	vpc-05ce3d5ab6c0b3608	launch-wizard-3
-	sg-0cb33b414efff59f0	launch-wizard-5	vpc-05ce3d5ab6c0b3608	launch-wizard-5
-	sg-f4a293be	default	vpc-2b99f140	default VPC secu

Then press on Edit inbound rules. Then add security configurations as you want

The screenshot shows the 'Edit inbound rules' page for the security group 'sg-050c67fec52ec92b9'. The 'Inbound rules' tab is selected. A red box highlights the 'Edit inbound rules' button. The page displays a table of inbound rules.

Name	Security group rule...	IP version	Type	Protocol
-	sgr-0cc4b81164454f501	IPv4	SSH	TCP
-	sgr-045b353a2f4ad3d3a	IPv4	HTTP	TCP
-	sgr-07db5e0e135f74466	IPv6	HTTP	TCP
-	sgr-0babba862d9610f...	IPv4	HTTPS	TCP