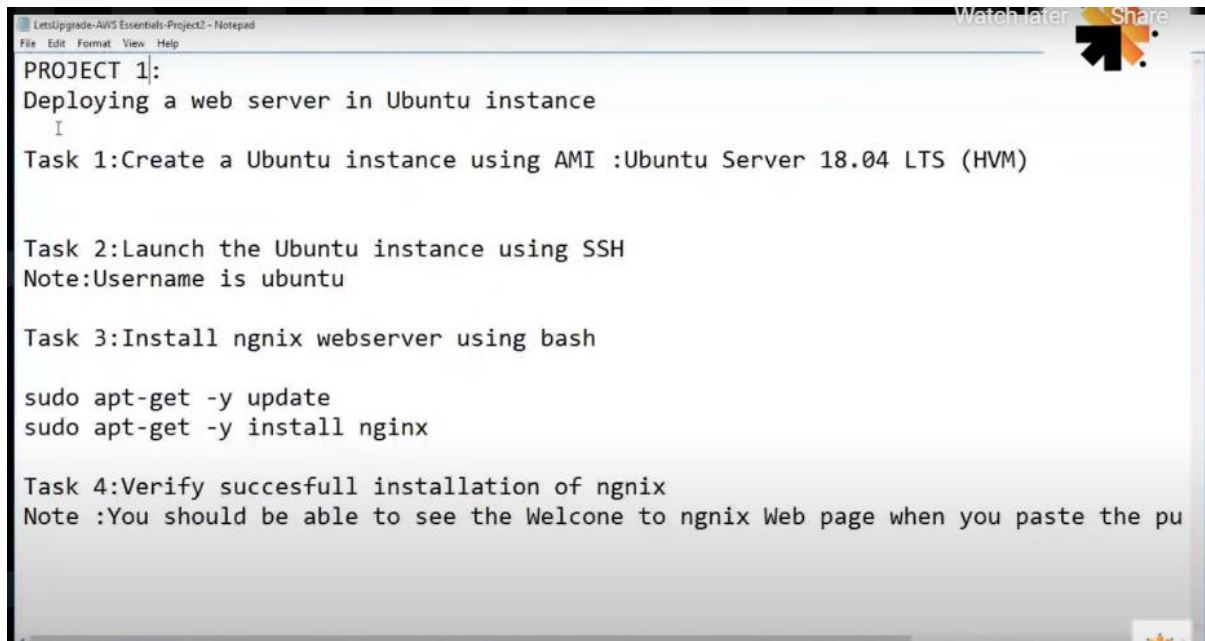


Assignment

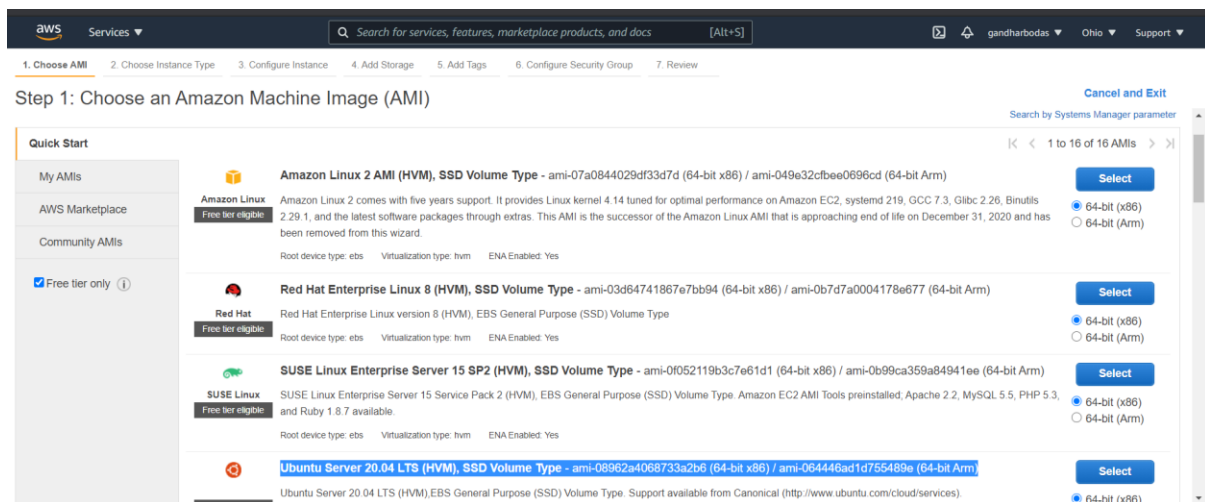
Day 2: Assignment 1:



```
PROJECT 1:  
Deploying a web server in Ubuntu instance  
  
Task 1: Create a Ubuntu instance using AMI :Ubuntu Server 18.04 LTS (HVM)  
  
Task 2: Launch the Ubuntu instance using SSH  
Note: Username is ubuntu  
  
Task 3: Install nginx webserver using bash  
  
sudo apt-get -y update  
sudo apt-get -y install nginx  
  
Task 4: Verify successful installation of nginx  
Note: You should be able to see the Welcome to nginx Web page when you paste the pu
```

Answer:

Step 1:



Click on select button then next page open:

Step 2:

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

Step 2: Choose an Instance Type

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

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

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

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

Selected Type: t2.micro (Free tier eligible) and then clicked on Next: configuration instance details.

Step 3:

RWS Services Search for services, features, marketplace products, and docs [Alt+S] gandharbadas Ohio Support

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

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances 1 Launch into Auto Scaling Group

Purchasing option ☐ Request Spot Instances

Network vpc-51129e3a (default) Create new VPC

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

Auto-assign Public IP Enable

Placement group ☐ Add instance to placement group

Capacity Reservation Open

Domain join directory No directory Create new directory

IAM role None Create new IAM role

CPU options ☐ Specify CPU options

Shutdown behavior Stop

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

Enable termination protection ☒ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
Additional charges apply.

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

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)

Cancel Previous Review and Launch Next: Add Storage

Later on click on Next: Add Storage button.

Step 4:

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

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption ⓘ
Root	/dev/sda1	snap-08d55512ce962b5e5	8	General Purpose SSD (gp2) ▾	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted ▾

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Keep setting as it is and click on Next: Add Tags button.

Step 5:

Add tag :

← → ↻ us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard: Google Welcome to HDFC... State Bank of India... Job Related Official... English Database Entertainment Linux & Shell Script... Openings DevOps & Other LetsUpgrade Online Marathi

aws Services Search for services, features, marketplace products, and docs [Alt+S] gandharbodas Ohio ▾

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

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ	Network Interfaces ⓘ
Name5	Ins5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

Later on, clicked on Next: Configuration Security Group button.

Step 6:

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere 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

Later on, clicked on Review and Launch button.

Step 7:

aws Services

Search for services, features, marketplace products, and docs [Alt+S]

gandharbodas Ohio Support

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. Review

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, Group8, 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

Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-08962a4068733a2b6

Free tier eligible

Ubuntu Server 20.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).
Root Device Type: ebs Virtualization type: hvm

Edit AMI

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

Edit instance type

Security Groups

Security group name Group8

Edit security groups

Cancel

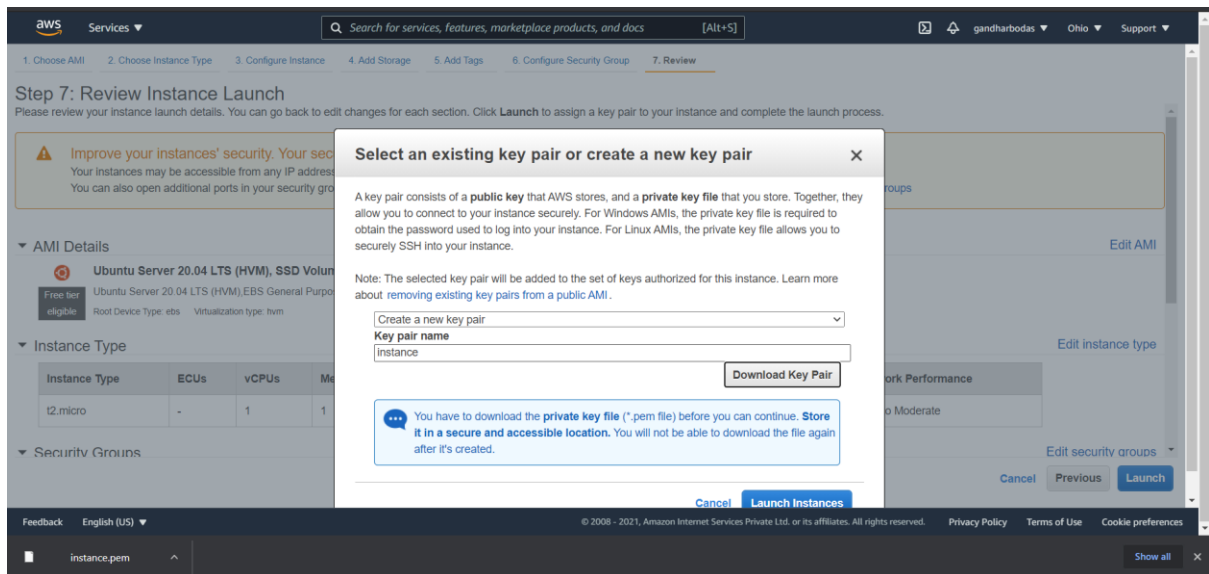
Previous

Launch

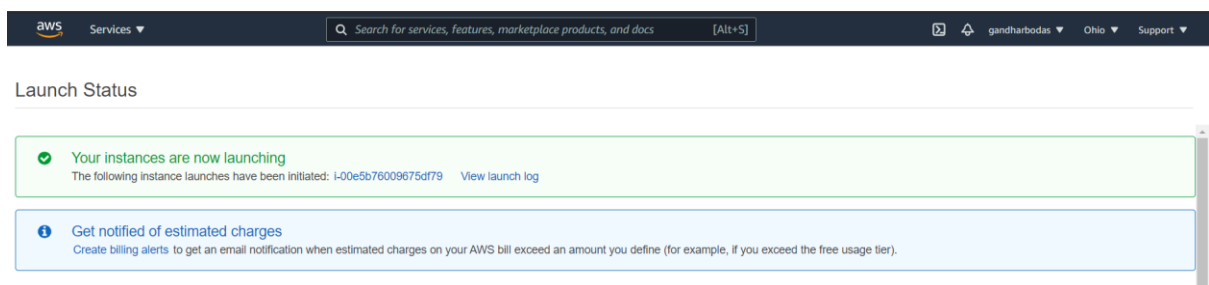
Then clicked on Launch button.

Step 8:

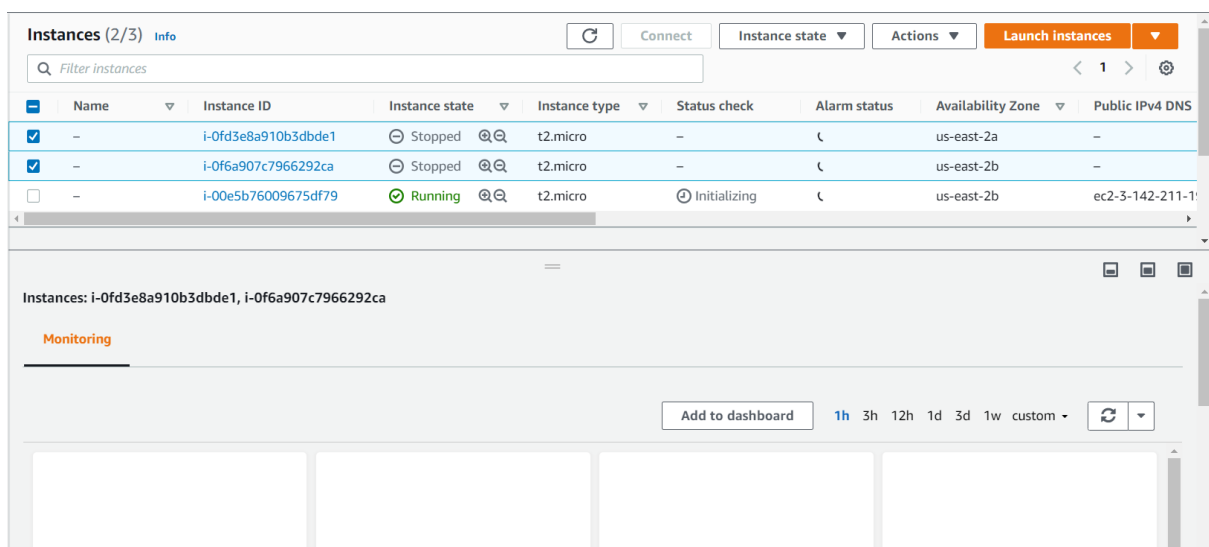
Create a new key pair and key pair name: instance. Then download key pair.



Now click on “Launch Instances” button.



Now click on “View Instances” button.



Now click on newly created instance and then click on connect button as below:

Instance summary for i-00e5b76009675df79 [info](#)

Updated less than a minute ago

Instance ID i-00e5b76009675df79	Public IPv4 address 3.142.211.196 open address	Private IPv4 addresses 172.31.27.37
Instance state Running	Public IPv4 DNS ec2-3-142-211-196.us-east-2.compute.amazonaws.com open address	Private IPv4 DNS ip-172-31-27-37.us-east-2.compute.internal
Instance type t2.micro	Elastic IP addresses -	VPC ID vpc-51129e3a
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	IAM Role -	Subnet ID subnet-57fc112a

[Details](#) [Security](#) [Networking](#) [Storage](#) [Status checks](#) [Monitoring](#) [Tags](#)

[Instance details](#) [info](#)

Connect to instance [info](#)

Connect to your instance i-00e5b76009675df79 using any of these options

[EC2 Instance Connect](#) [Session Manager](#) [SSH client](#)

Instance ID
i-00e5b76009675df79

Public IP address
3.142.211.196

User name

Connect using a custom user name, or use the default user name ubuntu for the AMI used to launch the instance.

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

[Cancel](#) [Connect](#)

Once clicked on Connect Button then fire a below commands:

```
sudo apt-get -y update
```

```
sudo apt-get -y install nginx
```

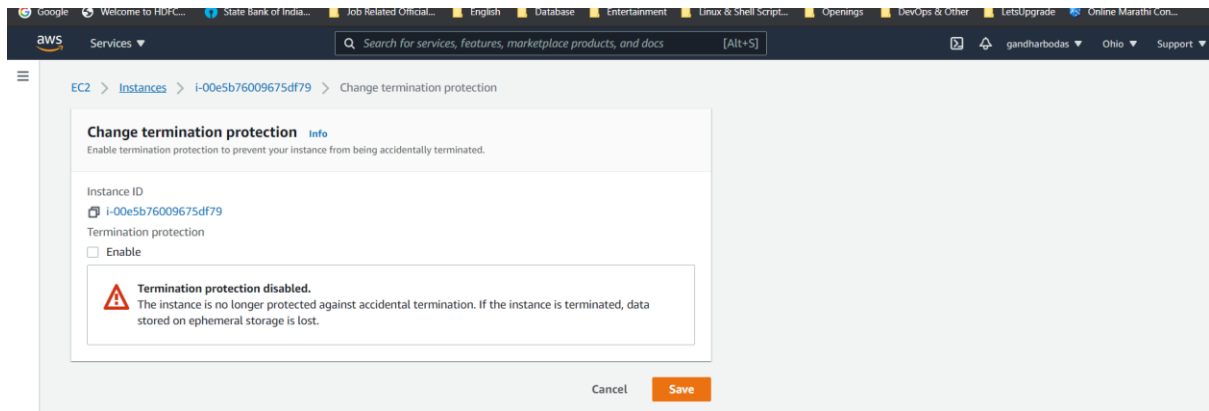
```
Get:12 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [204 kB]
Get:13 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [12.8 kB]
Get:14 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [163 kB]
Get:15 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [24.3 kB]
Get:16 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f Metadata [436 B]
Get:17 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [751 kB]
Get:18 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [157 kB]
Get:19 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [16.3 kB]
Get:20 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [21.6 kB]
Get:21 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/multiverse Translation-en [5508 B]
Get:22 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 c-n-f Metadata [596 B]
Get:23 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-backports/main amd64 c-n-f Metadata [112 B]
Get:24 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-backports/restricted amd64 c-n-f Metadata [116 B]
Get:25 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-backports/universe amd64 Packages [4032 B]
Get:26 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-backports/universe Translation-en [1448 B]
Get:27 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-backports/universe amd64 c-n-f Metadata [224 B]
Get:28 http://us-east-2.ec2.archive.ubuntu.com/ubuntu focal-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:29 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [548 kB]
Get:30 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [117 kB]
Get:31 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [7352 B]
Get:32 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [140 kB]
Get:33 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [20.6 kB]
Get:34 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [392 B]
Get:35 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [550 kB]
Get:36 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [80.7 kB]
Get:37 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [10.6 kB]
Get:38 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [14.8 kB]
Get:39 http://security.ubuntu.com/ubuntu focal-security/multiverse Translation-en [3160 B]
Get:40 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [340 B]
Fetched 18.3 MB in 3s (5642 kB/s)
Reading package lists... Done
```

```
Reading package lists... Done
ubuntu@ip-172-31-27-37:~$
ubuntu@ip-172-31-27-37:~$ sudo apt-get -y install nginx
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package nginx
ubuntu@ip-172-31-27-37:~$
```

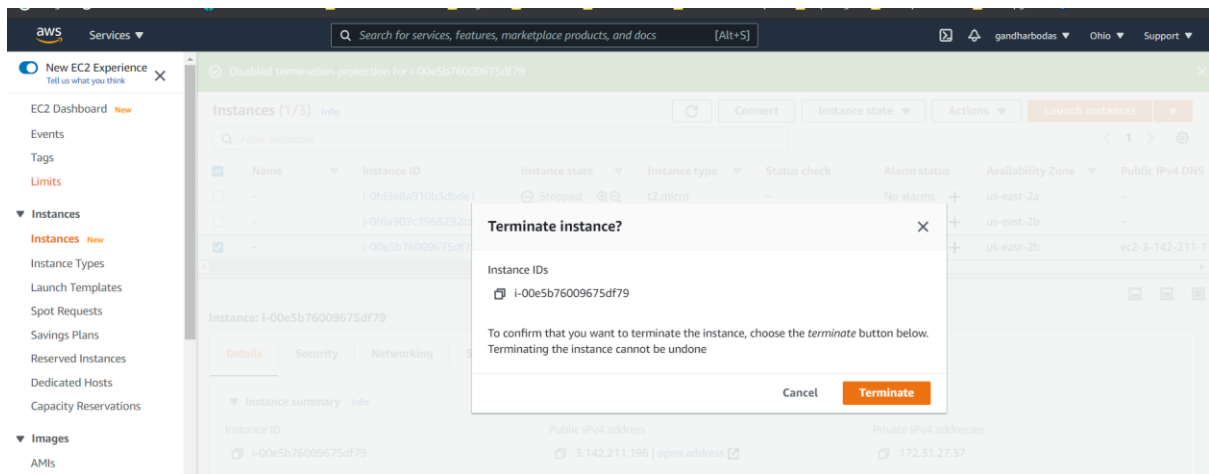
Step 9: Un-enable and terminate this instance:

The screenshot shows the AWS Management Console interface. At the top, there is a search bar and navigation links. A red error banner at the top states: "Failed to terminate the Instance i-00e5b76009675df79. The instance i-00e5b76009675df79 may not be terminated. Modify its 'disableApiTermination' instance attribute and try again." Below the error, the "Instances" page is displayed for the instance ID i-00e5b76009675df79. The instance summary shows it is a t2.micro instance in the "Running" state. The public IPv4 address is 3.142.211.196, and the private IPv4 address is 172.31.27.37. The instance type is t2.micro, and the IAM role is empty. The VPC ID is vpc-51129e3a, and the subnet ID is subnet-57fc112a.

So, for this go to the main page -> Actions->Instance Settings->Change termination protection->Un-check "Enable" option ->and click on Save button.



Now, click on Instance state-> Terminate instances



END