

ASSIGNMENT – 4

Cloud Computing Practical Assignment No 4
Working and Implementation of Infrastructure as
a service

Task 1: Launch Your Amazon EC2 Instance.

Write the shell script in User Data box. The script will: • Install an Apache web server (httpd) • Configure the web server to automatically start on boot • Run the Web server once it has finished installing • Create a simple web page

Task 2: Monitor Your Instance

Task 3: Update Your Security Group and Access the Web Server Task

4: Resize Your Instance: Instance Type and EBS Volume

Task 5: Test Termination Protection

Task 1: Launch Your Amazon EC2 Instance

1. Open EC2 Console:

- Go to AWS Management Console, choose Services, then Compute, and select EC2.
- Ensure the region is set to N. Virginia (us-east-1).

2. Launch Instance:

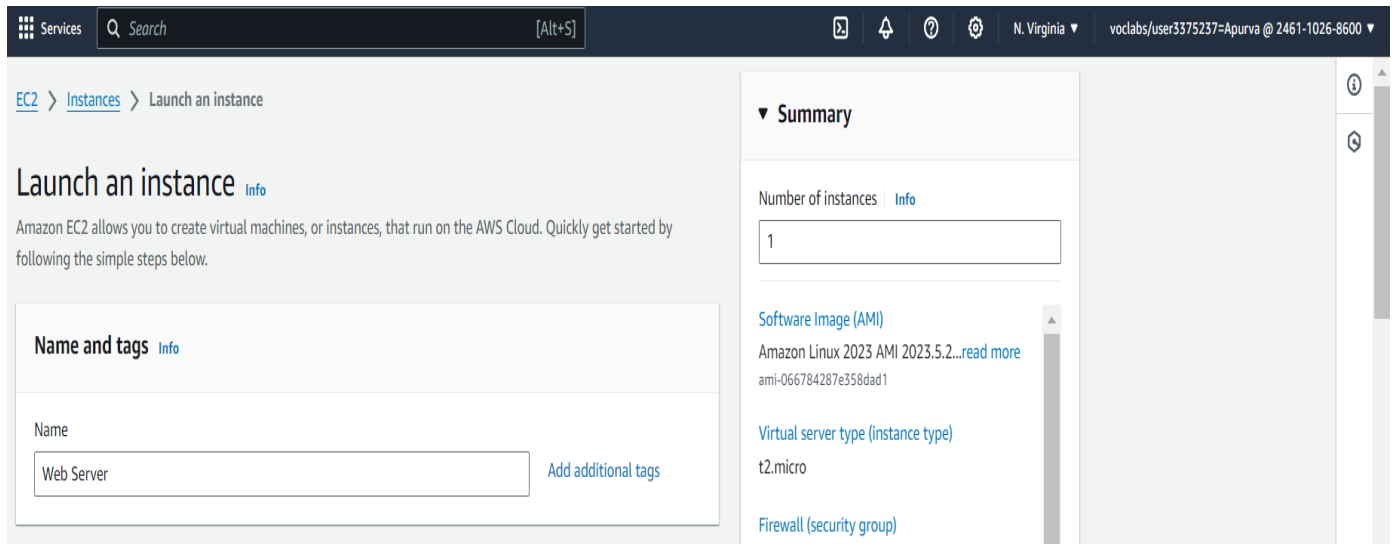
- Click Launch instance, then choose Launch instance.

The screenshot displays the AWS Management Console for the EC2 service in the N. Virginia region. The top navigation bar shows the user is logged in as 'voclabs/user3375237=Apurva' with a session ID of '2461-1026-8600'. The main content area is divided into several sections:

- Resource Summary:** A table showing the number of EC2 resources in the US East (N. Virginia) Region. The resources and their counts are: Instances (running) 0, Auto Scaling Groups 0, Capacity Reservations 0, Dedicated Hosts 0, Elastic IPs 1, Instances 1, Key pairs 8, Load balancers 0, Placement groups 0, Security groups 15, Snapshots 0, and Volumes 1.
- Default VPC:** A section showing the default VPC for the region, with ID 'vpc-0ca9c2c02fd652798'. It includes links to settings, data protection and security, zones, EC2 Serial Console, default credit specification, and EC2 console preferences.
- Launch instance:** A section with a description: 'To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.' It features a prominent orange 'Launch instance' button and a 'Migrate a server' link.
- Service health:** A section showing the status of the EC2 service. It indicates the region is 'US East (N. Virginia)' and the status is 'This service is operating normally.' There is a link to the 'AWS Health Dashboard'.
- Explore AWS:** A section with a close button and two promotional cards. The first card is titled 'Save up to 90% on EC2 with Spot Instances' and describes how to optimize price-performance by combining EC2 purchase options in a single EC2 ASG. The second card is titled '10 Things You Can Do Today to Reduce AWS Costs' and encourages exploring ways to effectively manage AWS costs.

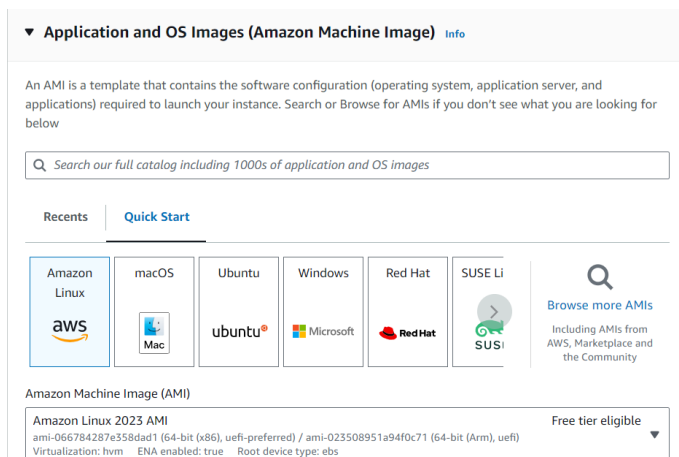
3. Name and Tags:

- Name the instance Web Server (this will create a tag with the key `Name` and value `Web Server`).



4. Select AMI:

- In Application and OS Images (AMI), keep the default Amazon Linux 2023 AMI selected.



5. Select Instance Type:

- In Instance type, keep the default t2.micro selected.

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

☒ All generations
[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

6. Configure Key Pair:

- In Key pair (login), select radhey as the key pair.

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

radhey

[Create new key pair](#)

7. Network Settings:

- Under Firewall (security groups), select Create security group.

- Name it Web Server security group with a description Security group for my web server.
- Remove any default inbound rules.

8. Configure Storage:

- In Configure storage, keep the default 8 GiB disk volume.

9. Advanced Details:

- Expand Advanced details.
- Enable Termination protection.



- Copy and paste the following script in the User data box:


```
#!/bin/bash  
  
dnf install -y httpd  
  
systemctl enable httpd
```

```
systemctl start httpd
```

```
echo '<html><h1>Hello From Your Web  
Server!</h1></html>' >  
/var/www/html/index.html
```

User data - optional [Info](#)

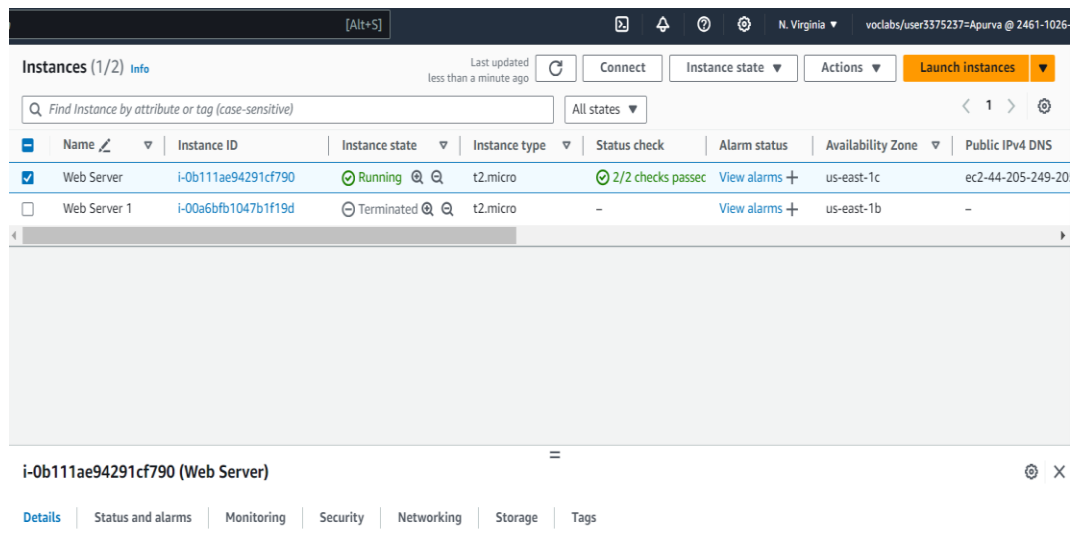
Upload a file with your user data or enter it in the field.

 Choose file

```
#!/bin/bash  
dnf install -y httpd  
systemctl enable httpd  
systemctl start httpd  
echo '<html><h1>Hello From Your Web Server!</h1></html>' >  
/var/www/html/index.html
```

10. Launch Instance:

- Scroll down and click Launch instance.
- Once launched, click View all instances and select Web Server.
- Wait until the instance state is Running with 2/2 status checks passed.



| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS |
|--------------|---------------------|----------------|---------------|-------------------|--------------|-------------------|-------------------|
| Web Server | i-0b111ae94291cf790 | Running | t2.micro | 2/2 checks passed | View alarms | us-east-1c | ec2-44-205-249-20 |
| Web Server 1 | i-00a6bfb1047b1f19d | Terminated | t2.micro | - | View alarms | us-east-1b | - |

i-0b111ae94291cf790 (Web Server)

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

▼ Instance summary Info

Instance ID
i-0b111ae94291cf790 (Web Server)

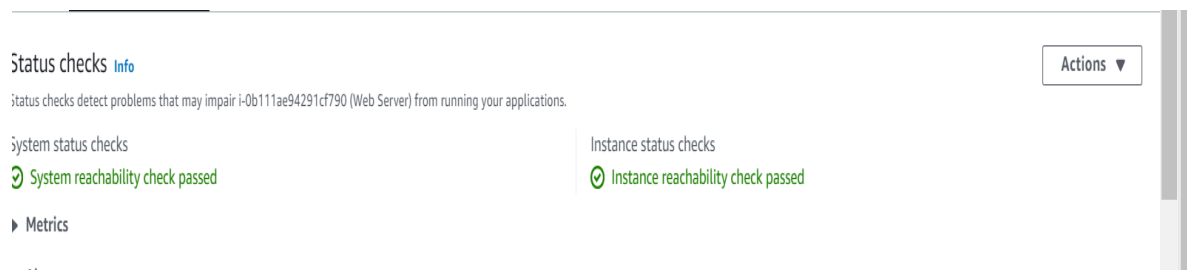
Public IPv4 address copied
44.205.249.205 | [open address](#)

Private IPv4 addresses
172.31.88.39

Task 2: Monitor Your Instance

1. Status Checks:

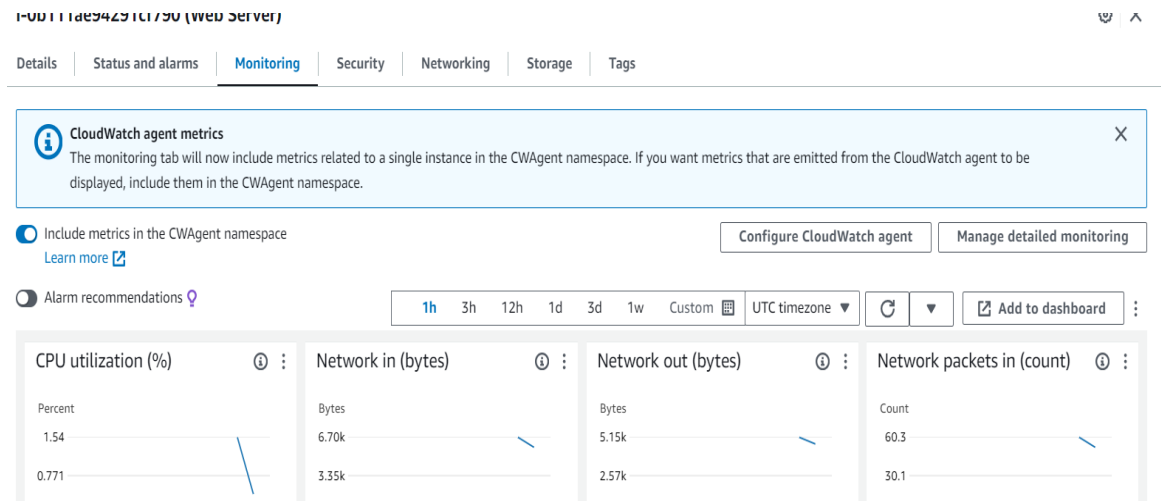
- Select the Status checks tab to verify that System reachability and Instance reachability checks have passed.



| Status checks Info | | Actions |
|--|------------------------------------|---------|
| Status checks detect problems that may impair i-0b111ae94291cf790 (Web Server) from running your applications. | | |
| System status checks | Instance status checks | |
| System reachability check passed | Instance reachability check passed | |
| Metrics | | |

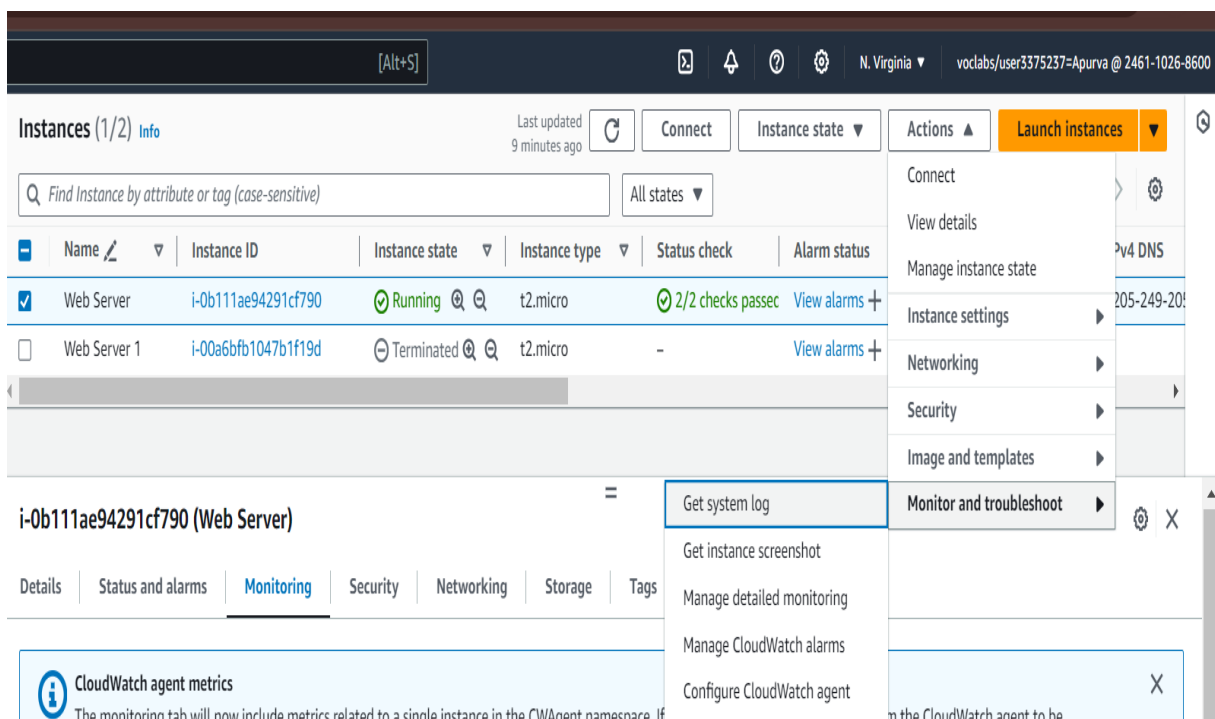
2. Monitoring:

- Select the Monitoring tab to view Amazon CloudWatch metrics for your instance.



3. System Log:




- In the Actions menu, select Monitor and troubleshoot > Get system log.
- Scroll through the output to confirm that the HTTP package was installed.



Get system log [Info](#)

When you experience issues with your EC2 instance, reviewing system logs can help you pinpoint the cause.

System log





  Copy log  Download

Review system log for instance i-0b111ae94291cf790 as of Fri Aug 30 2024 18:49:51 GMT+0530 (India Standard Time)



```
[ 34.539978] cloud-init[2214]: Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service â†’ /usr/lib/systemd/system/httpd.service
[ 34.598211] zram_generator::config[3697]: zram0: system has too much memory (949MB), limit is 800MB, ignoring.
ci-info: +-----+Authorized keys from /home/ec2-user/.ssh/authorized_keys for user ec2-user+-----+
ci-info: | Keytype |                               Fingerprint (sha256)                               | Options | Comment |
ci-info: +-----+-----+-----+-----+-----+-----+-----+-----+-----+
ci-info: | ssh-rsa | a3:12:fb:1e:2f:48:6f:ad:3d:8f:52:3e:9b:a7:79:b0:ae:43:7b:52:25:86:bc:0d:20:e4:7e:96:f6:0f:d9:0f | - | radhey |
ci-info: +-----+-----+-----+-----+-----+-----+-----+-----+-----+
<14>Aug 30 13:07:52 cloud-init: #####
<14>Aug 30 13:07:52 cloud-init: ----BEGIN SSH HOST KEY FINGERPRINTS-----
<14>Aug 30 13:07:52 cloud-init: 256 SHA256:KNluFf+5JBcsuH7ys9l3fC8z9YxYs$5KzmX7PU+HsC8 root@ip-172-31-88-39.ec2.internal (ECDSA)
<14>Aug 30 13:07:52 cloud-init: 256 SHA256:N780FR7E0rrI56MHfb8EXZhbofgrDj56Xo6wD03taIA root@ip-172-31-88-39.ec2.internal (ED25519)
<14>Aug 30 13:07:52 cloud-init: ----END SSH HOST KEY FINGERPRINTS-----
<14>Aug 30 13:07:52 cloud-init: #####
----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMAef3Mut2NnSPX3dK3sXVdGGo+Dcuag/OpzNC+kR5x01RH4UGtVQdBnZXCffJcZxYdNoQbnaH0e
ssh-ed25519 AAAAC3NzaC1lZD11NTE5AAAAIAW7jjwQM6TzYHg2401js8y9NcvjiuRoQ57v5zcPhjm root@ip-172-31-88-39.ec2.internal
----END SSH HOST KEY KEYS-----
[ 35.388176] cloud-init[2214]: Cloud-init v. 22.2.2 finished at Fri, 30 Aug 2024 13:07:52 +0000. Datasource DataSourceEc2. Up 35.37 seconds
```


4. Instance Screenshot:


- In the Actions menu, select Monitor and troubleshoot > Get instance screenshot to view the instance console.


[Alt+S]     N. Virginia voclabs/user3375237=Apurva @ 2461-1026-8600

instances (1/2) [Info](#)


Last updated 1 minute ago   Connect

Instance state 

Actions 

Launch instances 

Find Instance by attribute or tag (case-sensitive)

All states 

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|---------------------------------|-------------|----------------|---------------|--------------|--------------|
| -0b111ae94291cf790 (Web Server) | | | | | |

Get system log

Get instance screenshot

Connect

View details

Manage instance state

Instance settings

Networking

Security

Image and templates

Monitor and troubleshoot

Pv4 DNS

Task 3: Update Your Security Group and Access the Web Server

1. Copy Public IP:

- In the Details tab, copy the instance's Public IPv4 address.

2. Test Web Server Access:

- Open a new browser tab, paste the copied IP, and press Enter.
- Confirm that you cannot access the server yet.

3. Update Security Group:

- Go back to the EC2 Console, choose Security Groups in the left pane.
- Select Web Server security group.
- In the Inbound rules tab, click Edit inbound rules.
- Add a rule:

- Type:HTTP
- Source: Anywhere-IPv4
- Save the rules.

EC2 > Security Groups > sg-0af9fc40ee4557bb4 - Web Security Group > Edit inbound rules

Edit inbound rules [Info](#)

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

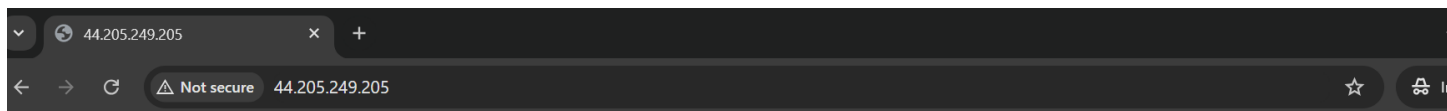
| Security group rule ID | Type Info | Protocol Info | Port range Info | Source Info | Description - optional Info |
|------------------------|---------------------------|-------------------------------|---------------------------------|---|---|
| sg-r-0e46cbc88cf256b77 | HTTP | TCP | 80 | Custom <input type="text" value="0.0.0.0/0"/> | Security group for my web serve |
| sg-r-07d17010e3d85be85 | SSH | TCP | 22 | Custom <input type="text" value="0.0.0.0/0"/> | |

[Add rule](#)

[Cancel](#) [Preview changes](#)

4. Access Web Server:

- Return to the web server tab in your browser and refresh the page.
- You should now see the message "Hello From Your Web Server!".

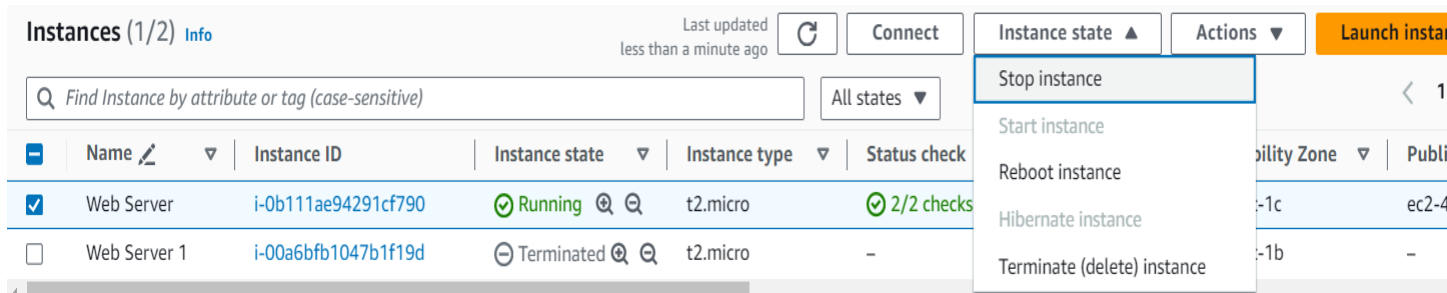


Hello From Your Web Server!

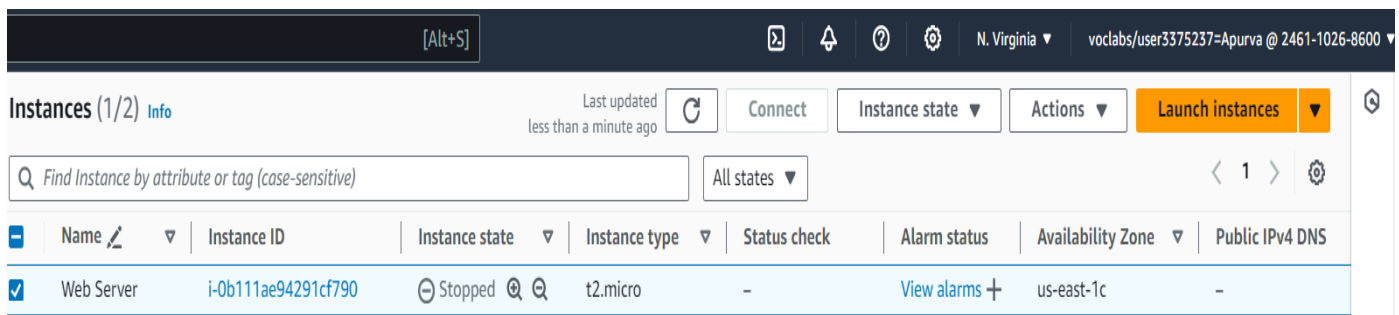
Task 4: Resize Your Instance: Instance Type and EBS Volume

1. Stop the Instance:

- Select the Web Server instance.

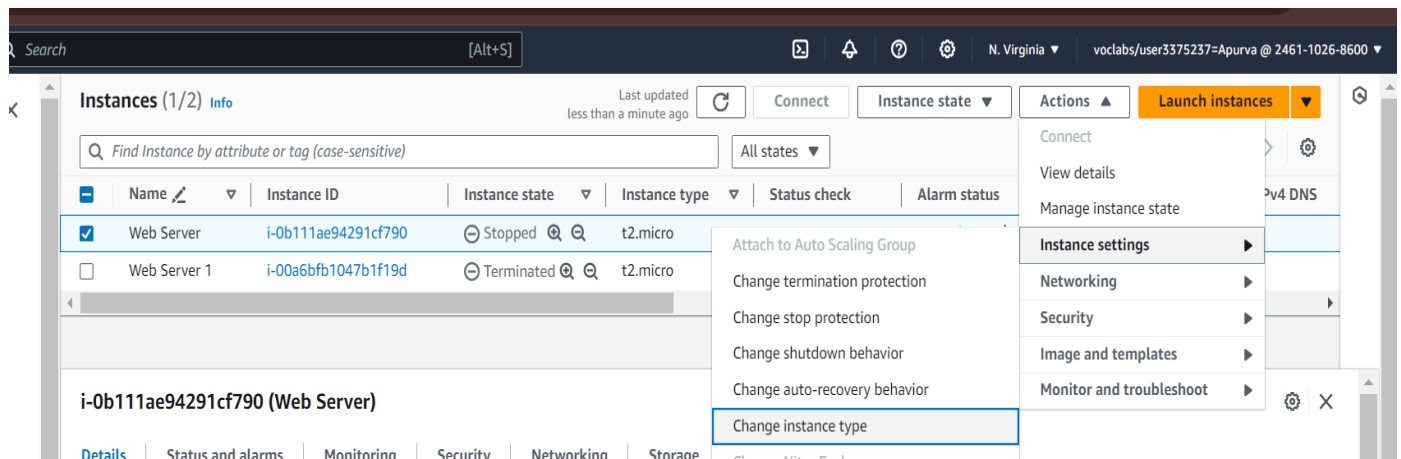


- In the Instance state menu, choose Stop instance and confirm the action.

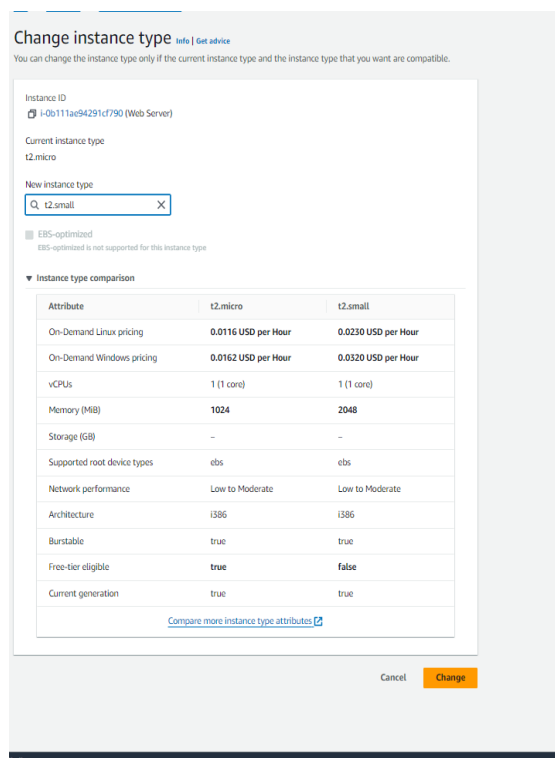


2. Change Instance Type:

- Once the instance is stopped, go to the Actions menu.
- Select Instance settings > Change instance type.

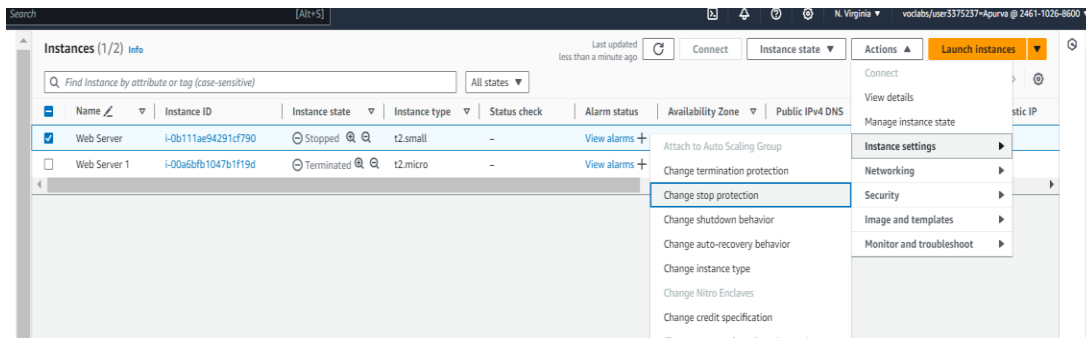


- Change Instance Type to t2.small and click Apply.

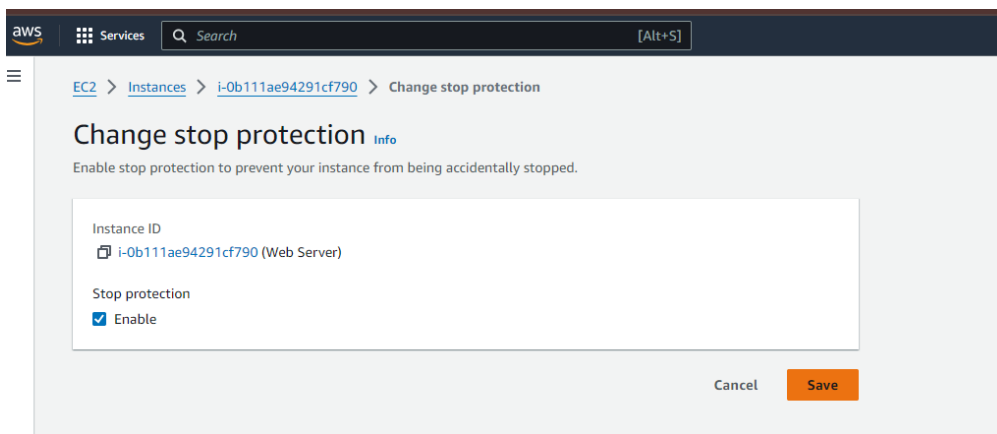


3. Enable Stop Protection:

- In the Actions menu, select Instance settings > Change stop protection.

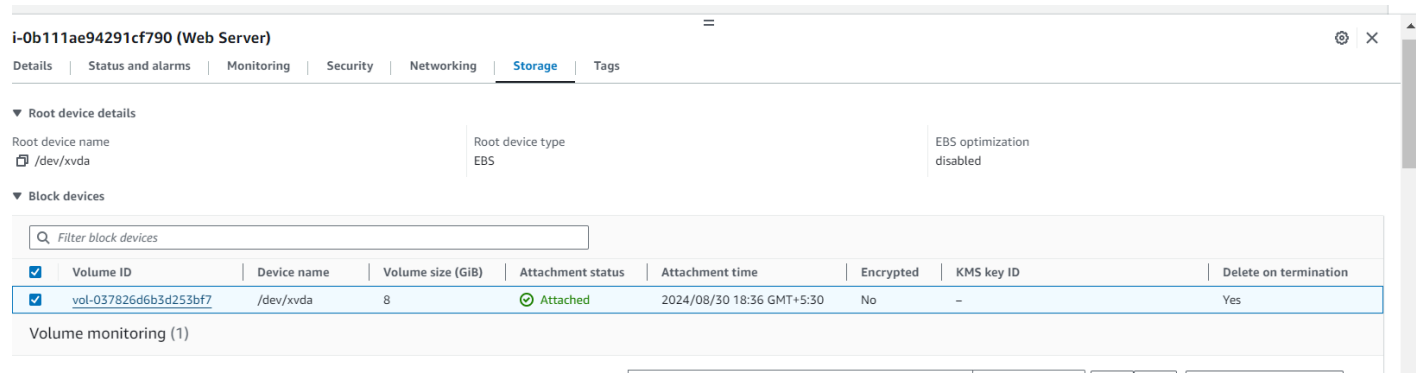


- Enable stop protection and save the changes.

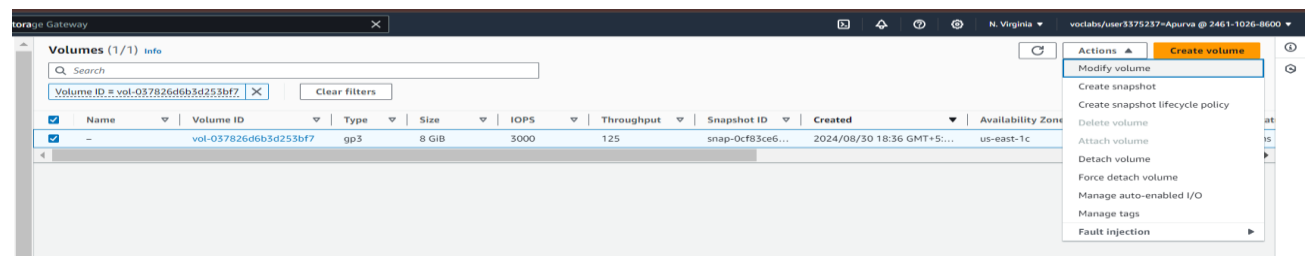


4. Resize EBS Volume:

- With the instance still selected, go to the Storage tab.
- Click on the Volume ID to view volumes, then check the volume.



- In the Actions menu, select Modify volume.
- Change the size to 10 GiB and confirm the modification.



5. Start the Resized Instance:

- Go back to Instances in the left pane.
- Select the Web Server instance, then choose Start instance from the Instance state menu.

Modify volume [Info](#)
Modify the type, size, and performance of an EBS volume.

Volume details

Volume ID
vol-037826d6b5d253bf7

Volume type [Info](#)
General Purpose SSD (gp3)

Size (GiB) [Info](#)
10
Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS [Info](#)
3000
Min: 3000 IOPS, Max: 16000 IOPS. The value must be an integer.

Throughput (MiB/s) [Info](#)
125
Min: 125 MiB, Max: 1000 MiB. Baseline: 125 MiB/s.

[Cancel](#) [Modify](#)

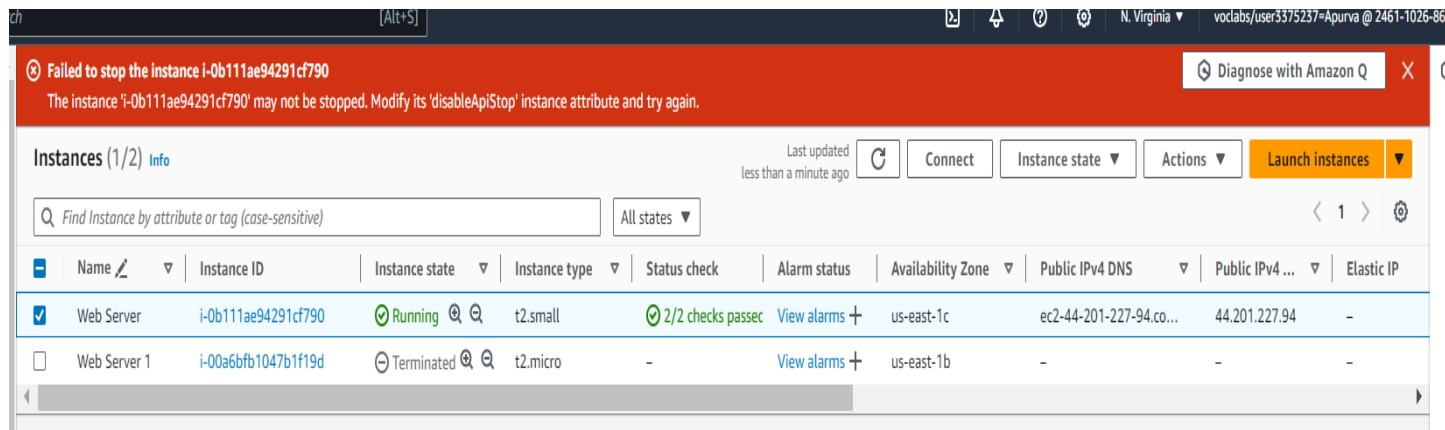
Task 5: Test Stop Protection

1. Attempt to Stop Instance:

- In the EC2 Console, select Web Server.
- From the Instance state menu, choose Stop instance.

2. Observe Error:

- You will see a message indicating that the instance cannot be stopped due to enabled stop protection.



3. Disable Stop Protection:

- In the Actions menu, select Instance settings > Change stop protection.
- Disable stop protection and save.

4. Stop the Instance:

- Again, select Stop instance from the Instance state menu to successfully stop the instance.

Successfully initiated stopping of i-0b111ae94291cf790

Instances (1/1) [Info](#)

Last updated less than a minute ago

Connect

Instance state

Actions

Launch instances

All states

< 1 >

☒

Name

☐

Instance ID

☐

Instance state

☐

Instance type

☐

Status check

☐

Alarm status

☐

Availability Zone

☐

Public IPv4 DNS

☐

Public IPv4 ...

☐

Elastic IP

| ☒ | Web Server | [i-0b111ae94291cf790](#) | Stopped | t2.small | - | [View alarms](#) | us-east-1c | - | - | - |