



**Department of Computer Science & Engineering  
Premier University.**

CSE 482: Contemporary Course of Computer Science  
Laboratory.

## **Introduction to Amazon EC2**

**Submitted By:**

Name	Sajjad Hosen Emon
ID	0222310005101105
Section	C
Semester	7 <sup>th</sup>
Submission Date	2/3/2026

**Remarks**

# Lab 3: Introduction to Amazon EC2

## Objective

The objective of this lab is to understand the basic functionality of Amazon EC2 and learn how to launch, configure, and manage a virtual server in a cloud environment. It provides hands-on experience in selecting an instance type, configuring network and security settings, enabling protection features, and automating web server installation using user data. The lab also helps develop skills in monitoring instance performance and scaling resources by modifying the instance type and storage. Overall, it builds foundational knowledge required for managing secure and efficient cloud infrastructure.

## Scenario

In this lab, you take on the role of a cloud engineer responsible for setting up a basic web server for an organization using AWS. The goal is to deploy a secure and reliable server that can host a webpage accessible from the internet.

To accomplish this, an EC2 instance is launched and configured with the necessary network and security settings. An Apache web server is automatically installed using a user data script so that the server can immediately begin hosting content. After deployment, the instance is monitored to ensure it is functioning properly.

Since cloud environments must adapt to changing demands, the server is later scaled by upgrading the instance type and increasing storage capacity. Protection features are also tested to prevent accidental stopping or termination of the server. This lab reflects practical cloud operations where engineers must ensure availability, security, and scalability while maintaining full control over computing resources.



# Working Procedure

## Step 1: Starting the Lab and Accessing AWS Console

1. Clicked Start Lab and waited until the AWS indicator turned green.
2. Opened the AWS link to access the AWS Management Console in a new browser tab.
3. Arranged the console and lab instructions side by side for easier navigation.

## Step 2: Launching the EC2 Instance

4. Navigated to Services → Compute → EC2.
5. Verified that the region was set to N. Virginia (us-east-1).
6. Clicked Launch Instance to begin creating the virtual server.

The screenshot shows the AWS EC2 Dashboard. On the left, a sidebar menu includes EC2 Global View, Events, Instances (with sub-options like Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager), Images (AMIs, AMI Catalog), and Elastic Block Store. The main content area displays 'Resources' and 'EC2 cost'. Under 'Resources', it shows 1 instance running, 0 Auto Scaling Groups, 0 Capacity Reservations, 0 Dedicated Hosts, 0 Elastic IPs, 1 instance, 1 Key pair, 0 Load balancers, 0 Placement groups, 4 Security groups, 0 Snapshots, 0 Volumes, and 1 Volume. The 'EC2 cost' section shows a total cost of \$0.00 for the past 6 months across 1 region. A large blue bar chart represents the cost distribution.

7. Entered the instance name 'Web Server'.

## Step 3: Selecting AMI, Instance Type, and Key Pair

8. Selected the default Amazon Linux 2023 AMI from the Quick Start list.

The screenshot shows the 'Launch an instance' wizard. The 'Quick Start' tab is selected, displaying a grid of AMI icons for Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian. Below the grid is a search bar labeled 'Search our full catalog including 1000s of application and OS images'. To the right, the 'Summary' section shows 1 instance, the Software Image (AMI) as Amazon Linux 2023 AMI 2023.10..., the Virtual server type (instance type) as t3.micro, and the Storage (volumes) as 1 volume(s) - 8 GiB. A message indicates a free tier for the first year. At the bottom are 'Cancel', 'Launch instance', and 'Preview code' buttons.

9. Chose t2.micro as the instance type.

The screenshot shows the AWS EC2 'Launch an instance' wizard. In the 'Instance type' section, 't2.micro' is selected. Other options like 'All generations' and 'Compare instance types' are available. On the right, the 'Summary' section shows 1 instance being launched with the following details:

- Software Image (AMI)**: Amazon Linux 2023 AMI 2023.10...
- Virtual server type (instance type)**: t2.micro
- Firewall (security group)**: New security group
- Storage (volumes)**: 1 volume(s) - 8 GiB

A 'Launch instance' button is prominently displayed at the bottom right.

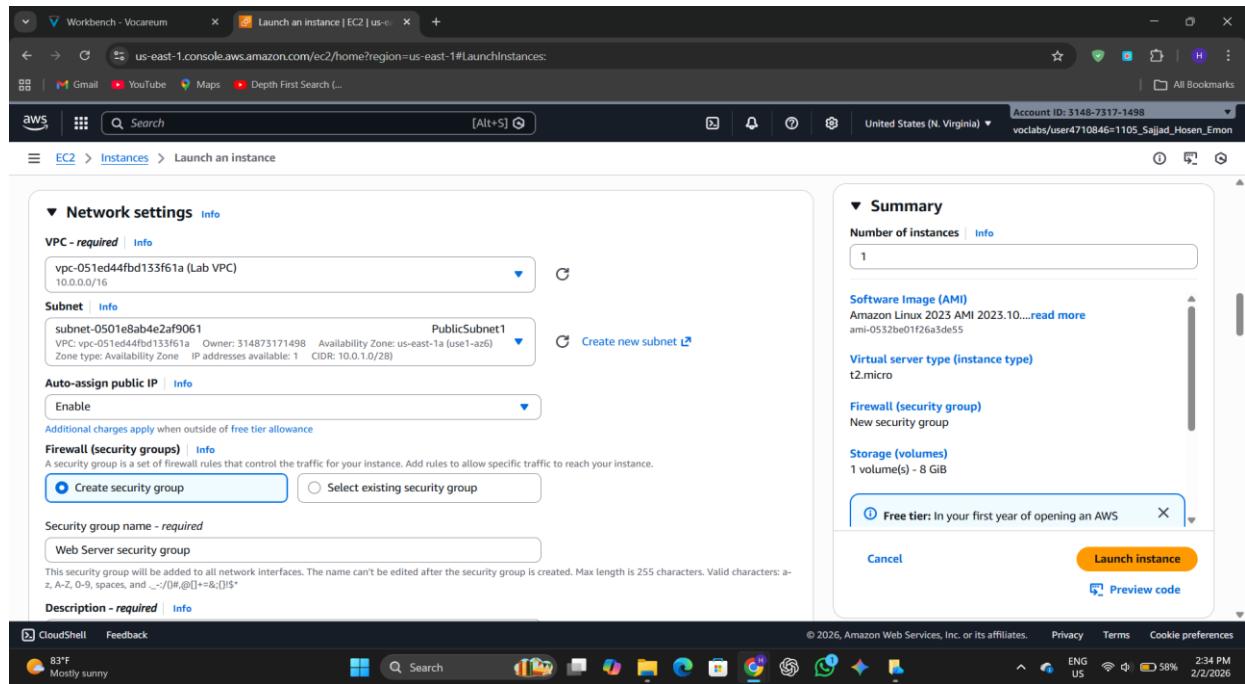
10. Selected the 'vokey' key pair for secure login authentication.

The screenshot shows the continuation of the 'Launch an instance' wizard. In the 'Key pair (login)' section, 'vokey' is selected from a dropdown menu. The 'Create new key pair' button is also visible. The 'Summary' section remains the same as in the previous step, showing 1 instance being launched with the specified configuration.

## Step 4: Configuring Network and Security Group

11. Edited Network Settings and selected the preconfigured Lab VPC.  
 12. Kept PublicSubnet1 so the instance would receive a public IP address.

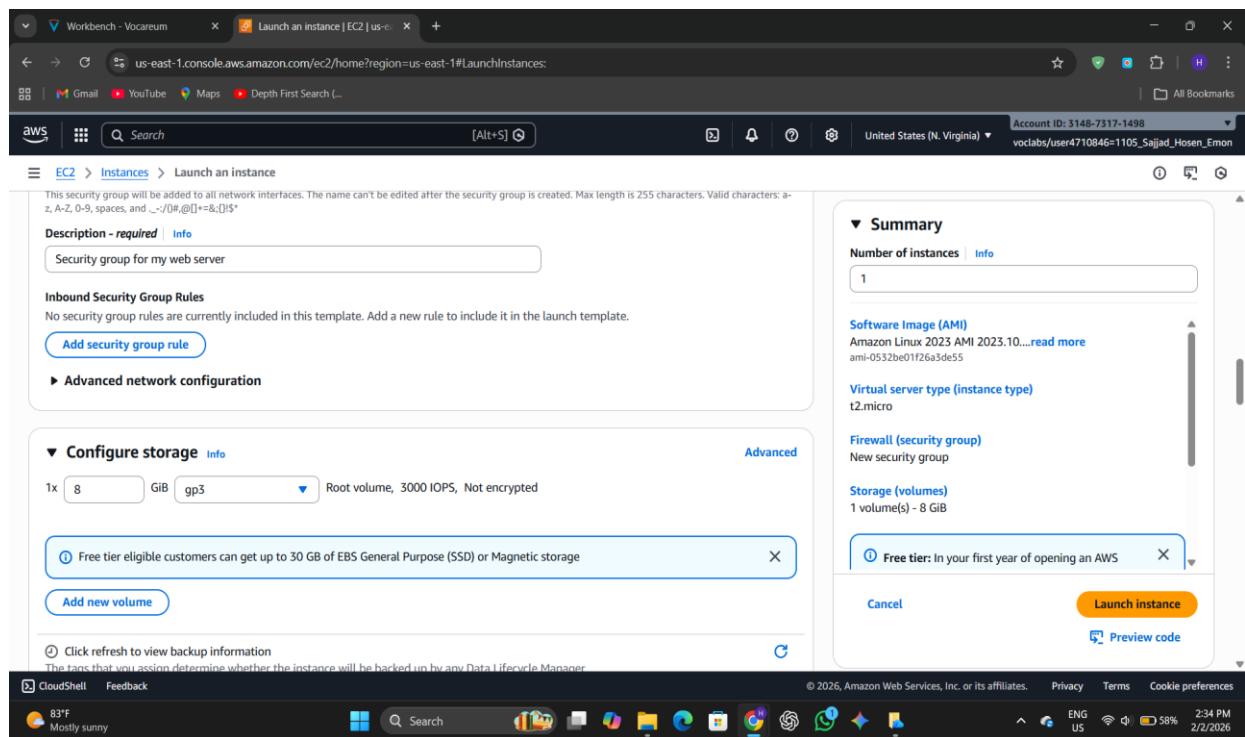
13. Created a security group named 'Web Server security group' with the description 'Security group for my web server'.



14. Removed the existing inbound rule to block unnecessary traffic.

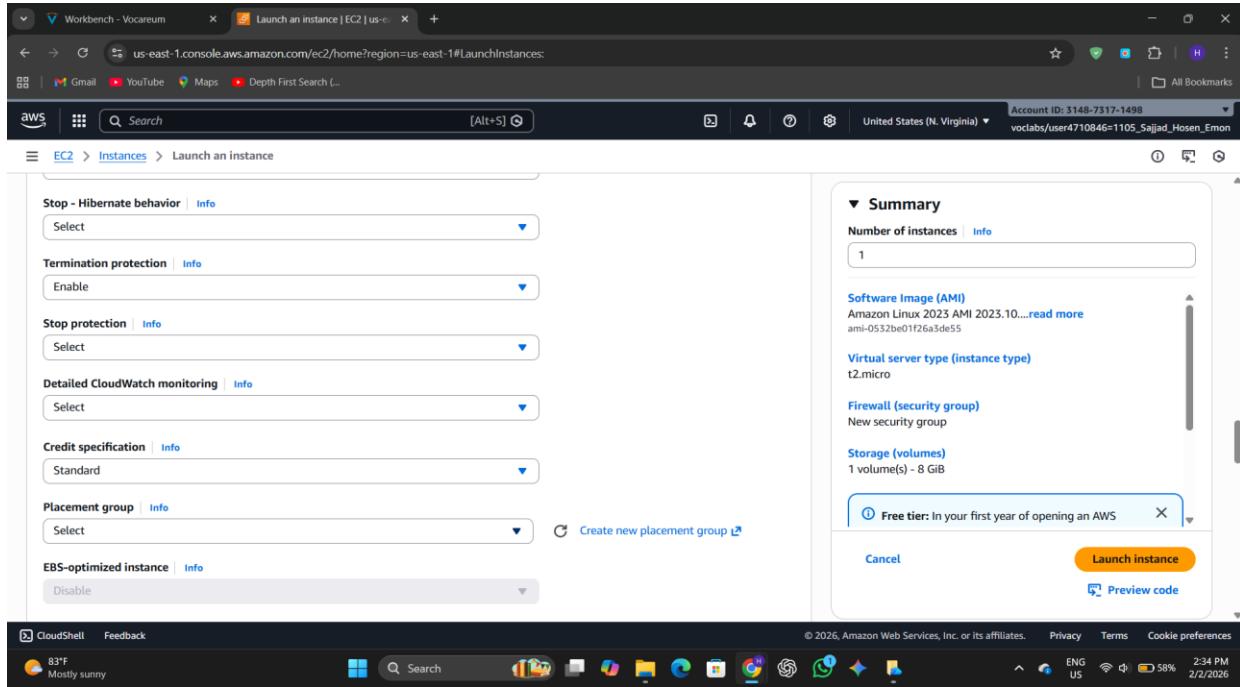
## Step 5: Configuring Storage

15. Kept the default 8 GiB Elastic Block Store (EBS) volume as the root disk for the instance.

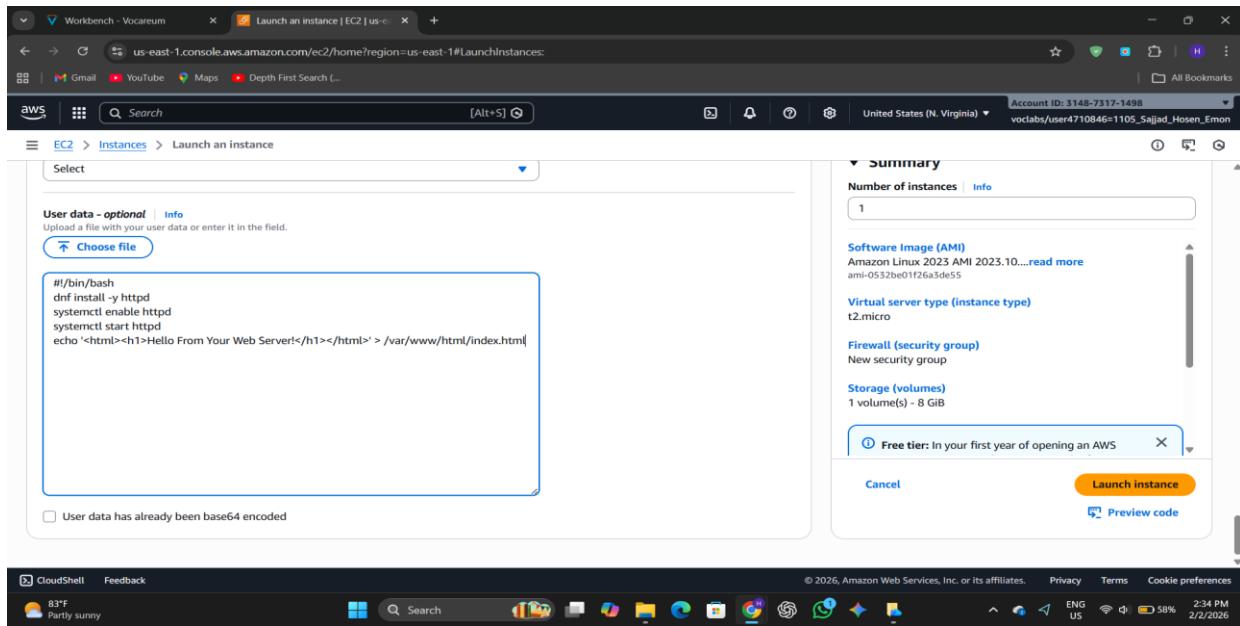


## Step 6: Enabling Termination Protection and Adding User Data

16. Expanded Advanced Details and enabled termination protection to prevent accidental deletion.

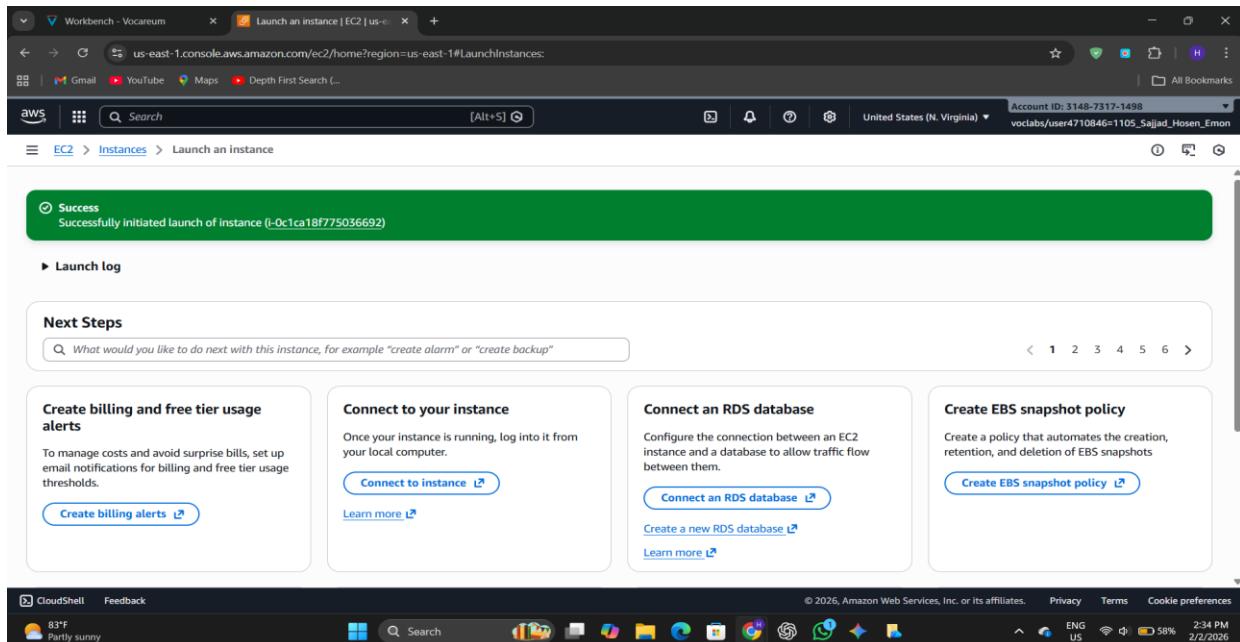


17. Added the provided user data script to automatically install Apache, start the service, enable auto-start on boot, and create a simple HTML webpage.

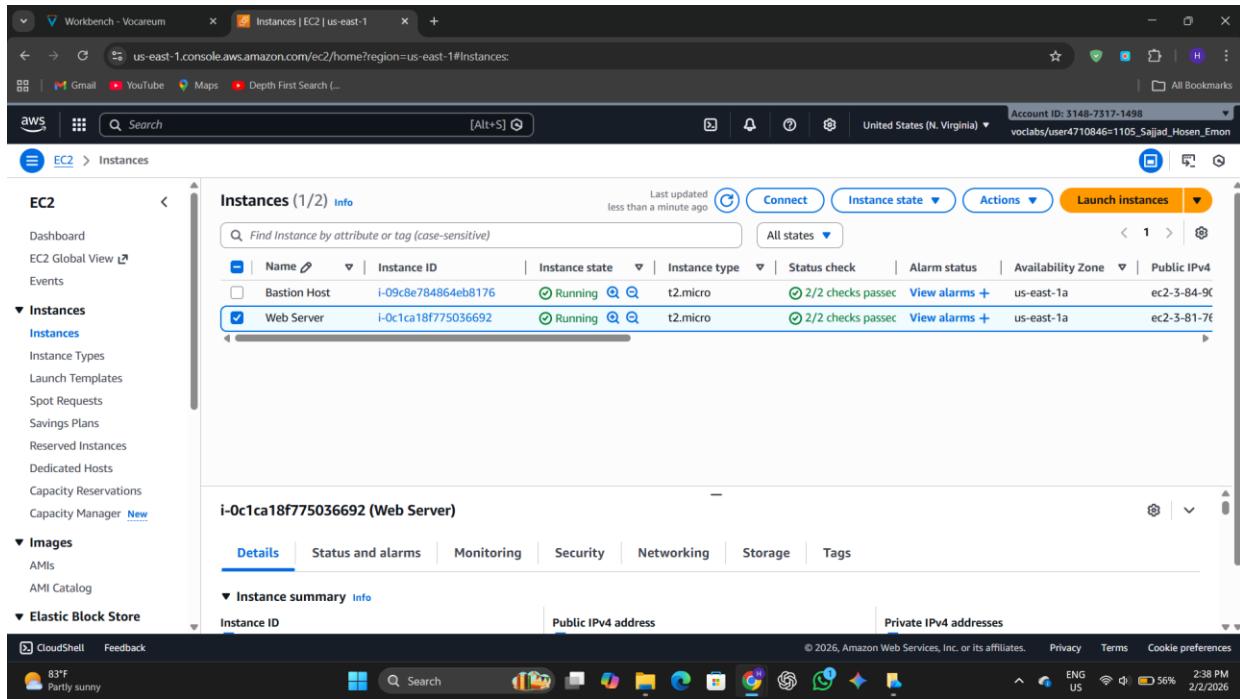


## Step 7: Launching and Verifying the Instance

18. Clicked Launch Instance and viewed the success message.

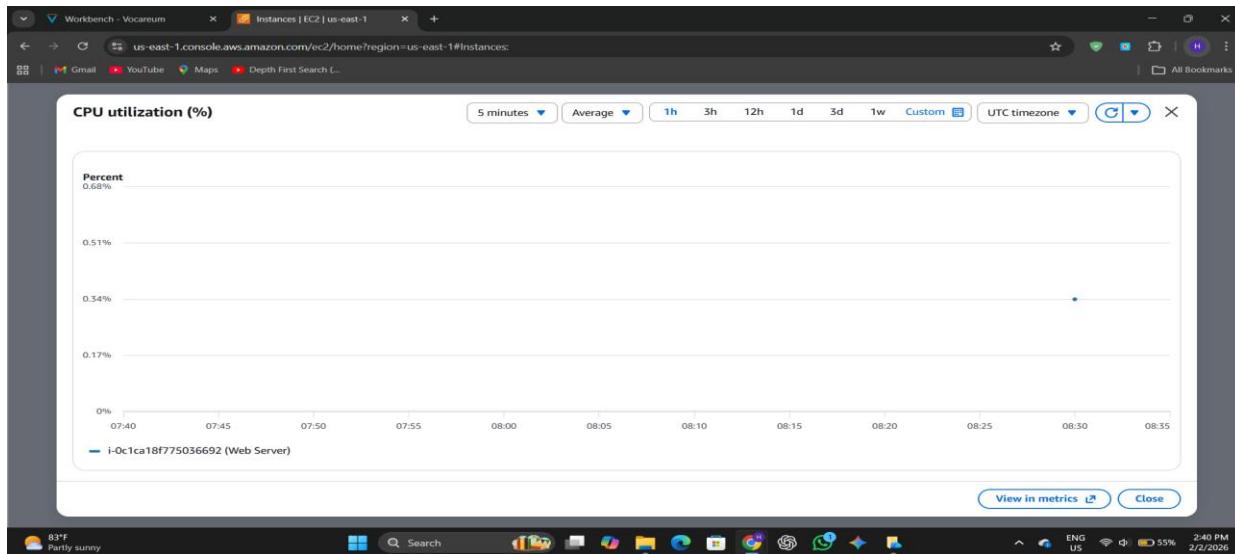


19. Opened the Instances page and selected the Web Server instance.
20. Observed the instance state change from Pending to Running.
21. Confirmed that both status checks showed 2/2 checks passed.

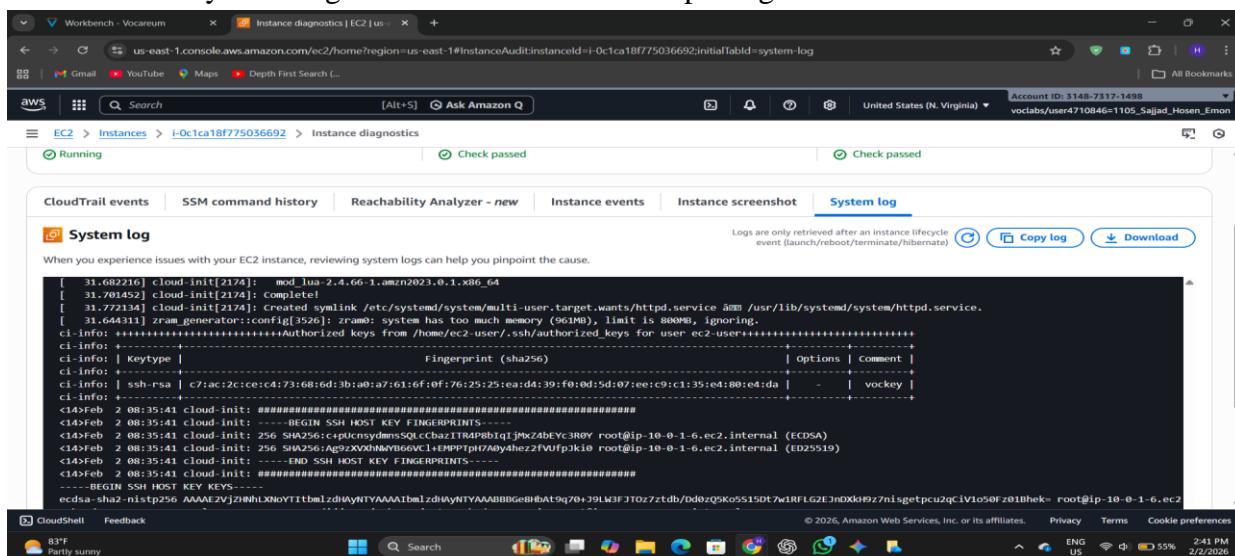


## Step 8: Monitoring the Instance

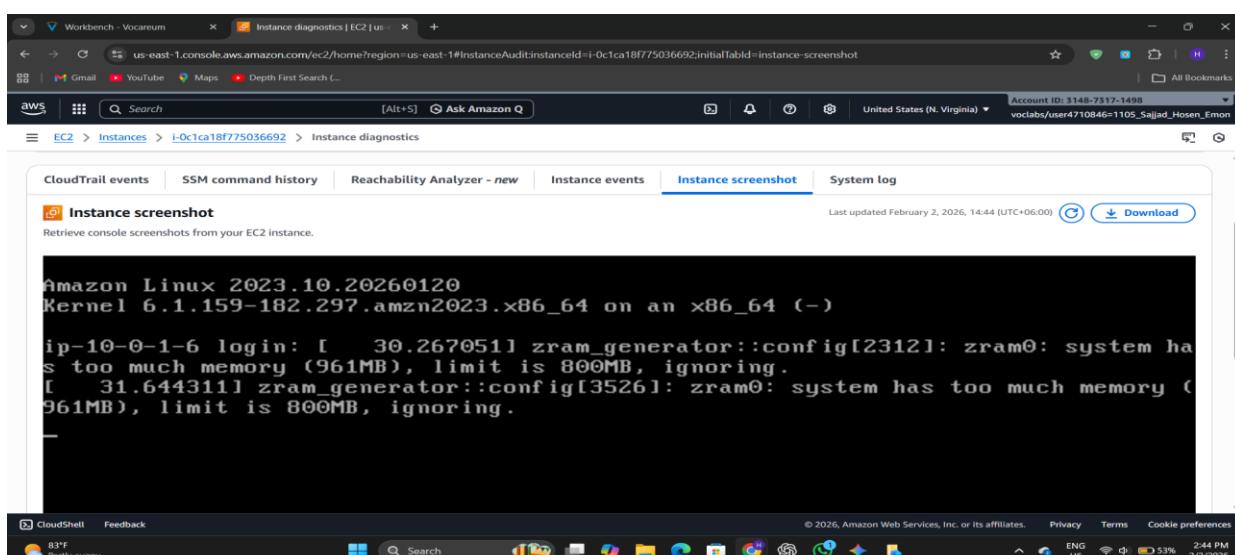
22. Opened the Status Checks tab to verify system and instance reachability.
23. Viewed the Monitoring tab to analyze CloudWatch metrics.



#### 24. Retrieved the System Log to confirm that the HTTP package was installed from the user data script



#### 25. Captured the Instance Screenshot to view the console display for troubleshooting.



## Step 9: Updating Security Group and Accessing the Web Server

26. Copied the Public IPv4 address from the Details tab.
27. Pasted the IP address into a browser and observed that the webpage was not accessible due to blocked HTTP traffic.
28. Navigated to Security Groups and selected 'Web Server security group'

The screenshot shows the AWS Management Console with the URL <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SecurityGroups>. The left sidebar is collapsed. The main content area shows the 'Security Groups (1/5) - Info' table. The 'Web Server security group' (sg-07ecc61ef0d2a83ae) is selected and highlighted with a blue border. The 'Inbound rules' tab is selected. Below it, a table titled 'Inbound rules' shows 'No security group rules found'.

29. Edited inbound rules and added a new rule allowing HTTP (Port 80) from Anywhere-IPv4.

The screenshot shows the 'Edit inbound rules' dialog for the 'Web Server security group'. The 'Inbound rules' table has a single row: 'No security group rules found'. A new rule is being added, with the 'Type' set to 'HTTP', 'Protocol' to 'TCP', 'Port range' to '80', 'Source' to 'Anywhere', and 'Description' to 'Allow HTTP traffic'. A warning message at the bottom states: 'Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.' The 'Save rules' button is highlighted.

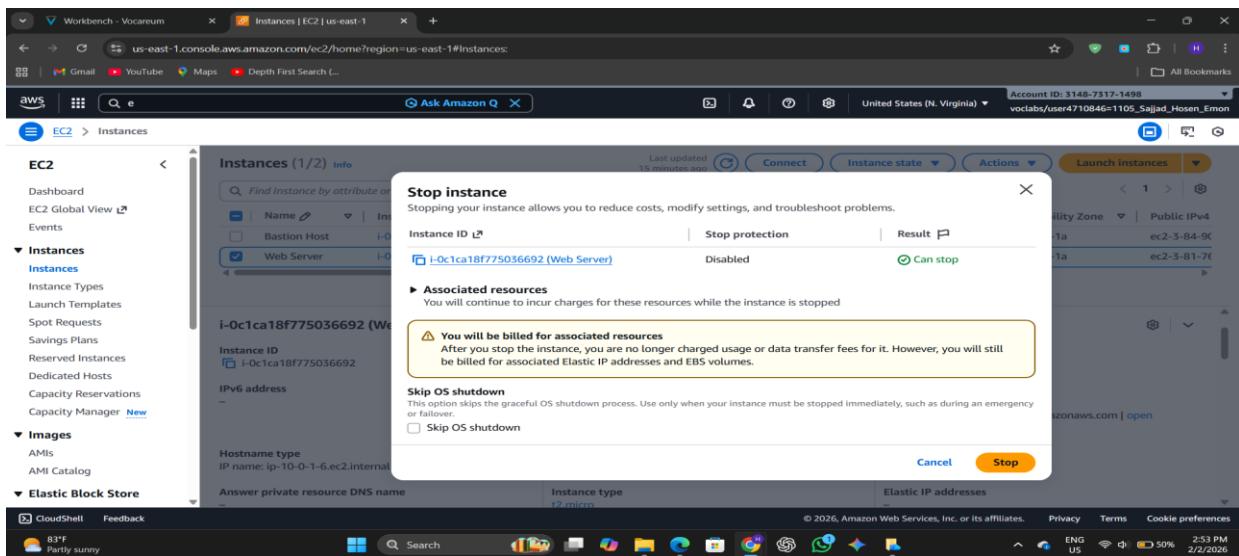
30. Saved the rules and refreshed the browser.
31. Verified that the webpage displayed 'Hello From Your Web Server!'.

### Hello From Your Web Server!

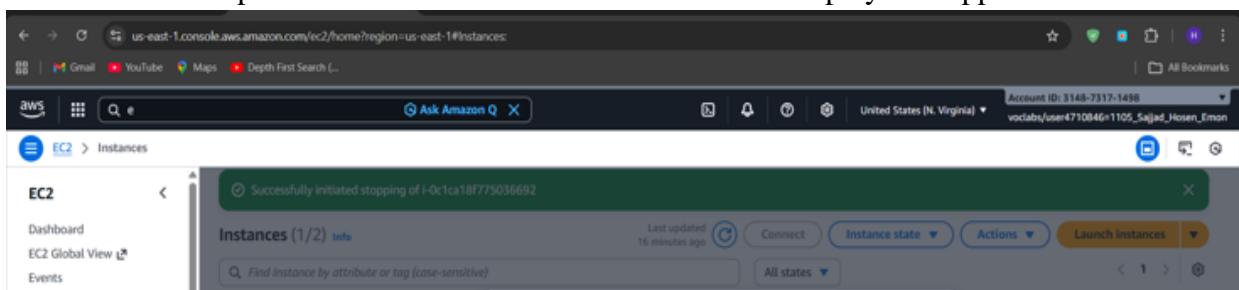


## Step 10: Stopping the Instance for Resizing

32. Selected the Web Server instance and chose Instance State → Stop Instance.

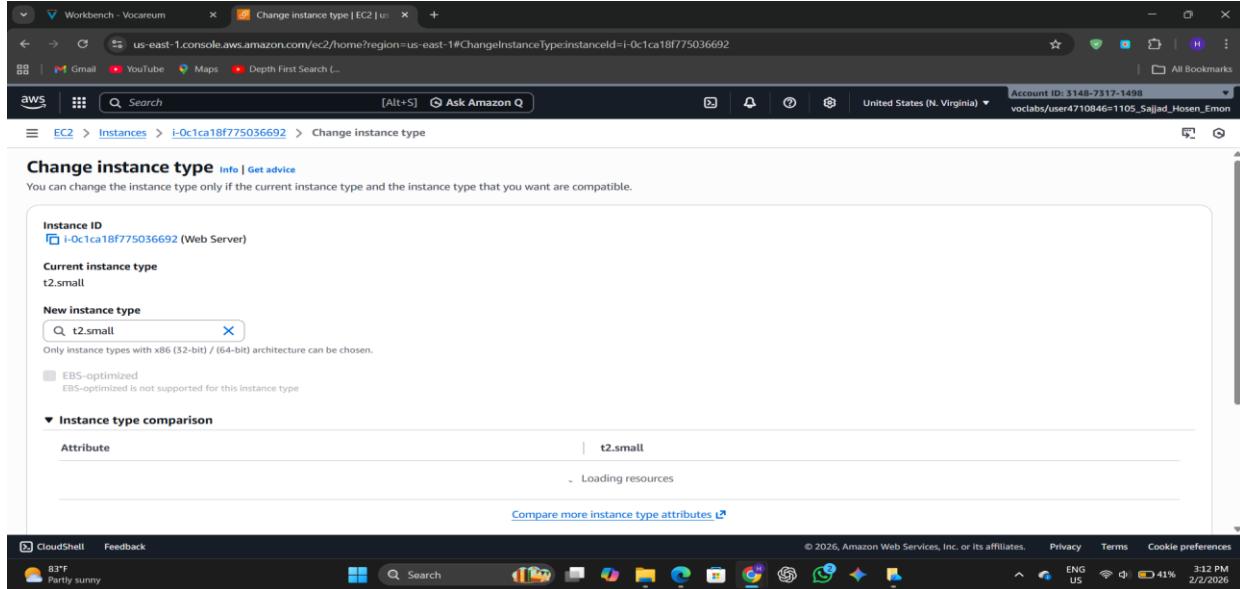


33. Confirmed the stop action and waited until the instance state displayed Stopped.

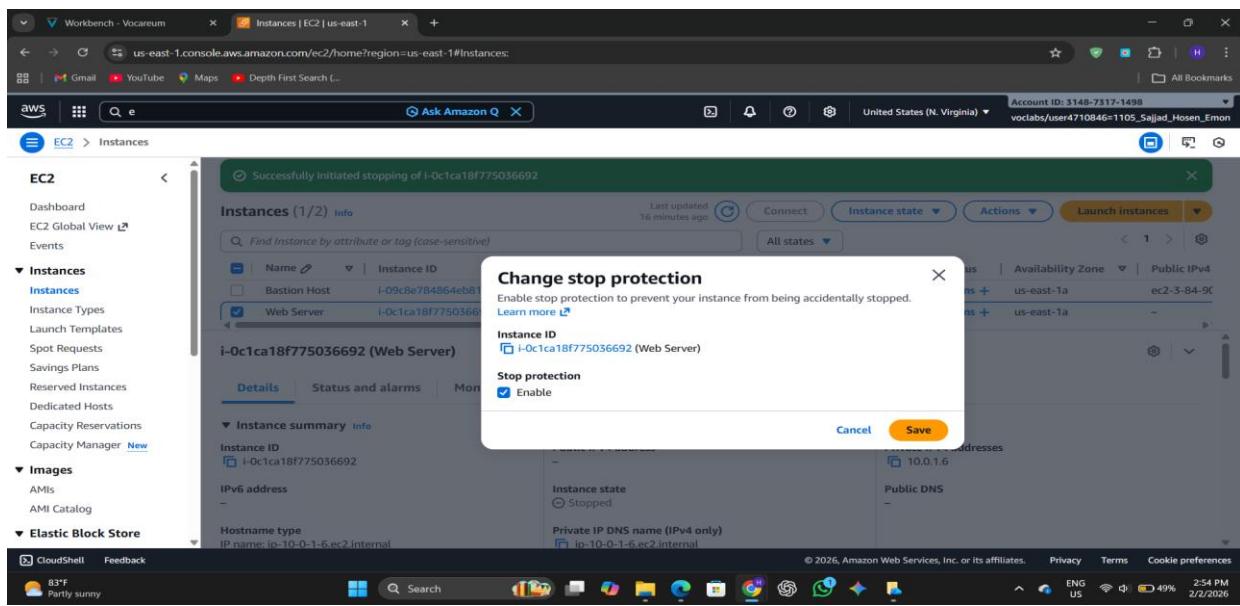


## Step 11: Changing Instance Type and Enabling Stop Protection

34. Opened Actions → Instance Settings → Change instance type.
35. Upgraded the instance from t2.micro to t2.small to increase memory.

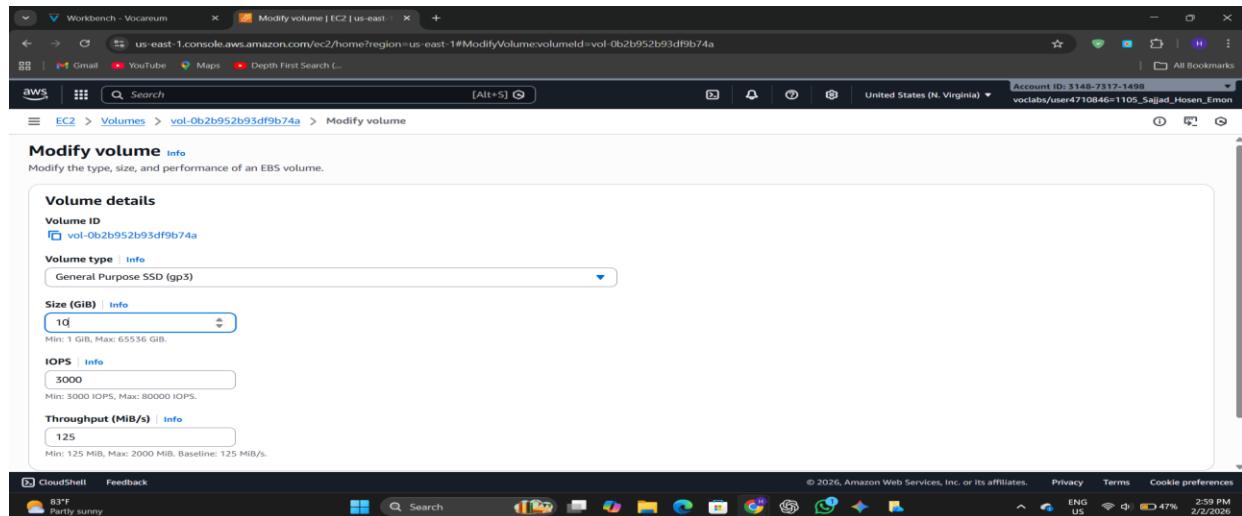


36. Enabled stop protection to prevent accidental shutdown.

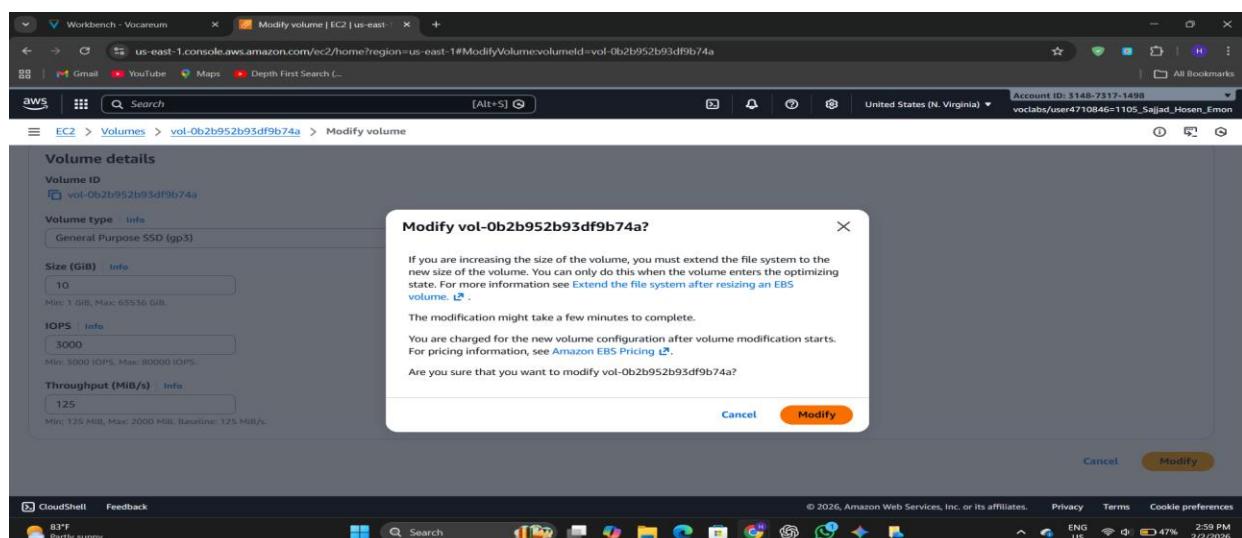


## Step 12: Modifying the EBS Volume

37. Navigated to the Storage tab and selected the attached volume.
38. Clicked Modify Volume and increased the disk size from 8 GiB to 10 GiB.



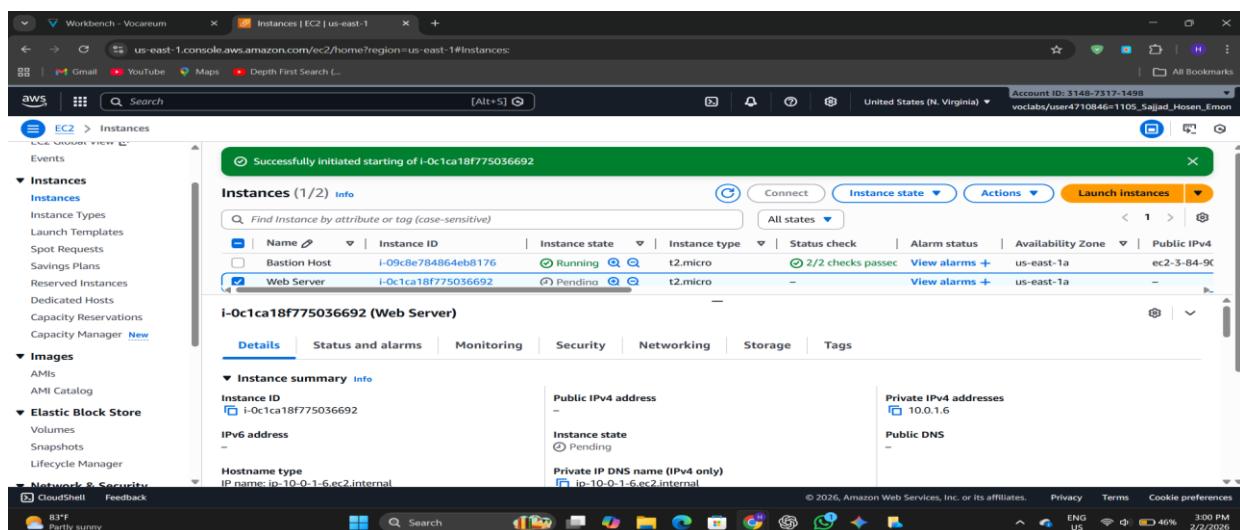
### 39. Confirmed the modification.



## Step 13: Restarting the Instance

40. Returned to the Instances page and clicked Start Instance.

41. Verified that the instance restarted successfully with upgraded resources.



The screenshot shows the AWS EC2 Instances page. At the top, a green success message says "Successfully initiated starting of i-0c1ca18f775036692". Below it, the "Instances (1/2) Info" section lists two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
Bastion Host	i-09c8e784864eb8176	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	us-east-1a	ec2-53-84-96
Web Server	i-0c1ca18f775036692	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	us-east-1a	ec2-54-210

On the left sidebar, under "Instances", there are links for Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, and Capacity Manager. Other sections like "Images" and "Elastic Block Store" are also visible.

## Step 14: Exploring EC2 Service Limits

42. Searched for Service Quotas from the AWS console.
43. Selected Amazon Elastic Compute Cloud (EC2).
44. Searched for 'running on-demand' quotas and reviewed the limits for instances in the region.

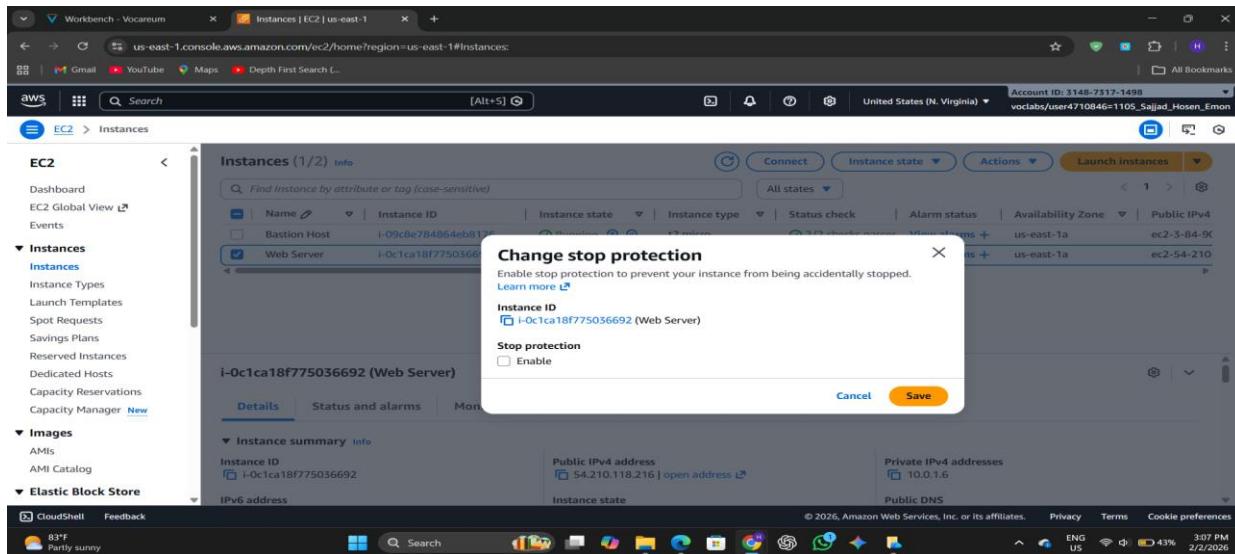
The screenshot shows the AWS Service Quotas page for EC2. A message box at the top says: "For Amazon Elastic Compute Cloud (Amazon EC2) quotas with Adjustability at the Resource-level, you can now request a quota increase at the resource level by clicking the quota name to navigate to the quota details page and choosing the resource for which you want to request a quota increase. [Learn more](#)".

The "Service quotas info" section displays a table of running on-demand quotas:

Quota name	Applied account-level quota value	AWS default quota value	Utilization	Adjustability
<a href="#">Running On-Demand DL Instances</a>	96	0	0	Account level
<a href="#">Running On-Demand F Instances</a>	64	0	0	Account level
<a href="#">Running On-Demand G and VT Instances</a>	0	0	0	Account level
<a href="#">Running On-Demand High Memory instances</a>	0	0	0	Account level
<a href="#">Running On-Demand HPC instances</a>	192	0	0	Account level
<a href="#">Running On-Demand I instances</a>	8	0	0	Account level
<a href="#">Running On-Demand P instances</a>	0	0	0	Account level
<a href="#">Running On-Demand Standard (A, C, D, H, I, M, R, T, Z)</a>	256	5	1	Account level

## Step 15: Testing Stop Protection

45. Attempted to stop the instance while stop protection was enabled and received an error message.
46. Opened Instance Settings and disabled stop protection.



47. Stopped the instance successfully afterward.

The screenshots show the following sequence:

- The first screenshot shows the 'Stop instance' dialog for instance i-0c1ca18f775036692. The 'Stop protection' dropdown is set to 'Disabled'. A note below says: "You will continue to incur charges for these resources while the instance is stopped." There is also a note about skipping OS shutdown.
- The second screenshot shows the same dialog after the 'Stop' button is clicked. A green notification bar at the top says: "Successfully initiated stopping of i-0c1ca18f775036692".
- The third screenshot shows the main EC2 Instances page after the stop operation. The instance status for i-0c1ca18f775036692 is now 'Stopping'.

## Step 16: Submitting and Ending the Lab

48. Clicked Submit to record the lab progress and viewed the grading panel.

01:03      ▶ Start Lab    ■ End Lab    AWS Details    ● Details    X

Submit    Submission Report    Grade

Total score	25/25
Task 1 - EC2 instance created correctly	5/5
Task 2 - get system log requested	5/5
Task 3 - security group updated	5/5
Task 4 - EC2 instance updated	5/5
Task 6 - Instance stopped on second try	5/5

#### 49. Reviewed the submission report for feedback.

```
[Executed at: Mon Feb 2 1:18:32 EST 2026]
64. V gradeFile = /mnt/vocwork5/grader/eee_G_2692329 asn4967429_3 asn4967430_1 /tmp/temp_uf_02022026/.hjnuvrmu8k703t7qUQ
A reportfile = /mnt/vocwork5/grader/eee_G_2692329 asn4967429_3 asn4967430_1 /tmp/temp_uf_02022026/.labt320r2ri7ifbyVFa
e /mnt/vocwork5/grader/eee_G_2692329 asn4967429_3 asn4967430_1 /tmp/temp_uf_02022026/.hjnuvrmu8k703t7qUQ
s Started: 2026-02-02 01:18:26
r region: us-east-1
p profile: default
d

if Evaluating Task 1 - EC2 instance created correctly
t Found instance with name Web Server
i instance_type: t2.small
n instance_subnet: subnet-0501e8ab4e2af9061
s instance_security_group: Web Server security group
Y Task 1 - Success! An instance with the name Web Server was found.

Evaluating Task 2 - get system log requested
t Task 2 - Success! Evidence found that the system log of the EC2 instance was requested.

65. T
```

Tip: For any checks where you did not receive full points, there are sometimes helpful details provided in the submission report.

#### Lab Complete

```
Evaluating Task 3 - security group updated
Security group named Web Server security group found.
Inbound rules found
Task 3 - Success! Evidence found that the inbound rules for the security group were updated to allow TCP port 80 (HTTP) traffic.

A Evaluating Task 4 - EC2 instance updated
e Found instance with name Web Server
i instance_type: t2.small
n volume_id: vol-0b2b952b93df9b74a
s volume_size: 10
if Task 4 - Success! The instance was found, it was changed to the correct instance type, and the volume was resized correctly.
ti
Evaluating Task 6 - Instance stopped on second try
t Found a failed attempt to stop the instance (which indicates instructions were followed)
s instance_state: stopped
Y Task 6 - Success! Evidence found that an attempt was first made to stop the instance before turning off stop protection, and then evidence

Completed: 2026-02-02 01:18:29
```

Tip: For any checks where you did not receive full points, there are sometimes helpful details provided in the submission report.

#### Lab Complete

#### 50. Clicked End Lab and confirmed to close the session.

## **Conclusion**

This lab provided practical experience in launching, configuring, and managing a virtual server using Amazon EC2. It covered essential tasks such as setting up security groups, enabling protection features, monitoring instance health, and automating web server installation. The lab also demonstrated how cloud resources can be scaled by modifying the instance type and storage based on requirements. Overall, it helped build a strong foundation in cloud computing and improved understanding of secure and efficient infrastructure management using AWS.