



Assignment 2

EC2 Windows and S3 Bucket

Cloud Computing (CIS443)

Prepared By

Yazeed AlKhalaf
202211123

Submitted To

Prof. Mohammad Mehedi Hassan

February 12, 2025

Contents

1 Part A: Amazon EC2 Windows VM	1
1.1 Create Windows VM	1
1.2 Connect to VM	3
2 Part B: Create Snapshots / Backups/Amazon Machine Image (AMI) Creation	6
3 Part C: How to host a static website on AWS S3	8

List of Figures

1	Windows VM Creation - Initial Configuration with Windows Selected	1
2	Selecting t2.micro instance type for Windows Server and the New Key Pair	1
3	Configuring VPC, subnet and security group settings	2
4	Instance launch status confirmation page	2
5	Setup Connect Using RDP Client	3
6	Uploading Private Key to Decrypt Windows Password	3
7	Opened RDP Client for Windows "Windows App Beta" on macOS	4
8	Add Credentials in RDP Client	4
9	Enter IP Address	5
10	PC Added Successfully	5
11	Successfully Connected	6
12	Right Click to Create Image	6
13	AMI Creation Options	7
14	AMI Created Successfully	7
15	Bucket Creation 1	8
16	Bucket Creation 2	8
17	Bucket Creation 3	9
18	Created Bucket Successfully	9
19	Uploaded <code>index.html</code> File Successfully	10
20	Static Web Hosting Setting Page	10
21	Static Website Hosting Enabled	11
22	Disabled "Block Public Access" Setting	11
23	Success Page for "Block Public Access" Being Disabled	12
24	Object Ownership Setting Change to Enable ACL	12
25	S3 Static Website - Make Public Menu Item	13
26	S3 Static Website - Make Public Page	13
27	Successfully hosted static website showing "Hello World"	14

1 Part A: Amazon EC2 Windows VM

1.1 Create Windows VM

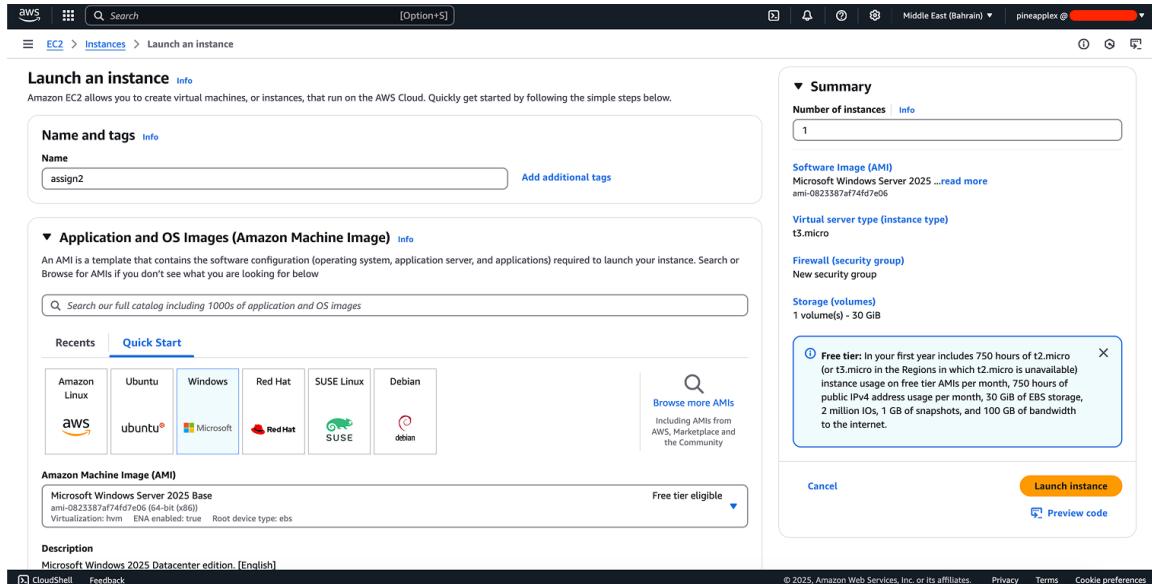


Figure 1: Windows VM Creation - Initial Configuration with Windows Selected

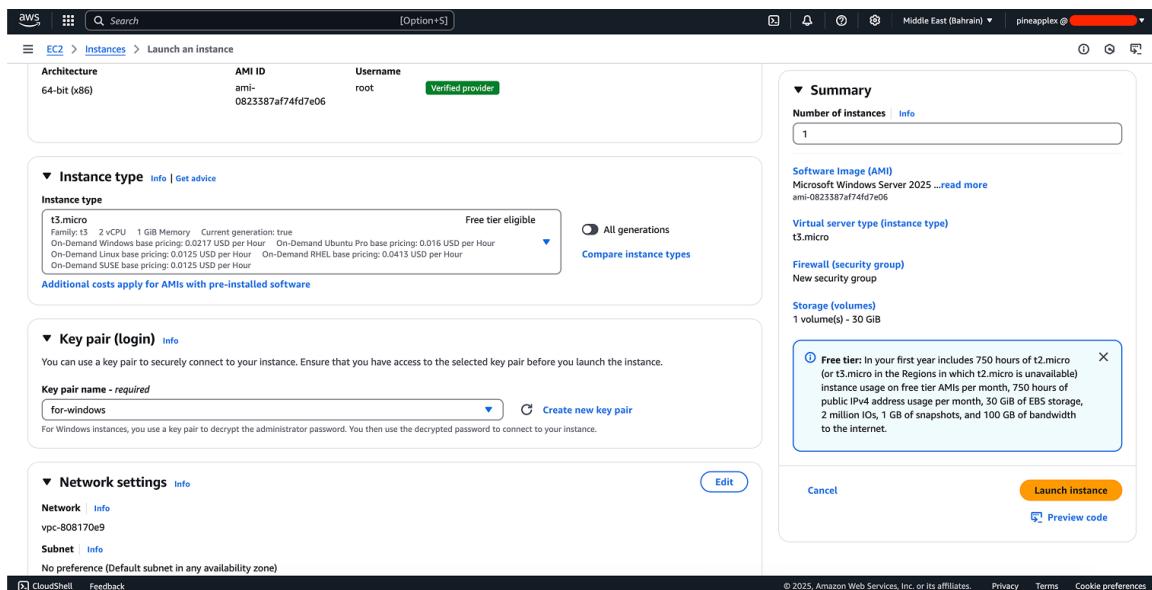


Figure 2: Selecting t2.micro instance type for Windows Server and the New Key Pair

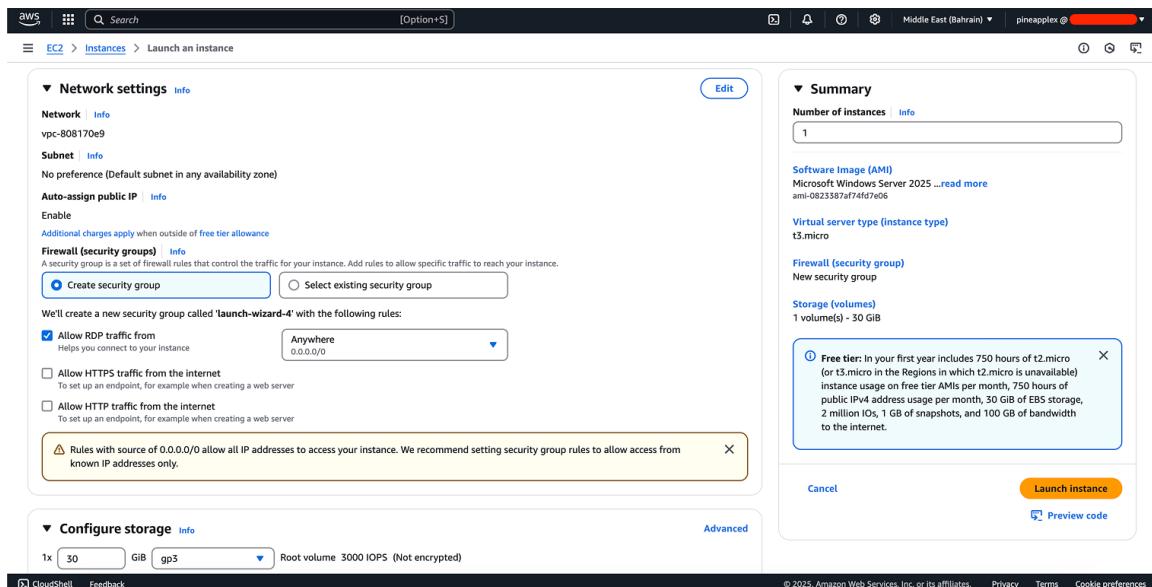


Figure 3: Configuring VPC, subnet and security group settings

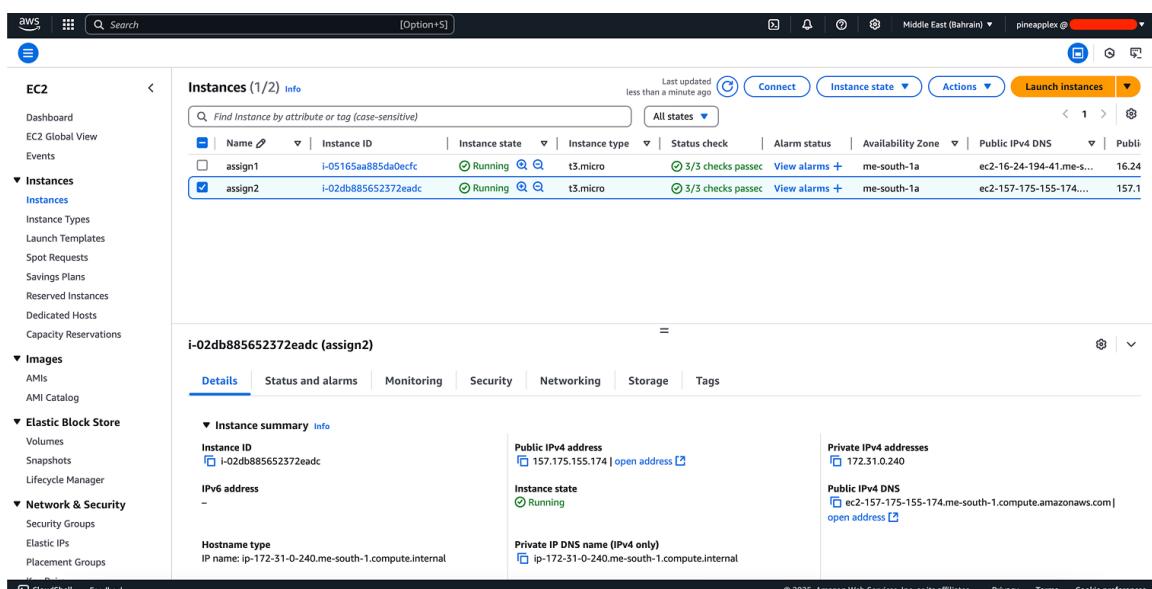


Figure 4: Instance launch status confirmation page

1.2 Connect to VM

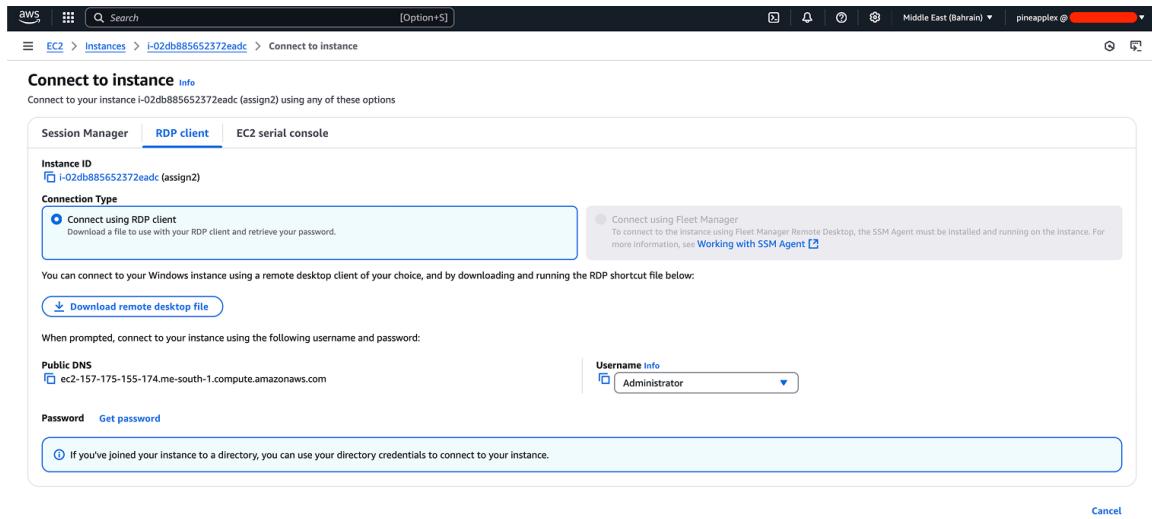


Figure 5: Setup Connect Using RDP Client

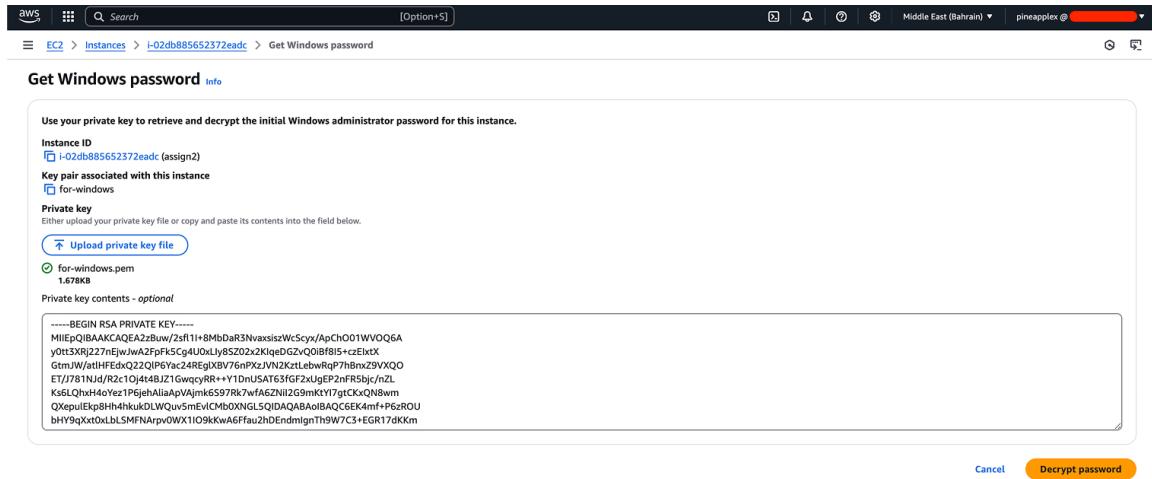


Figure 6: Uploading Private Key to Decrypt Windows Password

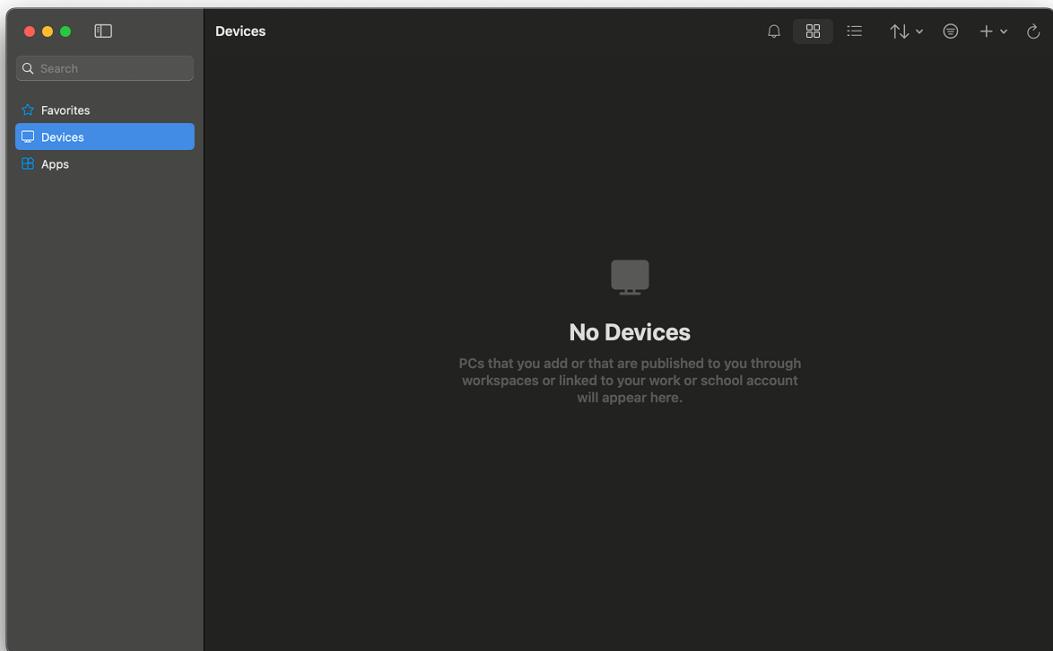


Figure 7: Opened RDP Client for Windows "Windows App Beta" on macOS

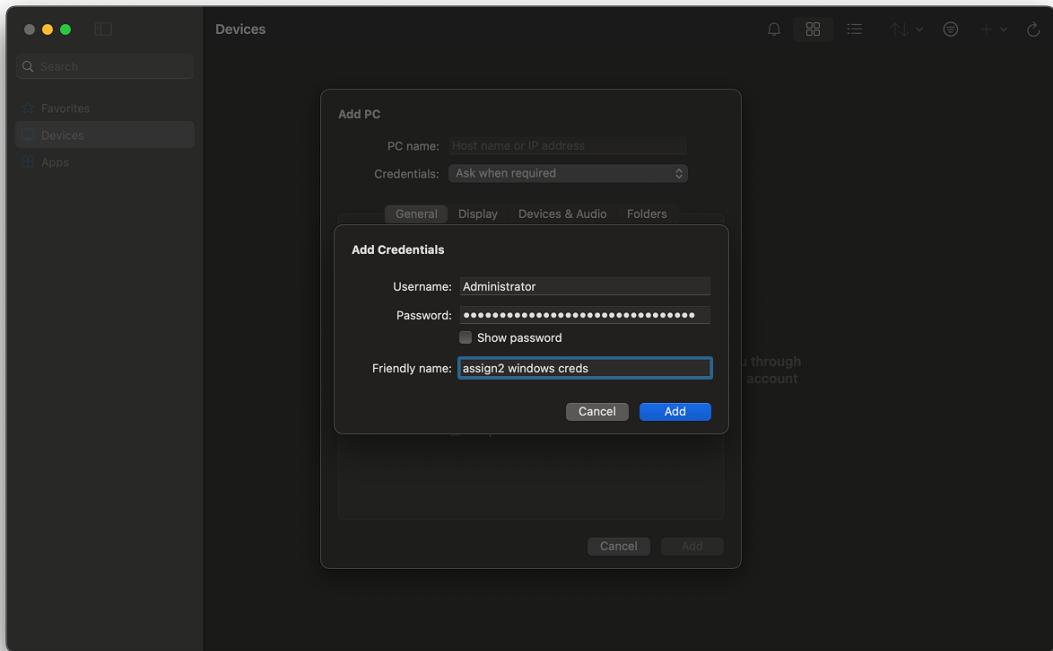


Figure 8: Add Credentials in RDP Client

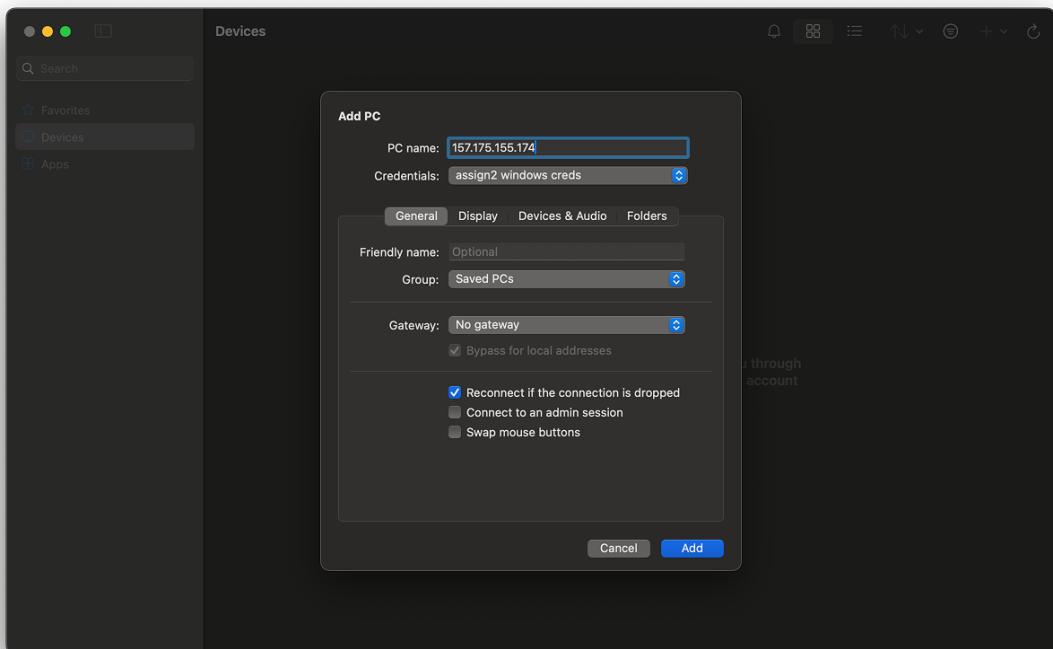


Figure 9: Enter IP Address

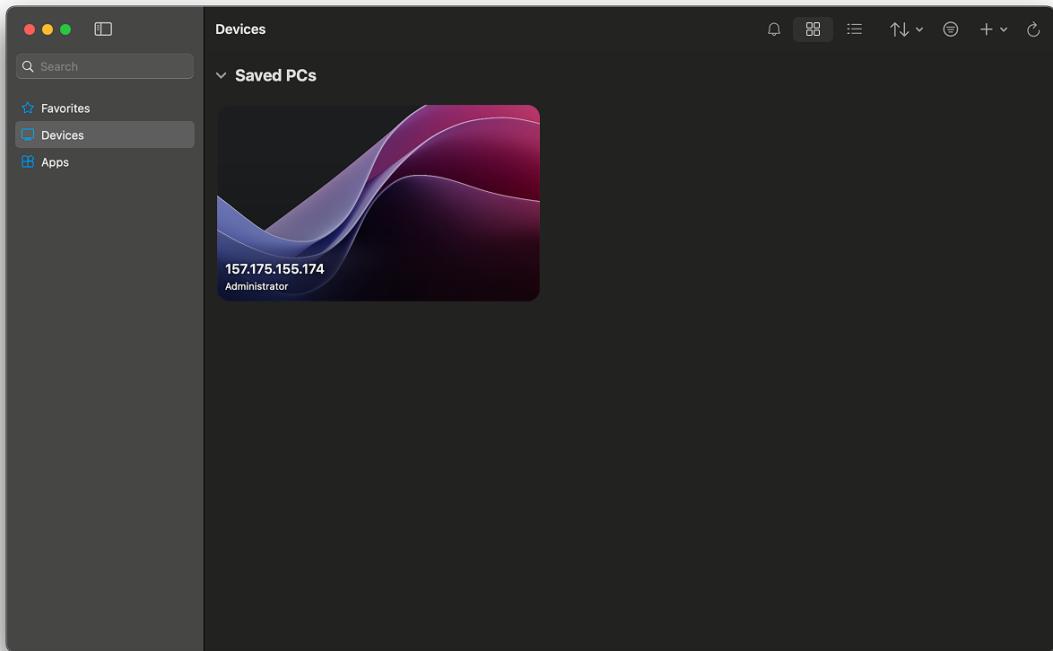


Figure 10: PC Added Successfully

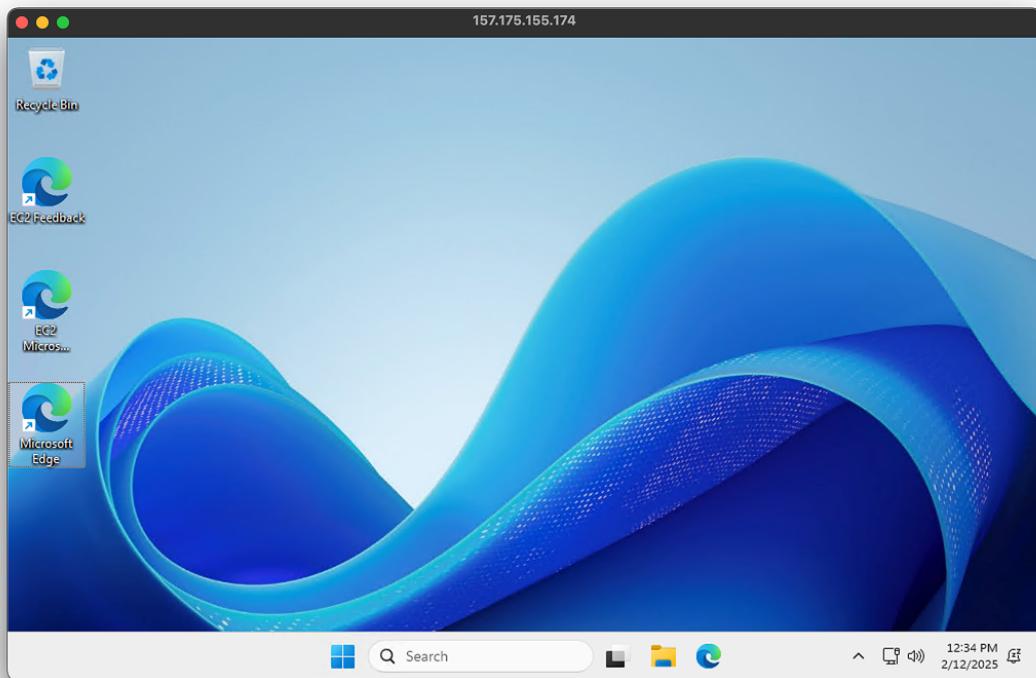


Figure 11: Successfully Connected

2 Part B: Create Snapshots / Backups/Amazon Machine Image (AMI) Creation

Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP	IPv6 IPs	Monitoring
t3.micro	3/3 checks passed	View alarms	me-south-1a	ec2-16-24-194-41.me-s...	16.24.194.41	16.24.194.41	-	disabled
i-02db885652372eadc (assign2)	3/3 checks passed	View alarms	me-south-1a	ec2-157-175-155-174....	157.175.155.174	-	-	disabled

Figure 12: Right Click to Create Image

The screenshot shows the 'Create image' configuration page for an EC2 instance. The instance ID is i-02db885652372eadc (assign2). The 'Image name' is set to 'assign2 windows image'. The 'Image description' field is empty. The 'Reboot instance' checkbox is checked. Under 'Instance volumes', there is one volume listed: an EBS volume of size 30 GB, type General Purpose SSD, IOPS 3000, throughput 1000, delete on termination enabled, and encrypted. An information box states that Amazon EC2 creates a snapshot of each volume during the process. The 'Tags - optional' section is empty. The bottom navigation bar includes CloudShell, Feedback, and links to 2025 AWS terms and cookie preferences.

Figure 13: AMI Creation Options

The screenshot shows the 'Amazon Machine Images (AMIs)' page. The left sidebar is expanded to show 'Instances' and 'Images'. The main table lists one AMI: 'assign2 windows image' with AMI ID ami-0b7861e00f654cbe4. The table columns include Name, AMI name, AMI ID, Source, Owner, Visibility, and Status. The status is 'Pending'. Below the table, the 'AMI ID: ami-0b7861e00f654cbe4' details page is shown. It has tabs for Details, Permissions, Storage, and Tags. A note about enabling fast launch is present. The 'Details' tab displays the following data:

AMI ID	Image type	Platform details	Root device type
ami-0b7861e00f654cbe4	machine	Windows	EBS
AMI name	Owner account ID	Architecture	Usage operation
assign2 windows image	[REDACTED]	x86_64	RunInstances:0002

Figure 14: AMI Created Successfully

3 Part C: How to host a static website on AWS S3

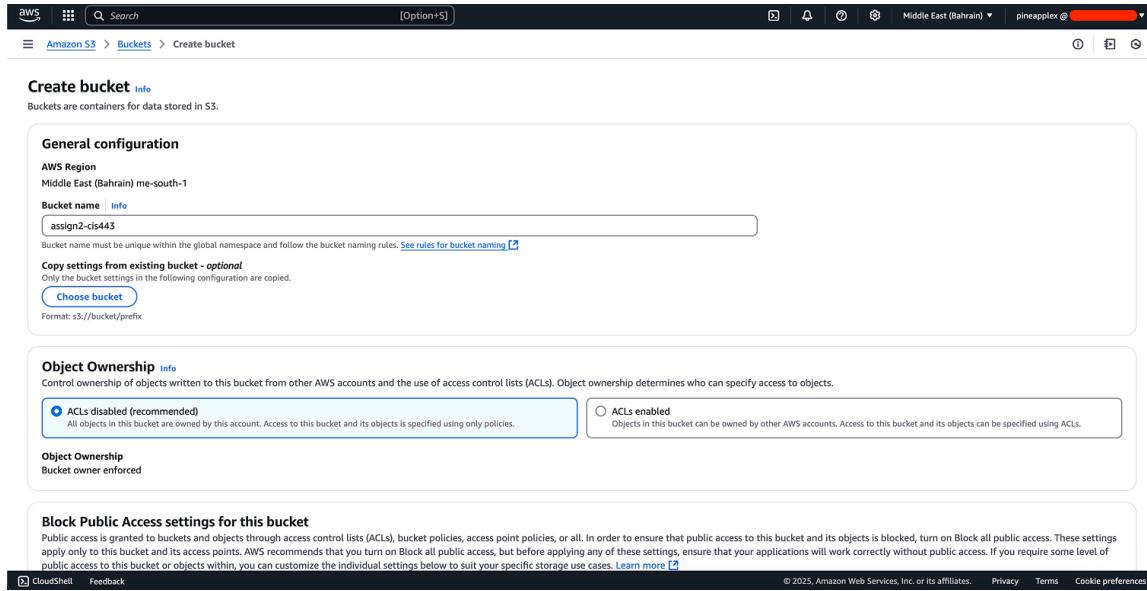


Figure 15: Bucket Creation 1

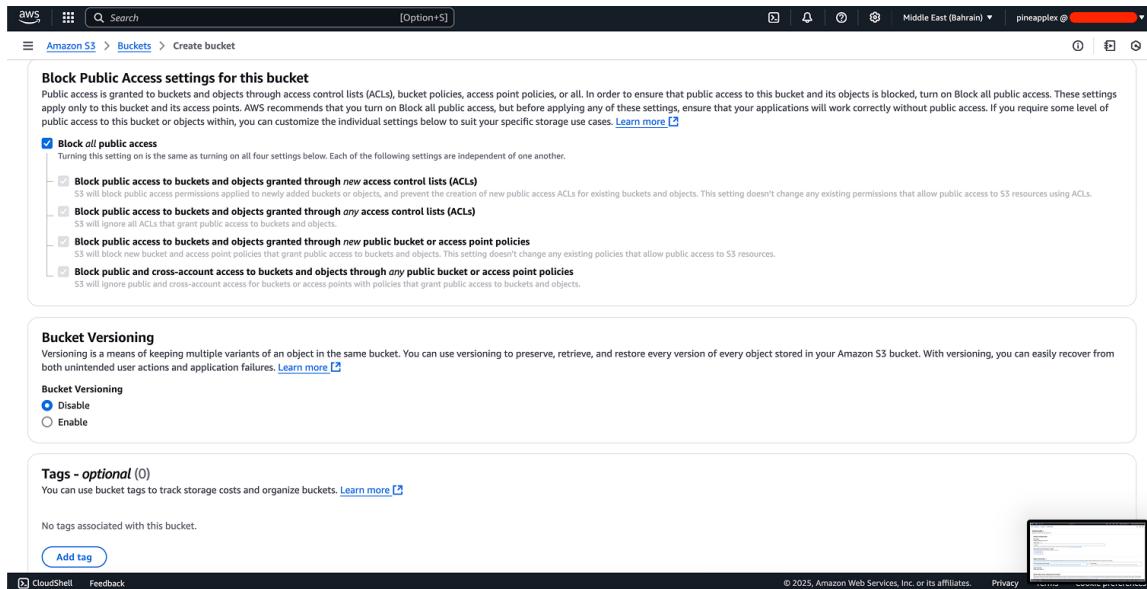


Figure 16: Bucket Creation 2

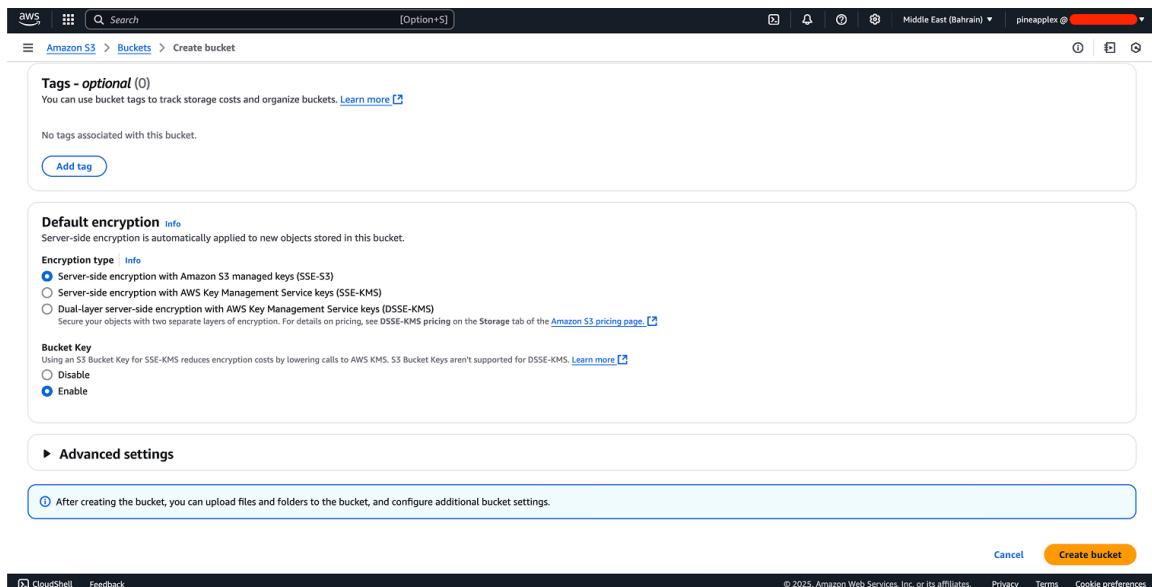


Figure 17: Bucket Creation 3

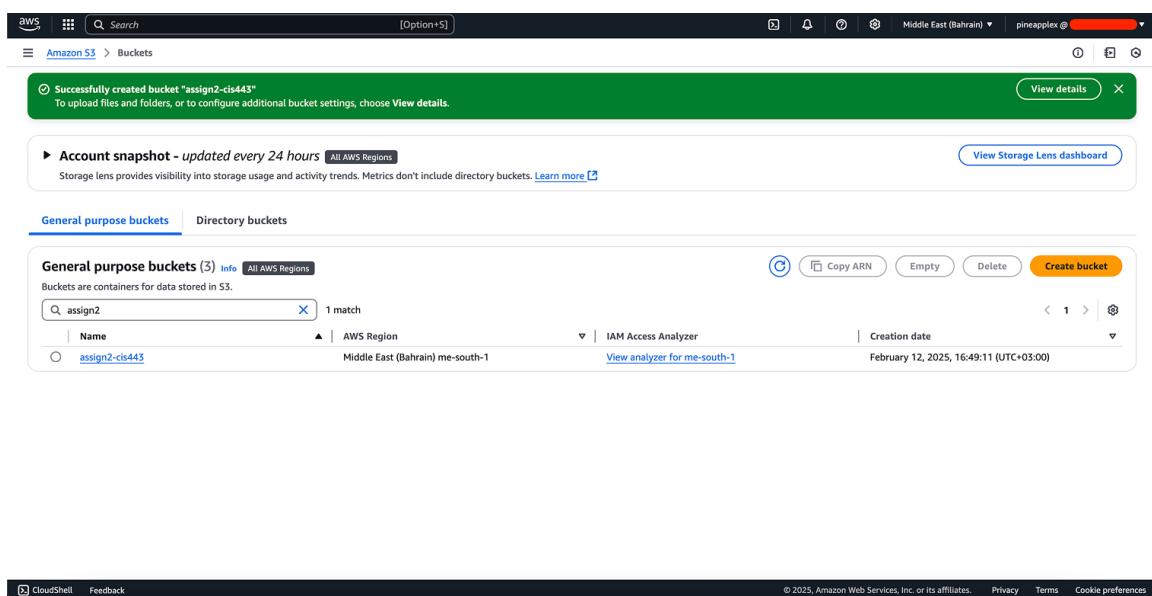


Figure 18: Created Bucket Successfully

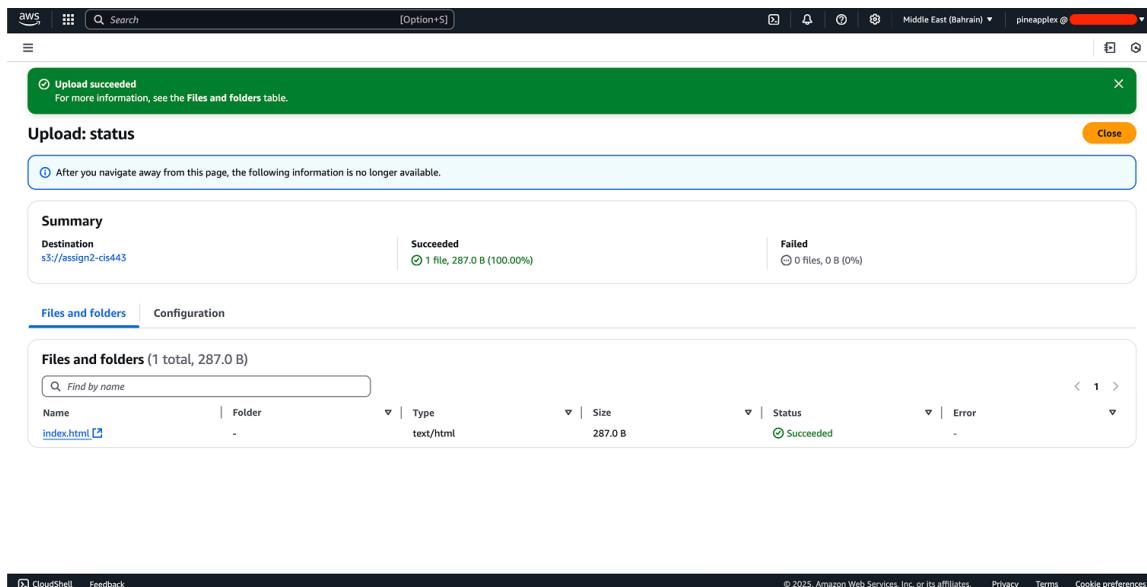
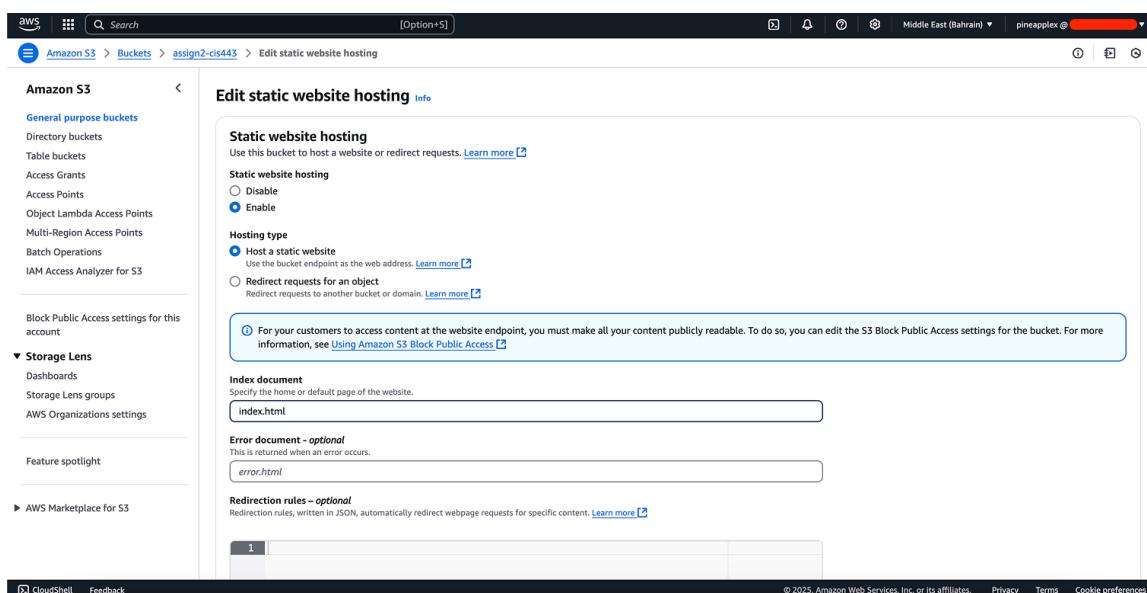
Figure 19: Uploaded `index.html` File Successfully

Figure 20: Static Web Hosting Setting Page

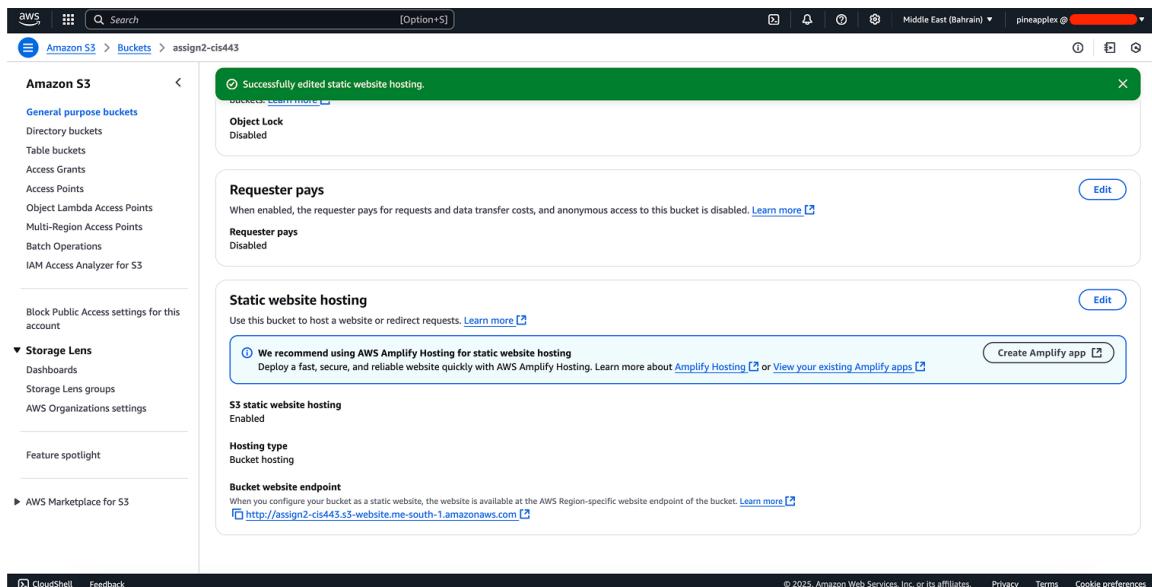


Figure 21: Static Website Hosting Enabled

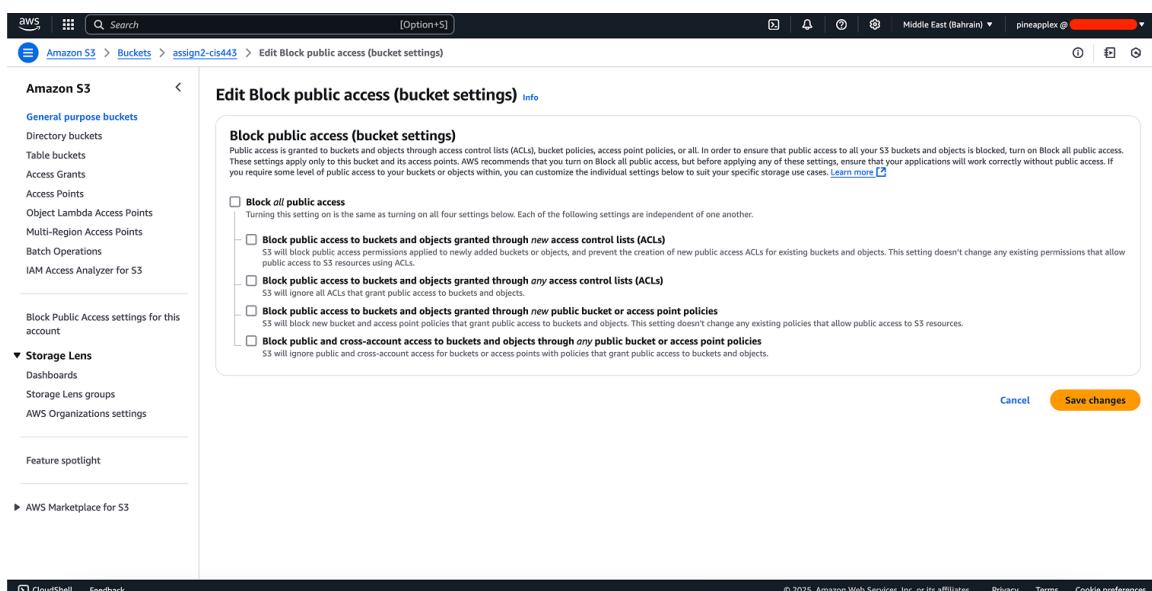


Figure 22: Disabled "Block Public Access" Setting

The screenshot shows the AWS S3 console with the bucket 'assign2-cis443' selected. The left sidebar includes options like General purpose buckets, Storage Lens, and Feature spotlight. The main content area is titled 'Permissions overview' under the 'Permissions' tab. A green success message at the top states: 'Successfully edited Block Public Access settings for this bucket.' Below this, the 'Block public access (bucket settings)' section shows the status as 'Off'. A link to 'Individual Block Public Access settings for this bucket' is present. Further down, the 'Bucket policy' section indicates 'No policy to display.' At the bottom right, there are 'Edit' and 'Delete' buttons.

Figure 23: Success Page for "Block Public Access" Being Disabled

The screenshot shows the 'Edit Object Ownership' page for the 'assign2-cis443' bucket. The left sidebar is identical to Figure 23. The main content area is titled 'Edit Object Ownership'. Under the 'Object Ownership' section, there are two radio button options: 'ACLs disabled (recommended)' (unchecked) and 'ACLs enabled' (checked). A note below states: 'Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using only policies.' A warning message below advises against enabling ACLs if individual object access control is needed. Another note explains that enabling ACLs turns off the bucket owner enforced setting. A checkbox 'I acknowledge that ACLs will be restored.' is checked. The 'Object Ownership' section also includes 'Bucket owner preferred' (radio button checked) and 'Object writer' (radio button unchecked). A note at the bottom says: 'If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads.' At the bottom right, there are 'Cancel' and 'Save changes' buttons.

Figure 24: Object Ownership Setting Change to Enable ACL

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with various AWS services like General purpose buckets, Storage Lens, and Feature spotlight. The main area shows the 'assign2-cis443' bucket with one object named 'index.html'. A context menu is open over this object, specifically the 'Actions' dropdown. The 'Make public using ACL' option is highlighted.

Figure 25: S3 Static Website - Make Public Menu Item

This screenshot shows the 'Make public' dialog box. It contains a warning message: '⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.' Below this, there's a table titled 'Specified objects' showing one object: 'index.html'. At the bottom right of the dialog, there are 'Cancel' and 'Make public' buttons, with 'Make public' being the larger, orange-colored button.

Figure 26: S3 Static Website - Make Public Page

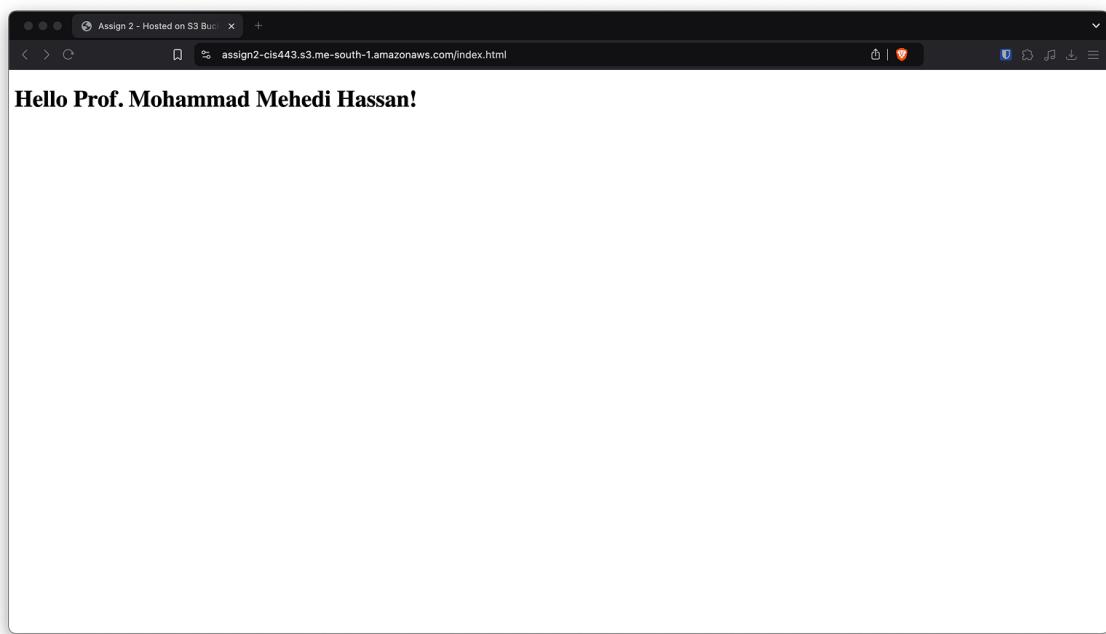


Figure 27: Successfully hosted static website showing "Hello World"