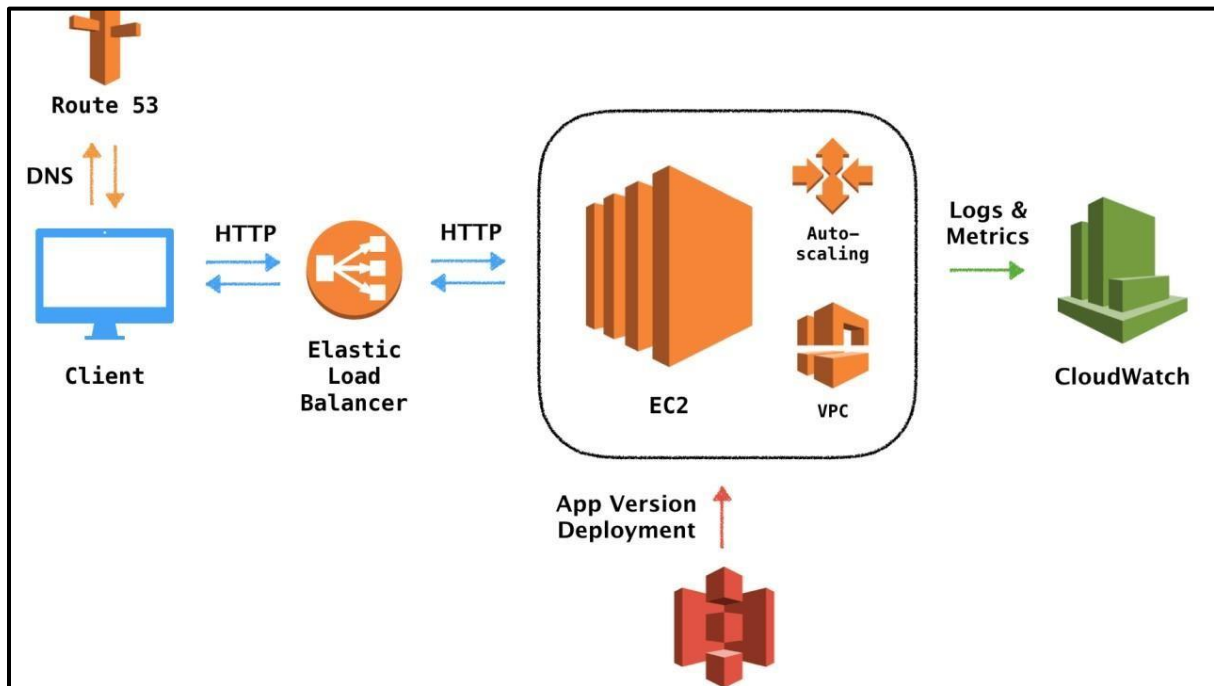


## DEPLOY A STATIC WEBSITE ON AWS



### Services Used: -

- **EC2-Instance:** - The EC2 instance is the compute resource that will run your application or website.
- **Amazon S3 Bucket:** - S3 buckets are used to store static assets such as images, videos, backups, and other files that your application might need.
- **IAM:** - IAM roles and policies are used to grant the necessary permissions for EC2 instances to access S3 buckets and other AWS services.
- **Route 53:** - Route 53 is used to manage DNS records, enabling you to route traffic to your load balancer.

- **Load Balancer:** - A load balancer distributes incoming traffic across multiple EC2 instances to ensure high availability and reliability.
- **Target Group:** - Target groups are used by the load balancer to direct traffic to specific EC2 instances based on health checks and routing rules.
- **Autoscaling Group:** - An Auto Scaling Group ensures that you have the right number of EC2 instances running to handle the load for your application.
- **CloudWatch:** - CloudWatch is used for monitoring and logging. It provides metrics, alarms, and logs to monitor the health and performance of your instances.
- **Launch Template:** - A launch template specifies the configuration for EC2 instances, including the AMI, instance type, key pair, security groups, and IAM roles.
- **AMI:** - AMIs are used to create new EC2 instances with predefined configurations and installed software.
- **Certificate Manager:** - ACM is used to manage SSL/TLS certificates for securing your website or application traffic.

## Procedure: -

### 1. Create an S3 Bucket

First, I created an Amazon S3 bucket to store the static website's contents. This bucket will serve as the primary storage for all the website files.

The screenshot shows the AWS Management Console interface for creating a new S3 bucket. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar, and a keyboard shortcut '[Alt+S]'. The breadcrumb trail indicates the path: 'Amazon S3 > Buckets > Create bucket'. The main heading is 'Create bucket' with an 'Info' link. Below this, a sub-header 'General configuration' is displayed. The 'AWS Region' is set to 'US East (N. Virginia) us-east-1'. Under 'Bucket type', there are two options: 'General purpose' (selected with a radio button) and 'Directory - New' (unselected). The 'General purpose' option includes a description: 'Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.' The 'Directory - New' option includes a description: 'Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.' Below the bucket type selection, the 'Bucket name' field is populated with 'sample-website-bucket'. A note states: 'Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming'. At the bottom, there is a 'Choose bucket' button and a format example: 'Format: s3://bucket/prefix'.

aws Services Search [Alt+S]

Amazon S3 > Buckets > Create bucket

## Create bucket [Info](#)

Buckets are containers for data stored in S3.

### General configuration

AWS Region  
US East (N. Virginia) us-east-1

Bucket type [Info](#)

☒ **General purpose**  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory - New**  
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)  
sample-website-bucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

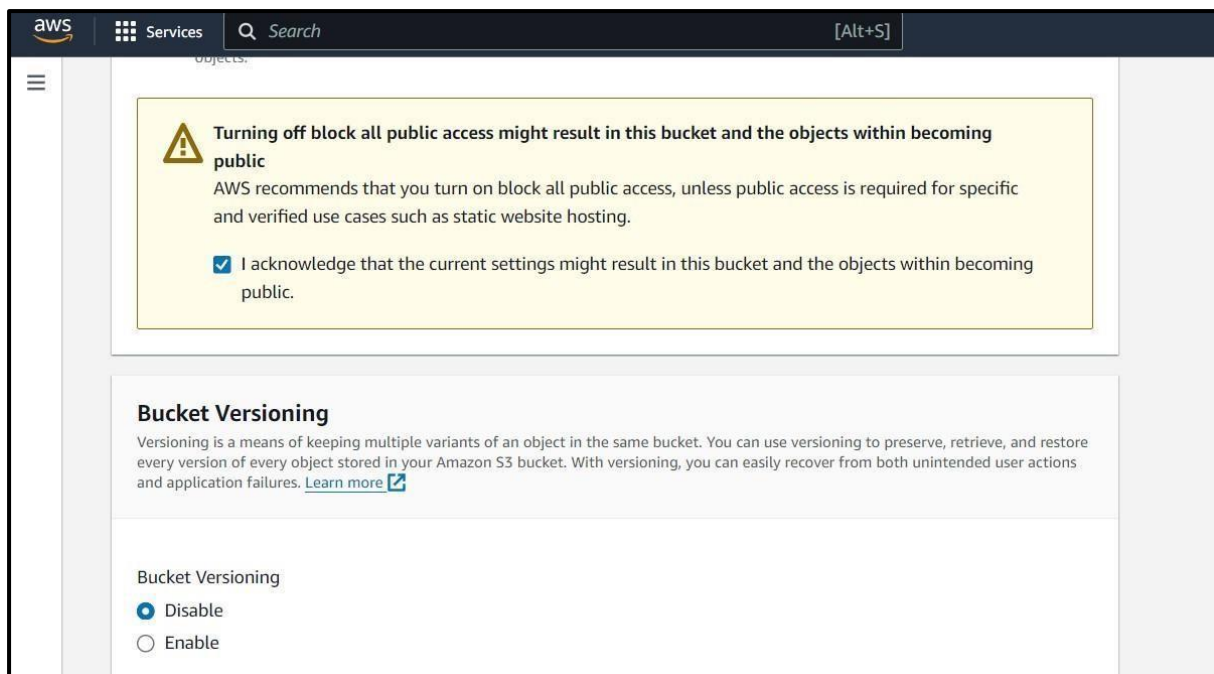
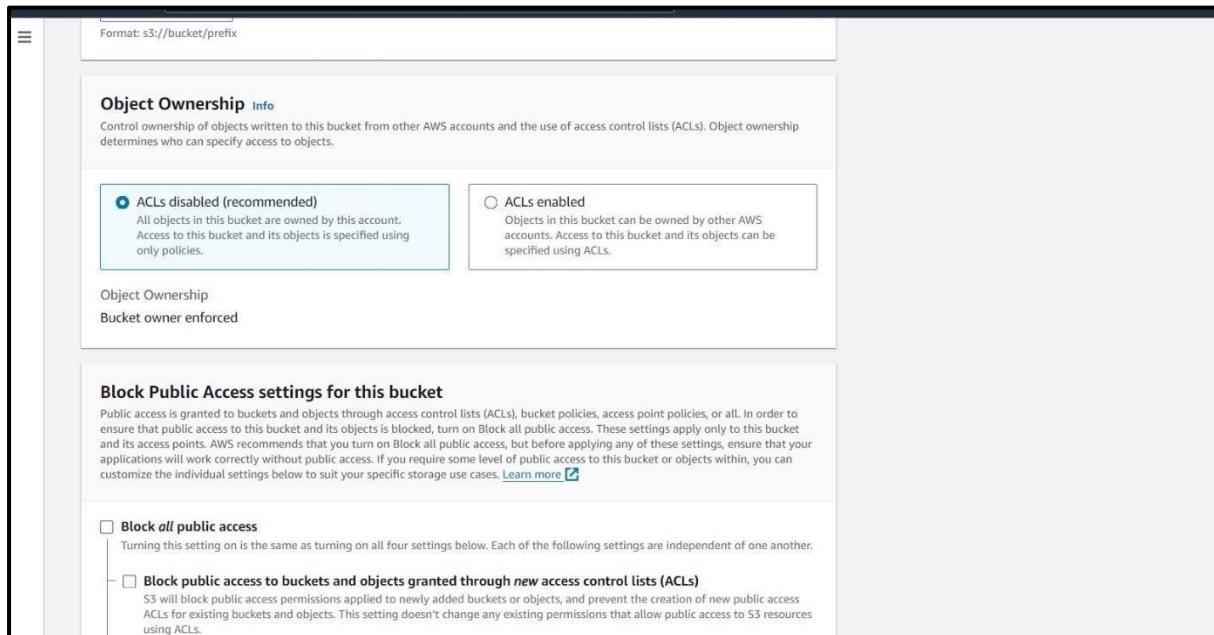
Copy settings from existing bucket - *optional*  
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

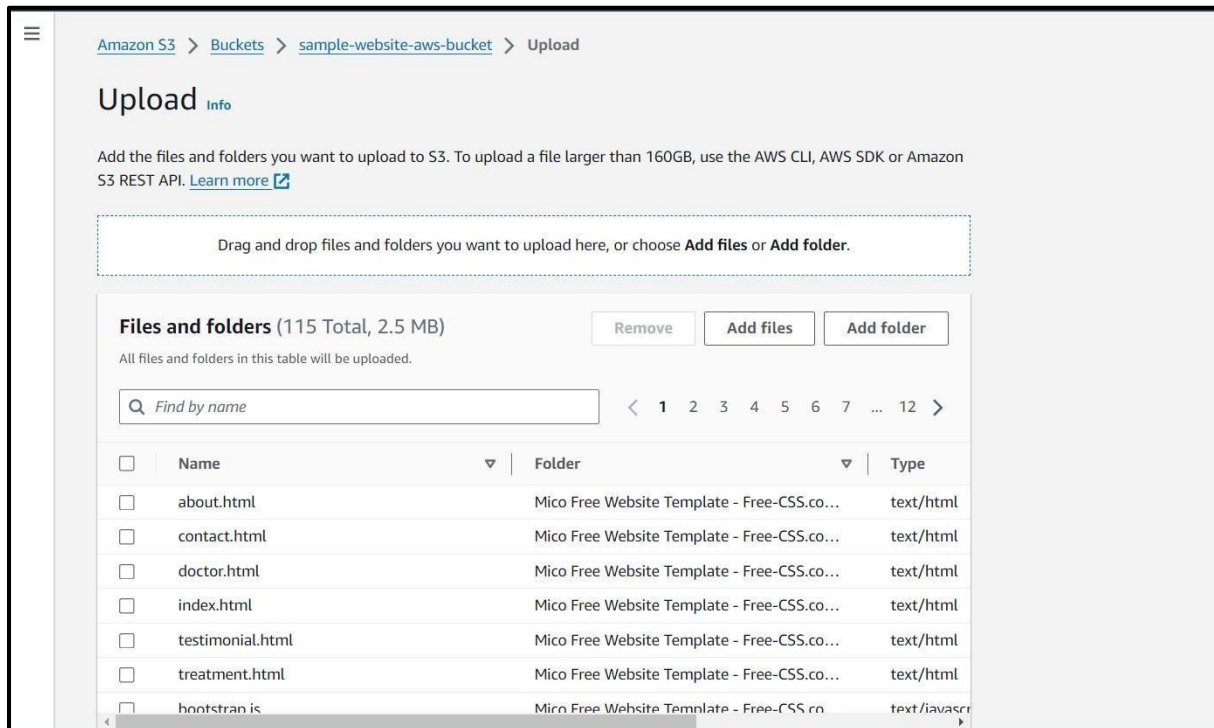
## 2. Enable Public Access

Next, I enabled public access to the bucket. This step is crucial for making the website accessible to the public.



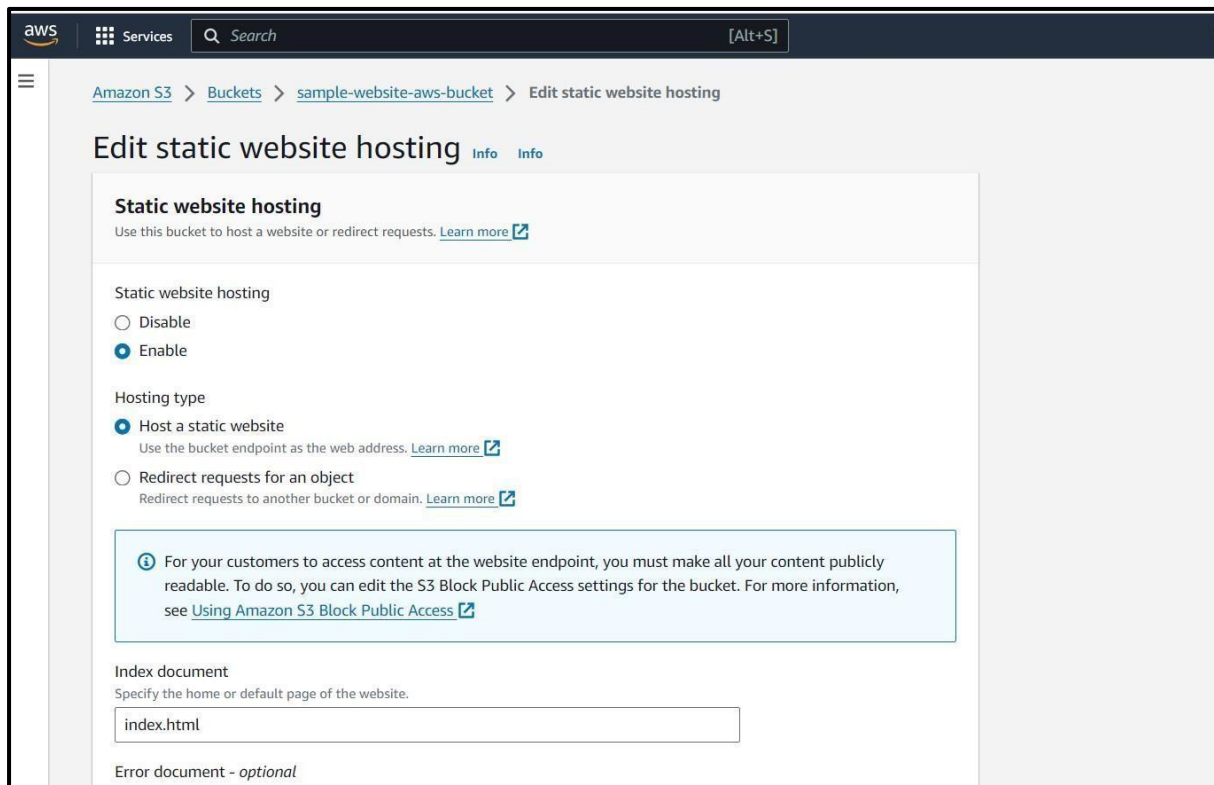
## 3. Upload Website Files

I uploaded the static website files into the newly created S3 bucket. This includes HTML, CSS, JavaScript, and any other assets needed for the website.



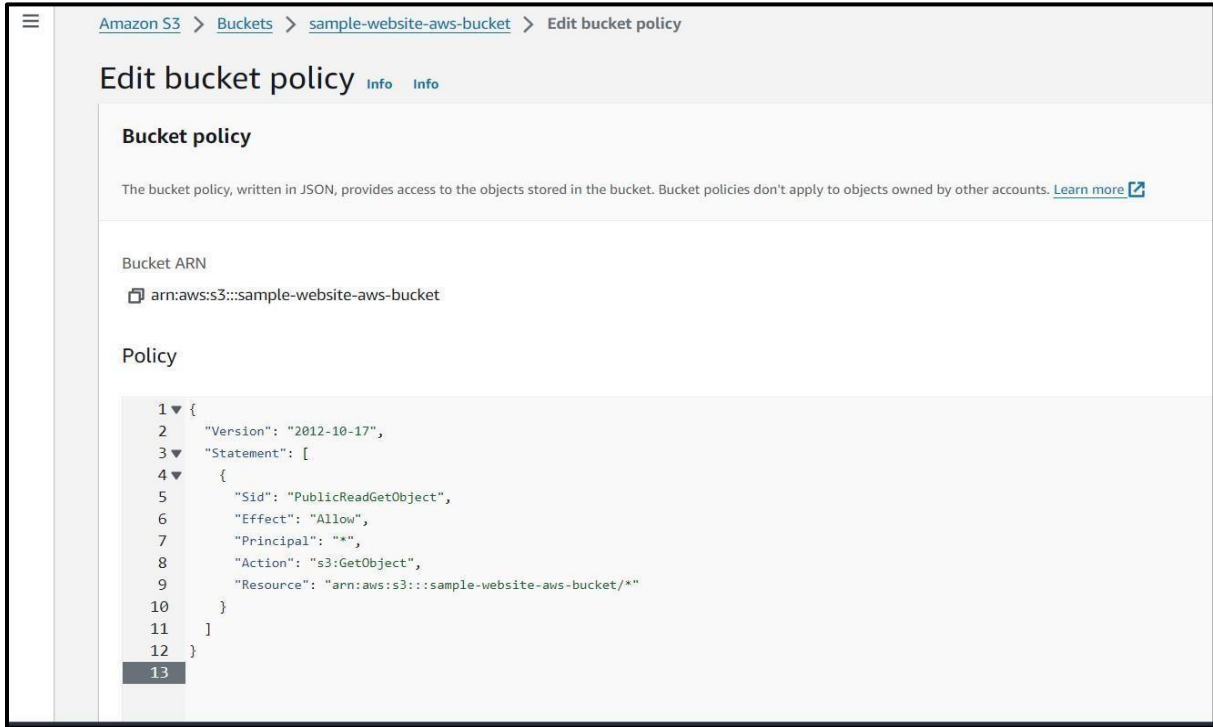
#### 4. Configure Static Website Hosting

In the S3 bucket's properties, I configured static website hosting by specifying the name of the landing page (e.g., index.html) and saved the changes.



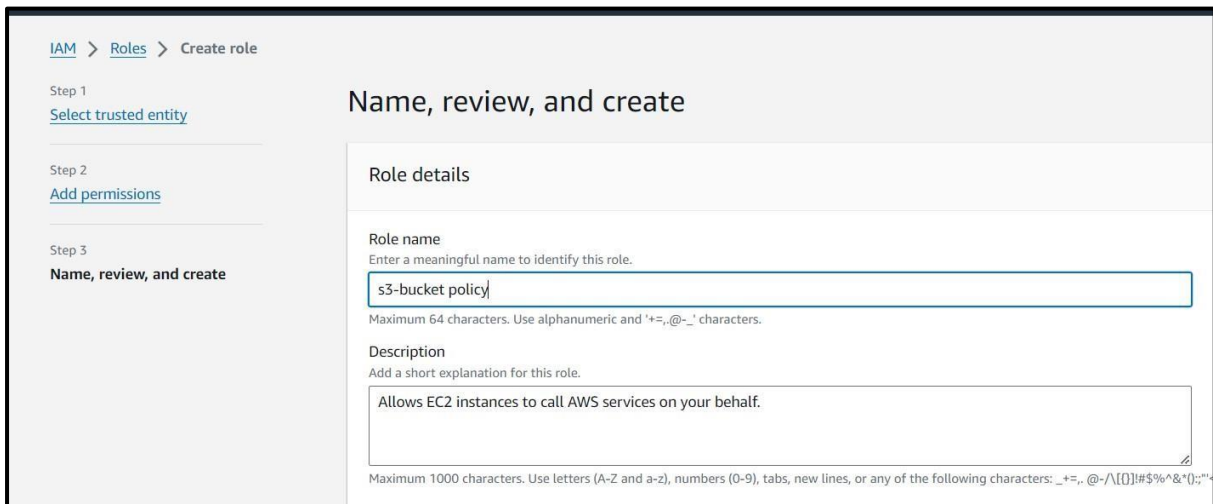
## 5. Edit Bucket Policy

To make the bucket publicly accessible, I edited the bucket policy. This step ensures that users can access the website files stored in the S3 bucket.



## 6. Create an IAM Role

I created an IAM role with an S3 bucket policy to grant necessary permissions for accessing the S3 bucket. This role is essential for managing access control.



Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

## Select trusted entity [Info](#)

### Trusted entity type

☒ **AWS service**  
 Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**  
 Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**  
 Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**  
 Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**  
 Create a custom trust policy to enable others to perform actions in this account.

### Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

☒ EC2

Step 3

Name, review, and create

Choose one or more policies to attach to your new role.

Filter by Type

×

All types

▼

9 matches

Policy name

▲

Type

▼

Description

⋮

<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed	⋮
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	⋮
<input type="checkbox"/>	AmazonS3ObjectLambdaExecutionRol...	AWS managed	⋮
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS managed	⋮
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS managed	⋮
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	⋮
<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Bac...	AWS managed	⋮
<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Res...	AWS managed	⋮
<input type="checkbox"/>	QuickSightAccessForS3StorageManage...	AWS managed	⋮

► Set permissions boundary - optional

Cancel

Previous

Next

## 7. Launch EC2 Instance

An EC2 instance of Amazon Linux 2 was launched, and the previously created IAM role was attached to it for accessing S3 resources.



EC2 > Instances > i-06cc0302684567acd > Modify IAM role

## Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

i-06cc0302684567acd (web-server)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

s3\_bucket\_policy

[Create new IAM role](#)

[Cancel](#) [Update IAM role](#)

## 8. Connect to EC2 Instance

Using x-shell, I connected to the EC2 instance through the .pem file and changed from ec2-user to the root user. I then installed the package manager httpd.

```
run sudo yum update to apply all updates.  
[ec2-user@ip-172-31-29-237 ~]$ sudo su  
[root@ip-172-31-29-237 ec2-user]# cd  
[root@ip-172-31-29-237 ~]# sudo yum update -y  
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd  
Resolving Dependencies
```

```
Complete!  
[root@ip-172-31-29-237 ~]# sudo yum install httpd -y
```

```
Complete!  
[root@ip-172-31-29-237 ~]# sudo systemctl start httpd  
[root@ip-172-31-29-237 ~]# sudo systemctl enable httpd  
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
```

## 9. Install AWS CLI

AWS CLI was installed on the EC2 instance using the command: `sudo yum install aws-cli -y`

```
[root@ip-172-31-29-237 ~]# sudo yum install aws-cli -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
```

#### 10. Synchronize S3 Bucket with EC2

The contents of the S3 bucket were synchronized with the EC2 instance's `/var/www/html` directory using: `aws s3 sync s3://sample-website-aws-bucket /var/www/html`

```
[root@ip-172-31-18-29 ~]# aws s3 ls s3://sample-website-aws-bucket
```

```
[root@ip-172-31-19-136 ~]# sudo aws s3 sync s3://my-aws-sample-website /var/www/html
download: s3://my-aws-sample-website/about.html to ../var/www/html/about.html
download: s3://my-aws-sample-website/contact.html to ../var/www/html/contact.html
download: s3://my-aws-sample-website/css/font-awesome.min.css to ../var/www/html/css/font-awesome.min.css
download: s3://my-aws-sample-website/css/bootstrap.css to ../var/www/html/css/bootstrap.css
download: s3://my-aws-sample-website/css/style.css to ../var/www/html/css/style.css
```

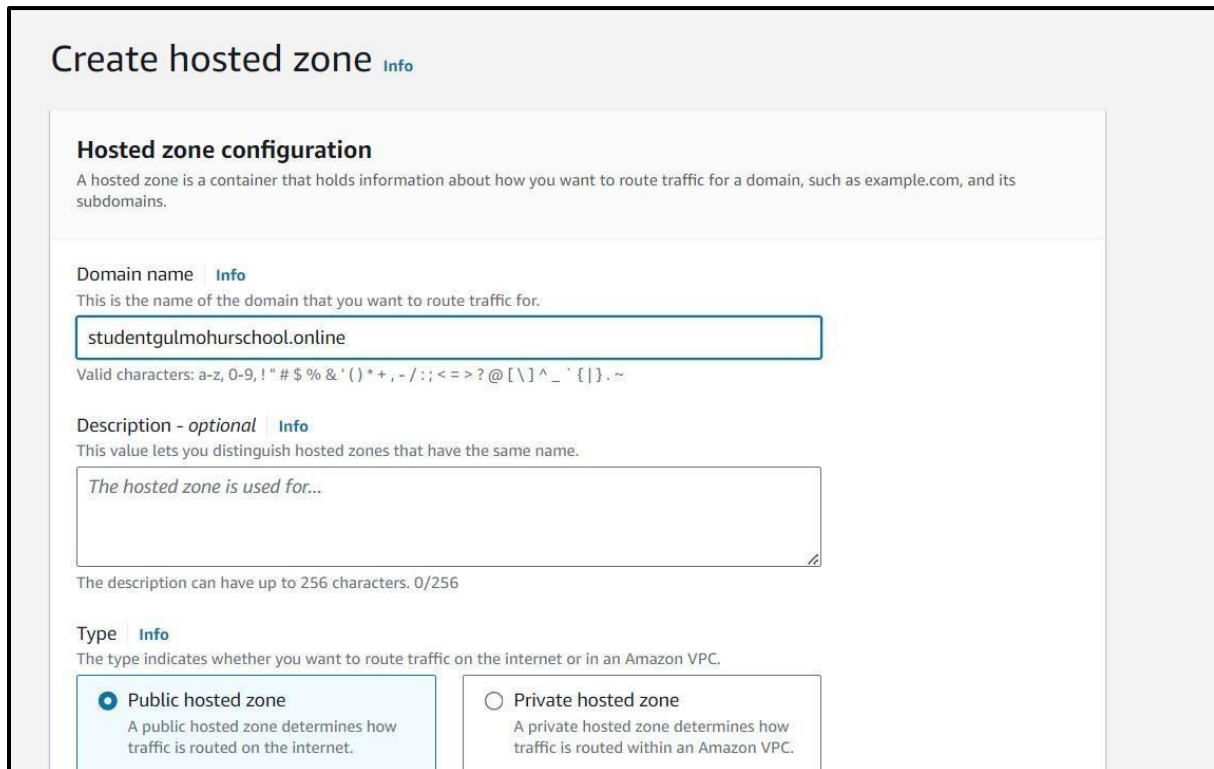
#### 11. Start the Web Server The server was started on the EC2 instance using: `sudo systemctl start httpd.`

#### 12. Enable Server on Boot

To ensure the server starts on boot, I enabled it with: `sudo systemctl start httpd,`  
`sudo systemctl enable httpd.`

### 13. Create a Hosted Zone in Route 53

A hosted zone was created in Route 53 for the domain name associated with the website.



The screenshot shows the 'Create hosted zone' page in the AWS Route 53 console. The page has a title 'Create hosted zone' with an 'Info' link. Below the title is a section titled 'Hosted zone configuration' with a descriptive paragraph: 'A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.' The configuration section contains three main fields: 1. 'Domain name' with an 'Info' link and a text box containing 'studentgulmohurschool.online'. Below the text box is a note: 'This is the name of the domain that you want to route traffic for.' and a list of 'Valid characters: a-z, 0-9, ! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } . ~'. 2. 'Description - optional' with an 'Info' link and a text box containing 'The hosted zone is used for...'. Below the text box is a note: 'This value lets you distinguish hosted zones that have the same name.' and a character count: 'The description can have up to 256 characters. 0/256'. 3. 'Type' with an 'Info' link and two radio button options: 'Public hosted zone' (selected) and 'Private hosted zone'. Each option has a brief description: 'A public hosted zone determines how traffic is routed on the internet.' and 'A private hosted zone determines how traffic is routed within an Amazon VPC.' respectively.

### 14. Update Domain Nameservers

The nameservers of the domain's hosting website were updated with the nameservers provided by AWS to direct traffic to AWS.

### 15. Request SSL Certificate

A certificate was requested from ACM for the domain name studentgulmohurschool.online to enable HTTPS encryption.

[AWS Certificate Manager](#) > [Certificates](#) > [Request certificate](#) > Request public certificate

## Request public certificate

**Domain names**  
Provide one or more domain names for your certificate.

Fully qualified domain name [Info](#)

[Add another name to this certificate](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

### 16. Request Wildcard SSL Certificate

Another certificate was requested for "\*.studentgulmohurschool.online" to include all subdomains.

[AWS Certificate Manager](#) > [Certificates](#) > [Request certificate](#) > Request public certificate

## Request public certificate

**Domain names**  
Provide one or more domain names for your certificate.

Fully qualified domain name [Info](#)

[Add another name to this certificate](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

## 17. Create CNAME Record

A CNAME record was created in Route 53 to map the domain to the load balancer's DNS name for better traffic management.

The screenshot shows the AWS Route 53 console. On the left, the 'Records (1/5)' tab is active, displaying a table of records. The record '\_942f37e...' is selected. On the right, the 'Record details' panel shows the configuration for this CNAME record.

Record ...	Type	Routin...	Differ...	Alias	Value/Route t
<input type="checkbox"/> studentgu...	A	Simple	-	Yes	dualstack.my-le
<input type="checkbox"/> studentgu...	NS	Simple	-	No	ns-1871.awsdn ns-1396.awsdn ns-25.awsdns- ns-1003.awsdn
<input type="checkbox"/> studentgu...	SOA	Simple	-	No	ns-1871.awsdn
<input type="checkbox"/> *.studentg...	A	Simple	-	Yes	dualstack.my-le
<input checked="" type="checkbox"/> _942f37e...	CNAME	Simple	-	No	_bce633547a3

**Record details**

Edit record

Record name  
\_942f37e84718d1b74bd0279f089f32ac.studentgulmoh

Record type  
CNAME

Value  
\_bce633547a3e74f84836dd54fe820a98.sdgjtdhdh  
z.acm-validations.aws.

Alias  
No

TTL (seconds)  
300

Routing policy  
Simple

## 18. Create Target Group

A target group was created for managing traffic distribution.

The screenshot shows the AWS EC2 console 'my-target-group' page. It displays the target group's details, including its ARN, target type (Instance), protocol (HTTP), and port (80). It also shows the target group's health status, with 1 healthy target and 0 unhealthy targets.

EC2 > Target groups > my-target-group

my-target-group

Details

arn:aws:elasticloadbalancing:us-east-1:851725447202:targetgroup/my-target-group/42eb05b3e46f1b5a

Target type	Protocol : Port	Protocol version	VPC
Instance	HTTP: 80	HTTP1	vpc-060f3ee2e08b11887
IP address type	Load balancer		
IPv4	my-load-balancer-sample-website		

1	1	0	0	0	0
Total targets	Healthy	Unhealthy	Unused	Initial	Draining
	0 Anomalous				

► Distribution of targets by Availability Zone (AZ)

Select values in this table to see corresponding filters applied to the Registered targets table below.

## 19. Create and Configure Load Balancer

A load balancer was created and attached to the target group. The ACM certificate was also attached, and both HTTP and HTTPS listeners were configured.

### ► How Application Load Balancers work

#### Basic configuration

**Load balancer name**  
Name must be unique within your AWS account and can't be changed after the load balancer is created.

my-load-balancer-new

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

**Scheme** [Info](#)  
Scheme can't be changed after the load balancer is created.

☒ **Internet-facing**  
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

☐ **Internal**  
An internal load balancer routes requests from clients to targets using private IP addresses. Compatible with the **IPv4** and **Dualstack** IP address types.

**IP address type** [Info](#)  
Select the type of IP addresses that your subnets use. Public IPv4 addresses have an additional cost.

☒ **IPv4**  
Includes only IPv4 addresses.

☐ **Dualstack**  
Includes IPv4 and IPv6 addresses.

☐ **Dualstack without public IPv4**  
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

### Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Remove

Protocol

Port

Default action

[Info](#)

HTTP ▼

:

80

1-65535

Forward to

my-target-group

Target type: Instance, IPv4

HTTP ▼

⌂

Create target group

**Listener tags - optional**  
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add listener tag

You can add up to 50 more tags.

▼ Listener HTTPS:443

Remove

Protocol

Port

Default action

[Info](#)

HTTPS ▼

:

443

1-65535

Forward to

my-target-group

Target type: Instance, IPv4

HTTP ▼

⌂

Create target group



## Secure listener settings [Info](#)

### Security policy [Info](#)

Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. [Compare security policies](#)

Security category

All security policies

Policy name

ELBSecurityPolicy-TLS13-1-2-2021-06 (recommended)

### Default SSL/TLS server certificate

The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), or import a certificate. This certificate will automatically be added to your listener certificate list.

Certificate source

☒ From ACM

☐ From IAM

☐ Import certificate

Certificate (from ACM)

The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.

studentgulmohurschool.online

18fc9eee-5e3d-4ab3-ab0e-d45f7...



[Request new ACM certificate](#)

### Client certificate handling [Info](#)

Client certificates are used to make authenticated requests to remote servers. [Learn more](#)

☐ Mutual authentication (mTLS)

Mutual TLS (Transport Layer Security) authentication offers two-way peer authentication. It adds a layer of security over TLS and allows your services to verify the client that's making the connection.

## my-load-balancer-new



Actions

### ▼ Details

Load balancer type

Application

Status

Active

VPC

[vpc-013c8a74b0b1087b8](#)

IP address type

IPv4

Scheme

Internet-facing

Hosted zone

Z35SXDOTRQ7X7K

Availability Zones

[subnet-0b023a29616e5eb6d](#) us-east-1e (use1-az3)

[subnet-005a2beee33b779a8](#) us-east-1c (use1-az4)

[subnet-0e996c7292f1f7ec0](#) us-east-1d (use1-az6)

[subnet-07a1e214791a939b5](#) us-east-1b (use1-az2)

[subnet-02dce3de4b7f2d2f](#) us-east-1f (use1-az5)

[subnet-01f0cd2bc2896f1e9](#) us-east-1a (use1-az1)

Date created

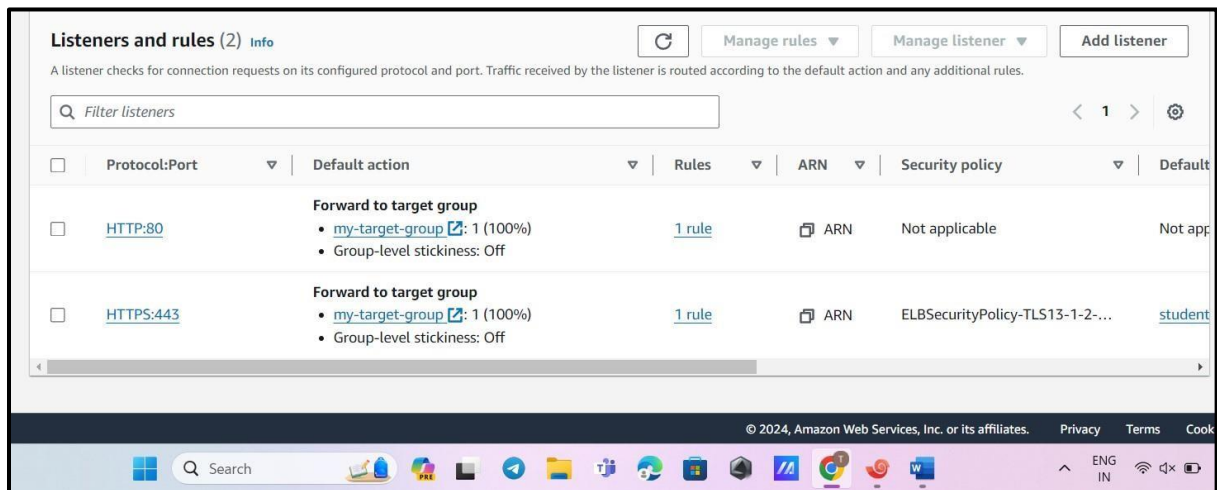
May 19, 2024, 23:08 (UTC+05:30)

Load balancer ARN

[arn:aws:elasticloadbalancing:us-east-1:818056053291:loadbalancer/app/my-load-balancer-new/42b6cb40f5814a13](#)

DNS name [Info](#)

[my-load-balancer-new-1108685440.us-east-1.elb.amazonaws.com](#) (A Record)



## 20. Redirect HTTP to HTTPS

HTTP requests were redirected to HTTPS for secure access.

### Listener configuration

The listener will be identified by the protocol and port.

**Protocol**  
Used for connections from clients to the load balancer.  

HTTP

**Port**  
The port on which the load balancer is listening for connections.  

80

1-65535

**Default actions** [Info](#)  
The default action is used if no other rules apply. Choose the default action for traffic on this listener.

**Routing actions**

☐ Forward to target groups

☒ Redirect to URL

☐ Return fixed response

**Redirect to URL** [Info](#)  
Redirect client requests from one URL to another. You cannot redirect HTTPS to HTTP. To avoid a redirect loop, you must modify at least one of the following components: protocol, port, hostname or path. Components that you do not modify retain their original values.

**URI parts**

**Full URL**

**Protocol**  
Used for connections from clients to the load balancer.  

HTTPS

**Port**  
The port on which the load balancer is listening for connections.  

443

1-65535 or to retain the original port enter #{port}



Listeners and rules (2) <a href="#">Info</a>						
A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.						
<input type="text" value="Filter listeners"/> <span>&lt; 1 &gt; ⚙</span>						
Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS	
<a href="#">HTTP:80</a>	<b>Redirect to HTTPS://#{host}:443/#{path}?#</b> {query} • Status code: HTTP_301	<a href="#">1 rule</a>	ARN	Not applicable	Not applicable	
<a href="#">HTTPS:443</a>	<b>Forward to target group</b> • <a href="#">target-group</a> : 1 (100%) • Group-level stickiness: Off	<a href="#">1 rule</a>	ARN	ELBSecurityPolicy-TLS13-1-2-...	<a href="#">*.studentgulmohu</a>	

## 21. Add SSL Certificate for Subdomains

The SSL certificate for subdomains was added to the HTTPS port to ensure secure connections for subdomains.

<a href="#">EC2</a> > <a href="#">Load balancers</a> > <a href="#">my-load-balancer-sample-website</a> > <a href="#">HTTPS:443 listener</a>		
<h2>HTTPS:443 <a href="#">Info</a></h2> <span>⌂</span> <span>Actions</span>		
<b>▼ Details</b> A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.		
Protocol:Port <b>HTTPS:443</b>	Load balancer <a href="#">my-load-balancer-sample-website</a>	Default SSL/TLS certificate <a href="#">studentgulmohurschoolonline</a> (Certificate ID: <a href="#">631df929-4098-40ad-ab6e-6a84c7d85</a> )
Default actions <b>Forward to target group</b> • <a href="#">my-target-group</a> : 1 (100%) • Group-level stickiness: Off		
Listener ARN <code>arn:aws:elasticloadbalancing:us-east-1:851725447202:listener/app/my-load-balancer-sample-website/17cef2d1214363ff/90f1d5f622c56920</code>		

Listener certificates for SNI (2) <a href="#">Info</a>							
Additional certificates support Server Name Indication (SNI). This enables the load balancer to support multiple domains on the same port and provide a different certificate for each domain.							
<input type="text" value="Filter certificates"/> <span>&lt; 1 &gt; ⚙</span>							
<input type="checkbox"/>	Certificate ID	Name or domain	Status	SAN	Expiration	Service	ARN
<input type="checkbox"/>	78be7c62-ee49-4...	*.studentgulmohursch...	Valid	<a href="#">1</a>	June 24, 2025, 05:29 (...)	<a href="#">ACM</a>	arn:aws:acm:us...
<input type="checkbox"/>	631df929-4098-4...	studentgulmohurscho...	Valid	<a href="#">1</a>	June 24, 2025, 05:29 (...)	<a href="#">ACM</a>	arn:aws:acm:us...

## 22. Create Route 53 Records

Records were created in Route 53 for both the root domain and subdomains to distribute the load, choosing alias as Classic and Application Load Balancer.

**Quick create record** [Switch to wizard](#)

▼ Record 1 [Delete](#)

Record name [Info](#)

studentgulmohurschool.online

Record type [Info](#)

A – Routes traffic to an IPv4 address and some AWS resources ▼

Keep blank to create a record for the root domain.

☒ Alias

Route traffic to [Info](#)

Alias to Application and Classic Load Balancer ▼

US East (N. Virginia) ▼

X

Alias hosted zone ID: Z35SXDOTRQ7X7K

Routing policy [Info](#)

Simple routing ▼

Evaluate target health ☒ Yes

[Add another record](#)

[Route 53](#) > [Hosted zones](#) > [studentgulmohurschool.online](#) > Create record

**Create record** [Info](#)

**Quick create record** [Switch to wizard](#)

▼ Record 1 [Delete](#)

Record name [Info](#)

.studentgulmohurschool.online

Record type [Info](#)

A – Routes traffic to an IPv4 address and some AWS resources ▼

Keep blank to create a record for the root domain.

☒ Alias

Route traffic to [Info](#)

Alias to Application and Classic Load Balancer ▼

US East (N. Virginia) ▼

X

Alias hosted zone ID: Z35SXDOTRQ7X7K

Routing policy [Info](#)

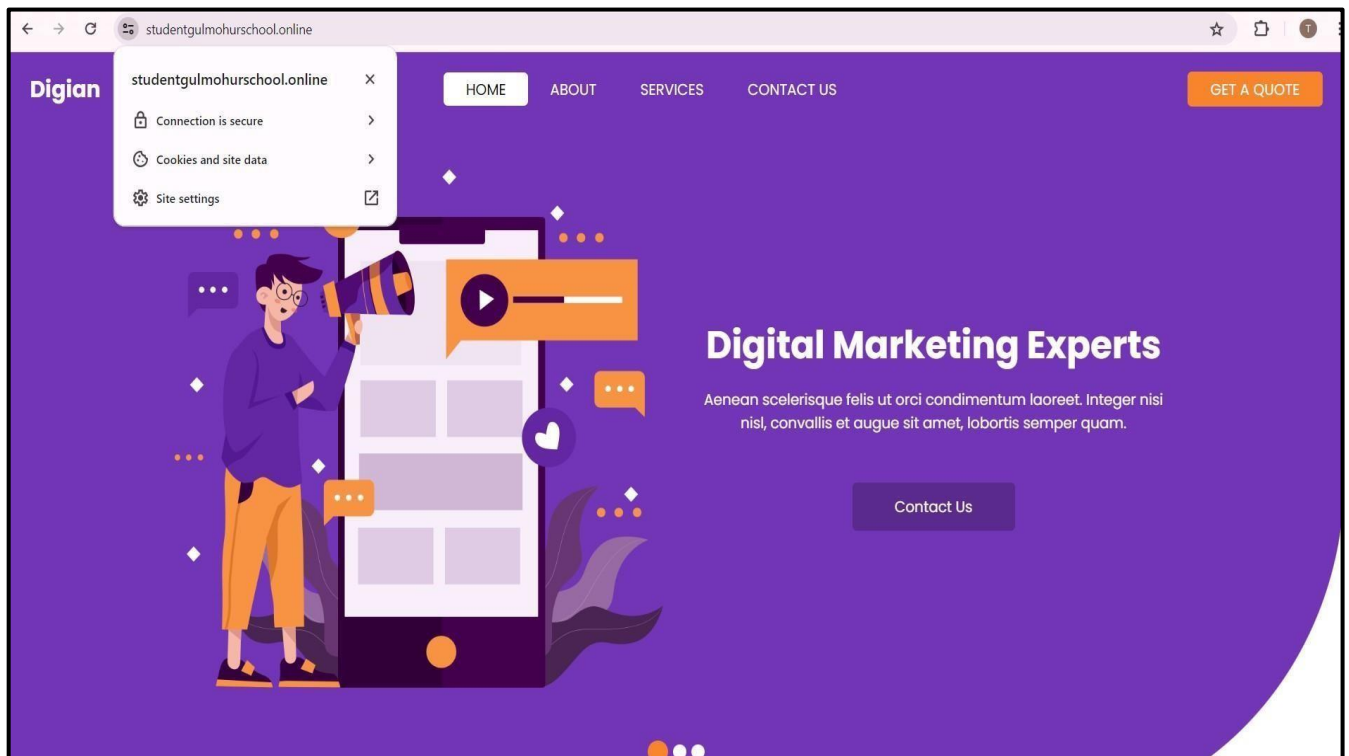
Simple routing ▼

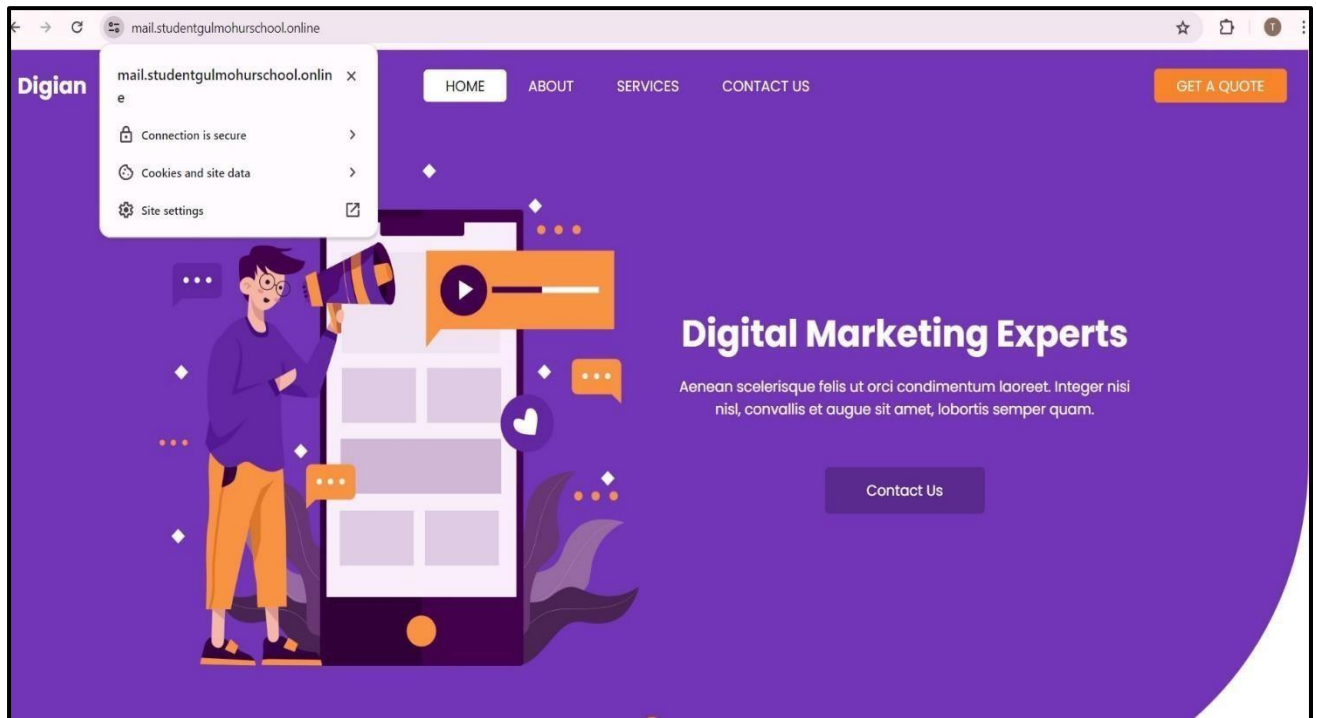
Evaluate target health ☒ Yes

Records (5)   DNSSEC signing   Hosted zone tags (0)								
<div> <div>Records (5) Info</div> <div> <div>↻</div> <div>Delete record</div> <div>Import zone file</div> <div>Create record</div> </div> </div> <div>Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.</div> <div> <div>Q Filter records by property or value</div> <div>Type ▼</div> <div>Routing policy ▼</div> <div>Alias ▼</div> <div>&lt; 1 &gt;</div> <div>⚙</div> </div>								
<input type="checkbox"/>	Record ... ▼	Type ▼	Routin... ▼	Differ... ▼	Alias ▼	Value/Route traffic to ▼	TTL (s... ▼	Health ... ▼
<input type="checkbox"/>	studentgu...	A	Simple	-	Yes	dualstack.my-load-balancer-...	-	-
<input type="checkbox"/>	studentgu...	NS	Simple	-	No	ns-1871.awsdns-41.co.uk. ns-1396.awsdns-46.org. ns-25.awsdns-03.com. ns-1003.awsdns-61.net.	172800	-
<input type="checkbox"/>	studentgu...	SOA	Simple	-	No	ns-1871.awsdns-41.co.uk. a...	900	-
<input type="checkbox"/>	*.studentg...	A	Simple	-	Yes	dualstack.my-load-balancer-...	-	-
<input type="checkbox"/>	_942f37e...	CNAME	Simple	-	No	_bce633547a3e74f84836dd...	300	-

## 23. Access the Website

The website was accessed using the root domain (studentgulmohurschool.online) and sub-domain (mail.studentgulmohurschool.online). Both connections were secured.





## 24. Create an Image to be used in auto-scaling group

An image of the EC2 instance was created where the web server is configured. A template was launched from this image.

EC2 > Instances > i-0f6a7f2539f62f7ac > Create image

### Create image Info

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

Instance ID  
i-0f6a7f2539f62f7ac (web-server-1)

Image name  
image-1  
Maximum 127 characters. Can't be modified after creation.

Image description - optional  
image-1  
Maximum 255 characters.

No reboot  
☐ Enable

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/...	Create new snapshot fr...	8	EBS General Purpose S...	3000		<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

## 25. Launch Template

A new security group was created for the template, allowing HTTP, HTTPS, and SSH. An auto-scaling group was then created from the template, selecting all availability zones and attaching it to the load balancer with the target group.

## Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

### Launch template name and description

Launch template name - *required*

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '\*', '@'.

Template version description

Max 255 chars

Auto Scaling guidance [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

☒ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

► **Template tags**

► **Source template**

## ▼ Network settings [Info](#)

### Subnet [Info](#)

Don't include in launch template ▼

 [Create new subnet](#)

When you specify a subnet, a network interface is automatically added to your template.

### Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Select existing security group

☒ Create security group

#### Security group name - *required*

Template-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and . \_ - / ( ) # , @ [ ] + = & ; { } ! \$ \*

#### Description - *required* [Info](#)

Allow HTTPS, HTTP, SSH

### VPC [Info](#)

vpc-060f3ee2e08b11887  
172.31.0.0/16

(default) ▼



Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
ssh ▼	TCP	22
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere ▼	<input type="text" value="Add CIDR, prefix list or security"/>	<input type="text" value="e.g. SSH for admin desktop"/>
<input type="text" value="0.0.0.0/0"/> X		
▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)		<a href="#">Remove</a>
Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
HTTP ▼	TCP	80
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere ▼	<input type="text" value="Add CIDR, prefix list or security"/>	<input type="text" value="e.g. SSH for admin desktop"/>
<input type="text" value="0.0.0.0/0"/> X		
▼ Security group rule 3 (TCP, 443, 0.0.0.0/0)		<a href="#">Remove</a>
Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
HTTPS ▼	TCP	443
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere ▼	<input type="text" value="Add CIDR, prefix list or security"/>	<input type="text" value="e.g. SSH for admin desktop"/>

## 26.Create an auto-scaling group.

Created an auto-scaling group with all availability zones. Attach it with the load balancer.



EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1

Choose launch template

Step 2

Choose instance launch options

Step 3 - optional

Configure advanced options

Step 4 - optional

Configure group size and scaling

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

Choose launch template [Info](#)

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name

Enter a name to identify the group.

my-auto-scaling-group

Must be unique to this account in the current Region and no more than 255 characters.

Launch template [Info](#)

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

My-template-1

Configure advanced options - optional [Info](#)

Integrate your Auto Scaling group with other services to distribute network traffic across multiple servers using a load balancer or to establish service-to-service communications using VPC Lattice. You can also set options that give you more control over health check replacements and monitoring.

Load balancing [Info](#)

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

☐ No load balancer

Traffic to your Auto Scaling group will not be fronted by a load balancer.

☒ Attach to an existing load balancer

Choose from your existing load balancers.

☐ Attach to a new load balancer

Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

☒ Choose from your load balancer target groups

This option allows you to attach Application, Network, or Gateway Load Balancers.

☐ Choose from Classic Load Balancers

### Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

☒ Choose from your load balancer target groups  
This option allows you to attach Application, Network, or Gateway Load Balancers.

☐ Choose from Classic Load Balancers

#### Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups



my-target-group | HTTP  
Application Load Balancer: my-load-balancer-sample-website



## 26. Set Scaling Policies

The desired, minimum, and maximum capacity for the servers was set up. A new instance was launched from the template, appearing in the EC2 dashboard.

#### Desired capacity

Specify your group size.

1

### Scaling [Info](#)

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

#### Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

##### Min desired capacity

1

Equal or less than desired capacity

##### Max desired capacity

3

Equal or greater than desired capacity

### Automatic scaling - optional

Choose whether to use a target tracking policy [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

☒ No scaling policies  
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

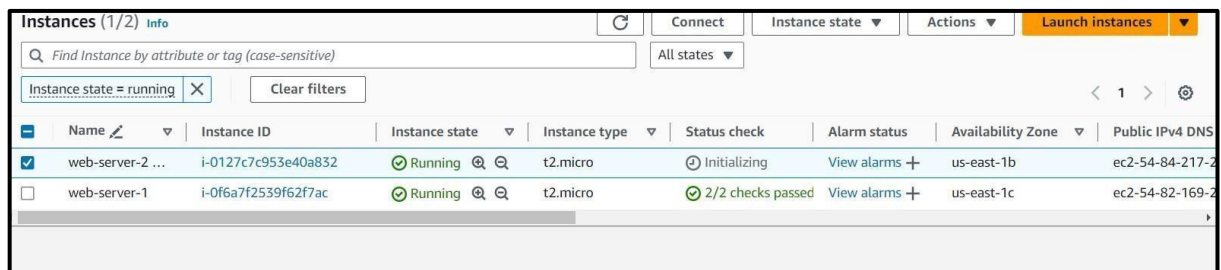
☐ Target tracking scaling policy  
Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

27. After creating the auto-scaling group  
the template chosen, appeared in the  
dashboard.

, a new instance was  
launched from

EC2

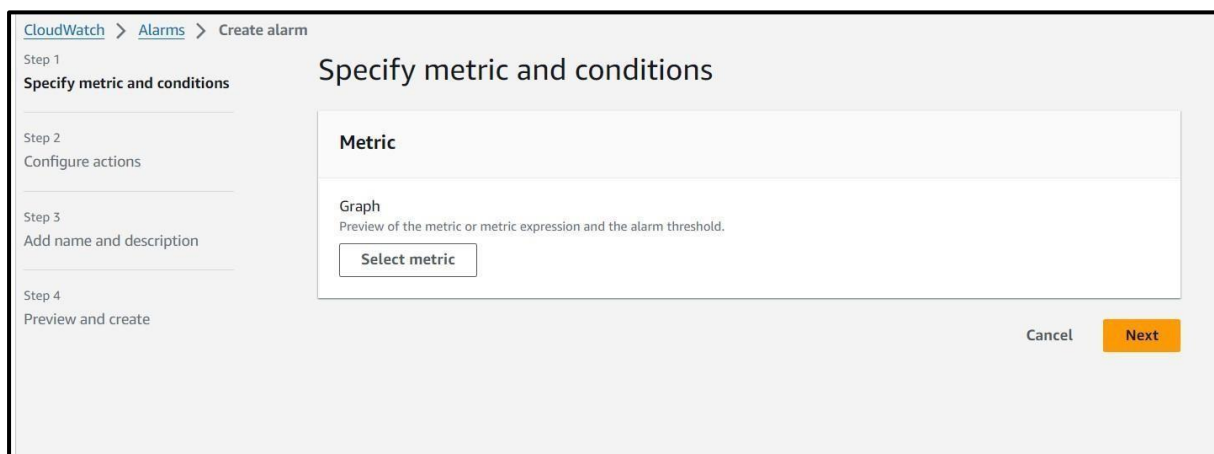
28. Create CloudWatch



	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input checked="" type="checkbox"/>	web-server-2 ...	i-0127c7c953e40a832	Running	t2.micro	Initializing	View alarms +	us-east-1b	ec2-54-84-217-2
<input type="checkbox"/>	web-server-1	i-0f6a7f2539f62f7ac	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c	ec2-54-82-169-2

## Alarms

CloudWatch alarms were created based on the CPU utilization metrics of the instances. If CPU utilization was  $\geq 50\%$ , new instances were launched. If  $< 40\%$ , instances were terminated to meet the desired and minimum capacity.



CloudWatch > Alarms > Create alarm

Step 1  
Specify metric and conditions

Step 2  
Configure actions

Step 3  
Add name and description

Step 4  
Preview and create

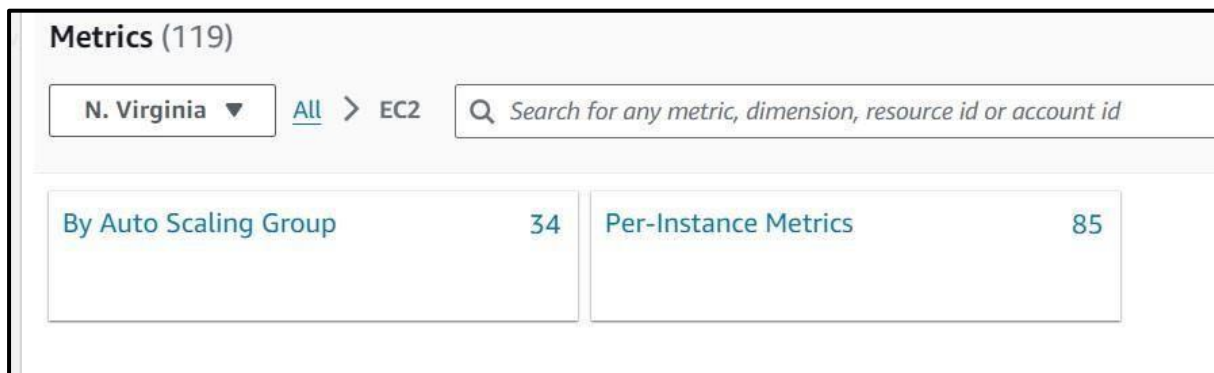
Specify metric and conditions

Metric

Graph  
Preview of the metric or metric expression and the alarm threshold.

Select metric

Cancel Next



Metrics (119)	
N. Virginia	All > EC2
Search for any metric, dimension, resource id or account id	
By Auto Scaling Group	34
Per-Instance Metrics	85

## Conditions

### Threshold type



Static

Use a value as a threshold



Anomaly detection

Use a band as a threshold

### Whenever CPUUtilization is...

Define the alarm condition.



Greater

> threshold



Greater/Equal

>= threshold



Lower/Equal

<= threshold



Lower

< threshold

### than...

Define the threshold value.

50

Must be a number

► Additional configuration

Cancel

Next

## Conditions

### Threshold type



Static

Use a value as a threshold



Anomaly detection

Use a band as a threshold

### Whenever CPUUtilization is...

Define the alarm condition.



Greater

> threshold



Greater/Equal

>= threshold



Lower/Equal

<= threshold



Lower

< threshold

### than...

Define the threshold value.

40

Must be a number

► Additional configuration

Cancel

Next

## 29. Attach Policies to Autoscaling Group

Two dynamic policies were created in the auto-scaling group and attached to the CloudWatch alarms.

### Create dynamic scaling policy

Policy type

Simple scaling ▼

Scaling policy name

scale-out-policy

CloudWatch alarm

Choose an alarm that can scale capacity whenever:

scale-out-alarm ▼

↻

[Create a CloudWatch alarm](#)

breaches the alarm threshold: CPUUtilization >= 50 for 1 consecutive periods of 60 seconds for the metric dimensions:

AutoScalingGroupName = my-auto-group

Take the action

Add ▼

1

capacity units ▼

And then wait

20

seconds before allowing another scaling activity

Cancel

Create

EC2 > Auto Scaling groups > my-auto-scaling-group

## Create dynamic scaling policy

Policy type  
Simple scaling

Scaling policy name  
scale-in-policy

CloudWatch alarm  
Choose an alarm that can scale capacity whenever:  
scale-in-alarm

[Create a CloudWatch alarm](#)

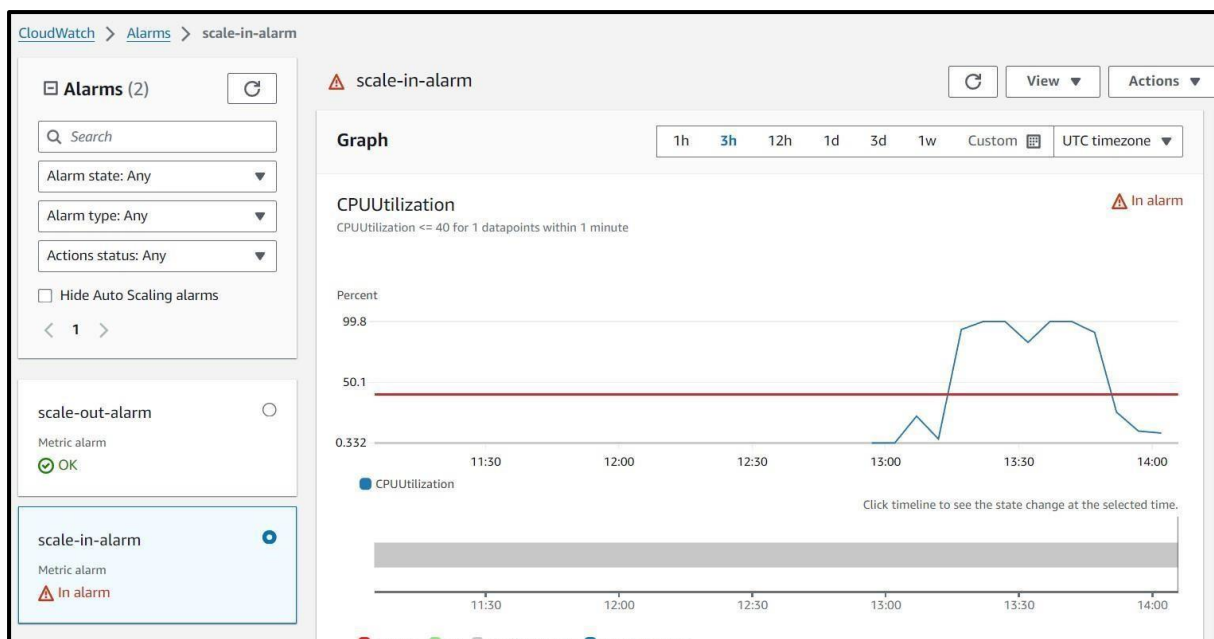
breaches the alarm threshold: CPUUtilization <= 40 for 1 consecutive periods of 60 seconds for the metric dimensions:

AutoScalingGroupName = my-auto-group

Take the action  
Remove 1 capacity units

And then wait  
20 seconds before allowing another scaling activity

30. As per the CPU, Utilisation, the alarms changed from **Insufficient data** -> **OK** -> **In-alarm** state. New instances were added and removed as per the CPU utilisation.



**Problems:**

The SSL certificate was initially issued only for "\*. studentgulmohurschool.online," covering all subdomains but not the root domain "studentgulmohurschool.online."

**Troubleshooting:**

I requested a new SSL certificate covering both the root domain and its subdomains. After obtaining the updated SSL certificate, the website became securely accessible via HTTPS, and HTTP requests were automatically redirected to HTTPS. An A type record was created in Route 53 to associate both the root domain and subdomains with the alias as Application and Classic Load Balance.

**Conclusion:**

By following these detailed steps, you can deploy a static website on AWS, ensuring it's secure, scalable, and efficiently managed. This comprehensive guide should help you navigate through the process seamlessly.