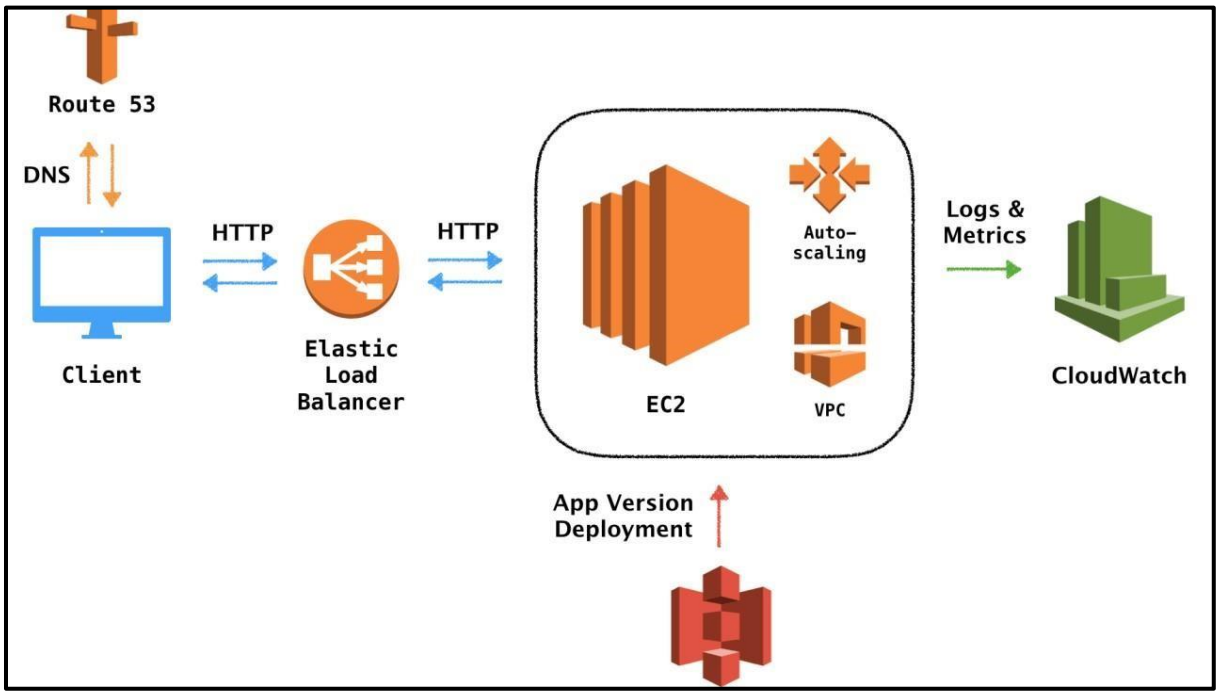
DEPLOY A STATIC WEBSITE ON AWS



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.

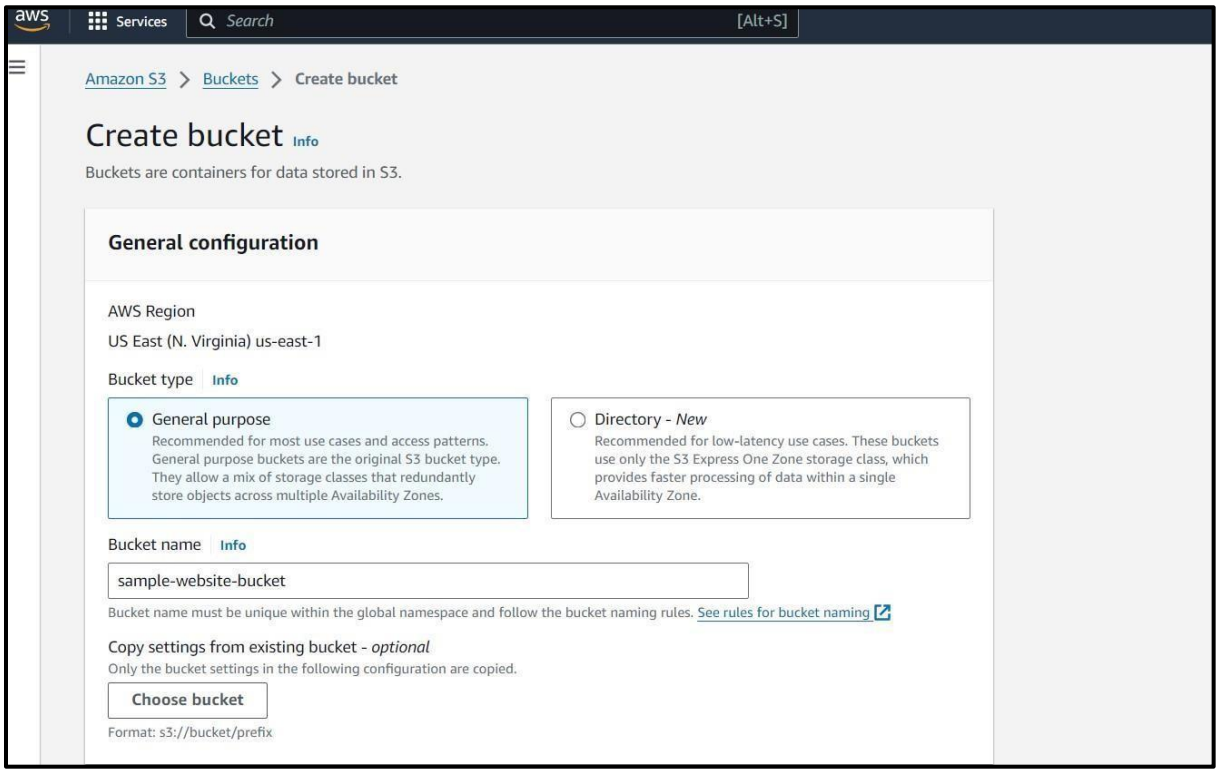
- **AMI: -** AMIs are used to create new EC2 instances with predefined configurations and installed software.

- **Certificate Manager: -** ACM is used to manage SSL/TLS certificates for securing your website or application traffic.

Procedure: -

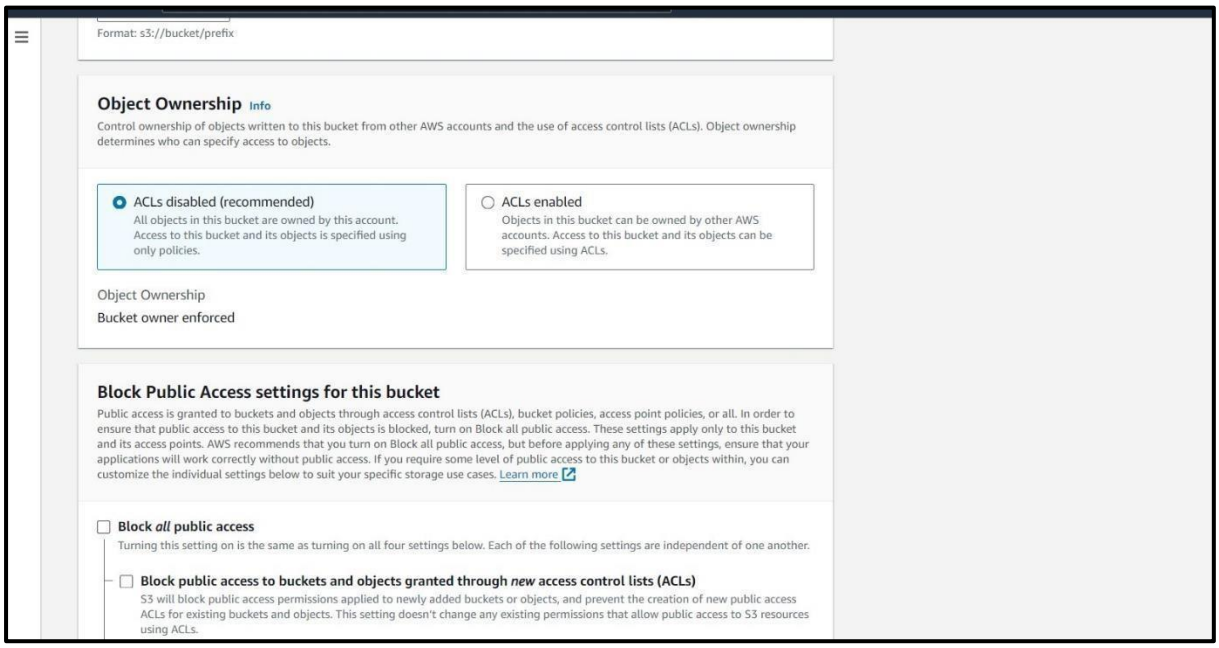
1. Create an S3 Bucket

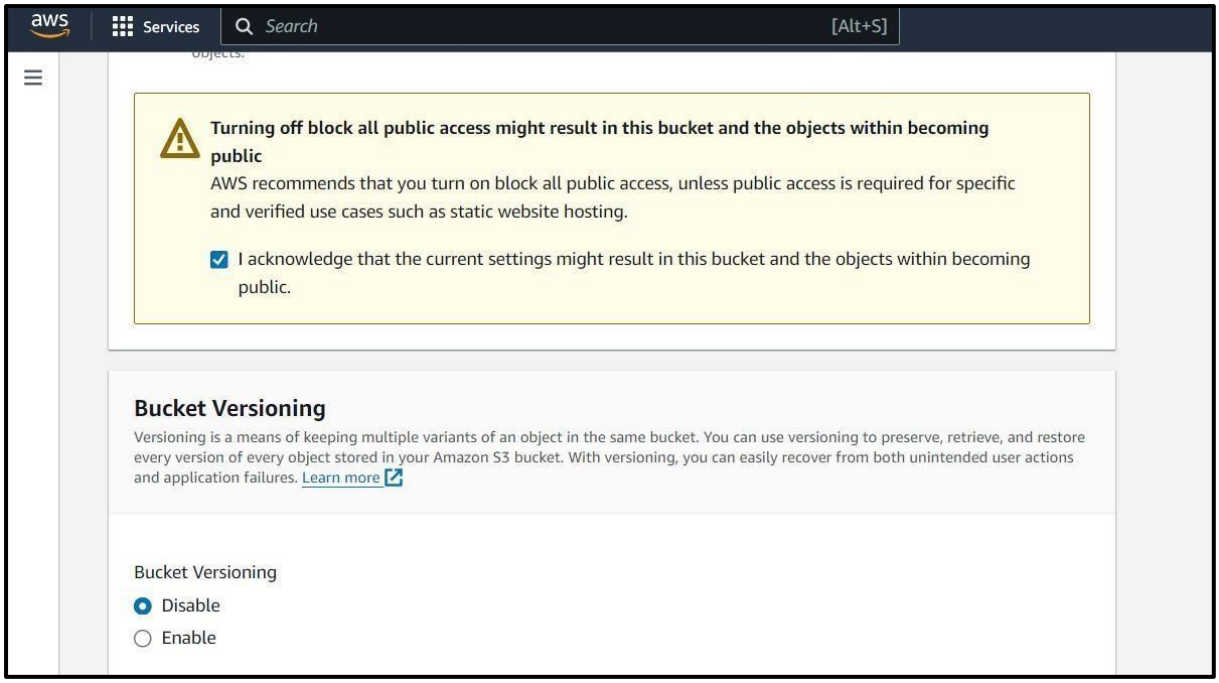
First, I created an Amazon S3 bucket to store the static website's contents. This bucket will serve as the primary storage for all the website files.



2. Enable Public Access

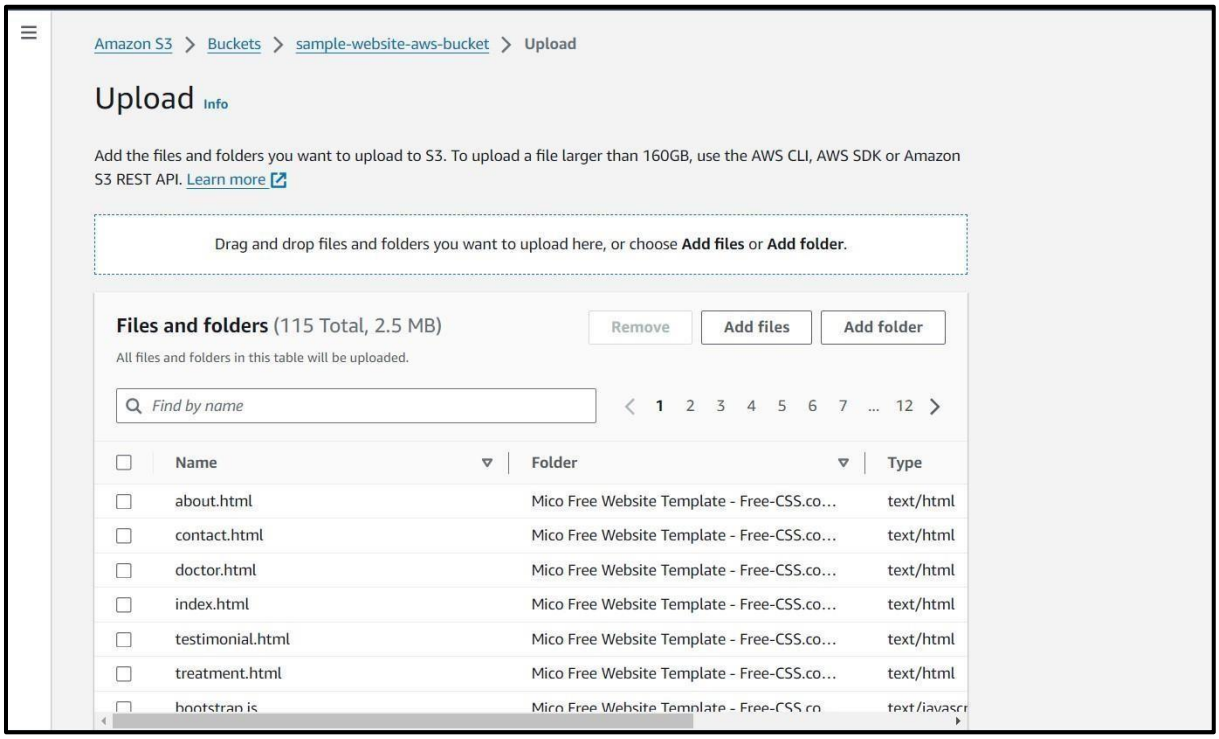
Next, I enabled public access to the bucket. This step is crucial for making the website accessible to the public.





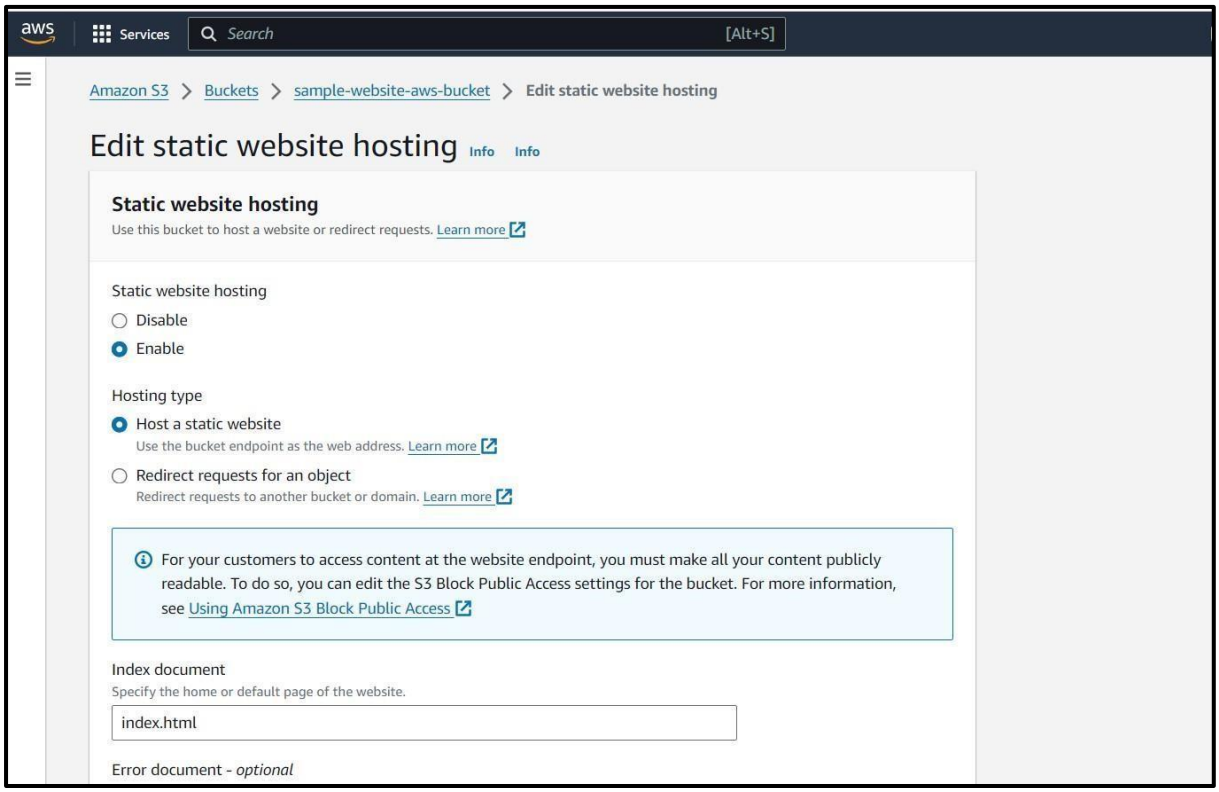
3. Upload Website Files

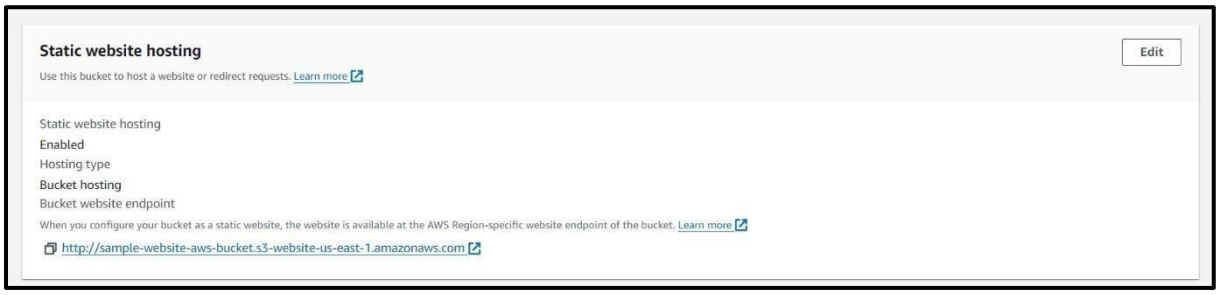
I uploaded the static website files into the newly created S3 bucket. This includes HTML, CSS, JavaScript, and any other assets needed for the website.



4. Configure Static Website Hosting

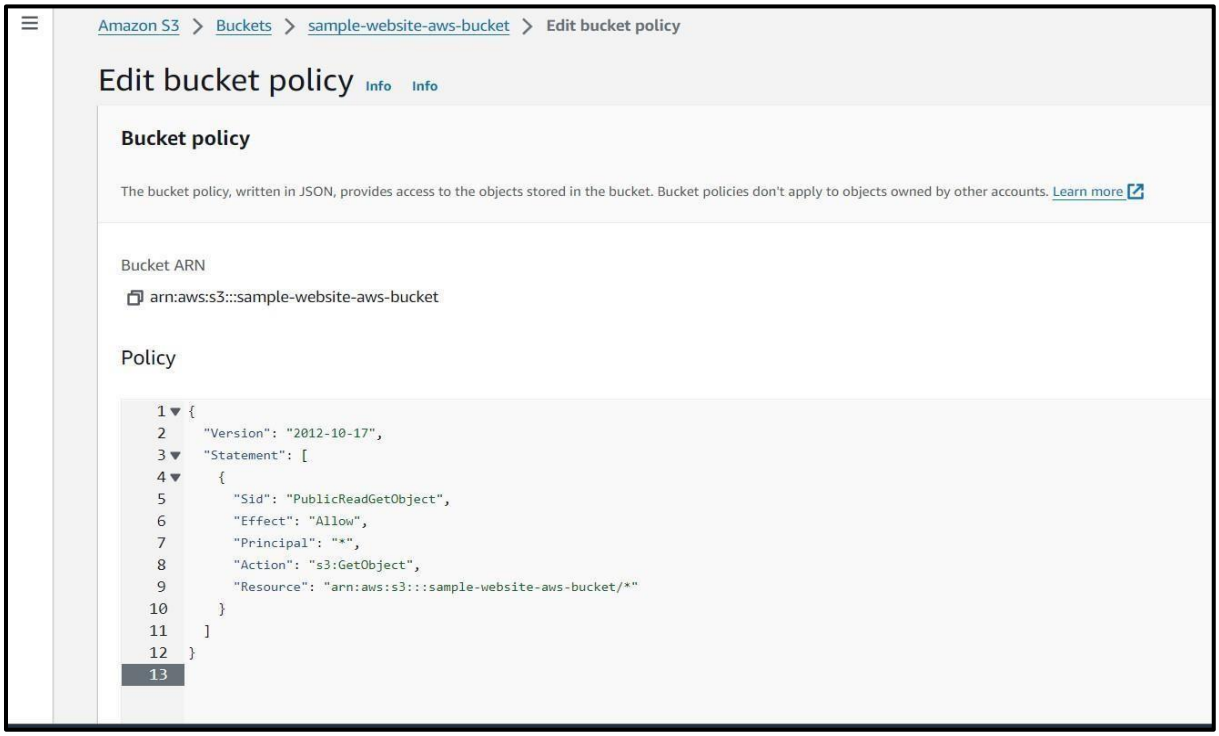
In the S3 bucket's properties, I configured static website hosting by specifying the name of the landing page (e.g., index.html) and saved the changes.





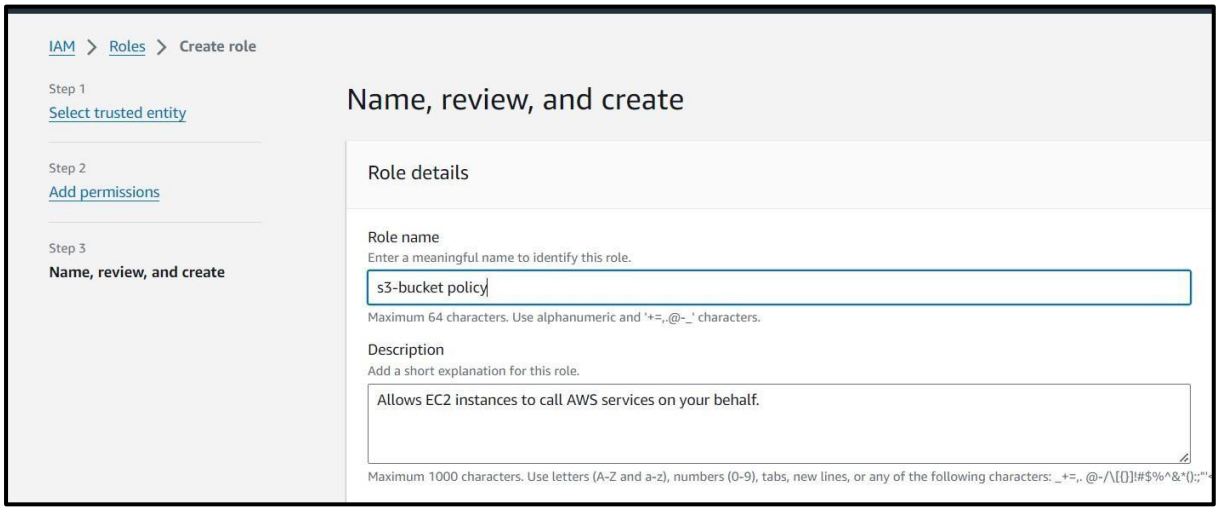
5. Edit Bucket Policy

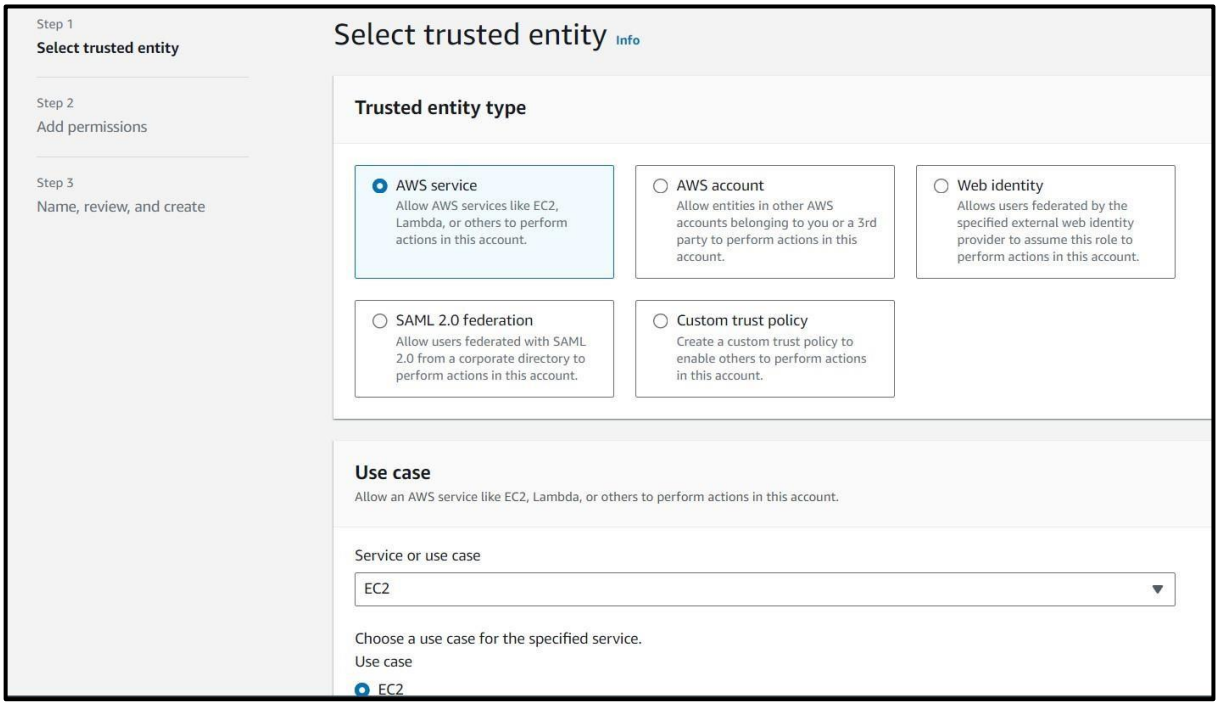
To make the bucket publicly accessible, I edited the bucket policy. This step ensures that users can access the website files stored in the S3 bucket.

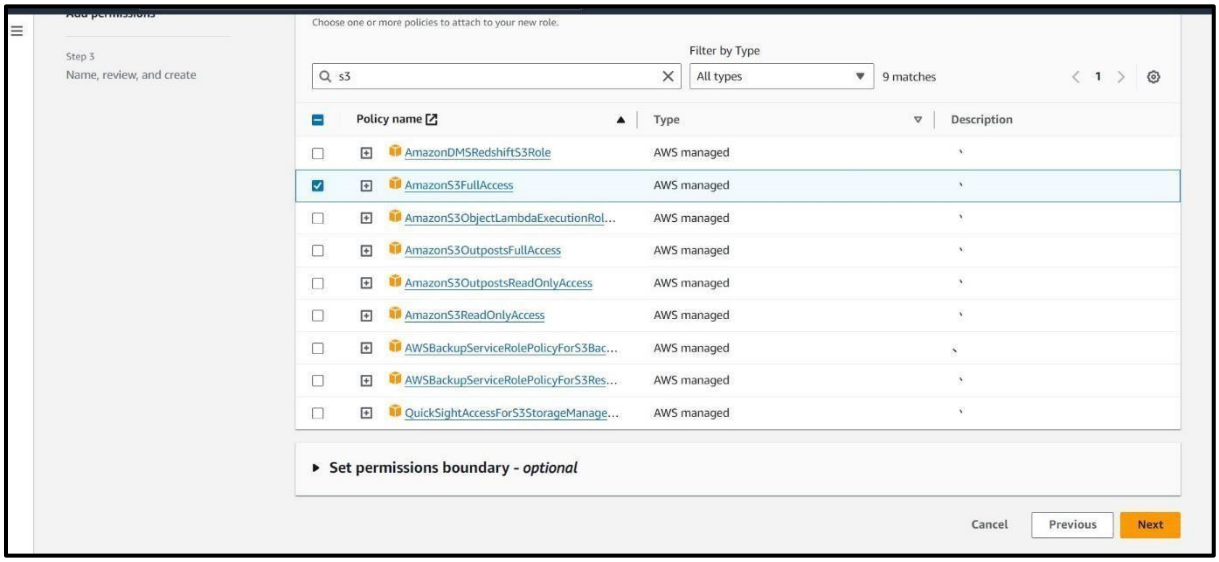


6. Create an IAM Role

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.

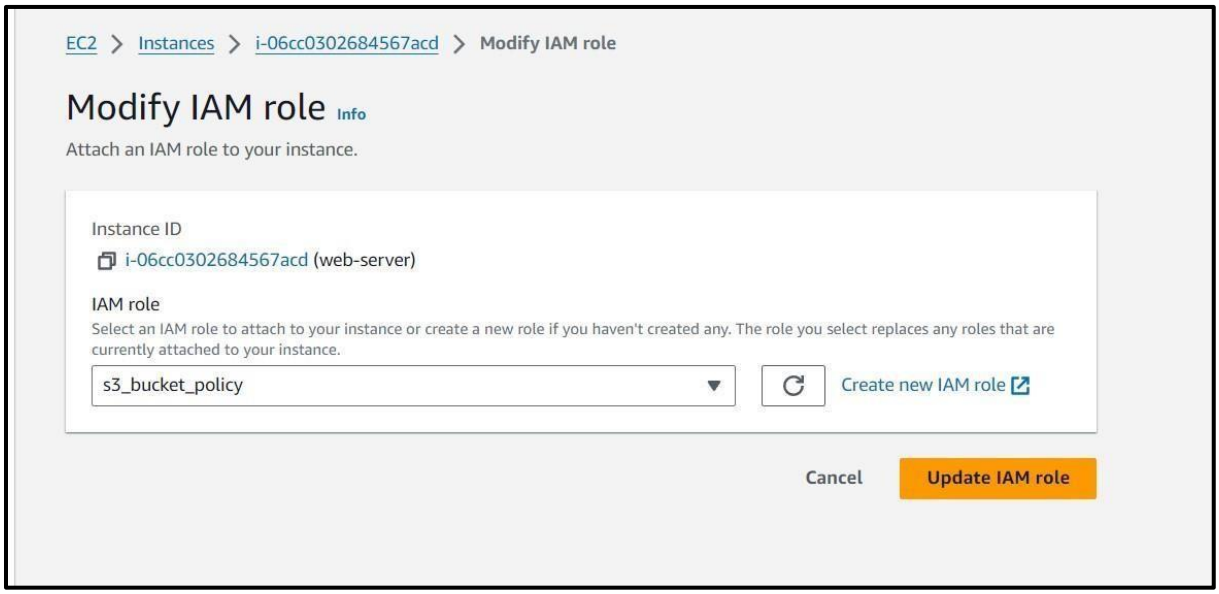






7. Launch EC2 Instance

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



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.

```
[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
```

```
[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
```

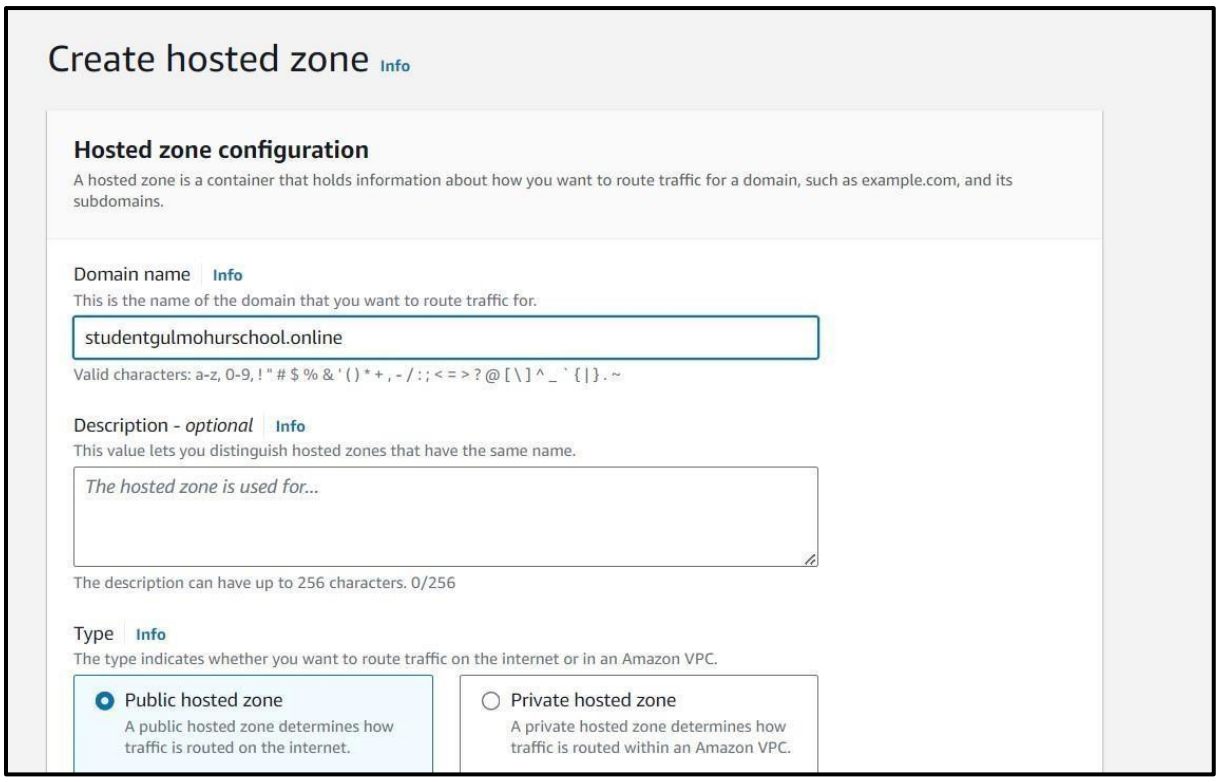
11. Start the Web Server The server was started on the EC2 instance using: sudo systemctl start httpd.

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.

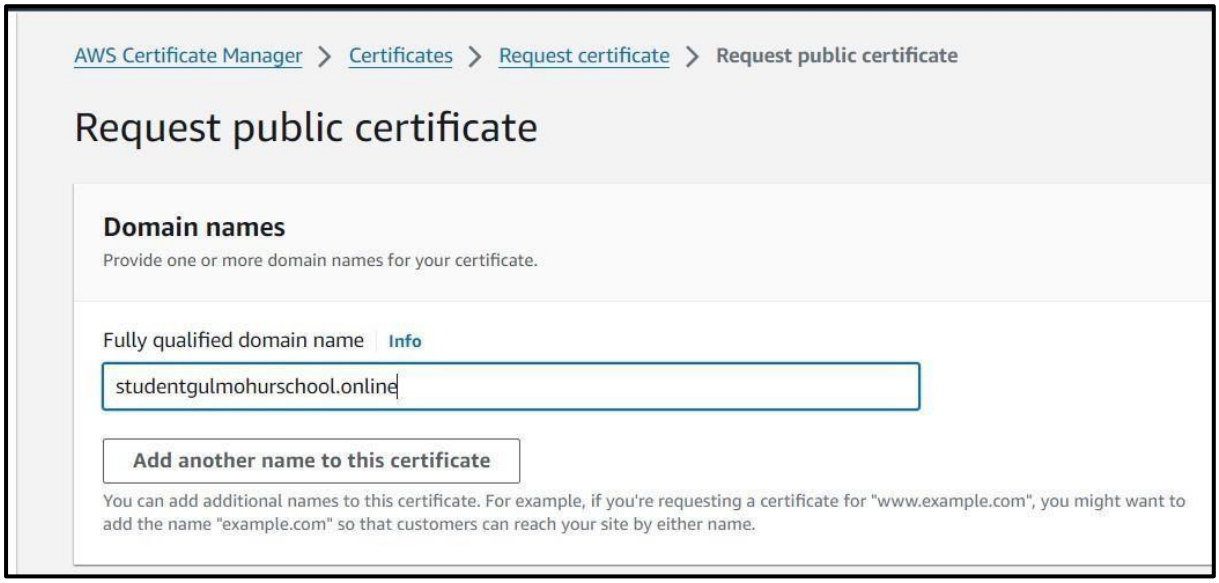


14. Update Domain Nameservers

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.

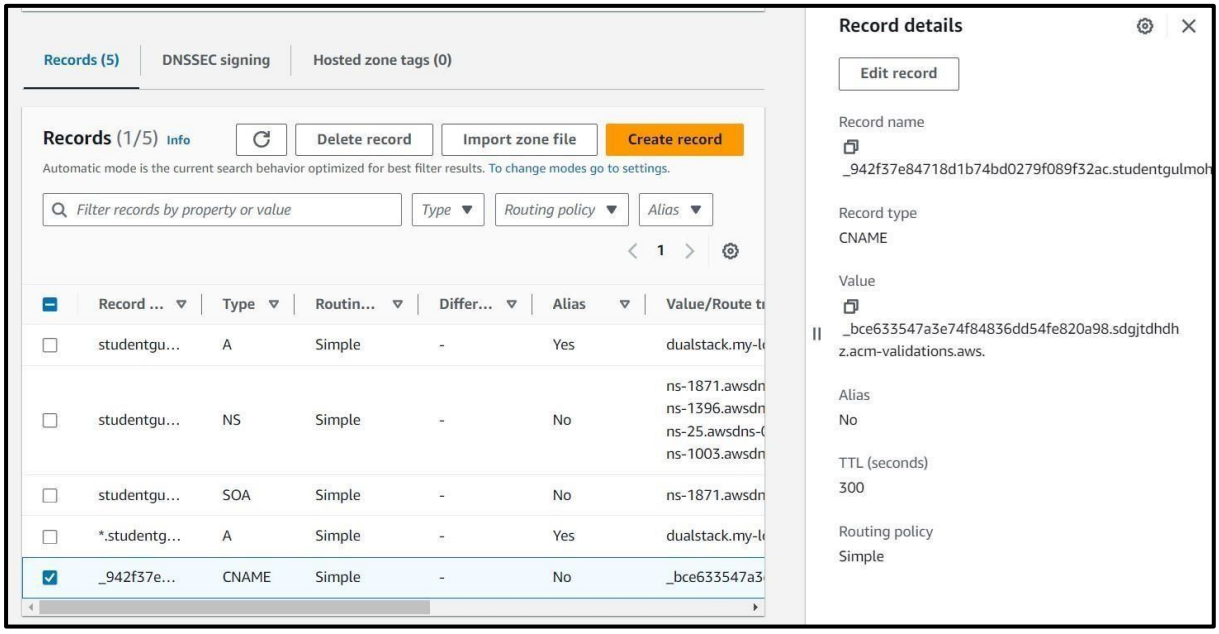


16. Request Wildcard SSL Certificate

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

17. Create CNAME Record

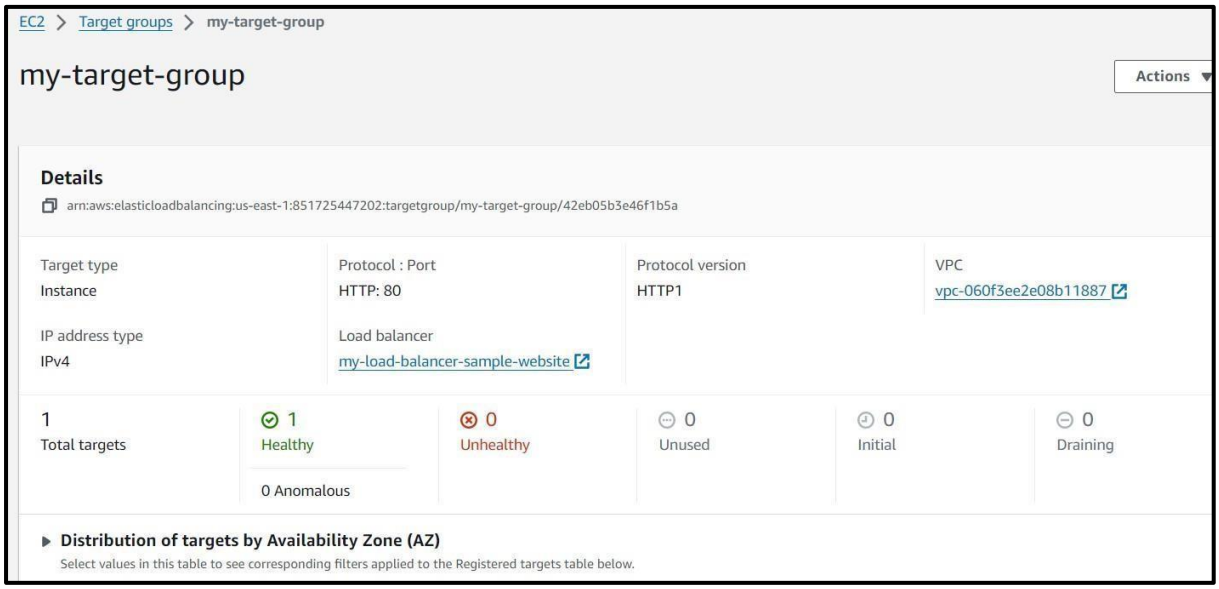
A CNAME record was created in Route 53 to map the domain to the load balancer's DNS name for better traffic management.



18. Create Target Group

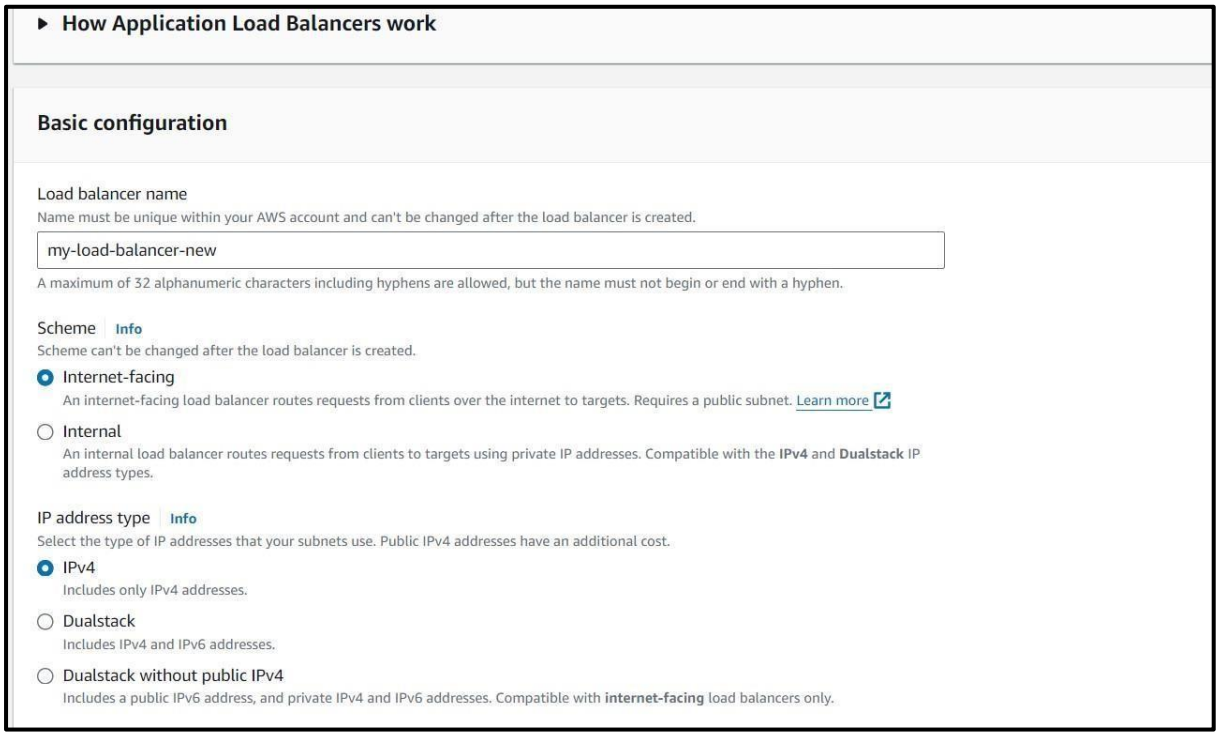
A target group was created for managing traffic distribution.

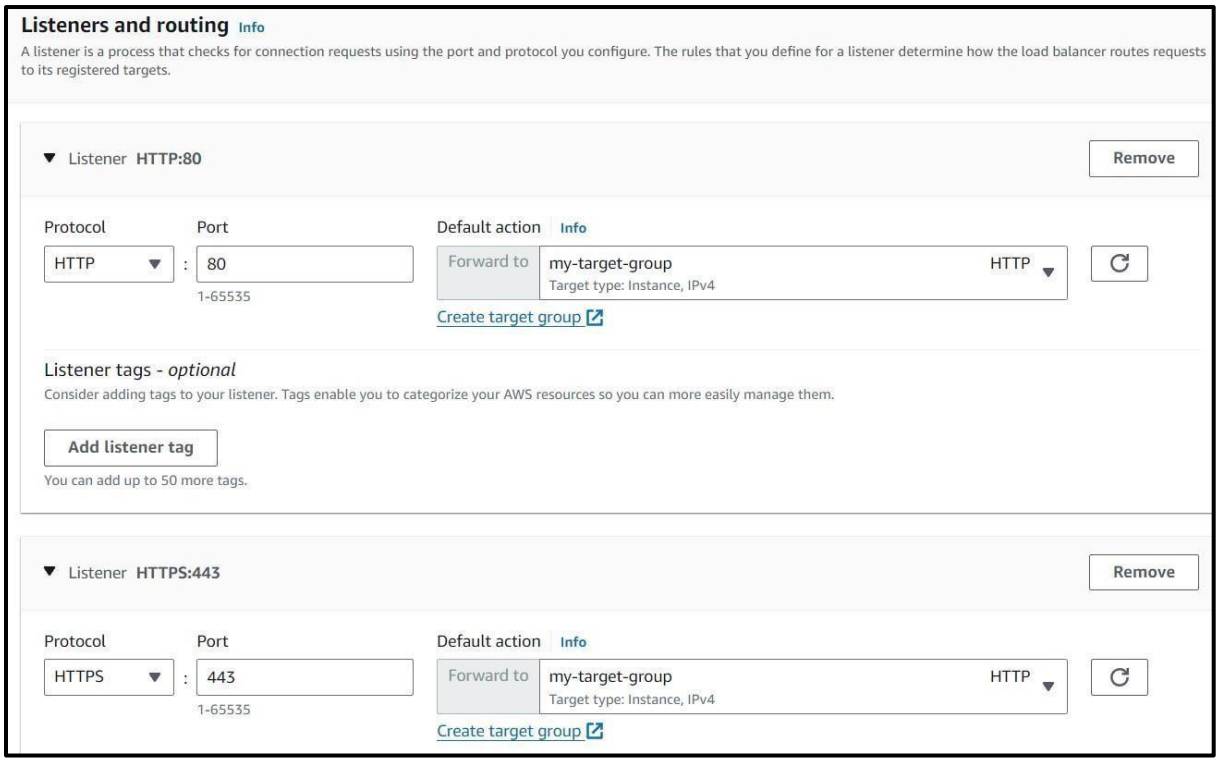
.



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.





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

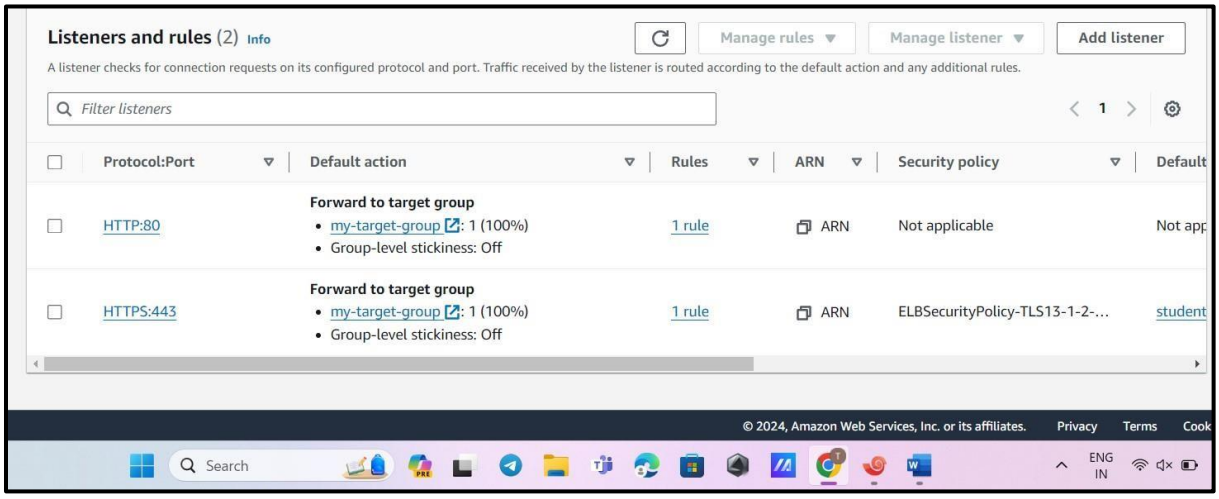
Load balancer type	Status	VPC	IP address type
Application	Active	vpc-013c8a74b0b1087b8	IPv4
Scheme	**Hosted zone**	**Availability Zones**	**Date created**
Internet-facing	Z35SXDOTRQ7X7K	subnet-0b023a29616e5eb6d us-east-1e (use1-az3) subnet-005a2beee33b779a8 us-east-1c (use1-az4) subnet-0e996c7292f1f7ec0 us-east-1d (use1-az6) subnet-07a1e214791a939b5 us-east-1b (use1-az2) subnet-02dcce3de4b7f2d2f us-east-1f (use1-az5) subnet-01f0cd2bc2896f1e9 us-east-1a (use1-az1)	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

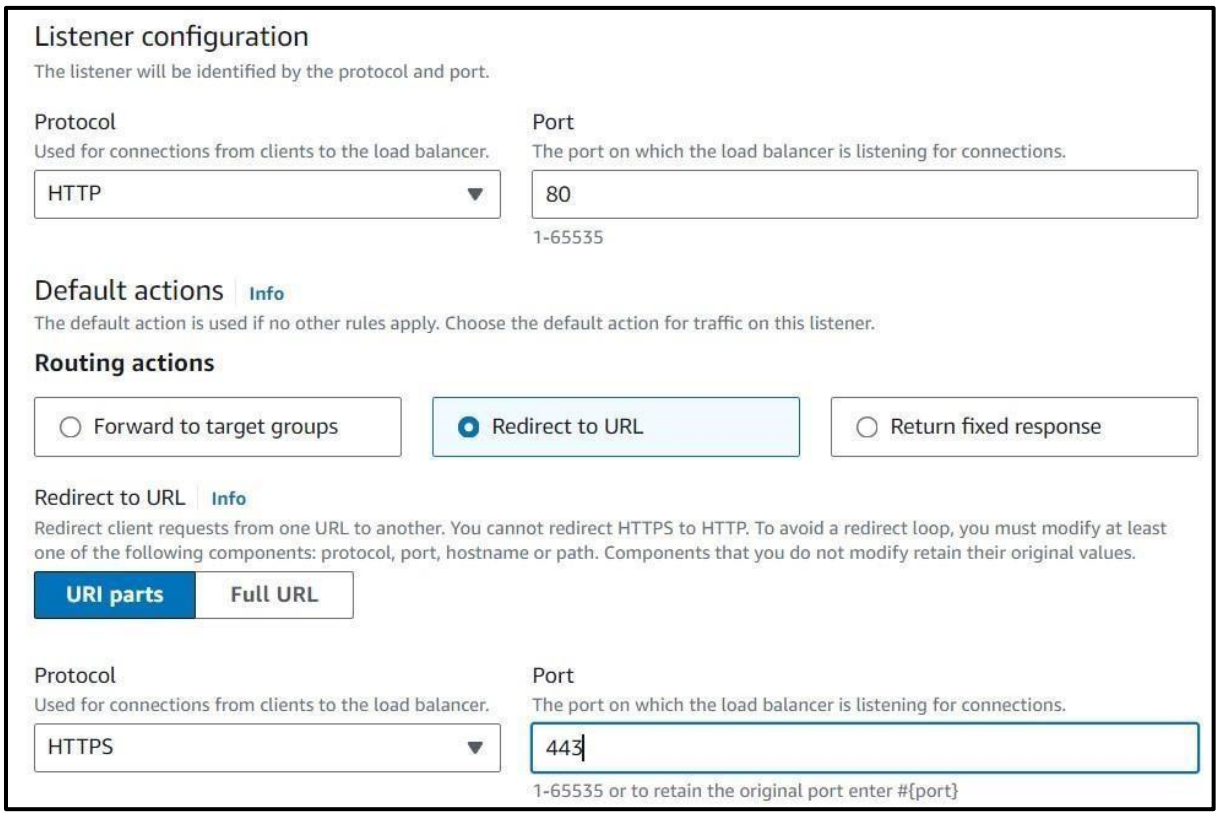
DNS name Info

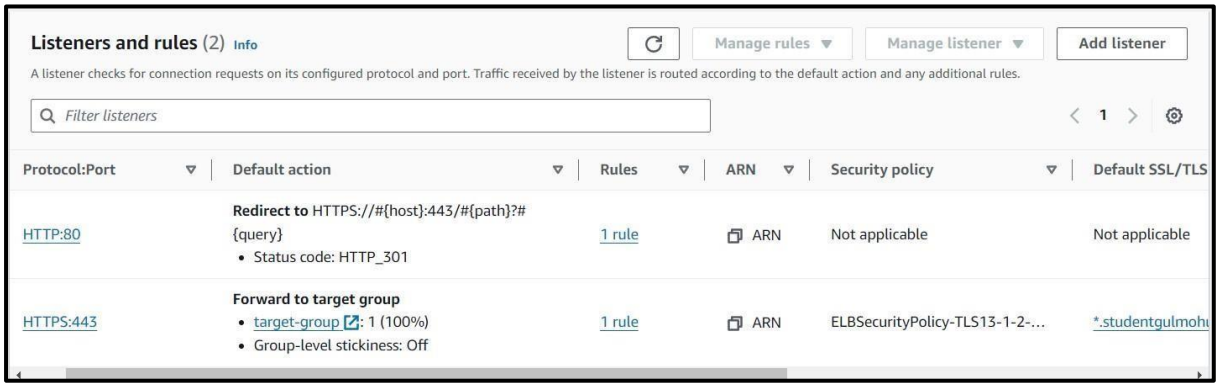
my-load-balancer-new-1108685440.us-east-1.elb.amazonaws.com (A Record)



20. Redirect HTTP to HTTPS

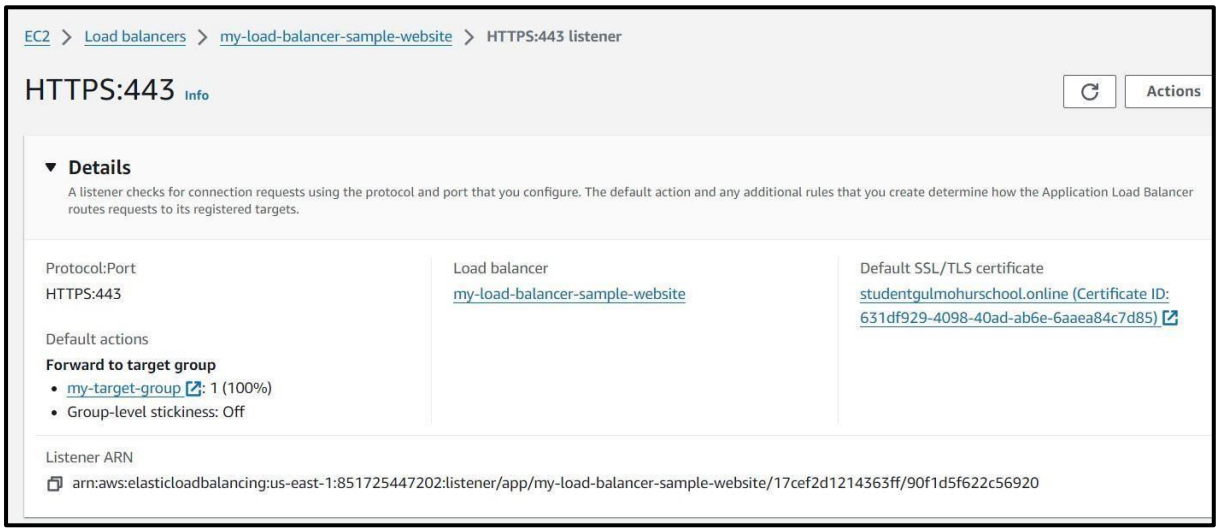
HTTP requests were redirected to HTTPS for secure access.

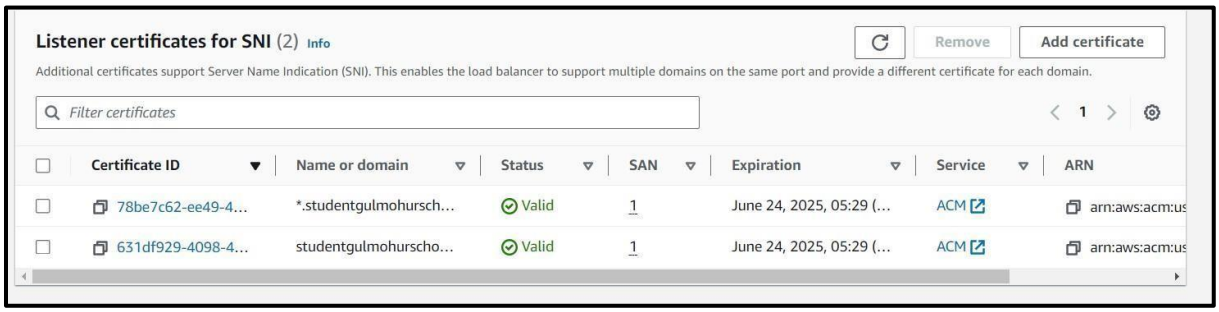




21. Add SSL Certificate for Subdomains

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

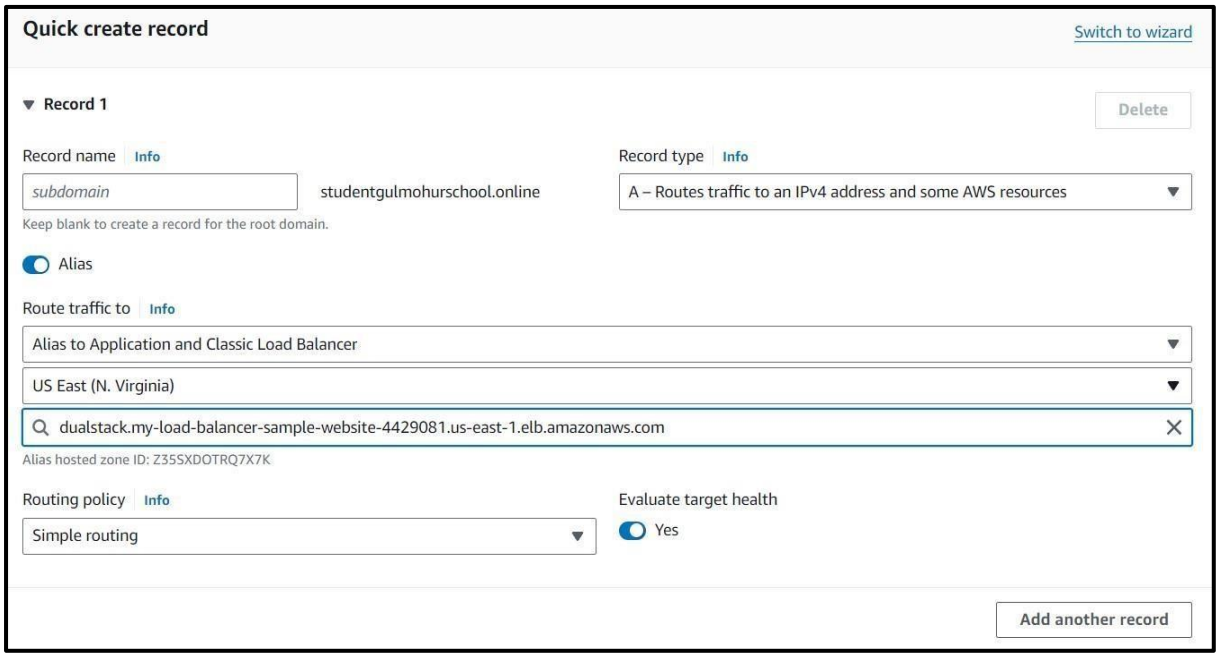


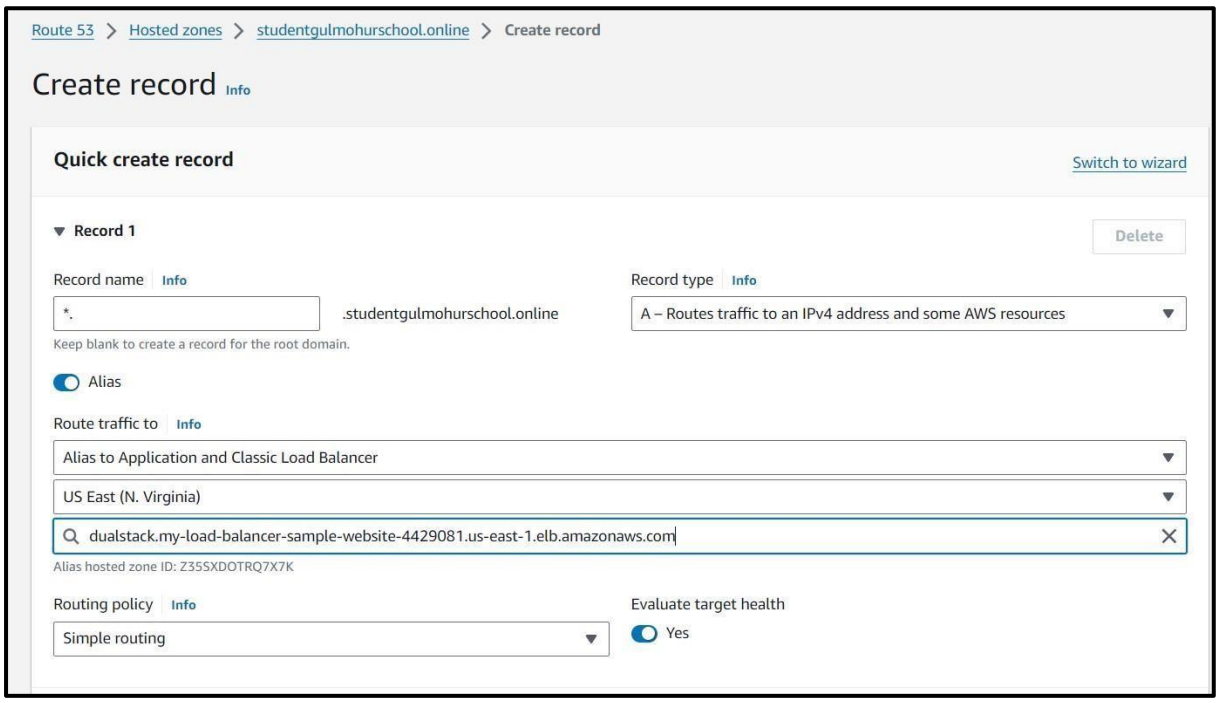


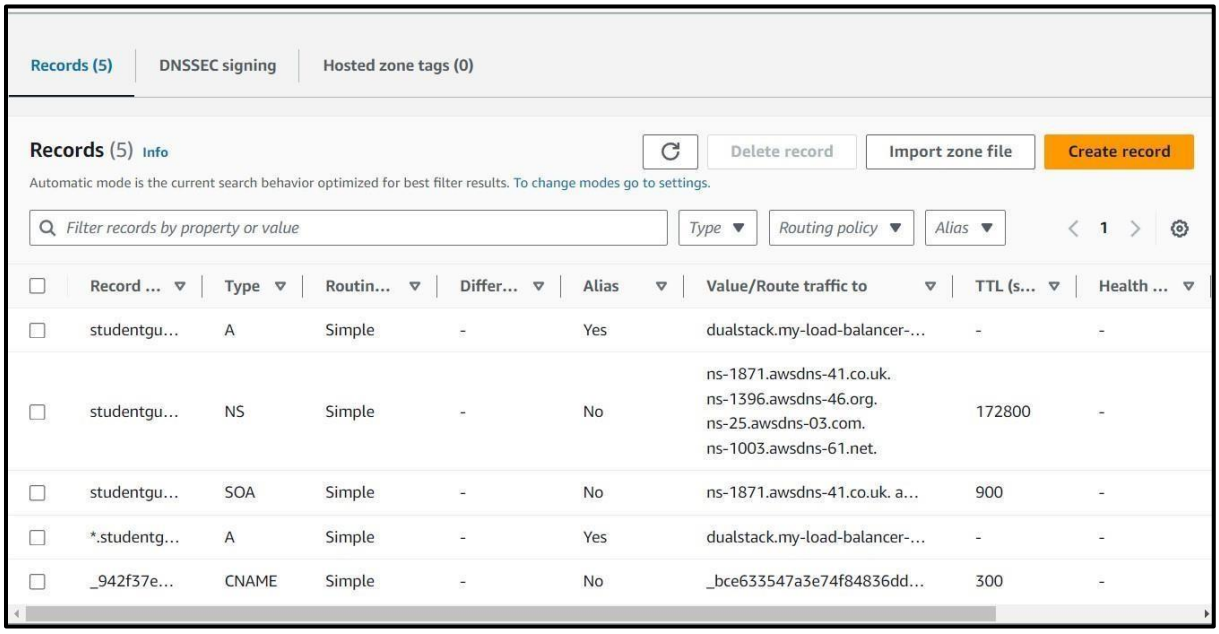
22. Create Route 53 Records

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.

.

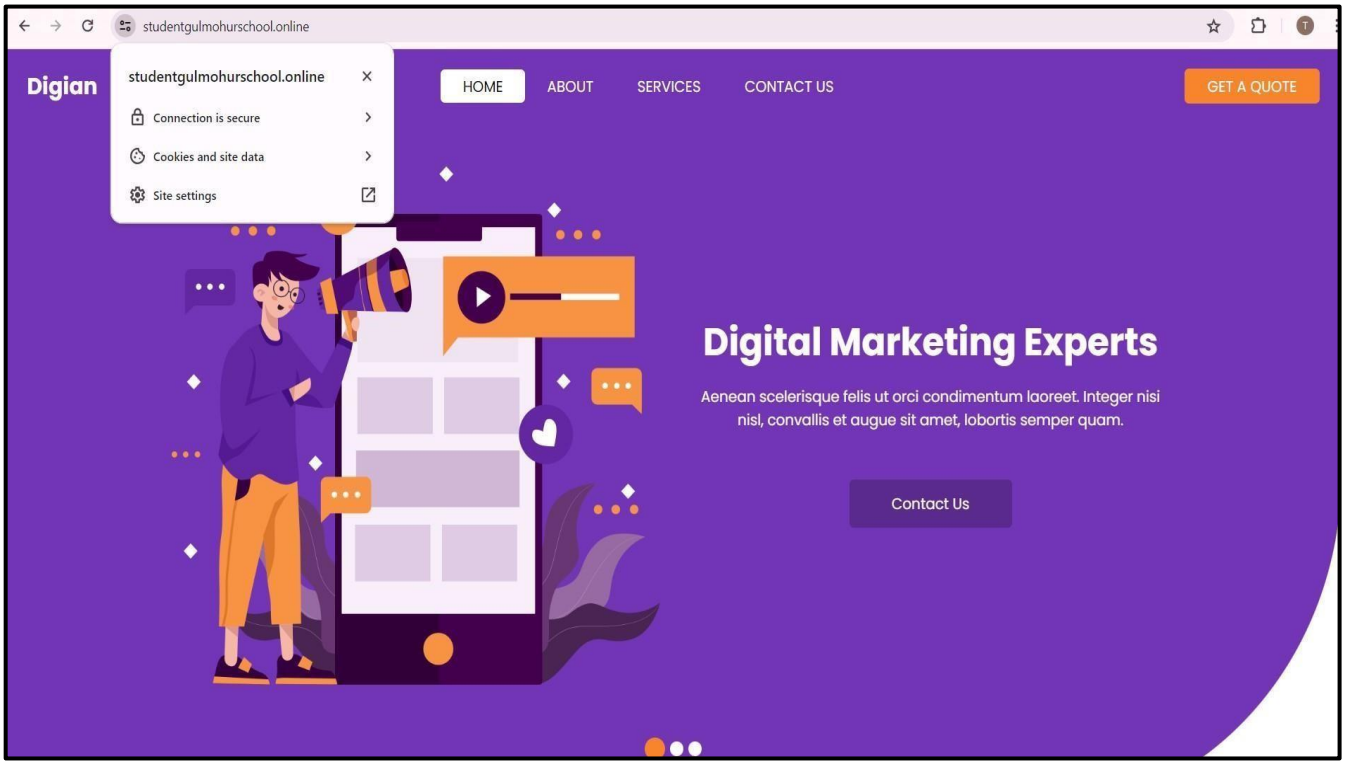


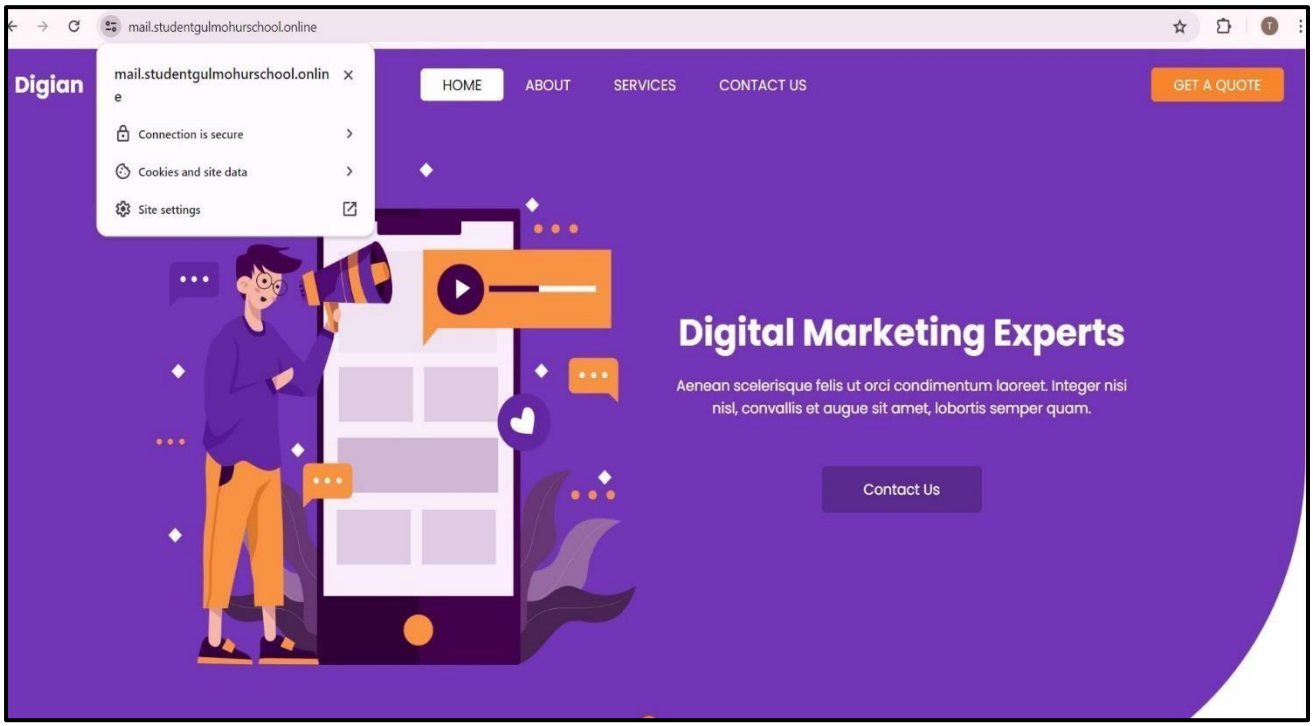




23. Access the Website

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





Certificate Viewer: studentgulmohurschool.online

General | Details

Issued To

Common Name (CN)	studentgulmohurschool.online
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Amazon RSA 2048 M03
Organization (O)	Amazon
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

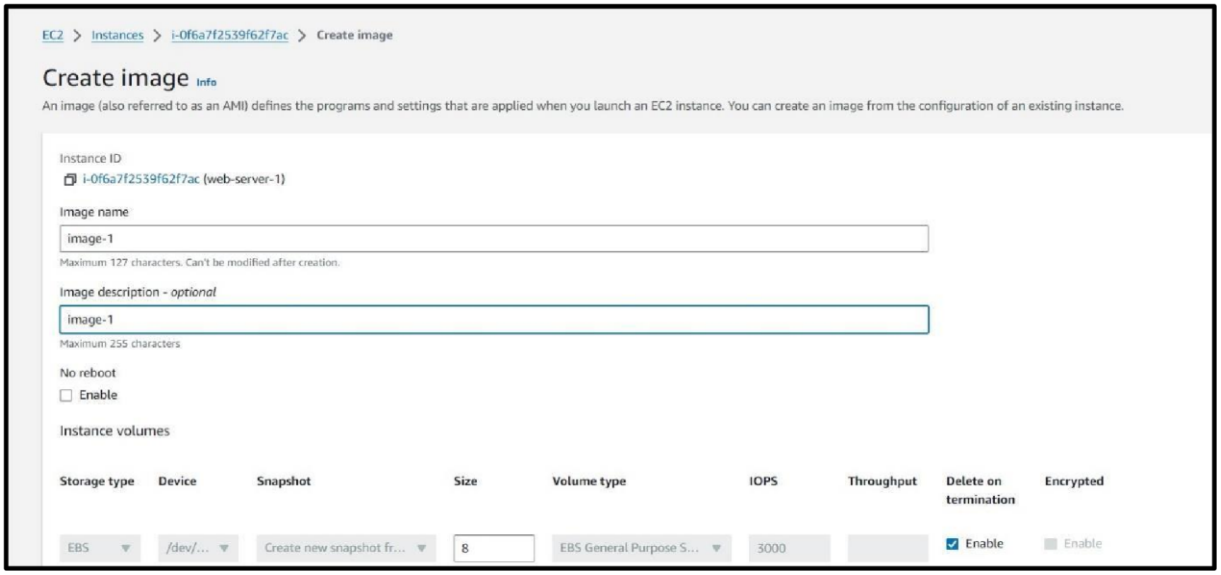
Issued On	Saturday, May 25, 2024 at 5:30:00 AM
Expires On	Tuesday, June 24, 2025 at 5:29:59 AM

SHA-256 Fingerprints

Certificate	24c02e3e1a9391d13c0a6a8a7f0948b3660f36246d537f7a000950d6e001be6c
Public Key	71437ce91fe569c19fb0384dc0dd30713434dcd7ccb6fcf94eb340228171d7a7

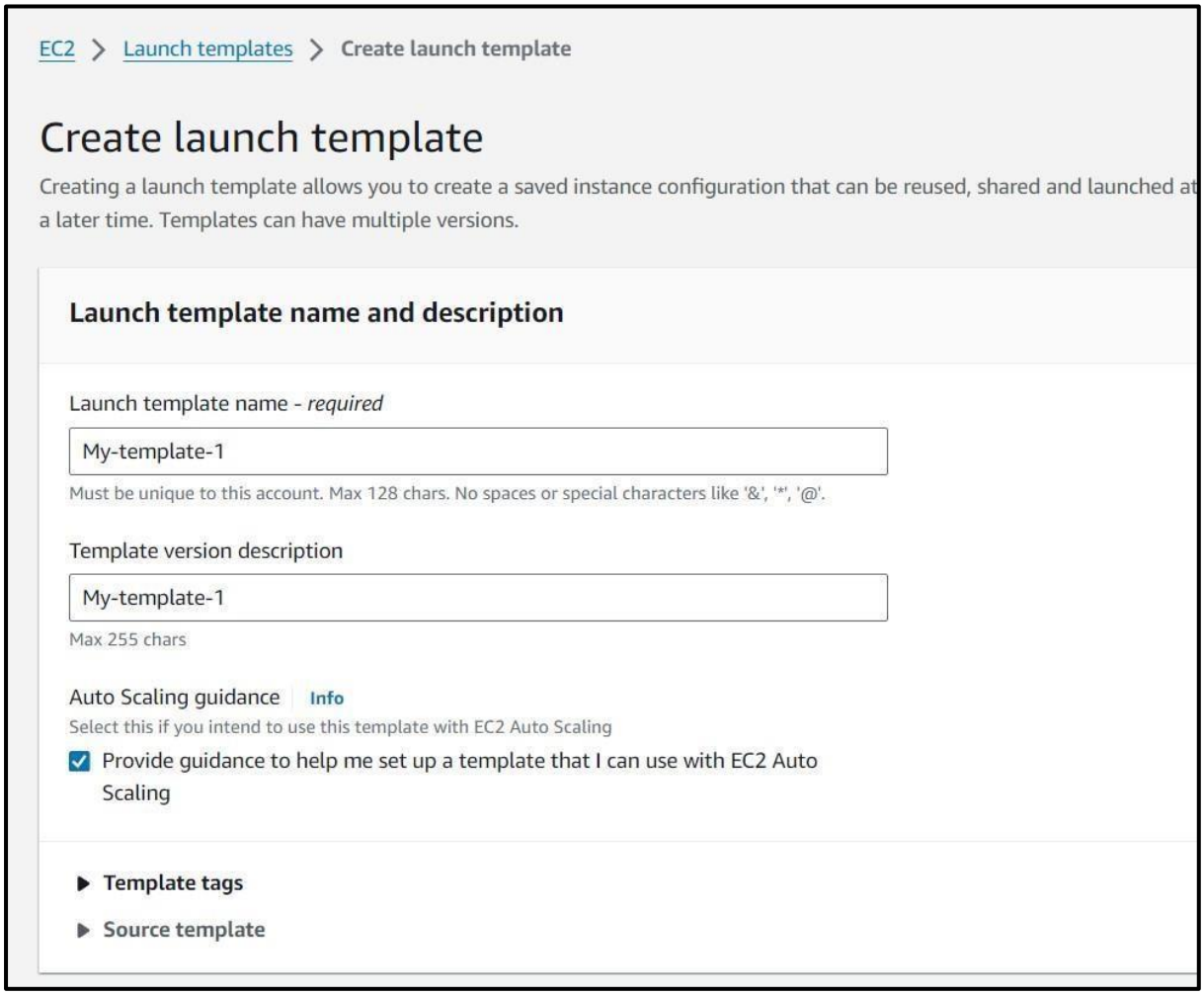
24. Create an Image to be used in auto-scaling group

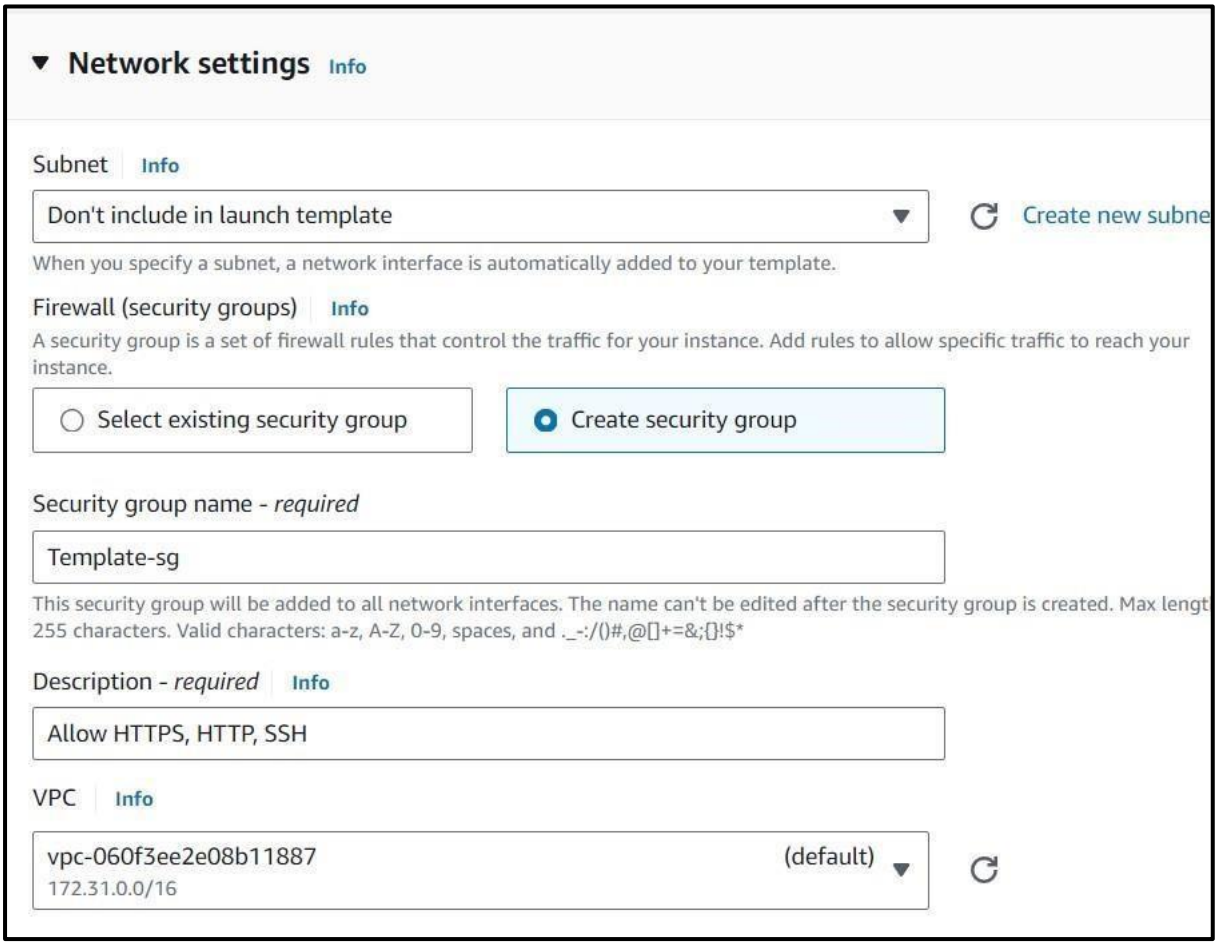
An image of the EC2 instance was created where the web server is configured. A template was launched from this image.

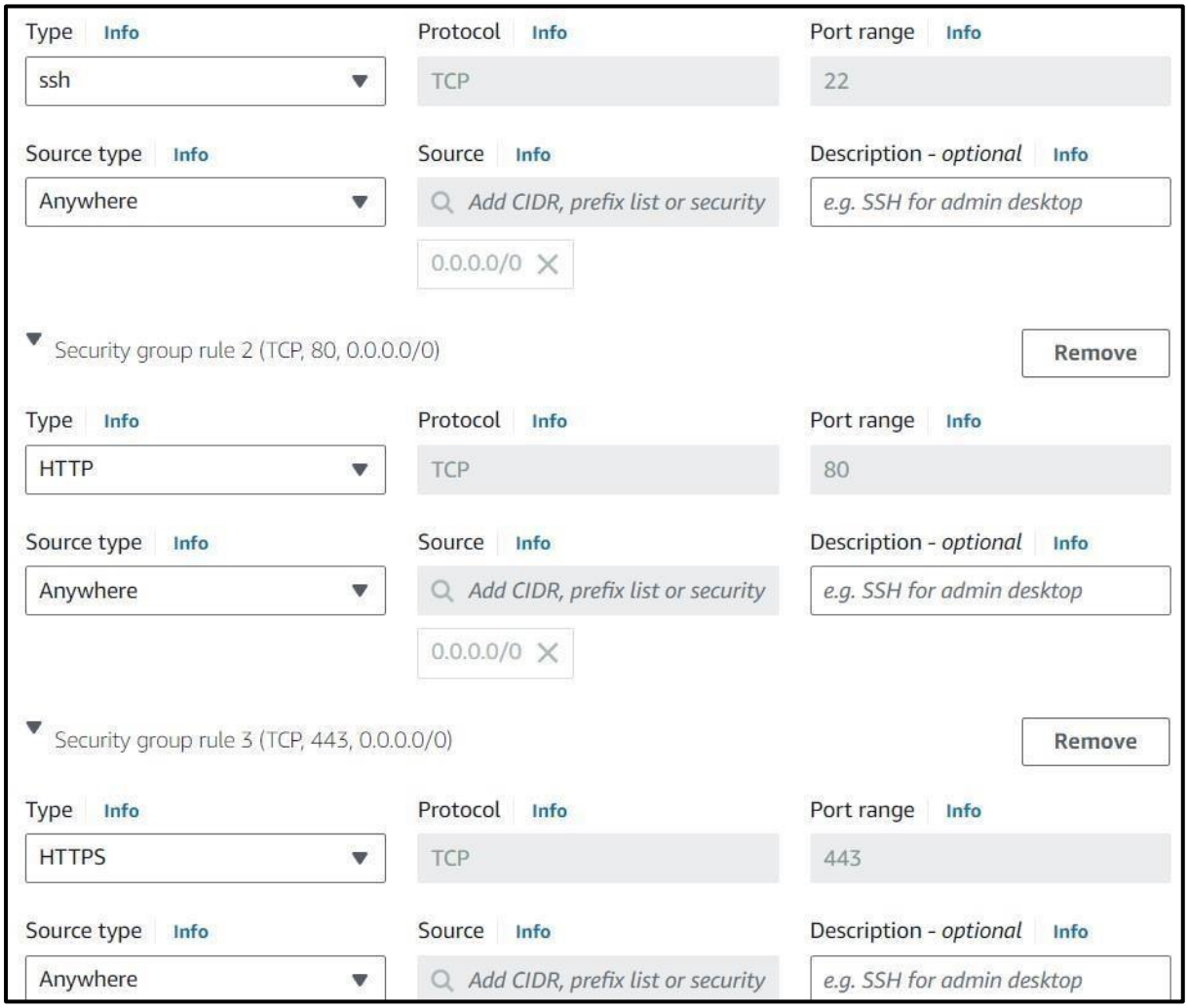


25. Launch Template

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.

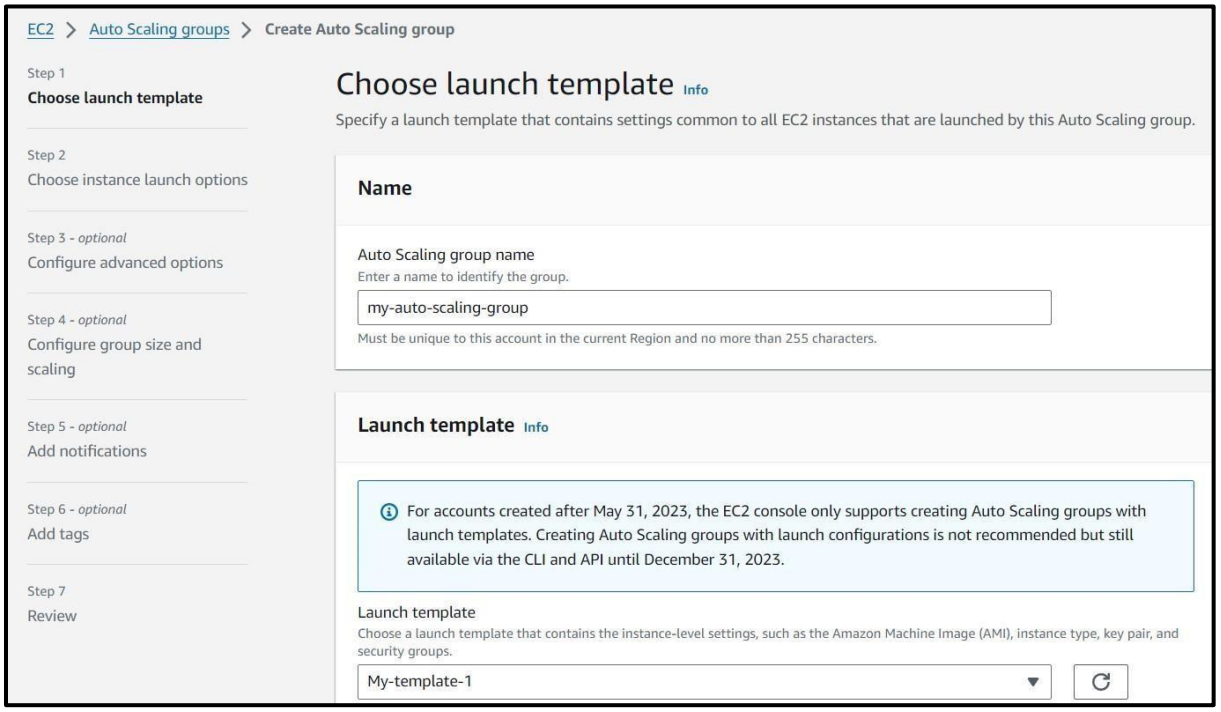

EC2 > Launch templates > Create launch template
Create launch template
Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at
a later time. Templates can have multiple versions.
Launch template name and description
Launch template name - required
My-template-1
Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.
Template version description
My-template-1
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

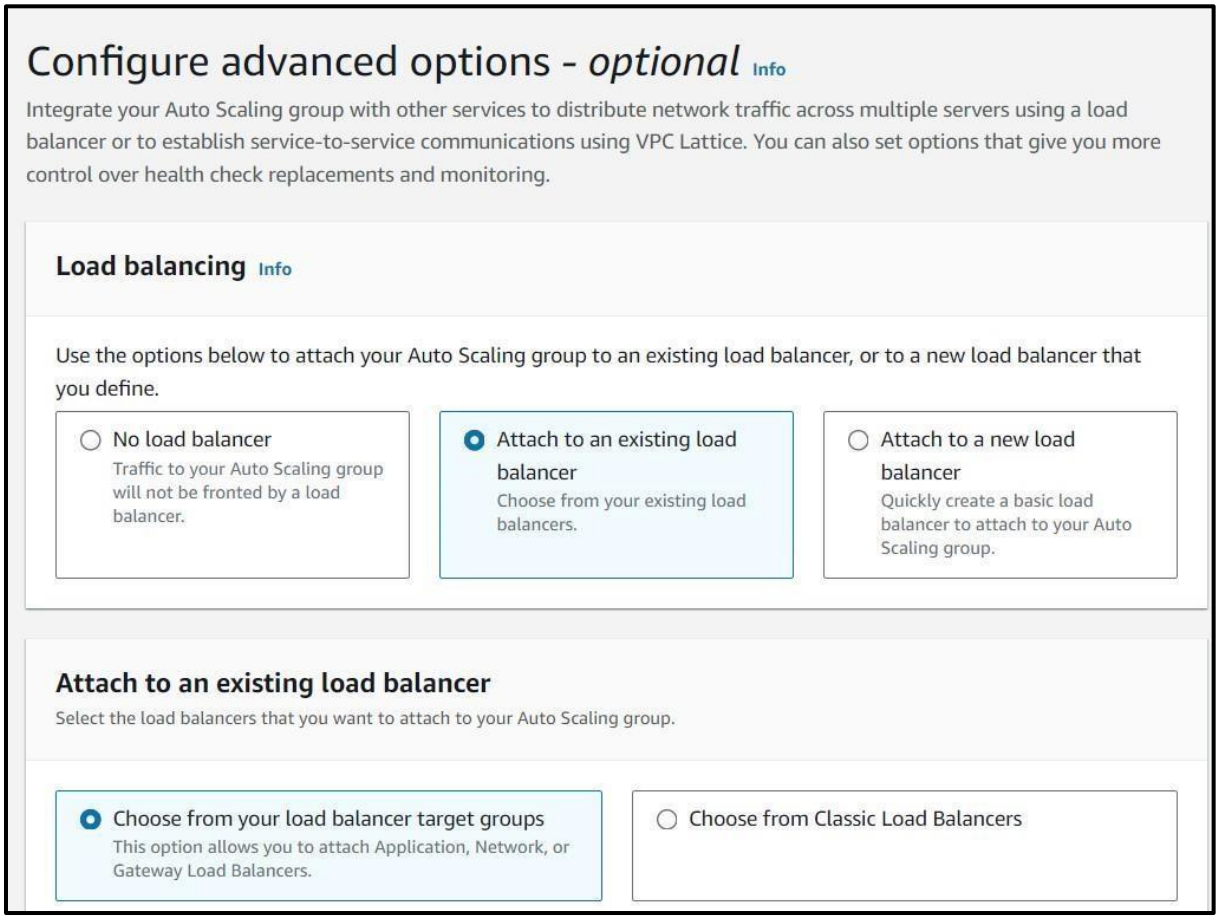

Network settings Info
Subnet Info
Don't include in launch template
Create new subne
When you specify a subnet, a network interface is automatically added to your template.
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules 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 lengt
255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
Allow HTTPS, HTTP, SSH
VPC Info
vpc-060f3ee2e08b11887 (default)
172.31.0.0/16

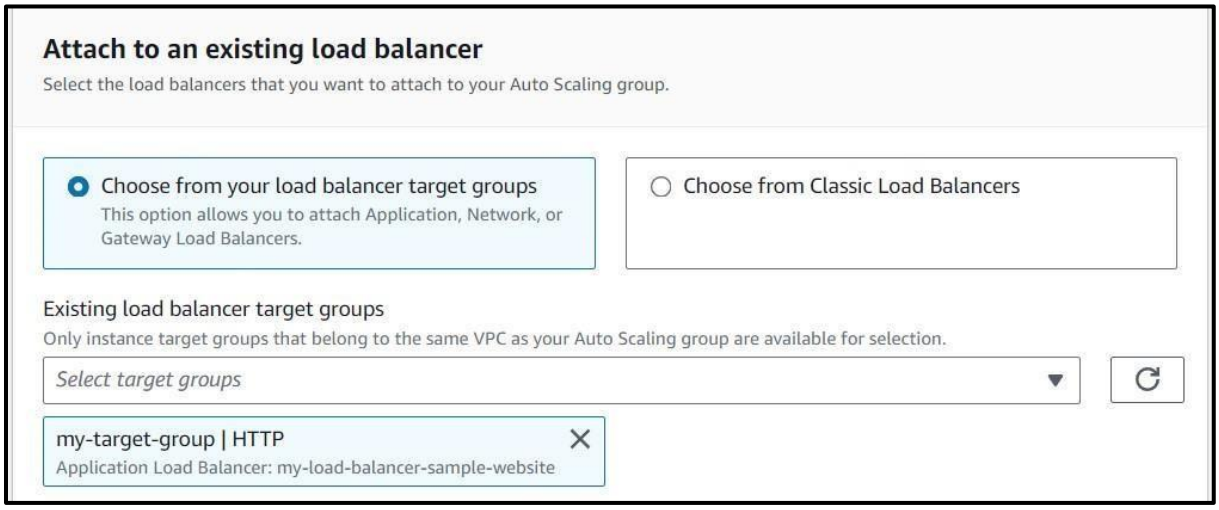


26.Create an auto-scaling group.

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

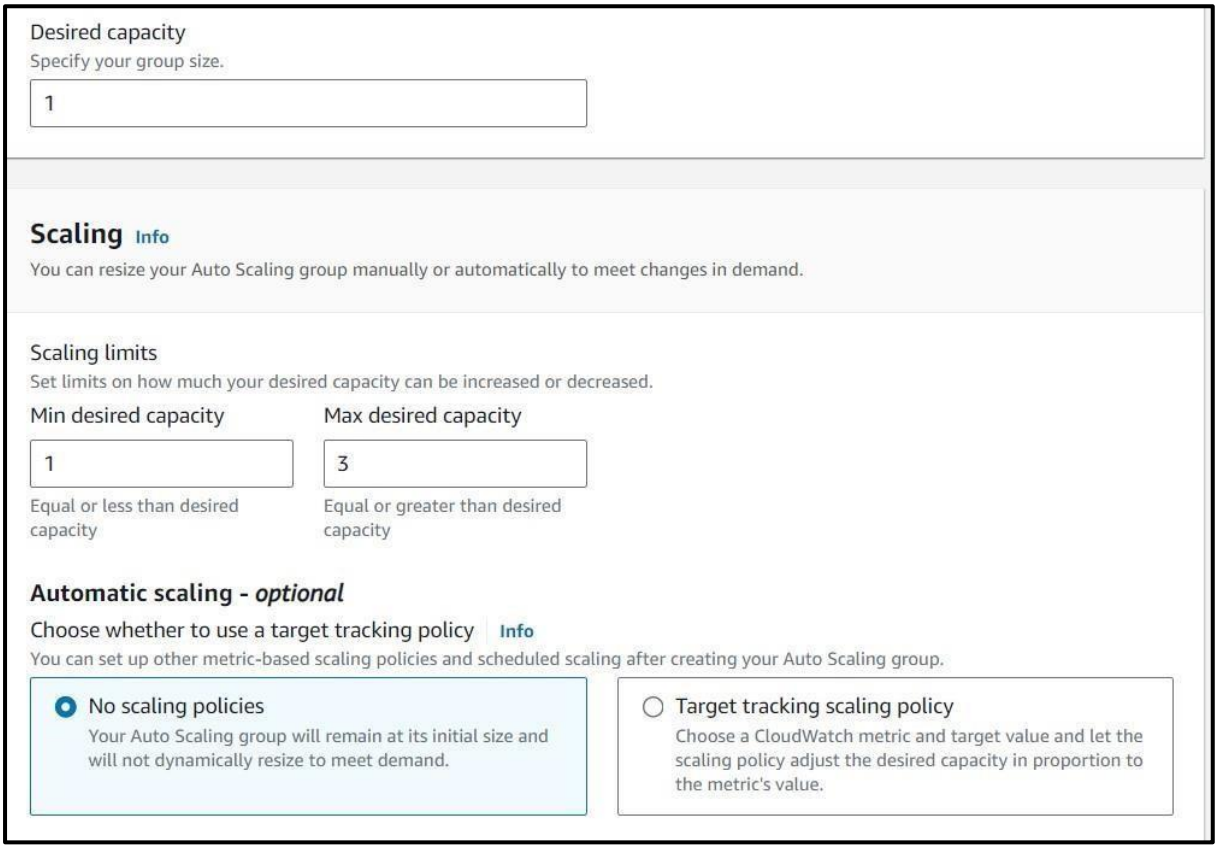

EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1
Choose launch template
Step 2
Choose instance launch options
Step 3 - optional
Configure advanced options
Step 4 - optional
Configure group size and scaling
Step 5 - optional
Add notifications
Step 6 - optional
Add tags
Step 7
Review
Choose 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



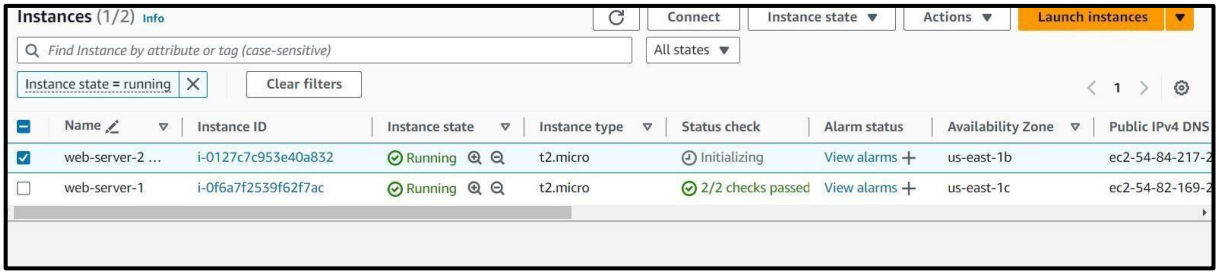
26. Set Scaling Policies

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.



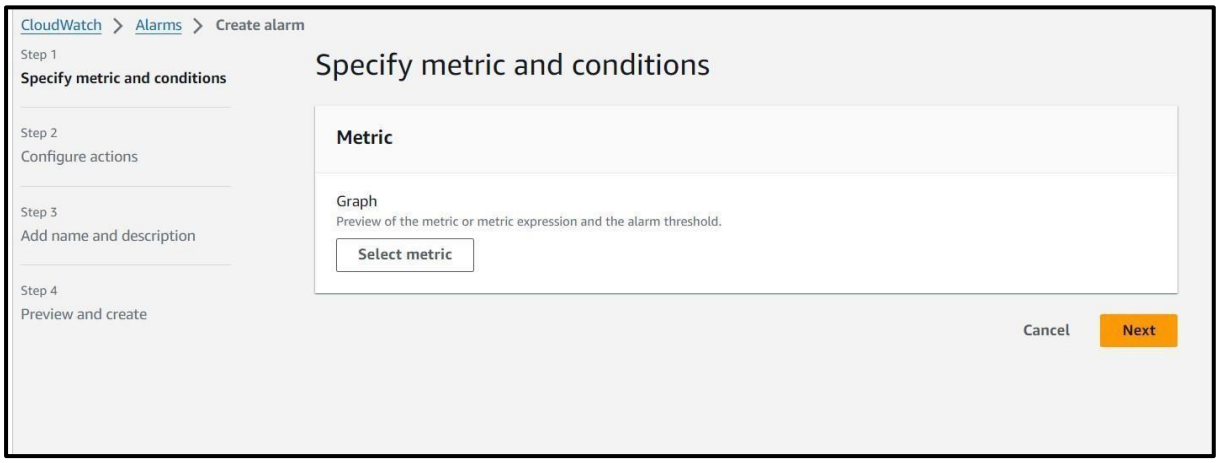
27. After creating the auto-scaling group , a new instance was launched from the template chosen, appeared in the EC2 dashboard.

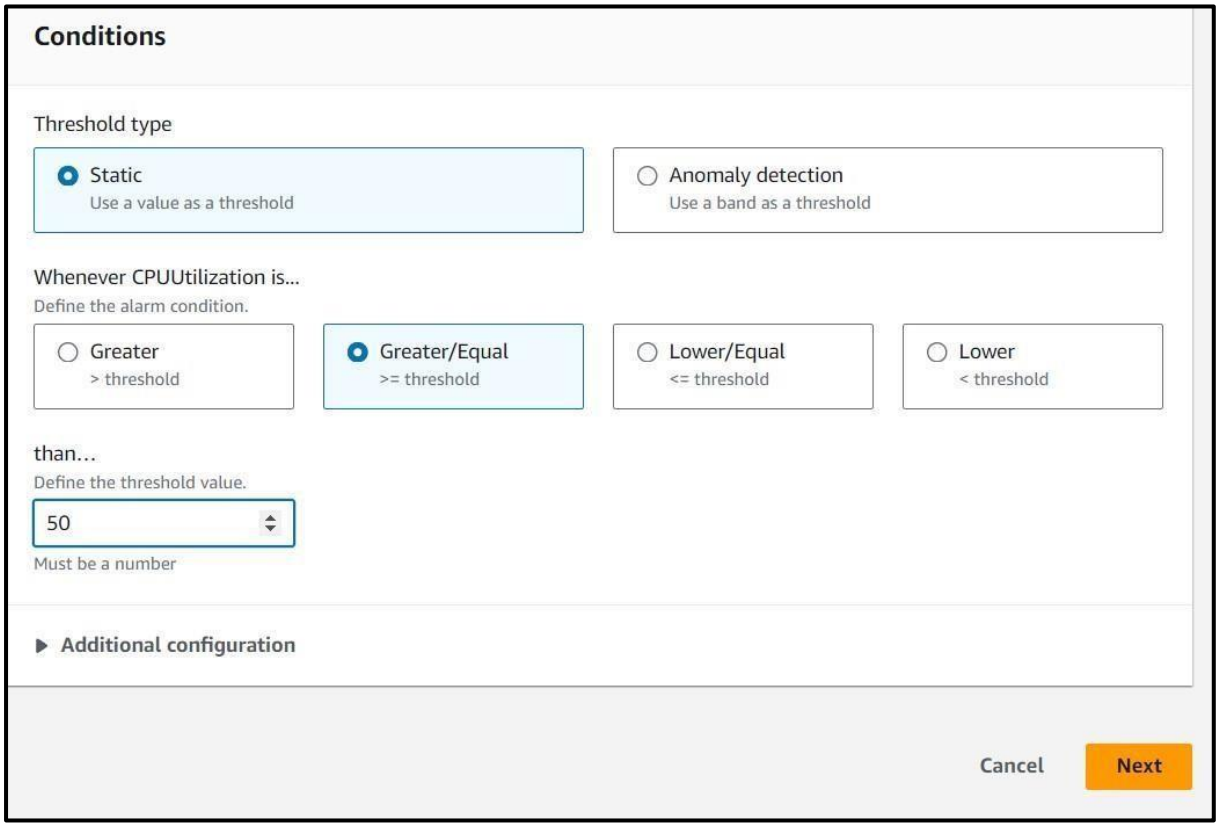
28. Create CloudWatch

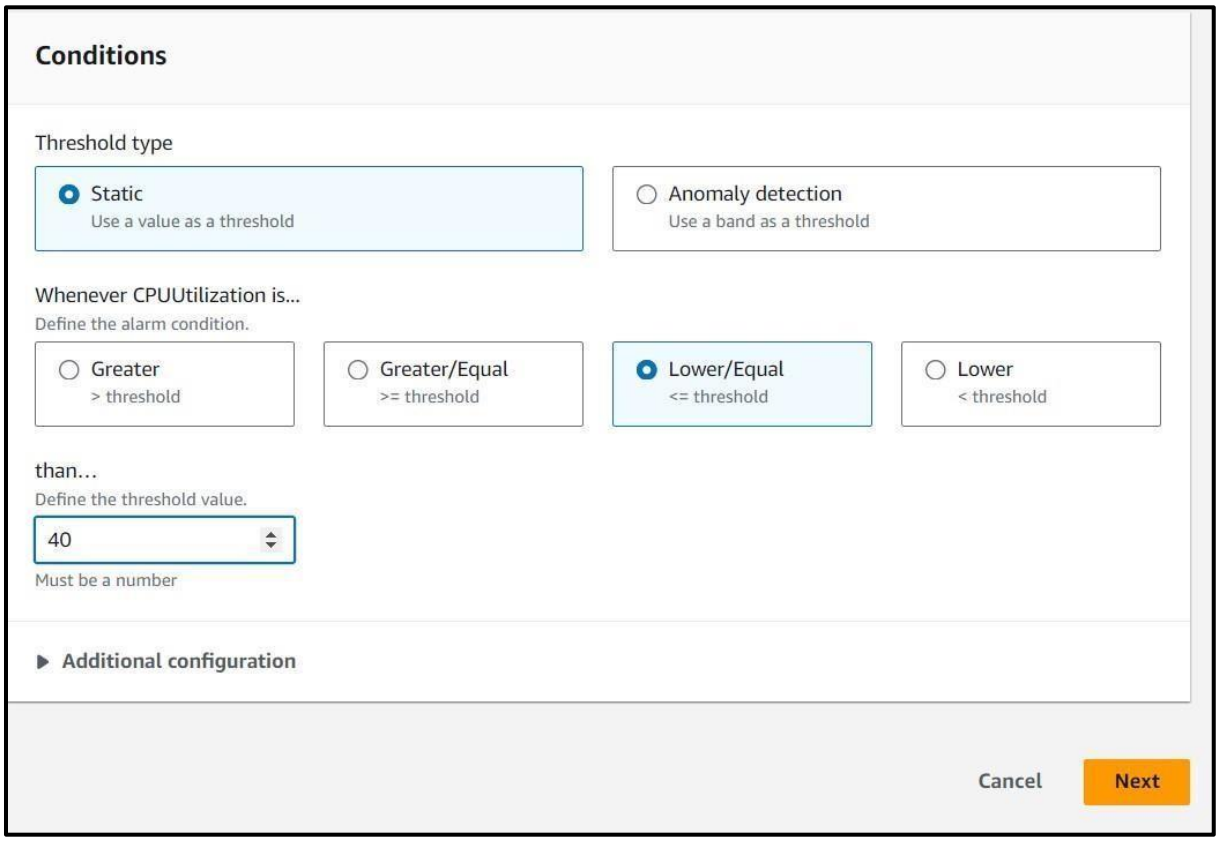


Alarms

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

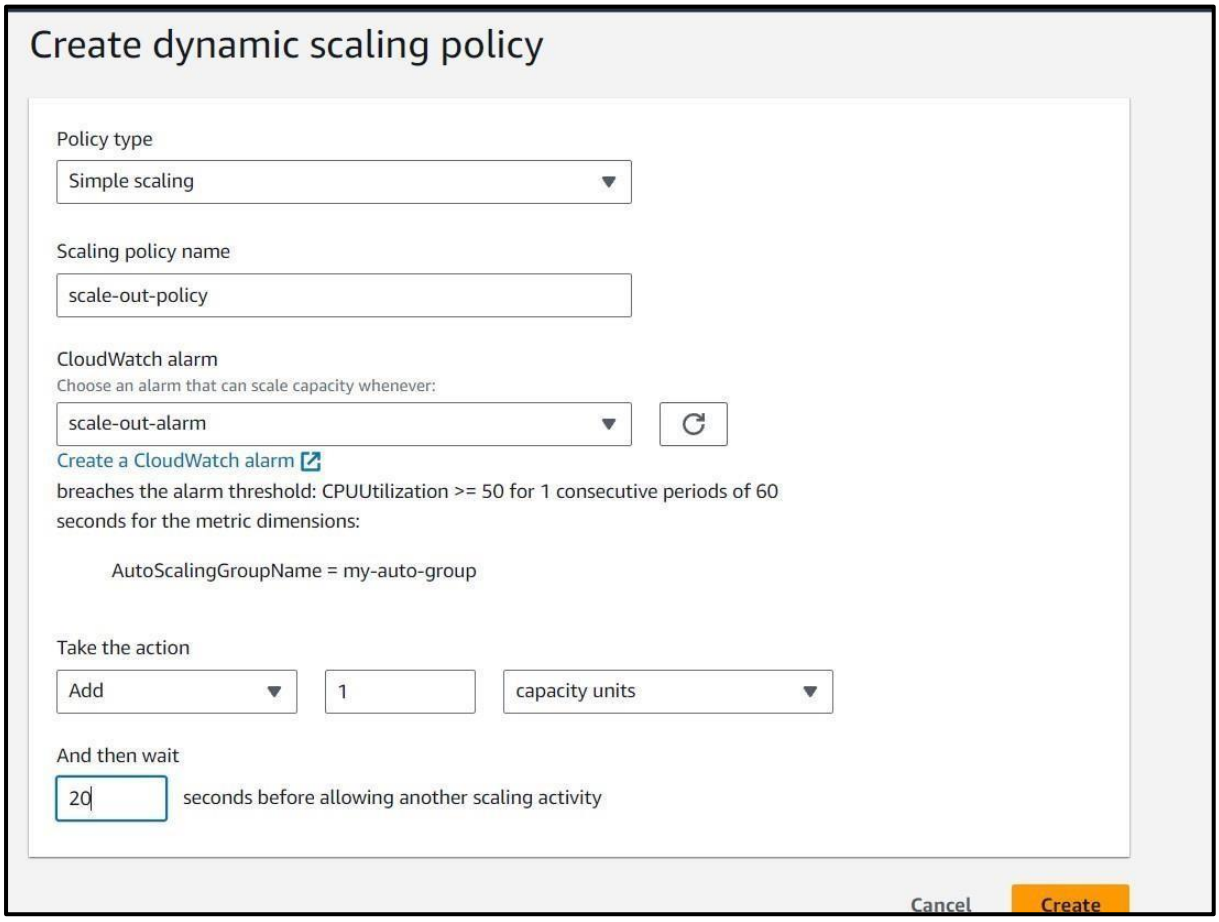


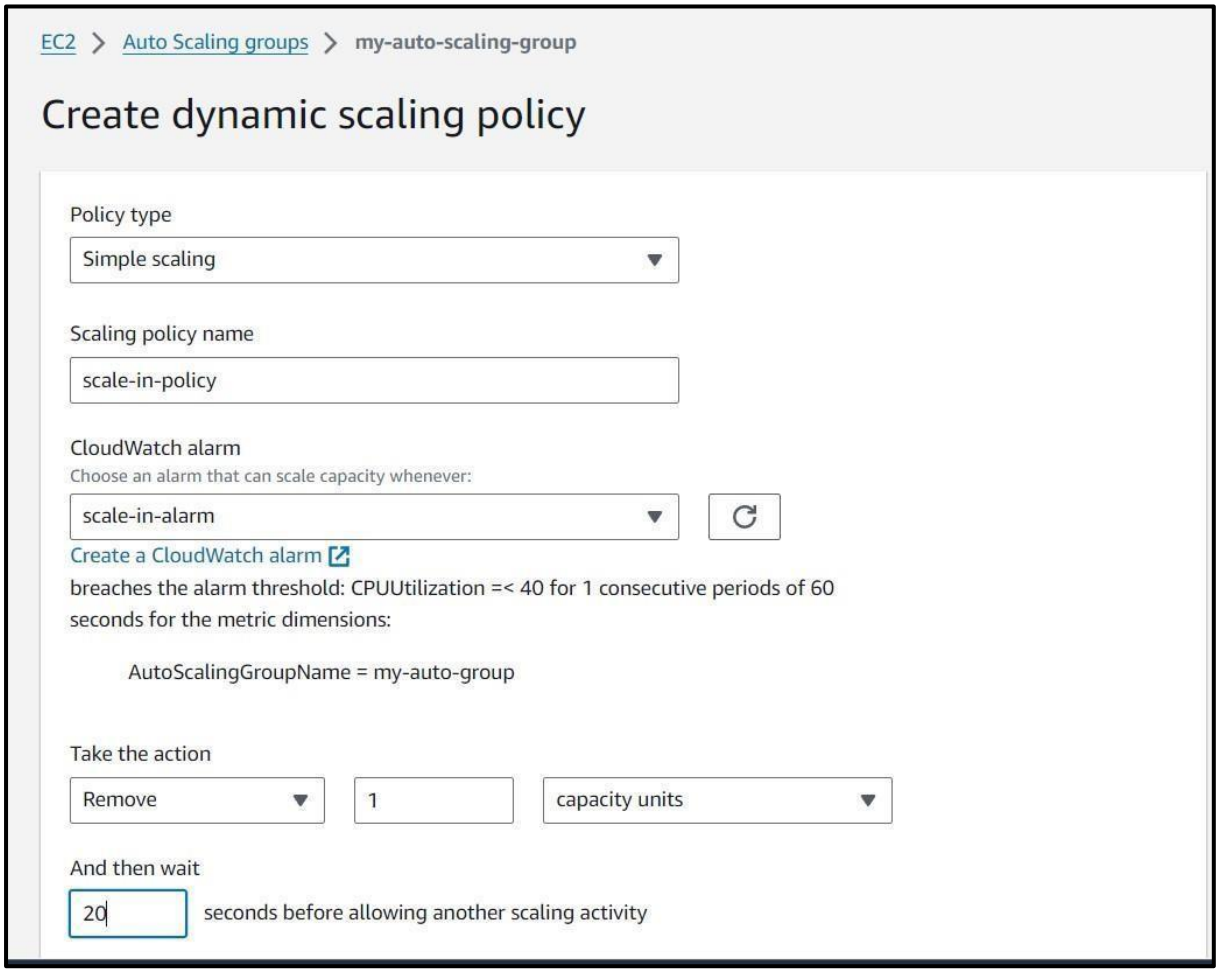

Conditions
Threshold type
Static
Use a value as a threshold
Anomaly detection
Use a band as a threshold
Whenever CPUUtilization is...
Define the alarm condition.
Greater
> threshold
Greater/Equal
>= threshold
Lower/Equal
<= threshold
Lower
< threshold
than...
Define the threshold value.
50
Must be a 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

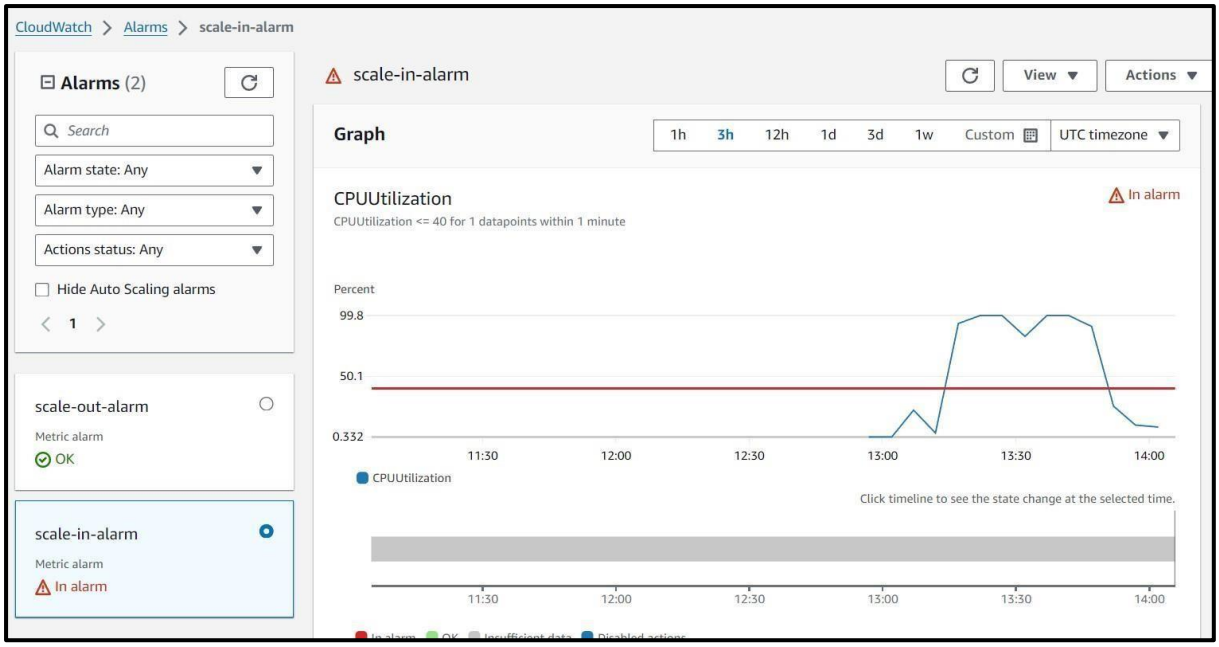
29. Attach Policies to Autoscaling Group

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





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.