

# SCALABLE & SECURE E-COMMERCE PLATFORM ON AWS

## **FINAL REPORT FOR MIDTERM PROJECT**

### **GROUP - 6**

**Team Members :**

**Neonidh Singh - 116009102**

**Goutham Patchipulusu - 120112669**

**Muskan Sagar - 120152764**

**Venkata Umesh Chandra Pothugunta 120427121**

## **TABLE OF CONTENTS**

<b>SCALABLE AND SECURE E-COMMERCE PLATFORM ON AWS</b>	<b>1</b>
<b>TABLE OF CONTENTS</b>	<b>2</b>
<b>OVERVIEW</b>	<b>3</b>
<b>INFRASTRUCTURE SETUP - PHASE 1</b>	<b>4</b>
<b>SECURING THE APPLICATION - PHASE 2</b>	<b>24</b>
<b>CONTENT DELIVERY AND PERFORMANCE OPTIMIZATION - PHASE 3</b>	<b>31</b>
<b>TESTING AND MONITORING - PHASE 4</b>	<b>35</b>
<b>REFERENCES</b>	<b>46</b>

## OVERVIEW

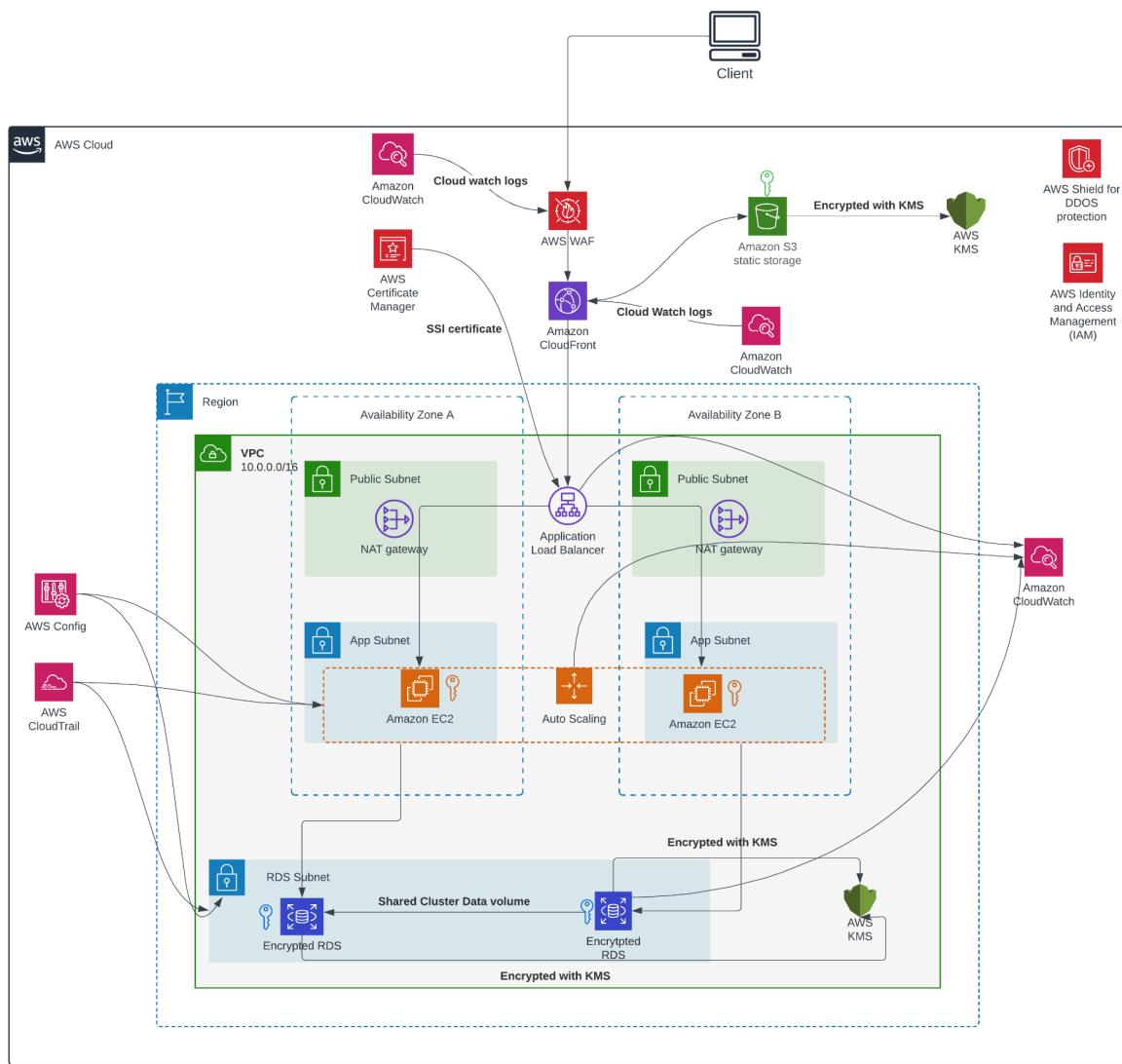
Our group will collaborate on designing, developing, and deploying a scalable e-commerce platform on AWS, focusing on creating a system that can handle fluctuating user traffic, secure customer data, and efficiently deliver content worldwide. To achieve this, we'll use key AWS services, starting with EC2 instances configured with Auto Scaling. This will allow our infrastructure to automatically adjust based on demand, ensuring a responsive platform that doesn't waste resources. Additionally, we'll set up Amazon RDS to securely store customer and product information in a database, ensuring that our data management is both efficient and protected.

Security is a critical component of our project. We'll integrate AWS WAF to defend our application against common cyber threats like SQL injection and cross-site scripting, building a strong layer of protection against potential vulnerabilities. Our team will also configure CloudFront CDN to enhance the speed and efficiency of content delivery, allowing us to cache and serve static assets globally. This setup will ensure that users, no matter their location, experience faster load times and seamless access to the platform, contributing to a better overall experience.

The outcome of our project will be a fully functional, scalable, and secure e-commerce platform hosted on AWS. By the end, we'll have created an infrastructure capable of automatically adjusting to traffic changes, securely storing sensitive data, and delivering fast content globally. Our platform will not only meet current e-commerce standards but will also provide a reliable, user-friendly experience that can scale as needed. This result demonstrates how cloud services can effectively support the growth and security needs of an e-commerce business, equipping us with practical experience in deploying secure, high-performing applications on AWS.

# INFRASTRUCTURE SETUP - PHASE 1

## Architecture Diagram:



## Explanation:

When a user accesses our application, their request first passes through AWS WAF, which acts as the primary layer of defense. The WAF filters out potential threats, such as DDoS attacks or SQL injection attempts. Once the request is validated by WAF, it reaches AWS CloudFront, our Content Delivery Network (CDN) located at edge locations. CloudFront is linked to an S3 bucket that stores images and static files, allowing for faster load times on the Ecommerce platform. The request then flows into the VPC, where the Application Load Balancer (ALB)

determines the optimal EC2 instance within the private subnets across two availability zones, ensuring traffic is directed based on health and availability checks.

To enable internet connectivity, the public subnets use NAT Gateways, allowing EC2 instances in private subnets to access necessary external resources. Auto Scaling is configured to manage fluctuations in demand automatically, scaling EC2 instances up or down within private subnets as needed. On the backend, the EC2 instances connect to an RDS database housed within a private subnet, which holds the ECommerce platform's data tables. Both database storage and network traffic are encrypted to secure all data exchanges.

## **Network Components**

### **AWS VPC (Virtual Private Cloud):**

- **Interaction:**

- This tool creates a private, isolated segment inside the AWS Cloud to allow resources to be securely deployed within a virtual network.
- Offers flexibility to create IP address ranges, configure subnets, and control traffic access via route tables and gateways.
- Facilitates the deployment of AWS resources such as Amazon EC2 instances and Amazon RDS databases within a secure, isolated network environment.

- **Our Approach:**

- We created the VPC. In this template, we defined the CIDR block to be 10.0.0.0/16.

The screenshot shows the AWS VPC dashboard with the following details:

- Your VPCs (1/3) Info:**

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set
VPC-v2	vpc-0a8e3b6415af503a7	Available	10.0.0.0/16	-	dopt-0facf303bb7b45676
MidtermVPC	vpc-012d54e5806a277c3	Available	10.0.0.0/16	-	dopt-0facf303bb7b45676
-	vpc-03b6b4deb8dbfb993	Available	172.31.0.0/16	-	dopt-0facf303bb7b45676
- Resource map:**
  - VPC Show details:** Your AWS virtual network (VPC-v2)
  - Subnets (4):**
    - us-east-1a: subnet-0bd2de0f5a057443b, subnet-0a09fc37c13abda0c
    - us-east-1b: subnet-07b3b408a3cded4c, subnet-013014a631213fb9
  - Route tables (4):**
    - rtb-0b75731fc9c9492c46, rtb-0c058e38fa6f5b671, rtb-01f0604fd1205249e, rtb-0208775f95b1e8e41
  - Network connections (3):**
    - igw-010c81a1b05016db5, nat-09eadc14dd55f33ed, nat-07b44ef5cb2720310

## Subnets:

- **Function:**
  - Divides a VPC into several network segments to control and isolate network traffic effectively.
  - Enables the placement of both publicly accessible resources, such as for our web servers, and privately accessible resources, like our RDS databases.
- **Our Approach:**
  - We created the Public and Private Subnets. We created each with 2 availability zones (US-East-1a and 1b) to make PublicSubnetA and PublicSubnetB, and then PrivateSubnetA and PrivateSubnetB.
  - Each Subnet had a CIDR block of /24.
  - The Public Subnet housed the NAT gateway which allowed the internal EC2 instances to talk to the internet for tasks such as report downloading. The Private Subnet contained the EC2 instances which housed our ECommerce Platform, along with the auto scaling technique that we set up. The Private Subnet also housed our RDS Database.
  - The load balancer allowed the talking of all of the instances to each other since they were housed in private subnets

**VPC dashboard**

**Subnets (1/12) Info**

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
PublicSubnet2	subnet-0fc8412eac9113623	Available	vpc-012d54e5806a277c3   MidtermVPC	10.0.2.0/24	-	-
-	subnet-013014a631213bf9	Available	vpc-0a8e3b6415af503a7   VPC-...	10.0.4.0/24	-	-
-	subnet-0c0454e06f037cbca	Available	vpc-03b6b4de8dfbf993	172.31.32.0/20	-	-
<b>PublicSubnet1</b>	<b>subnet-022a7470acce3290a</b>	<b>Available</b>	<b>vpc-012d54e5806a277c3   MidtermVPC</b>	<b>10.0.1.0/24</b>	<b>-</b>	<b>-</b>

**subnet-022a7470acce3290a / PublicSubnet1**

**Details**

Subnet ID subnet-022a7470acce3290a	Subnet ARN arn:aws:ec2:us-east-1:682033507876:subnet/subnet-022a7470acce3290a	State <span style="color: green;">Available</span>	IPv4 CIDR 10.0.1.0/24
Available IPv4 addresses 248	IPv6 CIDR -	IPv6 CIDR association ID -	Availability Zone us-east-1a
Availability Zone ID use1-az2	Network border group us-east-1	VPC vpc-012d54e5806a277c3   MidtermVPC	Route table rtb-01579ee48c2156701
Network ACL acl-06b2b5c108a0c761	Default subnet No	Auto-assign public IPv4 address No	Auto-assign IPv6 address No
Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -	Outpost ID -	IPv4 CIDR reservations -
IPv6 CIDR reservations -	IPv6-only No	Hostname type IP name	Resource name DNS A record Disabled
Resource name DNS AAAA record		Owner	

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**VPC dashboard**

**Subnets (1/12) Info**

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
<b>PublicSubnet2</b>	<b>subnet-0fc8412eac9113623</b>	<b>Available</b>	<b>vpc-012d54e5806a277c3   MidtermVPC</b>	<b>10.0.2.0/24</b>	<b>-</b>	<b>-</b>
-	subnet-013014a631213bf9	Available	vpc-0a8e3b6415af503a7   VPC-...	10.0.4.0/24	-	-
-	subnet-0c0454e06f037cbca	Available	vpc-03b6b4de8dfbf993	172.31.32.0/20	-	-
<b>PublicSubnet1</b>	<b>subnet-022a7470acce3290a</b>	<b>Available</b>	<b>vpc-012d54e5806a277c3   MidtermVPC</b>	<b>10.0.1.0/24</b>	<b>-</b>	<b>-</b>

**subnet-0fc8412eac9113623 / PublicSubnet2**

**Details**

Subnet ID subnet-0fc8412eac9113623	Subnet ARN arn:aws:ec2:us-east-1:682033507876:subnet/subnet-0fc8412eac9113623	State <span style="color: green;">Available</span>	IPv4 CIDR 10.0.2.0/24
Available IPv4 addresses 248	IPv6 CIDR -	IPv6 CIDR association ID -	Availability Zone us-east-1b
Availability Zone ID use1-az4	Network border group us-east-1	VPC vpc-012d54e5806a277c3   MidtermVPC	Route table rtb-01579ee48c2156701
Network ACL acl-06b2b5c108a0c761	Default subnet No	Auto-assign public IPv4 address No	Auto-assign IPv6 address No
Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -	Outpost ID -	IPv4 CIDR reservations -
IPv6 CIDR reservations -	IPv6-only No	Hostname type IP name	Resource name DNS A record Disabled
Resource name DNS AAAA record		Owner	

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Target group:

- **Function:**
  - Target groups specify where to send traffic within your architecture
  - Target groups monitor the health of their targets by running periodic health checks
- **Our Approach:**
  - We created a target group and attached it to our load balancer so when a user accesses the application, the load balancer distributes incoming requests to the EC2 instances in private subnets within the target group.

The screenshot shows the AWS EC2 Target Groups console. On the left, there's a sidebar with navigation links like EC2 Dashboard, EC2 Global View, Events, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots). The main content area shows the details for a target group named "EC2-Final-TG". The "Details" section includes the ARN: arn:aws:elasticloadbalancing:us-east-1:682033507876:targetgroup/EC2-Final-TG/3585e15e73375682, Target type: Instance, Protocol: Port (HTTP: 80), Protocol version: HTTP1, VPC: vpc-0a8e3b6415af503a7, IP address type: IPv4, Load balancer: MyApplicationALB, and a table showing target status: 2 Total targets (2 Healthy, 0 Unhealthy, 0 Anomalous), 0 Unused, 0 Initial, and 0 Draining. Below this is a section titled "Distribution of targets by Availability Zone (AZ)".

## Compute, Load Balancing, and Data Storage

### Amazon EC2 (Elastic Compute Cloud):

- **Interaction:**
  - EC2 instances to host our e-commerce application, ensuring scalability and flexibility.
  - EC2 was central to enabling the application's ability to handle varying traffic loads efficiently.
- **Our Approach:**
  - **Launch Template:** Configured EC2 instances with Amazon Machine Image(ami-005fc0f236362e99f), instance type (`t3.micro`), and SSH key (`ecommerce-v2`), as well as a custom **UserData** script.
  - **UserData Script:** The script, executed on instance launch, performs several key tasks:

- Updates the system, adds a repository for PHP 8.3, and installs Nginx, PHP, and Git with retries for resilience.
- Clones the e-commerce app from GitHub, transfers the app files to `/var/www/html`, and sets appropriate permissions for Nginx.
- Modifies the app's `connect.php` file to connect to a specified RDS database.
- Sets up a default Nginx server block to serve PHP files and restarts the service to apply configurations.
- **Security Group:** Allows inbound HTTP (port 80) and SSH (port 22) access from any IP address.

## Deployed EC2 instance -

The screenshot shows the AWS CloudFront interface for an EC2 instance. The URL is `us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#InstanceDetails:instanceId=i-0bdff71bdfc4c9a0e`. The main content area displays the 'Instance summary for i-0bdff71bdfc4c9a0e (EC2-FINAL-DEPLOYMENT-AutoScaledEC2V3)' with the following details:

Attribute	Value
Instance ID	i-0bdff71bdfc4c9a0e
IPv6 address	-
Hostname type	IP name: ip-10-0-4-134.ec2.internal
Answer private resource DNS name	-
Auto-assigned IP address	-
IAM Role	-
IMDSv2	Optional EC2 recommends setting IMDSv2 to required   Learn more
Public IPv4 address	-
Private IP DNS name (IPv4 only)	ip-10-0-4-134.ec2.internal
Instance state	Running
Instance type	t3.micro
VPC ID	vpc-0a8e3b6415af503a7 (VPC-v2)
Subnet ID	subnet-013014a631213bfb9
Instance ARN	arn:aws:ec2:us-east-1:682033507876:instance/i-0bdff71bdfc4c9a0e
Private IPv4 addresses	10.0.4.134
Public IPv4 DNS	-
Elastic IP addresses	-
AWS Compute Optimizer finding	<a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>
Auto Scaling Group name	EC2-FINAL-DEPLOYMENT-MyAutoScalingGroupV3-QsbBCLjsjzn

The left sidebar shows navigation links for EC2 Dashboard, EC2 Global View, Events, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images (with sub-links for AMIs, AMI Catalog), Elastic Block Store (with sub-links for Volumes, Snapshots, Lifecycle Manager), and Network & Security (with sub-links for Security Groups).

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#InstanceDetails:instanceId=i-0bdff71bdfc4c9a0e

**Instance details** [Info](#)

Platform	AMI ID	Monitoring
Ubuntu	<a href="#">ami-005fc0f236362e99f</a>	disabled
Platform details	AMI name	Termination protection
Linux/UNIX	<a href="#">ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-a-md64-server-20240927</a>	Disabled
Stop protection	Launch time	AMI location
Disabled	<a href="#">Tue Oct 29 2024 11:32:06 GMT-0400 (Eastern Daylight Time) (about 2 hours)</a>	<a href="#">amazon/ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-20240927</a>
Instance auto-recovery	Lifecycle	Stop-hibernate behavior
Default	normal	Disabled
AMI Launch index	Key pair assigned at launch	State transition reason
0	<a href="#">ecommerce-v2</a>	-
Credit specification	Kernel ID	State transition message
unlimited	-	-
Usage operation	RAM disk ID	Owner
RunInstances	-	<a href="#">682033507876</a>
Enclaves Support	Boot mode	Current instance boot mode
Disabled	<a href="#">uefi-preferred</a>	<a href="#">uefi</a>
Allow tags in instance metadata	Use RBN as guest OS hostname	Answer RBN DNS hostname IPv4
Disabled	<a href="#">Disabled</a>	<a href="#">Disabled</a>
Host ID	Affinity	Placement group
-	-	-

[CloudShell](#) [Feedback](#)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Connection to database from EC2 -

```
ubuntu@ip-10-0-1-100:~$ ssh -i "ecommerce-v2.pem" ubuntu@10.0.4.134
The authenticity of host '10.0.4.134 (10.0.4.134)' can't be established.
ED25519 key fingerprint is SHA256:hm8xDdm/cqhIiWuHxtSajdWqWuvahJcuj/A3S9fofAo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
[Warning: Permanently added '10.0.4.134' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1015-aws x86_64)

 * Documentation:  https://help.ubuntu.com
[ * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Tue Oct 29 17:24:55 UTC 2024

System load: 0.0          Processes:           112
Usage of /:   25.4% of 7.57GB  Users logged in:      0
Memory usage: 27%          IPv4 address for ens5: 10.0.4.134
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

25 updates can be applied immediately.
18 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

2 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm
```

The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo\_root" for details.

```
ubuntu@ip-10-0-4-134:~$ ls
818N-E_Commerce_Application
```

```

ubuntu@ip-10-0-4-134:~$ mysql -h rds-multiaz-myrd$instance-qeruumzj9v4d.ctiowscuz1b.us-east-1.rds.amazonaws.com -u dbadmin -p ecommerce_1
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1237
Server version: 8.0.39 Source distribution

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 

```

## Security group configuration -

(only ALB can communicate with EC2)

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0b6dba84faccfec80	SSH	TCP	22	Custom	0.0.0.0 / 0
sgr-04a987b6b115a5fe3	HTTP	TCP	80	Custom	sg-0f4b8548d4d849705

## Auto Scaling:

- **Interaction:**
  - To support high availability and manage traffic surges, we placed the EC2 instances in an Auto Scaling Group.
  - The ASG allowed for dynamic scaling, automatically adjusting the number of instances based on CPU usage thresholds, and optimizing cost-effectiveness.
- **Our Approach:**
  - Defined the ASG to deploy EC2 instances in specified private subnets.
  - We have set the MinSize to 1, MaxSize to 4, and DesiredCapacity to 2, providing a balance between resource availability and cost efficiency.

- Configured EC2-based health checks with a 5-minute grace period, which allows new instances to stabilize before they are monitored for health.

## Auto-scaling group -

The screenshot shows the AWS Auto Scaling Groups console with the following details:

**Group details**

Auto Scaling group name	Desired capacity	Desired capacity type	Amazon Resource Name (ARN)
EC2-FINAL-DEPLOYMENT-MyAutoScalingGroupV3-QsbBCLjfsjzn	2	Units (number of instances)	<input type="text"/> arn:aws:autoscaling:us-east-1:682033507876:autoScalingGroup:a10e1f3d-60b2-416b-92ee-250757e0cee0:autoScalingGroupName/EC2-FINAL-DEPLOYMENT-MyAutoScalingGroupV3-QsbBCLjfsjzn
Date created	Minimum capacity	Status	
Tue Oct 29 2024 11:31:54 GMT-0400 (Eastern Daylight Time)	1	<input type="text"/> Updating capacity	
	Maximum capacity		
	4		

**Launch template**

Launch template	AMI ID	Instance type	Owner
<input type="text"/> lt-0c726053ee39d8ef3 EC2-FINAL-DEPLOYMENT-LaunchTemplateV3	<input type="text"/> ami-005fc0f236362e99f	t3.micro	arn:aws:iam::682033507876:root
Version	Security groups	Security group IDs	Create time
-		<input type="text"/> sg-000000000000000000	-

## Auto-scaling policies -

The screenshot shows the AWS CloudFormation console with the EC2 service selected. On the left, a sidebar lists various EC2-related options like Instances, Images, and Launch Templates. Two Auto Scaling policies are displayed in the main pane:

- EC2-FINAL-DEPLOYMENT-ScaleDownPolicyV3-**  
nXcSTsuPCzHf  
Policy type: Simple scaling  
Enabled or disabled: Enabled  
Execute policy when: EC2-FINAL-DEPLOYMENT-ScaleDownAlarm-LlhTlpT8NAE breaches the alarm threshold: CPUUtilization < 10 for 1 consecutive periods of 30 seconds for the metric dimensions:  
AutoScalingGroupName = EC2-FINAL-DEPLOYMENT-MyAutoScalingGroupV3-QsbBCLjfsjzn  
Take the action: Remove 1 capacity units  
And then wait: 300 seconds before allowing another scaling activity
- EC2-FINAL-DEPLOYMENT-ScaleUpPolicyV3-**  
DmqKgZwhnRBL  
Policy type: Simple scaling  
Enabled or disabled: Enabled  
Execute policy when: EC2-FINAL-DEPLOYMENT-ScaleUpAlarm-29iiZVkWNnDI breaches the alarm threshold: CPUUtilization > 20 for 1 consecutive periods of 30 seconds for the metric dimensions:  
AutoScalingGroupName = EC2-FINAL-DEPLOYMENT-MyAutoScalingGroupV3-QsbBCLjfsjzn  
Take the action: Add 1 capacity units  
And then wait: 300 seconds before allowing another scaling activity

## Cloud Watch Alarms:

- **Interaction:**
  - CloudWatch metrics were monitored to track CPU utilization, memory usage, and network activity, helping us fine-tune the scaling policies for optimal performance.
- **Our Approach:**
  - **Scale-Up Policy:** Increase the ASG's instance count by one if triggered.
  - **Scale-Down Policy:** Decrease the ASG's instance count by one if triggered.
  - **ScaleUpAlarm:** Monitors CPU utilization of instances in the ASG and triggers the **Scale-Up Policy** if average CPU usage exceeds 20% for 30 seconds.
  - **ScaleDownAlarm:** Triggers the **Scale-Down Policy** if CPU usage drops below 10% for 30 seconds, allowing the ASG to reduce instance count during low usage.

AWS Services Search [Option+S] N. Virginia ENPM818N-Group6

**CloudWatch**

Favorites and recent dashboards

Alarms △ 1 ○ 1 ○ 2

In alarm

All alarms

Billing

Logs

Metrics

X-Ray traces

Events

Application Signals

Network monitoring

Insights △ 0

Settings

Getting Started

What's new

CloudFormation EC2

CloudWatch > Alarms > EC2-FINAL-DEPLOYMENT-ScaleUpAlarm-29iiZVkWNnDI

Alarms (4)

Search

Alarm state: Any

Alarm type: Any

Actions status: Any

Hide Auto Scaling alarms

EC2-FINAL-DEPLOYMENT-ScaleUpAlarm-29iiZVkWNnDI

Metric alarm

○ Insufficient data

EC2-FINAL-DEPLOYMENT-ScaleUpAlarm-29iiZVkWNnDI

Metric alarm

○ Insufficient data

EC2-FINAL-DEPLOYMENT-ScaleUpAlarm-29iiZVkWNnDI

Metric alarm

○ Insufficient data

EC2-FINAL-DEPLOYMENT-ScaleUpAlarm-29iiZVkWNnDI

Metric alarm

○ Actions enabled

Details

Tags Actions History Parent alarms

**Details**

Name	State	Namespace	Datapoints to alarm
EC2-FINAL-DEPLOYMENT-ScaleUpAlarm-29iiZVkWNnDI	○ Insufficient data	AWS/EC2	1 out of 1
Type	Threshold	Metric name	Missing data treatment
Metric alarm	CPUUtilization > 20 for 1 datapoints within 30 seconds	AutoScalingGroupName	Treat missing data as missing
Description	Last state update 2024-10-29 20:07:11 (Local)	EC2-FINAL-DEPLOYMENT-MyAutoScalingGroupV3-QsbBCLjfsjn	Percentiles with low samples evaluate
Scale up if CPU > 20% for 30 Seconds	Actions	Statistic	ARN
	○ Actions enabled	Average	arn:aws:cloudwatch:us-east-1:682033507876:alarm:E2-FINAL-DEPLOYMENT-ScaleUpAlarm-29iiZVkWNnDI
		Period	
		30 seconds	

View EventBridge rule

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Option+S] N. Virginia ENPM818N-Group6

**CloudWatch**

Favorites and recent dashboards

Alarms △ 1 ○ 1 ○ 2

In alarm

All alarms

Billing

Logs

Metrics

X-Ray traces

Events

Application Signals

Network monitoring

Insights △ 0

Settings

Getting Started

What's new

CloudFormation EC2

CloudWatch > Alarms > EC2-FINAL-DEPLOYMENT-ScaleDownAlarm-LlhtTLpT8NAE

Alarms (4)

Search

Alarm state: Any

Alarm type: Any

Actions status: Any

Hide Auto Scaling alarms

EC2-FINAL-DEPLOYMENT-ScaleDownAlarm-LlhtTLpT8NAE

Metric alarm

○ Insufficient data

EC2-FINAL-DEPLOYMENT-ScaleDownAlarm-LlhtTLpT8NAE

Metric alarm

○ Insufficient data

EC2-FINAL-DEPLOYMENT-ScaleUpAlarm-29iiZVkWNnDI

Metric alarm

○ Insufficient data

EC2-FINAL-DEPLOYMENT-ScaleUpAlarm-29iiZVkWNnDI

Metric alarm

○ Actions enabled

Details

Tags Actions History Parent alarms

**Details**

Name	State	Namespace	Datapoints to alarm
EC2-FINAL-DEPLOYMENT-ScaleDownAlarm-LlhtTLpT8NAE	○ Insufficient data	AWS/EC2	1 out of 1
Type	Threshold	Metric name	Missing data treatment
Metric alarm	CPUUtilization < 10 for 1 datapoints within 30 seconds	AutoScalingGroupName	Treat missing data as missing
Description	Last state update 2024-10-29 20:07:12 (Local)	EC2-FINAL-DEPLOYMENT-MyAutoScalingGroupV3-QsbBCLjfsjn	Percentiles with low samples evaluate
Scale down if CPU < 10% for 30 seconds	Actions	Statistic	ARN
	○ Actions enabled	Average	arn:aws:cloudwatch:us-east-1:682033507876:alarm:E2-FINAL-DEPLOYMENT-ScaleDownAlarm-LlhtTLpT8NAE
		Period	
		30 seconds	

View EventBridge rule

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Load Balancer:

### Application Load Balancer:

- **Interaction:**

- Able to distribute incoming HTTPS traffic across our EC2 instances and balance the load accordingly
- This ALB helps maintain availability for our platform and help with our zero downtime value
- Can check which instances are healthy and route traffic to the ones that are healthier to keep a balanced vision

- **Our Approach:**

- We set up a ALB to help forward the traffic for our ECommerce platform
- We made a security group for the ALB, and allowed access from port 443 for HTTPS inbound traffic
- We made a listener for the ALB on port 443 and secured the traffic using a SSL certificate for secure traffic

The screenshot shows the AWS EC2 Load Balancers console. The main view displays the details of an Application Load Balancer named "MyApplicationALB". Key information shown includes:

- Load balancer type:** Application
- Status:** Active
- VPC:** [vpc-0a8e3b6415af503a7](#)
- Load balancer IP address type:** IPv4
- Scheme:** Internet-facing
- Hosted zone:** Z35SXDOTRQ7X7K
- Availability Zones:** us-east-1a (use1-az2), us-east-1b (use1-az4)
- Date created:** October 24, 2024, 19:49 (UTC-04:00)
- Load balancer ARN:** arn:aws:elasticloadbalancing:us-east-1:682033507876:loadbalancer/app/MyApplicationALB/01a30b0d584164d8
- DNS name:** [MyApplicationALB-99927605.us-east-1.elb.amazonaws.com](#) (A Record)

The navigation pane on the left lists other services like EC2 Dashboard, EC2 Global View, Events, Instances, Images, and Elastic Block Store.

AWS Services Search [Option+S] N. Virginia ENPM818N-Group6

CloudFormation EC2

EC2 Dashboard EC2 Global View Events Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations New

Images AMIs AMI Catalog

Elastic Block Store Volumes Snapshots Lifecycle Manager

Network & Security Security Groups

**Load balancer type**: Application **Status**: Active **VPC**: [vpc-0a8e3b6415af503a7](#) **Load balancer IP address type**: IPv4

**Scheme**: Internet-facing **Hosted zone**: Z35SXDOTRQ7X7K **Availability Zones**: [subnet-0bd2de0f5a057443b](#) us-east-1a (use1-az2) [subnet-07b3b408a3cdead4c](#) us-east-1b (use1-az4)

**Date created**: October 24, 2024, 19:49 (UTC-04:00)

**Load balancer ARN**: [arn:aws:elasticloadbalancing:us-east-1:682033507876:loadbalancer/app/MyApplicationALB/01a30b0d584164db](#)

**DNS name Info**: [MyApplicationALB-99927605.us-east-1.elb.amazonaws.com \(A Record\)](#)

**Listeners and rules** (1) [Info](#) Manage rules Manage listener Add listener

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.

Filter listeners 1 / 1 [Edit](#)

Protocol:Port	Default action	Rules	ARN	Security policy
HTTPS:443	<b>Forward to target group</b> <ul style="list-style-type: none"> <li><a href="#">EC2-Final-TG</a>: 1 (100%)</li> <li>Target group stickiness: Off</li> </ul>	1 rule	<a href="#">ARN</a>	ELBSecurityPolicy-TLS13-1-2...

## **Amazon RDS (Relational Database Service):**

- **Function:**
  - Streamlines the configuration, management, and scaling of a relational database, making it easier to integrate into applications.
  - Delivers cost-effective and scalable capacity while handling tedious database administration tasks, allowing you to prioritize applications and business objectives.
- **Interaction:**
  - Connects seamlessly with AWS Identity and Access Management (IAM) to regulate access to RDS instances, enabling precise control over management privileges.
  - Engages with Amazon EC2 instances to furnish database services for applications operating within EC2, guaranteeing streamlined data retrieval and storage processes.
- **Approach:**
  - We selected MySQL as the database engine due to its reliability, performance, and support for a wide range of applications.
  - Multi-AZ deployment was enabled to enhance the availability and fault tolerance of the database.
  - Amazon Key Management Service (KMS) was used to encrypt the database at rest.
  - A security group was configured to control access to the RDS instance, allowing only trusted EC2 instances to communicate with the database. The subnet configuration was defined to ensure the RDS instance operates within a secure Virtual Private Cloud (VPC), providing network isolation and enhanced security.

The screenshot shows the AWS RDS Configuration page for a MySQL instance. The 'Encryption Enabled' and 'Multi-AZ Yes' fields are highlighted with red boxes.

Configuration	Instance class	Storage	Performance Insights
DB instance ID rds-multiaz-myrdinstance-qeruumzj9v4d	Instance class db.t3.micro	Encryption Enabled AWS KMS key aws/rds	Performance Insights enabled Turned off
Engine version 8.0.39	vCPU 2	Storage type General Purpose SSD (gp2)	
RDS Extended Support Enabled	RAM 1 GB	Storage 5 GiB	
DB name -	Availability	Provisioned IOPS -	
License model General Public License	Master username dbadmin	Storage throughput -	
Option groups <b>default:mysql-8-0</b> <span style="color: green;">In sync</span>	Master password *****	Storage autoscaling Disabled	
Amazon Resource Name (ARN) <code>arn:aws:rds:us-east-1:682033507876:db:rds-multiaz-myrdinstancे-queruumzj9v4d</code>	IAM DB authentication Not enabled	Storage file system configuration Current	
	Multi-AZ Yes		
	Secondary Zone		

Only EC2 can communicate with RDS -

The screenshot shows the AWS EC2 Security Groups Inbound Rules page. A rule for MySQL/Aurora is shown, with the target IP address 'sg-05f0f4c69abfe01d8' highlighted with a red box.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-099495e9705314aa	MySQL/Aurora	TCP	3306	Custom	<input type="text" value="sg-05f0f4c69abfe01d8"/> <span style="color: red;">X</span>

## Encrypted password in database -

```
ubuntu@ip-10-0-4-134:~$ mysql -h rds-multiaz-myrd$instance-qeruumzj9v4d.ctiowscuczib.us-east-1.rds.amazonaws.com -u dbadmin -p ecommerce_1
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1237
Server version: 8.0.39 Source distribution

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use ecommerce_1;
Database changed
mysql> Show tables;
+-----+
| Tables_in_ecommerce_1 |
+-----+
| admin_table
| brands
| card_details
| categories
| orders_pending
| products
| user_orders
| user_payments
| user_table
+-----+
9 rows in set (0.00 sec)

mysql> SELECT * FROM admin_table;
+-----+
| admin_id | admin_name | admin_email | admin_image | admin_password |
+-----+
| 1 | abdo | abdo@gmail.com | logo after 3d_2.png | $2y$10$M/A/r5j/GSeJrAZxI8NtRu9eG5yNltfgTrfQVoClfSIF/pzNUxa2W |
+-----+
1 row in set (0.00 sec)
```

## DEPLOYED APPLICATION

The screenshot shows a web browser displaying a deployed e-commerce application. The URL in the address bar is `app.somedomain.store`. The page features a black header bar with the text "Summer Sale For All Swim Suits And Free Express Delivery - OFF 50%! [Shop Now](#)". Below this is a navigation bar with links for Home, Products, About, Contact, Register, Search, a shopping cart icon with "1", and user account links for "Welcome guest" and "Login".  
On the left side, there is a sidebar titled "A1" containing a list of categories: Women's Fashion, men's Fashion, Electronics, Home & lifestyle, Medicine, Sports & Outdoor, Baby's & Toys, and Health & Beauty. Each category has a small arrow icon to its right.  
The main content area features a large promotional banner for the iPhone 14 series. It includes the text "Iphone 14 series", "Up to 10% off Voucher", and a link "[Shop now ->](#)". To the right of the text is a photograph of two iPhone 14 phones, one in a light color and one in a dark color, showing their rear camera systems.  
Below the banner, there is a section titled "Categories" with a red icon. Under this section, the text "Browse By Category" is displayed, followed by a grid of six categories: Phones, Computers, SmartWatch, Camera, Gaming, and HeadPhones. Each category has a small icon above it.

## CRUD OPERATIONS VIA E-COMMERCE PLATFORM

### LOGIN

The screenshot shows a login form for the application. The URL in the address bar is `app.somedomain.store/users_area/user_login.php`.  
The form consists of two input fields: "Username" and "Password", both with placeholder text "Enter your". Below the password field is a link "[Forgot your password?](#)".  
At the bottom of the form is a red "Login" button. To the right of the form, a modal dialog box is open, displaying the text "app.somedomain.store says" and "Login Successfully". A blue "OK" button is visible in the bottom right corner of the dialog.  
At the very bottom of the page, there is a link "Don't have an account? [Register](#)".

← → ⌛ app.somedomain.store

Summer Sale For All Swim Suits And Free Express Delivery - OFF 50%! [Shop Now](#)

A1 Home Products About Contact My Account Search [Search](#) [Cart 1](#) [Welcome abc](#) [Logout](#)

Women's Fashion >



## ADDING/UPDATING TO CART -

A1 Home Products About Contact My Account Search [Search](#) [Cart 1](#) [Welcome abc](#) [Logout](#)

Product Title	Product Image	Quantity	Total Price	Remove	Operations
HAVIT HV-G92 Gamepad		<input type="text" value="1"/>	120	<input type="checkbox"/>	<a href="#">Update</a> <a href="#">Remove</a>

**Sub-Total: 120** [Continue Shopping](#) [Continue Shopping](#) [Checkout](#) [Checkout](#)

→ ⌛ app.somedomain.store/cart.php

Summer Sale For All Swim Suits And Free Express Delivery - OFF 50%! [Shop Now](#)

A1 Home Products About Contact My Account Search [Search](#) [Cart 1](#) [Welcome abc](#) [Logout](#)

Product Title	Product Image	Quantity	Total Price	Remove	Operations
HAVIT HV-G92 Gamepad		<input type="text" value="2"/>	120	<input type="checkbox"/>	<a href="#">Update</a> <a href="#">Remove</a>

**Sub-Total: 240** [Continue Shopping](#) [Continue Shopping](#) [Checkout](#) [Checkout](#)

## ORDER PLACED

The screenshot shows a web application interface. At the top, there is a navigation bar with links for Home, Products, About, Contact, My Account, Search, and a shopping cart icon with '0' items. A banner at the top of the page reads "Summer Sale For All Swim Suits And Free Express Delivery - OFF 50%! Shop Now". On the left, there is a sidebar with a profile photo placeholder ("abc photo"), sections for Pending Orders, Edit Account, My Orders, Delete Account, and Logout. The main content area is titled "All my orders" and displays a table with one row of data:

Serial NO.	Order Number	Amount due	Total Products	Invoice Number	Date	Status	Confirm
1	4	700	1	1198053792	2024-10-29 18:10:43	pending	<a href="#">Confirm</a>

## DATABASE AFTER THE ABOVE OPERATIONS

```

mysql> use ecommerce_1;
Database changed
mysql> show tables;
+-----+
| Tables_in_ecommerce_1 |
+-----+
| admin_table           |
| brands                |
| card_details          |
| categories            |
| orders_pending         |
| products              |
| user_orders            |
| user_payments          |
| user_table             |
+-----+
9 rows in set (0.00 sec)

mysql> SELECT * FROM admin_table;
+-----+
| admin_id | admin_name | admin_email | admin_image |
+-----+
| 1       | abdo      | abdo@gmail.com | logo after 3d_2.png |
+-----+
1 row in set (0.00 sec)

mysql> SELECT * FROM user_table;
+-----+
| user_id | username | user_email | user_password | user_image | user_ip | user_address | user_mobile |
+-----+
| 1       | abdo     | abdo@gmail.com | $2y$10$5ynby9fq7wf2ZmH1kvehu.JGbK6r7zZLtzJz9Jt5FP03rGZ9Mj. | new logo after Edit1920.png | ::1    | Cairo        | 123456789 |
| 2       | abc      | abc@gmail.com | $2y$10$xwYuOxwwQQTk.RrKEqQveQ1/VZxgA5tTyz7DfKRe8pgL5FzaV2u | apple.png | 69.137.236.162 | street 123, apt 303 | 123456789 |
+-----+
2 rows in set (0.00 sec)

mysql> SELECT * FROM user_orders;
+-----+
| order_id | user_id | amount_due | invoice_number | total_products | order_date | order_status |
+-----+
| 1       | 1       | 1160      | 312346784    | 3             | 2023-10-22 15:31:28 | paid      |
| 2       | 1       | 769       | 1918753782   | 1             | 2023-10-24 00:25:18 | pending   |
| 3       | 1       | 249       | 351837813    | 1             | 2023-10-24 18:41:02 | pending   |
| 4       | 2       | 700       | 1198053792   | 1             | 2024-10-29 18:10:43 | pending   |
+-----+
4 rows in set (0.01 sec)

```

## SECURING THE APPLICATION - PHASE 2

### Introduction:

- In building an e-commerce application, one of the main concerns is to ensure the application is secure from any kind of security breaches.
- A security threat not only risks exposing sensitive information but also results in significant reputational damage and regulatory problems.
- To help mitigate this trouble we have to secure the application's infrastructure through AWS services which focus on application security and data protection.

In this phase we specially target **two critical security areas**:

- Protecting the application from web-based attacks using Web Application Firewall (WAF)
- Securing the data in transit between clients, the application servers, and the backend database

### AWS Web Application Firewall (WAF):

- **Interaction:**
  - AWS WAF blocks known attack patterns and web-based exploits such as SQL Injection and Cross-Site Scripting (XSS) by using the defined rules in WAF
  - AWS WAF inspects incoming traffic to the ALB, blocking threats before they reach application servers
  - Real-time WAF metrics and alarms in CloudWatch allow proactive monitoring and security responses

The screenshot shows the AWS WAF console interface. The top navigation bar includes tabs for Traffic overview, Rules, Associated AWS resources (which is currently selected), Custom response bodies, Logging and metrics, Sampled requests, and CloudWatch Log Insights. Below the navigation bar, a section titled "Associated AWS resources (1)" displays a table with one row. The table has columns for Name, Resource type, and Region. The single entry is "MyApplicationALB" (Application Load Balancer, US East (N. Virginia)). There are buttons for Disassociate and Add AWS resources, along with navigation controls for pages 1 and 2.

Name	Resource type	Region
MyApplicationALB	Application Load Balancer	US East (N. Virginia)

- **Our Approach:**

- We have set up WAF by creating a Web ACL (WAF-v2) to secure the platform

The screenshot shows the AWS WAF & Shield console with the 'Web ACLs' page selected. A single Web ACL named 'WAF-v2' is listed. The interface includes a search bar, a 'Create web ACL' button, and various navigation and configuration options.

- The WAF rules used for this project were selected to cover the most common and impactful web-based threats. They are:
  - **AWS-AWSManagedRulesSQLiRuleSet** : To detect and block the SQL injection attacks, which could allow unauthorized access or any unallowed CRUD operations to the database.
  - **AWS-AWSManagedRulesCommonRuleSet** : Adds an additional layer of security to the application and provides general protection against common vulnerabilities and other known attack patterns.

This screenshot shows the detailed configuration of the 'WAF-v2' Web ACL. The 'Rules' tab is active, listing two rules: 'AWS-AWSManagedRulesSQLiRuleSet' and 'AWS-AWSManagedRulesCommonRuleSet'. Below the rules, it shows the total WCUs used (900/5000 WCUs) and the default action for unmatched requests (Allow). The interface includes tabs for Traffic overview, Rules, Associated AWS resources, Custom response bodies, Logging and metrics, Sampled requests, and CloudWatch Log Insights.

- Amazon CloudWatch is integrated to monitor the Web ACL's performance and effectiveness. By enabling CloudWatch logging, insights into blocked requests, allowed requests, and frequently matched rules are analyzed carefully.

CloudWatch > Logs Insights

**Logs Insights** Info

Select log groups, and then run a query or [choose a sample query](#).

Start tailing
5m
30m
1h
3h
12h
Custom
Compare (Off)
UTC timezone ▾

Select up to 50 log groups.

aws-waf-logs-v4 X

Clear all

```
1 fields @timestamp, @message
2 | filter webaclId = 'arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c'
3 | sort @timestamp desc
4 | limit 20
```

Query generator

Browse log groups

Discovered fields

Queries

Run query

Cancel

Save

History

Logs Insights query can run for maximum of 60 minutes.

Logs (20)

Patterns (-)

Visualization

Export results ▾

Add to dashboard

...

Logs (20)

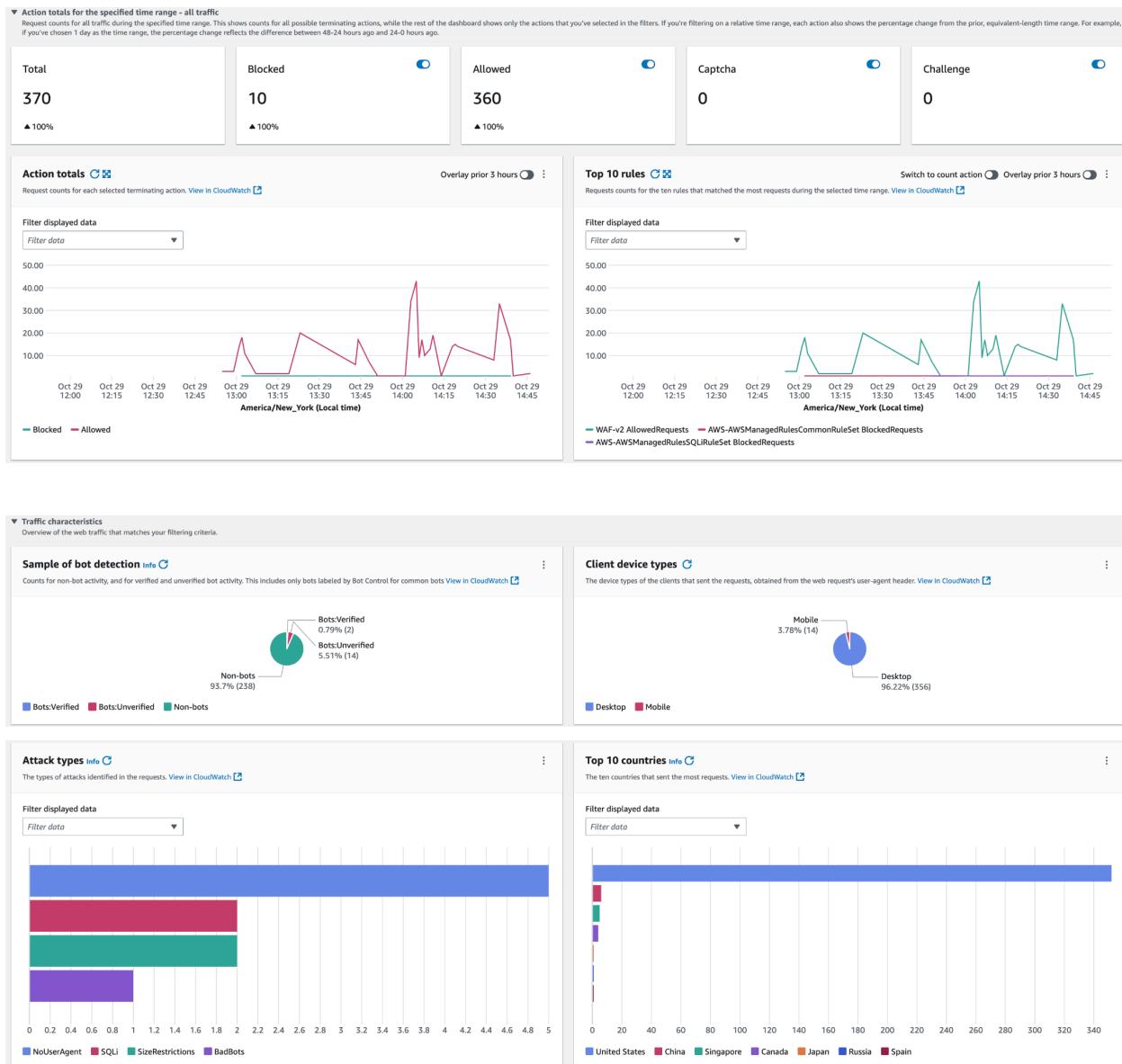
Hide histogram

Showing 20 of 27 records matched ⓘ

27 records (53.1 kB) scanned in 0.8s at 32 records/s (63.0 kB/s)

A histogram showing the distribution of log records over time. The x-axis represents time from 01:10 to 02:05. The y-axis represents the number of records from 0 to 15. A single blue bar is visible at 01:25, reaching a height of approximately 14.

#	@timestamp	@message
► 1	2024-10-29T01:37:29.9...	{"@timestamp": "1730165849973", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "1", "version": 1}
► 2	2024-10-29T01:26:44.8...	{"@timestamp": "1730165204812", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "2", "version": 1}
► 3	2024-10-29T01:26:26.6...	{"@timestamp": "1730165186663", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "3", "version": 1}
► 4	2024-10-29T01:26:03.1...	{"@timestamp": "1730165163189", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "4", "version": 1}
► 5	2024-10-29T01:26:03.1...	{"@timestamp": "1730165163160", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "5", "version": 1}
► 6	2024-10-29T01:26:01.4...	{"@timestamp": "1730165161482", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "6", "version": 1}
► 7	2024-10-29T01:26:01.4...	{"@timestamp": "1730165161438", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "7", "version": 1}
► 8	2024-10-29T01:25:39.9...	{"@timestamp": "1730165139905", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "8", "version": 1}
► 9	2024-10-29T01:25:36.9...	{"@timestamp": "1730165136958", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "9", "version": 1}
► 10	2024-10-29T01:25:36.9...	{"@timestamp": "1730165136954", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "10", "version": 1}
► 11	2024-10-29T01:25:36.9...	{"@timestamp": "1730165136901", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "11", "version": 1}
► 12	2024-10-29T01:25:31.0...	{"@timestamp": "1730165131044", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "12", "version": 1}
► 13	2024-10-29T01:25:30.6...	{"@timestamp": "1730165130627", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "13", "version": 1}
► 14	2024-10-29T01:25:30.5...	{"@timestamp": "1730165130515", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "14", "version": 1}
► 15	2024-10-29T01:25:30.5...	{"@timestamp": "1730165130515", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "15", "version": 1}
► 16	2024-10-29T01:25:30.5...	{"@timestamp": "1730165130515", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "16", "version": 1}
► 17	2024-10-29T01:25:30.5...	{"@timestamp": "1730165130514", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "17", "version": 1}
► 18	2024-10-29T01:25:30.5...	{"@timestamp": "1730165130513", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "18", "version": 1}
► 19	2024-10-29T01:25:30.5...	{"@timestamp": "1730165130507", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "19", "version": 1}
► 20	2024-10-29T01:25:30.4...	{"@timestamp": "1730165130458", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:682033507876:regional/webacl/WAF-v2/0f966df4-8492-4282-8ec3-c7c9942ffc7c", "terminatingRuleId": "20", "version": 1}



- **Test:** We conducted a proxy SQL injection test on the platform firewall using the command ' OR '1'='1 --. The attempt was successfully blocked by the AWSManagedRulesSQLiRuleSet in WAF.

Summer Sale For All Swim Suits And Free Express Delivery - OFF 50%! [Shop Now](#)

A1
[Home](#) [Products](#) [About](#) [Contact](#) [Register](#)


x
Search
!
Welcome guest
Login

---

[Women's Fashion >](#)
  
[men's Fashion >](#)
  
[Electronics](#)
  
[Home & lifestyle](#)
  
[Medicine](#)
  
[Sports & Outdoor](#)
  
[Baby's & Toys](#)
  
[Health & Beauty](#)

iPhone 14 series

Up to 10% off Voucher

[Shop now ->](#)

Categories

Phones
 Computers
 SmartWatch
 Camera
 Gaming
 HeadPhones

▼ 61	2024-10-29T18:39:29.3...
Field	Value
@ingestionTime	1730227186246
@log	682033587876:aws-waf-logs-v4
@logStream	us-east-1_WAF-v2_0
@message	<pre>{"@timestamp": "1730227169385", "formatVersion": 1, "webaclId": "arn:aws:wafv2:us-east-1:162203350767:regions/us-east-1/WAF/VAZ/v2/f9f6d74-4492-4282-8ec3-07c942fffc7c", "terminatingRuleId": "AWS-AWSManagerRulesSQLRuleSet1", "terminatingRuleType": "MANAGED_RULE_GROUP", "action": "BLOCK", "terminatingRuleMatchDetails": [{"conditionType": "SQL_INJECTION", "location": "BODY", "matchedData": ["user_username"], "operator": "OR", "value": ""}], "matchedRuleName": "", "sensitivityLevel": "LOW"}, {"httpSourceName": "ALB", "httpSourceId": "682033397876-app/MyApplicationLB/01a3b0bd58416408", "ruleGroupList": [{"ruleGroupId": "AWSLambdaNameRulesSQLRuleSet", "terminatingRule": {"ruleId": "SQL_BODY", "action": "BLOCK", "ruleMatchDetails": []}, "nonTerminatingMatchingRules": []}, {"ruleGroupId": "AWSLambdaNameRulesSQLRuleSet", "terminatingRule": {"ruleId": "SQL_BODY", "action": "BLOCK", "ruleMatchDetails": []}, "nonTerminatingMatchingRules": []}], "excludedRules": null, "customerConfig": null}, {"@retainedRuleList": [], "nonTerminatingMatchingRules": []}, {"@requestHeadersInserted": null, "responseCodeSent": null, "httpRequest": {"clientIp": "69.132.232.252", "country": "US", "headers": [{"name": "host", "value": "app.somedomain.store"}, {"name": "content-length", "value": "100"}, {"name": "cache-control", "value": "max-age=0"}, {"name": "sec-ch-usa", "value": "chromium"}, {"name": "sec-ch-ua", "value": "\"Chromium\";v=\"138\", \"Google Chrome\";v=\"138\", \"Not_A_Brand\";v=\"99\""}, {"name": "sec-ch-ua-mobile", "value": "70"}, {"name": "sec-ch-ua-platform", "value": "macOS"}, {"name": "origin", "value": "https://app.somedomain.store"}, {"name": "content-type", "value": "application/x-www-form-urlencoded"}, {"name": "upgrade-insecure-requests", "value": "1"}, {"name": "user-agent", "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/137.36"}, {"name": "accept", "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7"}, {"name": "sec-fetch-site", "value": "same-origin"}, {"name": "sec-fetch-mode", "value": "navigate"}, {"name": "sec-fetch-user", "value": "?1"}, {"name": "sec-fetch-dst", "value": "document"}, {"name": "referrer", "value": "https://app.somedomain.store/users_area/user_login.php"}, {"name": "accept-encoding", "value": "gzip, deflate, br, zstd"}, {"name": "accept-language", "value": "en-US,en;q=0.9"}, {"name": "priority", "value": "u=0, 1"}, {"name": "cookie", "value": "JSESSIONID=k7vlp5si2oeiqmjicub9c10"}, {"url": "/users_area/user_login.php", "args": "", "httpVersion": "HTTP/2.0", "httpMethod": "POST", "requestId": "1-67212be1-37f9f2d2241f87372bf333c"}, "labels": [{"name": "awsel:managed:aws:sql-database:SQL1_Body"}], "requestBodySize": 100, "requestBodySizeInspectedByWAF": 100, "ja3Fingerprint": "07ec163066a81b3fdddab6c78eb9707"}}</pre>
@timestamp	1730227169385
action	BLOCK
formatVersion	1

## Ensuring a secure data transit through AWS Certificate Manager:

- **Interaction:**
  - ACM provides SSL certificates to the ALB, enabling HTTPS and encrypting data in transit between clients and the application.
  - ACM certificate is applied to the ALB to continue to provide SSL/TLS encryption, even as EC2 instances are scaled in and out.
- **Our Approach:**
  - A certificate was issued to our domain name (app.somedomain.store) and by AWS Certificate Manager.
  - Using ACM, a HTTPS listener was added to our load balancer to establish a secure entry point for all incoming traffic, which is crucial in protecting data and providing a trustworthy user experience.

27b63043-597f-407d-9cc9-c9be3de47d18

[Reimport](#) [Delete](#)

### Certificate status

Identifier 27b63043-597f-407d-9cc9-c9be3de47d18	Status <span style="color: green;">Issued</span>
ARN <a href="#">arn:aws:acm:us-east-1:682033507876:certificate/27b63043-597f-407d-9cc9-c9be3de47d18</a>	
Type Imported	

### Domains (1)

Domain app.somedomain.store
--------------------------------

< 1 >

### Details

In use Yes	Serial number 03:63:44:04:09:ff:16:c2:17:a5:04:67:88:a9:47:74:72:91	Requested at October 28, 2024, 13:22:59 (UTC-04:00)	Renewal eligibility Ineligible
Domain name app.somedomain.store	Public key info ECDSA P 256	Imported at October 28, 2024, 13:22:59 (UTC-04:00)	Expires in 89 days
Number of additional names 0	Signature algorithm SHA-384 with ECDSA	Not before October 28, 2024, 11:56:02 (UTC-04:00)	Not after January 26, 2025, 10:56:01 (UTC-05:00)
	Can be used with CloudFront, Elastic Load Balancing		

### Associated resources (1)

Resources <a href="#">arn:aws:elasticloadbalancing:us-east-1:682033507876:loadbalancer/app/MyApplicationALB/01a30b0d584164d8</a>
---

< 1 >

### ▼ Details

Load balancer type Application	Status <span style="color: green;">Active</span>	VPC <a href="#">vpc-0a8e3b6415af503a7</a>	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone Z355XDOTRQ7X7K	Availability Zones <a href="#">subnet-0bd2de0f5a057443b</a> us-east-1a (use1-az2) <a href="#">subnet-07b3b408a3cdead4c</a> us-east-1b (use1-az4)	Date created October 24, 2024, 19:49 (UTC-04:00)
Load balancer ARN <a href="#">arn:aws:elasticloadbalancing:us-east-1:682033507876:loadbalancer/app/MyApplicationALB/01a30b0d584164d8</a>	DNS name Info <a href="#">MyApplicationALB-99927605.us-east-1.elb.amazonaws.com</a> (A Record)		

[Listeners and rules](#) [Network mapping](#) [Resource map - new](#) [Security](#) [Monitoring](#) [Integrations](#) [Attributes](#) [Tags](#)

### Listeners and rules (1) [Info](#)

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.

[Filter listeners](#)

[C](#) [Manage rules](#) [Manage listener](#) [Add listener](#)

<input type="checkbox"/> Protocol:Port <a href="#">▼</a> Default action <a href="#">▼</a> Rules <a href="#">▼</a> ARN <a href="#">▼</a> Security policy <a href="#">▼</a> Default SSL/TLS certificate <a href="#">▼</a>	mTLS <a href="#">▼</a>
<input type="checkbox"/> <a href="#">HTTPS:443</a> Forward to target group • <a href="#">EC2-Final-TG</a> : 1 (100%) • Target group stickiness: Off	ARN ELBSecurityPolic... <a href="#">app.somedomain.store (Certificate ID: 27b63043-597f-407d-9cc9-c9be3de47d18)</a> Off

## Ensuring a secure connection between RDS and EC2 instance through SSL

- **Interaction:**
  - Safeguards data exchanged between EC2 and RDS
  - Protects logins and payment processes
- **Our Approach:**
  - Obtained the Amazon RDS root certificate and saved it to the EC2 instance.
  - Connected to the RDS instance using the MySQL client with the SSL certificate.
  - Configured the MySQL Client to Use SSL

### SSL enabled

```
ubuntu@ip-10-0-3-150:~$ mysql -h rds-multiaz-myrdinstance-qeruumzj9v4d.ctiowscucz1b.us-east-1.rds.amazonaws.com -u dbadmin -p --ssl-ca=rds-ca-cert.pem --ssl-mode=VERIFY_CA
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or g.
Your MySQL connection id is 999088
Server version: 8.0.39 Source distribution

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW STATUS LIKE 'Ssl_cipher';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| Ssl_cipher | TLS_AES_256_GCM_SHA384 |
+-----+-----+
1 row in set (0.03 sec)

mysql> SHOW VARIABLES LIKE '%ssl%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| admin_ssl_ca |          |
| admin_ssl_capath |          |
| admin_ssl_cert |          |
| admin_ssl_cipher |          |
| admin_ssl_crl |          |
| admin_ssl_crlpath |          |
| admin_ssl_key |          |
| have_openssl | YES |
| have_ssl | YES |
| performance_schema_show_processlist | OFF |
| ssl_ca | /rdsdbdata/rds-metadata/ca-cert.pem |
| ssl_capath |          |
| ssl_cert | /rdsdbdata/rds-metadata/server-cert.pem |
| ssl_cipher |          |
| ssl_crl |          |
| ssl_crlpath |          |
| ssl_fips_mode | OFF |
| ssl_key | /rdsdbdata/rds-metadata/server-key.pem |
| ssl_session_cache_mode | ON |
| ssl_session_cache_timeout | 300 |
+-----+-----+
20 rows in set (0.01 sec)
```

### Cannot access DB without SSL

```
ubuntu@ip-10-0-3-150:~$ mysql -h rds-multiaz-myrdinstance-qeruumzj9v4d.ctiowscucz1b.us-east-1.rds.amazonaws.com -u dbadmin -p --ssl-mode=DISABLED
Enter password:
ERROR 3159 (HY000): Connections using insecure transport are prohibited while --require_secure_transport=ON.
ubuntu@ip-10-0-3-150:~$
```

# CONTENT DELIVERY AND PERFORMANCE OPTIMIZATION

## - PHASE 3

### Introduction:

- The main objective of this phase is to improve the user experience of the website by reducing latency and increasing content delivery globally.
- Amazon Cloudfront and S3 are the key resources leveraged here to optimize performance and improve content delivery quickly.
- We will also be compressing objects and cache images to improve the load time and reduce latency.

### Amazon CloudFront:

- **Interaction:**
  - As a content delivery network (CDN), AWS CloudFront distributes our applications' dynamic content such as images, and files that are used on the website, at a cached location on the edge, making it widely available for my users.
  - Engages with AWS services like Amazon EC2, Amazon S3, and Elastic Load Balancing to dynamically load website content for user traffic.
- **Our Approach:**
  - Implemented Amazon CloudFront to serve static content (like images), reducing latency by caching these assets closer to users around the world.

The screenshot shows the AWS CloudFront Distribution Details page. At the top, the distribution ID is E2I2RD7JUEGLJF. Below it, there are tabs for General, Security, Origins, Behaviors, Error pages, Invalidations, and Tags. The General tab is selected. In the Details section, the Distribution domain name is dr4lgaoycjwo.cloudfront.net, and the ARN is arn:aws:cloudfront::682033507876:distribution/E2I2RD7JUEGLJF. The Last modified date is October 29, 2024 at 9:58:27 PM UTC. In the Settings section, the Description is blank, Alternate domain names are blank, Standard logging is On, Cookie logging is Off, and Default root object is blank. There is an 'Edit' button in the top right corner of the Settings section.

- Enabled gzip compression to reduce the size of images transferred over the network, thereby reducing the load times and costs for data transfer.

**Default cache behavior**

Path pattern | [Info](#)

Default (\*)

Compress objects automatically | [Info](#)

No  
 Yes

- Added the policy “Managed-CachingOptimized” in the behavior which caches all objects to maintain efficient performance and reduce the EC2 load by providing the frequently accessed images directly from the cache.

E2I2RD7JUEGLJF [View metrics](#)

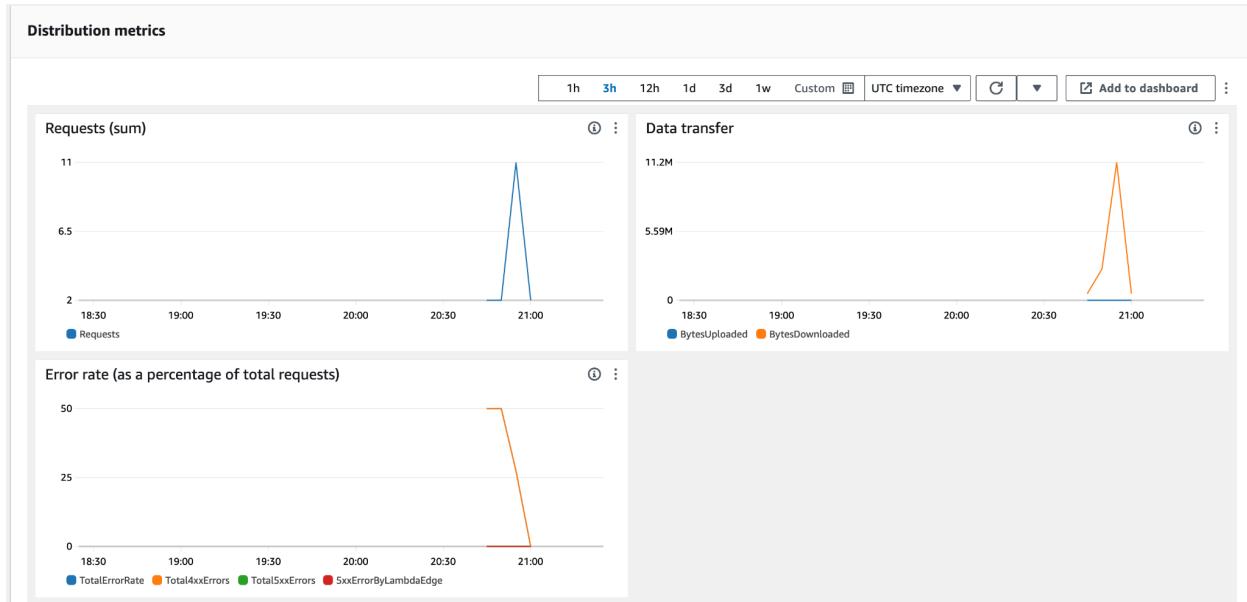
General | Security | Origins | **Behaviors** | Error pages | Invalidations | Tags

**Behaviors**

0 Default (\*) testbucket010898.s3.us-east-1.amazonaws.com HTTP and HTTPS Managed-CachingOptimized -

[Save](#) [Move up](#) [Move down](#) [Edit](#) [Delete](#) [Create behavior](#)

- Amazon Cloudwatch is integrated here as well to track the key performance metrics and adjust the configuration based on the performance



## Amazon S3 (Simple Storage Service):

- **Function:**
  - Supplies object storage designed to efficiently store and retrieve vast amounts of data from various sources such as websites and mobile applications.
- **Our Approach:**
  - We set up a S3 Bucket to hold the static assets (like images) from our platform. The S3 was then connected to the cloud front to distribute and cache the images.

**testbucket010898** [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

**Objects (2)** [Info](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">bg.png</a>	png	October 28, 2024, 13:04:22 (UTC-04:00)	487.0 KB	Standard
<input type="checkbox"/>	<a href="#">bgsecond.png</a>	png	October 29, 2024, 16:51:44 (UTC-04:00)	2.4 MB	Standard

E2I2RD7JUEGLJF

[View metrics](#)

[General](#) [Security](#) [Origins](#) [Behaviors](#) [Error pages](#) [Invalidations](#) [Tags](#)

**Origins**

Filter origins by property or value

Origin name	Origin domain	Origin path	Origin type	Origin Shield region	Origin access
<input type="radio"/> testbucket010898.s3.us-east-1.amazonaws.com	testbucket010898.s3.us-east-1.amazonaws.com		S3	-	E5TR16WJKUFMME

## Static content delivery through cloudfront & S3:

```
/* End NavBar */
/* ****
**** Index.php ****
*****
*/
/* Start Landing Section */
.landing .container .cover {
    background-image: url("https://dr4lgauoycjwo.cloudfront.net/bg.png");
    background-size: cover;
    height: 100%;
    display: flex;
    flex-direction: column;
    gap: 18px;
    align-items: flex-start;
    padding: 40px;
    color: white;
}

/* End Category Section */
/* Start Advertise Section */
.adver {
    padding-top: 20px;
    padding-bottom: 40px;
    margin-bottom: 20px;
}

.adver .container .cover {
    background-image: url("https://dr4lgauoycjwo.cloudfront.net/bgsecond.png");
    background-position: center;
    background-size: cover;
    height: 60vh;
    display: flex;
    flex-direction: column;
    gap: 25px;
    align-items: flex-start;
    justify-content: center;
    color: white;
    padding: 70px;
}
```

## TESTING AND MONITORING - PHASE 4

### Stress Testing

- **Intention:**

- To validate the application's resilience under heavy user load and assess the effectiveness of our Auto Scaling and RDS configurations.
- To ensure the infrastructure can dynamically handle traffic spikes without degradation in performance.

- **Our Approach:**

- We employed Apache JMeter to try simulating the real-world load conditions, and aimed for approximately 1 million requests to the target page.
- Once the requests were sent key performance metrics, such as CPU utilization, memory usage, number requests were monitored to gauge the system's performance in handling load.
- CloudWatch alarms were also setup to actively monitor the CPU utilization

Thread Group.jmx (/Users/umeshchandra/Downloads/apache-jmeter-5.6.3/bin/Thread Group.jmx) - Apache JMeter (5.6.3)

00:00:14 ⚠ 0 4048/100000

Test Plan

- Thread Group
  - View Results Tree
  - HTTP Request

**View Results Tree**

Name: View Results Tree

Comments:

Write results to file / Read from file

Filename:

Search: Case sensitive Regular exp Search Reset

Text Sampler result Request Response data

Response Body Response headers

```

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>E-commerce Home Page</title>
<link rel="stylesheet" href="/assets/css/bootstrap.css" />
<link rel="stylesheet" href="/assets/css/main.css" />
</head>

<body>
<!-- upper-nav -->
<div class="upper-nav primary-bg p-2 px-3 text-center text-break">
<span>Summer Sale For All Swim Suits And Free Express Delivery - OFF 50%! <a>Shop Now</a></span>
</div>
<!-- upper-nav -->
<!-- Start NavBar -->
<nav class="navbar navbar-expand-lg navbar-light bg-light">
<div class="container">
<a class="navbar-brand fw-bold" href="#">A1</a>
<button class="navbar-toggler" type="button" data-bs-toggle="collapse" data-bs-target="#navbarSupportedContent" aria-controls="navbarSupportedContent" aria-expanded="false" aria-label="Toggle navigation">
<span class="navbar-toggler-icon"></span>
</button>
<div class="collapse navbar-collapse" id="navbarSupportedContent">
<ul class="navbar-nav mx-auto mb-2 mb-lg-0">
<li class="nav-item">
<a class="nav-link active" aria-current="page" href="/index.php">Home</a>
</li>
<li class="nav-item">
<a class="nav-link" href="/products.php">Products</a>
</li>
<li class="nav-item">
<a class="nav-link" href="#">About</a>
</li>
<li class="nav-item">
<a class="nav-link" href="#">Contact</a>
</li>
<li class="nav-item">
<a class="nav-link" href="/users_area/user_registration.php">Register</a>
</li>
</ul>
</div>
<form class="d-flex">
<input class="form-control me-2" type="search" placeholder="Search" aria-label="Search" value="Search" data-bbox="488 558 528 568"/>
<button class="btn btn-outline-primary" type="submit" data-bbox="528 558 568 568">>Search</button>
</form>
<ul class="nav navbar-nav mb-2 mb-lg-0">
<li class="nav-item">
<a class="nav-link" href="/cart.php"><svg width="28" height="28" viewBox="0 0 32 32" fill="none" xmlns="http://www.w3.org/2000/svg"><path d="M11 27C11 55Z 27 12 26,55Z 31 12 26C12 25,4477 11,55Z 32 25 11 25C10,4477 25 10 25,4477 20,25C25,4477 25 24,4477 24,25Z" style="width: 1em; height: 1em; vertical-align: middle;"/></a>
</li>
</ul>
</div>
</nav>

```

Scroll automatically?

Thread Group.jmx (/Users/umeshchandra/Downloads/apache-jmeter-5.6.3/bin/Thread Group.jmx) - Apache JMeter (5.6.3)

00:00:20 ⚠ 0 4048/100000

Test Plan

- Thread Group
  - View Results Tree
  - HTTP Request

**Thread Group**

Name: Thread Group

Comments:

Action to be taken after a Sampler error

Continue  Start Next Thread Loop  Stop Thread  Stop Test  Stop Test Now

**Thread Properties**

Number of Threads (users): 100000

Ramp-up period (seconds): 30

Loop Count:  Infinite 100000

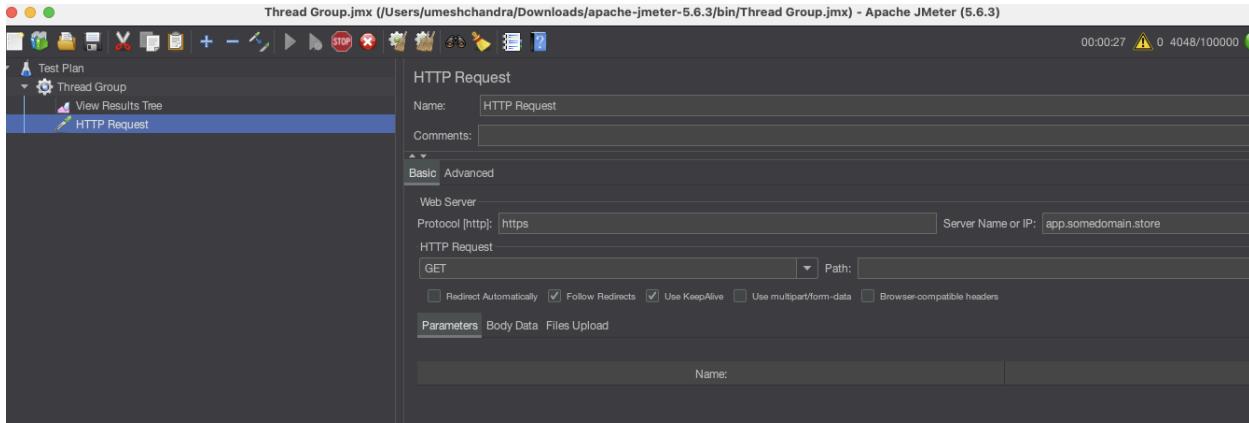
Same user on each iteration

Delay Thread creation until needed

Specify Thread lifetime

Duration (seconds):

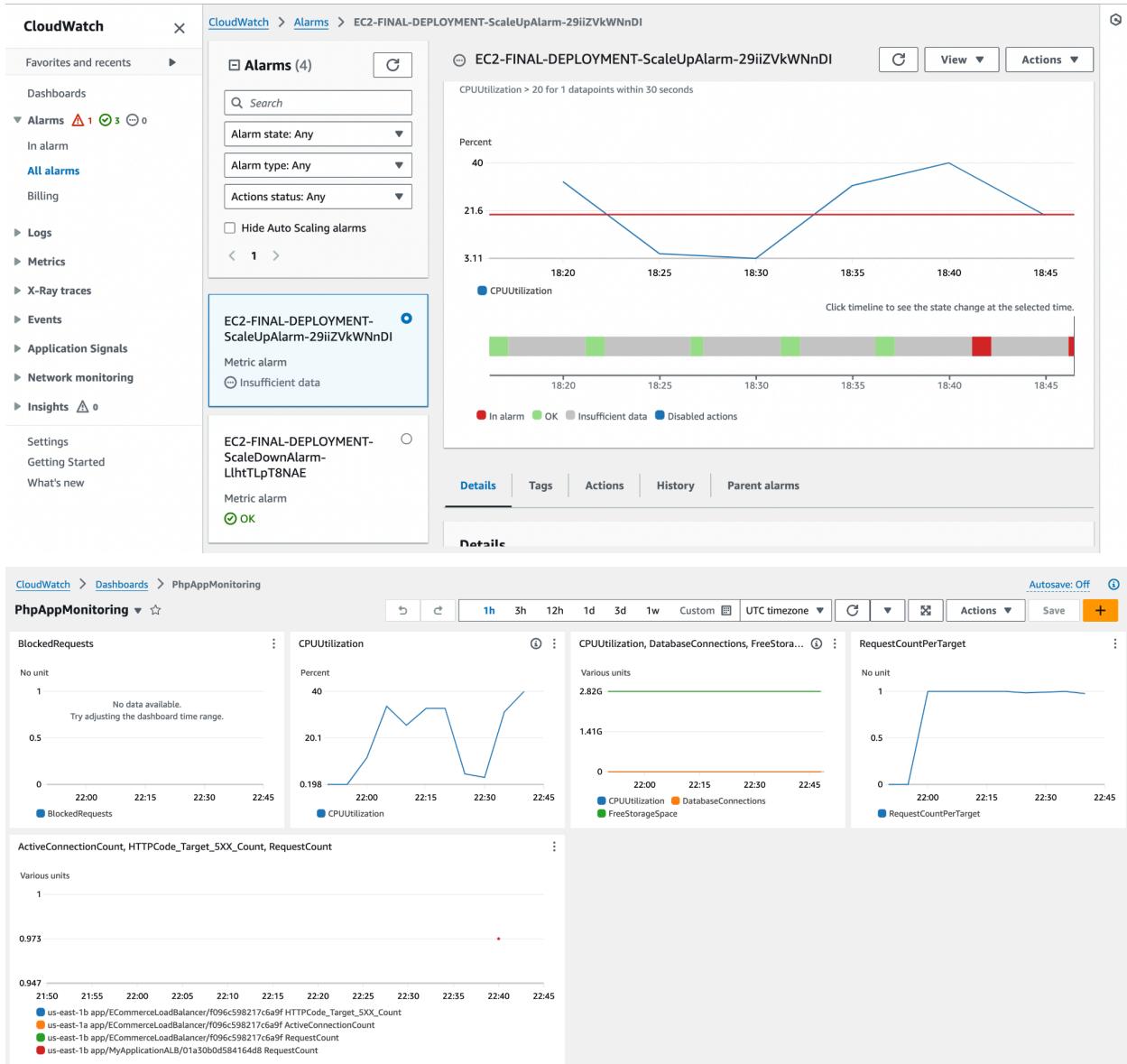
Startup delay (seconds):



- During the bombardment of requests when the CPU utilization has crossed 20% the number of EC2 instances has scaled up and once the CPU utilization has gone less than 10% the number EC2 instances has also scaled down.
- Screenshot showing Autoscaled Ec2 instances when subjected to more load.

Activity history (9)						
Status	Description	Cause	Start time	End time		
⌚ Waiting for instance warmup	Launching a new EC2 instance: i-0226625b07bcb0357	At 2024-10-29T22:45:46Z a monitor alarm TargetTracking-EC2-FINAL-DEPLOYMENT-MyAutoScalingGroupV3-QsbBLjfsjn-AlarmHigh-5152cedd-b5ce-4d2c-9e62-9ebad5daadc2 in state ALARM triggered policy Target Tracking Policy changing the desired capacity from 2 to 4. At 2024-10-29T22:45:58Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 2 to 4.	2024 October 29, 06:46:00 PM -04:00			
⌚ Waiting for instance warmup	Launching a new EC2 instance: i-0eb4196f972760f4c	At 2024-10-29T22:45:46Z a monitor alarm TargetTracking-EC2-FINAL-DEPLOYMENT-MyAutoScalingGroupV3-QsbBLjfsjn-AlarmHigh-5152cedd-b5ce-4d2c-9e62-9ebad5daadc2 in state ALARM triggered policy Target Tracking Policy changing the desired capacity from 2 to 4. At 2024-10-29T22:45:58Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 2 to 4.	2024 October 29, 06:46:00 PM -04:00			
⌚ Successful	Launching a new EC2 instance: i-0f3b1b2918dbf13d8	At 2024-10-29T22:39:46Z a monitor alarm TargetTracking-EC2-FINAL-DEPLOYMENT-MyAutoScalingGroupV3-QsbBLjfsjn-AlarmHigh-5152cedd-b5ce-4d2c-9e62-9ebad5daadc2 in state ALARM triggered policy Target Tracking Policy changing the desired capacity from 1 to 2. At 2024-10-29T22:39:55Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 1 to 2.	2024 October 29, 06:39:57 PM -04:00	2024 October 29, 06:45:03 PM -04:00		
⌚ Successful	Terminating EC2 instance: i-0bdff71bdfc4c9a0e	At 2024-10-29T17:57:07Z a monitor alarm EC2-FINAL-DEPLOYMENT-ScaleDownAlarm-LihtTlpT8NAE in state ALARM triggered policy EC2-FINAL-DEPLOYMENT-ScaleDownPolicyV3-nxCSuPCzHf changing the desired capacity from 2 to 1. At 2024-10-29T17:57:09Z an instance was taken out of service in response to a difference between desired and actual capacity, shrinking the capacity from 2 to 1. At 2024-10-29T17:57:09Z instance i-0bdff71bdfc4c9a0e was selected for termination.	2024 October 29, 01:57:09 PM -04:00	2024 October 29, 02:03:12 PM -04:00		
⌚ Successful	Launching a new EC2 instance: i-0a05e67b7rr50855a	At 2024-10-29T17:51:45Z a user request update of AutoScalingGroup constraints to min: 1, max: 4, desired: 2 changing the desired capacity from 1 to 2. At 2024-10-29T17:51:48Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 1 to 2.	2024 October 29, 01:51:49 PM -04:00	2024 October 29, 01:51:56 PM -04:00		

Instances (5) <small>info</small>										
<span>Last updated less than a minute ago</span> <span>Connect</span> <span>Instance state ▾</span> <span>Actions ▾</span> <span>Launch instances ▾</span> <span>⋮</span>										
<span>Find Instance by attribute or tag (case-sensitive)</span> <span>All states ▾</span>										
<span>Instance state = running</span> <span>Clear filters</span>										
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Publ		
EC2-FINAL-DE...	i-0f3b1b2918dbf13d8	Running	t3.micro	2/3 checks passed	View alarms +	us-east-1b	-	-		
EC2-FINAL-DE...	i-0226625b07bcb0357	Running	t3.micro	2/3 checks passed	View alarms +	us-east-1b	-	-		
BastionInstance	i-09f22cc2aa1275456	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-44-204-25-173.co...	44.204.25.173		
EC2-FINAL-DE...	i-0495e67b7cc50865a	Running	t3.micro	2/3 checks passed	View alarms +	us-east-1a	-	-		
EC2-FINAL-DE...	i-0eb4196f972760f4c	Running	t3.micro	2/3 checks passed	View alarms +	us-east-1a	-	-		

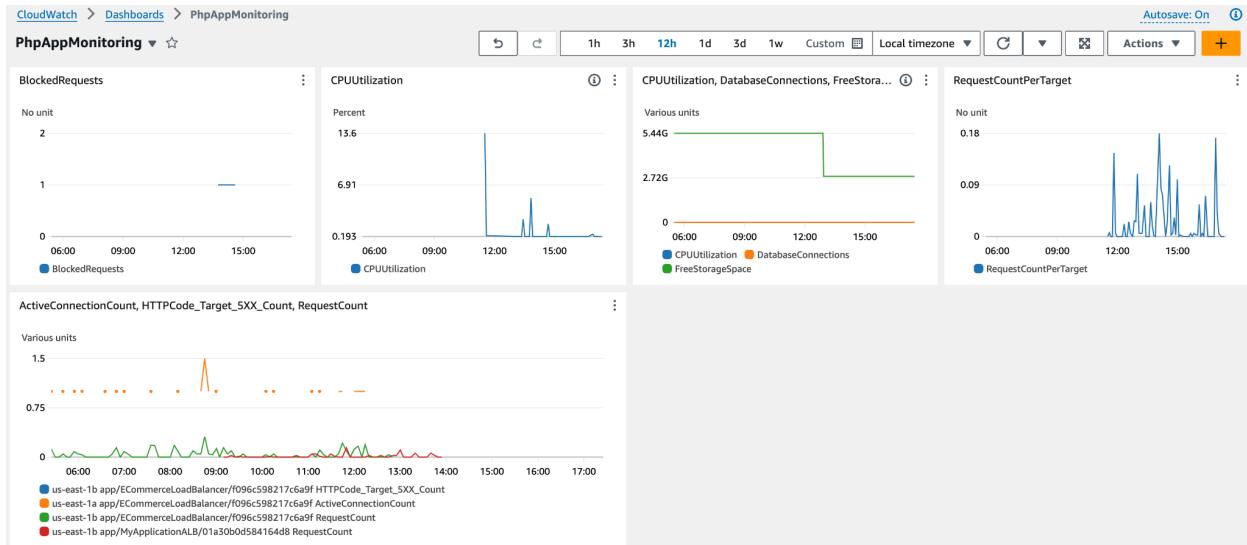


## Monitoring Setup

### AWS CloudWatch

- **Intention:**
  - Collects the monitoring metrics such as disk space, and health of the app
  - CloudWatch collects and stores log files for errors, debugging, and other types of logging
  - Can set up alarms for triggering if a metric crosses a certain threshold
- **Our Approach:**

- We set up the CloudWatch dashboard to see the CPU utilization, amount of Requests Per Instance, any blocked requests, and how many active connections there are per availability zone



## CloudTrail

- **Intention:**
  - CloudTrail allows for the event logging of account activity by users in the form of an event history log file
  - These are conducted through API calls within the past 90 days of the console
- **Our Approach:**
  - We set up CloudTrail to monitor the logs within the console and maintain visibility into the actions taken within our infrastructure
  - We set up CloudTrail Insights to alert us on any unusual activity that is detected and enabled KMS encryption for added security
  - The logs are stored in a new S3 bucket that we created and are set to alert us via SNS email delivery for each log file
  - We enabled Log File validation to ensure SHA-256 is used for each log file delivery

## management-events

[Delete](#) [Stop logging](#)

## General details

[Edit](#)

Trail logging	Logging	Trail log location	aws-cloudtrail-logs-682033507876-4811105b/AWSLogs/682033507876	Log file validation	Enabled	SNS notification delivery
Trail name	management-events		6	Last file validation delivered	-	arn:aws:sns:us-east-1:682033507876:aws-cloudtrail-logs-682033507876-4c23d83c
Multi-region trail		Last log file delivered	October 29, 2024, 12:57:55 (UTC-04:00)			Last SNS notification
Yes		Log file SSE-KMS encryption	Enabled			-
Apply trail to my organization	Not enabled	AWS KMS key	arn:aws:kms:us-east-1:682033507876:key/a38c17b7-a105-4821-8ad0-5cc1fe70fe58			
		AWS KMS key alias	cloudtrail-kms-key-s3			

Event history [Info](#)

Event name	Event time	Event source
<a href="#">DetachInternetGate...</a>	October 29, 2024, 12:58:46 (UT...)	ec2.amazonaws.com
<a href="#">DetachInternetGate...</a>	October 29, 2024, 12:58:30 (UT...)	ec2.amazonaws.com
<a href="#">DeleteSecurityGroup</a>	October 29, 2024, 12:58:29 (UT...)	ec2.amazonaws.com
<a href="#">UpdateTrail</a>	October 29, 2024, 12:58:24 (UT...)	cloudtrail.amazonaws.com
<a href="#">CreateAlias</a>	October 29, 2024, 12:58:23 (UT...)	kms.amazonaws.com

## AWS Config

- **Intention:**

- AWS Config tracks and records changes in settings for AWS resources such as EC2 instances and RDS Databases
- It also conducts compliance monitoring to define rules and then check against those rules to see if the resources comply with the predefined rules

- **Our Approach:**

- We set up AWS Config with predefined rules to test against our set up and see if we have everything set up correctly
- Some of the rules include: Checking if WAF is enabled in our ALB, checking if our DB has backups enabled, checking cloudtrail enablement, and making sure the SSL certificate is not expired.

**AWS Config > Rules**

A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

Name	Remediation action	Type	Enabled evaluation mode	Detective compliance
db-instance-backup-enabled	Not set	AWS managed	DETECTIVE	Compliant
cloudtrail-enabled	Not set	AWS managed	DETECTIVE	Compliant
alb-waf-enabled	Not set	AWS managed	DETECTIVE	Compliant
cloud-trail-log-file-validation-enabled	Not set	AWS managed	DETECTIVE	Compliant
alb-https-to-https-redirection-check	Not set	AWS managed	DETECTIVE	Compliant
cloud-trail-encryption-enabled	Not set	AWS managed	DETECTIVE	Compliant

**AWS Config > Resources**

Resource Inventory

Search existing or deleted resources recorded by AWS Config. For a specific resource, view the resource details or resource timeline. The resource timeline allows you to view all the configuration items captured over time for a specific resource and the compliance status changes. For accurate reporting on the compliance status, you must record the AWS Config ResourceCompliance resource type. To query your resource configurations, use the advanced SQL query editor.

Resource category	Resource type	Compliance
All resource categories	All resource types	Compliant
Resource identifier - optional		
<input type="text" value="Enter resource identifier"/>		
<input type="checkbox"/> Include deleted resources		
Resource identifier	Type	Compliance
rds-mariadb-myridinstance-0eraumjy4vd	RDS DBInstance	Compliant
arn:aws:acm:us-east-1:682035507876:certificate/77b63043-597f-407d-9cc9-c9be3de47c18	ACM Certificate	Compliant

**AWS Config usage metrics**

AWS Config usage metrics by resource type

Choose Resource types: All

Time range: 3h, 1d, 1w, 3h (selected), Local timezone, C, ⏪, ⋮

**Configuration Items Recorded**

Count

11  
6  
1

18:00 19:00 20:00

All

**Configuration Recorder Insufficient P...**

Count

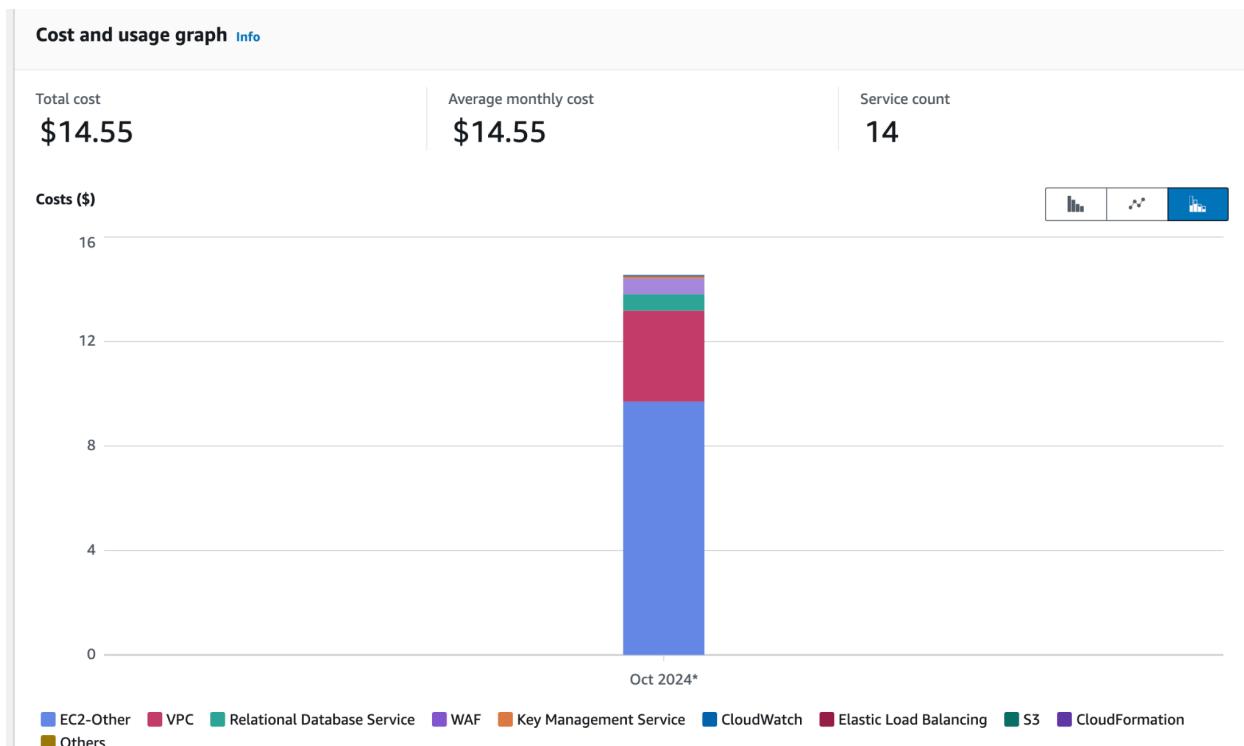
1  
0.5  
0

18:00 19:00 20:00

All

## Cost Optimization Analysis:

- **Intention:**
  - To analyze resource usage and explore options to reduce long-term costs, ensuring efficient allocation and potential savings.
- **Our Approach:**
  - Leveraged AWS Cost Explorer to assess current spending trends and identify opportunities for cost reductions.



Cost and usage breakdown		
Find cost and usage data		Download as CSV
Service	Service total	October 2024*
Total costs	\$14.55	\$14.55
EC2-Other	\$9.70	\$9.70
VPC	\$3.48	\$3.48
Relational Database Service	\$0.63	\$0.63
WAF	\$0.60	\$0.60
Key Management Service	\$0.08	\$0.08
CloudWatch	\$0.05	\$0.05
Elastic Load Balancing	\$0.00	\$0.00
S3	\$0.00	\$0.00
CloudFormation	\$0.00	\$0.00
CloudTrail	\$0.00	\$0.00
CloudFront	\$0.00	\$0.00
EC2-Instances	\$0.00	\$0.00
SNS	\$0.00	\$0.00
Tax	\$0.00	\$0.00

## Recommendations:

### Reserved Instances (RIs):

- RIs are suitable for workloads when we know the specific instance types and regions that the project will consistently require over long periods of time. RIs are useful for predictable costs and stable workloads as they come with substantial discounts.
- For the stable resources like RDS Instance, standard RIs can be used because of the targeted discounts, thereby offering the best cost savings.

### Saving Plans:

- They are more flexible alternatives than RI, and focus on reducing costs on various instances. Savings plan is more adaptable for dynamic environments where we may need to switch between regions.
- The Compute Savings Plan is likely the better choice for the dynamic EC2 components that run within Auto Scaling groups, as it provides flexibility and significant cost savings.

## **Lessons Learned:**

Working on the Scalable and Secure E-commerce Platform project on AWS gave our team some valuable hands-on experience in building a secure, flexible, and efficient cloud infrastructure. Setting up Auto Scaling for EC2 instances was an eye-opener, teaching us how to handle traffic spikes without overspending on resources. Tackling the RDS setup together helped us navigate database management challenges, especially around encryption for data protection. Implementing the Web Application Firewall (WAF) showed us practical ways to safeguard against common web attacks, while configuring CloudFront highlighted how global content delivery can improve user experience through caching and faster load times. Beyond the technical skills we gained with core AWS services, this project underscored how essential teamwork is when developing secure, scalable cloud solutions.

## **Potential improvements for production environments:**

To make our e-commerce platform even more robust and secure for a production environment, we could fine-tune configurations and incorporate key AWS services. First, we could implement Multi-Regional Deployment, which would add a secondary region for disaster recovery. This setup would replicate critical data and services, ensuring high availability and quick failover in case of regional issues. It would also reduce latency for users on the West Coast for example, by offering a region closer to them.

Since we use S3 buckets for functions like storing images on CloudFront, logging with CloudTrail, and AWS Config, we can enable automatic backups for these buckets to prevent data loss. This would also allow us to implement versioning for log files and move older files to lower-cost storage, helping manage expenses. Although we avoided this in our sample project to keep costs down, it would be essential in a real-world deployment.

Additionally, we could add Network Access Control Lists (NACLs) at the subnet level to secure our inbound and outbound traffic further. Finally, implementing AWS ElastiCache would introduce a caching layer for frequently accessed data, significantly improving database load times.

## REFERENCES

### Core Infrastructure Concepts

- [Global Infrastructure - Overview](#)
- [AWS Resource Management Documentation](#)
- [AWS Well-Architected Framework](#)
- [Organizing Your AWS Environment Using Multiple Accounts](#)
- [Design Isolated Resource Environments](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [AWS Systems Manager](#)
- [AWS Service Catalog](#)

### Infrastructure as Code (IaC)

- [Choosing an Infrastructure as Code Tool](#)
- [Reviewing IaC Tools for the AWS Cloud](#)
- [AWS Cloud Development Kit \(AWS CDK\)](#)
- [AWS Serverless Application Model \(AWS SAM\)](#)
- [Using the AWS Infrastructure Composer Console](#)
- [What is AWS Infrastructure Composer?](#)
- [Infrastructure Composer Enhanced Component Cards](#)

### Infrastructure Management Tools

- [AWS Config](#)
- [AWS Trusted Advisor](#)
- [AWS Organizations](#)
- [AWS Cost Management](#)
- [AWS CloudTrail](#)
- [AWS CloudWatch](#)

- [AWS Config Rules](#)

## **Security and Compliance**

- [Best Practices for Tagging AWS Resources](#)
- [AWS Key Management Service \(KMS\)](#)
- [AWS Security Hub](#)
- [AWS Shield and WAF](#)
- [AWS Secrets Manager](#)
- [AWS Identity and Access Management \(IAM\) Best Practices](#)
- [Security and Compliance Documentation](#)
- [AWS Compliance](#)

## **Application and Deployment Services**

- [Amazon EC2 Auto Scaling](#)
- [AWS CodePipeline](#)
- [AWS CodeBuild](#)
- [AWS Step Functions](#)
- [Amazon ECS](#)
- [AWS Elastic Load Balancing \(ELB\)](#)
- [Amazon VPC](#)