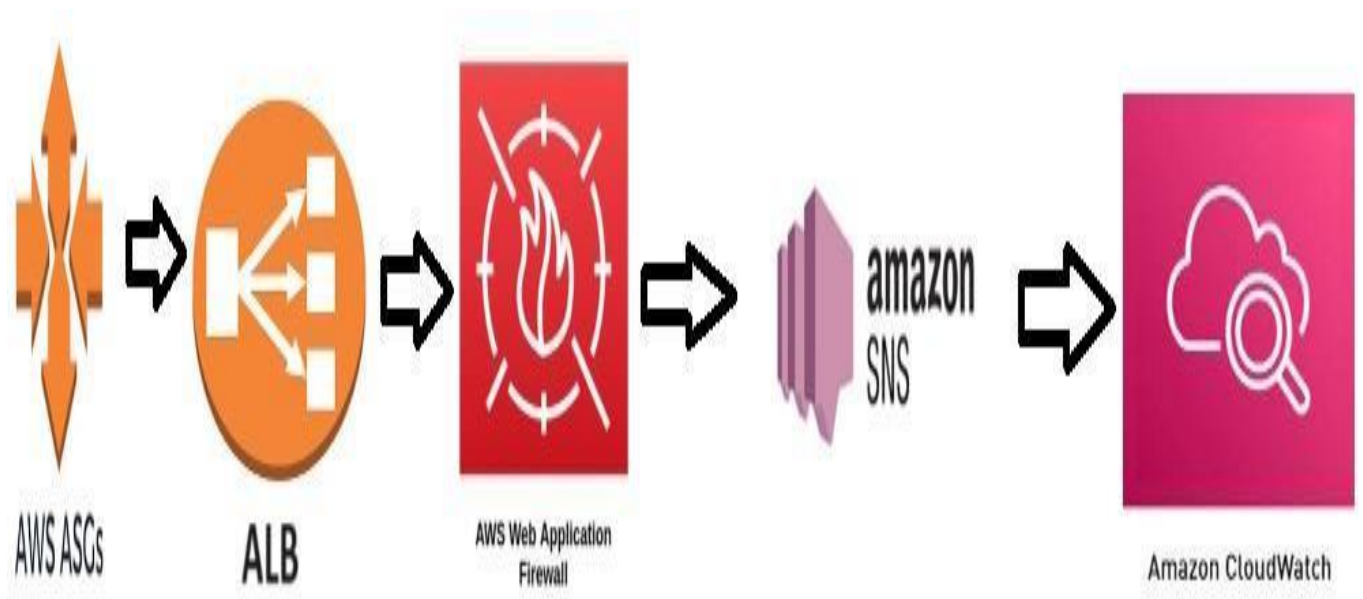


Hosting a website on AWS EC2 Instance with Auto Scaling group, Application Load Balancer and Web Application Firewall (WAF) and Monitor with Cloud Watch and Add Simple Notification Service (SNS) for it.



Create launch template

Step 1: Create launch template.

The screenshot shows the AWS Management Console 'Create launch template' page. The page is titled 'Create launch template' and includes a description: '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.' The page is divided into two main sections: 'Launch template name and description' and 'Launch template contents'. The 'Launch template name and description' section contains a 'Launch template name' field (required) with the value 'mytemp-1', a 'Template version description' field with the value 'A prod webserver for MyApp', and an 'Auto Scaling guidance' section with a checkbox for 'Provide guidance to help me set up a template that I can use with EC2 Auto Scaling'. The 'Launch template contents' section is currently empty. The 'Summary' section on the right shows the configuration details: Software Image (AMI) Canonical, Ubuntu, 22.04 LTS, Virtual server type (instance type) t2.micro, Firewall (security group) default, and Storage (volumes) 1 volume(s) - 8 GiB. The 'Create launch template' button is highlighted in orange.

Step 2: Add user data in template

- Add web server(apache2)
- Download the website code file in it.
- Unzip the code file.

The screenshot shows the AWS Management Console 'Create launch template' page for EC2. The page is titled 'Create launch template | EC2' and the URL is 'us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateTemplate:'. The page is divided into two main sections: 'User data' and 'Summary'.

User data - optional (Info):
Upload a file with your user data or enter it in the field.

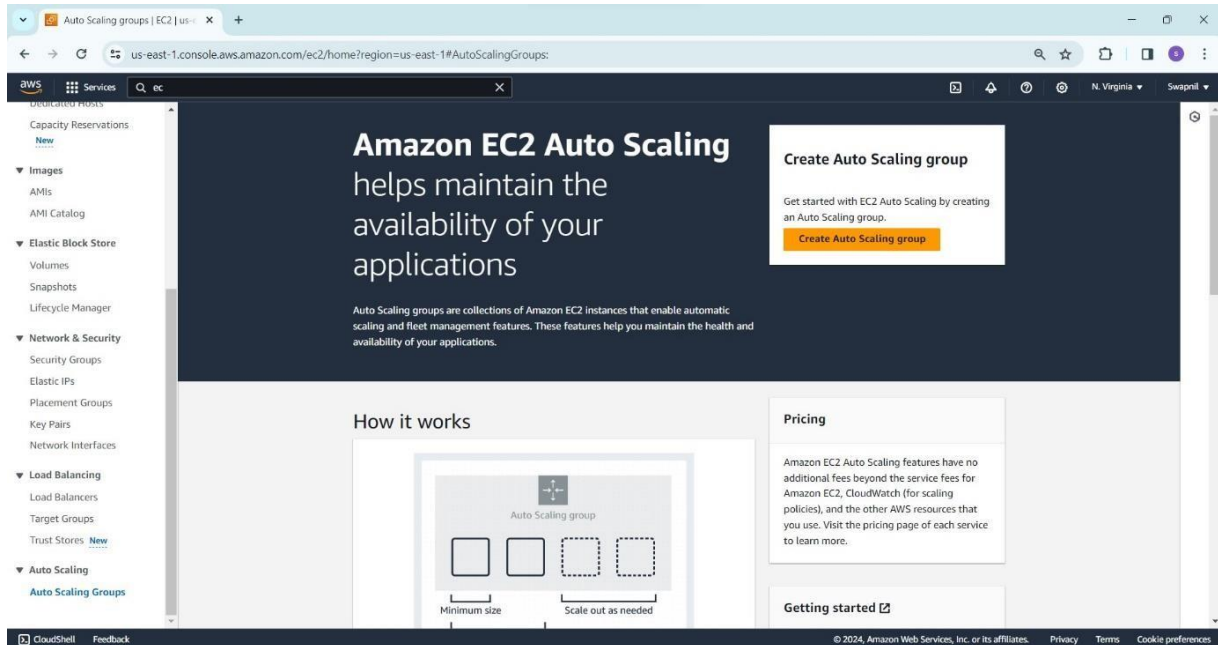

```
#!/bin/bash
sudo apt update -y
sudo apt install apache2 -y
sudo apt install unzip -y
sudo wget https://www.free-css.com/assets/files/free-css-
templates/download/page296/over.zip
sudo unzip over.zip
sudo mv over-html/ * /var/www/html
sudo systemctl restart apache2
sudo systemctl enable apache2
```


☐ User data has already been base64 encoded

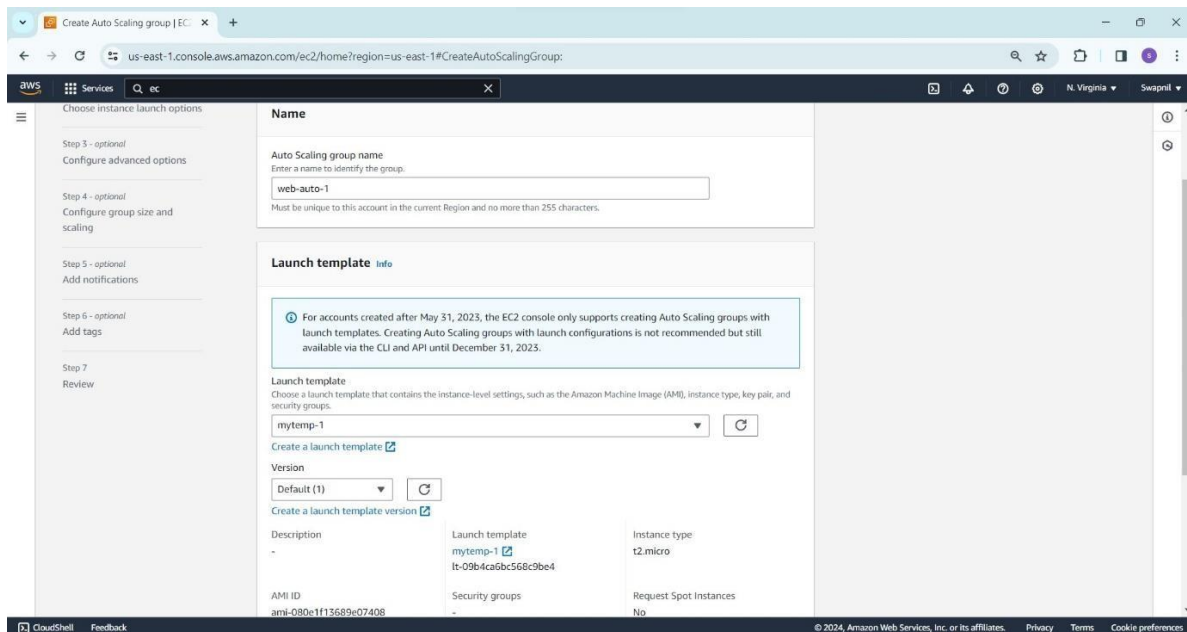
Summary
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-080e1f13689e07408
Virtual server type (instance type)
t2.micro
Firewall (security group)
default
Storage (volumes)
1 volume(s) - 8 GiB

Create auto scaling group from launch template.

Step 3: Create auto scaling group.



Step 4: Define name and template.



Step 5: Choose instance launch options.

➤ Select availability zones and subnets.

The screenshot shows the AWS Management Console interface for creating an Auto Scaling group. The page is titled 'Create Auto Scaling group | EC2' and is at Step 5 of the wizard. The 'Network info' section is active, showing a VPC selection dropdown with 'vpc-01cb5a8ab8705ce3c' selected. Below the VPC, there are two Availability Zones and subnets selected: 'us-east-1a | subnet-0944f8f8a381654d6' and 'us-east-1b | subnet-02f3c70a0399e1248'. The instance type is 't2.micro'. The page includes a sidebar with navigation links for Step 5 (optional), Step 6 (optional), and Step 7 (Review). At the bottom, there are buttons for 'Cancel', 'Skip to review', 'Previous', and 'Next'.

Step 6: Configure advanced options.

➤ Add application Load balancer option.

The screenshot shows the AWS Management Console interface for creating an Auto Scaling group, specifically the 'Load balancing info' section. The page is titled 'Create Auto Scaling group | EC2' and is at Step 6 of the wizard. The 'Attach to a new load balancer' option is selected. Below this, the 'Load balancer type' is set to 'Application Load Balancer' (HTTP, HTTPS). The 'Load balancer name' is 'web-auto-1-1'. The 'Load balancer scheme' is set to 'Internet-facing'. The page includes a sidebar with navigation links for Step 3 (optional), Step 4 (optional), Step 5 (optional), and Step 6 (optional). At the bottom, there are buttons for 'Cancel', 'Skip to review', 'Previous', and 'Next'.

Step 7: Add load balancer and target group.

The screenshot shows the 'Create Auto Scaling group' page in the AWS Management Console, specifically Step 7: Add load balancer and target group. The page is for the 'us-east-1' region. Under 'Listeners and routing', the 'Protocol' is set to 'HTTP' and the 'Port' is '80'. The 'Default routing (forward to)' dropdown is set to 'Create a target group'. Below this, the 'New target group name' is 'web-auto-1-1'. The 'Tags - optional' section shows 'Add tag' and '50 remaining'.

Listeners and routing

If you require secure listeners, or multiple listeners, you can configure them from the Load Balancing console [after](#) your load balancer is created.

Protocol: HTTP Port: 80 Default routing (forward to): Create a target group

New target group name: web-auto-1-1

An instance target group with default settings will be created.

Tags - optional

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add tag

50 remaining

Step 8: Configure group size and scaling. Select the minimum, desired and maximum capacity.

The screenshot shows the 'Create Auto Scaling group' page in the AWS Management Console, specifically Step 8: Configure group size and scaling. The page is for the 'us-east-1' region. Under 'Specify your group size', the 'Min desired capacity' is '1' and the 'Max desired capacity' is '4'. The 'Automatic scaling - optional' section shows 'No scaling policies' selected. The 'Instance maintenance policy - new' section shows 'Control availability and cost during replacement events' selected.

Specify your group size.

1

Scaling info

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

Scaling limits

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

Min desired capacity: 1 Max desired capacity: 4

Automatic scaling - optional

Choose whether to use a target tracking policy

No scaling policies

Target tracking scaling policy

Instance maintenance policy - new

Control your Auto Scaling group's availability during instance replacement events. This includes health checks, instance refreshes, maximum instance lifetime features and events that happen automatically to keep your group balanced, called rebalancing events.

Control availability and cost during replacement events

An instance maintenance policy determines how much availability your application has when EC2 Auto Scaling replaces instances. It also establishes guardrails that limit the amount of capacity that

Step 9: Add notifications.

➤ Create a new topic. Enter name and endpoint user email.

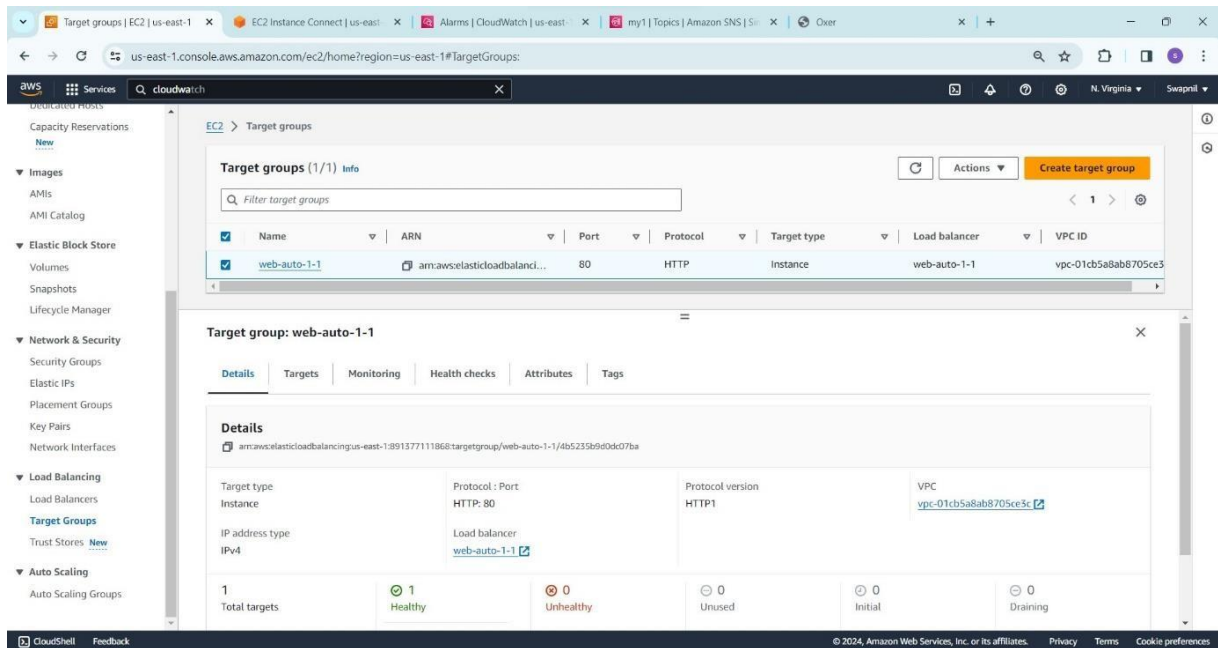
The screenshot shows the 'Add notifications - optional' step in the AWS Management Console. The left sidebar lists steps 1 through 7, with 'Add notifications' selected for Step 5. The main content area has a title 'Add notifications - optional' and a description: 'Send notifications to SNS topics whenever Amazon EC2 Auto Scaling launches or terminates the EC2 instances in your Auto Scaling group.' Below this is a form for 'Notification 1'. It includes a 'Send a notification to' field with the value 'my_topic', a 'With these recipients' field with the value 'swap12321232@gmail.com', and a 'Use existing topic' button. Under 'Event types', there are four checkboxes: 'Launch' (checked), 'Terminate' (checked), 'Fail to launch' (checked), and 'Fail to terminate' (checked). At the bottom are buttons for 'Add notification', 'Cancel', 'Skip to review', 'Previous', and 'Next'.

Step 10: Add tags and review. Click on create Auto Scaling groups.

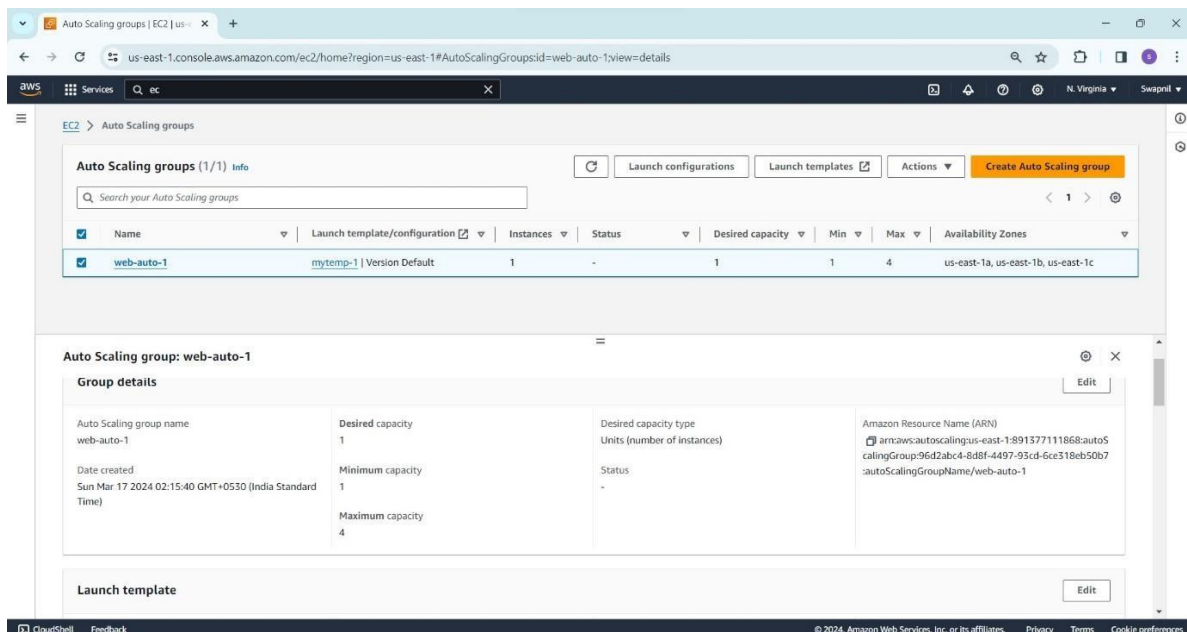
The screenshot shows the 'Step 6: Add tags' section of the AWS Management Console. Above it is the 'Instance scale-in protection' section with a checkbox 'Enable instance protection from scale in' that is unchecked. The 'Step 5: Add notifications' section is visible above, showing the notification details. The 'Step 6: Add tags' section has a title 'Tags (0)' and a table with columns 'Key', 'Value', and 'Tag new instances'. The table is currently empty, with a 'No tags' message at the bottom. At the bottom of the console are buttons for 'Cancel', 'Previous', and 'Create Auto Scaling group'.

Application load balancer is automatically created

Step 11: New target group is automatically created.

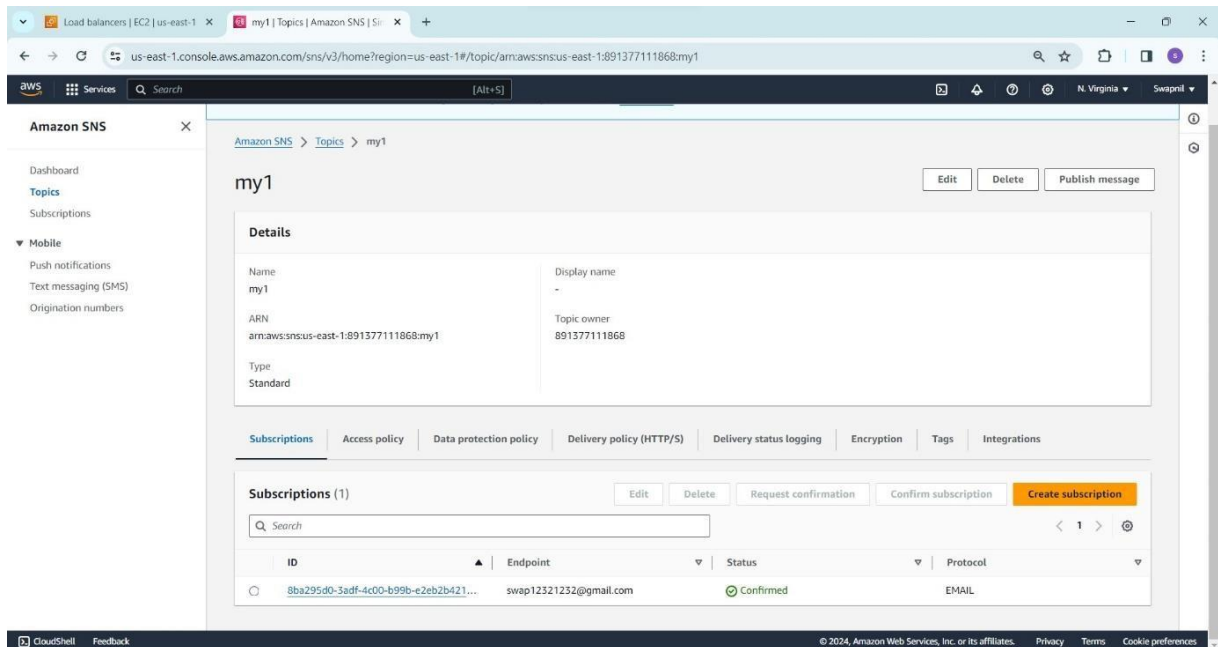


Step 12: New Application Load Balancer is created automatically.

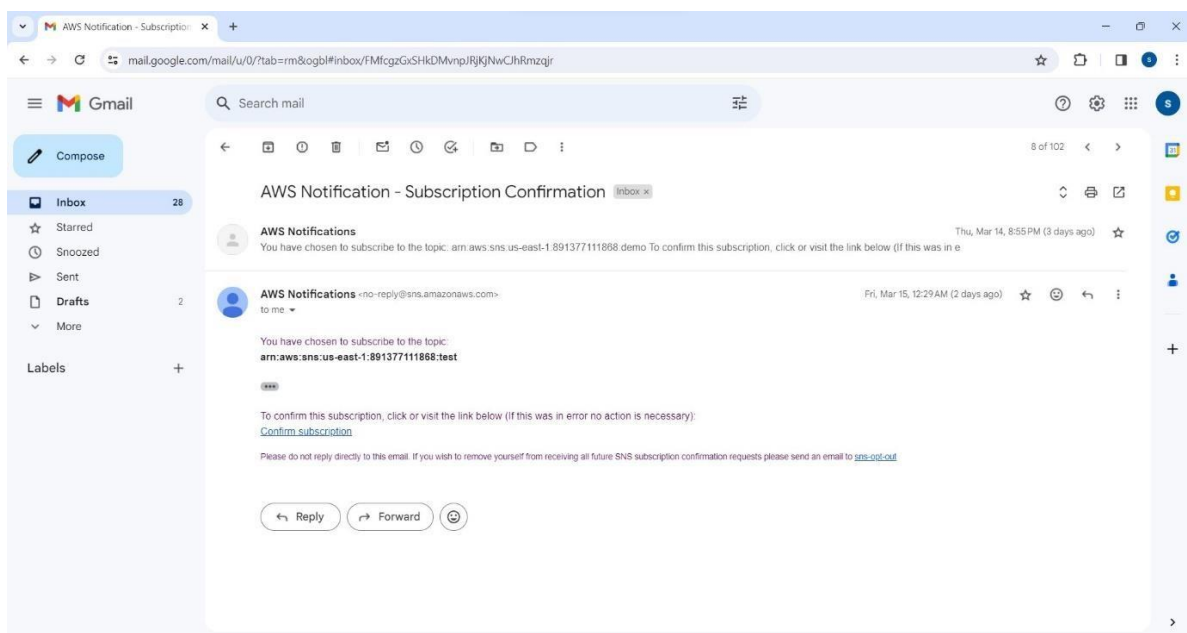


Check Simple Notification Service (SNS) Step 13:

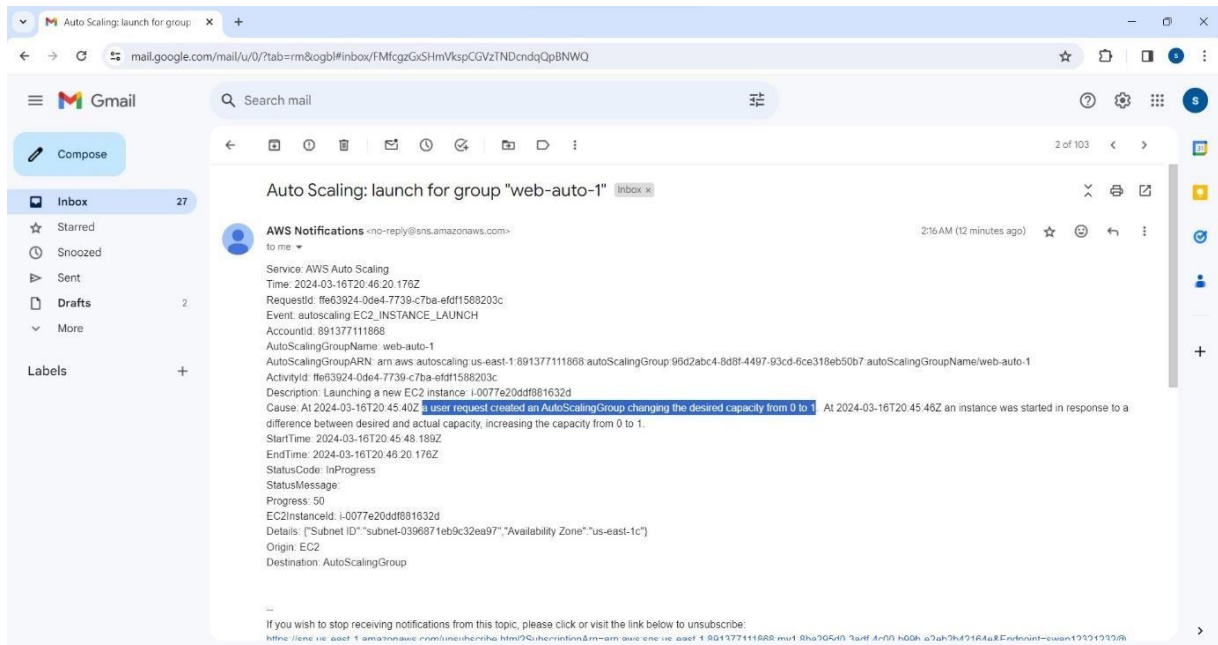
Check SNS service. New topic and subscription is created.



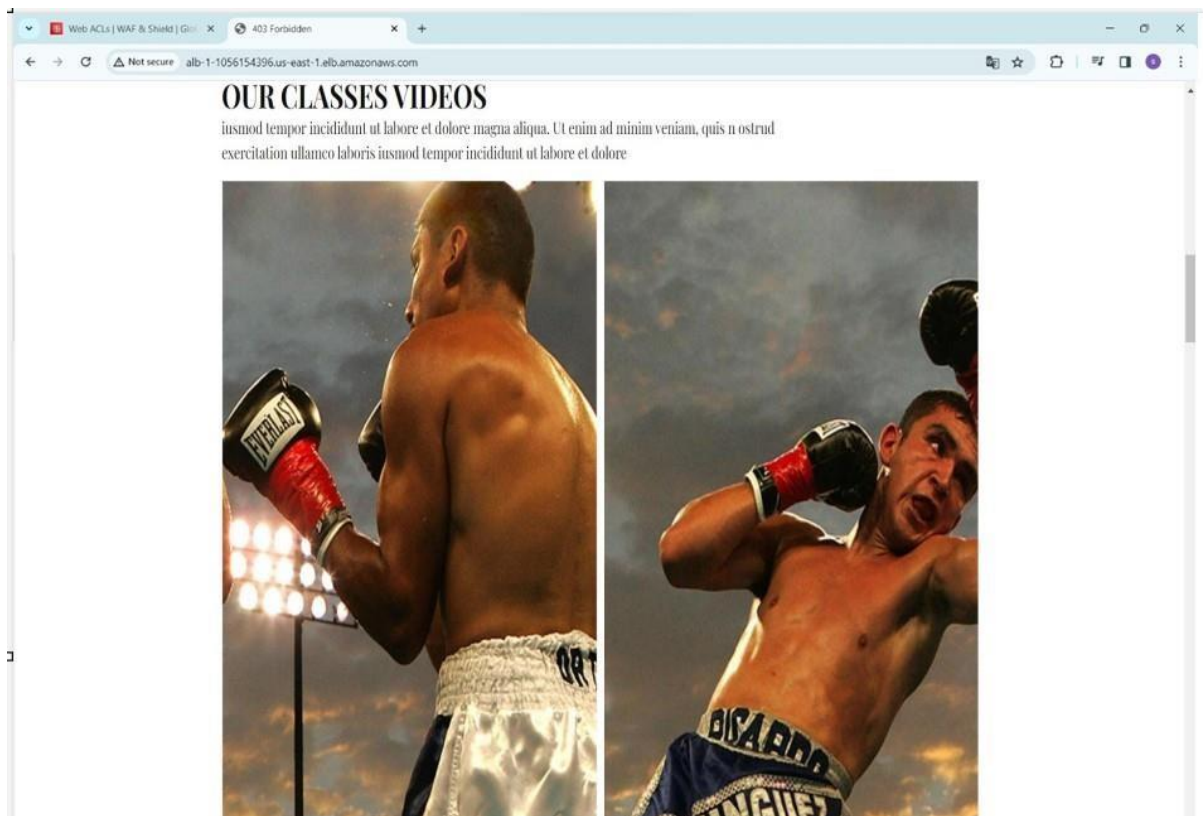
Step 14: Confirm subscription email.



Step 15: We get the notification mail of launch an instance.



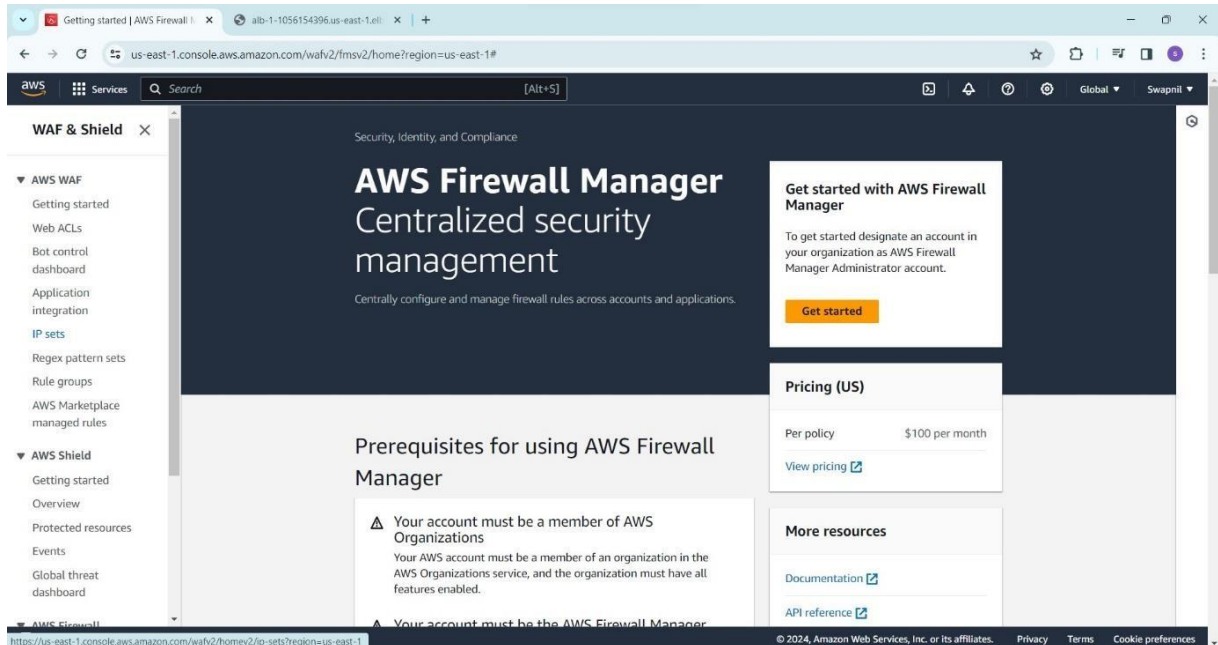
Step 16: Access the webpage through the load balancer DNS.



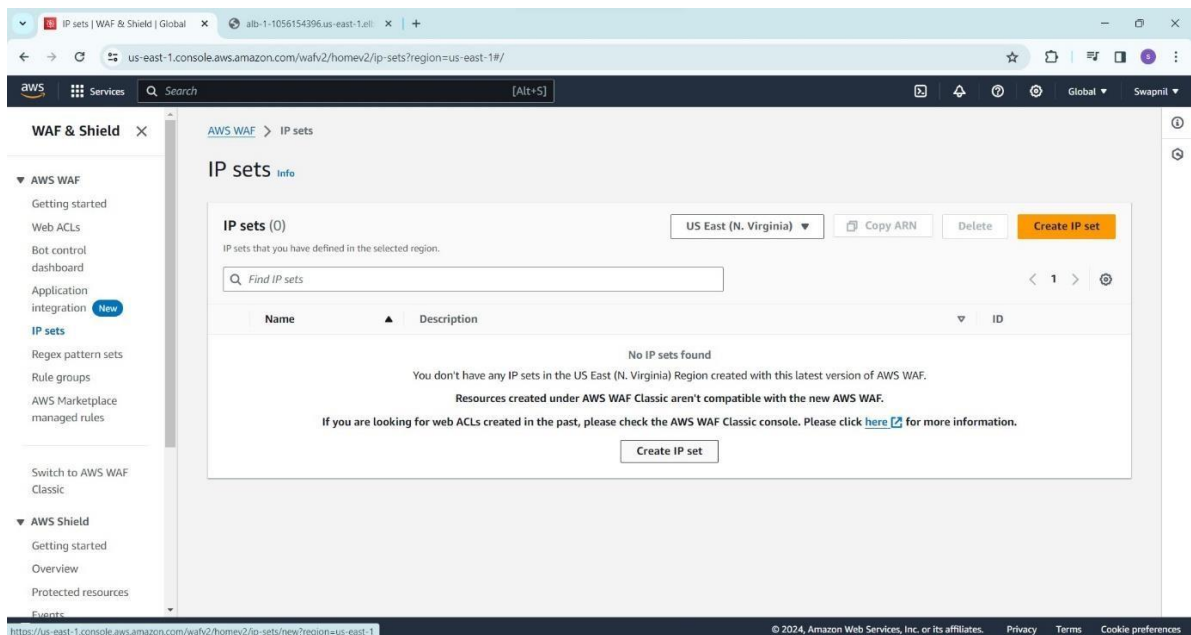
Add web application firewall

Step 17: Add Web Application Firewall (WAF) to load balancer.

➤ Go to the navigation panel and select WAF.



Step 18: Create IP sets.



Step 19: IP set details.

- Enter IP set rule name. Choose region and IP version
- Add the IP address list

Create IP set | WAF & Shield | G

us-east-1.console.aws.amazon.com/wafv2/homev2/ip-sets/new?region=us-east-1

IP set details

IP set name

ip_rule

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
Description - optional

The description can have 1-256 characters.

Region

Choose the AWS region to create this IP set in.

US East (N. Virginia)

IP version

☒ IPv4
☐ IPv6

IP addresses

103.162.158.172/31

Enter one IP address per line in CIDR format.

CloudShell Feedback

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

Step 20: Create web ACL (access control list)

Web ACLs | WAF & Shield | G

us-east-1.console.aws.amazon.com/wafv2/web-acls?region=us-east-1

Web ACLs

New AWS WAF dashboards are now available. Check them out by selecting any of your web ACLs.

Web ACLs (0)

Web ACLs that you have defined in the selected region.

US East (N. Virginia) Copy ARN Delete Create web ACL

Find web ACLs

Name	Description	ID
No web ACLs found		
You don't have any web ACLs in the US East (N. Virginia) Region created with this latest version of AWS WAF.		
Resources created under AWS WAF Classic aren't compatible with the new AWS WAF.		
If you are looking for web ACLs created in the past, please check the AWS WAF Classic console. Please click here for more information.		

Create web ACL

CloudShell Feedback

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

Step 21: Describe web ACL and associate it to AWS resources

Web ACL details

Resource type
Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

☐ Amazon CloudFront distributions

☒ Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, Amazon App Runner services, AWS AppSync GraphQL APIs, Amazon Cognito user pools and AWS Verified Access Instances)

Region
Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

US East (N. Virginia)

Name
ACL-1
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - optional

The description can have 1-256 characters.

CloudWatch metric name
ACL-1
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Associated AWS resources - optional (1) Remove Add AWS resources

➤ Add AWS resources

Add AWS resources

Resource type
Select the resource type and then select the resource you want to associate with this web ACL.

☒ Application Load Balancer ☐ Amazon API Gateway REST API ☐ Amazon App Runner service

☐ AWS AppSync GraphQL API ☐ Amazon Cognito user pool ☐ AWS Verified Access

Select the resources you want to associate with the web ACL.

Find AWS resources to associate

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	ALB-1

Cancel Add

Step 22: Add rule and rule groups.

The screenshot shows the AWS WAF console interface for adding a new rule. The left sidebar contains a navigation menu with steps: Step 1 (Describe web ACL and associate it to AWS resources), Step 2 (Add my own rules and rule groups), Step 3 (Set rule priority), Step 4 (Configure metrics), and Step 5 (Review and create web ACL). The main content area is titled 'Add my own rules and rule groups' and includes three radio button options for 'Rule type': 'IP set' (selected), 'Rule builder', and 'Rule group'. Below these, the 'Rule' section has a text input for 'Name' with the value 'rule-1'. The 'IP set' section has a dropdown menu for 'IP set' with the value 'ip_rule'. At the bottom, there is a note about IP address usage.

Rule type

☒ **IP set**
Use IP sets to identify a specific list of IP addresses.

☐ **Rule builder**
Use a custom rule to inspect for patterns including query strings, headers, countries, and rate limit violations.

☐ **Rule group**
Use a rule group to combine rules into a single logical set.

Rule

Name
rule-1
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

IP set

IP set
ip_rule

IP address to use as the originating address
When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent.

Step 23: Set rule priority.

The screenshot shows the AWS WAF console interface for setting rule priority. The left sidebar contains a navigation menu with steps: Step 1 (Describe web ACL and associate it to AWS resources), Step 2 (Add rules and rule groups), Step 3 (Set rule priority), Step 4 (Configure metrics), and Step 5 (Review and create web ACL). The main content area is titled 'Set rule priority' and includes a table with one rule. The table has columns for 'Name', 'Capacity', and 'Action'. The rule 'rule-1' has a capacity of 1 and an action of 'Block'. There are 'Move up' and 'Move down' buttons above the table. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

Rules (1/1)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

Name	Capacity	Action
rule-1	1	Block

Cancel Previous Next

Step 24: Configure metrics

The screenshot shows the 'Configure metrics' step in the AWS WAF console. On the left, a sidebar lists five steps: Step 1 (Describe web ACL and associate it to AWS resources), Step 2 (Add rules and rule groups), Step 3 (Set rule priority), Step 4 (Configure metrics), and Step 5 (Review and create web ACL). Step 4 is currently selected. The main content area is titled 'Configure metrics' and contains two sections. The first section, 'Amazon CloudWatch metrics', explains that CloudWatch metrics allow monitoring of web requests, web ACLs, and rules. It includes a table with two columns: 'Rules' and 'CloudWatch metric name'. The 'rule-1' rule is selected with a checkbox, and its corresponding metric name 'rule-1' is entered in the adjacent text field. The second section, 'Request sampling options', states that disabling request sampling prevents viewing requests that match the web ACL rules. It provides three radio button options: 'Enable sampled requests' (which is selected), 'Disable sampled requests', and 'Enable sampled requests with exclusions'. At the bottom right of the configuration area are three buttons: 'Cancel', 'Previous', and 'Next'.

Step 1
[Describe web ACL and associate it to AWS resources](#)

Step 2
[Add rules and rule groups](#)

Step 3
[Set rule priority](#)

Step 4
Configure metrics

Step 5
[Review and create web ACL](#)

Configure metrics Info

Amazon CloudWatch metrics
CloudWatch metrics allow you to monitor web requests, web ACLs, and rules.

Rules	CloudWatch metric name
<input checked="" type="checkbox"/> rule-1	<input type="text" value="rule-1"/>

Request sampling options
If you disable request sampling, you can't view requests that match your web ACL rules.

Options

- ☒ Enable sampled requests
- ☐ Disable sampled requests
- ☐ Enable sampled requests with exclusions

Cancel Previous **Next**

Step 25: Review and create web ACL.

The screenshot shows the 'Review and create web ACL' step in the AWS WAF console. The left sidebar is identical to the previous step, with Step 4 'Configure metrics' selected. The main content area is titled 'Step 4: Configure metrics' and includes an 'Edit step 4' button. It displays a summary of the configuration. At the top, there is a 'Token domain list (0)' section showing 'No items' and 'No items to display'. Below this is a table for 'Amazon CloudWatch metrics (1)' with columns 'Rules' and 'CloudWatch metric name', showing 'rule-1' mapped to 'rule-1'. Underneath is a 'Sampled requests' section with two rows: 'Sampled requests' and 'Enabled', both showing 'Enabled' for the 'Sampled requests for web ACL default actions'. At the bottom right are three buttons: 'Cancel', 'Previous', and 'Create web ACL'.

Token domain list (0)

Name
No items No items to display

Step 4: Configure metrics Edit step 4

Amazon CloudWatch metrics (1)

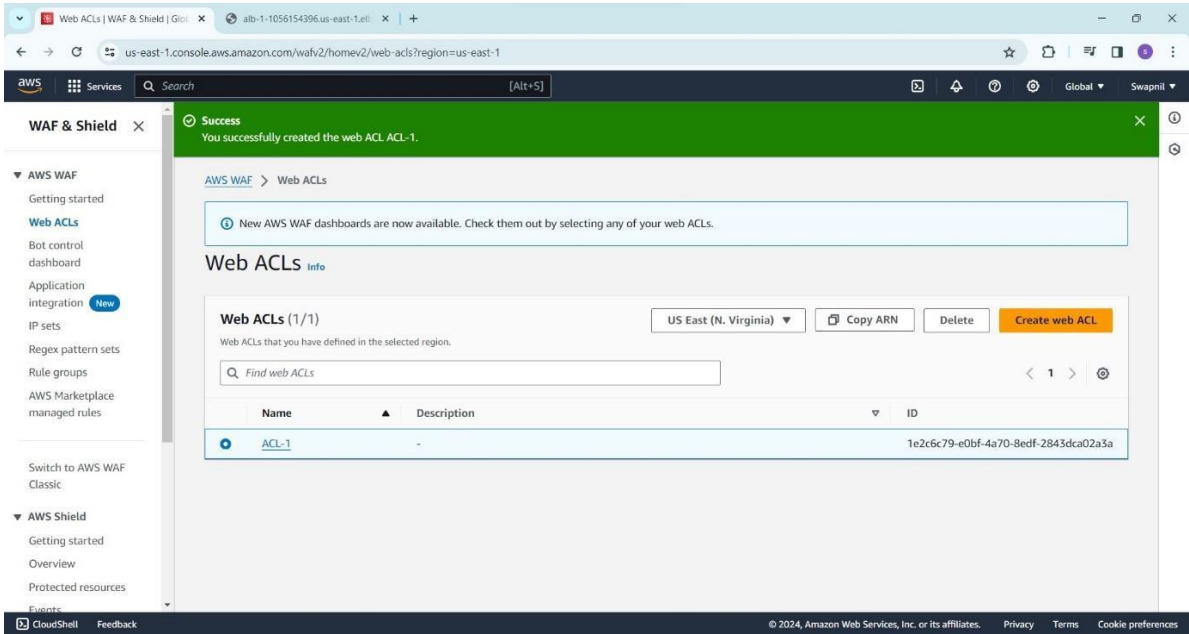
Rules	CloudWatch metric name
rule-1	rule-1

Sampled requests

Sampled requests	Sampled requests for web ACL default actions
Enabled	Enabled

Cancel Previous **Create web ACL**

Step 26: Web ACL is created.



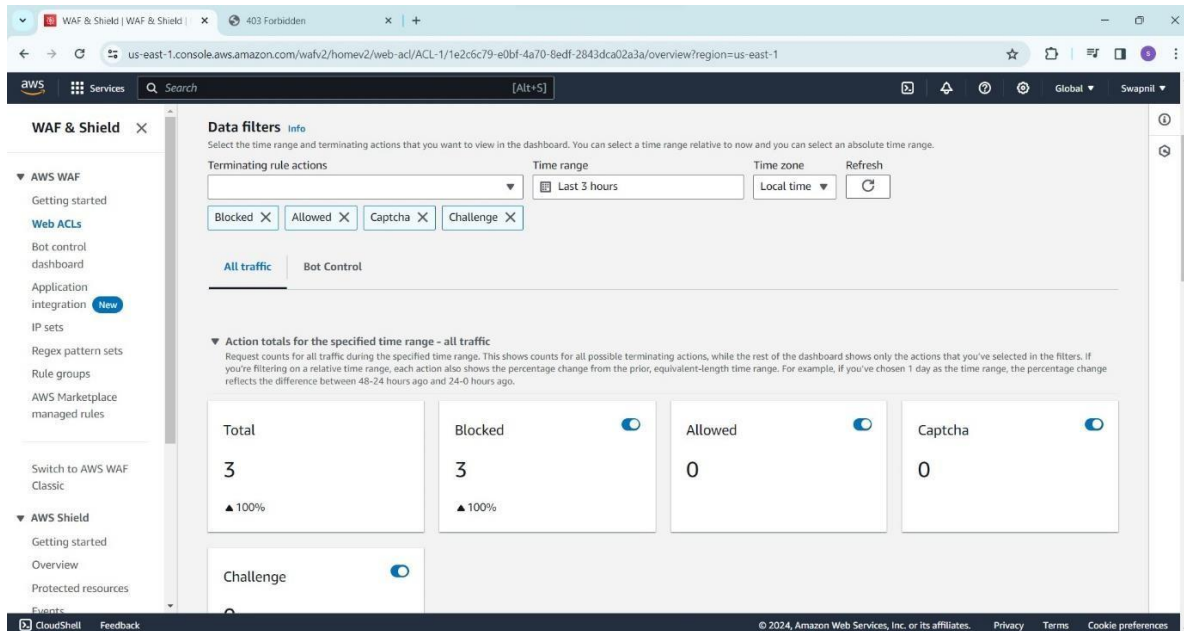
Step 27: Check the result

Try to access a load balancer from the IP which is define in the IP sets rules group. We get 403 forbidden message because WAF block that IP. 403 Forbidden error, it means that you do not have permission to view the requested file or resource.



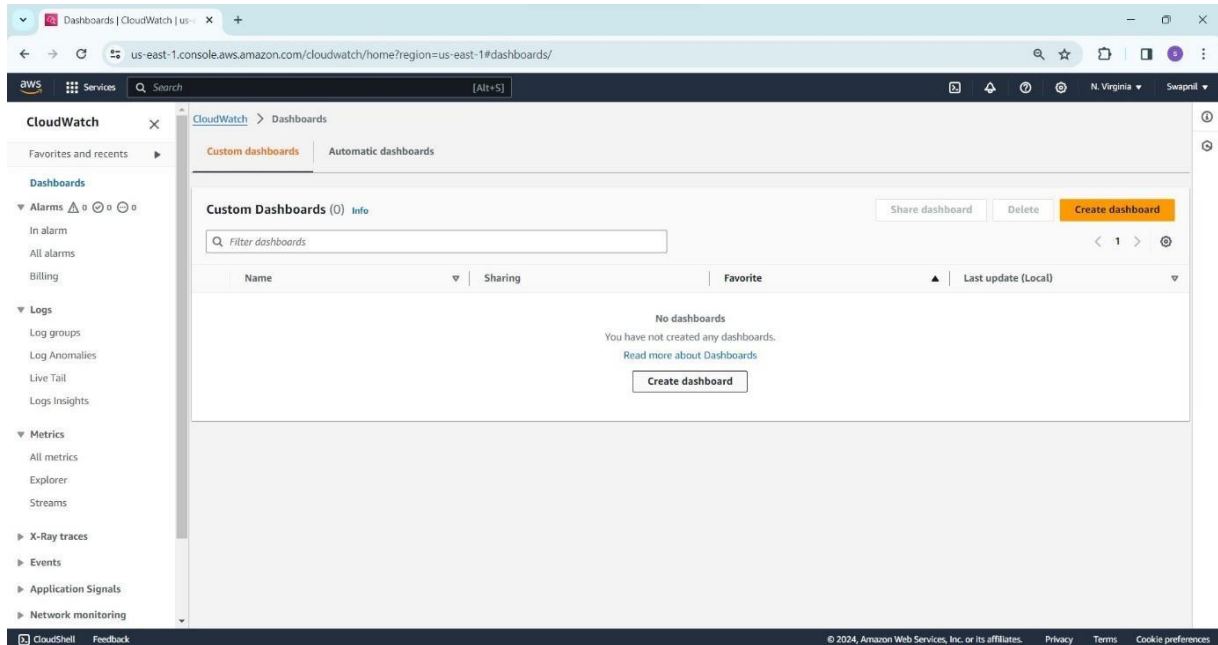
Step 28:

From WEB ACL we filter the traffic and check all details. Like blocked, allowed IP, Sample of bot detection, client device types, attack type, top 10 countries, etc.

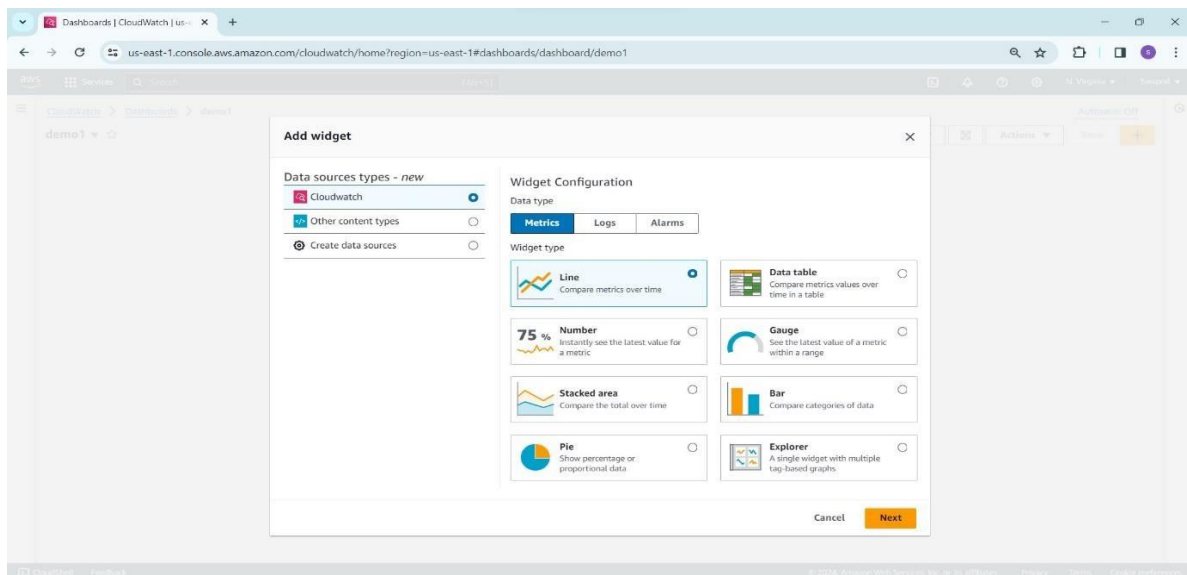


Add cloud watch: monitor the system services from the cloud watch.

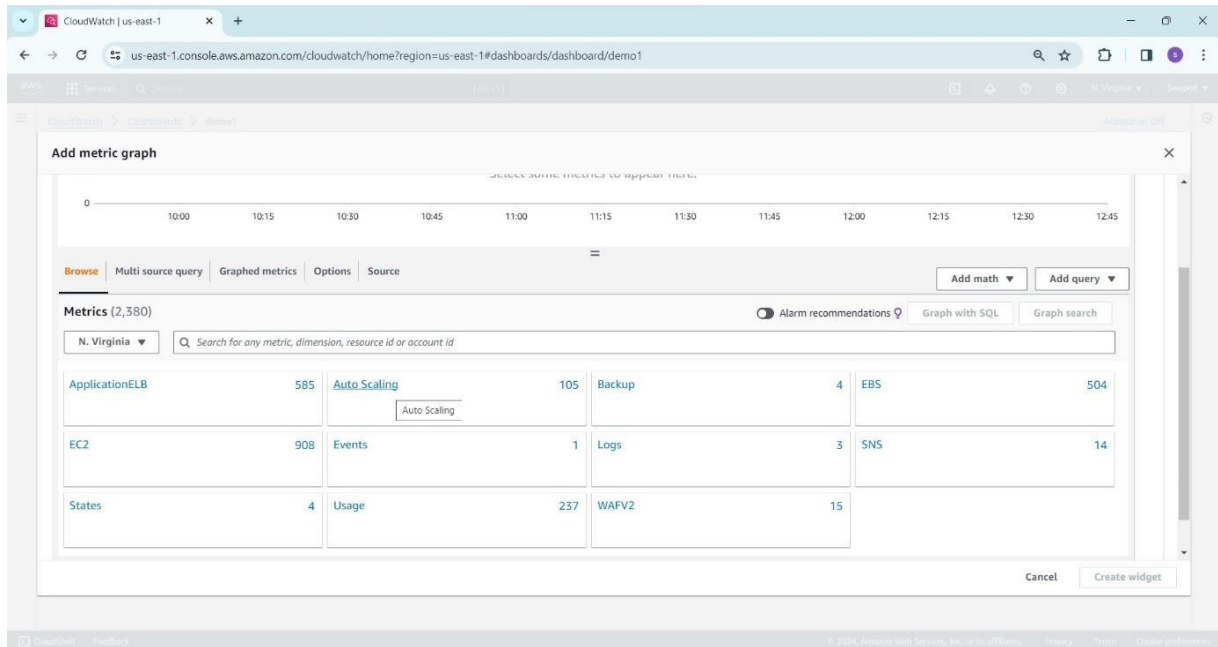
Step 29: Create a dashboard. Define the name to dashboard.



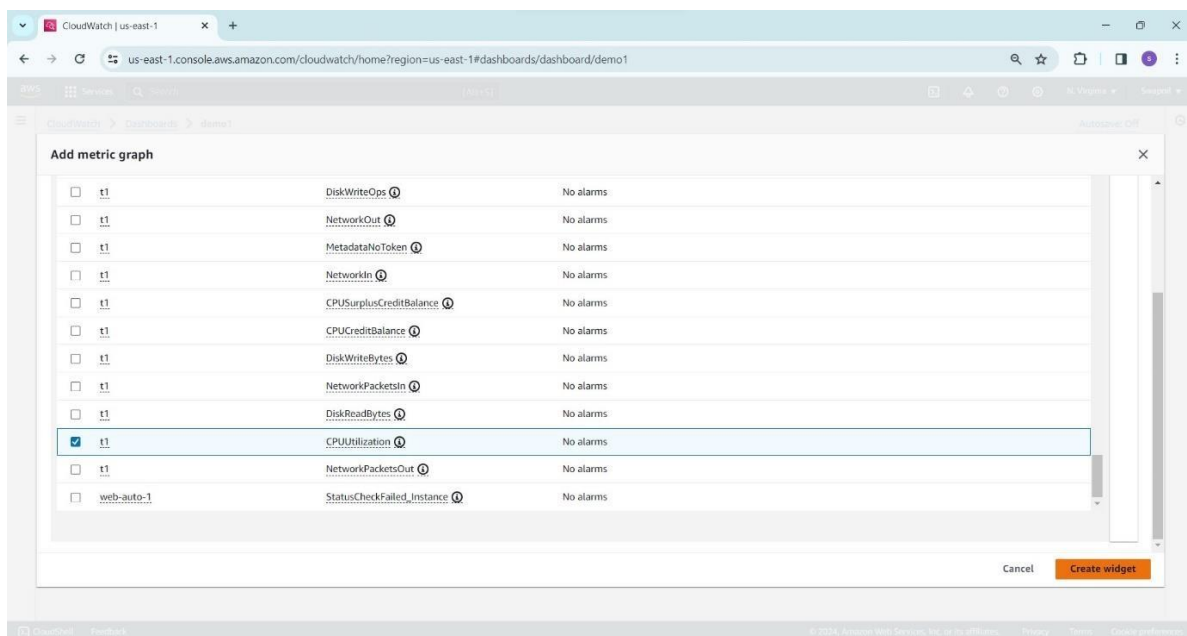
Step 30: Add the widget.



Step 31: Select metrics graph.



Step.32: Add the selected metrics graph to widget.



Step 33: Monitor the system performance.

