Static Website Deployment

With AWS S3, CloudFront, WAF, and Shield: Cloud Watch

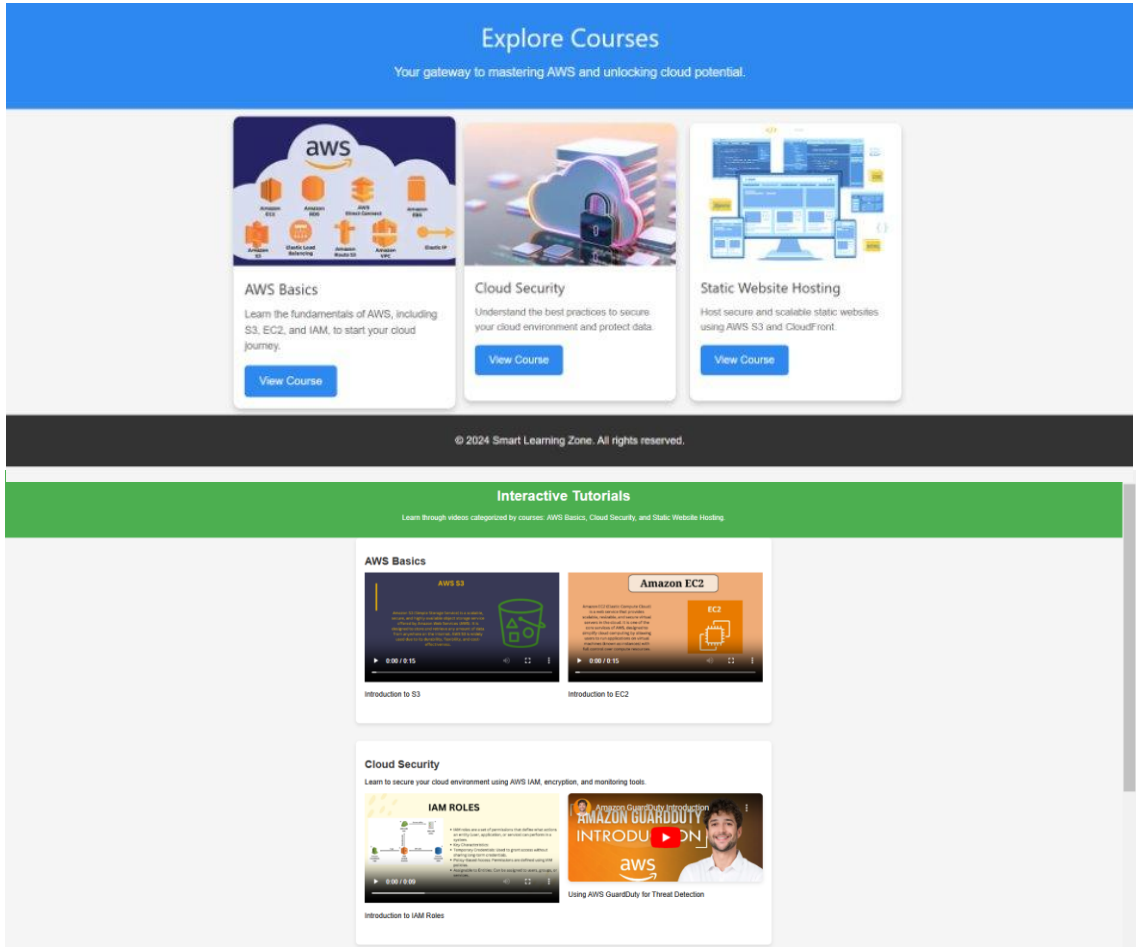
TEAM-2

- Akanksha Saxena
- Gangadhara Sai
- Bhanu Pemmaraju
- Akshitha Chimbili
- Swetha Reddy

Overview of our website

Smart Learning Zone

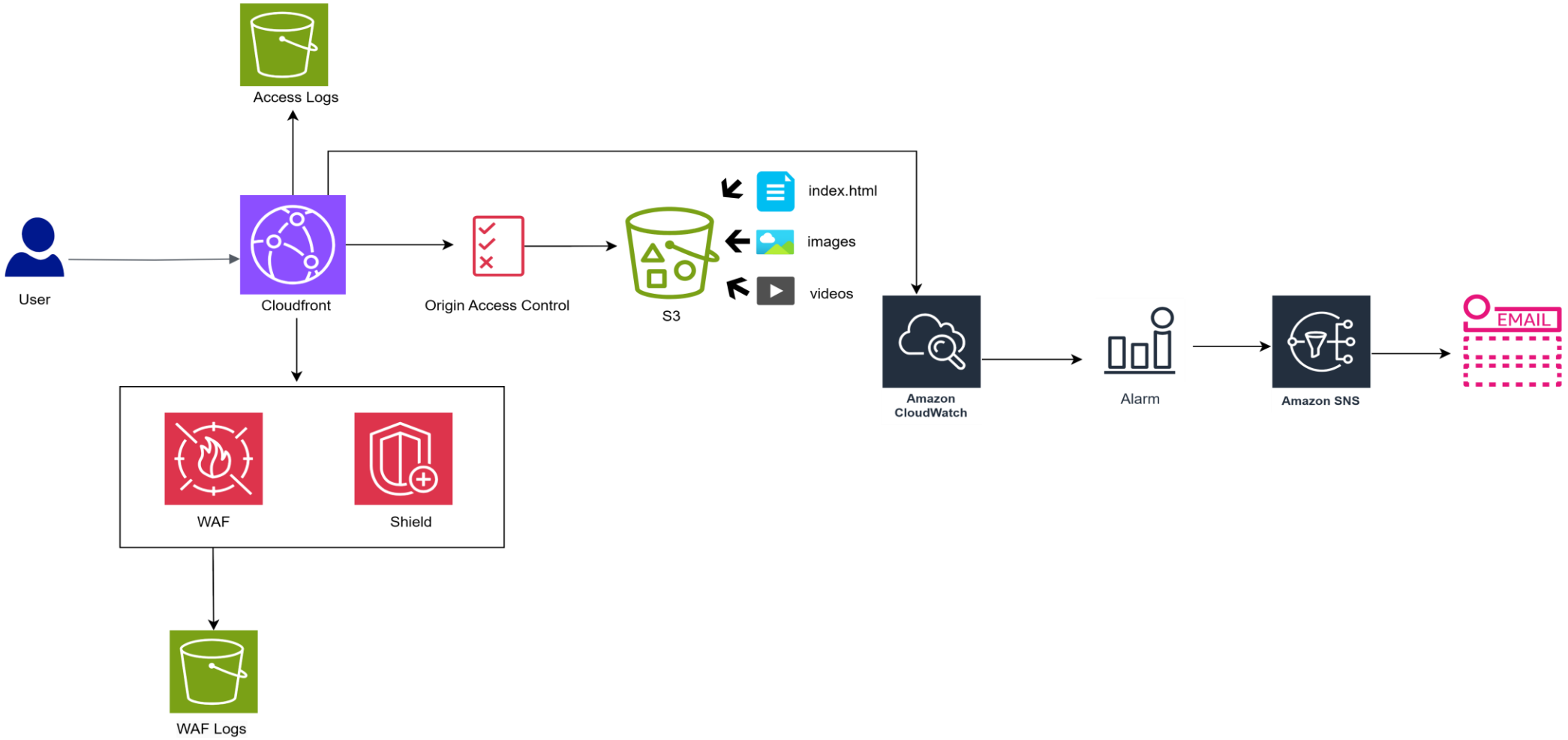
- **Purpose:**
  Smart Learning Zone is an e-learning platform designed to provide tutorials, downloadable resources, and course content on AWS technologies.
- **Core Features:**
- Hosts **static web pages** for course content and tutorials.
  Offers **downloadable resources** such as PDFs, images, and cheatsheets stored securely in S3.
- **Target Audience:**
  Individuals or organizations looking to learn about AWS services and explore real-world applications of cloud technologies.



Overview of Secure Website Deployment

- **Objective:**Deploy a highly available, secure, and scalable static website using AWS services.
- **Key AWS Services Used:**
- **Amazon S3:** Stores the static website files.
- **CloudFront:** Distributes the content globally with low latency.
- **AWS WAF (Web Application Firewall):** Protects against common web exploits.
- **AWS Shield:** Provides DDoS protection.
- **Security and Monitoring:**Implement logging and monitoring using CloudWatch and S3 logs.
- Apply IAM users for secure access.

Cloud Architecture for Smart Learning Zone on AWS



IAM Users

IAM

IAM (Identity and Access Management) is a feature of AWS that enables secure control of access to AWS resources.

IAM User:

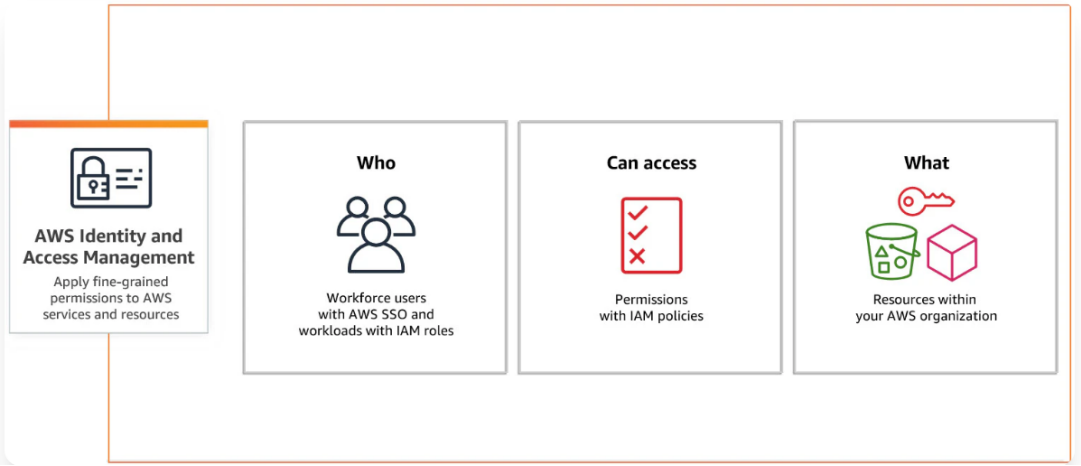
- Represents an individual with specific credentials to interact with AWS.
- IAM users can have passwords for AWS Management Console and access keys for API/CLI access.

Key Features of IAM Users:

- Access permissions can be customized with policies.
- Users are part of an AWS account and inherit permissions via IAM roles or policies.
- Essential for controlling **who** can access resources and **what actions** they can perform.

Example Scenario:

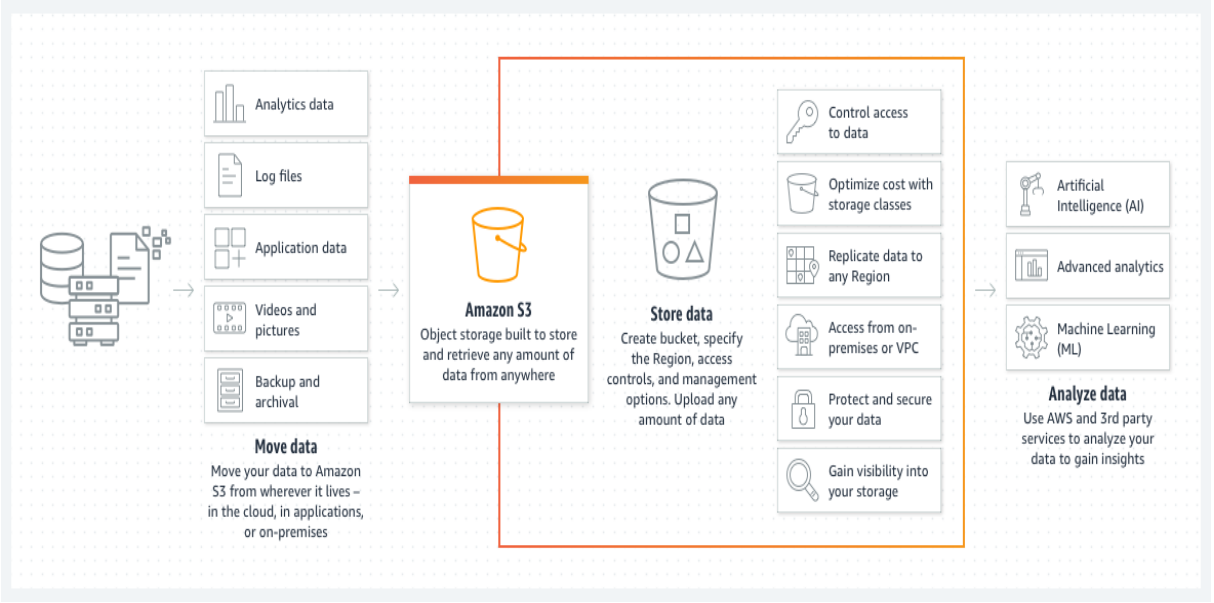
An IAM user "Developer1" can be assigned permissions to upload files to S3 but restricted from modifying other settings in the AWS environment.



	Role	Permissions	Responsibilities
	Root Account	Full access to all services	Initial setup and IAM role assignment
	S3 Manager	Manage S3 buckets and objects	File uploads and bucket-level management
	CloudFront Manager	Create and update distributions	Optimize content delivery
	Security Specialist	Configure WAF and security policies	Protect against web-based attacks
	Monitoring Specialist	Access CloudWatch and configure alarms	Monitor performance and detect anomalies

WHAT IS S3?

- Amazon S3 (Simple Storage Service) is a cloud-based object storage service offering scalability, data availability, security, and performance for a wide range of use cases.
- **Scalable Object Storage:** Amazon S3 offers virtually unlimited storage with elastic scalability and pay-as-you-go pricing.
- **Durability and Availability:** Provides 99.99% data durability and 99.99% availability, backed by strong SLAs.
- **Advanced Security:** Ensures secure, private, and encrypted data storage with robust access controls and auditing.
- **Cost-Effective Storage Classes:** Supports multiple storage classes and automated lifecycle management for cost optimization.
- **High Performance:** Delivers low latency, high throughput, and resilience for seamless data management and analysis.



S3 Static Website Setup Step

Step 1: Create Bucket

Step 2: Bucket Properties Overview

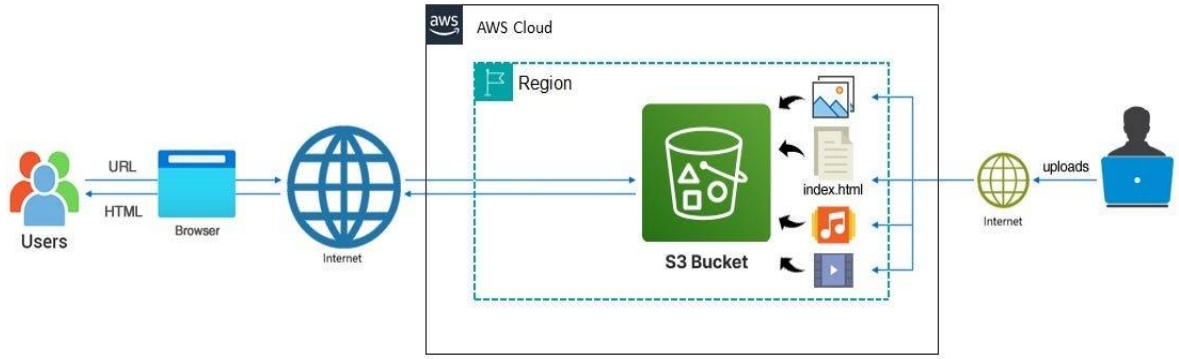
Step 3: Static Website Hosting Configuration

Step 4: Bucket Objects Overview

Step 5: Configuring Block Public Access Settings

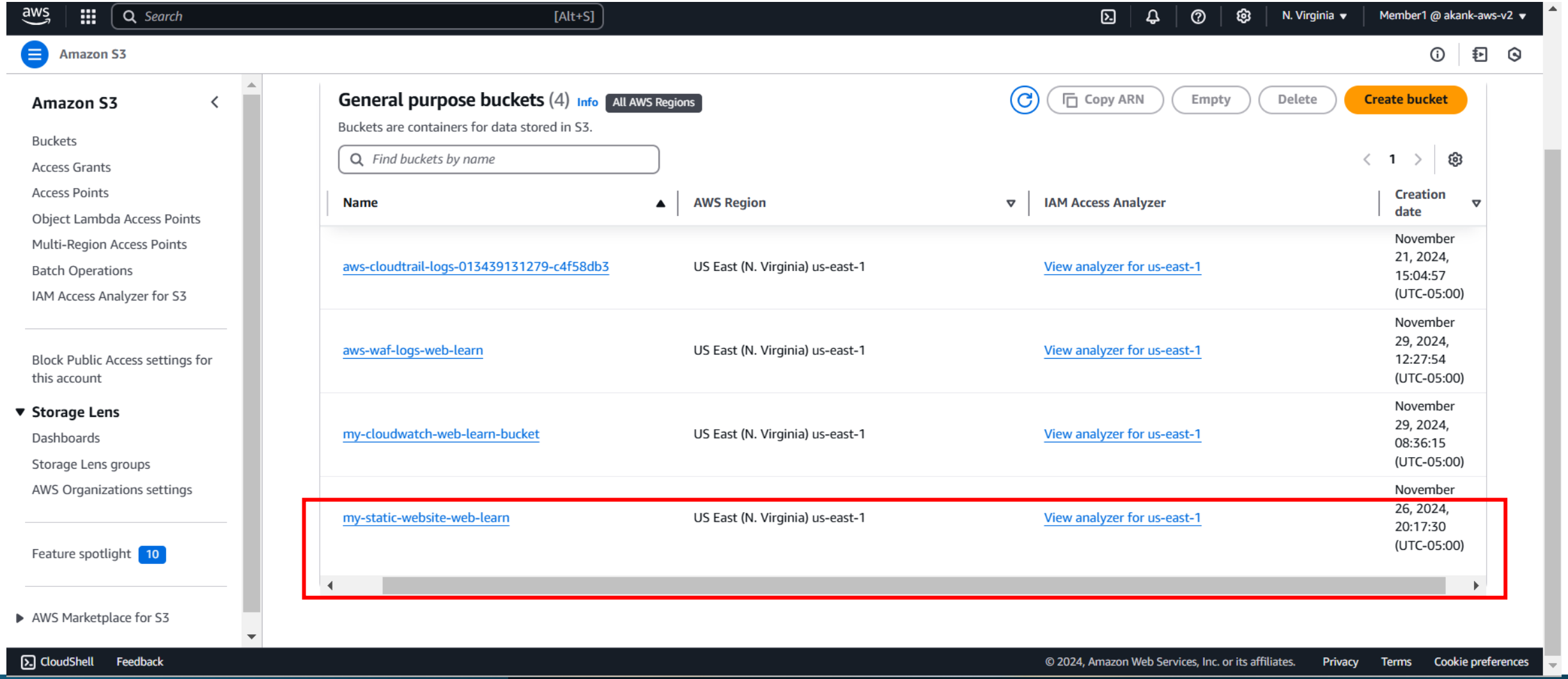
Step 6: Configuring Bucket Policy

Step 7: Testing Website



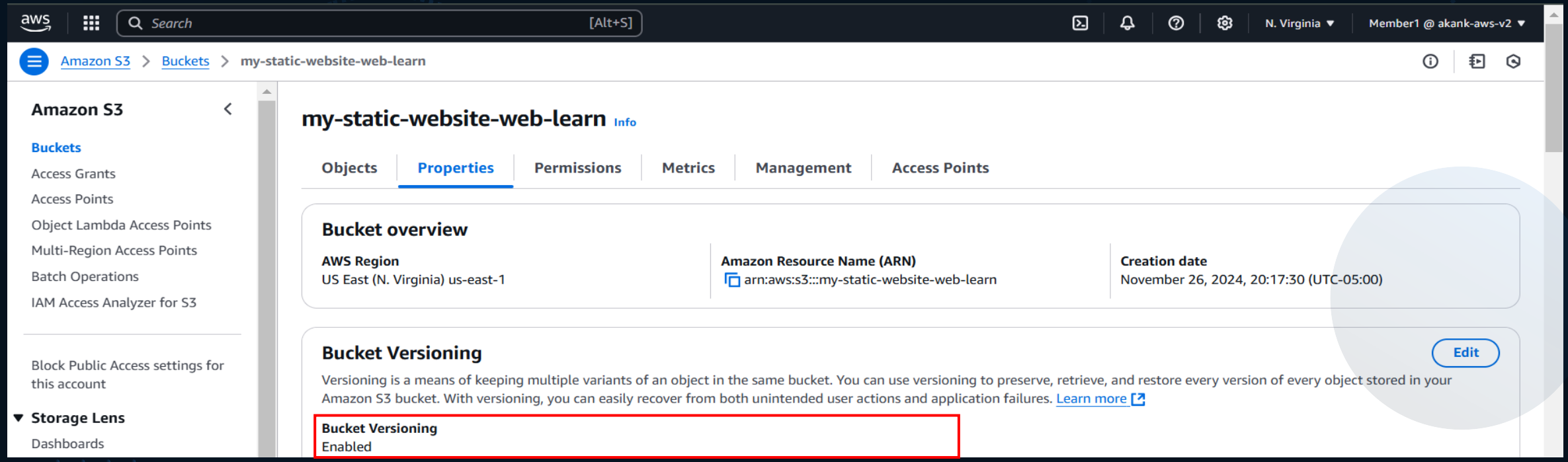
Step 1: Create Bucket

- This screen represents the Amazon S3 dashboard where all buckets are listed and managed.
- The bucket named "my-static-website-web-learn" is selected as the static website hosting bucket, located in the US East (N. Virginia) region.



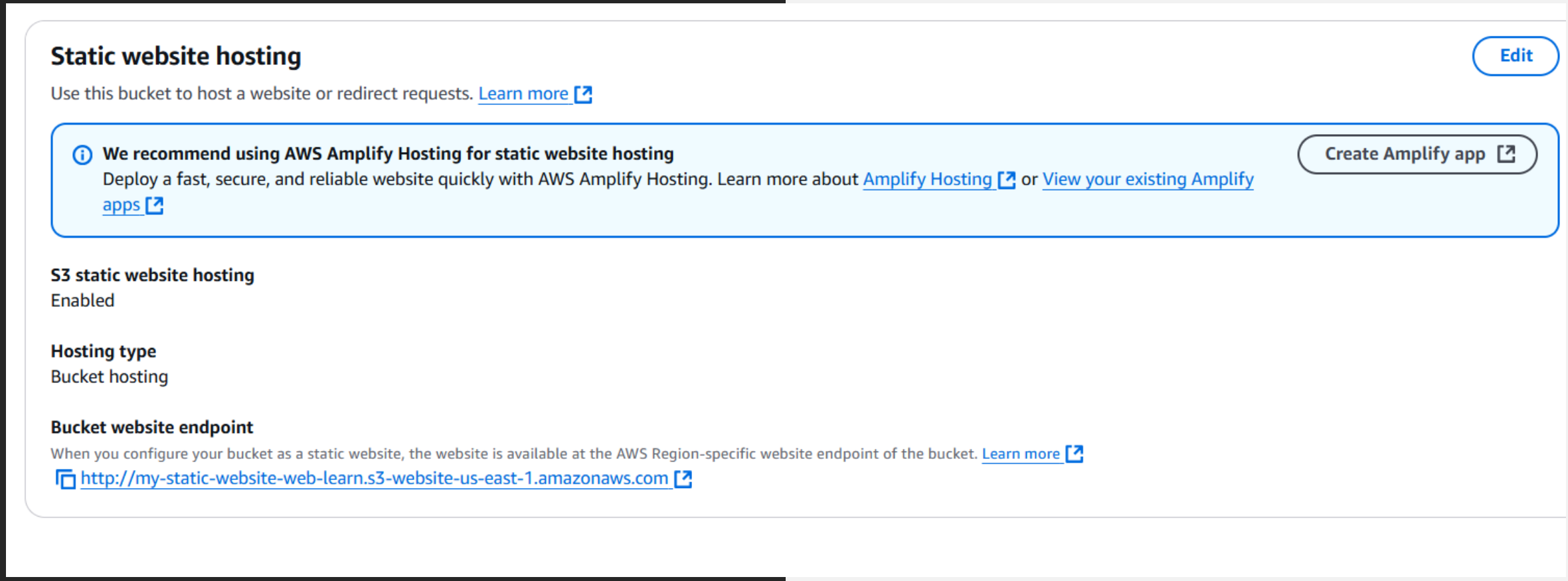
Step 2: Enable Versioning

- **Bucket Overview:** Includes key details like the AWS Region (us-east-1), ARN, and creation date for identification and management.
- **Versioning Enabled:** Ensures data recovery and protection by storing multiple versions of objects in the bucket.



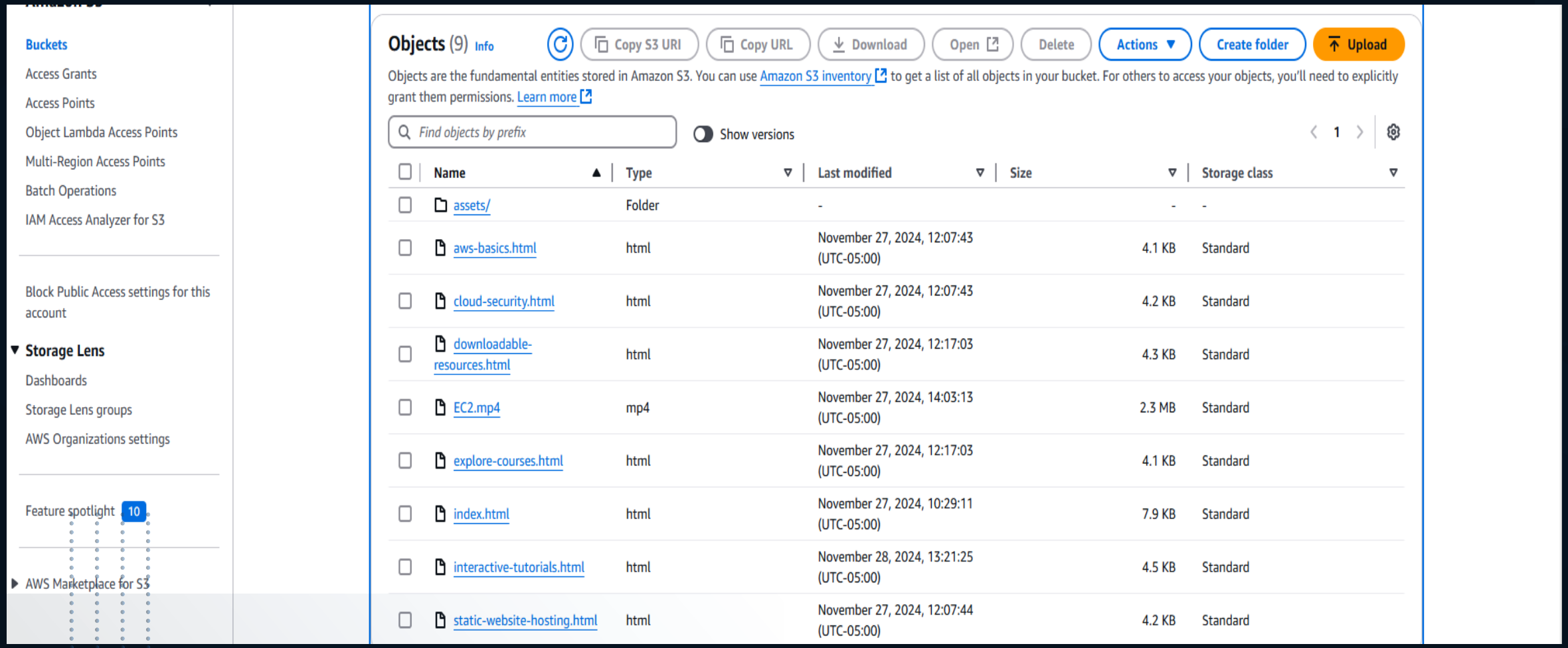
Step 3: Static Website Hosting Configuration

- Static website hosting is enabled for this bucket with "Bucket Hosting" type.
- Website is accessible via the endpoint: http://my-static-website-web-learn.s3-website-us-east-1.amazonaws.com.



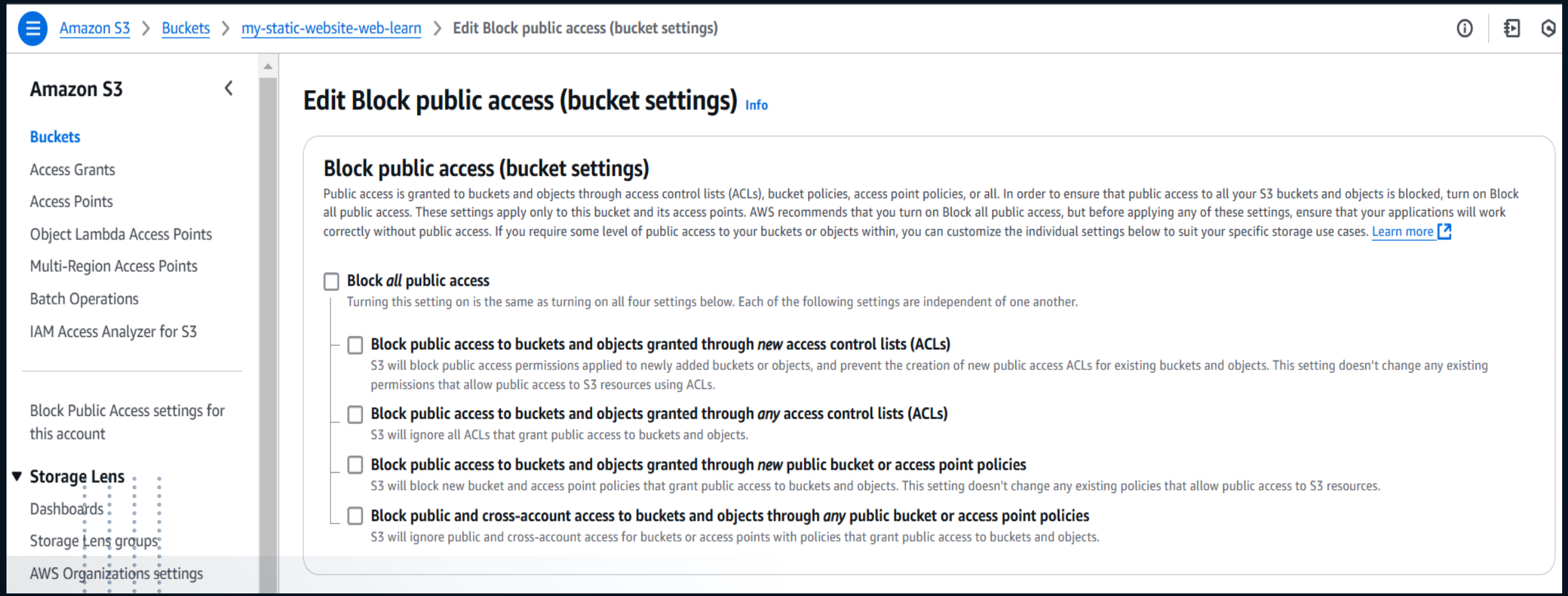
Step 4: Upload Bucket Objects

- Displays the files (HTML, PDFs, MP4, etc.) stored for the static website, including index.html as the main page.



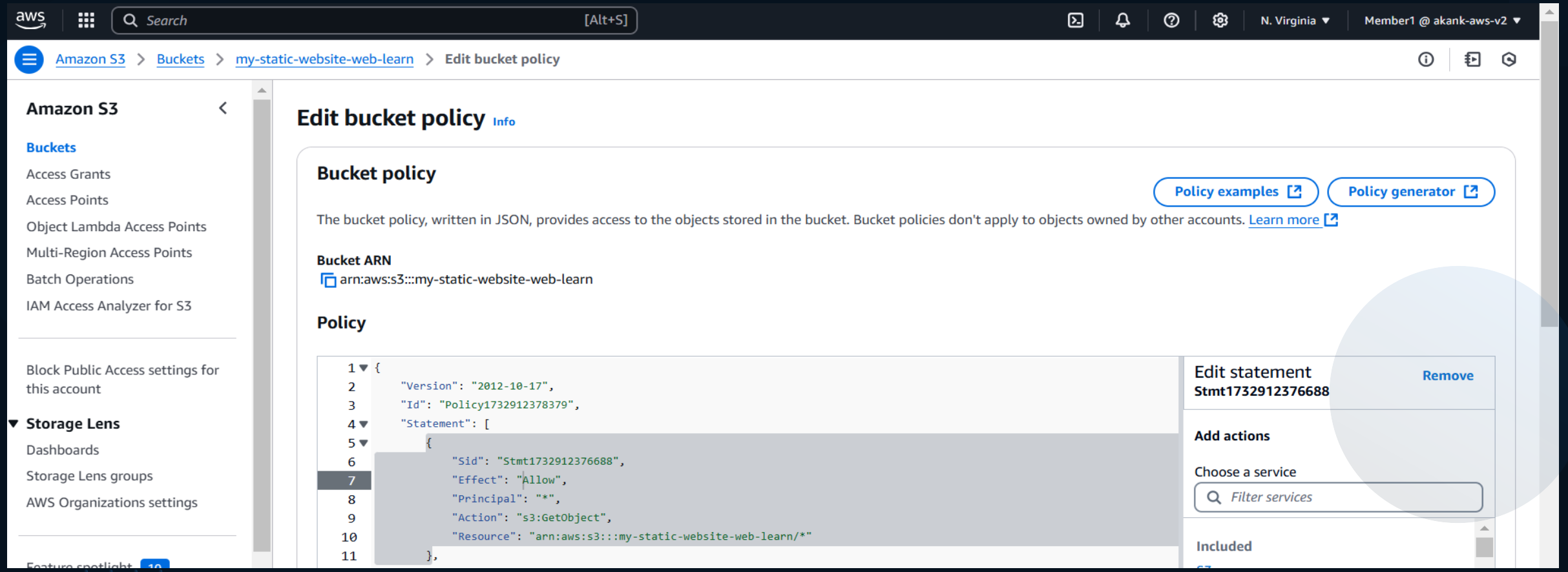
Step 5: Configuring Block Public Access Settings

- By default, public access is blocked to ensure security and prevent unauthorized data exposure.
- Hosting a static website requires unchecking "Block all public access" and adjusting permissions.



Step 6: Configuring Bucket Policy

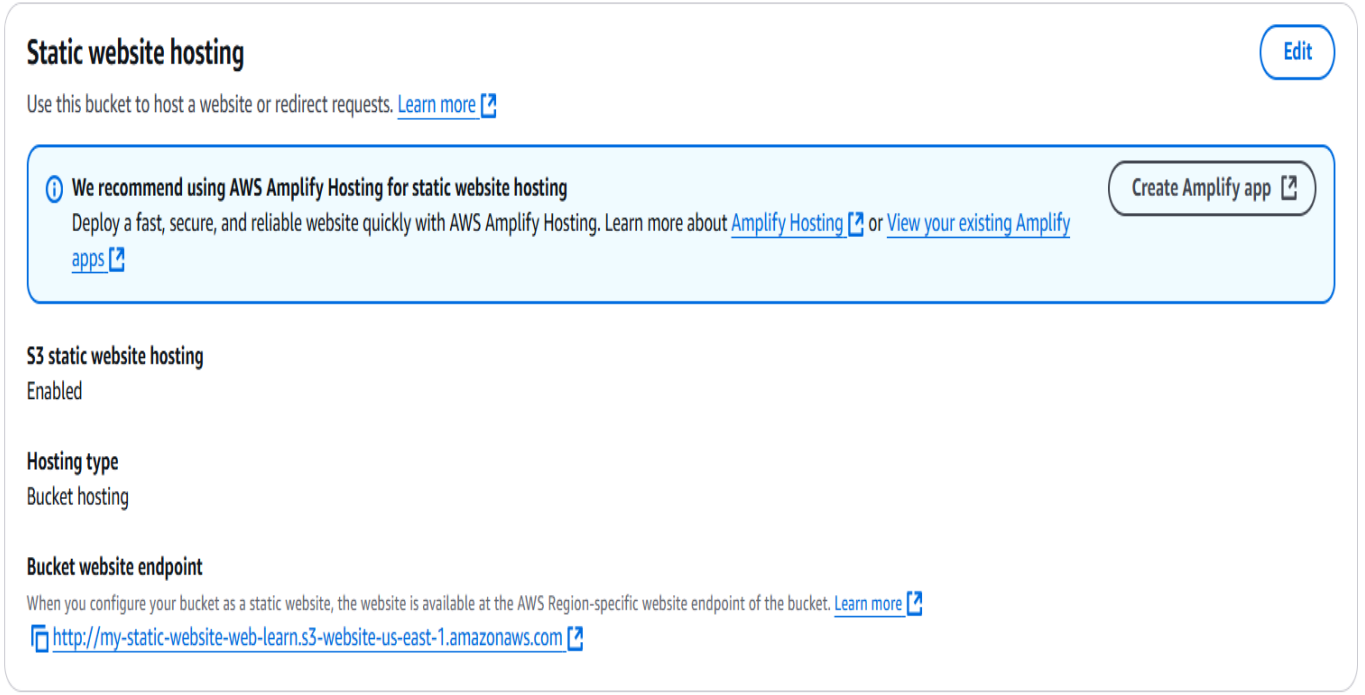
- Bucket policies define access control rules for the objects in the bucket using JSON.
- Public read access is enabled by allowing the s3:GetObject action for all users (Principal: "*").
- Policy applies to all objects in the bucket (arn:aws:s3:::my-static-website-web-learn/*).



Step 7: Testing website

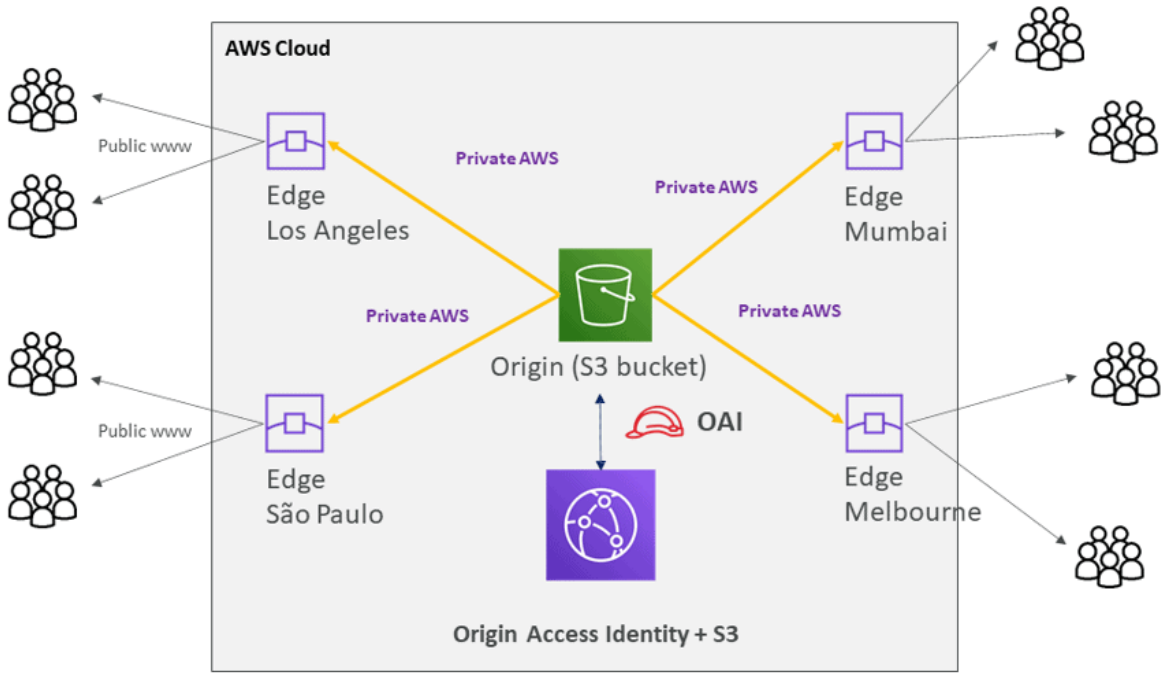
http://my-static-website-web-learn.s3-website-us-east-1.amazonaws.com

- S3 static website hosting is enabled, allowing the bucket to serve static web content directly.
- The website is accessible via the endpoint:http://my-static-website-web-learn.s3-website-us-east-1.amazonaws.com



Coudfront

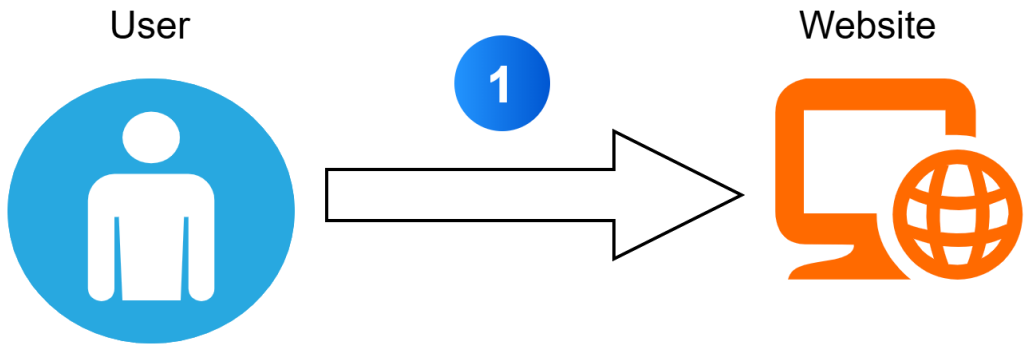
- Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the request is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.



How cloud front works?

- Step 1

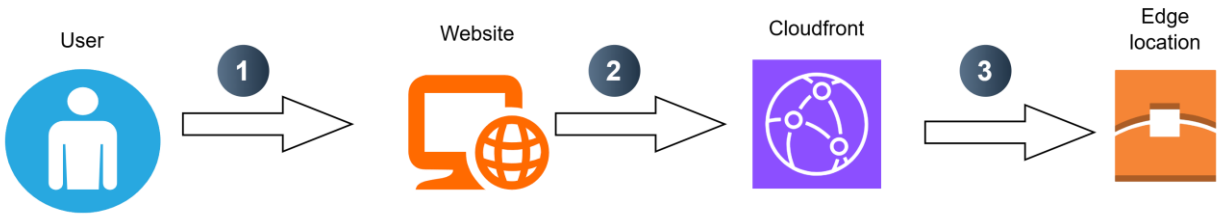
The client accesses a website and requests to download a file



How cloud front works?

- Step 2

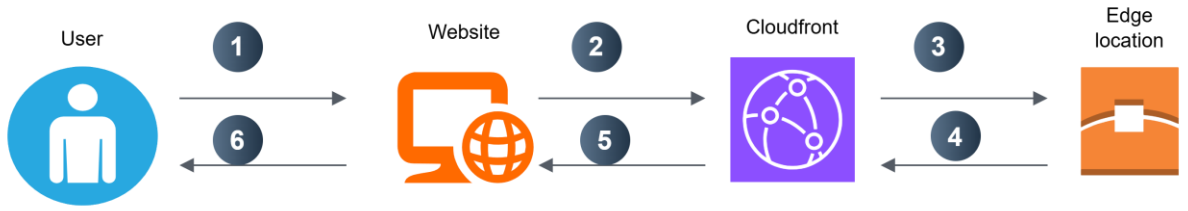
Now, the DNS routes the client request to the nearest edge location through CloudFront to serve the user request.



How cloud front works?

- Step 3

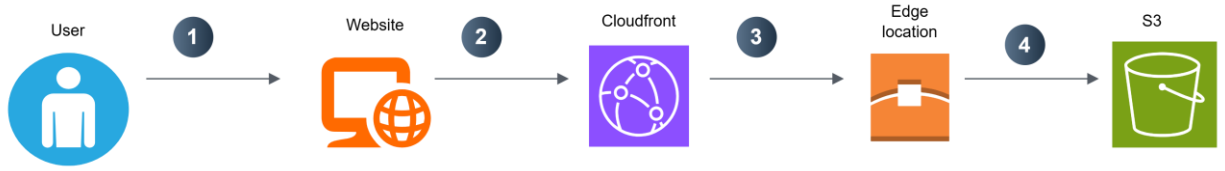
At edge location, CloudFront looks for its requested cache file. Once the file is found, CloudFront sends the file to the user.



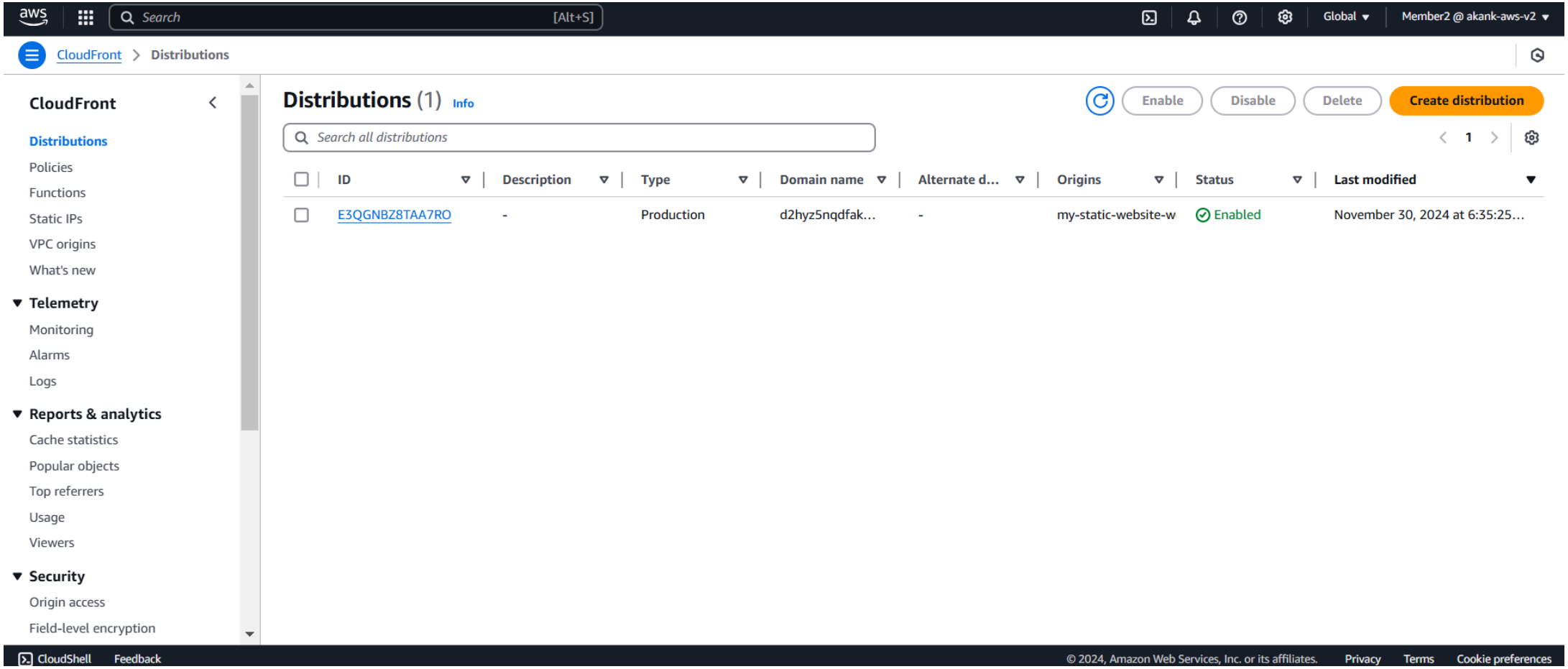
How cloud front works?

- Step 4

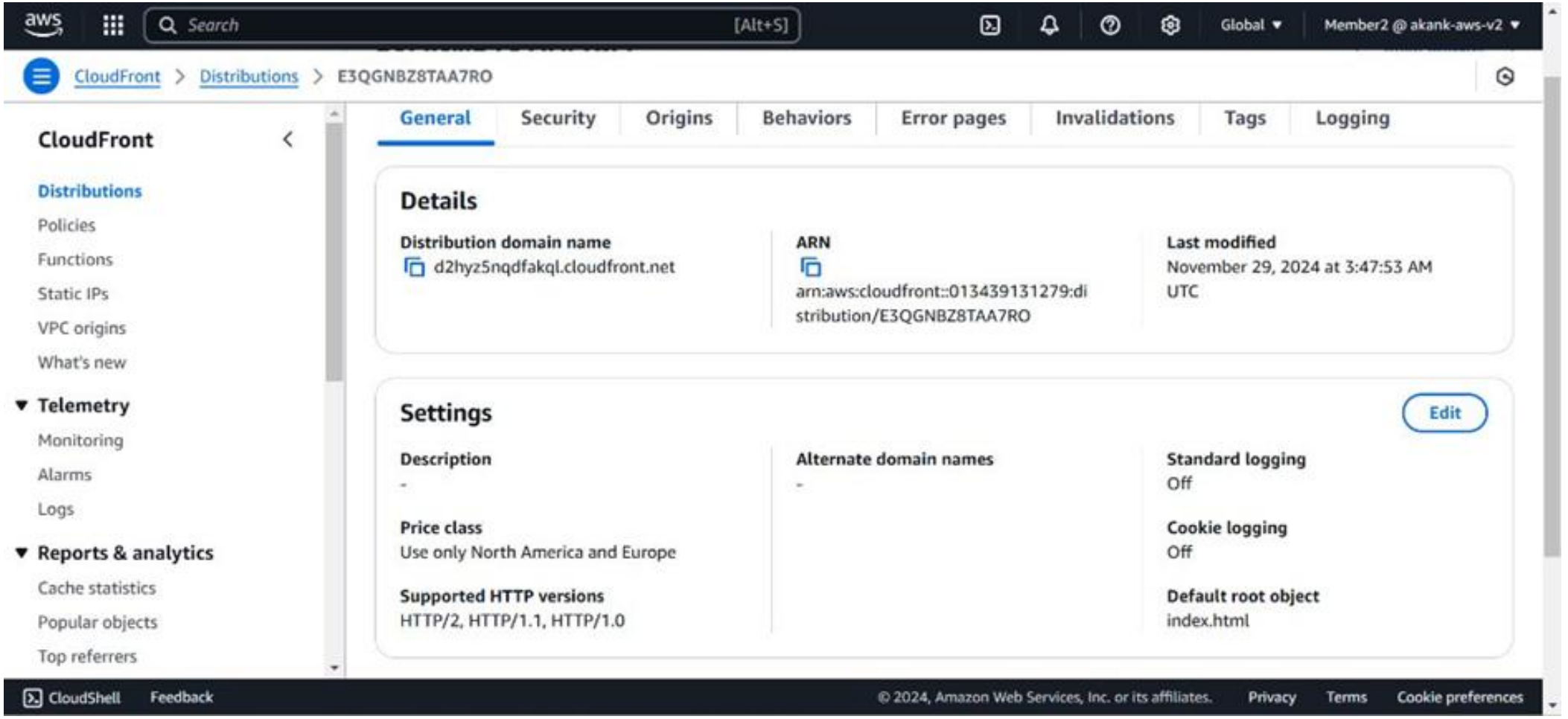
If the file is not found in the cache, CloudFront forwards the request to the origin server, such as an S3 bucket. Once the file is retrieved, it is cached at the edge location for future requests, improving performance for subsequent users.



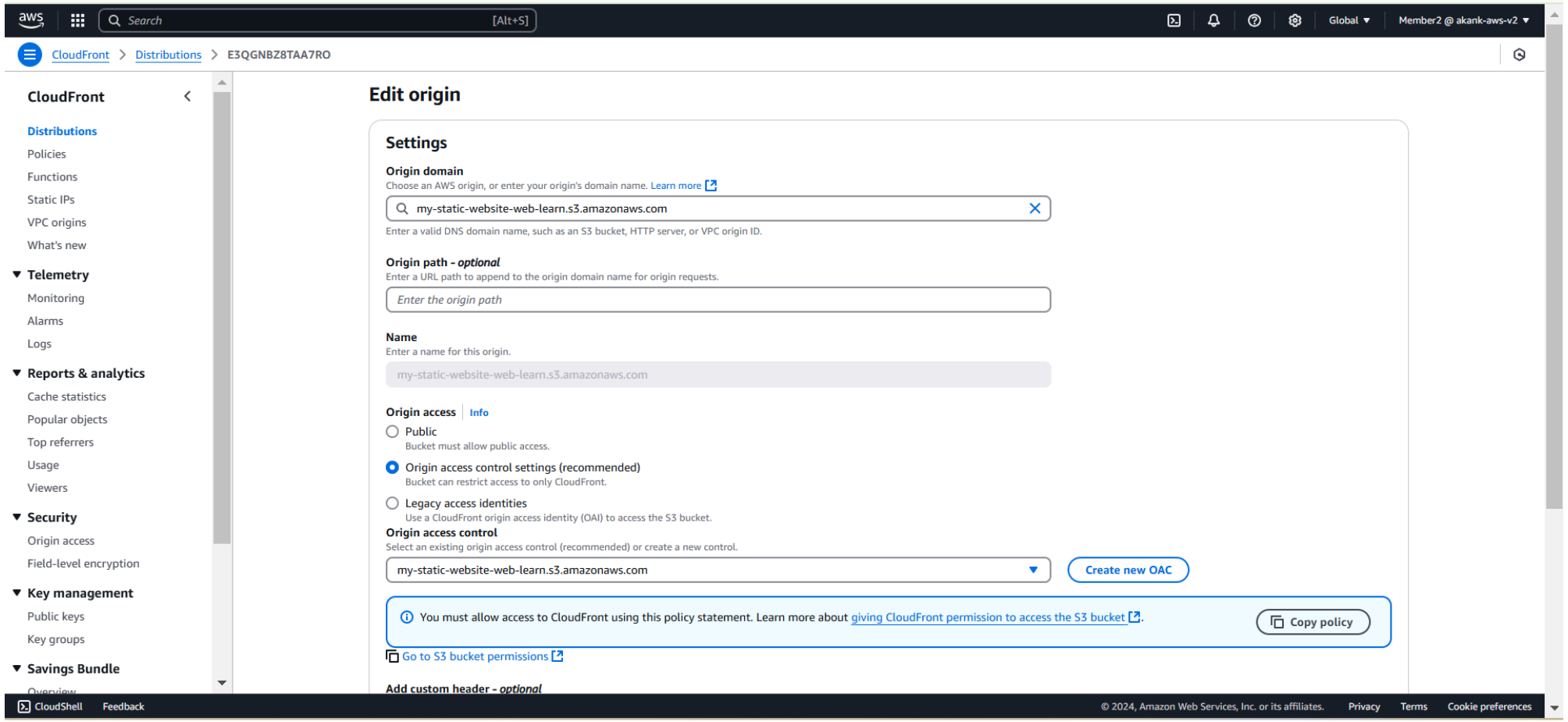
Create a CloudFront Distribution



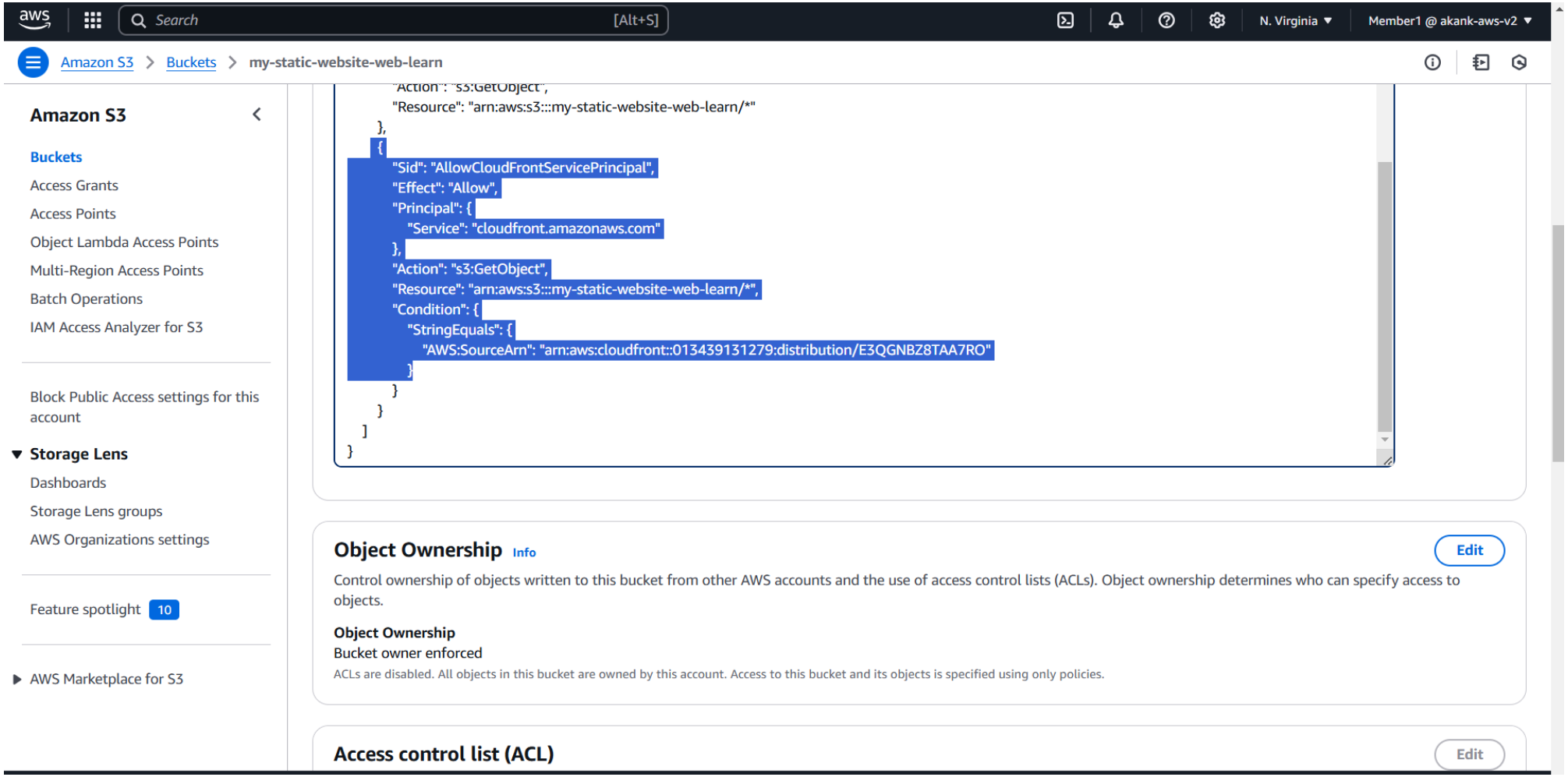
AWS CloudFront Configuration



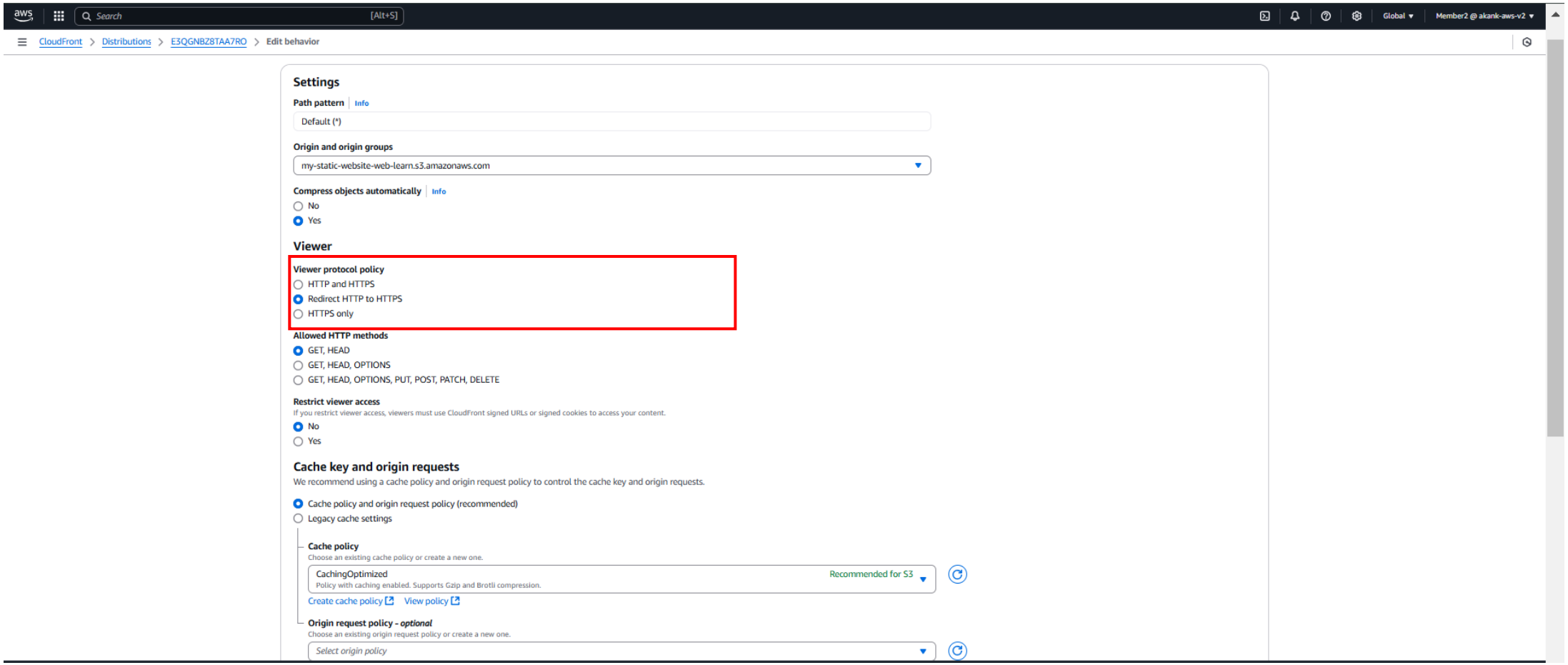
CloudFront Origin Access Control (OAC) Settings



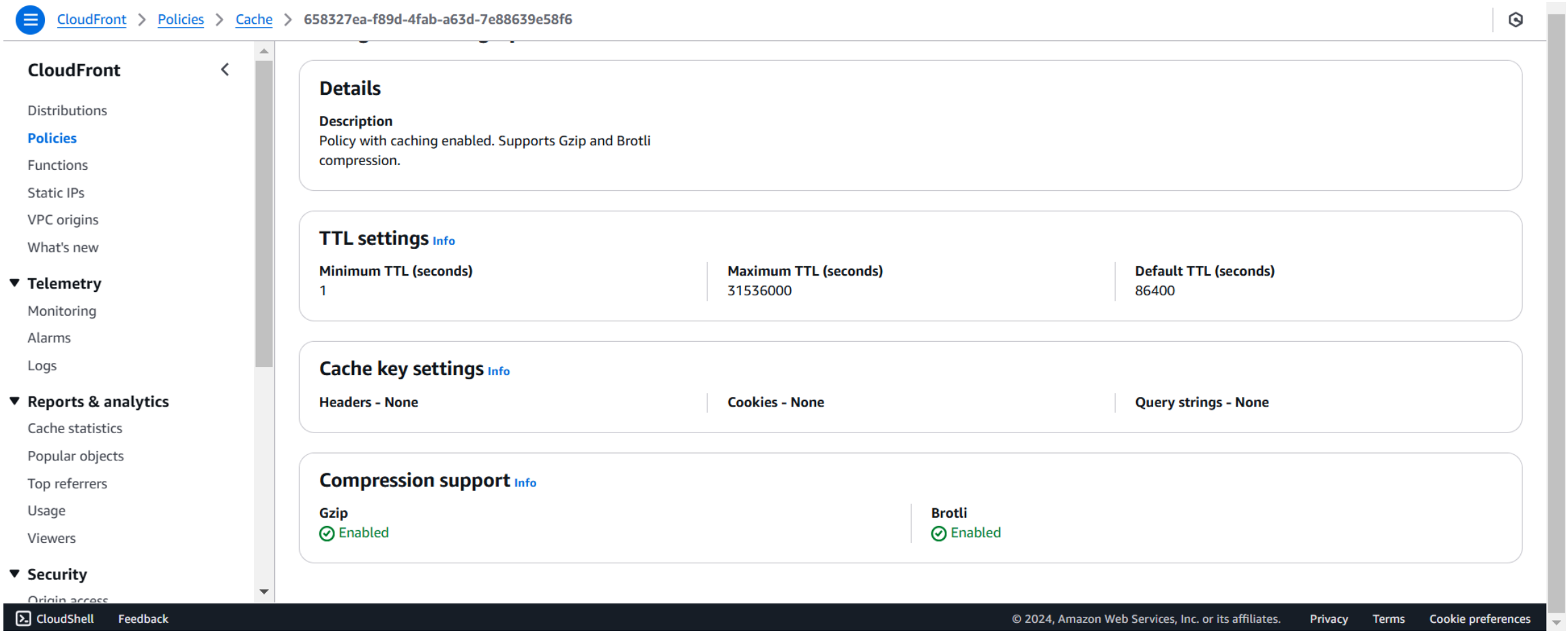
Update S3 Bucket Policy



CloudFront Distribution Behavior



Cache Policy

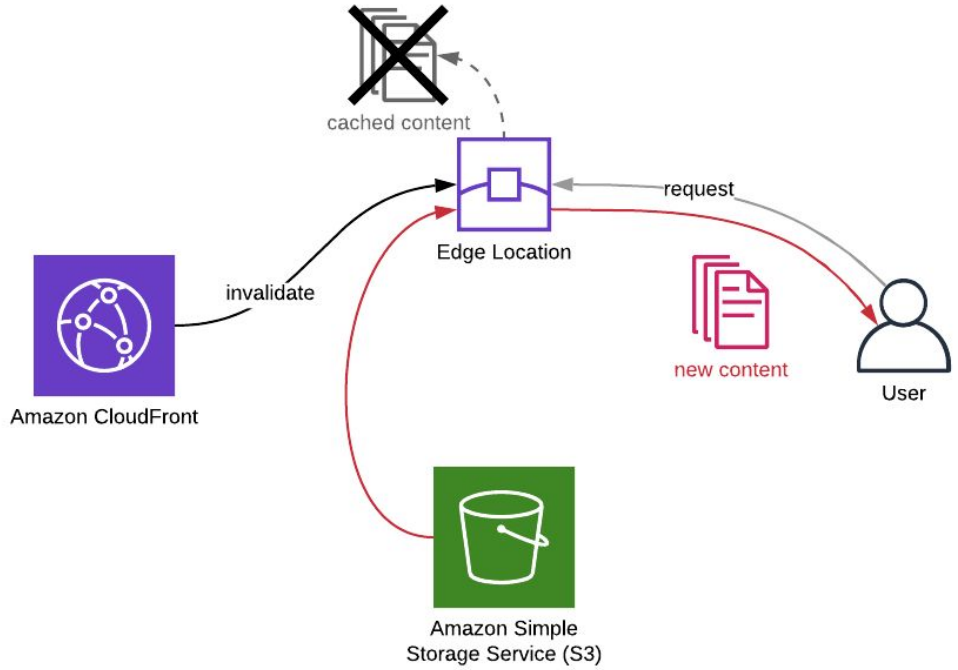


Invalidation

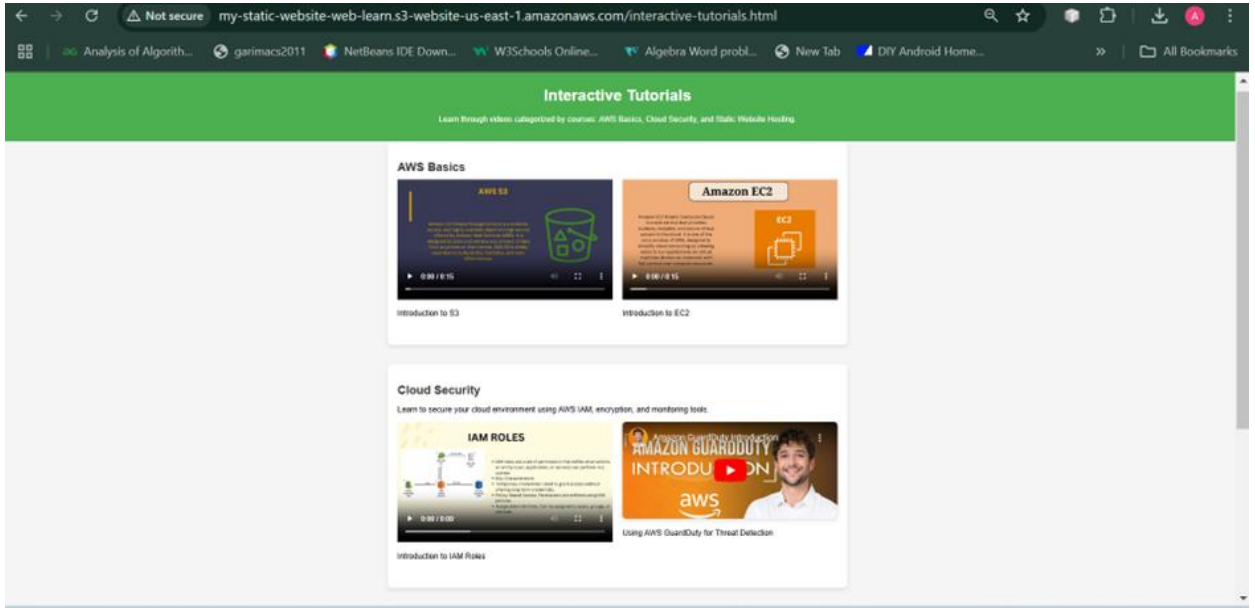
AWS CloudFront Invalidation is the process of removing or **purging cached content** from CloudFront edge locations before the content expires. This action forces CloudFront to fetch the updated content from the origin server the next time it's requested.

Purpose:

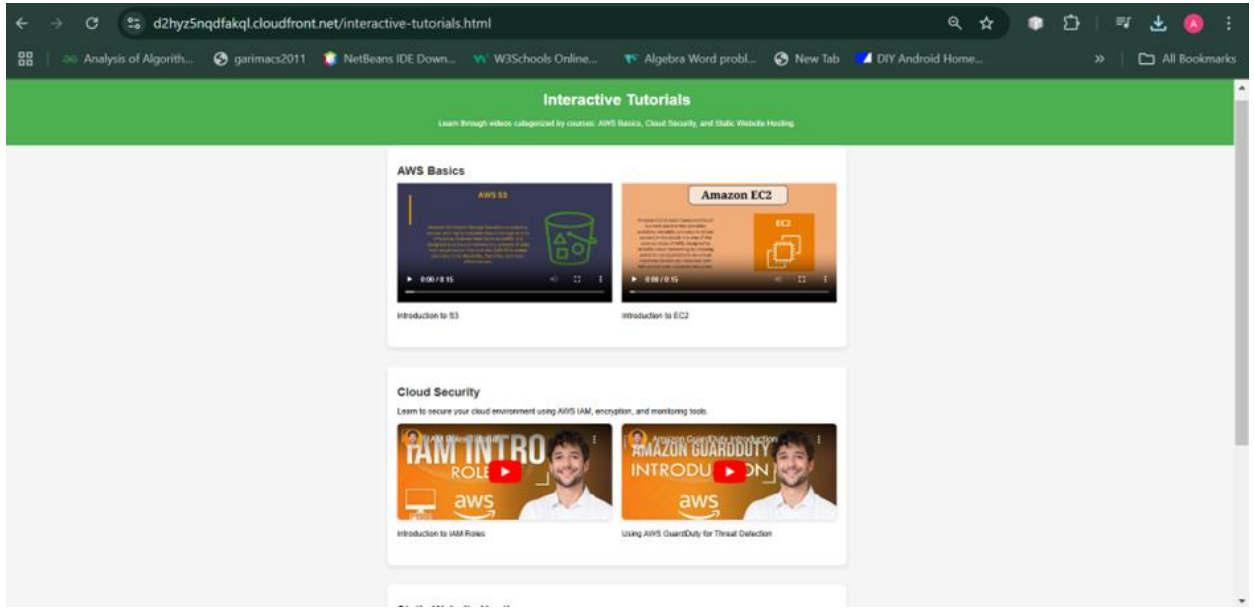
- To remove outdated or incorrect content from CloudFront's cache and replace it with the latest version from the origin server (e.g., S3, EC2).
- This is useful when content has been updated (e.g., a new version of a website or a file), but the old version is still cached at CloudFront edge locations.



Before CloudFront Invalidation

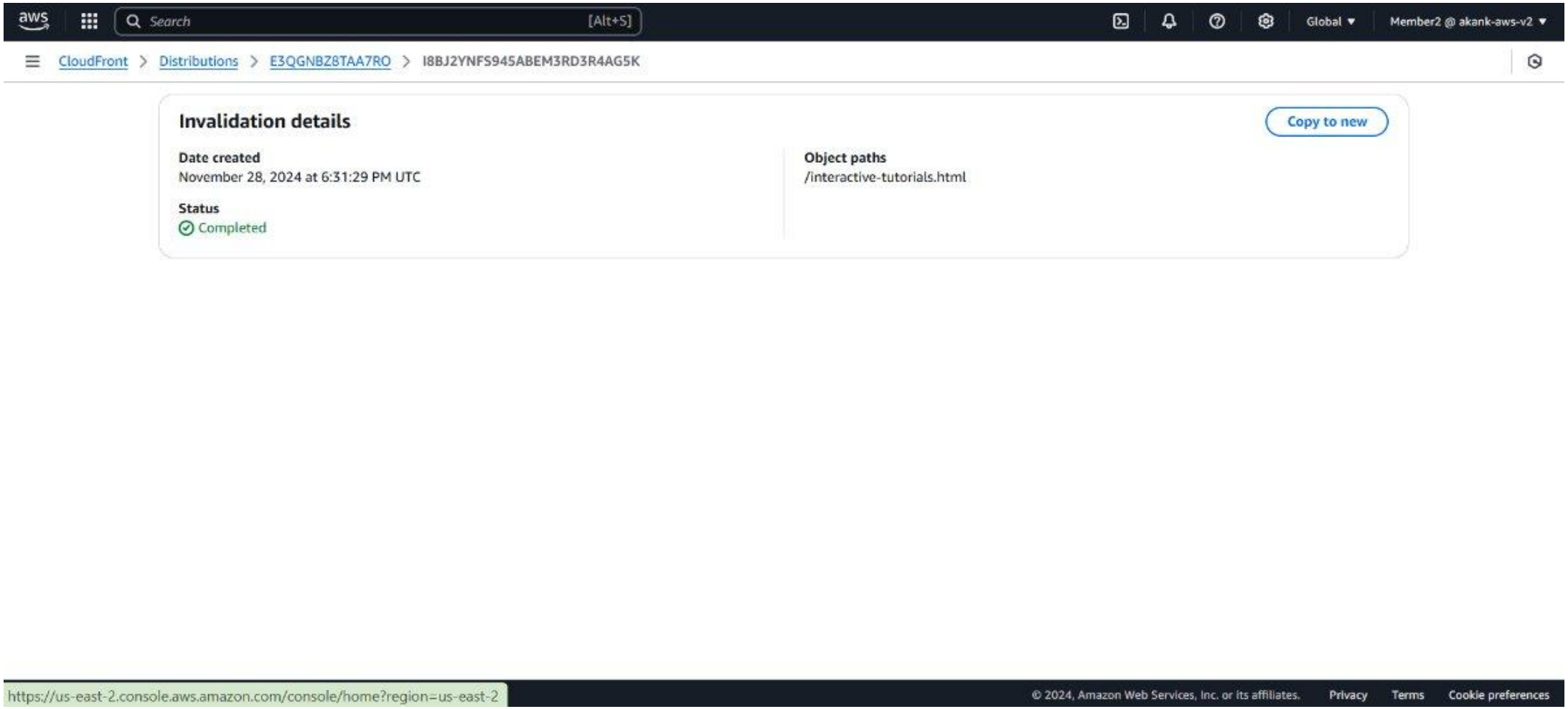


The **latest content** (e.g., updated course PDFs, images, or HTML files) is uploaded to **Amazon S3**

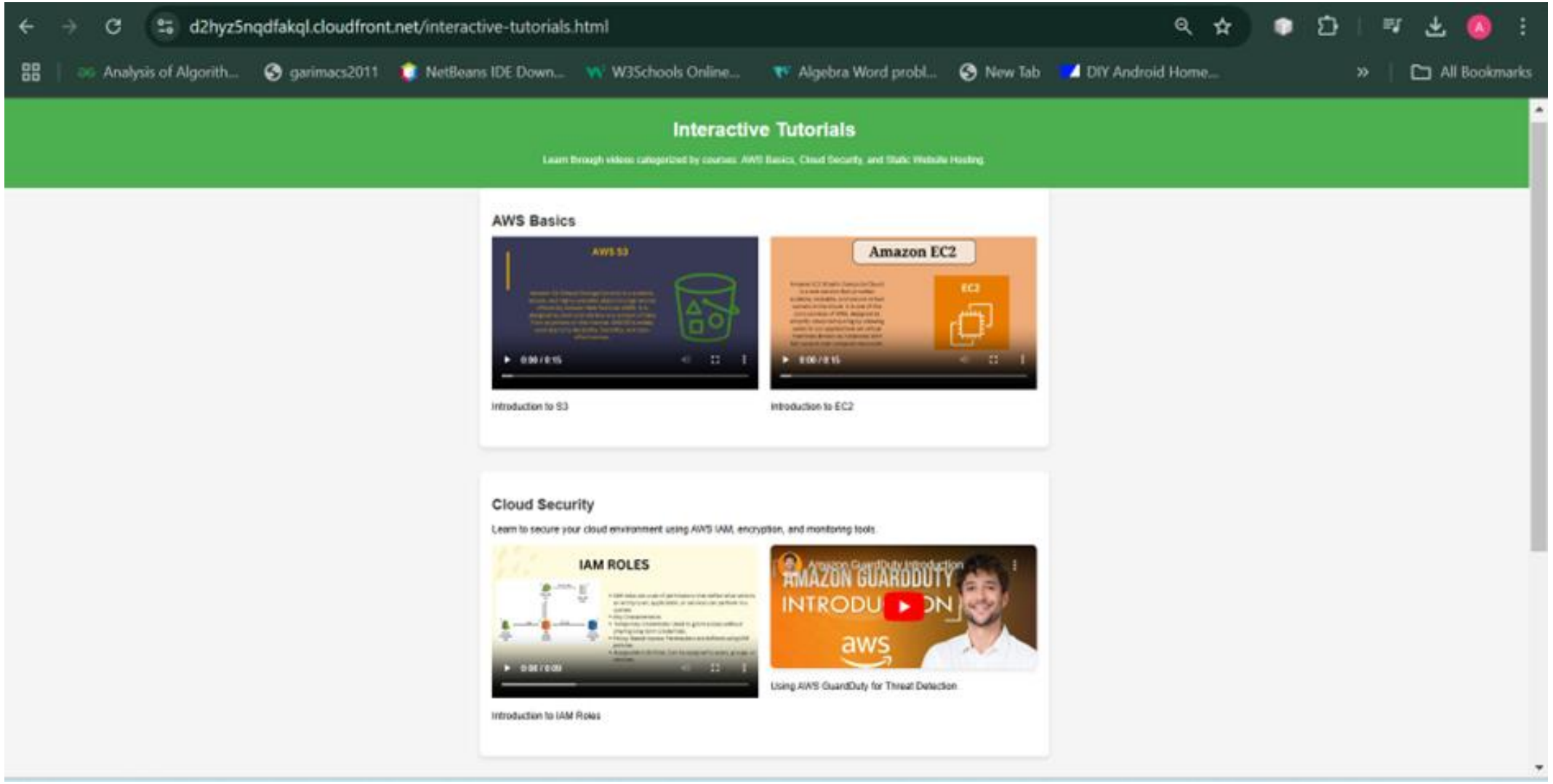


CloudFront caches the old content in edge locations, meaning users may still see outdated versions of the website or files.

Path-based Invalidation



After CloudFront Invalidation

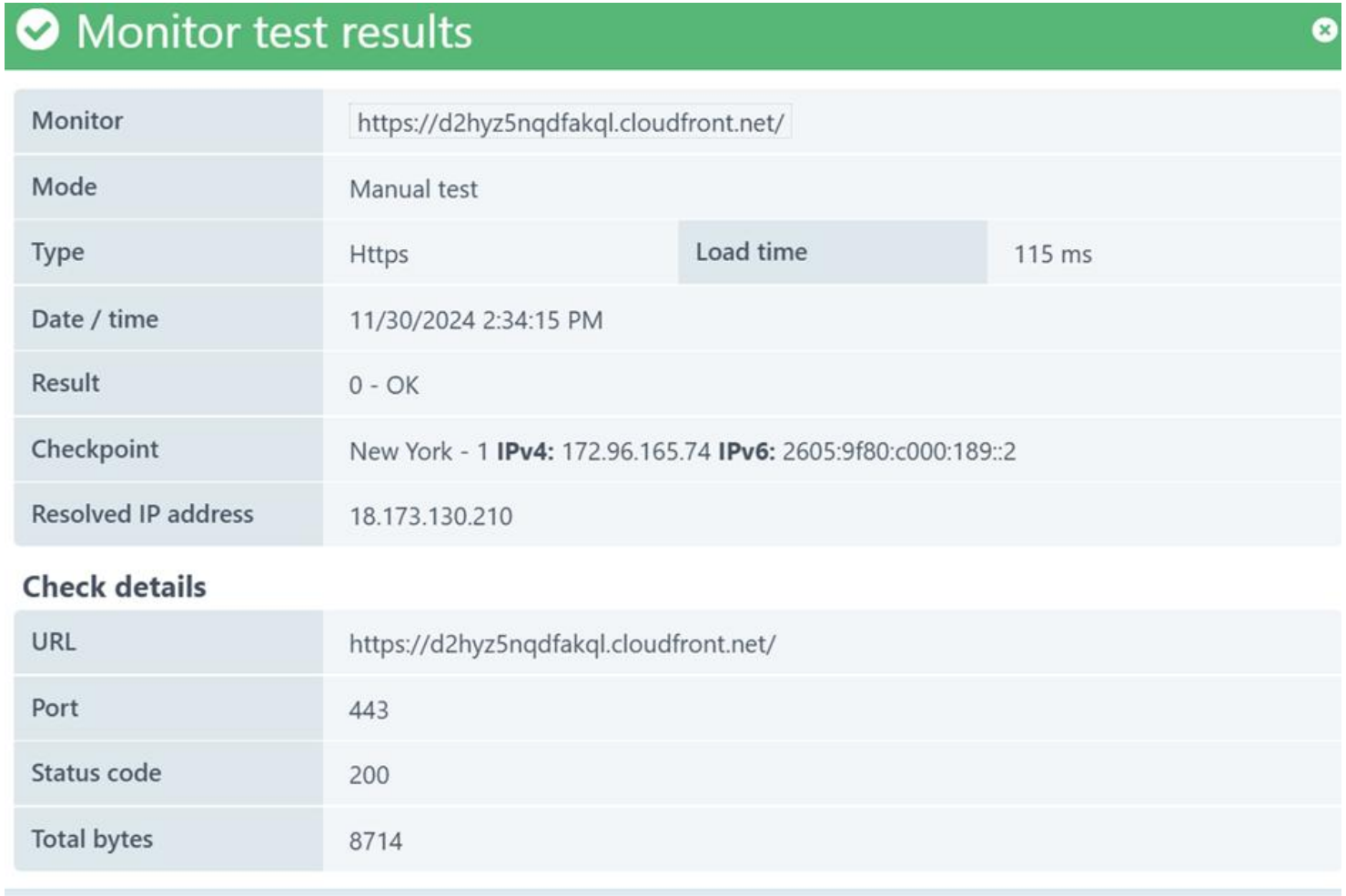


CloudFront Invalidation removes the old cached content from the edge locations.

Testing website

https://d2hyz5nqdfakql.cloudfront.net

Monitor Test Results from New York



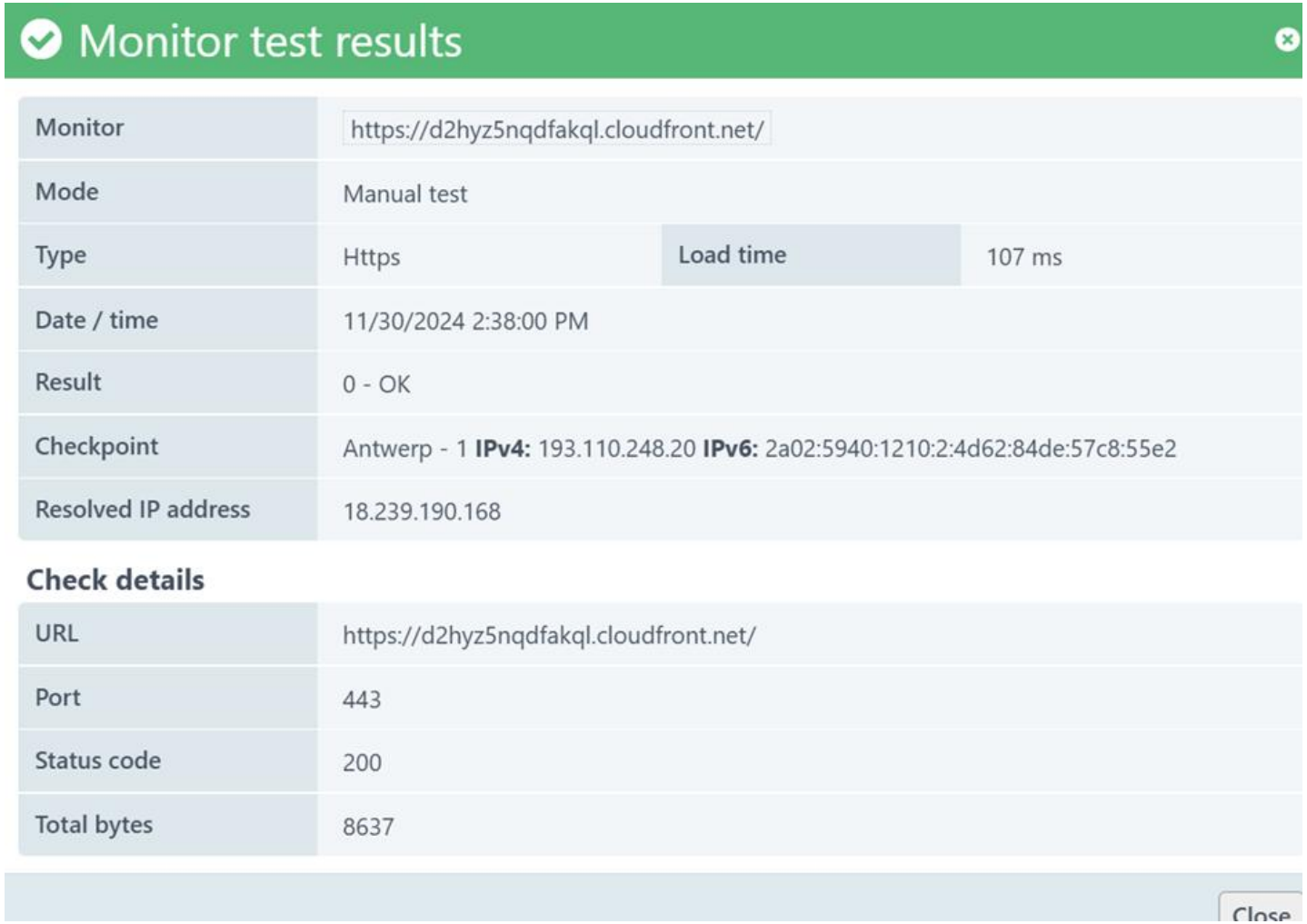
Monitor test results

Monitor	https://d2hyz5nqdfakql.cloudfront.net/		
Mode	Manual test		
Type	Https	Load time	115 ms
Date / time	11/30/2024 2:34:15 PM		
Result	0 - OK		
Checkpoint	New York - 1 **IPv4:** 172.96.165.74 **IPv6:** 2605:9f80:c000:189::2		
Resolved IP address	18.173.130.210		

Check details

URL	https://d2hyz5nqdfakql.cloudfront.net/
Port	443
Status code	200
Total bytes	8714

Monitor Test Results from Europe (Antwerp)



Monitor test results

Monitor	https://d2hyz5nqdfakql.cloudfront.net/
Mode	Manual test
Type	Https
Load time	107 ms
Date / time	11/30/2024 2:38:00 PM
Result	0 - OK
Checkpoint	Antwerp - 1 **IPv4:** 193.110.248.20 **IPv6:** 2a02:5940:1210:2:4d62:84de:57c8:55e2
Resolved IP address	18.239.190.168

Check details

URL	https://d2hyz5nqdfakql.cloudfront.net/
Port	443
Status code	200
Total bytes	8637

Close

Monitor Test Results from New Delhi (India)

Monitor test results

Monitor	https://d2hyz5nqdfakql.cloudfront.net/		
Mode	Manual test		
Type	Https	Load time	668 ms
Date / time	11/30/2024 2:39:55 PM		
Result	0 - OK		
Checkpoint	New Delhi **IPv4:** 164.52.195.81 **IPv6:** 2001:df0:411:8005::13		
Resolved IP address	54.230.104.26		

Check details

URL	https://d2hyz5nqdfakql.cloudfront.net/
Port	443
Status code	200
Total bytes	8637

Close

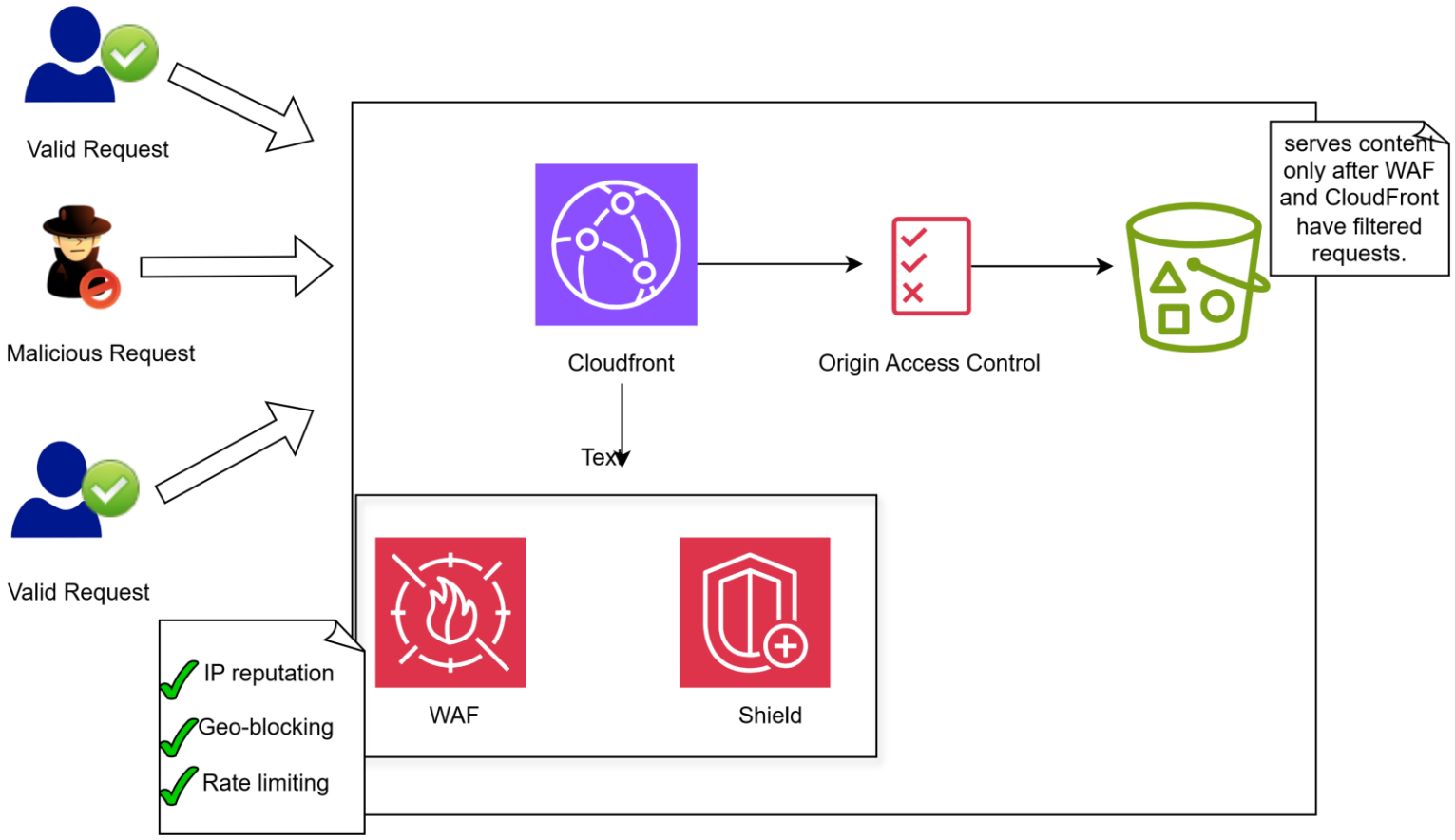
AWS WAF

AWS WAF (Web Application Firewall) is a **cloud-based firewall service** designed to protect web applications and APIs from:

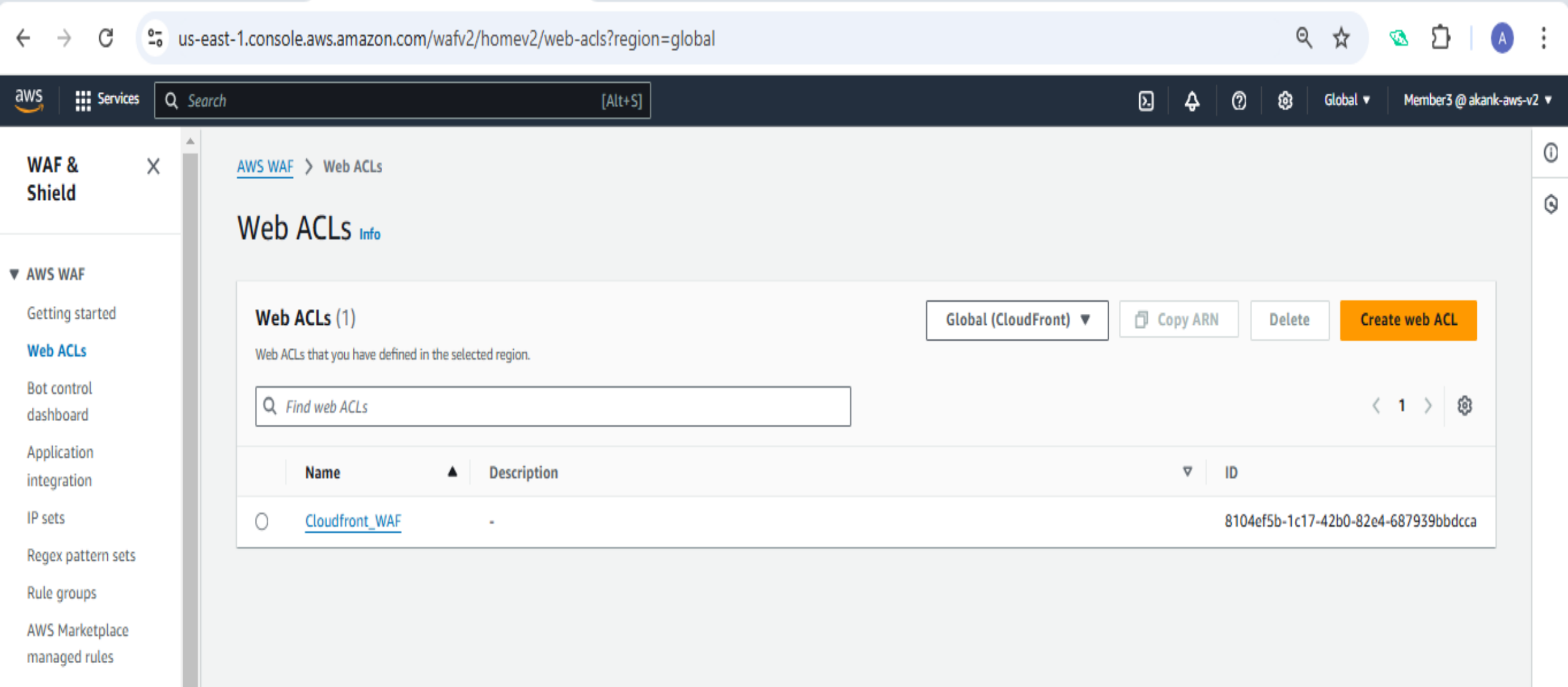
Common web exploits (e.g., **SQL injection**, **Cross-Site Scripting (XSS)**).

- AWS WAF integrates seamlessly with the following AWS services:
  - Amazon CloudFront - Protects against common web exploits
  - Application Load Balancer (ALB) - Manages bot traffic
  - Amazon API Gateway - Rate-based blocking
  - AWS App Runner - Scalable and cost-effective

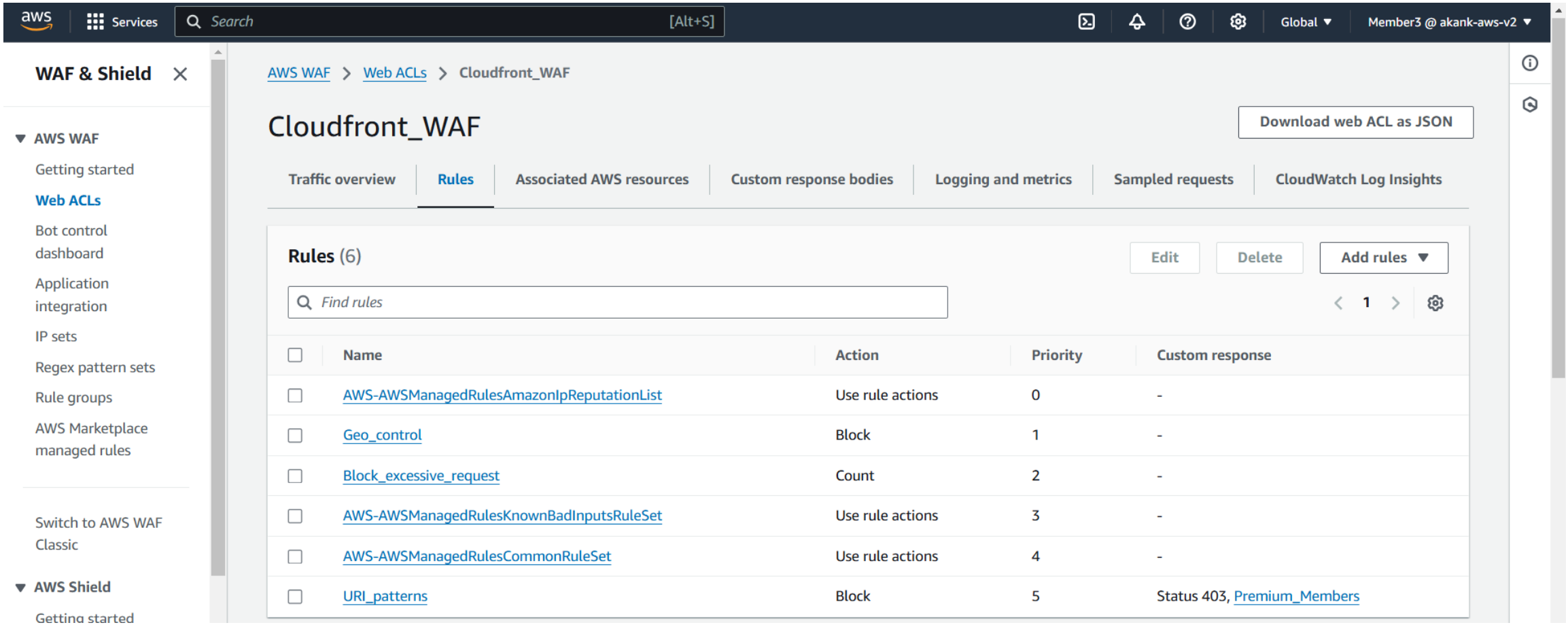
CloudFront with WAF and Shield for Content Protection



Step 1: Create a Web ACL



Step 2: Add Rules to the Web ACL



AWS Managed Rules

- **AWSManagedRulesAmazonIpReputationList** : Filters and blocks traffic originating from IP addresses with a history of malicious activity, enhancing security against known threats.
- **AWSManagedRulesCommonRuleSet**: Defends against common web vulnerabilities, including SQL injection and cross-site scripting (XSS), ensuring a secure application environment.
- **AWSManagedRulesBadInputRuleSet**: Blocks potentially harmful input data, such as malformed or malicious payloads, to protect applications from unexpected attacks.

AWS Custom rules

- **Geo_Control**: Restricts access by blocking traffic from specific geographical regions, ensuring compliance or reducing risk from certain locations.
- **Block_Excessive_Request**: Implements rate-limiting to block users generating excessive requests, protecting the application from abuse or denial-of-service (DoS) attacks.
- **URI_Patterns**: Customizable rule to allow or block access to specific URL patterns, providing fine-grained control over resource accessibility.

Priority

- AWS WAF rules are evaluated in **ascending priority order**, starting from 0.
- Rules are processed **sequentially**, and once a request matches a rule, no further lower-priority rules are evaluated.
- The Web ACL ensures protection against common web threats, **rate-limiting traffic**, and monitoring specific patterns.

- **Evaluation Process**

- **Priority 0: AWSManagedRulesAmazonIpReputationList**
  - **Function:** Checks if the user's IP is flagged as malicious.
  - **Result:**
    - If the IP is on the list, the request is blocked.
    - If not, the evaluation proceeds to the next rule.
- **Priority 1: Geo_control**
  - **Function:** Verifies if the user is from a restricted geographic region.
  - **Result:**
    - If the user is from a restricted region, the request is blocked.
    - If allowed, the evaluation proceeds to the next rule.
- **Priority 2: Block_excessive_request**
  - **Function:** Monitors the number of requests from the user's IP to detect excessive activity.
  - **Result:**
    - The request is counted but not blocked.
    - Evaluation continues to the next rule.

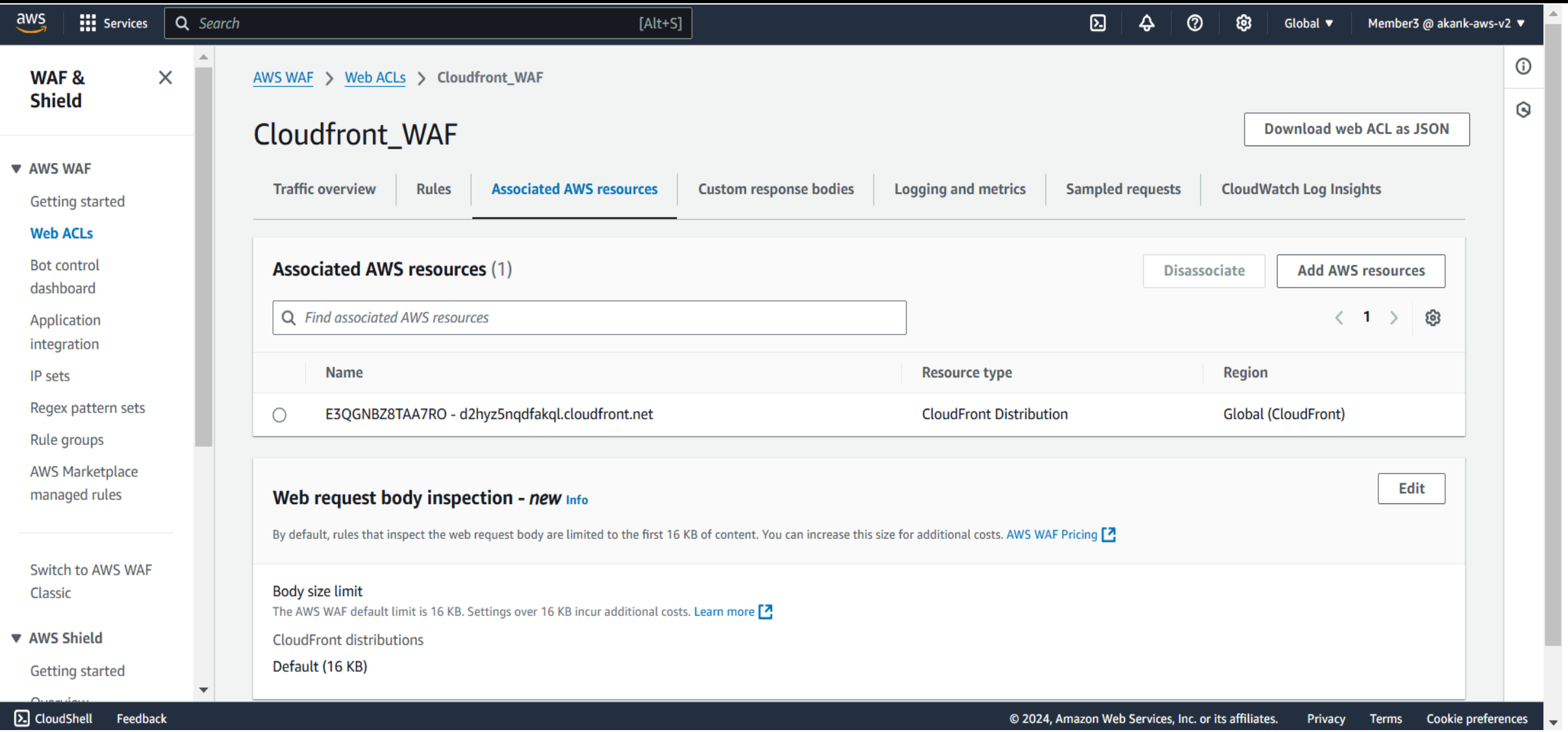
- **Evaluation Process**

- **Priority 3: AWSManagedRulesKnownBadInputsRuleSet**
  - **Function:** Checks for malicious payloads such as SQL injection or XSS attacks.
  - **Result:**
    - If a malicious payload is detected, the request is blocked.
    - Otherwise, the evaluation proceeds to the next rule.

- **Priority 4: AWSManagedRulesCommonRuleSet**
  - **Function:** Protects against general web vulnerabilities.
  - **Result:**
    - If a vulnerability is detected, the request is blocked.
    - If not, the evaluation proceeds to the next rule.

- **Priority 5: URI_patterns**
  - **Function**: Checks if the request targets restricted URL patterns (e.g., /admin).
  - **Result**:
    - If the URL matches restricted patterns, the request is blocked.
    - If not, the request is allowed.

Step 3: Associate the Web ACL with CloudFront



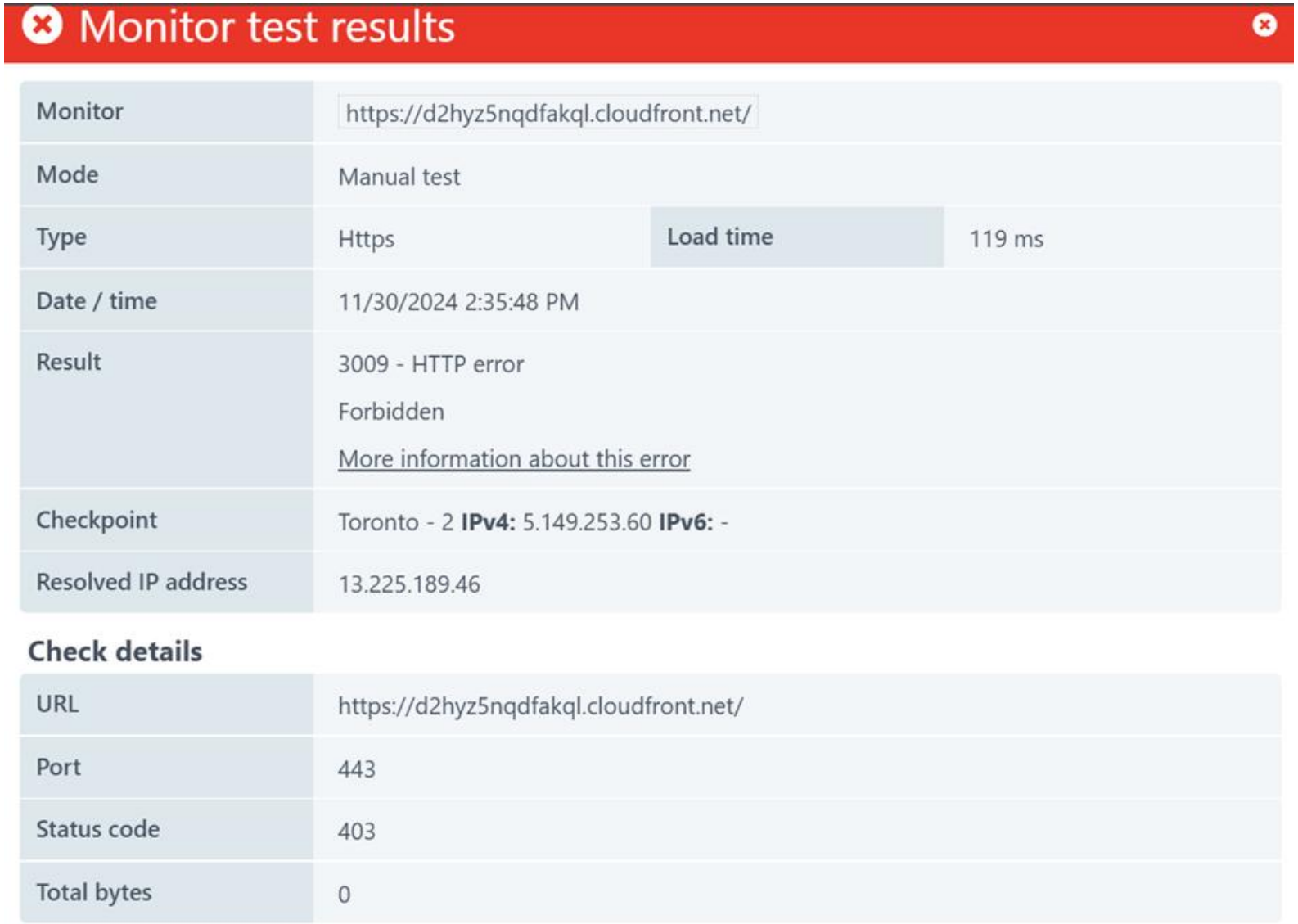
Purpose: The Web ACL (Web Access Control List) is linked to the CloudFront distribution (d2hyz5nqdfakq1.cloudfront.net) to apply the configured rules to all incoming traffic.

Key Benefit: Ensures that traffic is filtered through WAF (Web Application Firewall), providing enhanced security against malicious activity and unauthorized access.

Outcome: All requests reaching the CloudFront distribution are evaluated and processed according to the Web ACL rules, ensuring compliance with security policies.

Example – Geo control

- **Scenario**
- A user from **Country Canada** (restricted by the **Geo_control** rule) sends a request to access a URL containing a malicious payload (e.g., SQL injection).



Monitor test results

Monitor	https://d2hyz5nqdfakql.cloudfront.net/		
Mode	Manual test		
Type	Https	Load time	119 ms
Date / time	11/30/2024 2:35:48 PM		
Result	3009 - HTTP error Forbidden More information about this error		
Checkpoint	Toronto - 2 **IPv4:** 5.149.253.60 **IPv6:** -		
Resolved IP address	13.225.189.46		

Check details

URL	https://d2hyz5nqdfakql.cloudfront.net/
Port	443
Status code	403
Total bytes	0

Page content

Response headers

```
X-Cache: Error from cloudfront
Via: 1.1 1df98836515ac348d12c9af86e1ecc48.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C1
X-Amz-Cf-Id: mVPRFrGLO7rBpK8roAuNAWqPI-rrpMdOuDCz50sh4BndInHzKP3JSA==
```

HTML result

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<HTML><HEAD><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<TITLE>ERROR: The request could not be satisfied</TITLE>
</HEAD><BODY>
<H1>403 ERROR</H1>
<H2>The request could not be satisfied.</H2>
<HR noshade size="1px">
Request blocked.
We can't connect to the server for this app or website at this time. There might be too much traffic or a cor
<BR clear="all">
If you provide content to customers through CloudFront, you can find steps to troubleshoot and help prevent t
<BR clear="all">
<HR noshade size="1px">
<PRE>
Generated by cloudfront (CloudFront)
Request ID: mVPRFrGLO7rBpK8roAuNAWqPI-rrpMdOuDCz50sh4BndInHzKP3JSA==
</PRE>
```

AWS Shield

Purpose: Provides protection against **Distributed Denial of Service (DDoS)** attacks.
Versions:

- **AWS Shield Standard:** Automatically enabled for all AWS customers, offering basic DDoS protection.
- **AWS Shield Advanced:** Offers enhanced DDoS protection, detailed monitoring, and response capabilities for a subscription fee.

Why Use AWS Shield?

- **Protects against:**
  - **Volumetric DDoS attacks:** Flood of requests aimed at exhausting network capacity.
  - **Application-layer attacks:** Target services such as **CloudFront**, **ALB**, or **EC2**.
- **Key Benefits:**
  - Reduces downtime and ensures application availability.
  - Integrated with **CloudFront** to provide automated, edge-level mitigation for improved performance and security.

AWS logging and monitoring

What is ?

AWS logging and monitoring utilize services like **CloudWatch**, **CloudTrail**, **S3 Access Logs**, and **WAF Logs** to track resource activity, improve performance, and ensure system security.

Why needed ?

- Enhanced Security: Identify risks and maintain compliance with detailed logs.
- Optimized Performance: Detect inefficiencies and streamline resource usage.
- Operational Transparency: Monitor usage patterns to manage costs effectively.
- Quick Incident Resolution: Use real-time alerts and log analysis to address issues rapidly.

Example Scenario:

- Investigate abnormal S3 access, audit actions with CloudTrail, and leverage CloudWatch metrics to track system health.

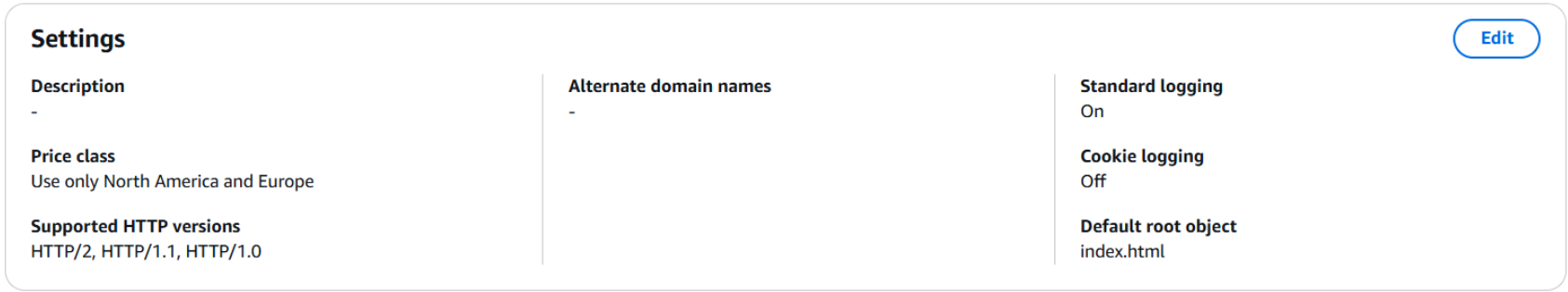
Enable CloudFront Access Logging

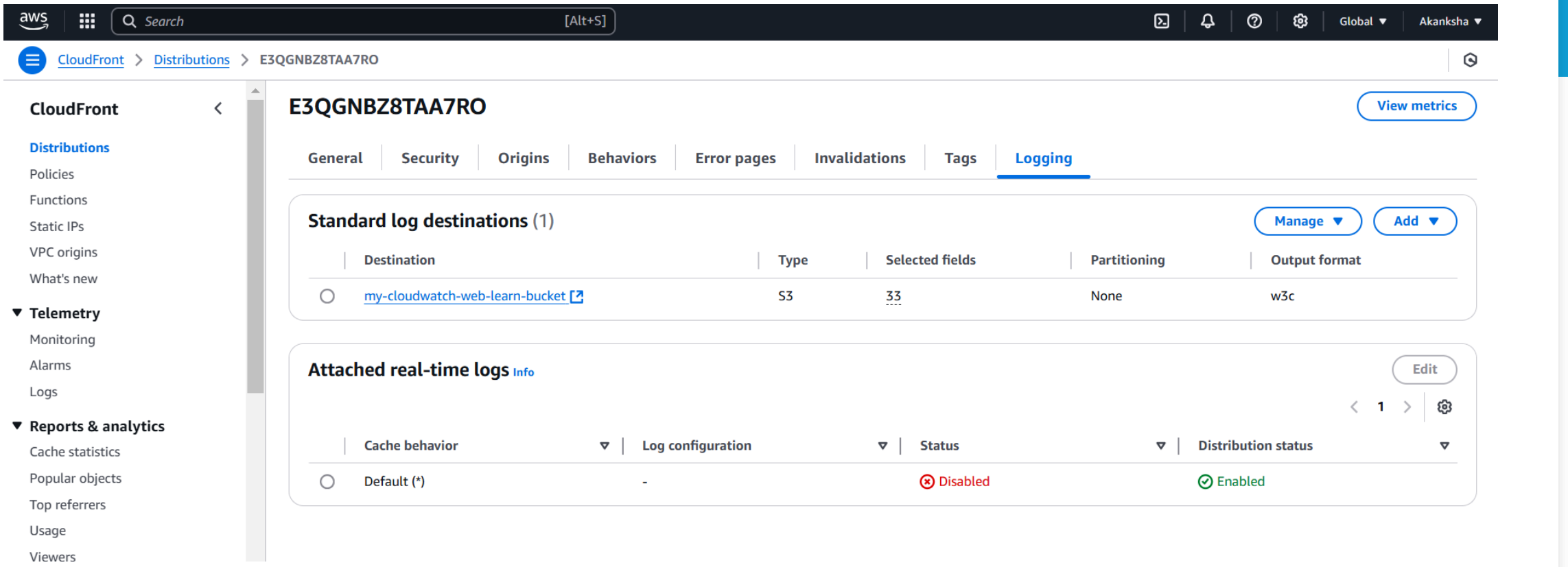
Why Enable Access Logging?

- Performance Monitoring
- Security Analysis
- Audit and Compliance
- Troubleshooting

Steps to Enable Logging:

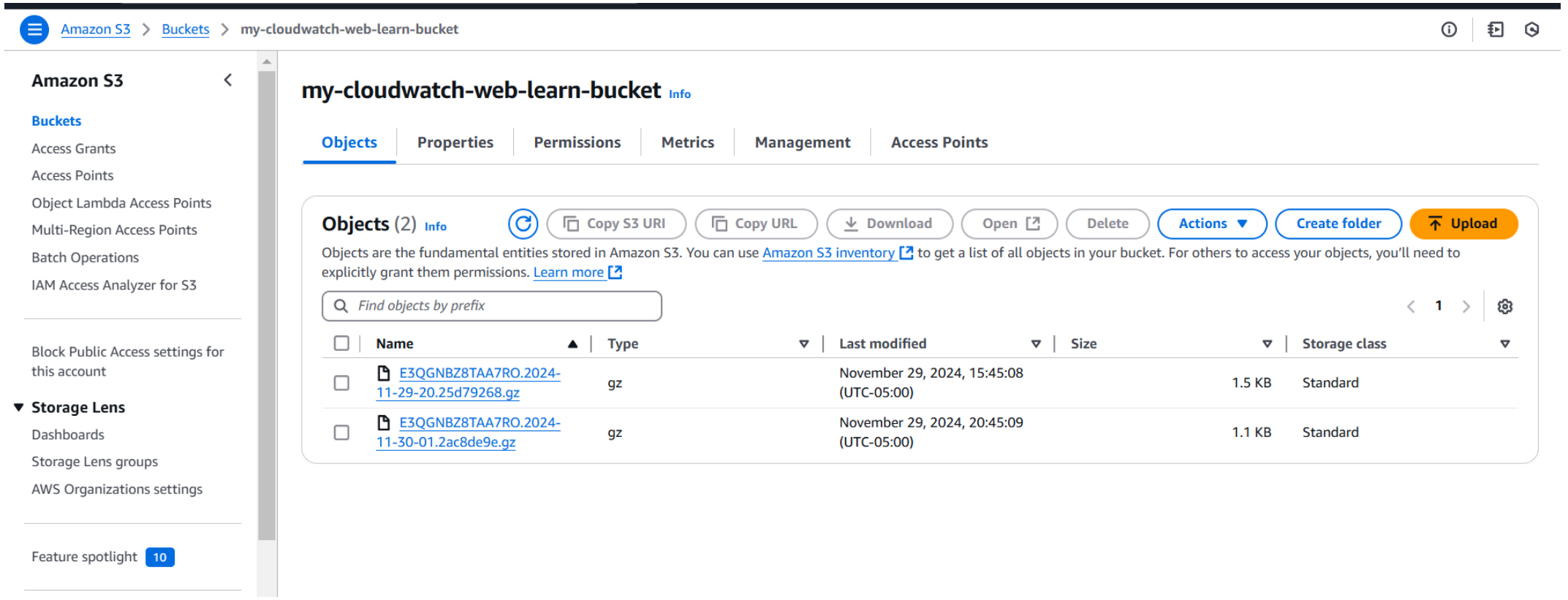
- Access CloudFront Settings
- Enable Standard Logging





Specify S3 Bucket:

- The S3 bucket stores CloudFront logs, capturing user request details to analyze traffic, monitor performance, and troubleshoot issues.
- **How to Configure?**
- **Key Benefit**
  - Logs provide actionable insights into traffic patterns and help improve system performance and security.



Logs stored in S3 bucket

Key Highlights

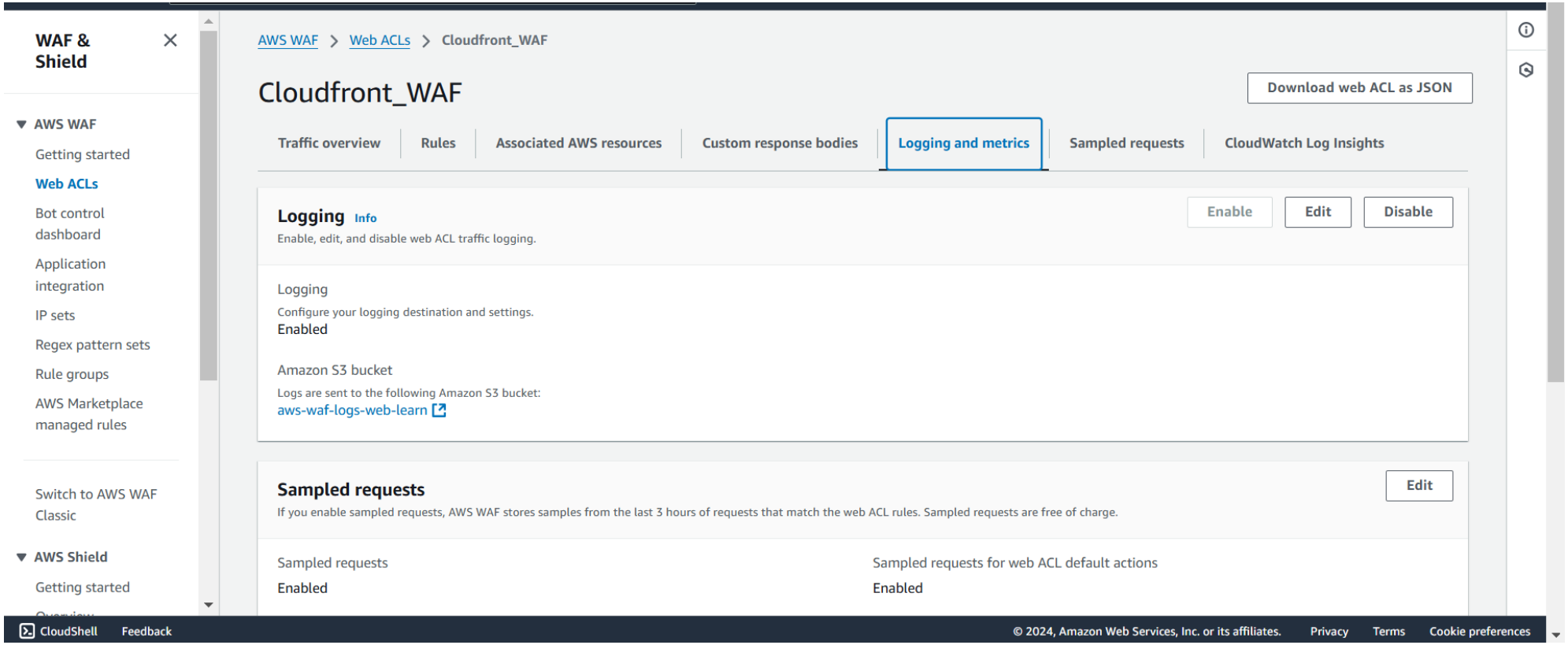
- Storage Format
- Log Information
- Ease of Access

Purpose

- Stored logs help track usage patterns, identify unusual activities, and optimize performance.

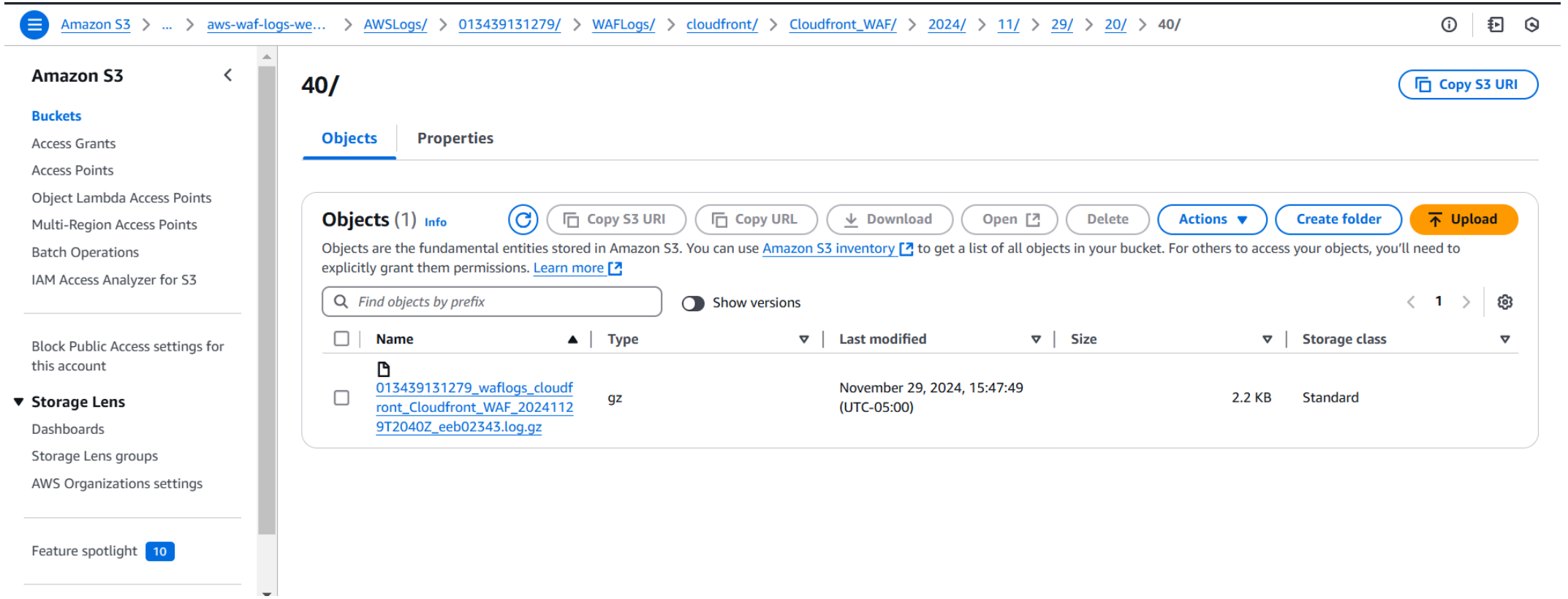
CloudFront Access Logs Capture

- **Date and Time**: When the request was processed.
- **Edge Location**: The CloudFront server serving the request.
- **Client IP**: IP address of the requester.
- **HTTP Method**: Type of request (e.g., GET, POST).
- **URL**: The requested resource (e.g., /index.html).
- **HTTP Status Code**: Response status (e.g., 200, 404).
- **Bytes Sent**: Size of the response in bytes.
- **Cache Details**: Whether it was a **Hit**, **Miss**, or **Error**.
- **User-Agent**: Device or browser making the request.
- **Referrer**: Page that referred the request (if available).



Enable WAF Logging

- What is WAF Logging?
- How to Enable WAF Logging?



S3 bucket to store WAF logs

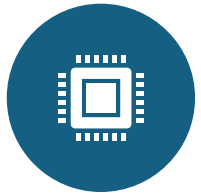
The S3 bucket (aws-waf-logs-web-learn) is used to store logs generated by AWS WAF ensuring secure storage for analysis and monitoring purposes.

Highlights

- Compressed Format
- Log Details
- Easy Access

What is Cloud Watch?

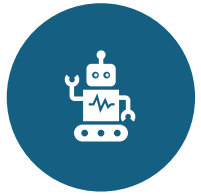
CloudWatch is a powerful monitoring and observability service provided by AWS. It enables organizations to gain real-time insights into the performance, availability, and health of their AWS resources and applications.



Monitoring the performance and availability of web applications.

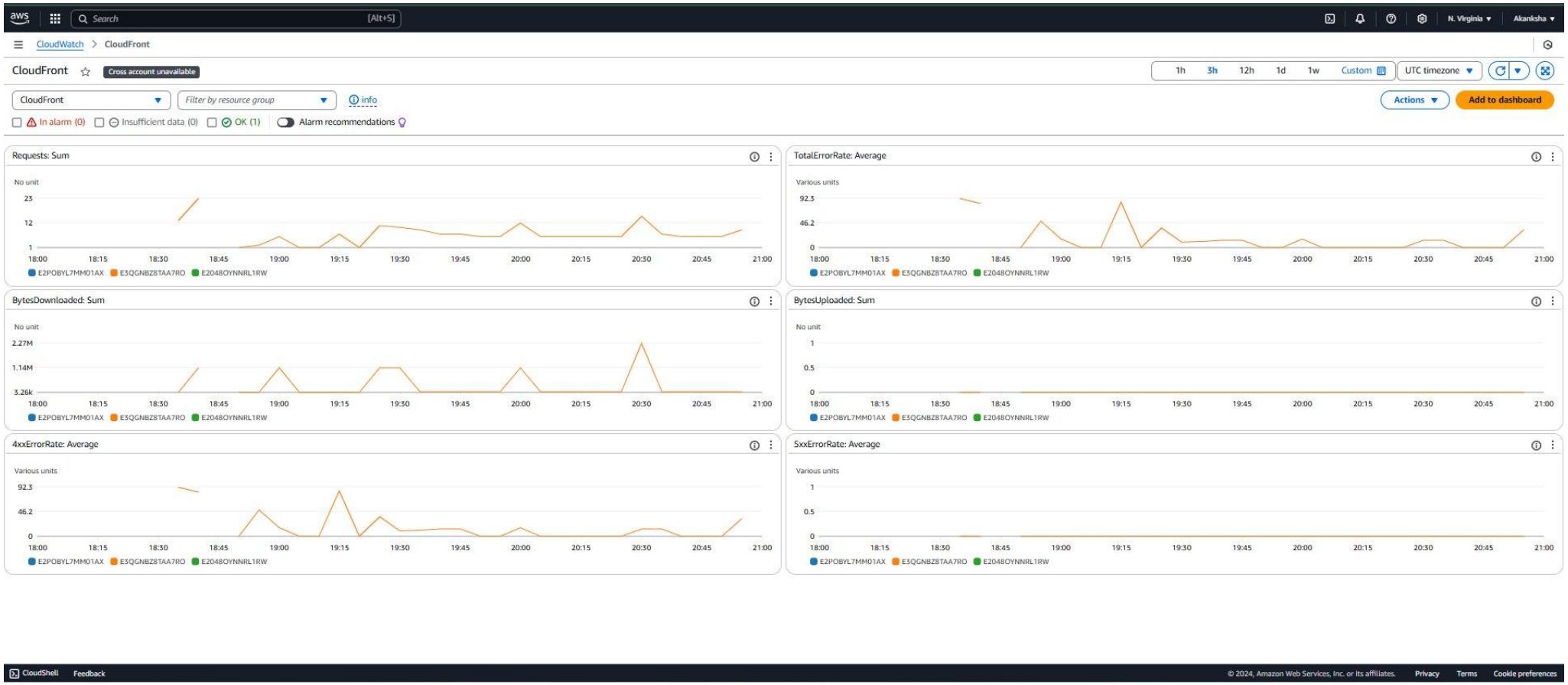
Troubleshooting application failures by analyzing logs and metrics.

With Amazon CloudWatch, we can ensure that our applications and infrastructure run smoothly while enabling proactive maintenance to avoid costly downtime. It’s an essential tool for anyone building on the AWS cloud.

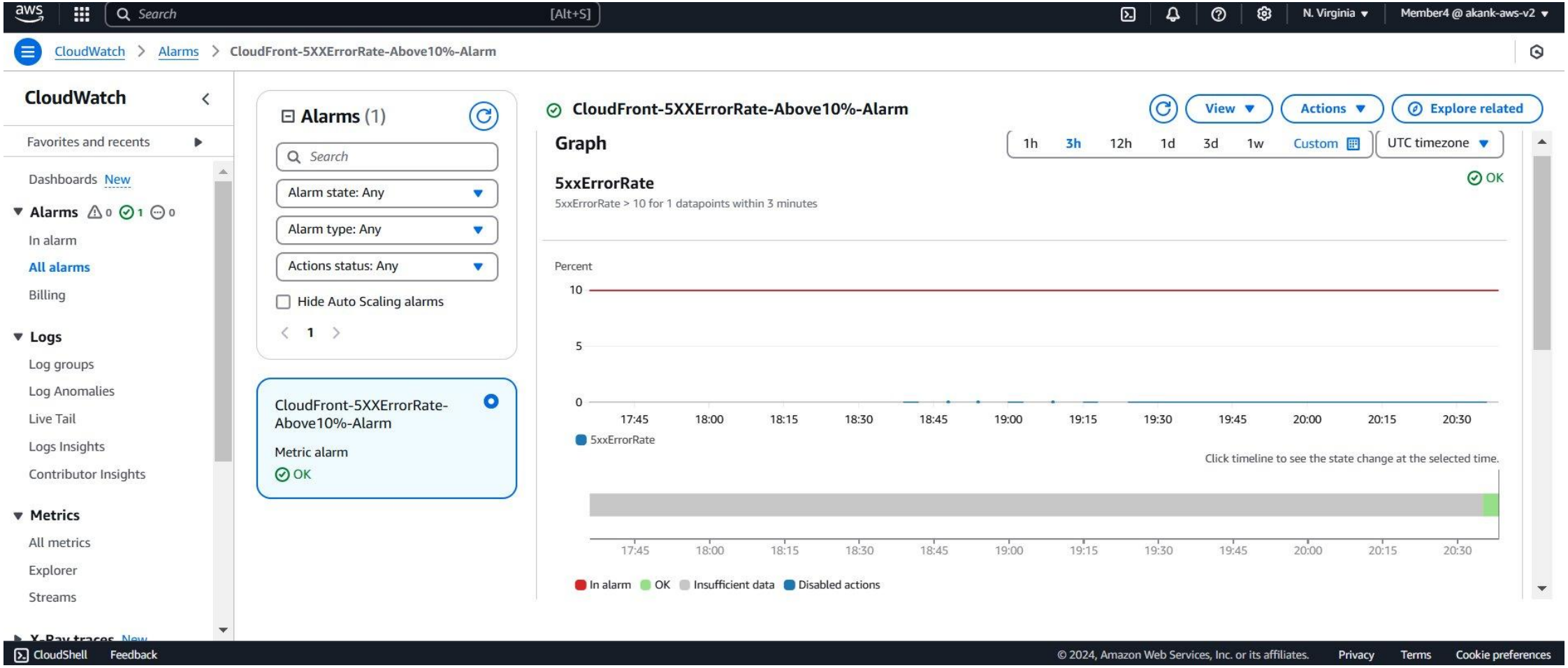


Automating scaling decisions based on real-time performance data.

Ensuring compliance by auditing system changes and activities.

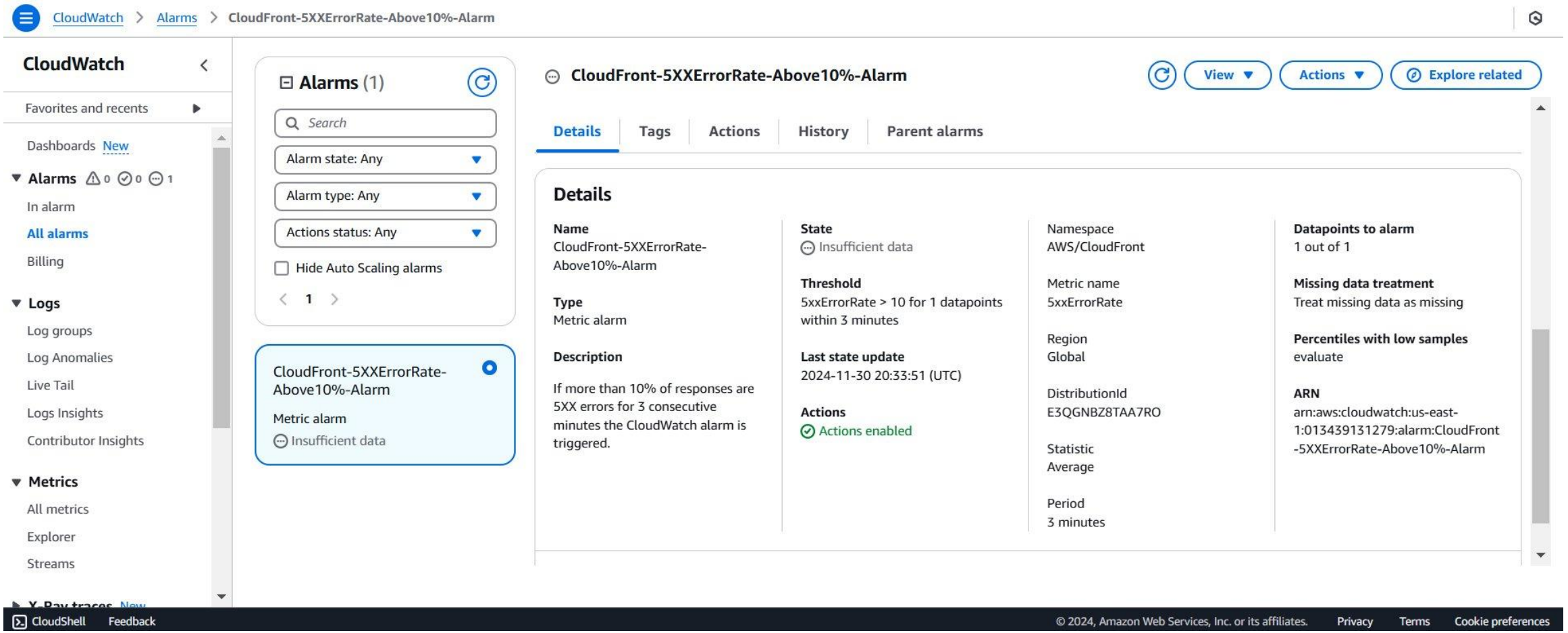


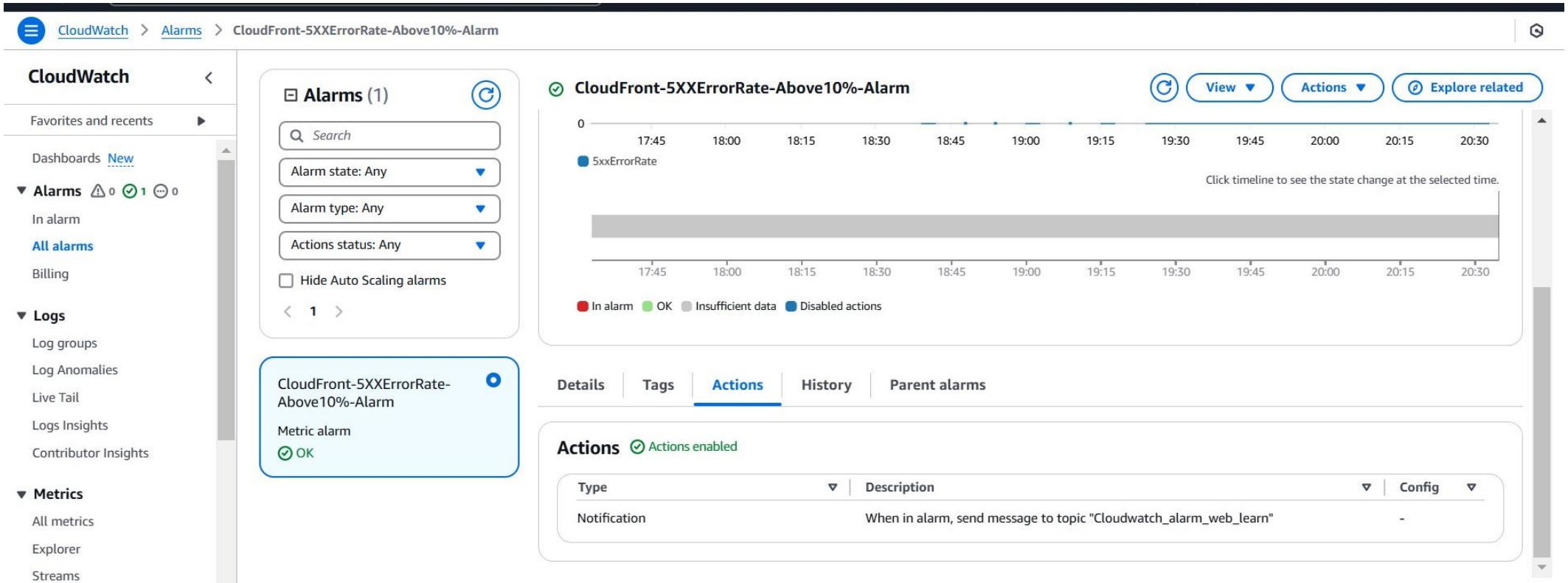
- CloudFront automatically integrates with CloudWatch.
- View metrics such as cache hit rates, error rates, and traffic patterns in CloudFront Monitoring.



Cloud watch Alarms

Configuration





Notification Settings

- An alert is triggered when the threshold is breached (e.g., high error rates).
- Notifications are sent to your team via **SNS**, enabling quick investigation and mitigation.

Amazon SNS

What is SNS?

Amazon Simple Notification Service (SNS) is a fully managed messaging service provided by AWS.

It enables seamless communication between distributed systems, microservices, and end-users by sending notifications or messages to multiple subscribers or endpoints.

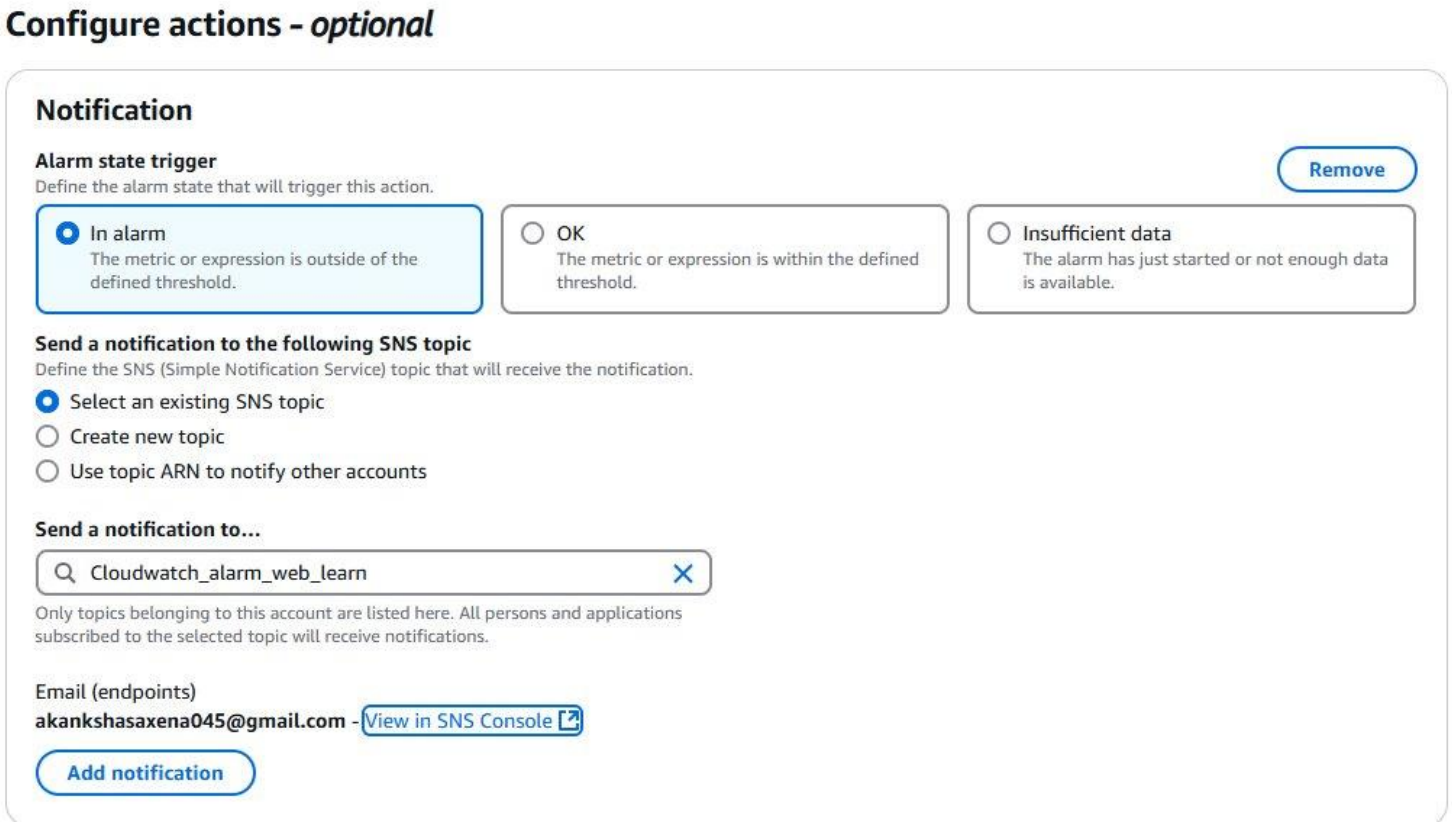
SNS is designed to deliver messages efficiently and reliably across a range of platforms, making it an integral part of modern application architectures.

Sending promotional messages or alerts to customers.

Triggering automated workflows or processes through Lambda.

Delivering system health notifications to DevOps teams.

SNS TOPIC


Configure actions - optional
Notification
Alarm state trigger
Define the alarm state that will trigger this action.
Remove
In alarm
The metric or expression is outside of the defined threshold.
OK
The metric or expression is within the defined threshold.
Insufficient data
The alarm has just started or not enough data is available.
Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.
Select an existing SNS topic
Create new topic
Use topic ARN to notify other accounts
Send a notification to...
Cloudwatch_alarm_web_learn
Only topics belonging to this account are listed here. All persons and applications subscribed to the selected topic will receive notifications.
Email (endpoints)
akankshasaxena045@gmail.com - View in SNS Console
Add notification

Future Scope

1.Adding a Custom Domain with Route 53

- As part of expanding the "Smart Learning Zone," integrate a custom domain name using Amazon Route 53 to enhance the platform’s branding and user experience.

2. Add Dynamic Features

- **User Authentication & Login**:
- Integrate **Amazon Cognito** to enable secure user authentication and management.
- Allow users to create accounts, log in, and save course progress.
- **Dynamic Content Delivery**:
- Use **AWS Lambda** and **API Gateway** to serve personalized content such as progress tracking, recommendations, or user-specific dashboards.

3.Advanced Analytics

- **User Behavior Insights**:
- Use **Amazon QuickSight** to create dashboards showing user behavior, such as the most downloaded resources or frequently accessed tutorials.
- **AI-Powered Recommendations**:
- Leverage **Amazon Personalize** to suggest courses, tutorials, or materials tailored to individual users' interests and history.

Resources

- https://aws.amazon.com/pm/serv-s3/?gclid=CjwKCAiA0rW6BhAcEiwAQH28ImqupeKYP7vCkWPNT5vNyvPkZdKSOA0eOvhexKKvGT6AXnVziRtncRoCxjgQAvD_BwE&trk=20e04791-939c-4db9-8964-ee54c41bc6ad&sc_channel=ps&ef_id=CjwKCAiA0rW6BhAcEiwAQH28ImqupeKYP7vCkWPNT5vNyvPkZdKSOA0eOvhexKKvGT6AXnVziRtncRoCxjgQAvD_BwE:G:s&s_kwcid=AL!4422!3!651751060977!p!!g!!s3!19852662362!145019251617
- https://docs.aws.amazon.com/cloudfront/
- https://docs.aws.amazon.com/sns/latest/dg/welcome.html
- https://aws.amazon.com/waf/
- https://aws.amazon.com/cloudwatch/
- https://www.uptrends.com/lp/website-monitoring?utm_source=google_ads&utm_medium=cpc&utm_term=brandname&utm_campaign=US-HGK-X&gad_source=1&gclid=EAIaIQobChMIyPzx74OKigMV9UNHAR2-WBVVEAAYASAAEgKBh_D_BwE
- https://app.diagrams.net/
- https://aws.amazon.com/architecture/icons/
- https://www.simplilearn.com/tutorials/aws-tutorial/aws-cloudfront
- https://docs.aws.amazon.com/prescriptive-guidance/latest/logging-monitoring-for-application-owners/aws-services-logging-monitoring.html

THANK YOU