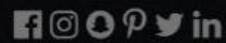


# Smart Learning Zone

Master AWS for Cloud-Based Learning Solutions

Learn more and start today



# 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.

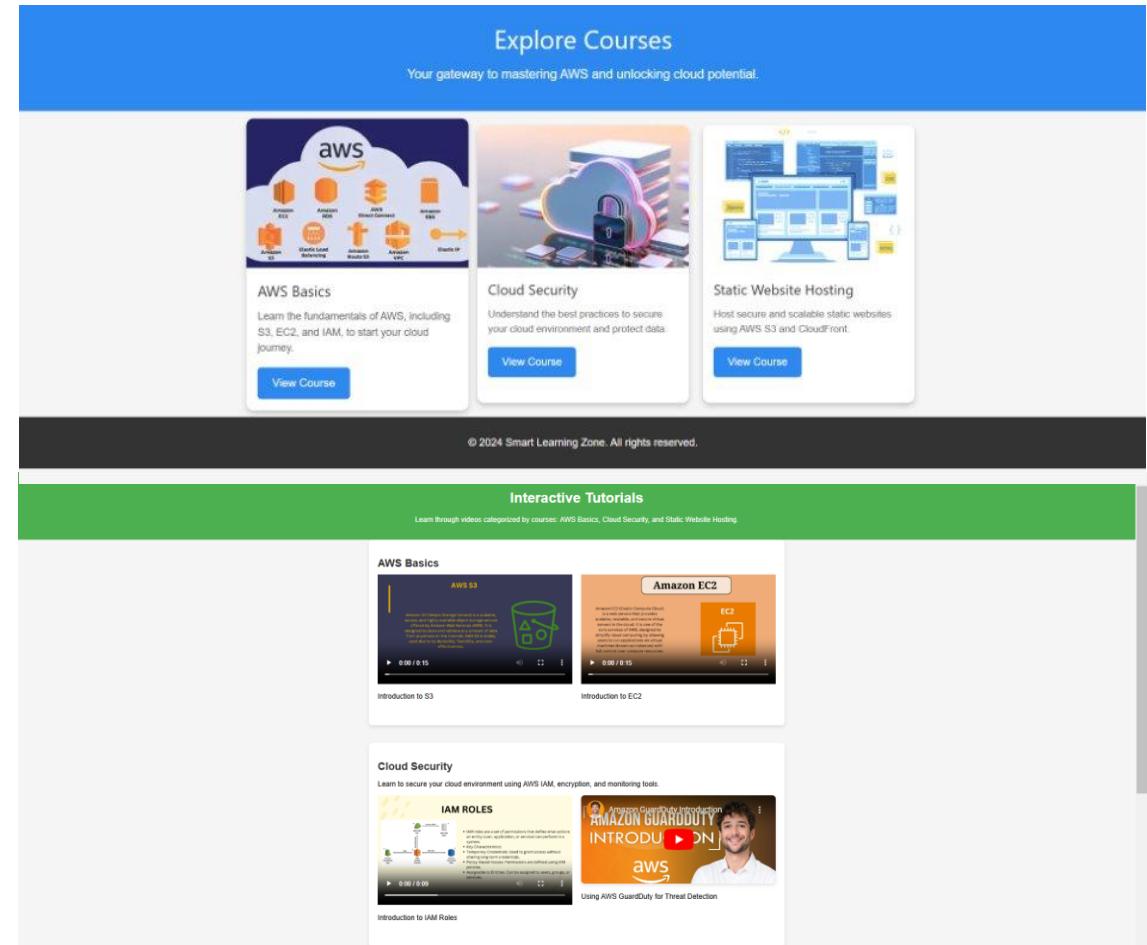
- Core Features:**

- Hosts **static web pages** for course content and tutorials.

Offers **downloadable resources** such as PDFs, images, and cheatsheets stored securely in S3.

- Target Audience:**

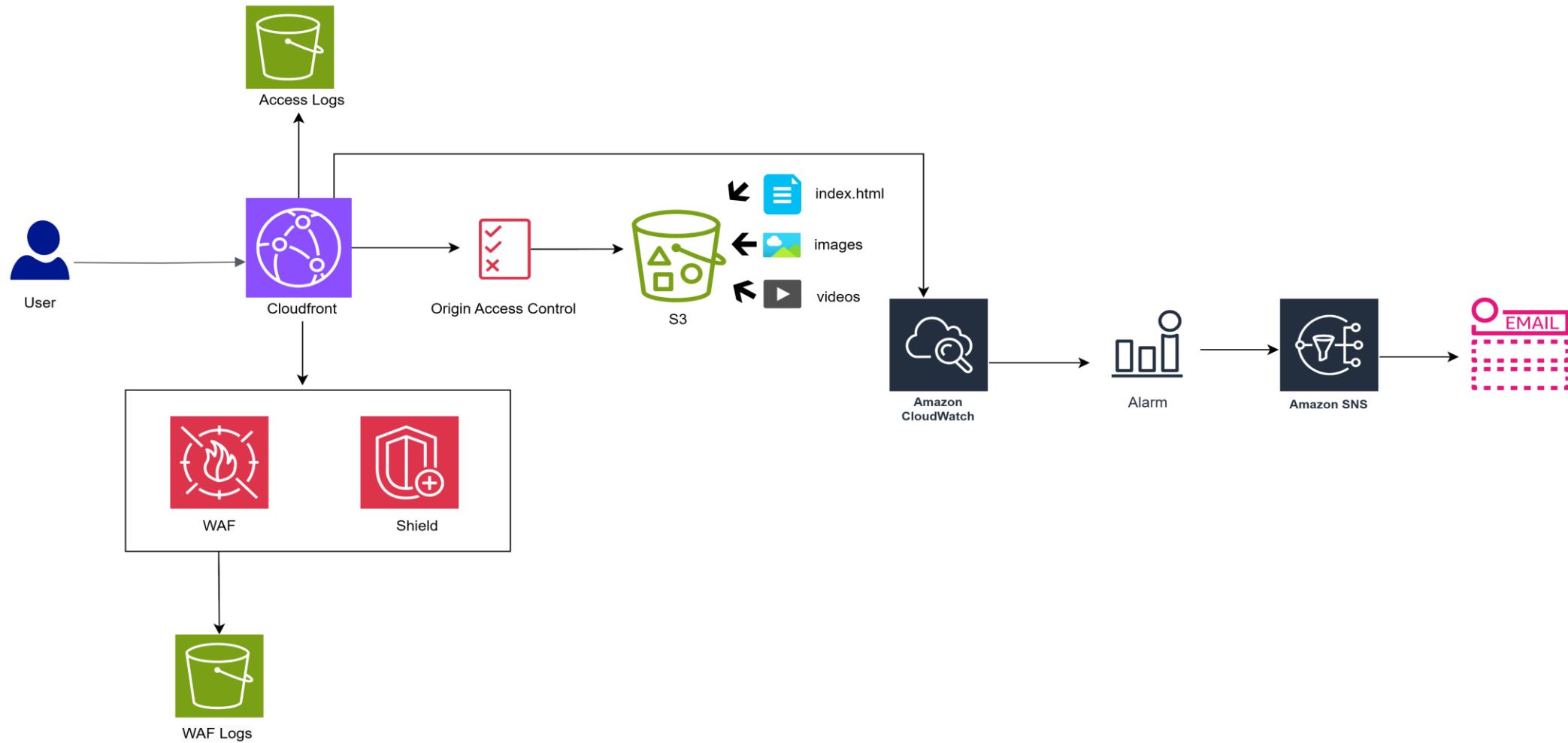
Individuals or organizations looking to learn about AWS services and explore real-world applications of cloud technologies.



# 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

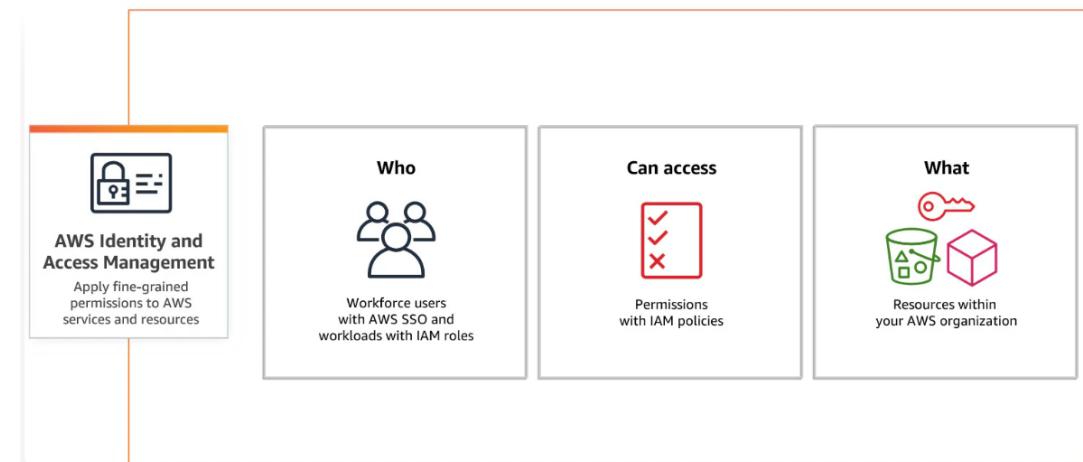
IAM (Identity and Access Management) is a feature of AWS that enables secure control of access to AWS resources.

### 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**

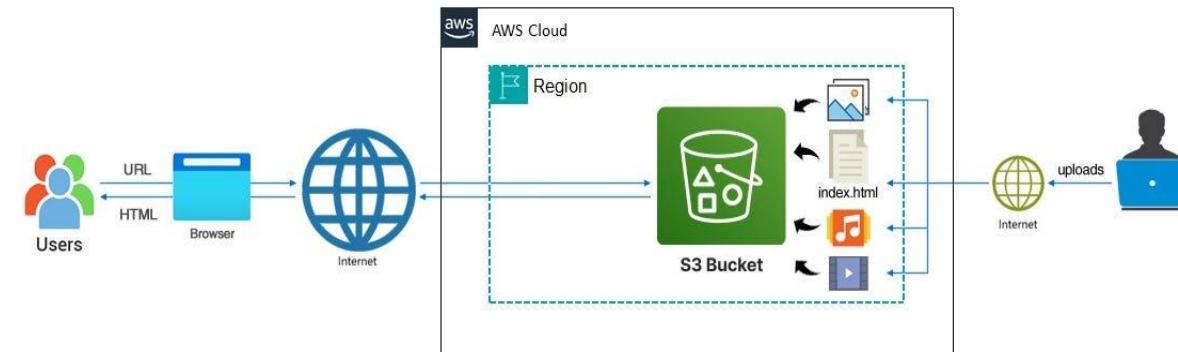
**Step 3: Static Website Hosting Configuration**

**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.

The screenshot shows the Amazon S3 General purpose buckets list. The left sidebar includes links for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens (Dashboards, Storage Lens groups, AWS Organizations settings), Feature spotlight (10), and AWS Marketplace for S3. The main area displays four buckets in a table format:

Name	AWS Region	IAM Access Analyzer	Creation date
<a href="#">aws-cloudtrail-logs-013439131279-c4f58db3</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	November 21, 2024, 15:04:57 (UTC-05:00)
<a href="#">aws-waf-logs-web-learn</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	November 29, 2024, 12:27:54 (UTC-05:00)
<a href="#">my-cloudwatch-web-learn-bucket</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	November 29, 2024, 08:36:15 (UTC-05:00)
<a href="#">my-static-website-web-learn</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	26, 2024, 20:17:30 (UTC-05:00)

A red box highlights the last row, which corresponds to the bullet point in the text above. The top navigation bar includes the AWS logo, search bar, and various icons like CloudShell, Feedback, and Member1 @ akank-aws-v2.

# 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.

The screenshot shows the AWS S3 Bucket Properties page for the bucket 'my-static-website-web-learn'. The 'Properties' tab is selected. In the 'Bucket overview' section, the 'AWS Region' is listed as 'US East (N. Virginia) us-east-1'. The 'Amazon Resource Name (ARN)' is shown as 'arn:aws:s3:::my-static-website-web-learn'. The 'Creation date' is 'November 26, 2024, 20:17:30 (UTC-05:00)'. In the 'Bucket Versioning' section, it is indicated that 'Bucket Versioning' is 'Enabled'. A red box highlights this 'Enabled' status. An 'Edit' button is located in the bottom right corner of this section. On the left sidebar, under 'Buckets', 'Access Grants' and 'Access Points' are listed. Under 'Storage Lens', 'Dashboards' is listed. A large circular callout points to the 'Bucket Versioning' section.

# 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>.

## Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

[Edit](#)

 We recommend using AWS Amplify Hosting for static website hosting

[Create Amplify app](#)

Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

### S3 static website hosting

Enabled

### Hosting type

Bucket hosting

### Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

 <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.

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with navigation links like 'Buckets', 'Access Grants', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Block Public Access settings for this account', 'Storage Lens' (with 'Dashboards' and 'Storage Lens groups'), 'AWS Organizations settings', 'Feature spotlight' (with a '10' badge), and 'AWS Marketplace for S3'. The main area is titled 'Objects (9) Info' and contains a table of files. The table has columns for Name, Type, Last modified, Size, and Storage class. The objects listed are:

Name	Type	Last modified	Size	Storage class
assets/	Folder	-	-	-
aws-basics.html	html	November 27, 2024, 12:07:43 (UTC-05:00)	4.1 KB	Standard
cloud-security.html	html	November 27, 2024, 12:07:43 (UTC-05:00)	4.2 KB	Standard
downloadable-resources.html	html	November 27, 2024, 12:17:03 (UTC-05:00)	4.3 KB	Standard
EC2.mp4	mp4	November 27, 2024, 14:03:13 (UTC-05:00)	2.3 MB	Standard
explore-courses.html	html	November 27, 2024, 12:17:03 (UTC-05:00)	4.1 KB	Standard
index.html	html	November 27, 2024, 10:29:11 (UTC-05:00)	7.9 KB	Standard
interactive-tutorials.html	html	November 28, 2024, 13:21:25 (UTC-05:00)	4.5 KB	Standard
static-website-hosting.html	html	November 27, 2024, 12:07:44 (UTC-05:00)	4.2 KB	Standard

# 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.

The screenshot shows the 'Edit Block public access (bucket settings)' page in the Amazon S3 console. The left sidebar has a 'Buckets' section and a 'Storage Lens' section expanded, showing 'Dashboards' and 'Storage Lens groups'. The main content area is titled 'Edit Block public access (bucket settings)'. It contains a section titled 'Block public access (bucket settings)' with a note about public access being granted through various methods like ACLs and bucket policies. It includes a checkbox for 'Block all public access' and four sub-options for blocking specific types of public access through ACLs, new bucket policies, or cross-account policies.

Amazon S3 <

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Edit Block public access (bucket settings) [Info](#)

### Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

**Block public access to buckets and objects granted through *new* access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

**Block public access to buckets and objects granted through *any* access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.

**Block public access to buckets and objects granted through *new* public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

**Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

# 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/\*).

The screenshot shows the AWS S3 'Edit bucket policy' page. The left sidebar has 'Buckets' selected under 'Amazon S3'. The main area shows the 'Bucket policy' section with a JSON editor. A specific line in the JSON is highlighted with a gray background and a black border:

```
1 {  
2     "Version": "2012-10-17",  
3     "Id": "Policy1732912378379",  
4     "Statement": [  
5         {  
6             "Sid": "Stmt1732912376688",  
7             "Effect": "Allow",  
8             "Principal": "*",  
9             "Action": "s3:GetObject",  
10            "Resource": "arn:aws:s3:::my-static-website-web-learn/*"  
11        },  
12    ]  
13}
```

To the right of the JSON editor, there's a panel with 'Edit statement Stmt1732912376688' and a 'Remove' button. Below it is a 'Add actions' section with a 'Choose a service' dropdown containing a search bar labeled 'Filter services'. At the bottom, there's an 'Included' section with a single item.

# Step 7: Testing website

- 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>

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

**Static website hosting** Edit

Use this bucket to host a website or redirect requests. [Learn more](#)

**ⓘ We recommend using AWS Amplify Hosting for static website hosting**  
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

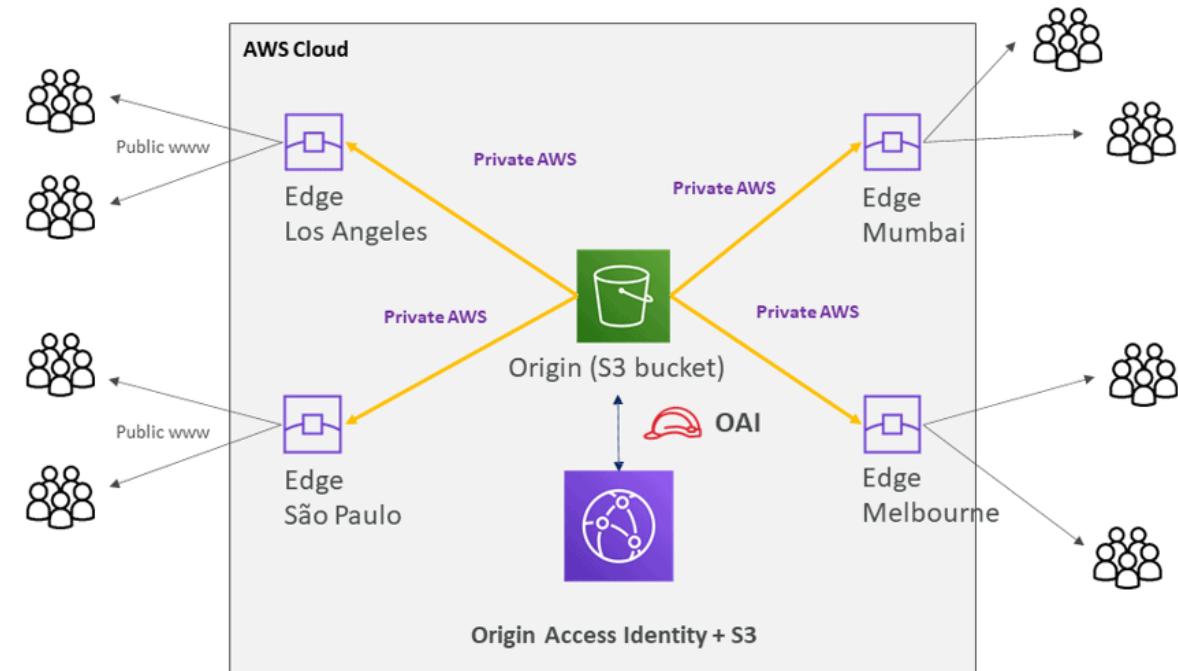
**S3 static website hosting**  
Enabled

**Hosting type**  
Bucket hosting

**Bucket website endpoint**  
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)  
<http://my-static-website-web-learn.s3-website-us-east-1.amazonaws.com>

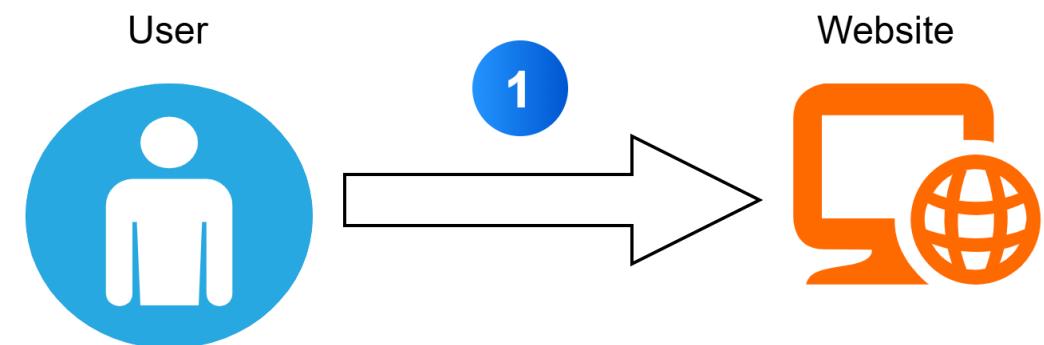
# Cloudfront

- 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?

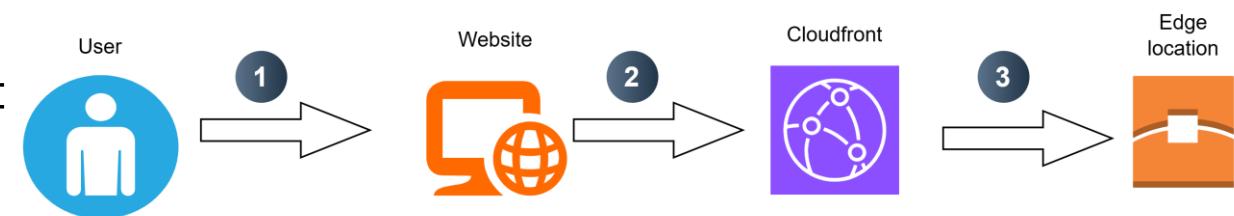
- Step 1  
The client accesses a website and requests to download a file



# How cloud front works?

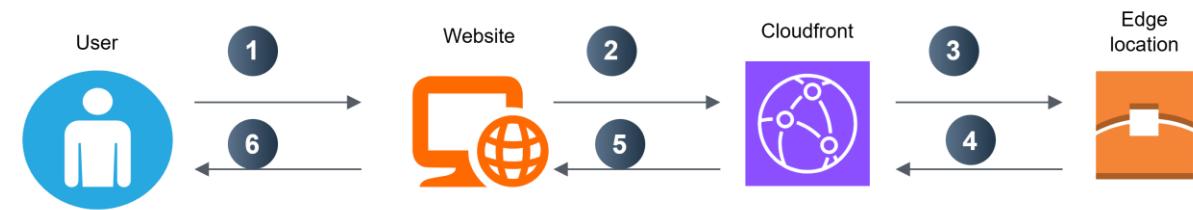
- Step 2

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



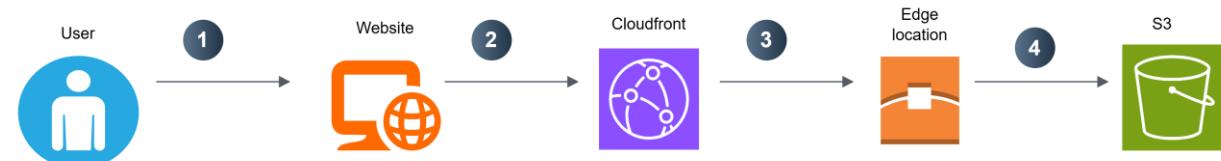
# How cloud front works?

- 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

The screenshot shows the AWS CloudFront Distributions page. The left sidebar contains navigation links for CloudFront (selected), Distributions, Policies, Functions, Static IPs, VPC origins, What's new, Telemetry (Monitoring, Alarms, Logs), Reports & analytics (Cache statistics, Popular objects, Top referrers, Usage, Viewers), and Security (Origin access, Field-level encryption). The main content area displays a table titled "Distributions (1)" with one item listed:

ID	Description	Type	Domain name	Alternate d...	Origins	Status	Last modified
E3QGNBZ8TAA7RO	-	Production	d2hyz5nqdfak...	-	my-static-website-w	Enabled	November 30, 2024 at 6:35:25...

Actions available for the distribution include Enable, Disable, Delete, and Create distribution. The top navigation bar includes the AWS logo, search bar, and user information (Member2 @ akank-aws-v2).

# AWS CloudFront Configuration

The screenshot shows the AWS CloudFront distribution configuration interface. The top navigation bar includes the AWS logo, a search bar, and various global settings like 'Global' and 'Member2 @ akank-aws-v2'. The main navigation on the left lists 'Distributions', 'Policies', 'Functions', 'Static IPs', 'VPC origins', 'What's new', 'Telemetry' (with 'Monitoring', 'Alarms', and 'Logs' sub-options), and 'Reports & analytics' (with 'Cache statistics', 'Popular objects', and 'Top referrers' sub-options). The current view is under the 'General' tab of a specific distribution named 'E3QGNBZ8TAA7RO'. The 'Details' section displays the 'Distribution domain name' as 'd2hyz5nqdfakql.cloudfront.net', the 'ARN' as 'arn:aws:cloudfront::013439131279:distribution/E3QGNBZ8TAA7RO', and the 'Last modified' time as 'November 29, 2024 at 3:47:53 AM UTC'. The 'Settings' section includes fields for 'Description' (empty), 'Alternate domain names' (empty), 'Standard logging' (status 'Off'), 'Cookie logging' (status 'Off'), and 'Default root object' set to 'index.html'. An 'Edit' button is located in the top right corner of the settings area.

CloudFront

Distributions

Policies

Functions

Static IPs

VPC origins

What's new

Telemetry

Monitoring

Alarms

Logs

Reports & analytics

Cache statistics

Popular objects

Top referrers

General Security Origins Behaviors Error pages Invalidations Tags Logging

**Details**

Distribution domain name  
d2hyz5nqdfakql.cloudfront.net

ARN  
arn:aws:cloudfront::013439131279:distribution/E3QGNBZ8TAA7RO

Last modified  
November 29, 2024 at 3:47:53 AM UTC

**Settings**

Description  
-

Alternate domain names  
-

Standard logging  
Off

Cookie logging  
Off

Default root object  
index.html

Edit

CloudShell Feedback

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

# CloudFront Origin Access Control (OAC) Settings

The screenshot shows the AWS CloudFront 'Edit origin' configuration page. The left sidebar lists various CloudFront management options like Distributions, Telemetry, Reports & analytics, Security, Key management, and Savings Bundle. The main 'Edit origin' section has a 'Settings' tab selected. Under 'Origin domain', the value 'my-static-website-web-learn.s3.amazonaws.com' is entered. The 'Origin path - optional' field is empty. The 'Name' field contains 'my-static-website-web-learn.s3.amazonaws.com'. In the 'Origin access' section, the 'Origin access control settings (recommended)' radio button is selected. The 'Origin access control' dropdown also shows 'my-static-website-web-learn.s3.amazonaws.com'. A note at the bottom states: 'You must allow access to CloudFront using this policy statement. Learn more about giving CloudFront permission to access the S3 bucket.' Below this is a 'Copy policy' button and a link to 'Go to S3 bucket permissions'. An 'Add custom header - optional' section is at the bottom.

**CloudFront**

**Distributions**

- Policies
- Functions
- Static IPs
- VPC origins
- What's new

**Telemetry**

- Monitoring
- Alarms
- Logs

**Reports & analytics**

- Cache statistics
- Popular objects
- Top referrers
- Usage
- Viewers

**Security**

- Origin access
- Field-level encryption

**Key management**

- Public keys
- Key groups

**Savings Bundle**

Overview

CloudShell Feedback

Search [Alt+S]

Global Member2 @ akank-aws-v2

## Edit origin

### Settings

**Origin domain**  
Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

my-static-website-web-learn.s3.amazonaws.com

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

**Origin path - optional**  
Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

**Name**  
Enter a name for this origin.

my-static-website-web-learn.s3.amazonaws.com

**Origin access** | [Info](#)

Public  
Bucket must allow public access.

Origin access control settings (recommended)  
Bucket can restrict access to only CloudFront.

Legacy access identities  
Use a CloudFront origin access identity (OAI) to access the S3 bucket.

**Origin access control**  
Select an existing origin access control (recommended) or create a new control.

my-static-website-web-learn.s3.amazonaws.com

Create new OAC

ⓘ You must allow access to CloudFront using this policy statement. Learn more about [giving CloudFront permission to access the S3 bucket](#).

Go to S3 bucket permissions

Add custom header - optional

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

# Update S3 Bucket Policy

The screenshot shows the AWS S3 console interface for managing a bucket policy. The left sidebar lists various bucket-related options like Access Grants, Access Points, and IAM Access Analyzer. The main area displays a JSON policy document with a specific section highlighted in blue, indicating it is selected or being edited.

```
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::my-static-website-web-learn/*"
},
{
  "Sid": "AllowCloudFrontServicePrincipal",
  "Effect": "Allow",
  "Principal": [
    "Service": "cloudfront.amazonaws.com"
  ],
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-static-website-web-learn/*",
  "Condition": {
    "StringEquals": {
      "AWS:SourceArn": "arn:aws:cloudfront::013439131279:distribution/E3QGNBZ8TAA7RO"
    }
  }
}
```

**Object Ownership** Info Edit  
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.  
**Object Ownership**  
Bucket owner enforced  
ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

**Access control list (ACL)** Edit

# CloudFront Distribution Behavior

The screenshot shows the AWS CloudFront distribution behavior configuration page. The top navigation bar includes the AWS logo, search bar, and user information (Member2 @ akank-aws-v2). The main content area is titled "Settings" and contains the following sections:

- Path pattern**: Default (\*)
- Origin and origin groups**: my-static-website-web-learn.s3.amazonaws.com
- Compress objects automatically**: Yes (radio button selected)
- Viewer** (highlighted with a red box):
  - Viewer protocol policy**: Redirect HTTP to HTTPS (radio button selected)
  - Allowed HTTP methods**: GET, HEAD (radio button selected)
  - Restrict viewer access**: No (radio button selected)
- Cache key and origin requests**: We recommend using a cache policy and origin request policy to control the cache key and origin requests.
  - Cache policy**: CachingOptimized (selected)
  - Origin request policy - optional**: Select origin policy (dropdown menu)

# Cache Policy

CloudFront Policies Cache 658327ea-f89d-4fab-a63d-7e88639e58f6

**CloudFront**

- Distributions
- Policies**
- Functions
- Static IPs
- VPC origins
- What's new

▼ Telemetry

- Monitoring
- Alarms
- Logs

▼ Reports & analytics

- Cache statistics
- Popular objects
- Top referrers
- Usage
- Viewers

▼ Security

- Origin access

**Details**

**Description**  
Policy with caching enabled. Supports Gzip and Brotli compression.

**TTL settings** Info

Minimum TTL (seconds) 1	Maximum TTL (seconds) 31536000	Default TTL (seconds) 86400
----------------------------	-----------------------------------	--------------------------------

**Cache key settings** Info

Headers - None	Cookies - None	Query strings - None
----------------	----------------	----------------------

**Compression support** Info

Gzip <span>Enabled</span>	Brotli <span>Enabled</span>
------------------------------	--------------------------------

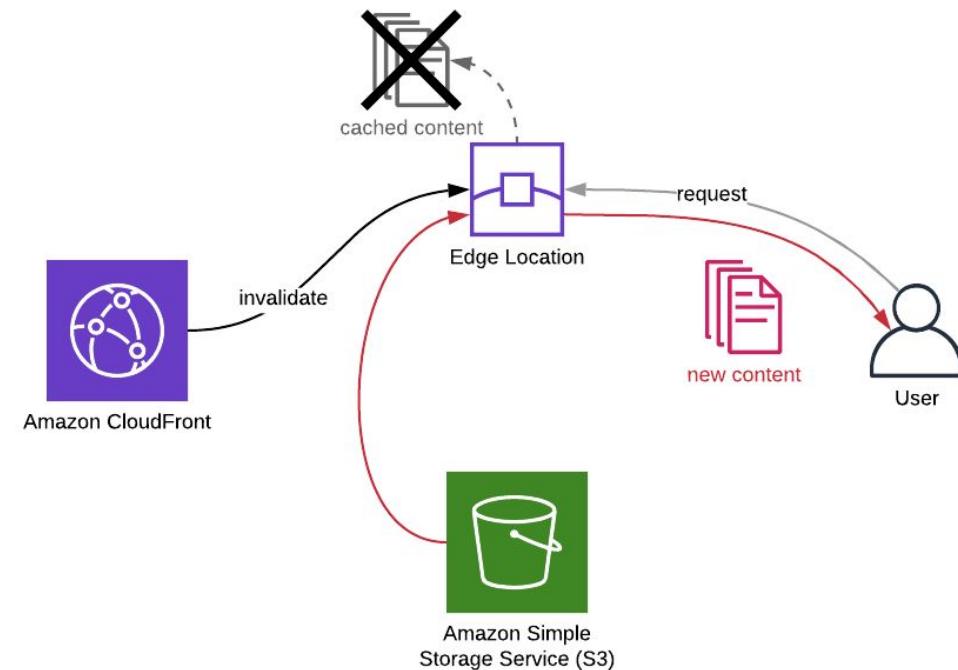
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# Invalidation

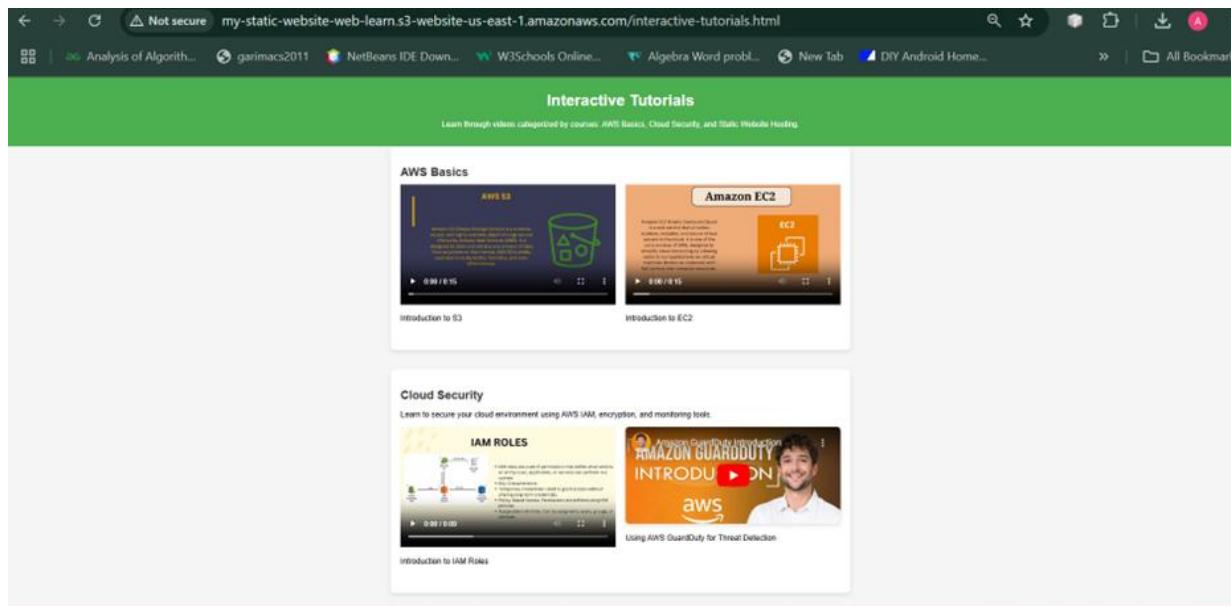
**AWS CloudFront Invalidation** is the process of removing or **purging cached content** from CloudFront edge locations before the content expires. This action forces CloudFront to fetch the updated content from the origin server the next time it's requested.

## Purpose:

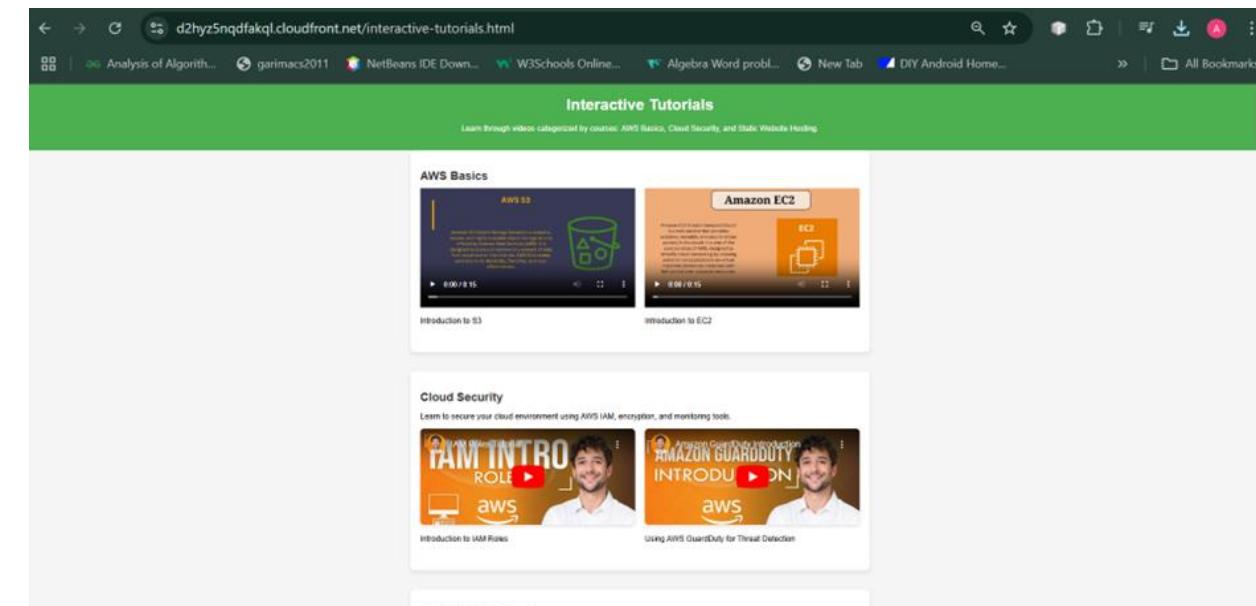
- To remove outdated or incorrect content from CloudFront's cache and replace it with the latest version from the origin server (e.g., S3, EC2).
- This is useful when content has been updated (e.g., a new version of a website or a file), but the old version is still cached at CloudFront edge locations.



# 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

The screenshot shows the AWS CloudFront Invalidations page. At the top, there's a navigation bar with the AWS logo, a search bar, and various global settings. Below the navigation, the breadcrumb trail indicates the path: CloudFront > Distributions > E3QGNBZ8TAA7RO > I8BJ2YNFS945ABEM3RD3R4AG5K. On the left, under 'Invalidation details', it shows the 'Date created' as November 28, 2024 at 6:31:29 PM UTC and the 'Status' as 'Completed'. To the right, under 'Object paths', it lists '/interactive-tutorials.html' with a 'Copy to new' button. The entire page has a light gray background with white text and blue links.

# After CloudFront Invalidations

The screenshot shows a web browser window with the URL [d2hyz5nqdfakql.cloudfront.net/interactive-tutorials.html](https://d2hyz5nqdfakql.cloudfront.net/interactive-tutorials.html). The page displays a grid of video thumbnails under the heading "Interactive Tutorials".

**AWS Basics:**

- AWS S3:** A thumbnail for a video titled "Introduction to S3" showing a green bucket icon.
- Amazon EC2:** A thumbnail for a video titled "Introduction to EC2" showing an orange EC2 instance icon.

**Cloud Security:**

- IAM ROLES:** A thumbnail for a video titled "Introduction to IAM Roles" showing a diagram of AWS IAM roles.
- Amazon GuardDuty Introduction:** A thumbnail for a video titled "Using AWS GuardDuty for Threat Detection" featuring a man speaking.

**CloudFront Invalidations** removes the old cached content from the edge locations.

# Testing website

<https://d2hyz5nqdfakql.cloudfront.net>

LOGO

ABOUT WORK CONTACT

# Smart Learning Zone

Master AWS for Cloud-Based Learning Solutions

Learn more and start today

Facebook Instagram Pinterest Twitter LinkedIn

# 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 <b>IPv4:</b> 172.96.165.74 <b>IPv6:</b> 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	<a href="https://d2hyz5nqdfakql.cloudfront.net/">https://d2hyz5nqdfakql.cloudfront.net/</a>
Mode	Manual test
Type	Https
	Load time 107 ms
Date / time	11/30/2024 2:38:00 PM
Result	0 - OK
Checkpoint	Antwerp - 1 <b>IPv4:</b> 193.110.248.20 <b>IPv6:</b> 2a02:5940:1210:2:4d62:84de:57c8:55e2
Resolved IP address	18.239.190.168
Check details	
URL	<a href="https://d2hyz5nqdfakql.cloudfront.net/">https://d2hyz5nqdfakql.cloudfront.net/</a>
Port	443
Status code	200
Total bytes	8637

# Monitor Test Results from New Delhi (India)

Monitor test results	
Monitor	<a href="https://d2hyz5nqdfakql.cloudfront.net/">https://d2hyz5nqdfakql.cloudfront.net/</a>
Mode	Manual test
Type	Https
	Load time 668 ms
Date / time	11/30/2024 2:39:55 PM
Result	0 - OK
Checkpoint	New Delhi <b>IPv4:</b> 164.52.195.81 <b>IPv6:</b> 2001:df0:411:8005::13
Resolved IP address	54.230.104.26
Check details	
URL	<a href="https://d2hyz5nqdfakql.cloudfront.net/">https://d2hyz5nqdfakql.cloudfront.net/</a>
Port	443
Status code	200
Total bytes	8637
<a href="#">Close</a>	

# AWS WAF

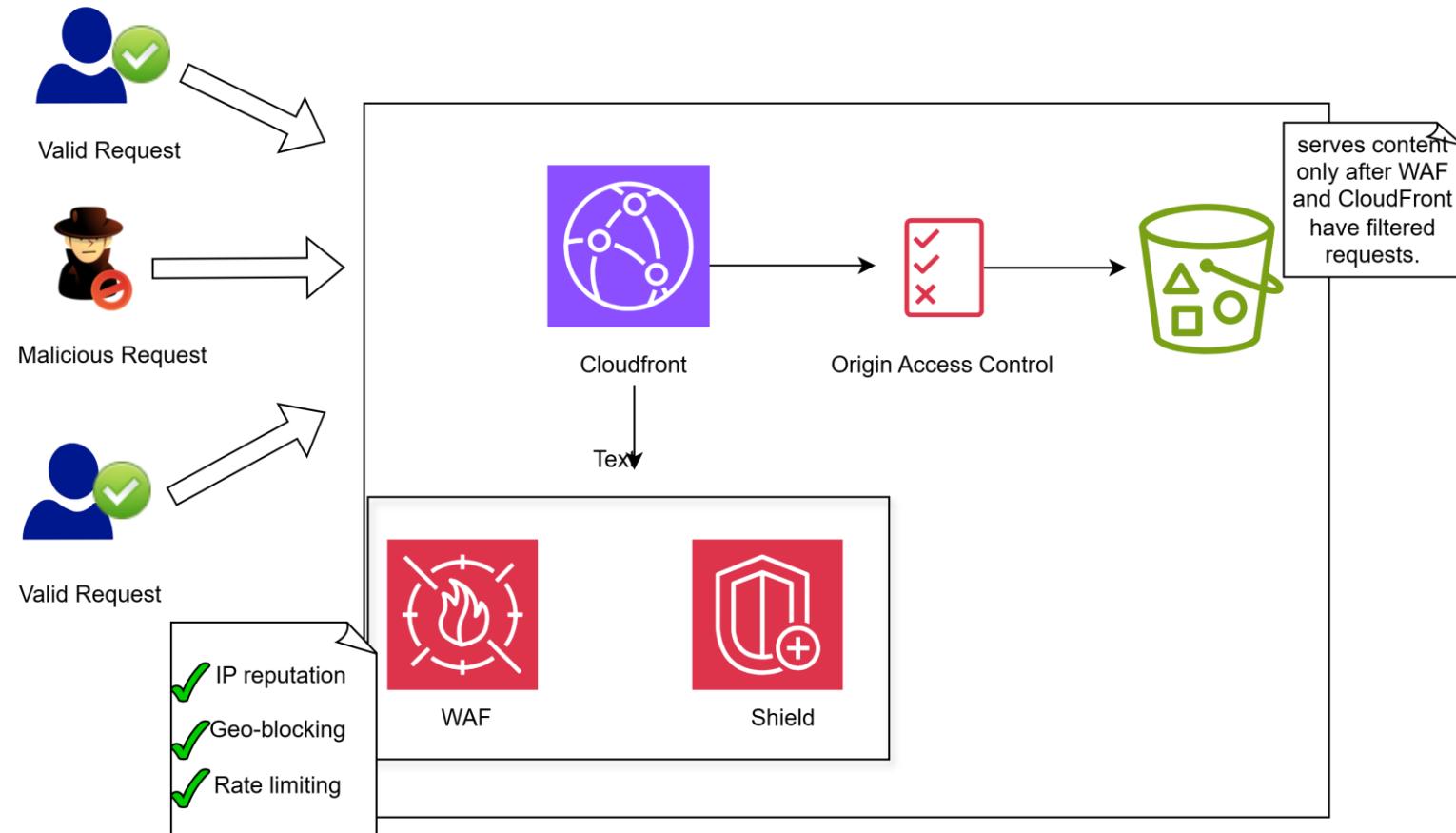
AWS WAF (Web Application Firewall) is a **cloud-based firewall service** designed to protect web applications and APIs from:

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

The screenshot shows the AWS WAF Web ACLs page. The URL in the browser is `us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls?region=global`. The left sidebar under 'AWS WAF' has 'Web ACLs' selected. The main content area displays a table titled 'Web ACLs (1)'. The table shows one entry: 'Cloudfront\_WAF' with ID `8104ef5b-1c17-42b0-82e4-687939bbdcc`. The table includes columns for Name, Description, and ID. Action buttons at the top right include 'Global (CloudFront)', 'Copy ARN', 'Delete', and 'Create web ACL'.

Name	Description	ID
Cloudfront_WAF	-	8104ef5b-1c17-42b0-82e4-687939bbdcc

# Step 2: Add Rules to the Web ACL

The screenshot shows the AWS WAF & Shield console interface. The left sidebar has sections for AWS WAF (Getting started, Web ACLs, Bot control dashboard, Application integration, IP sets, Regex pattern sets, Rule groups, AWS Marketplace managed rules) and AWS Shield (Getting started). The main navigation bar includes services, search, and global settings. The current view is under AWS WAF, specifically for the Cloudfront\_WAF rule set. The top navigation bar for this page includes AWS WAF, Web ACLs, Cloudfront\_WAF, a download button for the JSON file, and various monitoring tabs (Traffic overview, Rules, Associated AWS resources, Custom response bodies, Logging and metrics, Sampled requests, CloudWatch Log Insights). The Rules tab is selected, showing a list of 6 rules. Each rule is listed with columns for checkbox, Name, Action, Priority, and Custom response. The rules are:

	Name	Action	Priority	Custom response
<input type="checkbox"/>	<a href="#">AWS-AWSManagedRulesAmazonIpReputationList</a>	Use rule actions	0	-
<input type="checkbox"/>	<a href="#">Geo_control</a>	Block	1	-
<input type="checkbox"/>	<a href="#">Block_excessive_request</a>	Count	2	-
<input type="checkbox"/>	<a href="#">AWS-AWSManagedRulesKnownBadInputsRuleSet</a>	Use rule actions	3	-
<input type="checkbox"/>	<a href="#">AWS-AWSManagedRulesCommonRuleSet</a>	Use rule actions	4	-
<input type="checkbox"/>	<a href="#">URI_patterns</a>	Block	5	Status 403, <a href="#">Premium_Members</a>

# 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

The screenshot shows the AWS WAF & Shield console with the 'Web ACLs' section selected. The main view is for a Web ACL named 'Cloudfront\_WAF'. The 'Associated AWS resources' tab is active, showing one association:

Name	Resource type	Region
E3QGNBZ8TAA7RO - d2hyz5nqdfakql.cloudfront.net	CloudFront Distribution	Global (CloudFront)

Below this, there's a section for 'Web request body inspection' with a 'Body size limit' setting of 'Default (16 KB)'.

**Associated AWS resources (1)**

Find associated AWS resources

Disassociate Add AWS resources

1

Name	Resource type	Region
E3QGNBZ8TAA7RO - d2hyz5nqdfakql.cloudfront.net	CloudFront Distribution	Global (CloudFront)

Web request body inspection - new [Info](#)

By default, rules that inspect the web request body are limited to the first 16 KB of content. You can increase this size for additional costs. [AWS WAF Pricing](#)

Body size limit

The AWS WAF default limit is 16 KB. Settings over 16 KB incur additional costs. [Learn more](#)

CloudFront distributions

Default (16 KB)

CloudShell Feedback

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



**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	<a href="https://d2hyz5nqdfakql.cloudfront.net/">https://d2hyz5nqdfakql.cloudfront.net/</a>
Mode	Manual test
Type	Https
	Load time 119 ms
Date / time	11/30/2024 2:35:48 PM
Result	3009 - HTTP error Forbidden <a href="#">More information about this error</a>
Checkpoint	Toronto - 2 <b>IPv4:</b> 5.149.253.60 <b>IPv6:</b> -
Resolved IP address	13.225.189.46
Check details	
URL	<a href="https://d2hyz5nqdfakql.cloudfront.net/">https://d2hyz5nqdfakql.cloudfront.net/</a>
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

**Settings**

**Description**  
-

**Price class**  
Use only North America and Europe

**Supported HTTP versions**  
HTTP/2, HTTP/1.1, HTTP/1.0

**Alternate domain names**  
-

**Standard logging**  
On

**Cookie logging**  
Off

**Default root object**  
index.html

**Edit**

The screenshot shows the AWS CloudFront Distributions page with the distribution ID E3QGNBZ8TAA7RO selected. The left sidebar shows navigation options like CloudFront, Policies, Functions, Static IPs, VPC origins, What's new, Telemetry (Monitoring, Alarms, Logs), and Reports & analytics (Cache statistics, Popular objects, Top referrers, Usage, Viewers). The main content area is titled 'E3QGNBZ8TAA7RO' and has a 'View metrics' button. It features tabs for General, Security, Origins, Behaviors, Error pages, Invalidations, Tags, and Logging, with 'Logging' selected. Under 'Standard log destinations', there is one entry: 'my-cloudwatch-web-learn-bucket' (S3 type, selected fields '33', partitioning 'None', output format 'w3c'), with 'Manage' and 'Add' buttons. Under 'Attached real-time logs', there is one entry: 'Default (\*)' (Cache behavior, Log configuration ' - ', Status 'Disabled', Distribution status 'Enabled'), with an 'Edit' button.

## 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.

The screenshot shows the Amazon S3 console interface. The left sidebar has a tree view with 'Amazon S3' selected, under which 'Buckets' is expanded, showing 'my-cloudwatch-web-learn-bucket'. Other options like 'Access Grants', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', and 'IAM Access Analyzer for S3' are also listed. Below that is a section for 'Block Public Access settings for this account'. Under 'Storage Lens', there are links for 'Dashboards', 'Storage Lens groups', and 'AWS Organizations settings'. At the bottom of the sidebar is a 'Feature spotlight' section with a '10' badge. The main content area is titled 'my-cloudwatch-web-learn-bucket' with an 'Info' link. It has tabs for 'Objects' (selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Below the tabs is a toolbar with 'Objects (2) Info', 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A note says '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.' with a 'Learn more' link. There's a search bar 'Find objects by prefix' and a pagination indicator '1'. The main table lists two objects:

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	E3QGNBZ8TAA7RO.2024-11-29-20.25d79268.gz	gz	November 29, 2024, 15:45:08 (UTC-05:00)	1.5 KB	Standard
<input type="checkbox"/>	E3QGNBZ8TAA7RO.2024-11-30-01.2ac8de9e.gz	gz	November 29, 2024, 20:45:09 (UTC-05:00)	1.1 KB	Standard

# 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).

The screenshot shows the AWS WAF & Shield interface for a Cloudfront\_WAF. The left sidebar has sections for AWS WAF (Getting started, Web ACLs, Bot control dashboard, Application integration, IP sets, Regex pattern sets, Rule groups, AWS Marketplace managed rules) and AWS Shield (Getting started). The main content area shows the Cloudfront\_WAF configuration with tabs for Traffic overview, Rules, Associated AWS resources, Custom response bodies, Logging and metrics (which is selected and highlighted with a blue border), Sampled requests, and CloudWatch Log Insights. Under Logging, it shows an info section for enabling, editing, or disabling traffic logging, with buttons for Enable, Edit, and Disable. It also shows a configuration for an Amazon S3 bucket where logs are sent. Under Sampled requests, it shows settings for enabling sampled requests and selecting default actions.

# Enable WAF Logging

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

## Amazon S3

### Buckets

- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

### Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 10

40/

### Objects

### Properties

Objects (1) Info



Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

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](#)

Find objects by prefix

Show versions

< 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">013439131279_waflogs_cloudfront_Cloudfront_WAF_20241129T2040Z_eeb02343.log.gz</a>	gz	November 29, 2024, 15:47:49 (UTC-05:00)	2.2 KB	Standard

# 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.

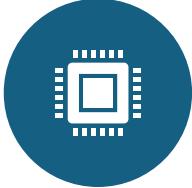
## Highlights

- 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.



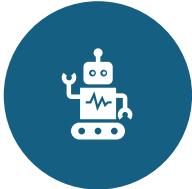
Monitoring the performance and availability of web applications.



Troubleshooting application failures by analyzing logs and metrics.



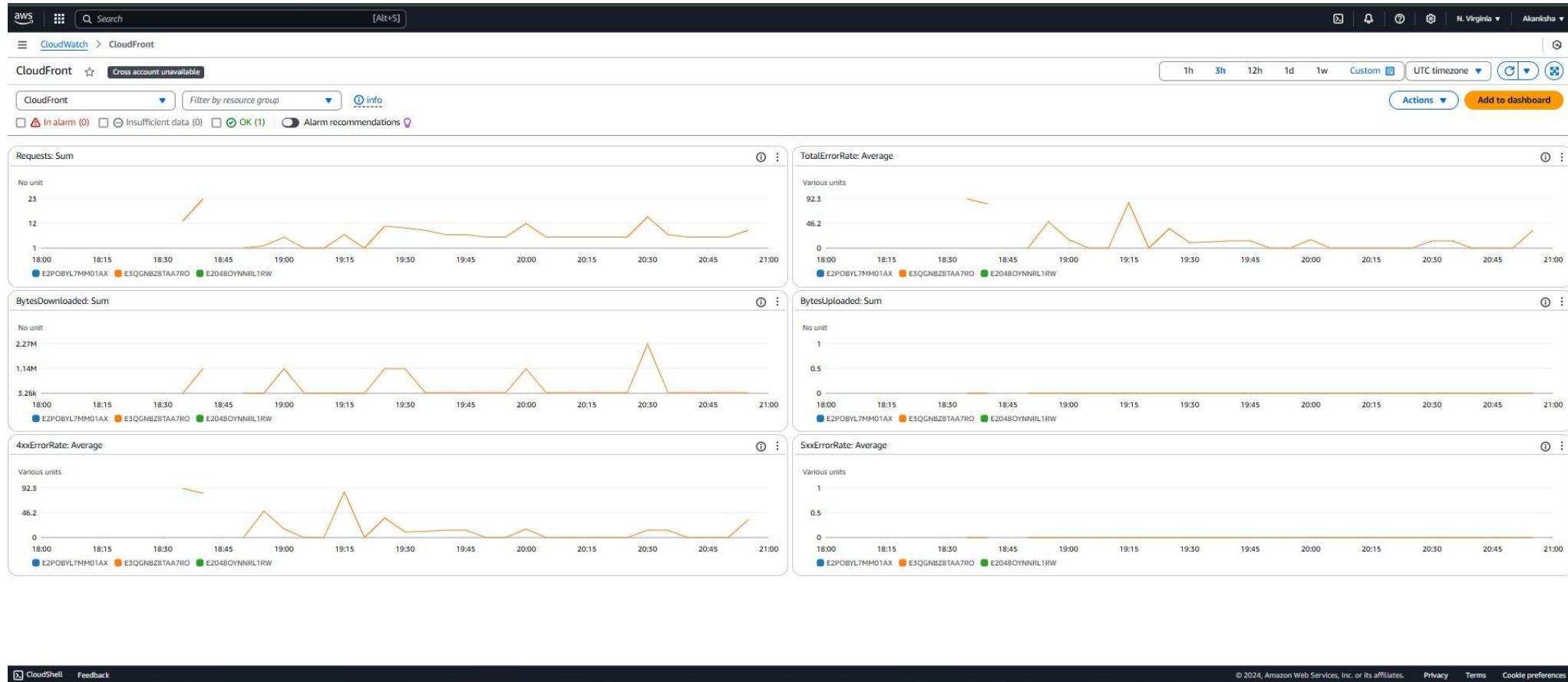
With Amazon CloudWatch, we can ensure that our applications and infrastructure run smoothly while enabling proactive maintenance to avoid costly downtime. It's an essential tool for anyone building on the AWS cloud.



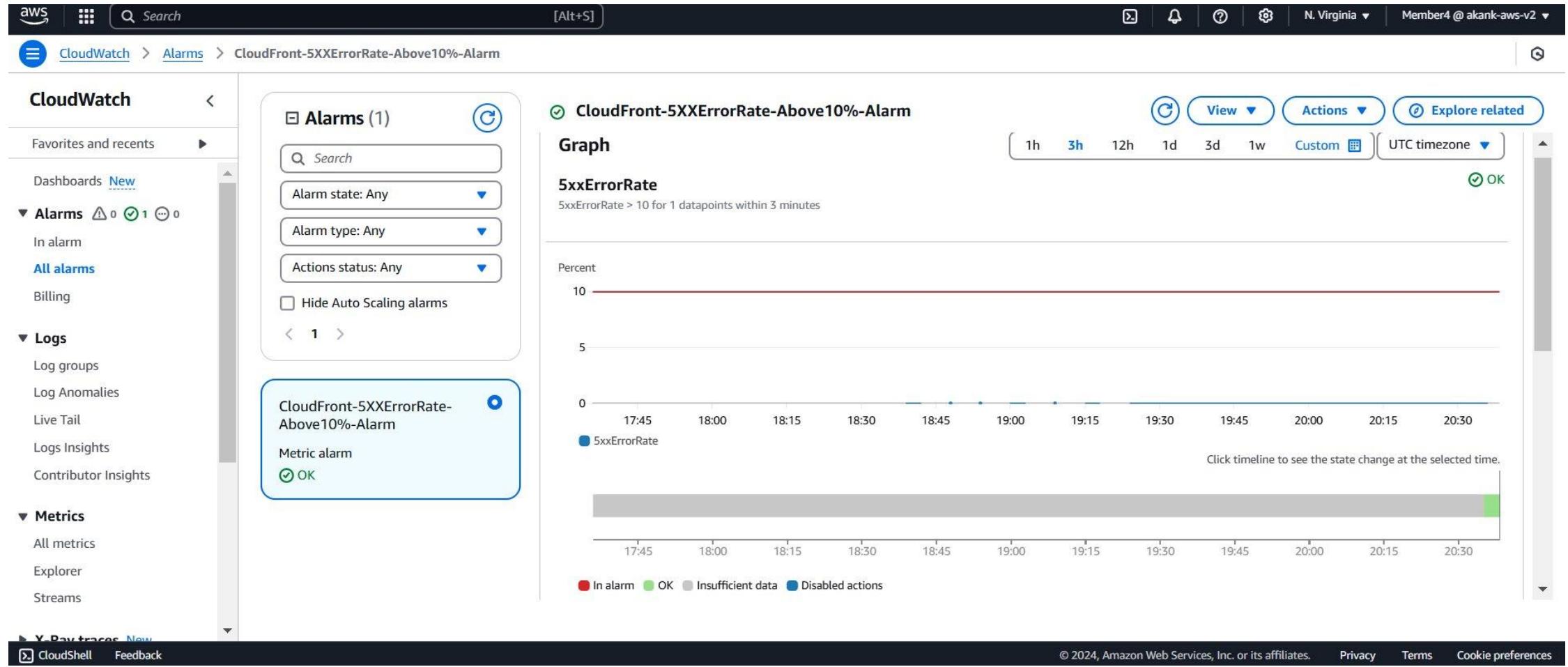
Automating scaling decisions based on real-time performance data.



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

CloudWatch > Alarms > CloudFront-5XXErrorRate-Above10%-Alarm

CloudWatch CloudShell

Favorites and recents

Dashboards New

Alarms △ 0 ○ 0 ⌚ 1

In alarm

All alarms

Billing

Logs

Log groups

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

Metrics

All metrics

Explorer

Streams

Y-Ray traces New

CloudWatch Alarms (1) ⟳

Search

Alarm state: Any

Alarm type: Any

Actions status: Any

Hide Auto Scaling alarms

< 1 >

CloudFront-5XXErrorRate-Above10%-Alarm ●

Metric alarm

⌚ Insufficient data

CloudFront-5XXErrorRate-Above10%-Alarm

CloudFront-5XXErrorRate-Above10%-Alarm

Details Tags Actions History Parent alarms

Details

Name: CloudFront-5XXErrorRate-Above10%-Alarm

State: ⌚ Insufficient data

Type: Metric alarm

Description: If more than 10% of responses are 5XX errors for 3 consecutive minutes the CloudWatch alarm is triggered.

Threshold: 5xxErrorRate > 10 for 1 datapoints within 3 minutes

Last state update: 2024-11-30 20:33:51 (UTC)

Actions: ✓ Actions enabled

Namespace: AWS/CloudFront

Metric name: 5xxErrorRate

Region: Global

DistributionId: E3QGNBZ8TAA7RO

Statistic: Average

Period: 3 minutes

Datapoints to alarm: 1 out of 1

Missing data treatment: Treat missing data as missing

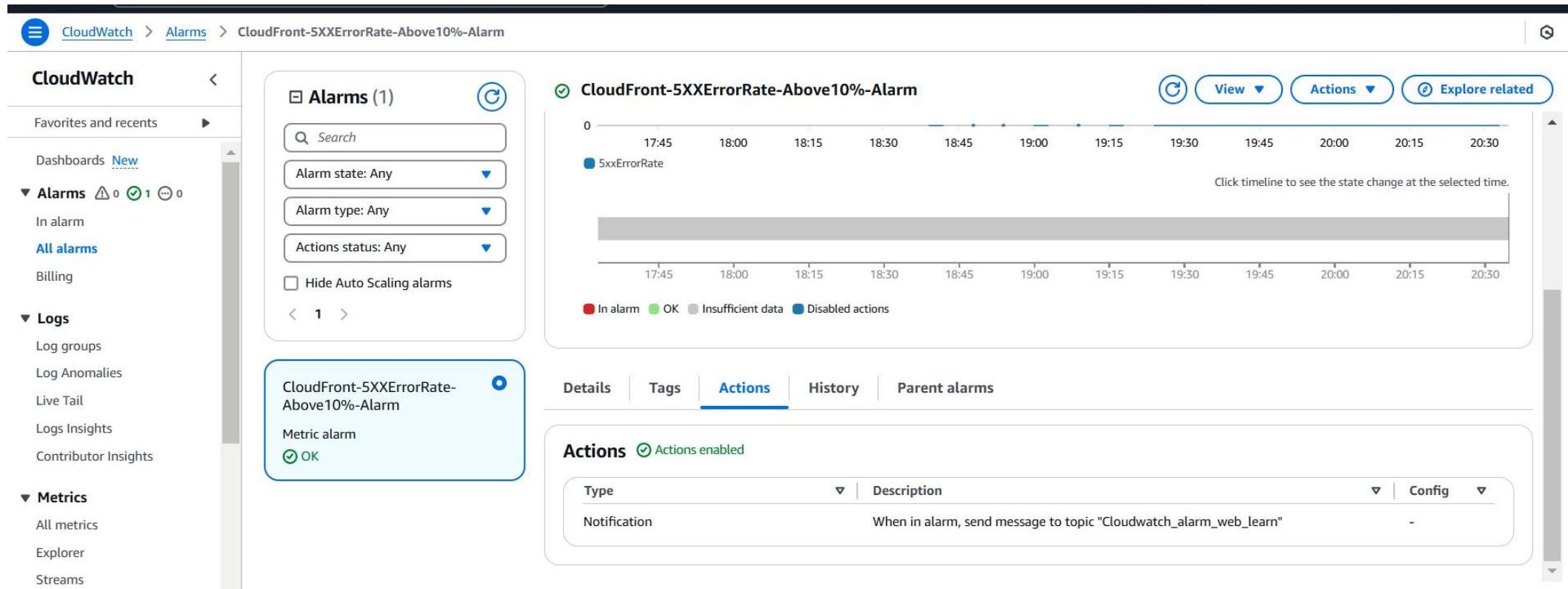
Percentiles with low samples: evaluate

ARN: arn:aws:cloudwatch:us-east-1:013439131279:alarm:CloudFront-5XXErrorRate-Above10%-Alarm

View ☰

Actions ▼

Explore related  ⓘ



## 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.



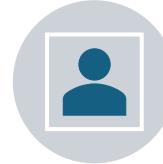
SNS is designed to deliver messages efficiently and reliably across a range of platforms, making it an integral part of modern application architectures.



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 X

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/servicecatalog/?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://aws.amazon.com/pm/servicecatalog/?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=EAIalQobChMlyPzx74OKigMV9UNHAR2-WBVVEAYASAAEgKBh\\_D\\_BwE](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=EAIalQobChMlyPzx74OKigMV9UNHAR2-WBVVEAYASAAEgKBh_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**