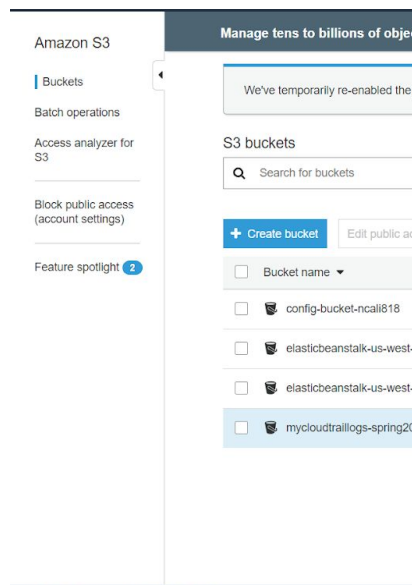


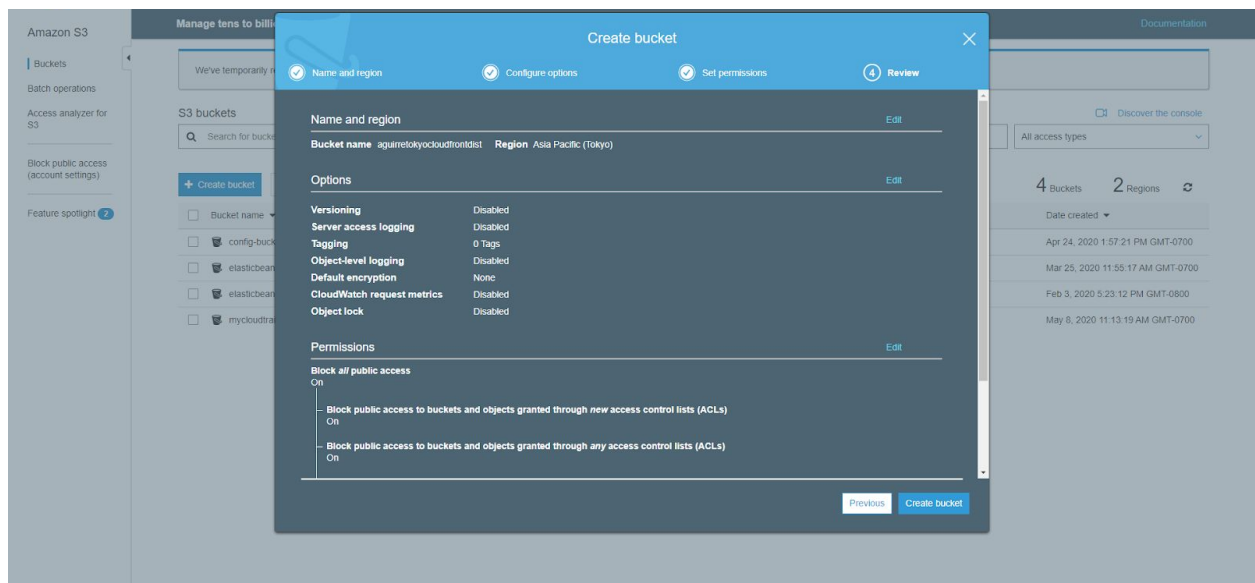
Module 8 Lab 1: WAF Tutorial

Amazon S3 - S3 buckets



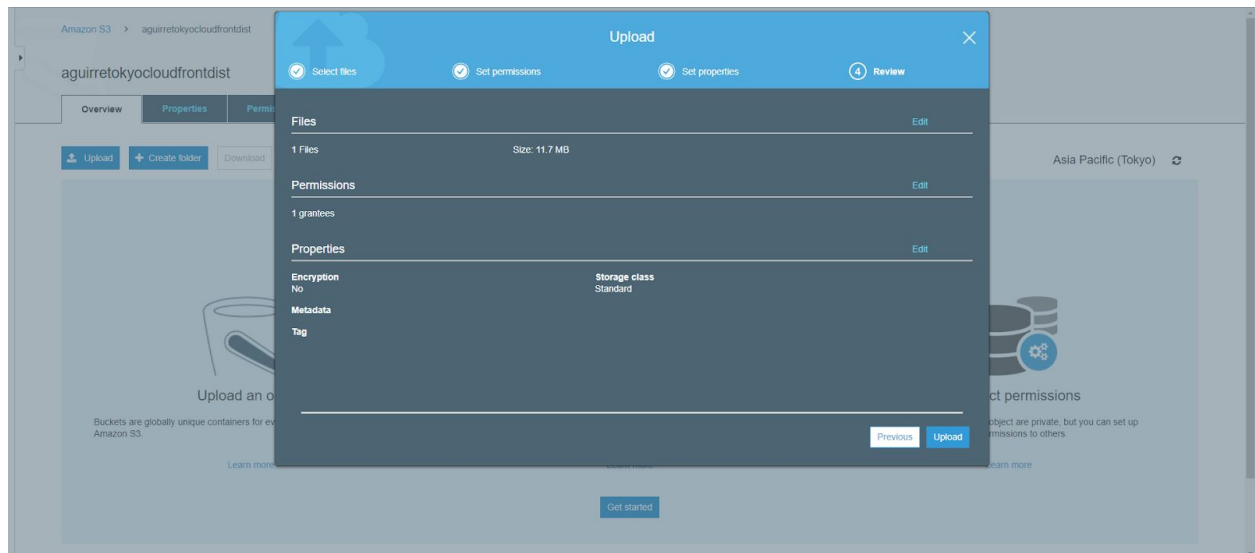
Starting with a S3 bucket, use a large file to help realize benefits of the CloudFront service.

Amazon S3 - Create bucket Review



Note that all settings were left default. Choose a distant Region in locality.

S3 - Upload



No permissions are changed when uploading to the S3 bucket. This is because CloudFront will do those changes for us. Note the 11.7MB size

Amazon S3 - S3 bucket image



The image is stored in Tokyo. Before Cloudfront optimization the webpage load took about 14 seconds with a file size of 11.7 MB

Step 1: Select delivery method
Step 2: Create distribution

Select a delivery method for your content.



Web

Create a web distribution if you want to:

- Speed up distribution of static and dynamic content, for example, .html, .css, .php, and graphics files.
- Distribute media files using HTTP or HTTPS.
- Add, update, or delete objects, and submit data from web forms.
- Use live streaming to stream an event in real time.

You store your files in an origin - either an Amazon S3 bucket or a web server. After you create the distribution, you can add more origins to the distribution.

[Get Started](#)

RTMP

CloudFront is discontinuing support for RTMP distributions on December 31, 2020. For more information, please [read the announcement](#).

Create an RTMP distribution to speed up distribution of your streaming media files using Adobe Flash Media Server's RTMP protocol. An RTMP distribution allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location. Note the following:

- To create an RTMP distribution, you must store the media files in an Amazon S3 bucket.
- To use CloudFront live streaming, create a web distribution.

[Get Started](#)

[Cancel](#)

For this lab, the Web option was selected. Note the discontinuation support date for Adobe Flash Media Server's RTMP protocol is the end of 2020.

CloudFront - Create Distribution

Step 1: Select delivery method
Step 2: Create distribution

Create Distribution



Origin Settings

Origin Domain Name



Origin Path



Origin ID



Restrict Bucket Access

☒ Yes

☐ No



If you want to require that users always access your Amazon S3 content using CloudFront URLs, not Amazon S3 URLs, click Yes. This is useful when you are using signed URLs or signed cookies to restrict access to your content. In the help, see "Serving Private Content through CloudFront".

Origin Access Identity

☒ Create a New Identity

☐ Use an Existing Identity



Comment



Grant Read Permissions on Bucket

☒ Yes, Update Bucket Policy

☐ No, I Will Update Permissions



Origin Custom Headers

Header Name



Value



Default Cache Behavior Settings

Path Pattern



Viewer Protocol Policy

☒ HTTP and HTTPS

☐ Redirect HTTP to HTTPS

☐ HTTPS Only



Allowed HTTP Methods

☒ GET, HEAD

☐ GET, HEAD, OPTIONS

☐ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE



Field level Encryption Config



Cached HTTP Methods



Cache Based on Selected Request Headers



[Learn More](#)

Object Caching

☒ Use Origin Cache Headers

☐ Customize



[Learn More](#)

Creating a CloudFront distribution offers many options. Note Restrict Bucket Access and Grant Read Permissions on Bucket are set to yes. The previous public setting should be overridden.

CloudFront - Create Distribution

Step 1: Select delivery method
Step 2: Create distribution

Object Caching ☒ Use Origin Cache Headers ☐ Customize [Learn More](#)

Minimum TTL

Maximum TTL

Default TTL

Forward Cookies ☐ None (Improves Caching) ☒ All

Query String Forwarding and Caching ☐ None (Improves Caching) ☒ All

Smooth Streaming ☐ Yes ☒ No

Restrict Viewer Access (Use Signed URLs or Signed Cookies) ☐ Yes ☒ No

Compress Objects Automatically ☐ Yes ☒ No [Learn More](#)

Lambda Function Associations

CloudFront Event [Learn More](#)

Lambda Function ARN

Include Body ☐

Distribution Settings

Price Class

AWS WAF Web ACL

Alternate Domain Names (CNAMEs)

SSL Certificate ☒ Default CloudFront Certificate (* cloudfront.net) ☐ Custom SSL Certificate (example.com)

Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d111111abcdef8.cloudfront.net/logo.jpg). Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.example.com/logo.jpg. You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

[Request or Import a Certificate with ACM](#)

[Learn more about using custom SSL/TLS certificates with CloudFront](#)
[Learn more about using ACM](#)

Supported HTTP Versions ☒ HTTP2, HTTP1.1, HTTP1.0 ☐ HTTP1.1, HTTP1.0

Default Root Object

Logging ☐ On ☒ Off

Bucket for Logs

Log Prefix

Cookie Logging ☐ On ☒ Off

Enable IPv6 ☒ [Learn more](#)

Comment

Distribution State ☒ Enabled ☐ Disabled

[Cancel](#) [Back](#) [Create Distribution](#)

Note that the Price Class is set to Best Performance.

CloudFront - Create Distribution

Step 1: Select delivery method
Step 2: Create distribution

AWS WAF Web ACL

Alternate Domain Names (CNAMEs)

SSL Certificate ☒ Default CloudFront Certificate (* cloudfront.net) ☐ Custom SSL Certificate (example.com)

Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d111111abcdef8.cloudfront.net/logo.jpg). Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.example.com/logo.jpg. You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

[Request or Import a Certificate with ACM](#)

[Learn more about using custom SSL/TLS certificates with CloudFront](#)
[Learn more about using ACM](#)

Supported HTTP Versions ☒ HTTP2, HTTP1.1, HTTP1.0 ☐ HTTP1.1, HTTP1.0

Default Root Object

Logging ☐ On ☒ Off

Bucket for Logs

Log Prefix

Cookie Logging ☐ On ☒ Off

Enable IPv6 ☒ [Learn more](#)

Comment

Distribution State ☒ Enabled ☐ Disabled

[Cancel](#) [Back](#) [Create Distribution](#)

Note that AWS WAF Web ACL will be updated later in this lab. All other options left at default.

CloudFront - Distributions

CloudFront

Use CloudFront to serve a static website hosted on Amazon Simple Storage Service. [Learn more](#)

CloudFront Distributions

[Create Distribution](#) [Distribution Settings](#) [Delete](#) [Enable](#) [Disable](#)

Viewing: Any Delivery Method Any State << < Viewing 1 to 1 of 1 items > >

Delivery Method	ID	Domain Name	Comment	Origin	CNAME's	Status	State	Last Modified
<input type="checkbox"/> Web	E2VSP63GKOC325	dmoxcdhsrw01.cloud	-	agumetokyo	-	Deployed	Enabled	2020-05-25 19:32 UT

<< < Viewing 1 to 1 of 1 items > >

The complete CloudFront setup process took about 8 minutes.

CloudFront

CloudFront Distributions > E2VSP63GKOC325

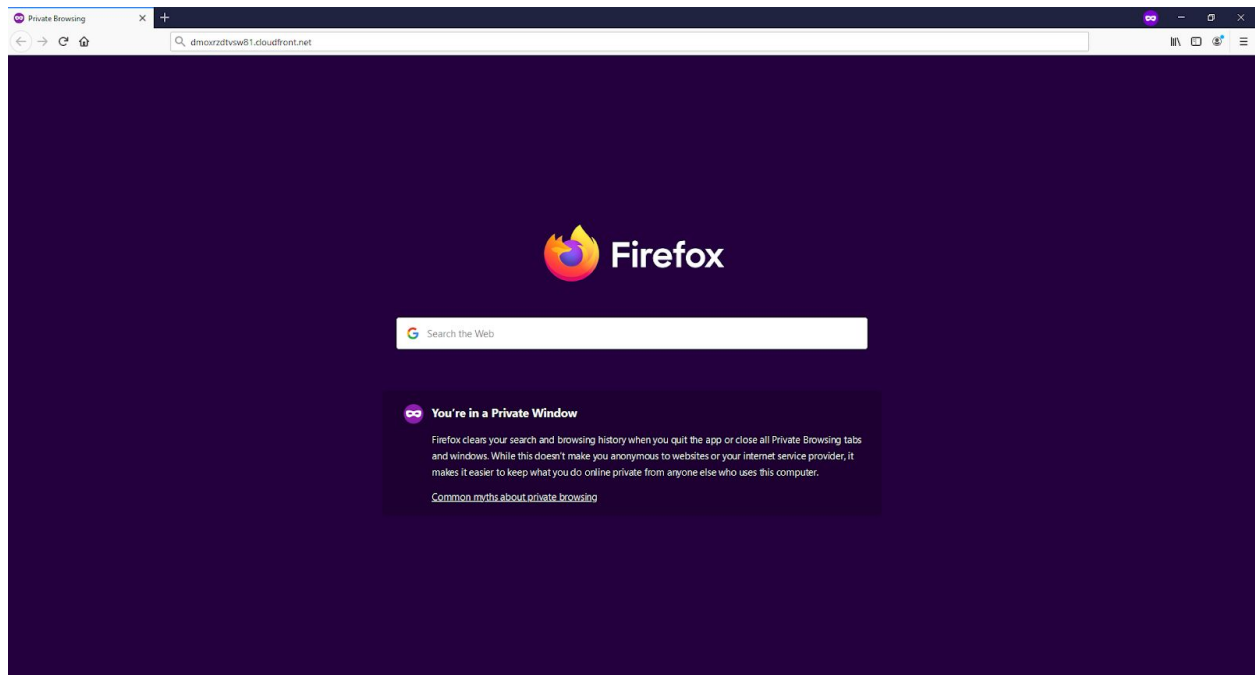
[General](#) [Origins and Origin Groups](#) [Behaviors](#) [Error Pages](#) [Restrictions](#) [Invalidations](#) [Tags](#)

[Edit](#)

Distribution ID: E2VSP63GKOC325
ARN: arn:aws:cloudfront:750287676061:distribution:E2VSP63GKOC325
Log Prefix: -
Delivery Method: Web
Cookie Logging: Off
Distribution Status: Deployed
Comment: -
Price Class: Use All Edge Locations (Best Performance)
AWS WAF Web ACL: -
State: Enabled
Alternate Domain Names (CNAMEs): -
SSL Certificate: Default CloudFront Certificate (*.cloudfront.net)
Domain Name: dmoxcdhsrw01.cloudfront.net
Custom SSL Client Support: -
Security Policy: TLSv1
Supported HTTP Versions: HTTP/2, HTTP/1.1, HTTP/1.0
IPv6: Enabled
Default Root Object: -
Last Modified: 2020-05-25 19:32 UTC-7
Log Bucket: -

Note the domain name. The S3 bucket permissions should have been reset, thus removing the bucket from public access.

Firefox - Before CloudFront Redirect



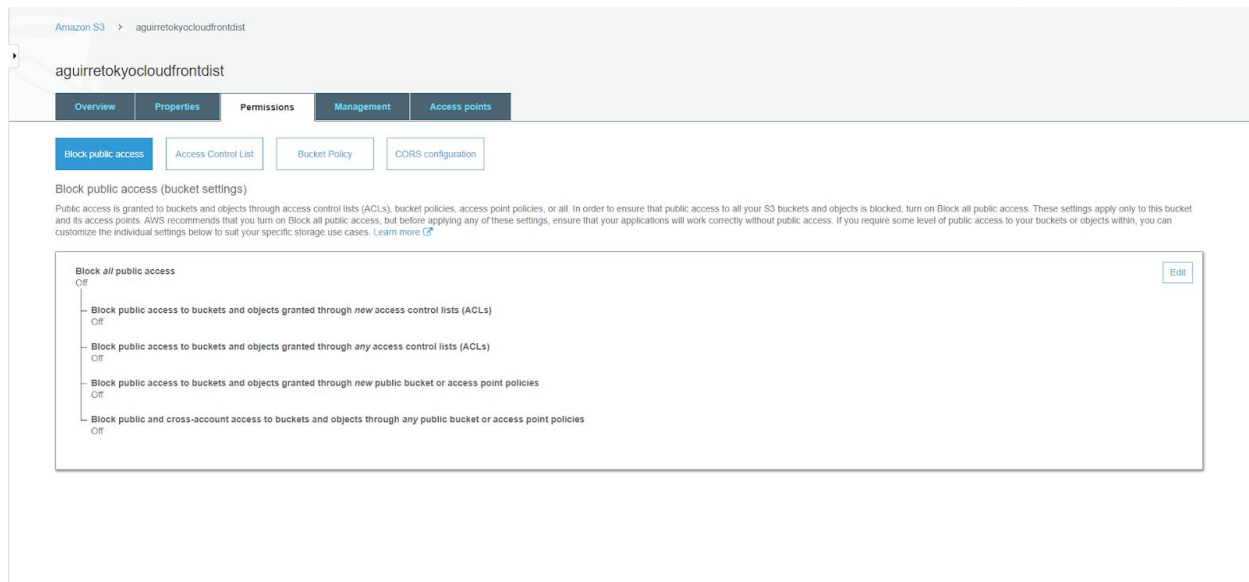
The new domain is entered.

Firefox - After Redirect



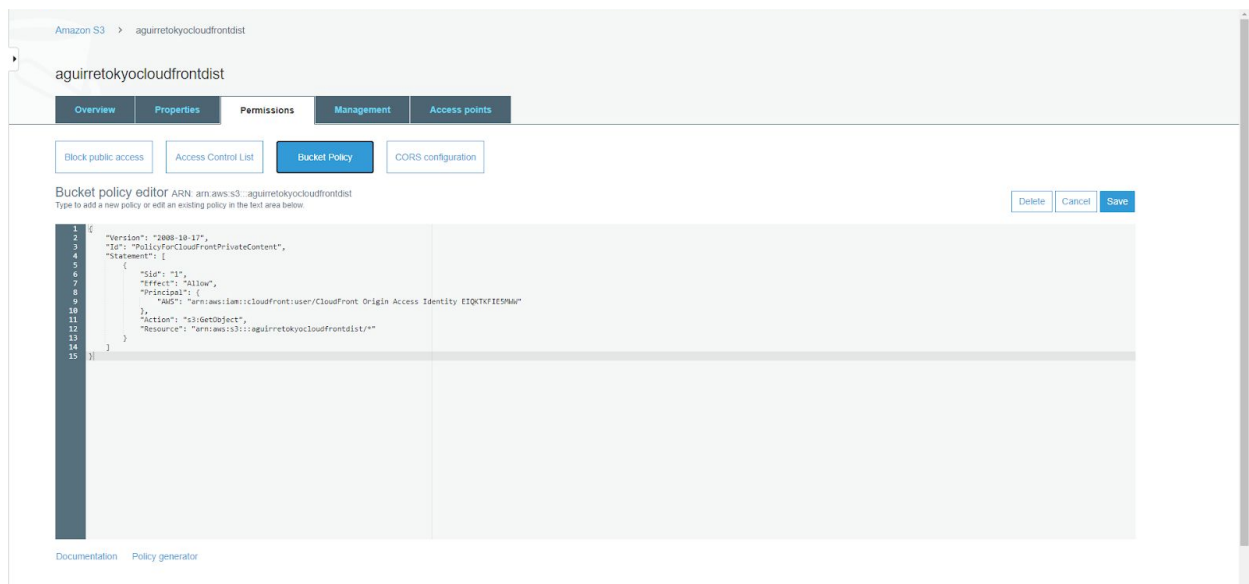
The access is blocked due to CloudFront.

Amazon S3 - Bucket Permissions



Note the bucket setting to block all public access

Amazon S3 - Bucket Policy



However, the Bucket policy is set to allow GetObject.

AWS WAF

Set up a web access control list (web ACL)

Concepts overview

Step 1: Name web ACL

Step 2: Create conditions

Step 3: Create rules

Step 4: Review and create

Name web ACL

To create a web ACL that you want to use to filter web requests, type a name for your web ACL, and then choose Next. [Learn more](#)

Web ACL name* mywafdemo

CloudWatch metric name* mywafdemo

Region* Global (CloudFront)

Use global to create WAF resources that you would associate with CloudFront distributions and other regions for WAF resources that you would associate with ALBs and API Gateway stages in that region.

AWS resource to associate EZVSP63GKOC325 - dmoxyzdvw...

[Reset selected resource](#)

You can associate this web ACL with more resources after you finish the wizard. On the Web ACLs page for this web ACL, see the Rules tab.

* Required

[Cancel](#) [Previous](#) [Next](#)

Setting up the web ACL as a WAF service.

AWS WAF - web ACL

Set up a web access control list (web ACL)

Concepts overview

Step 1: Name web ACL

Step 2: Create conditions

Step 3: Create rules

Step 4: Review and create

Create conditions

Conditions specify the filters that you want to use to allow or block requests that are AWS resources such as Amazon CloudFront distributions.

Cross-site scripting match conditions

Name [Create condition](#)

You don't have any cross-site scripting match conditions. Choose [Create XSS match condition](#) to get started.

A cross-site scripting match condition specifies the parts of web requests (such as a User-Agent header) that you use WAF to inspect for cross-site scripting threats. [Learn more](#)

Geo match conditions

Name [Create condition](#)

You don't have any geo match conditions. Choose [Create geo match condition](#) to get started.

A geo match condition lets you allow, block, or count web requests based on the geographic origin of the request. [Learn more](#)

IP match conditions

Name [Create condition](#)

You don't have any IP match conditions. Choose [Create IP match condition](#) to get started.

An IP match condition specifies the IP addresses and/or address ranges that you want to use to control access to content. Put IP addresses that you want to allow and IP addresses that you want to block into separate IP match conditions. [Learn more](#)

Size constraint conditions

Name [Create condition](#)

You don't have any size constraint conditions. Choose [Create size constraint condition](#) to get started.

A size constraint condition specifies the parts of a web request (such as a User-Agent header) that you want AWS WAF to inspect for size constraints. [Learn more](#)

A geo match condition lets you allow, block, or count web requests based on the geographic origin of the request. [Learn more](#)

Name* geoAF

Region* Global (CloudFront)

Choose Global (CloudFront) to create AWS WAF resources to use with CloudFront distributions in all AWS Regions. Choose a specific AWS Region to create AWS WAF resources to use with an Application Load Balancer in that region.

Filter settings

Add one or more locations.

Location type* Country

Location* Afghanistan - AF

[Add location](#)

Filters in this geo match condition

Geographic origin of the request to filter on

This condition has no filters.

* Required

[Cancel](#) [Create](#)

AWS WAF works via creating conditions that point to a desired outcome. In this case the Afghanistan geolocation will be blocked.

AWS WAF - web ACL

IP match condition created successfully.

Set up a web access control list (web ACL)

[Concepts overview](#)
[Step 1: Name web ACL](#)
[Step 2: Create conditions](#)
[Step 3: Create rules](#)
[Step 4: Review and create](#)

Create conditions

Conditions specify the filters that you want to use to allow or block requests that are forwarded to AWS resources such as Amazon CloudFront distributions.

Cross-site scripting match conditions
You don't have any cross-site scripting match conditions. Choose [Create XSS match condition](#) to get started.

A cross-site scripting match condition specifies the parts of a web request (such as a User-Agent header) that you want AWS WAF to inspect for cross-site scripting threats. [Learn more](#)

Geo match conditions
Geo match condition created successfully.

IP match conditions
IP match condition created successfully.

Size constraint conditions
You don't have any size constraint conditions. Choose [Create size constraint condition](#) to get started.

A size constraint condition specifies the parts of a web request (such as a User-Agent header) that you want AWS WAF to compare to a set size. [Learn more](#)

SQL injection match conditions
You don't have any SQL injection match conditions. Choose [Create SQL injection match condition](#) to get started.

A SQL injection match condition specifies the parts of a request (such as a User-Agent header) that you want AWS WAF to inspect for SQL queries. Create separate conditions that you want to allow SQL queries in and parts that you don't. [Learn more](#)

String and regex match conditions
You don't have any string or regex match conditions. Choose [Create condition](#) to get started.

A string match condition, or a regex match condition, is the part of a web request (such as a User-Agent header) that you want to use to access to your content. Create separate conditions for regex patterns that you want to allow or block. [Learn more](#)

Concepts overview

Web ACL example
if requests match

Rule 1: Bad User-Agents, then block

IP match condition
Suspicious IP's

and

String match condition
Bad bots

or if requests match

Rule 2: Detect SQLi, then block

SQL injection match condition
SQLi checks

otherwise, perform the default action

Default action
Allow requests that don't match any rules

A specific IP will be blocked when a IP condition match.

AWS WAF - Create Conditions

IP match condition created successfully.

Size constraint conditions
You don't have any size constraint conditions. Choose [Create size constraint condition](#) to get started.

A size constraint condition specifies the parts of a web request (such as a User-Agent header) that you want AWS WAF to compare to a set size. [Learn more](#)

SQL injection match conditions
You don't have any SQL injection match conditions. Choose [Create SQL injection match condition](#) to get started.

A SQL injection match condition specifies the parts of a request (such as a User-Agent header) that you want AWS WAF to inspect for SQL queries. Create separate conditions that you want to allow SQL queries in and parts that you don't. [Learn more](#)

String and regex match conditions
You don't have any string or regex match conditions. Choose [Create condition](#) to get started.

A string match condition, or a regex match condition, is the part of a web request (such as a User-Agent header) that you want to use to access to your content. Create separate conditions for regex patterns that you want to allow or block. [Learn more](#)

Create regex match condition

A regex match condition contains a list of the regex patterns that matches particular part in web requests that you want to allow or block. [Learn more](#)

Name* block

Region* Global (CloudFront)

Type* Regex match

To create a standard string match condition, choose String match. To create a regular expression match condition, choose Regex match.

Filter settings

Specify the settings that you want to use to allow or block web requests. You can only have one filter in a regex match condition, but you can have up to 10 regex patterns in the regex pattern set used in the filter. All patterns within a pattern set will be used in request matching together without priority.

Part of the request to filter on Header

Header* User-Agent

Transformation Please select

Regex patterns to match to request*
☒ Create regex pattern set
☐ Use saved regex pattern set

New pattern set name*

+

[Create pattern set and add filter](#)

Filter in this regex match condition

Part of the request to filter on

This condition has no filters.

* Required

[Cancel](#) [Create](#)

Note that regex match conditions can also be utilized.

AWS WAF - Create rules

IP match condition created successfully.

Set up a web access control list (web ACL)

Concepts overview

Step 1: Name web ACL

Step 2: Create conditions

Step 3: Create rules

Step 4: Review and create

Create rules

Rules contain the conditions that you want to use to filter web requests. You add rules to a web ACL, and then specify whether you want to allow or block requests based on each rule.

Add rules to a web ACL

Rules:

Create new rule using IP match or string match conditions created in previous steps

If a request matches all of the conditions in a rule, take the corresponding action

Order	Rule	Action
1	myruledemo	<input type="radio"/> Allow <input checked="" type="radio"/> Block <input type="radio"/> Count

Create new rule using IP match or string match conditions created in previous steps

If a request doesn't match any rules, take the default action

Default action: ☐ Allow all requests that don't match any rules ☒ Block all requests that don't match any rules

* Required

Create rule

Specify the conditions that you want to use to filter web requests. If you add more than one condition to a rule, a request must match all of the conditions to be allowed or blocked based on that rule. [Learn more](#)

Name:

CloudWatch metric name:

Rule type:

Region:

Use global to create WAF resources that you would use with CloudFront distributions and other regions for WAF resources that you would use with ALBs in that region.

Add conditions

When a request does originate from a geographic location in geoAP

There is no filter in this geo match condition. [Edit](#)

And

When a request does originate from an IP address in blockCSUN

No IP addresses are in this IP match condition. [Edit](#)

* Required

A rule must be created to give meaning to the conditions.

AWS WAF - Create Rules

IP match condition created successfully.

Set up a web access control list (web ACL)

Concepts overview

Step 1: Name web ACL

Step 2: Create conditions

Step 3: Create rules

Step 4: Review and create

Create rules

Rules contain the conditions that you want to use to filter web requests. You add rules to a web ACL, and then specify whether you want to allow or block requests based on each rule. [Learn more](#)

Add rules to a web ACL

Rules:

Rule created successfully.

If a request matches all of the conditions in a rule, take the corresponding action

Order	Rule	Action
1	myruledemo	<input type="radio"/> Allow <input checked="" type="radio"/> Block <input type="radio"/> Count

If a request doesn't match any rules, take the default action

Default action: ☒ Allow all requests that don't match any rules ☐ Block all requests that don't match any rules

* Required

Concepts overview

Web ACL example if requests match

Rule 1, Bad User-Agents, then block

IP match condition
Suspicious IP's

and

String match condition
Bad bots

or if requests match

Rule 2, Detect SQLi, then block

SQL injection match condition
SQLi checks

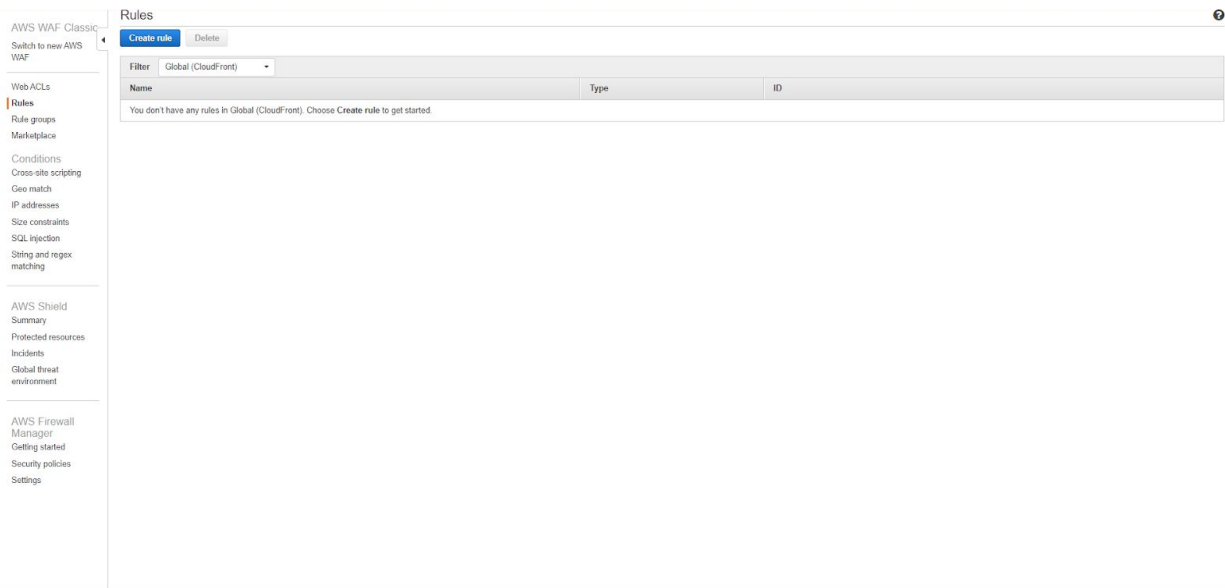
otherwise, perform the default action

Default action

Allow requests that don't match any rules

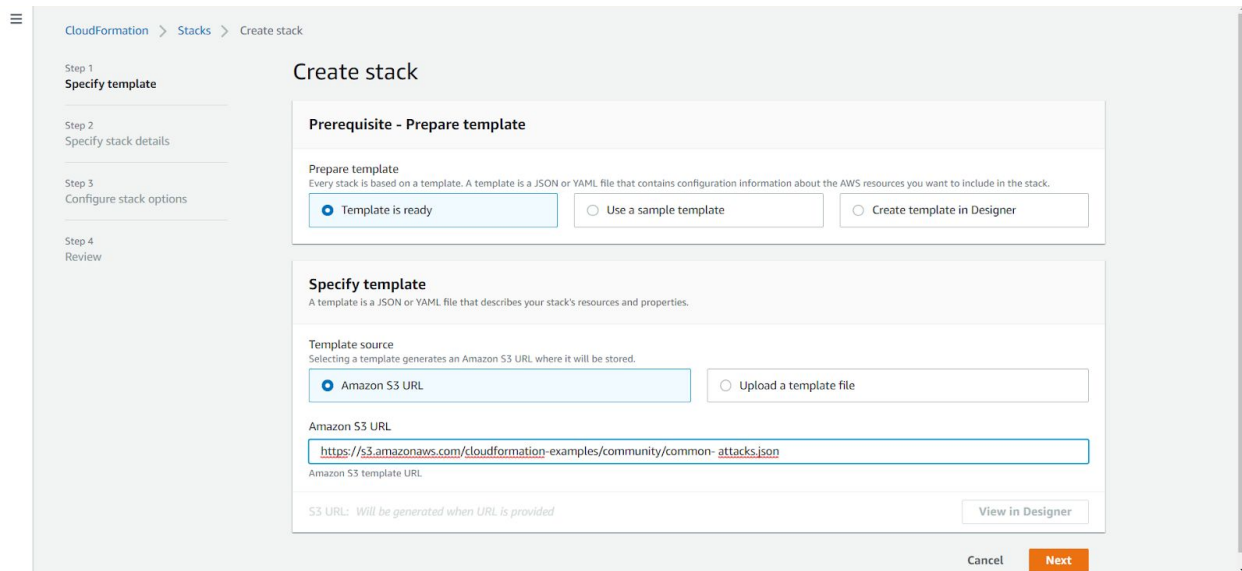
Note what actions are taken when a request matches all conditions in a rule. Conversely, note what will happen when a request does not match any rules.

AWS WAF Classic



All rules were deleted.

CloudFormation - Create Stack



Using CloudFormation, a tutorial template will be created that already contains the proper WAF settings.¹

¹ <https://s3.amazonaws.com/cloudformation-examples/community/common-attacks.json>

CloudFormation - Create stack

The screenshot shows the 'Specify stack details' step in the AWS CloudFormation console. On the left, a sidebar lists four steps: Step 1 (Specify template), Step 2 (Specify stack details), Step 3 (Configure stack options), and Step 4 (Review). The main area is titled 'Specify stack details' and contains two sections. The first section, 'Stack name', has a text input field with the value 'wafTutorial1' and a note stating: 'Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-)'. The second section, 'Parameters', is titled 'Web ACL Name for Common Attack Protection' and has a text input field with the value 'CommonAttackProtection'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

The stack is defined as wafTutorial1. All other settings left at default.

CloudFormation - Create stack

The screenshot shows the 'Configure stack options' step in the AWS CloudFormation console. On the left, a sidebar lists four steps: Step 1 (Specify template), Step 2 (Specify stack details), Step 3 (Configure stack options), and Step 4 (Review). The main area is titled 'Configure stack options' and contains three sections. The first section, 'Tags', has a table with two rows: one with 'department' as the key and 'dev' as the value, and another with 'Key' and 'Value' as placeholders. There is an 'Add tag' button and a 'Remove' button for each row. The second section, 'Permissions', is titled 'IAM role - optional' and has a dropdown menu for 'IAM role name' with 'Sample-role-name' selected, and a 'Remove' button. The third section, 'Advanced options', has three expandable sections: 'Stack policy', 'Rollback configuration', and 'Notification options'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

Tags established while no roles were set. CloudFormation will create one automatically.

CloudFormation - Create stack

CloudFormation > Stacks > Create stack

Step 1: Specify template

Template

Template URL
https://s3.amazonaws.com/cloudformation-examples/community/common-attacks.json

Stack description
Creates an AWS WAF configuration that protects against common attacks

Estimate cost

Step 2: Specify stack details

Parameters (1)

Search parameters

Key	Value
WebACLName	CommonAttackProtection

Step 3: Configure stack options

Tags (1)

Search tags

Key	Value
department	dev

The review page for the CloudFormation stack, wafTutorial1.

AWS WAF - Web ACLs

Associate CommonAttackProtection with CloudFront distribution

To associate this web ACL with an additional CloudFront distribution, choose a distribution from the list.

You can associate only one web ACL with a distribution. If a different web ACL is already associated with the selected distribution, the distribution configuration will be updated to use the current web ACL.

Resource type: CloudFront Distribution

Resource: E2VSP63GKOC325 - dmsoc2b3w...

Cancel Add

Web ACLs

Filter: Global (CloudFront)

Name: CommonAttackProtection

Rules

Type	Action
Regular	Block requests
Regular	Count requests
Regular	Block requests
Regular	Block requests

AWS resources using this web ACL

Resource	Type
No resource is using this web ACL.	

Once the CloudFormation stack is complete, to enable protections an association will be made with the CloudFront distribution.

AWS WAF - CommonAttackProtection WAF

CloudFront association added successfully.

Web ACLs

Create web ACL Delete

Filter: Global (CloudFront)

Name: CommonAttackProtection

CommonAttackProtection

Requests Rules Logging

If a request matches all of the conditions in a rule, take the corresponding action Edit web ACL

Order	Rule	Type	Action
1	CommonAttackProtectionManualIPBlockRule	Regular	Block requests
2	CommonAttackProtectionLargeBody/MatchRule	Regular	Count requests
3	CommonAttackProtectionSqlRule	Regular	Block requests
4	CommonAttackProtectionXssRule	Regular	Block requests

If a request doesn't match any rules, take the default action

Default action: Allow all requests that don't match any rules

The following rules within the rule group will be overridden to count

Rule group name	Status
No rules within the rule group will be overridden to count.	

AWS resources using this web ACL Add association

Resource	Type
EZVSP63GKOC325 - dmoozdhvsw01.cloudfront.net	CloudFront distribution

The CloudFront resource has been provisioned with the CommonAttackProtection WAF.

CloudFront - General tab

Cache statistics

Monitoring

Alarms

Popular objects

Top referers

Usage

Viewers

▼ Security

Origin access identity

Public key

Field-level encryption

Log Prefix: Web

Delivery Method: Off

Cookie Logging: InProgress

Distribution Status: Use All Edge Locations (Best Performance)

Comment: Price Class

AWS WAF: Web ACL: CommonAttackProtection (waf1)

State: Enabled

Alternate Domain Names (CNAMEs): Default CloudFront Certificate (*.cloudfront.net)

SSL Certificate: dmoozdhvsw01.cloudfront.net

Domain Name: Custom SSL Client Support: TLSv1

Security Policy: HTTP/2, HTTP/1.1, HTTP/1.0

Supported HTTP Versions: Enabled

IPv6: Default Root Object: 2020-05-25 20:45 UTC-7

Log Bucket:

To verify correct AWS WAF provisioning, check the CloudFront distribution created at the beginning of the lab. This WAF can be applied to other CloudFront projects.