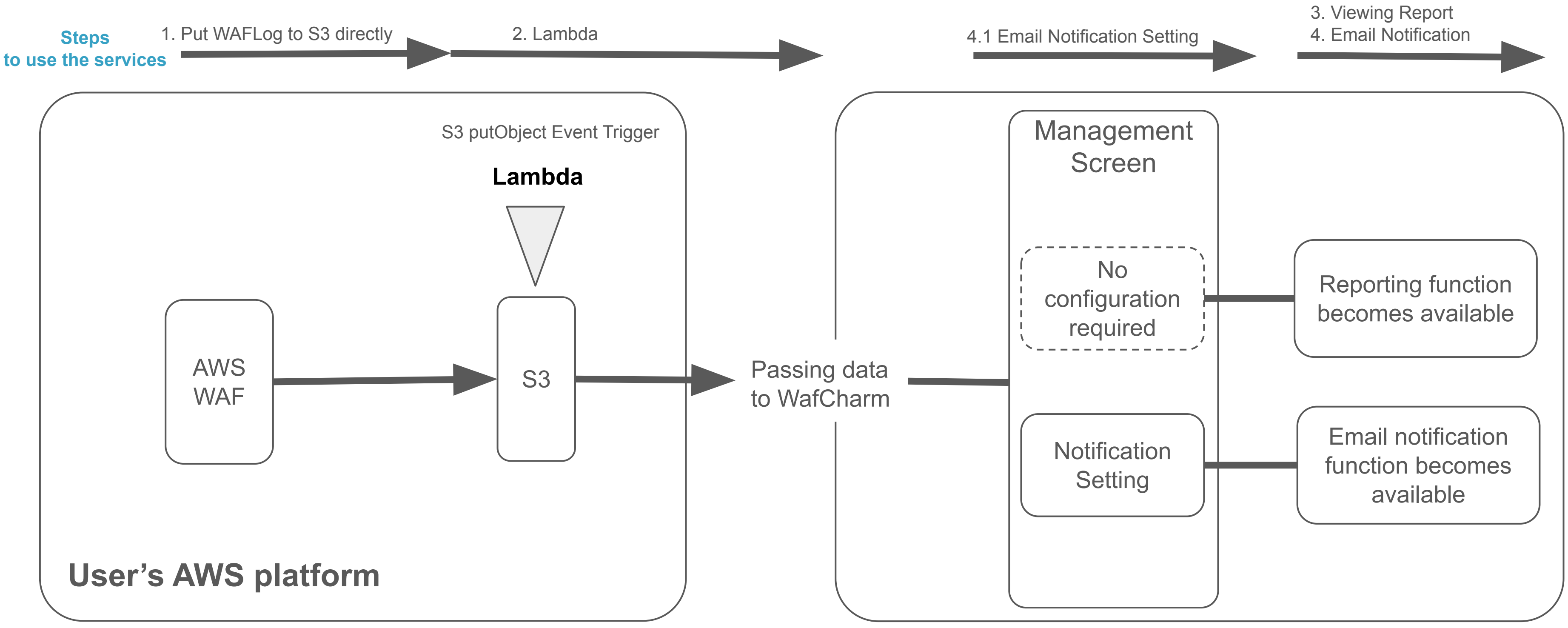
User Manual for
Reporting & Notification function
new AWS WAF (S3)
Ver 1.2

WafCharm

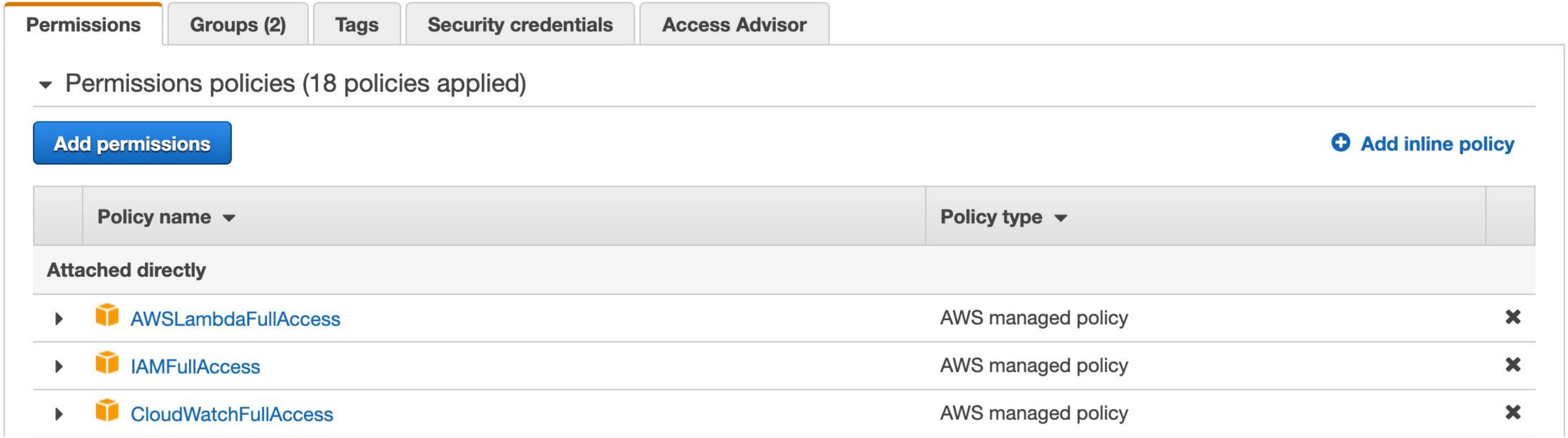
Architectural Overview of Reporting & Notification Function


Steps
to use the services
1. Put WAFLog to S3 directly
2. Lambda
4.1 Email Notification Setting
3. Viewing Report
4. Email Notification
S3 putObject Event Trigger
Lambda
AWS WAF
S3
User’s AWS platform
Passing data to WafCharm
Management Screen
No configuration required
Notification Setting
Reporting function becomes available
Email notification function becomes available

WafCharm

Authorization required to perform this procedure

This is an example of using the default permissions policies in AWS.



Permissions policies (18 policies applied)

Policy name	Policy type
Attached directly	
AWSLambdaFullAccess	AWS managed policy
IAMFullAccess	AWS managed policy
CloudWatchFullAccess	AWS managed policy

Operational Overview of
Reporting & Notification Function (1/2)

In order to use the reporting and notification features, you must first complete the following steps in your AWS environment.

1. Put WAFLog to S3 directly
    - Configure Logging and metrics of Web ACL
    - Create/Configure S3 bucket
    - Confirmation of completion of step 1
2. Lambda
    - Create the read permission policy for the WAFLog output destination S3
    - Create S3 put permission policy for WafCharm integration
    - Create a role for Lambda to integrate with WafCharm
    - Create/Configure Lambda
3. Using the reporting function
    - Viewing the monthly report on WafCharm management screen

Operational Overview of Reporting & Notification Function (2/2)

After completing steps 1 and 2, we recommend that you use the functions in accordance with this manual, as the items to be set are different for each function you want to use.

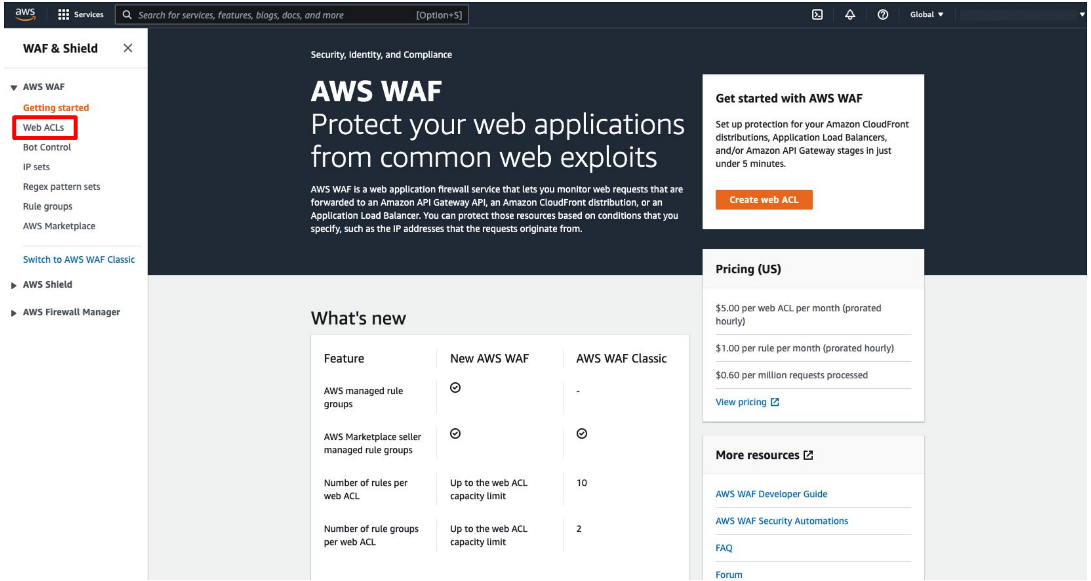
4. Using the email notification function
   - ○ Email notification destination setting
   - ○ Email notification setting
   - ○ Email notification content
5. Additional information about the notification function
6. Other additional information

1. Put WAFLog to S3 directly

Set up Logging and metrics of Web ACL to put WAFLog to S3 directly

- Configure Logging and metrics of Web ACL
- Create/Configure S3 bucket
- Confirmation of completion of step 1

1.1. Configure Logging and metrics of Web ACL



Security, Identity, and Compliance

AWS WAF

Protect your web applications from common web exploits

AWS WAF is a web application firewall service that lets you monitor web requests that are forwarded to an Amazon API Gateway API, an Amazon CloudFront distribution, or an Application Load Balancer. You can protect those resources based on conditions that you specify, such as the IP addresses that the requests originate from.

Get started with AWS WAF

Set up protection for your Amazon CloudFront distributions, Application Load Balancers, and/or Amazon API Gateway stages in just under 5 minutes.

Pricing (US)

$5.00 per web ACL per month (prorated hourly)

$1.00 per rule per month (prorated hourly)

$0.60 per million requests processed

More resources

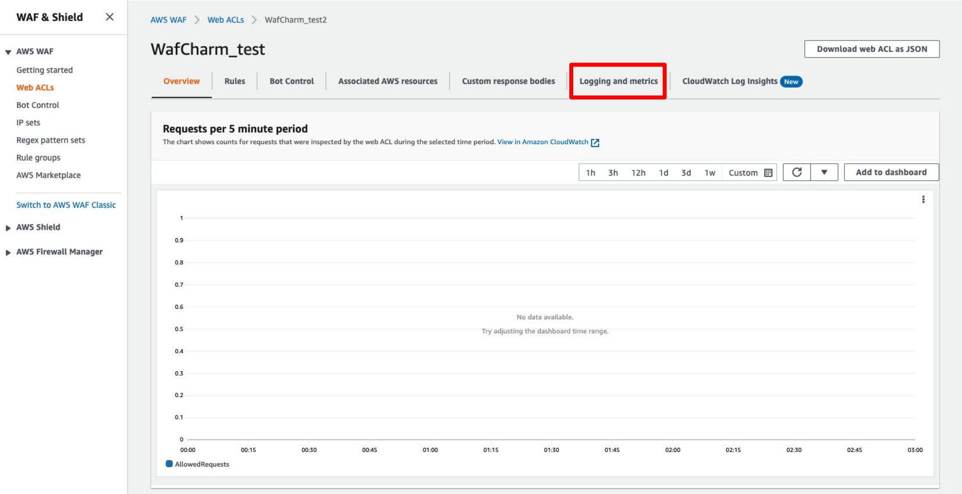
What's new

Feature	New AWS WAF	AWS WAF Classic
AWS managed rule groups	✓	-
AWS Marketplace seller managed rule groups	✓	✓
Number of rules per web ACL	Up to the web ACL capacity limit	10
Number of rule groups per web ACL	Up to the web ACL capacity limit	2

Search「WAF & Shield」in AWS Console

Click「Web ACLs」

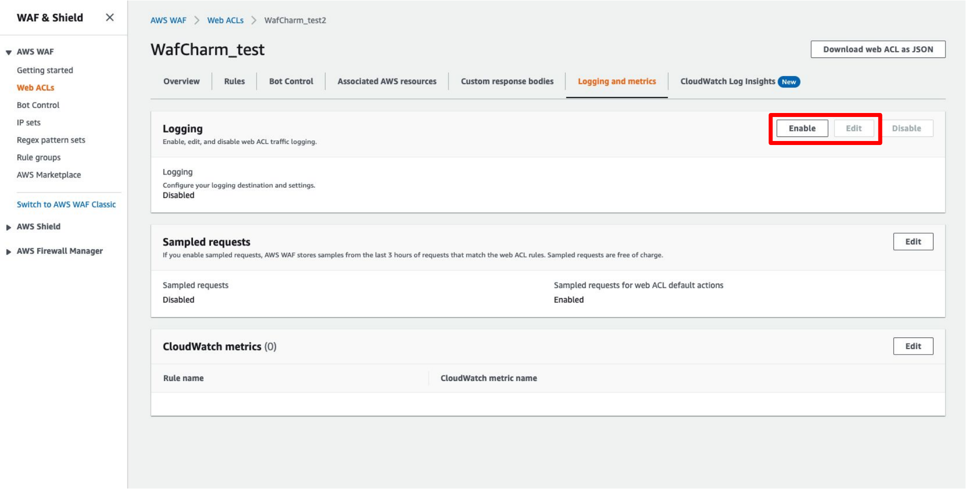
1.2. Configure Logging and metrics of Web ACL



Select Web ACL which you want to configure

Click「Logging and metrics」

1.3. Configure Logging and metrics of Web ACL



WafCharm_test

Logging

Enable, edit, and disable web ACL traffic logging.

Logging

Configure your logging destination and settings.

Disabled

Sampled requests

If you enable sampled requests, AWS WAF stores samples from the last 3 hours of requests that match the web ACL rules. Sampled requests are free of charge.

Sampled requests	Sampled requests for web ACL default actions
Disabled	Enabled

CloudWatch metrics (0)

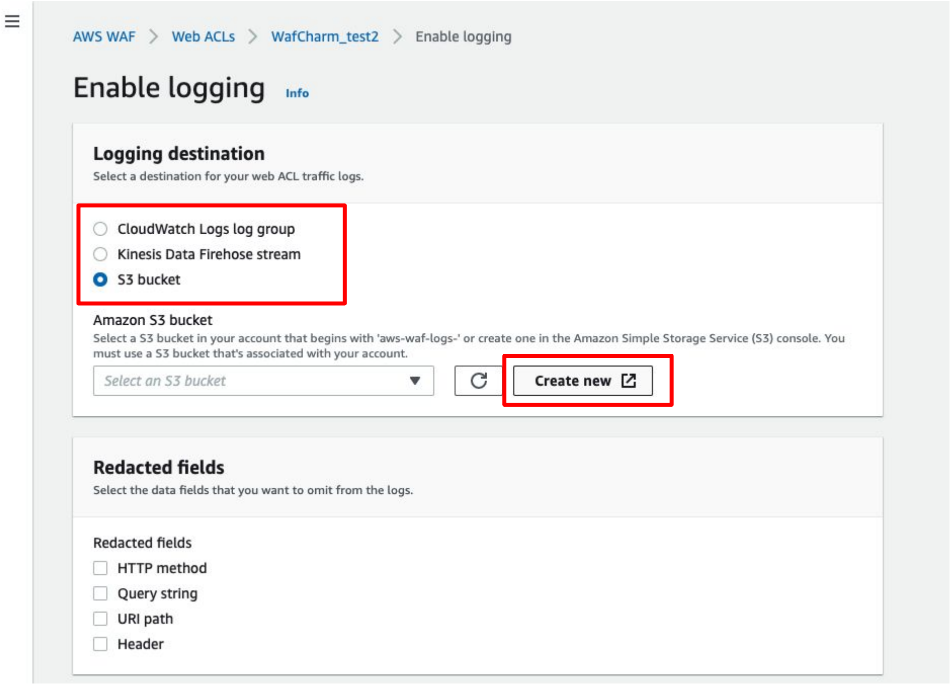
Rule name	CloudWatch metric name

Click「Enable」

※ If you had any configuration before,

Click「Edit」

1.4. Configure Logging and metrics of Web ACL



Enable logging Info

Logging destination

Select a destination for your web ACL traffic logs.

○ CloudWatch Logs log group
○ Kinesis Data Firehose stream
● S3 bucket

Amazon S3 bucket

Select a S3 bucket in your account that begins with 'aws-waf-logs-' or create one in the Amazon Simple Storage Service (S3) console. You must use a S3 bucket that's associated with your account.

Redacted fields

Select the data fields that you want to omit from the logs.

Redacted fields
□ HTTP method
□ Query string
□ URI path
□ Header

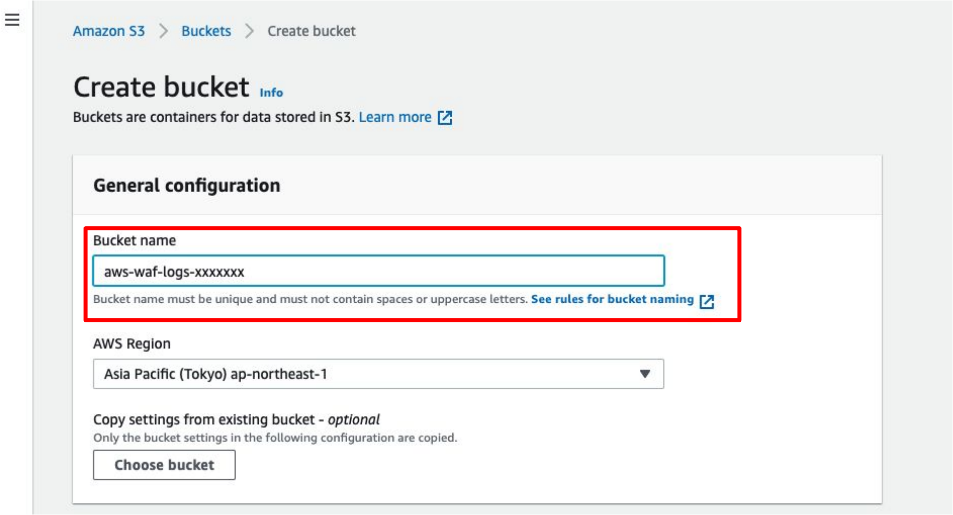
Logging destination:

Select「S3 bucket」

Amazon S3 bucket:

Click「Create new」

1.5. Create/Configure S3 bucket



Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

aws-waf-logs-xxxxxxx

Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

Asia Pacific (Tokyo) ap-northeast-1

Copy settings from existing bucket - *optional*

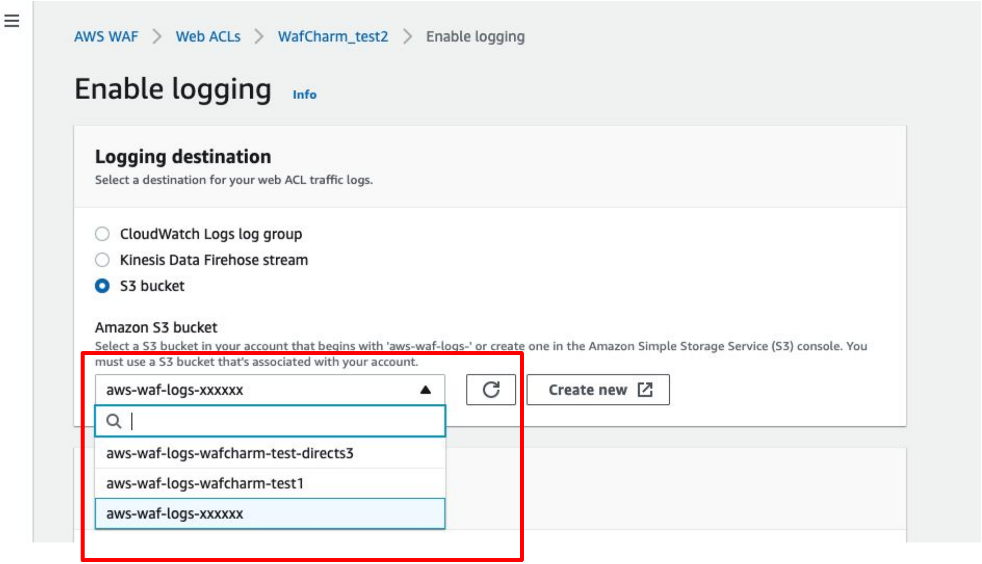
Only the bucket settings in the following configuration are copied.

Bucket name:

aws-waf-logs-<Random Name>

※ Please note that the “Bucket name” should have "aws-waf-logs-" added as a prefix.

1.6. Create/Configure S3 bucket



AWS WAF > Web ACLs > WafCharm_test2 > Enable logging

Enable logging Info

Logging destination

Select a destination for your web ACL traffic logs.

○ CloudWatch Logs log group
○ Kinesis Data Firehose stream
● S3 bucket

Amazon S3 bucket

Select a S3 bucket in your account that begins with 'aws-waf-logs-' or create one in the Amazon Simple Storage Service (S3) console. You must use a S3 bucket that's associated with your account.

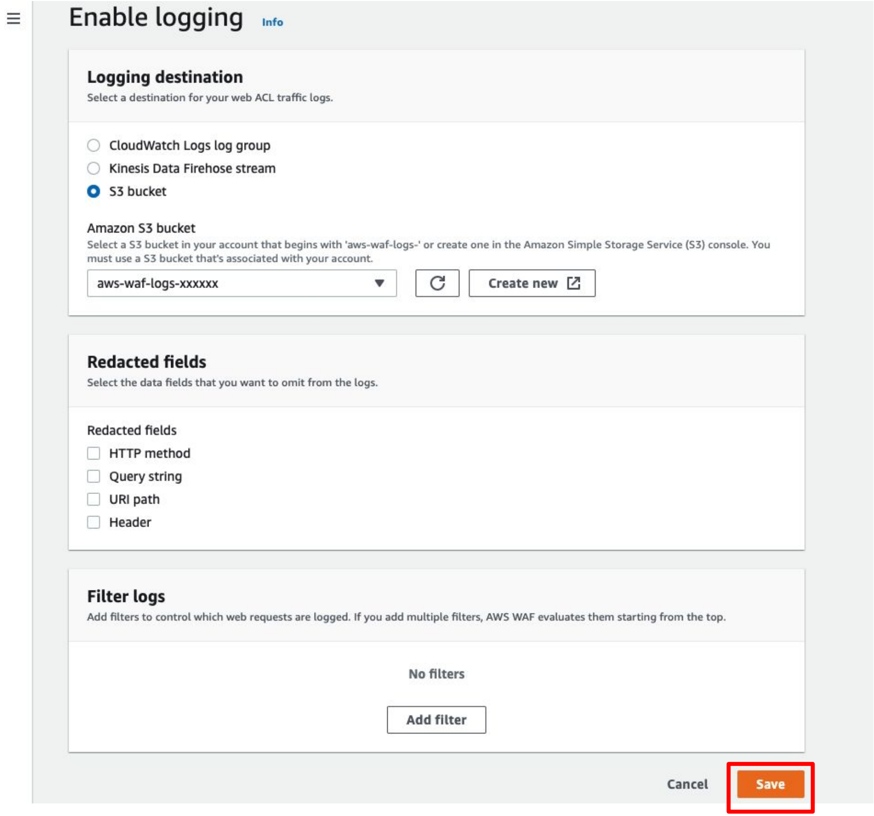
aws-waf-logs-xxxxxx ▲

aws-waf-logs-wafcharm-test-directs3
aws-waf-logs-wafcharm-test1
aws-waf-logs-xxxxxx

Return to “Enable logging”

Select the S3 bucket setup in 1.5

1.7. Create/Configure S3 bucket



Enable logging

Logging destination

Select a destination for your web ACL traffic logs.

○ CloudWatch Logs log group
○ Kinesis Data Firehose stream
● S3 bucket

Amazon S3 bucket

Select a S3 bucket in your account that begins with 'aws-waf-logs-' or create one in the Amazon Simple Storage Service (S3) console. You must use a S3 bucket that's associated with your account.

aws-waf-logs-xxxxxx

Redacted fields

Select the data fields that you want to omit from the logs.

Redacted fields

□ HTTP method
□ Query string
□ URI path
□ Header

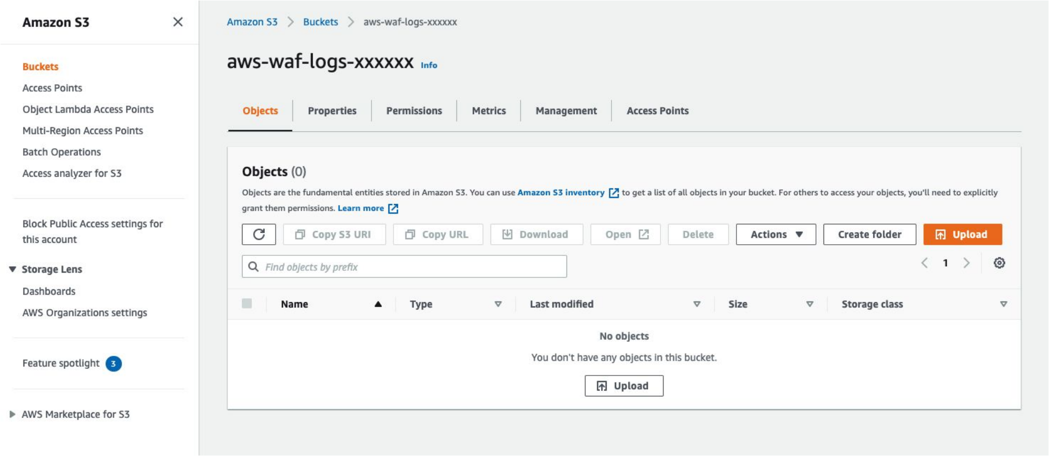
Filter logs

Add filters to control which web requests are logged. If you add multiple filters, AWS WAF evaluates them starting from the top.

No filters

「Save」to complete configuration of 1st chapter, Put WAFLog to S3 directly

1.8. Confirmation of completion of 1st chapter



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

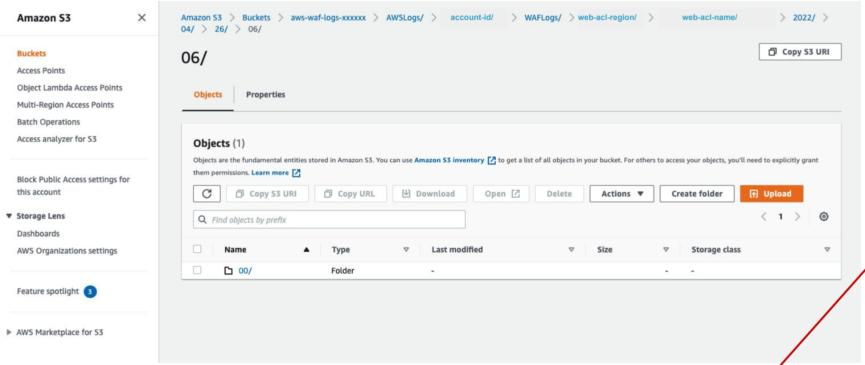
No objects

You don't have any objects in this bucket.

Check if full log file is generated in S3

In the screenshot on the left, no detection has been made yet and no file has been generated.

1.9. Confirmation of completion of 1st chapter

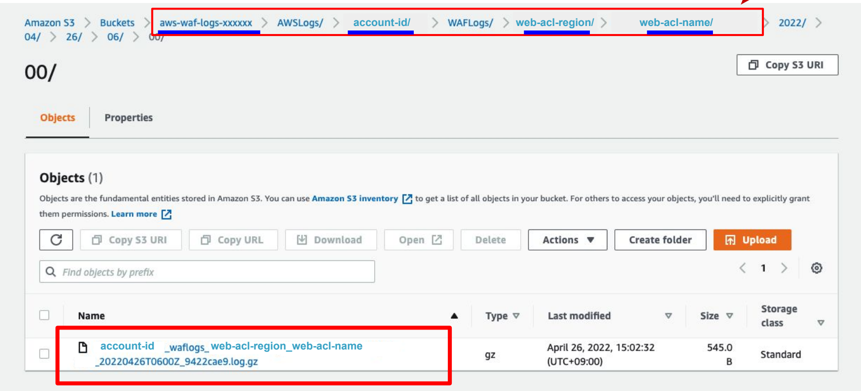

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets > aws-waf-logs-xxxxxx > AWSLogs/ > account-id/ > WAFLogs/ > web-acl-region/ > web-acl-name/ > 2022/ > 04/ > 26/ > 06/
Copy S3 URI
Objects
Properties
Copy S3 URI
Copy URL
Download
Open
Delete
Actions ▼
Create folder
Upload
Find objects by prefix
1

06/

Objects (1)

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

□	Name ▲	Type	Last modified	Size	Storage class
□	00/	Folder	-	-	-


Amazon S3 > Buckets > aws-waf-logs-xxxxxx > AWSLogs/ > account-id/ > WAFLogs/ > web-acl-region/ > web-acl-name/ > 2022/ > 04/ > 26/ > 06/ > 00/
Copy S3 URI
Objects
Properties
Copy S3 URI
Copy URL
Download
Open
Delete
Actions ▼
Create folder
Upload
Find objects by prefix
1

00/

Objects (1)

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

□	Name ▲	Type	Last modified	Size	Storage class
□	account-id _waflogs_ web-acl-region_web-acl-name _20220426T0600Z_9422cae9.log.gz	gz	April 26, 2022, 15:02:32 (UTC+09:00)	545.0 B	Standard

※ we will use this path information at 2.2, 2.11

The blue line will vary depending on your environment

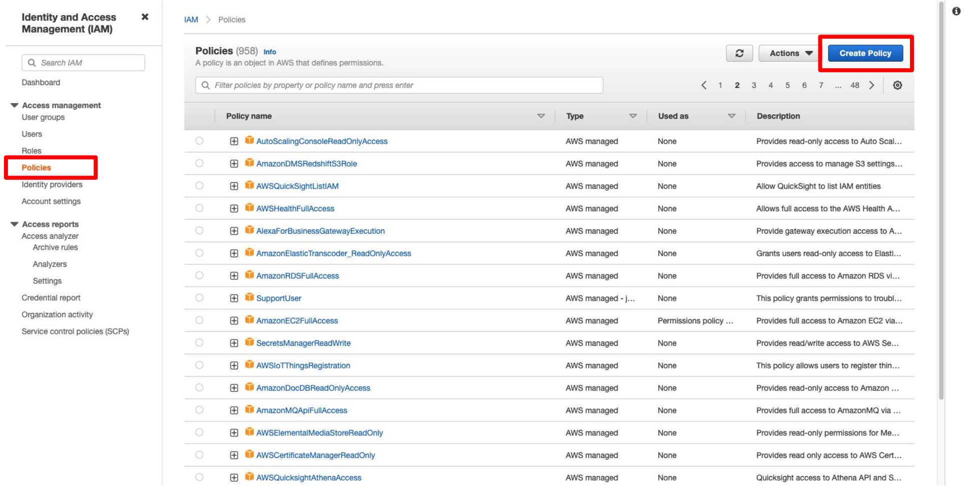
Once a file like the one on the left screen is generated, first chapter of the setup is complete.

2. Lambda

Setup for transferring the output file in S3 on the user side to S3 on the CSC side.

- Create the read permission policy for the WAFLog output destination (User side S3)
- Create put permission policy for WafCharm integration (CSC side S3)
- Create a role for Lambda to integrate with WafCharm
- Create/Configure Lambda
- Change CloudWatch log settings (Lambda output log) * Optional

2.1. Create read permission policy for WAFLog output destination S3



Policies (958) Info

A policy is an object in AWS that defines permissions.

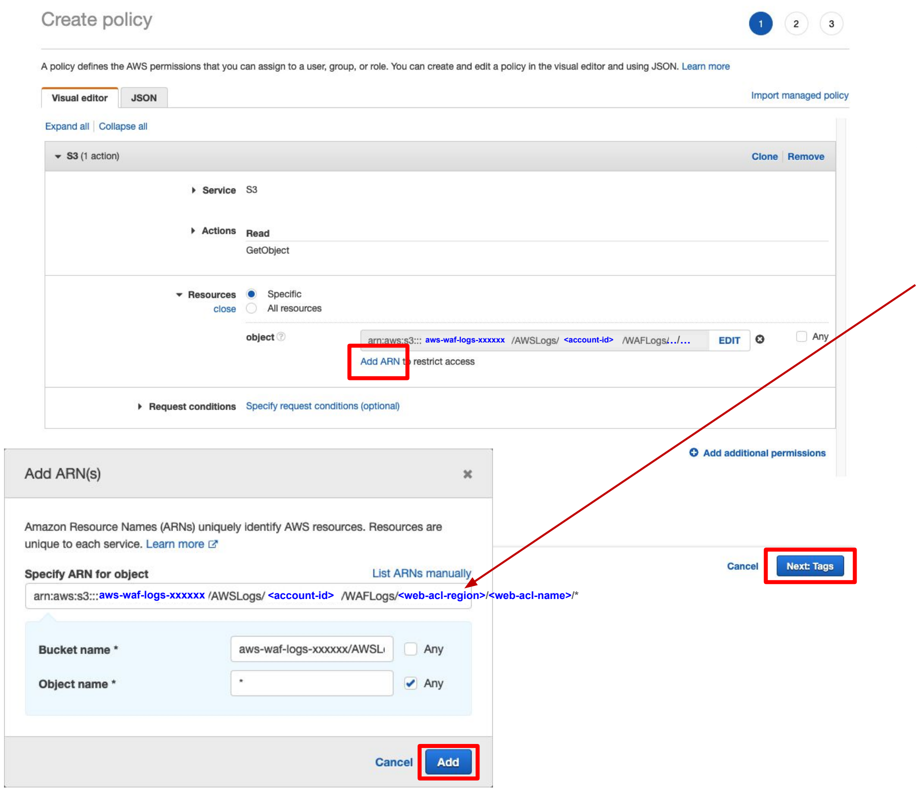
Filter policies by property or policy name and press enter

	Policy name	Type	Used as	Description
○	AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only access to Auto Scal...
○	AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manage S3 settings...
○	AWSQuickSightListIAM	AWS managed	None	Allow QuickSight to list IAM entities
○	AWSHealthFullAccess	AWS managed	None	Allows full access to the AWS Health A...
○	AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to A...
○	AmazonElasticTranscoder_ReadOnlyAccess	AWS managed	None	Grants users read-only access to Elasti...
○	AmazonRDSFullAccess	AWS managed	None	Provides full access to Amazon RDS vi...
○	SupportUser	AWS managed - j...	None	This policy grants permissions to troubl...
○	AmazonEC2FullAccess	AWS managed	Permissions policy ...	Provides full access to Amazon EC2 via...
○	SecretsManagerReadWrite	AWS managed	None	Provides read/write access to AWS Se...
○	AWSIoTThingsRegistration	AWS managed	None	This policy allows users to register thin...
○	AmazonDocDBReadOnlyAccess	AWS managed	None	Provides read-only access to Amazon ...
○	AmazonMQApiFullAccess	AWS managed	None	Provides full access to AmazonMQ via ...
○	AWSElementalMediaStoreReadOnly	AWS managed	None	Provides read-only permissions for Me...
○	AWSCertificateManagerReadOnly	AWS managed	None	Provides read only access to AWS Cert...
○	AWSQuicksightAthenaAccess	AWS managed	None	Quicksight access to Athena API and S...

From the “IAM” service,

Select “Policy” > “Create policy”

2.2. Create read permission policy for WAFLog output destination S3



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Service S3

Actions Read
GetObject

Resources ● Specific ○ All resources
close

object arn:aws:s3::: aws-waf-logs-xxxxxx /AWSLogs/ <account-id> /WAFLogs/…/… EDIT □ Any

Add ARN to restrict access

Request conditions Specify request conditions (optional)

Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for object

arn:aws:s3:::aws-waf-logs-xxxxxx /AWSLogs/ <account-id> /WAFLogs/<web-acl-region>/<web-acl-name>/*

Bucket name * aws-waf-logs-xxxxxx/AWSL □ Any

Object name * * ☑ Any

Service : S3

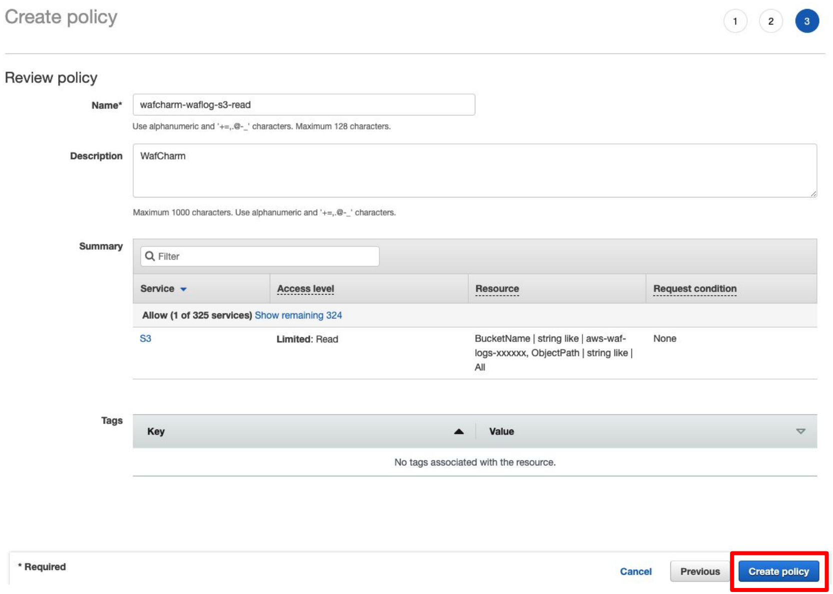
Action : GetObject

Resources :
arn:aws:s3:::aws-waf-logs-xxxxxx/AWSLogs/<account-id>/WAFLogs/<web-acl-region>/<web-acl-name>/*
※ As path information in 1.9, please edit the blue area to suit your environment

※ Make sure to add “ /* ” to the path specified in Resources

Click「Add」
Click「Next: Tags」→ Click「Review policy」

2.3. Create read permission policy for WAFLog output destination S3



Review policy

Name* wafcharm-waflog-s3-read

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description WafCharm

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 325 services) Show remaining 324			
S3	Limited: Read	BucketName | string like | aws-waf-logs-xxxxxx, ObjectPath | string like | All	None

Tags

Key	Value
No tags associated with the resource.	

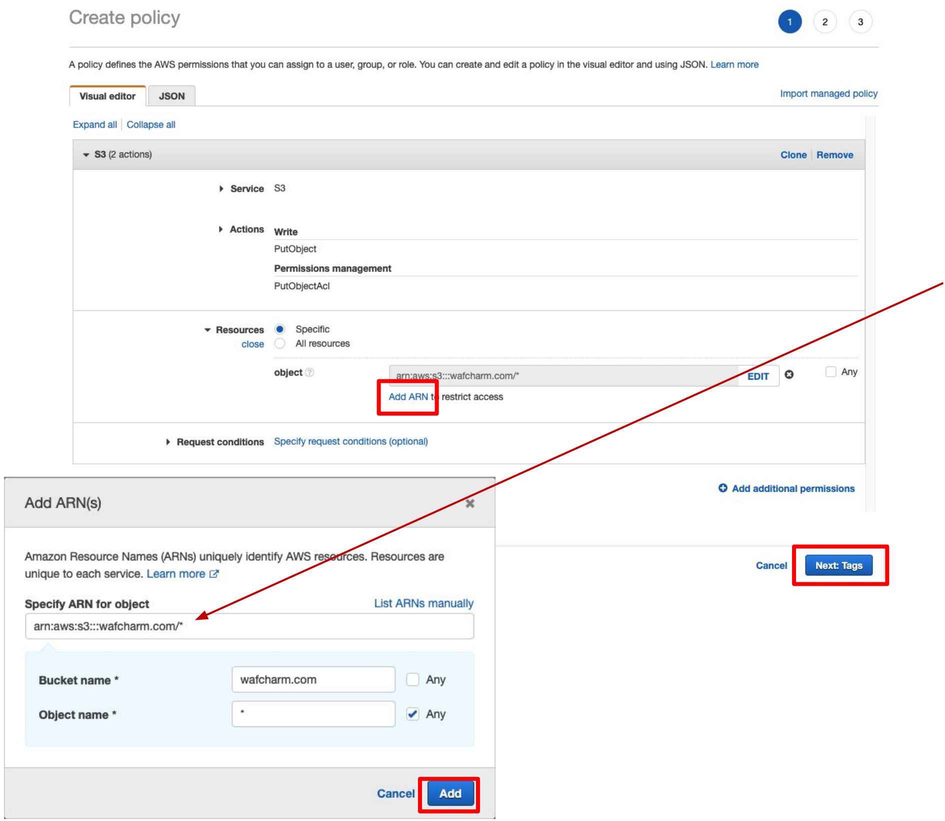
* Required

Name :
wafcharm-waflog-s3-read (Any name)

Description : WafCharm (Arbitrary)

Click「Create policy」

2.4. Create put permission policy for WafCharm integration



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

▾ S3 (2 actions)

▸ Service S3

▸ Actions
Write
PutObject
Permissions management
PutObjectAcl

▾ Resources close
● Specific
○ All resources

object: arn:aws:s3:::wafcharm.com/* EDIT ☐ Any

Add ARN to restrict access

▸ Request conditions Specify request conditions (optional)

Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for object — List ARNs manually

arn:aws:s3:::wafcharm.com/*

Bucket name * wafcharm.com ☐ Any

Object name * * ☑ Any

Service : S3

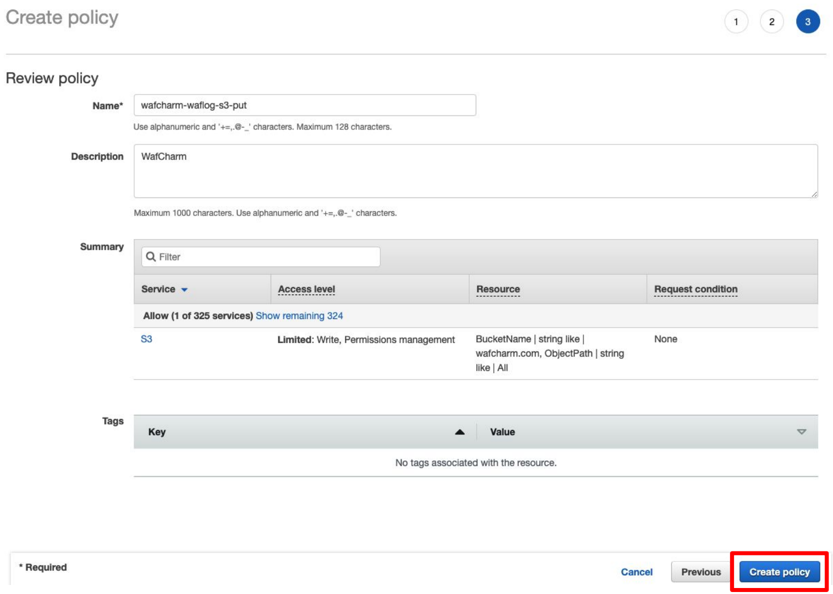
Action : PutObject, PutObjectACL

Resources :
arn:aws:s3:::wafcharm.com/*

※ Access permission to S3 on CSC side

Click「Add」
Click「Next: Tags」→ Click「Review policy」

2.5. Create put permission policy for WafCharm integration



Create policy

Review policy

Name* wafcharm-waflog-s3-put

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description WafCharm

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 325 services) Show remaining 324			
S3	**Limited:** Write, Permissions management	BucketName | string like | wafcharm.com, ObjectPath | string like | All	None

Tags

Key	Value
No tags associated with the resource.	

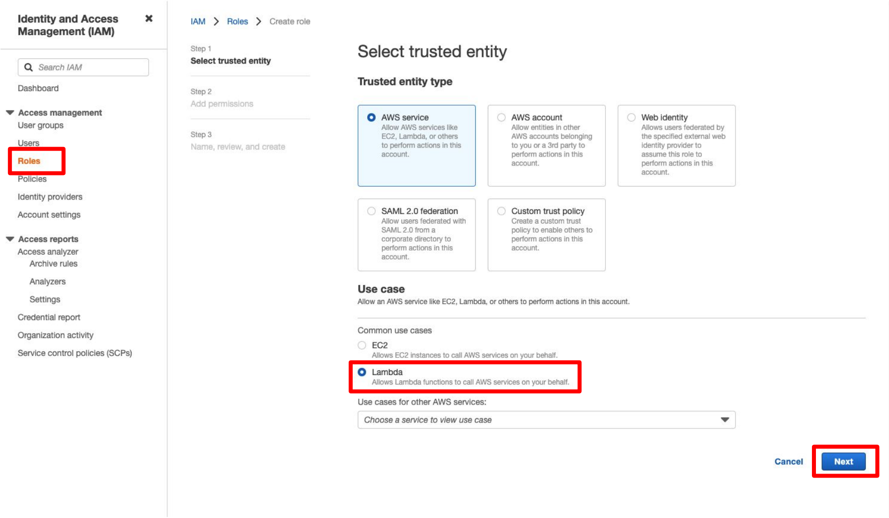
* Required

Name :
wafcharm-waflog-s3-put (Any name)

Description : WafCharm (Arbitrary)

「Create policy」

2.6. Create a role for Lambda to integrate with WafCharm



Select trusted entity

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

○ EC2
Allows EC2 instances to call AWS services on your behalf.

● Lambda
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Choose a service to view use case

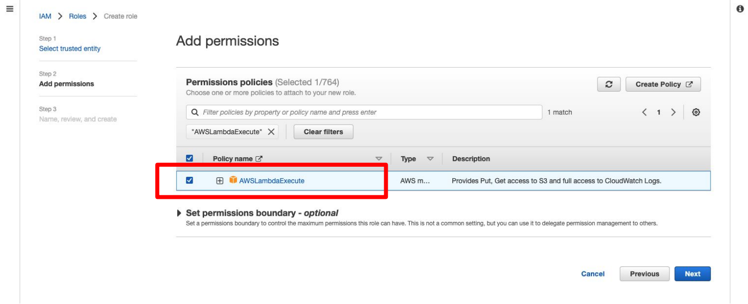
From the “IAM” service,

Select “Roles” > “Create role”

Select「Lambda」for Use case

Click「Next」

2.7. Create a role for Lambda to integrate with WafCharm



Add permissions

Permissions policies (Selected 1/764)

Choose one or more policies to attach to your new role.

"AWSLambdaExecute" — 1 match

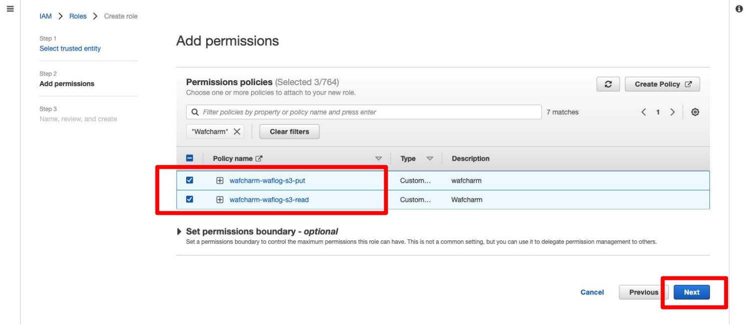
☑	Policy name	Type	Description
☑	AWSLambdaExecute	AWS m...	Provides Put, Get access to S3 and full access to CloudWatch Logs.

Set permissions boundary - *optional*

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Enter「AWSLambdaExecute」in Filter policies and

Select「AWSLambdaExecute」from the list.



Add permissions

Permissions policies (Selected 3/764)

Choose one or more policies to attach to your new role.

"Wafcharm" — 7 matches

▬	Policy name	Type	Description
☑	wafcharm-waflog-s3-put	Custom...	wafcharm
☑	wafcharm-waflog-s3-read	Custom...	Wafcharm

Set permissions boundary - *optional*

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

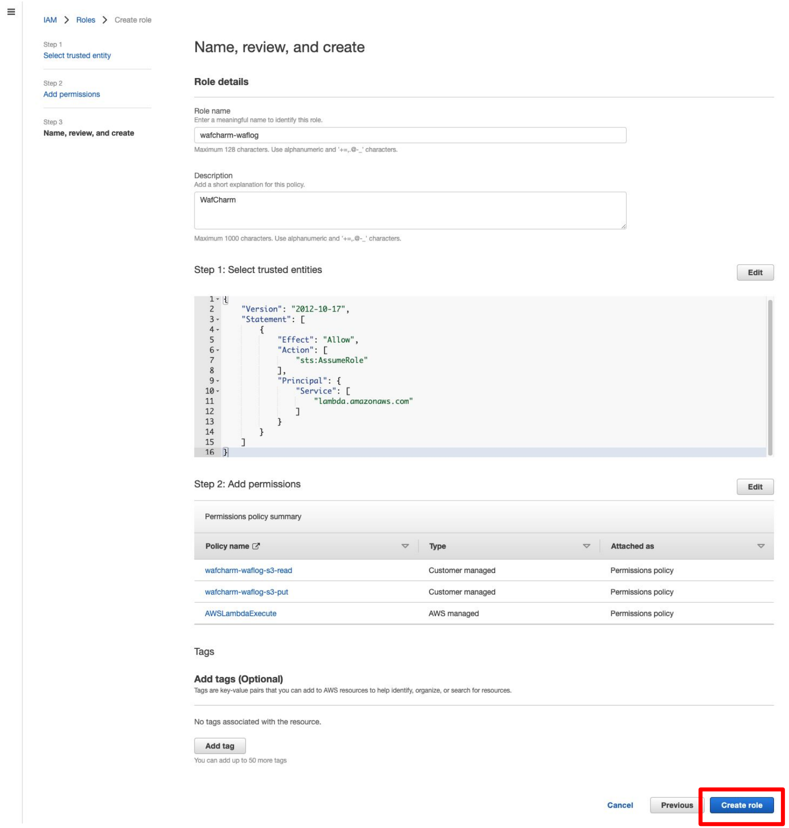
Enter「wafcharm」in Filter policies and select the following from the list.

「wafcharm-waflog-s3-put」
「wafcharm-waflog-s3-read」

※ Policies created in 2.3 and 2.5

Click「Next」

2.8. Create a role for Lambda to integrate with WafCharm



Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
wafcharm-waflog
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this policy.
WafCharm
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            }
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
wafcharm-waflog-s3-read	Customer managed	Permissions policy
wafcharm-waflog-s3-put	Customer managed	Permissions policy
AWSLambdaExecute	AWS managed	Permissions policy

Tags

Add tags (Optional)
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags

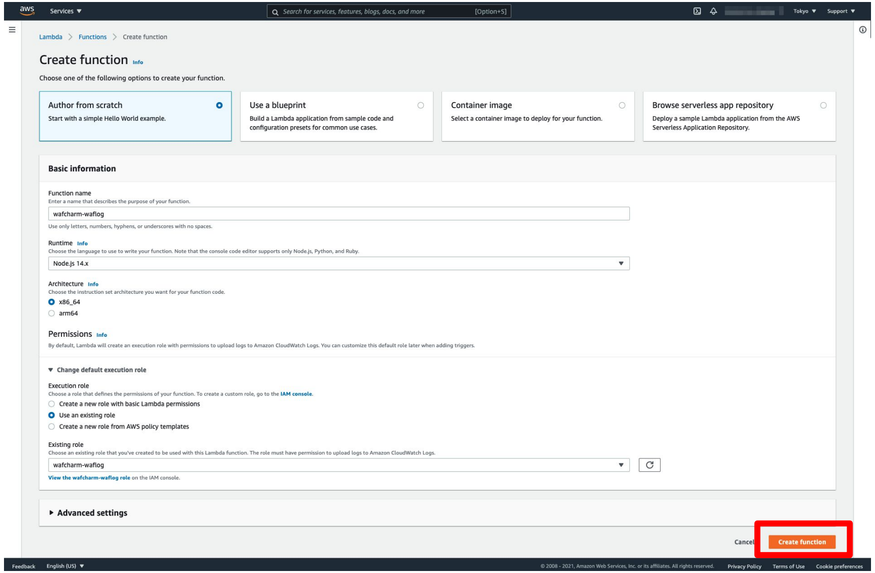
Role name:
wafcharm-waflog (Arbitrary)

Role description :
WafCharm (Arbitrary)

Adding tags is optional.

Click「Create role」

2.9. Create Lambda



Lambda > Functions > Create function

Create function Info

Choose one of the following options to create your function.

- ● Author from scratch — Start with a simple Hello World example.
- ○ Use a blueprint — Build a Lambda application from sample code and configuration presets for common use cases.
- ○ Container image — Select a container image to deploy for your function.
- ○ Browse serverless app repository — Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

Function name
Enter a name that describes the purpose of your function.
wafcharm-waflog
Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.
Node.js 14.x

Architecture Info
Choose the instruction set architecture you want for your function code.
● x86_64
○ arm64

Permissions Info
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

▼ Change default execution role

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.
○ Create a new role with basic Lambda permissions
● Use an existing role
○ Create a new role from AWS policy templates

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.
wafcharm-waflog
View the wafcharm-waflog role on the IAM console.

▶ Advanced settings

aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
Tokyo
Support
Cancel
Create function
Feedback
English (US)
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences

Function name : wafcharm-waflog (Arbitrary)

Runtime : Node.js 12.x ~ Node.js 18.x

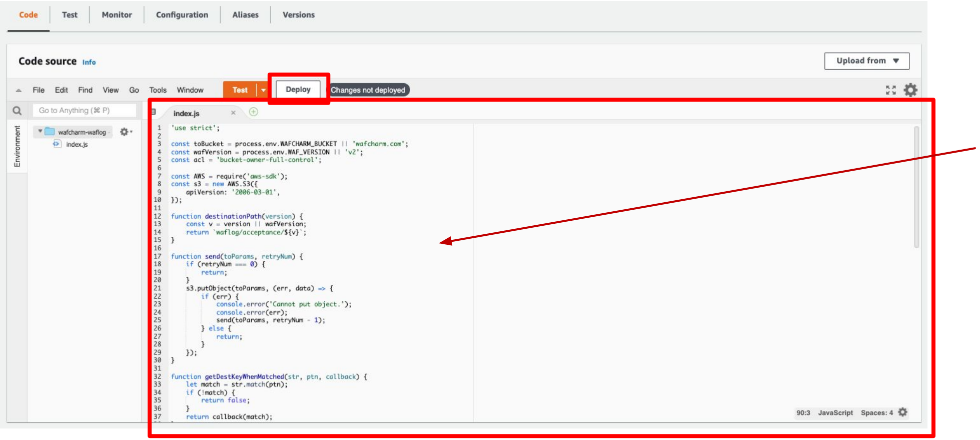
Execution Role : Use an existing role

Existing Role : wafcharm-waflog
※ Created in 2.8

※ Make sure to create it in the same region as the S3 bucket specified in 1.6

Click「Create function」

2.10. Create Lambda (Code Source)



```
'use strict';

const toBucket = process.env.WAFCHARM_BUCKET || 'wafcharm.com';
const wafVersion = process.env.WAF_VERSION || 'v2';
const acl = 'bucket-owner-full-control';

const AWS = require('aws-sdk');
const s3 = new AWS.S3({
    apiVersion: '2006-03-01',
});

function destinationPath(version) {
    const v = version || wafVersion;
    return `waflog/acceptance/${v}`;
}

function send(toParams, retryNum) {
    if (retryNum === 0) {
        return;
    }
    s3.putObject(toParams, (err, data) => {
        if (err) {
            console.error('Cannot put object.');
            console.error(err);
            send(toParams, retryNum - 1);
        } else {
            return;
        }
    });
}

function getDestKeyWhenMatched(str, ptn, callback) {
    let match = str.match(ptn);
    if (!match) {
        return false;
    }
    return callback(match);
```

Code source:

Paste the following source code

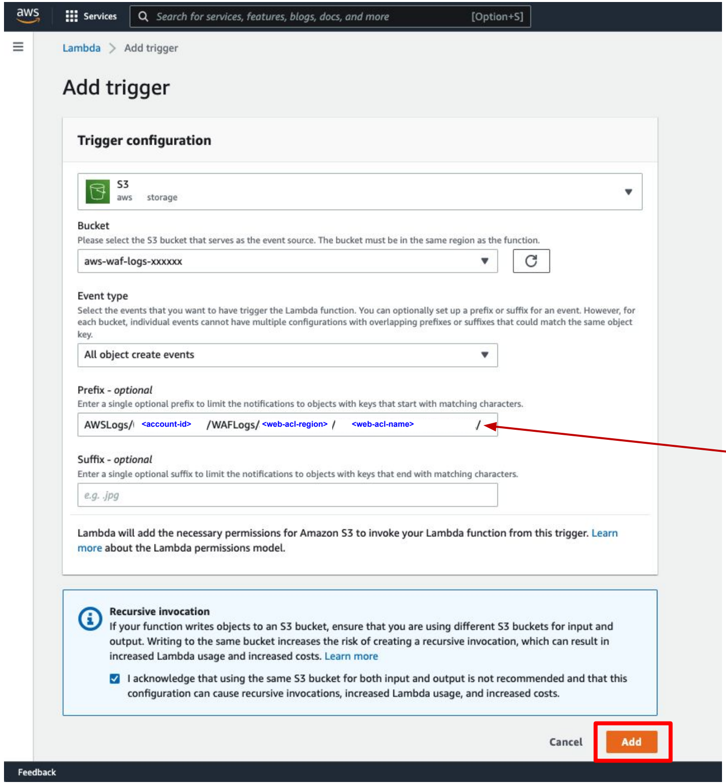
http://docs.wafcharm.com/manual/new_aws_waf/index.js

※ Be careful that the source varies depending on the version of AWS WAF

※ Rename the filename of the code from index.mjs to index.js if you are using Node.js 18.x.

Click「Deploy」

2.11. Create Lambda (Trigger)



Add trigger

Trigger configuration

S3
aws storage

Bucket
Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.
aws-waf-logs-xxxxxx

Event type
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.
All object create events

Prefix - *optional*
Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters.
AWSLogs/ <account-id> /WAFLogs/ <web-acl-region> / <web-acl-name> /

Suffix - *optional*
Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters.
e.g. .jpg

Lambda will add the necessary permissions for Amazon S3 to invoke your Lambda function from this trigger. Learn more about the Lambda permissions model.

Recursive invocation
If your function writes objects to an S3 bucket, ensure that you are using different S3 buckets for input and output. Writing to the same bucket increases the risk of creating a recursive invocation, which can result in increased Lambda usage and increased costs. Learn more

☑ I acknowledge that using the same S3 bucket for both input and output is not recommended and that this configuration can cause recursive invocations, increased Lambda usage, and increased costs.

Add trigger :
Select S3 as trigger

Bucket: Select the S3 bucket setup in 1.6

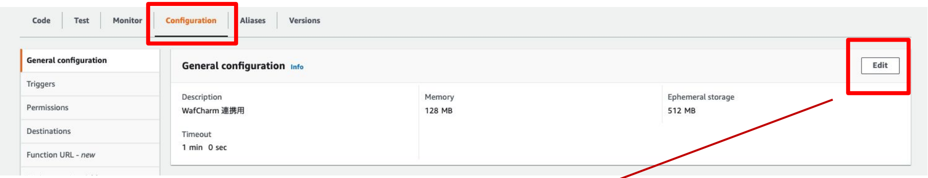
Event Type: Select “All object create events”

Prefix :
AWSLogs/<account-id>/WAFLogs/<web-acl-region>/<web-acl-name>/

※ As path information in 1.9, please edit the blue area to suit your environment

Click「Add」

2.12. Create Lambda



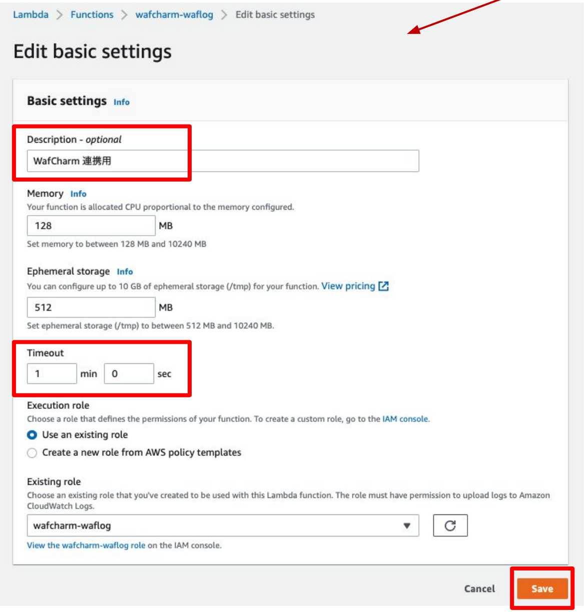
General configuration Info

Description
WafCharm 連携用

Memory
128 MB

Ephemeral storage
512 MB

Timeout
1 min 0 sec



Edit basic settings

Basic settings Info

Description - *optional*
WafCharm 連携用

Memory Info
Your function is allocated CPU proportional to the memory configured.
128 MB
Set memory to between 128 MB and 10240 MB

Ephemeral storage Info
You can configure up to 10 GB of ephemeral storage (/tmp) for your function. View pricing
512 MB
Set ephemeral storage (/tmp) to between 512 MB and 10240 MB.

Timeout
1 min 0 sec

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.
● Use an existing role
○ Create a new role from AWS policy templates

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.
wafcharm-waflog
View the wafcharm-waflog role on the IAM console.

Click「Configuration」

Click「General configuration」

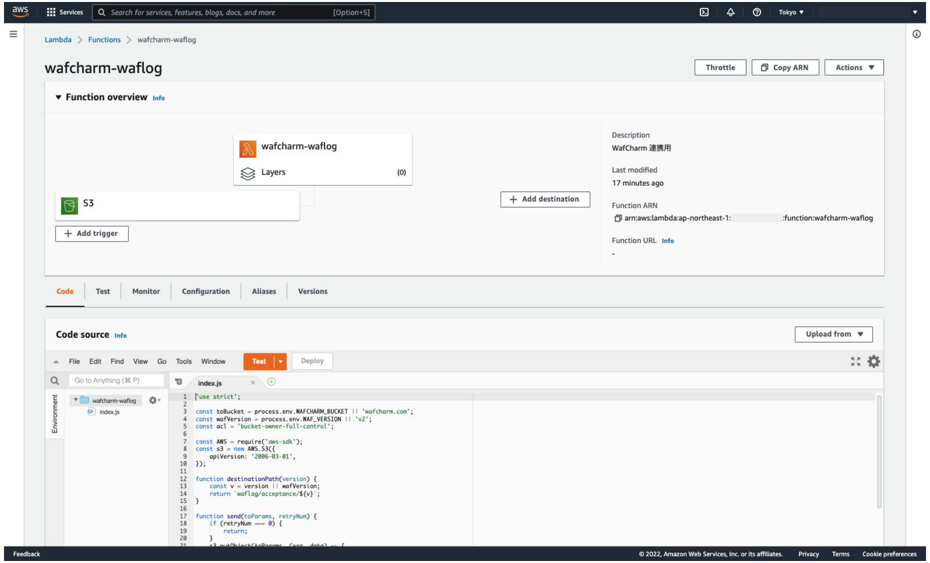
Click「Edit」

Description : For WafCharm integration(Arbitrary)

Timeout : 1 min

Click「Save」

2.13. Create Lambda



wafcharm-waflog

Description
WafCharm 連携用

Last modified
17 minutes ago

Function ARN
arn:aws:lambda:ap-northeast-1: :function:wafcharm-waflog

Function URL Info
-

Code source Info

index.js

```
'use strict';

const toBucket = process.env.WAFCHARM_BUCKET || 'wafcharm.com';
const wafVersion = process.env.WAF_VERSION || 'v2';
const acl = 'bucket-owner-full-control';

const AWS = require('aws-sdk');
const s3 = new AWS.S3({
    apiVersion: '2006-03-01',
});

function destinationPath(version) {
    const v = version || wafVersion;
    return `waflog/acceptance/${v}`;
}

function send(toParams, retryNum) {
    if (retryNum === 0) {
        return;
    }
    s3.putObject(toParams, (err, data) => {
```

Complete

2.14. CloudWatch

It is not created until after the Lambda function is executed.

Select AWS console > CloudWatch > Log

Since the default value of “Invalidate event after next period of time” is set as,

Default Value：“Never expire”

Please change the retention period of the log as necessary.

3. Using the reporting function

The following conditions must be met in order to use the monthly report function.

1. Complete Kinesis Data Firehose & Lambda function settings.

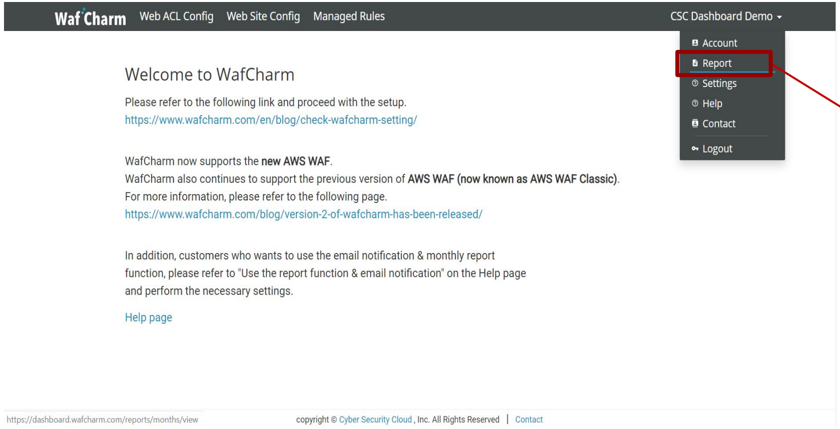
2. Detection in the previous month.

※ Please note that no monthly report will be generated in case there wasn’t any detection in the previous month.

3.1. Viewing the monthly report on WafCharm management screen

On WafCharm management screen,

Select｢Report｣from the top right menu.



Welcome to WafCharm

Please refer to the following link and proceed with the setup.
https://www.wafcharm.com/en/blog/check-wafcharm-setting/

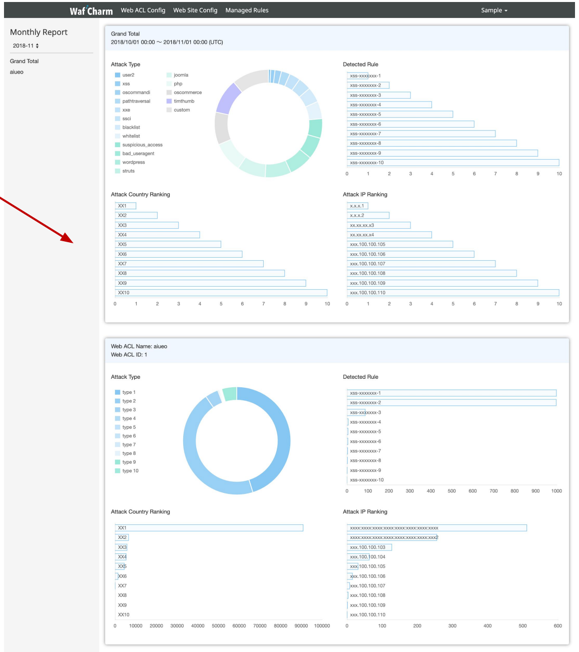
WafCharm now supports the **new AWS WAF**.
WafCharm also continues to support the previous version of **AWS WAF (now known as AWS WAF Classic)**.
For more information, please refer to the following page.
https://www.wafcharm.com/blog/version-2-of-wafcharm-has-been-released/

In addition, customers who wants to use the email notification & monthly report function, please refer to "Use the report function & email notification" on the Help page and perform the necessary settings.

Help page

https://dashboard.wafcharm.com/reports/months/view

copyright © Cyber Security Cloud , Inc. All Rights Reserved | Contact



※ At the beginning of each month, reports for the previous month are available.

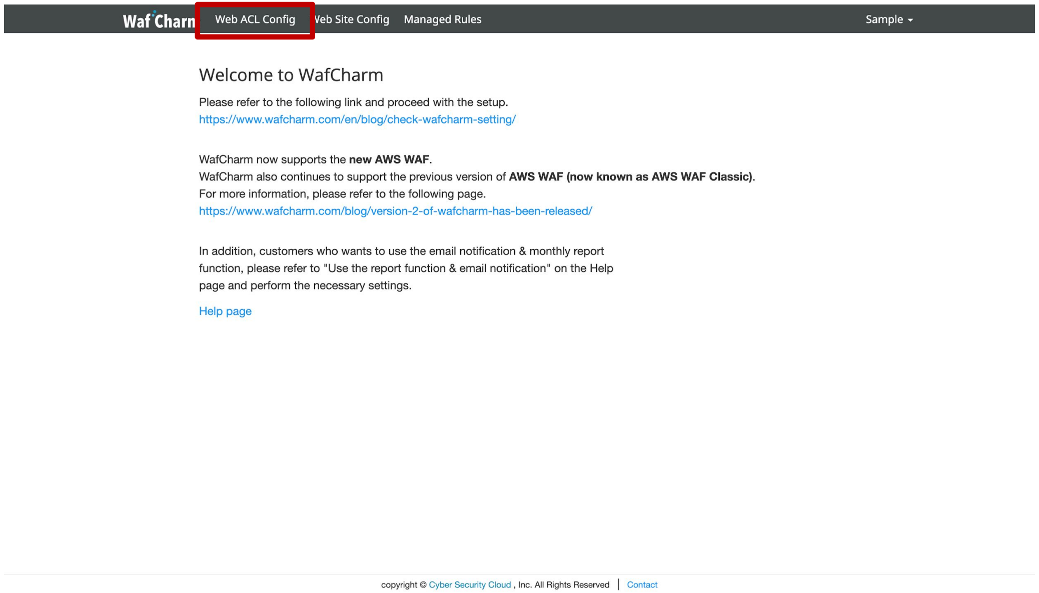
※ The above report is an image only

4. Using the email notification function

After completing Kinesis Firehose and Lambda settings in Steps 1 & 2, you can start using the Email notification function by setting up the email notification destination and turning on the notification on the WafCharm management screen.

- Email notification destination setting
- Email notification setting
- Email notification content

4.1. Email notification destination setting



Welcome to WafCharm

Please refer to the following link and proceed with the setup.
https://www.wafcharm.com/en/blog/check-wafcharm-setting/

WafCharm now supports the **new AWS WAF**.
WafCharm also continues to support the previous version of **AWS WAF (now known as AWS WAF Classic)**.
For more information, please refer to the following page.
https://www.wafcharm.com/blog/version-2-of-wafcharm-has-been-released/

In addition, customers who wants to use the email notification & monthly report function, please refer to "Use the report function & email notification" on the Help page and perform the necessary settings.

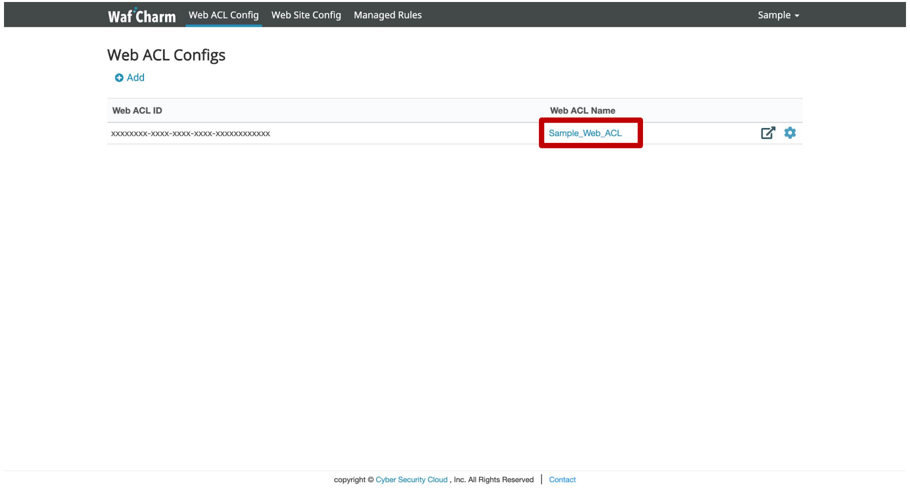
Help page

copyright © Cyber Security Cloud , Inc. All Rights Reserved | Contact

On WafCharm management screen,

Select「Web ACL Config」from the top menu.

4.2. Email notification destination setting



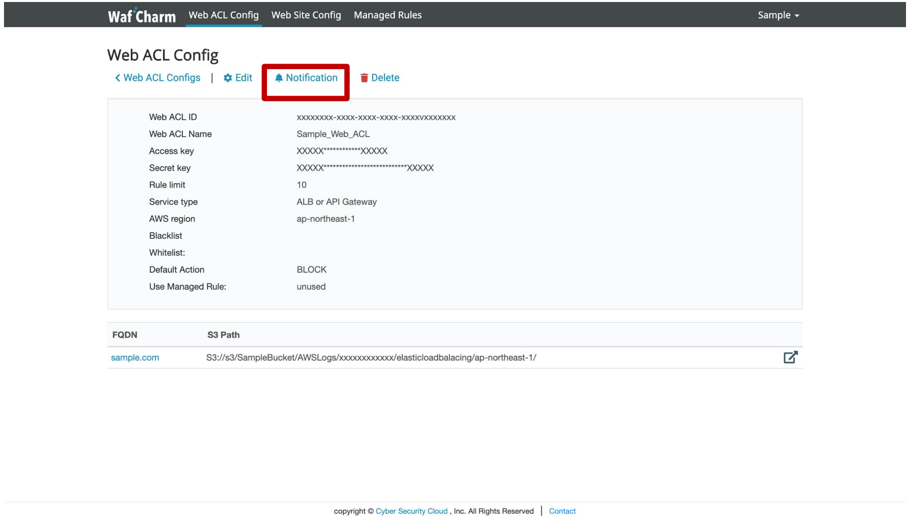
Web ACL Configs

Web ACL ID	Web ACL Name
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	Sample_Web_ACL

copyright © Cyber Security Cloud , Inc. All Rights Reserved | Contact

Select the target「Web ACL Name」

4.3. Email notification destination setting



Web ACL Config

< Web ACL Configs | Edit Notification Delete

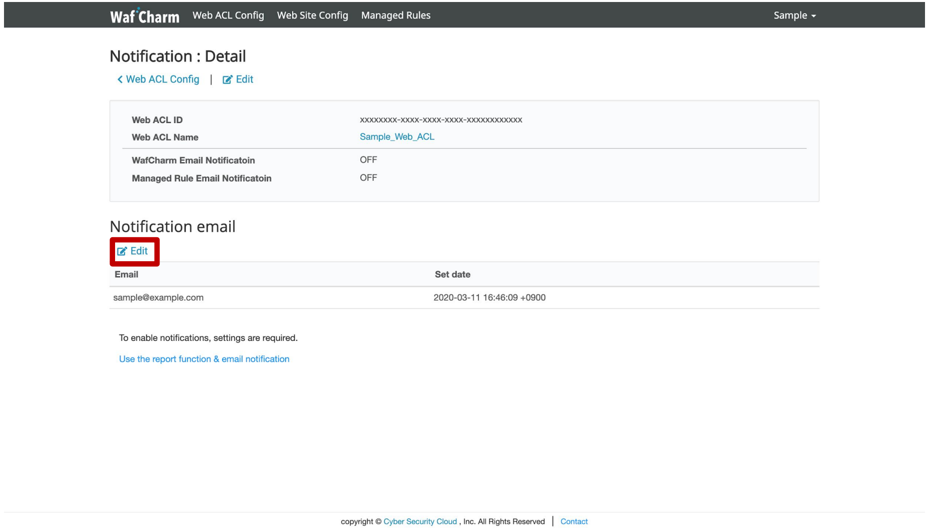
Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxvxxxxxxxx
Web ACL Name	Sample_Web_ACL
Access key	XXXXX************XXXXX
Secret key	XXXXX***************************XXXXX
Rule limit	10
Service type	ALB or API Gateway
AWS region	ap-northeast-1
Blacklist	
Whitelist:	
Default Action	BLOCK
Use Managed Rule:	unused

FQDN	S3 Path
sample.com	S3://s3/SampleBucket/AWSLogs/xxxxxxxxxxxx/elasticloadbalacing/ap-northeast-1/

copyright © Cyber Security Cloud , Inc. All Rights Reserved | Contact

Click「Notification」

4.4. Email notification destination setting



Notification : Detail

< Web ACL Config | Edit

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificatoin	OFF
Managed Rule Email Notificatoin	OFF

Notification email

Edit

Email	Set date
sample@example.com	2020-03-11 16:46:09 +0900

To enable notifications, settings are required.

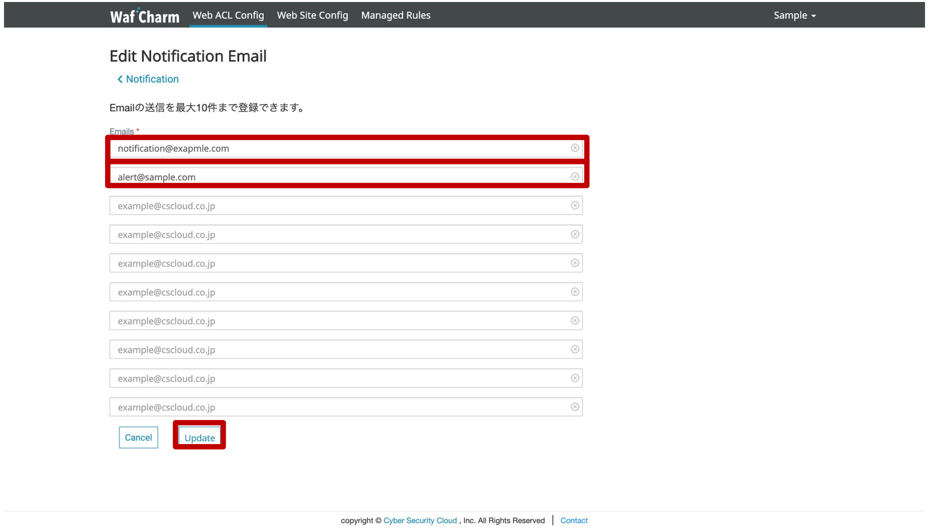
Use the report function & email notification

copyright © Cyber Security Cloud , Inc. All Rights Reserved | Contact

Under “Notification email”, Click「Edit」

※ By default, the email address used to login to the WafCharm management screen is set.

4.5. Email notification destination setting



Edit Notification Email

< Notification

Emailの送信を最大10件まで登録できます。

Emails *

notification@exapmle.com

alert@sample.com

example@cscloud.co.jp

example@cscloud.co.jp

example@cscloud.co.jp

example@cscloud.co.jp

example@cscloud.co.jp

example@cscloud.co.jp

example@cscloud.co.jp

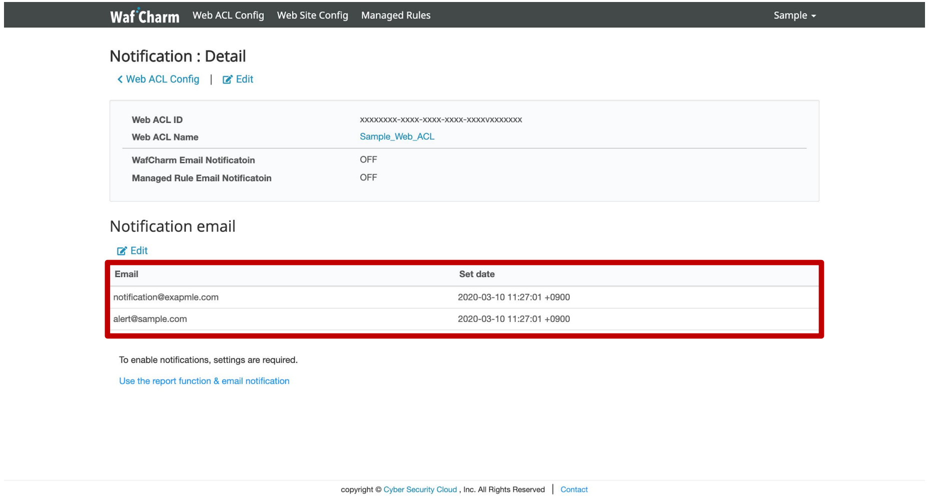
example@cscloud.co.jp

copyright © Cyber Security Cloud , Inc. All Rights Reserved | Contact

Set any email address in "Emails" and click「Update」

※ Up to 10 emails can be registered.

4.6. Email notification destination setting



Notification : Detail

< Web ACL Config | Edit

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxvxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificatoin	OFF
Managed Rule Email Notificatoin	OFF

Notification email

Edit

Email	Set date
notification@exapmle.com	2020-03-10 11:27:01 +0900
alert@sample.com	2020-03-10 11:27:01 +0900

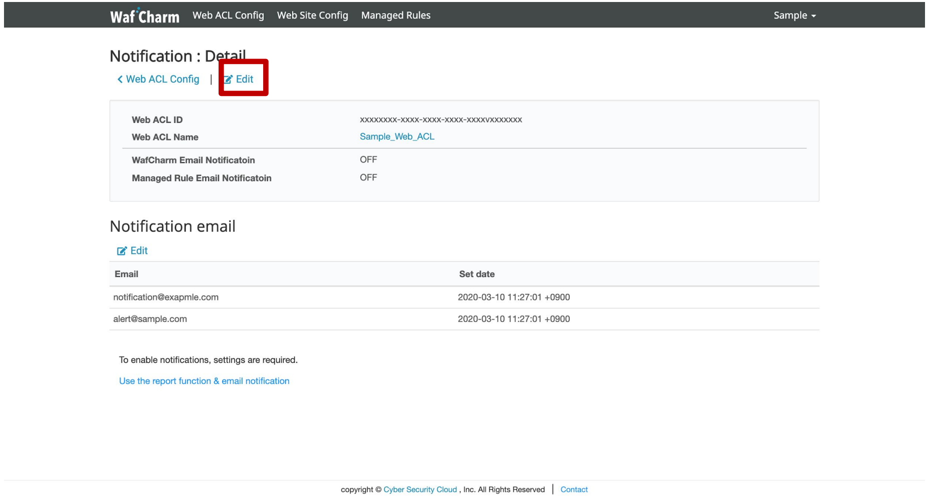
To enable notifications, settings are required.

Use the report function & email notification

copyright © Cyber Security Cloud , Inc. All Rights Reserved | Contact

Confirm that the "Notification email" has been updated to the email address you set.

4.7. Email notification setting



Notification : Detail

< Web ACL Config | Edit

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxvxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificatoin	OFF
Managed Rule Email Notificatoin	OFF

Notification email

Edit

Email	Set date
notification@exapmle.com	2020-03-10 11:27:01 +0900
alert@sample.com	2020-03-10 11:27:01 +0900

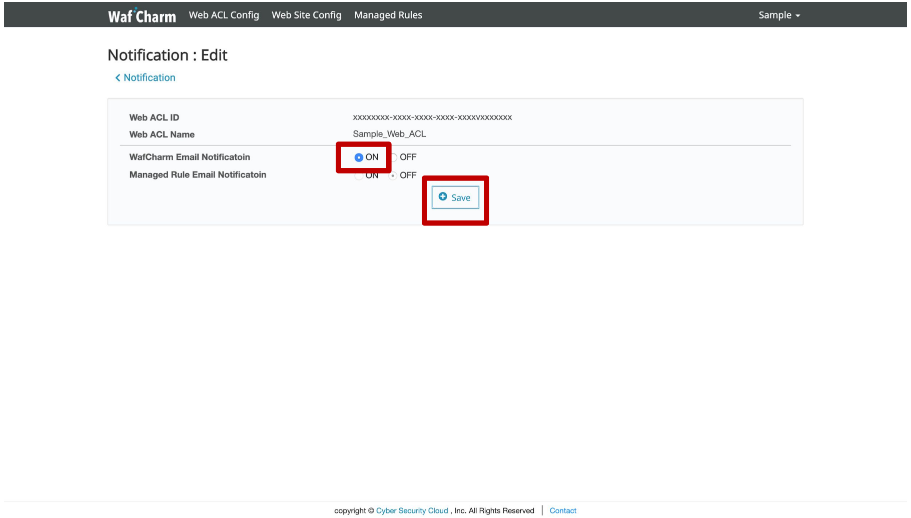
To enable notifications, settings are required.

Use the report function & email notification

copyright © Cyber Security Cloud , Inc. All Rights Reserved | Contact

Click「Edit」

4.8. Email notification setting



Notification : Edit

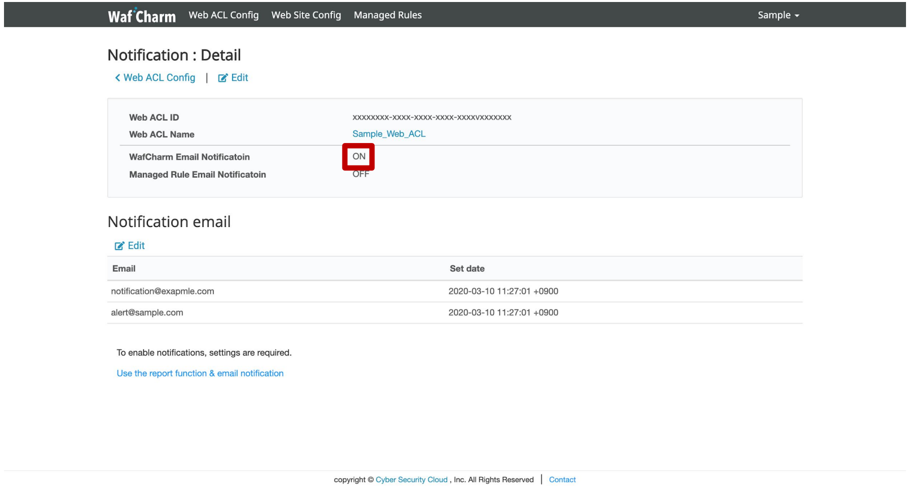
< Notification

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxvxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificatoin	● ON ○ OFF
Managed Rule Email Notificatoin	○ ON ● OFF

copyright © Cyber Security Cloud , Inc. All Rights Reserved | Contact

Switch “WafCharm Email Notification” to「ON」 and Click「Save」

4.9. Email notification setting



Notification : Detail

< Web ACL Config | Edit

Web ACL ID xxxxxxxx-xxxx-xxxx-xxxx-xxxxvxxxxxxx

Web ACL Name Sample_Web_ACL

WafCharm Email Notificatoin ON

Managed Rule Email Notificatoin OFF

Notification email

Edit

Email	Set date
notification@exapmle.com	2020-03-10 11:27:01 +0900
alert@sample.com	2020-03-10 11:27:01 +0900

To enable notifications, settings are required.

Use the report function & email notification

copyright © Cyber Security Cloud , Inc. All Rights Reserved | Contact

Confirm that the “WafCharm Email Notification” is turned「ON」

4.10. Email notification content

In the event of a detection (BLOCK/COUNT), you will receive the following email

- Email Title： WafCharm Attack Detected.
- Mailer：WafCharm Notification wafcharm-notification@cscloud.co.jp
- Email address：WafCharm Notification wafcharm-notification@cscloud.co.jp
- Email BCC destination：Email address registered under “Notification email” (4.6)

Attacks as follows were detected
This report includes up to 10 attacks detected in every buffer interval.
If you need to check more information and attacks, visit your AWS console.

WebACL Name(Web ACL ID): < User’s Web ACL Name> (< User’s Web ACL ID>)

Matches Rule Name: wafcharm-blacklist-685
Time(UTC): Thu, 01 Apr 2020 20:20:00 GMT
Source IP: 153.156.84.123
Source Country: JP
Action: BLOCK
URI: /

5. Additional information about the notification function

- Each email (log file) contains details of a maximum of 10 detections.

- The notification interval is 5 min.

- Since WafCharm for the new AWS WAF specification cannot integrate with the CSC Managed Rules, there is no CSC managed rule-specific notification feature available for the new AWS WAF, as there is one available for AWS WAF Classic.

- COUNT detection for rules that do not use a customer-generated rule group will not be notified.

6. Other additional information

- It is recommended that log files output to S3 be periodically (e.g., every month) deleted or backup to S3 Glacier using the lifecycle function as necessary.

- If AWS does not identify the region of the IP address, you may see "-" in the country name of the monthly report.

- If you wish for us to confirm the WAF log transfer, please confirm the following two points in advance and share the "Web ACL ID" and the “prefix of WAFLog”(<account-id>_waflogs_<Region>_<web-acl-name>) that you set in 2.11.
  - WAF log is being output to the S3 specified in Kinesis Data Firehose.
  - There is no ERROR output in the CloudWatch event log.
    - Checking the ERROR

      CloudWatch -> Log groups -> /aws/lambda/Lambda Function name (In case of manual: wafcharm-waflog)

      -> Select the latest (top) Log Stream -> Check for ERROR messages

6. Other additional information

- If you edit the role (policy) permissions after Lambda starts, the changes may not be reflected in the running Lambda, so please add blank lines to the last line of index.js and try deploying again.

- Configuration of the log filtering feature provided by AWS is basically **deprecated.**
  - action: If you configure filtering to save only Block:
    - Only BLOCK logs are created, so notification functions and monthly reports are based on BLOCK logs.
  - action: If you configure filtering to save Count only:
    - Notifications and monthly reports do not work properly because the WafCharm count is different from the AWS-defined count.