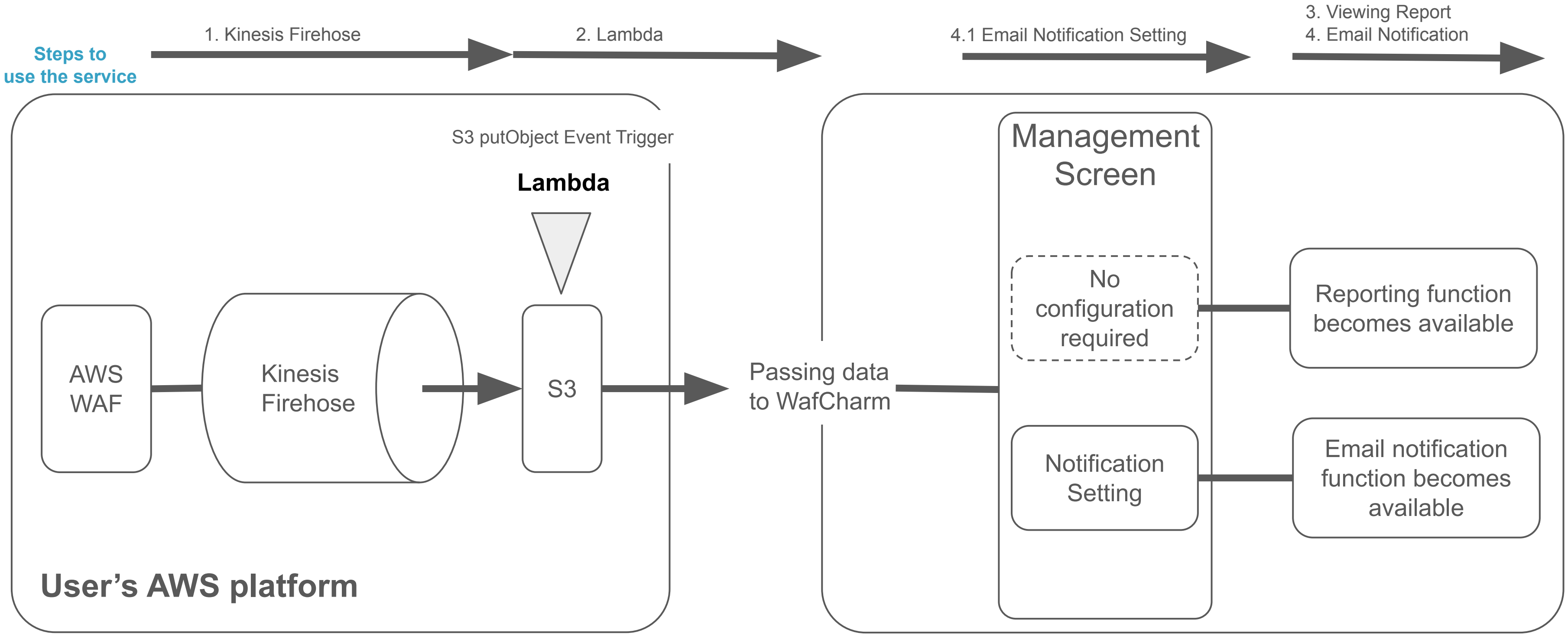
User Manual for
Reporting & Notification function
new AWS WAF
Ver 1.6

WafCharm

Architectural Overview of Reporting & Notification Function

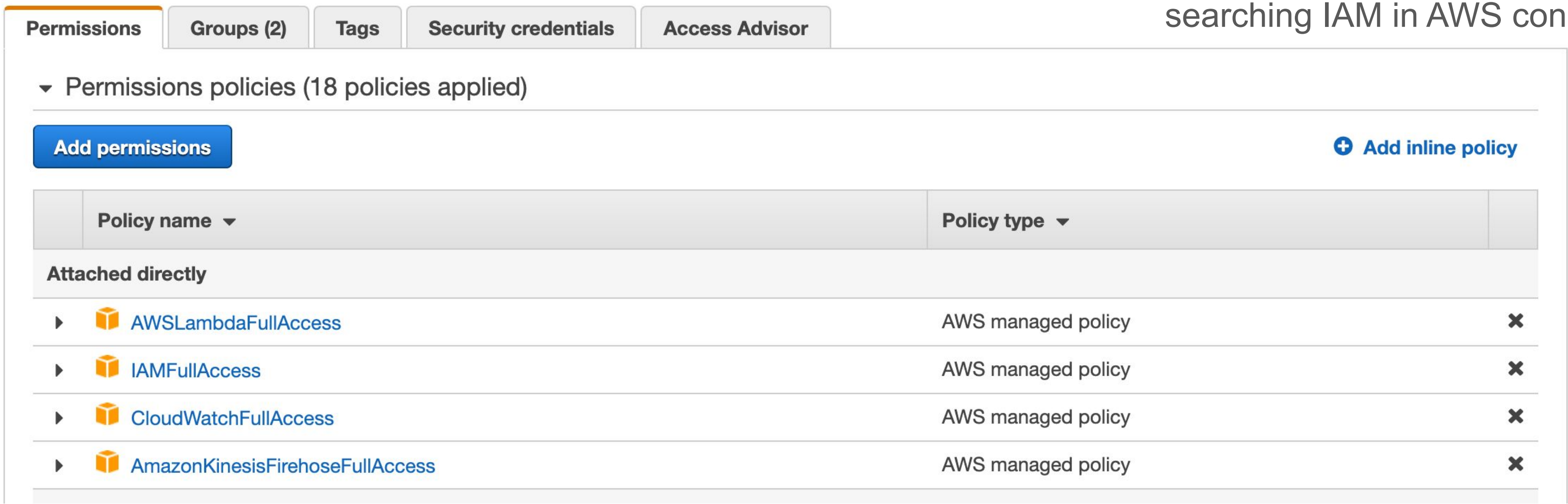


WafCharm

Authorization required to perform this procedure

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

You can set the policies with searching IAM in AWS console.



▾ Permissions policies (18 policies applied)

Policy name ▾	Policy type ▾	
Attached directly		
▸ AWSLambdaFullAccess	AWS managed policy	✖
▸ IAMFullAccess	AWS managed policy	✖
▸ CloudWatchFullAccess	AWS managed policy	✖
▸ AmazonKinesisFirehoseFullAccess	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. Kinesis Firehose
   - Create/Configure Kinesis Firehose
   - Role settings to run Kinesis Firehose
   - Configure Kinesis Firehose and AWS WAF integration
   - 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

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.

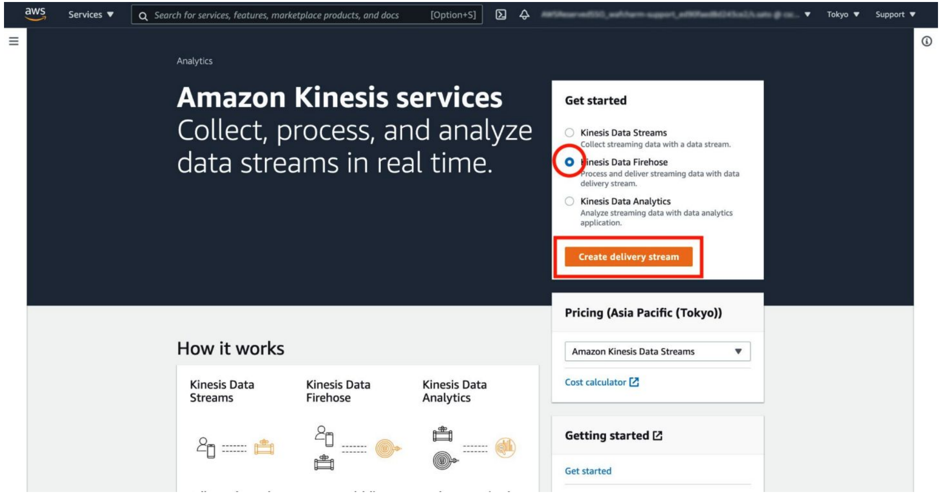
3. Using the reporting function
    - Viewing the monthly report on WafCharm management screen
4. Using the email notification function
    - Email notification destination setting
    - Email notification setting
    - Email notification content
5. Additional information about the notification function
6. Other additional information

1. Kinesis Firehose

Set up Kinesis Firehose to stream WAF log to S3.

- Create/Configure Kinesis Firehose
- Role settings to run Kinesis Firehose
- Configure Kinesis Firehose and AWS WAF integration
- Confirmation of completion of step 1

1.1. Kinesis Firehose Setting


aws
Services ▼
Search for services, features, marketplace products, and docs
[Option+S]
[redacted]
Tokyo ▼
Support ▼

Analytics

Amazon Kinesis services
Collect, process, and analyze data streams in real time.

Get started

○ Kinesis Data Streams
Collect streaming data with a data stream.

● Kinesis Data Firehose
Process and deliver streaming data with data delivery stream.

○ Kinesis Data Analytics
Analyze streaming data with data analytics application.

Create delivery stream

Pricing (Asia Pacific (Tokyo))

Amazon Kinesis Data Streams ▼

Cost calculator

Getting started

Get started

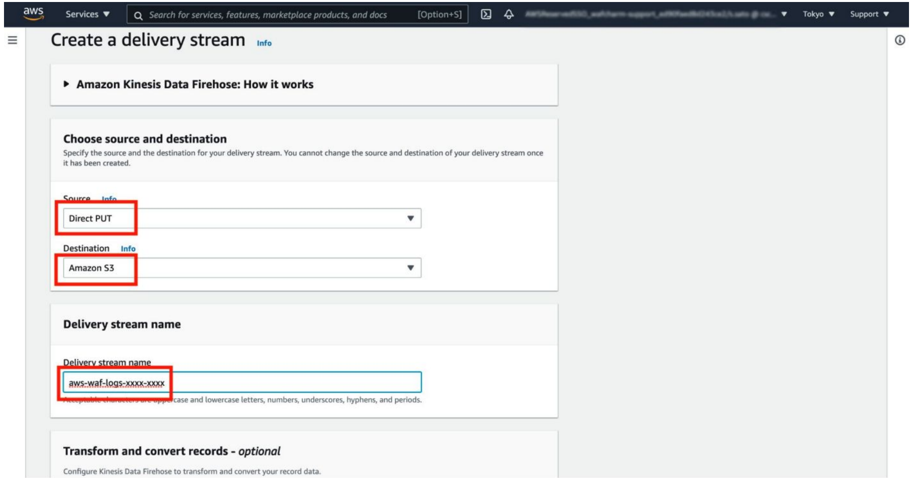
How it works

Select「Kinesis Data Firehose」from「Get started」, and click「Create delivery stream」

Create in the same region as AWS WAF (Web ACL)

※For those who use CloudFront, set "Region" to "N. Virginia (US East)"

1.2. Kinesis Firehose Setting


aws
Services ▼
Search for services, features, marketplace products, and docs
[Option+S]
[redacted] ▼
Tokyo ▼
Support ▼
Info

Create a delivery stream

▸ Amazon Kinesis Data Firehose: How it works

Choose source and destination

Specify the source and the destination for your delivery stream. You cannot change the source and destination of your delivery stream once it has been created.

Source: Direct PUT

Destination: Amazon S3

Delivery stream name

Delivery stream name: aws-waf-logs-xxxx-xxxx

case and lowercase letters, numbers, underscores, hyphens, and periods.

Transform and convert records - *optional*

Configure Kinesis Data Firehose to transform and convert your record data.

Choose source and destination.

Source: Direct PUT

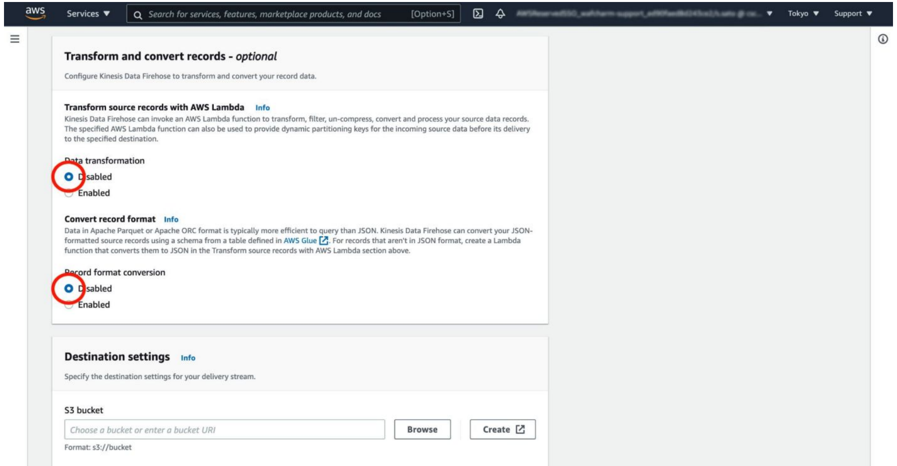
Destination: Amazon S3

Delivery Stream Name:

aws-waf-logs-<Random Name>

※ Please note that the “Delivery Stream Name” should have "aws-waf-logs-" added as a prefix.

1.3. Kinesis Firehose Setting


aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
[redacted] ▼
Tokyo ▼
Support ▼

Transform and convert records - *optional*

Configure Kinesis Data Firehose to transform and convert your record data.

Transform source records with AWS Lambda Info

Kinesis Data Firehose can invoke an AWS Lambda function to transform, filter, un-compress, convert and process your source data records. The specified AWS Lambda function can also be used to provide dynamic partitioning keys for the incoming source data before its delivery to the specified destination.

Data transformation

● Disabled

○ Enabled

Convert record format Info

Data in Apache Parquet or Apache ORC format is typically more efficient to query than JSON. Kinesis Data Firehose can convert your JSON-formatted source records using a schema from a table defined in AWS Glue. For records that aren't in JSON format, create a Lambda function that converts them to JSON in the Transform source records with AWS Lambda section above.

Record format conversion

● Disabled

○ Enabled

Destination settings Info

Specify the destination settings for your delivery stream.

S3 bucket

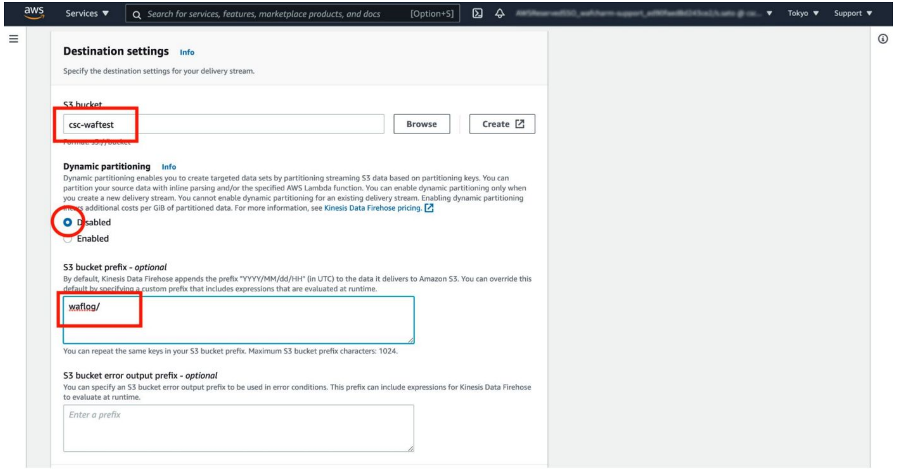
Choose a bucket or enter a bucket URI

Format: s3://bucket

The following are not used.

- Transform source records with AWS Lambda
- Convert record format

1.4. Kinesis Firehose Setting


aws
Services ▼
Search for services, features, marketplace products, and docs
[Option+S]
[redacted] ▼
Tokyo ▼
Support ▼

Destination settings Info

Specify the destination settings for your delivery stream.

S3 bucket

csc-waftest

Format: s3://bucket

Dynamic partitioning Info

Dynamic partitioning enables you to create targeted data sets by partitioning streaming S3 data based on partitioning keys. You can partition your source data with inline parsing and/or the specified AWS Lambda function. You can enable dynamic partitioning only when you create a new delivery stream. You cannot enable dynamic partitioning for an existing delivery stream. Enabling dynamic partitioning incurs additional costs per GiB of partitioned data. For more information, see Kinesis Data Firehose pricing.

● Disabled

○ Enabled

S3 bucket prefix - *optional*

By default, Kinesis Data Firehose appends the prefix "YYYY/MM/dd/HH" (in UTC) to the data it delivers to Amazon S3. You can override this default by specifying a custom prefix that includes expressions that are evaluated at runtime.

waflog/

You can repeat the same keys in your S3 bucket prefix. Maximum S3 bucket prefix characters: 1024.

S3 bucket error output prefix - *optional*

You can specify an S3 bucket error output prefix to be used in error conditions. This prefix can include expressions for Kinesis Data Firehose to evaluate at runtime.

Enter a prefix

S3 bucket :

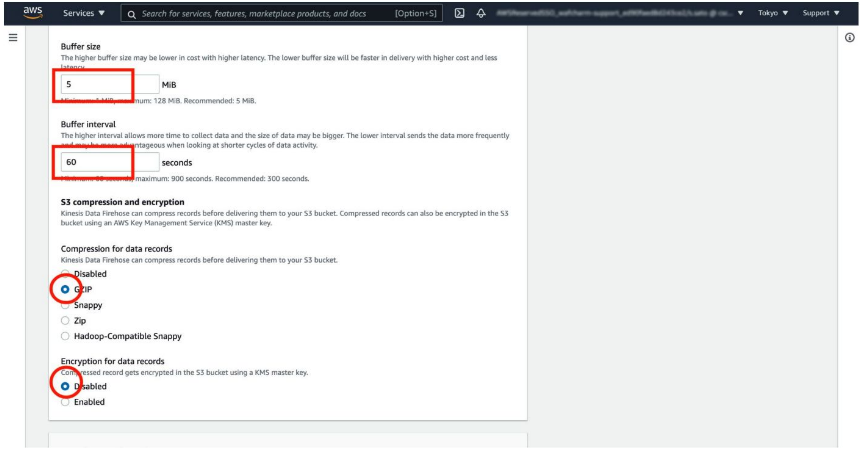
Specify any S3 bucket (ex : csc-waftest)

Prefix :

Specify any Prefix (ex : waflog/)

※Please make sure that the Prefix ends with "/", such as "waflog/".

1.5. Kinesis Firehose Setting


aws
Services ▼
Search for services, features, marketplace products, and docs
[Option+S]
[redacted]
Tokyo ▼
Support ▼

Buffer size

The higher buffer size may be lower in cost with higher latency. The lower buffer size will be faster in delivery with higher cost and less latency.

5 MiB

Minimum: 1 MiB, maximum: 128 MiB. Recommended: 5 MiB.

Buffer interval

The higher interval allows more time to collect data and the size of data may be bigger. The lower interval sends the data more frequently and may be more advantageous when looking at shorter cycles of data activity.

60 seconds

Minimum: 60 seconds, maximum: 900 seconds. Recommended: 300 seconds.

S3 compression and encryption

Kinesis Data Firehose can compress records before delivering them to your S3 bucket. Compressed records can also be encrypted in the S3 bucket using an AWS Key Management Service (KMS) master key.

Compression for data records

Kinesis Data Firehose can compress records before delivering them to your S3 bucket.

○ Disabled
● GZIP
○ Snappy
○ Zip
○ Hadoop-Compatible Snappy

Encryption for data records

Compressed record gets encrypted in the S3 bucket using a KMS master key.

● Disabled
○ Enabled

Buffer intervals :
60 seconds is recommended

Buffer size :
5 MB is recommended

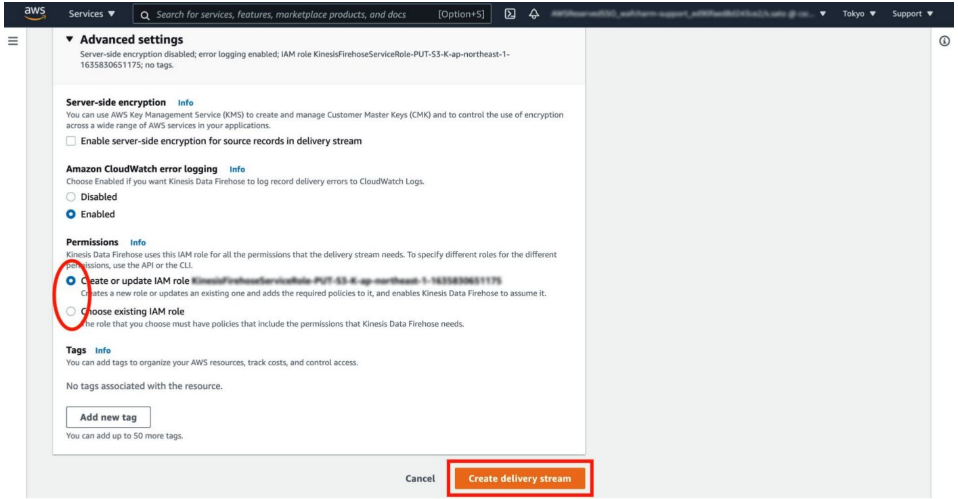
S3 compression :
GZIP

S3 encryption :
Disable

※ A log is created in S3 when the Buffer intervals, or Buffer size, is reached.

Click「Advanced settings」

1.6. IAM role Setting



aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
[redacted] ▼
Tokyo ▼
Support ▼

▼ **Advanced settings**

Server-side encryption disabled; error logging enabled; IAM role KinesisFirehoseServiceRole-PUT-S3-K-ap-northeast-1-1635830651175; no tags.

Server-side encryption Info

You can use AWS Key Management Service (KMS) to create and manage Customer Master Keys (CMK) and to control the use of encryption across a wide range of AWS services in your applications.

□ Enable server-side encryption for source records in delivery stream

Amazon CloudWatch error logging Info

Choose Enabled if you want Kinesis Data Firehose to log record delivery errors to CloudWatch Logs.

○ Disabled

● Enabled

Permissions Info

Kinesis Data Firehose uses this IAM role for all the permissions that the delivery stream needs. To specify different roles for the different permissions, use the API or the CLI.

● Create or update IAM role [redacted]

Creates a new role or updates an existing one and adds the required policies to it, and enables Kinesis Data Firehose to assume it.

○ Choose existing IAM role

The role that you choose must have policies that include the permissions that Kinesis Data Firehose needs.

Tags Info

You can add tags to organize your AWS resources, track costs, and control access.

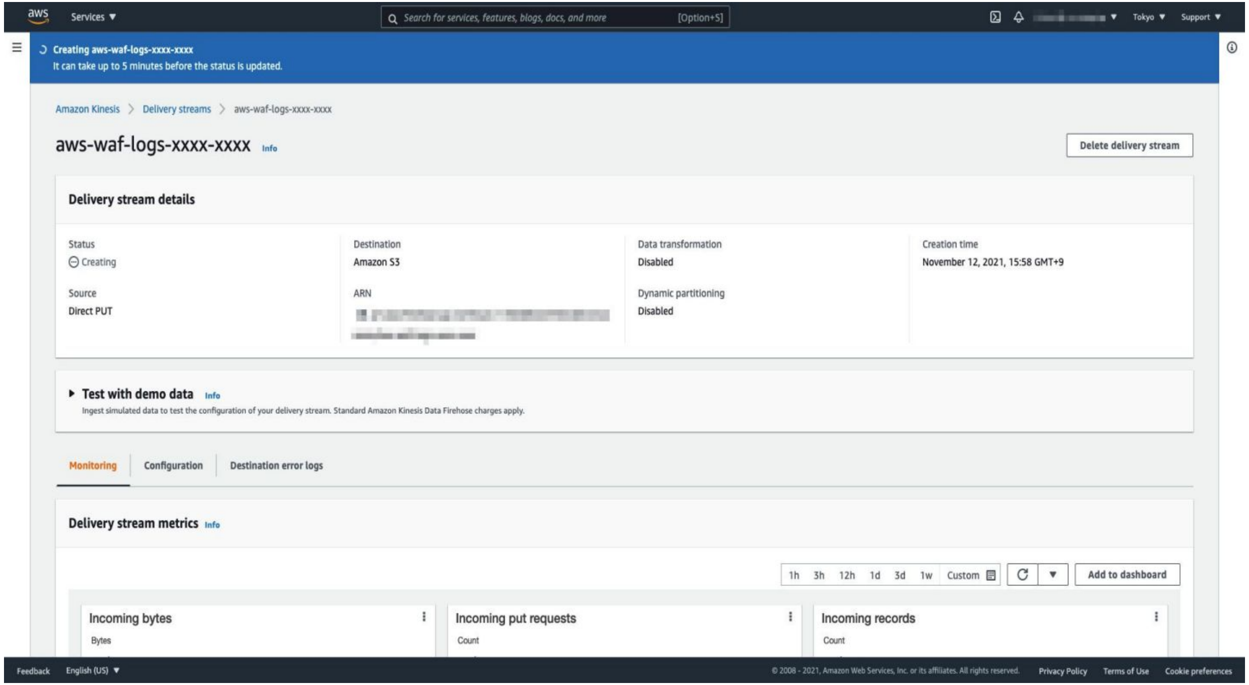
No tags associated with the resource.

You can add up to 50 more tags.

IAM Role : Create or Choose IAM role

Click「Create delivery stream」

1.7. Kinesis Firehose Setting


aws
Services ▼
Search for services, features, blogs, docs, and more [Option+S]
[redacted] ▼
Tokyo ▼
Support ▼

Creating aws-waf-logs-xxxx-xxxx
It can take up to 5 minutes before the status is updated.

Amazon Kinesis > Delivery streams > aws-waf-logs-xxxx-xxxx

aws-waf-logs-xxxx-xxxx Info

Delivery stream details

Status
Creating

Source
Direct PUT

Destination
Amazon S3

ARN
[redacted]

Data transformation
Disabled

Dynamic partitioning
Disabled

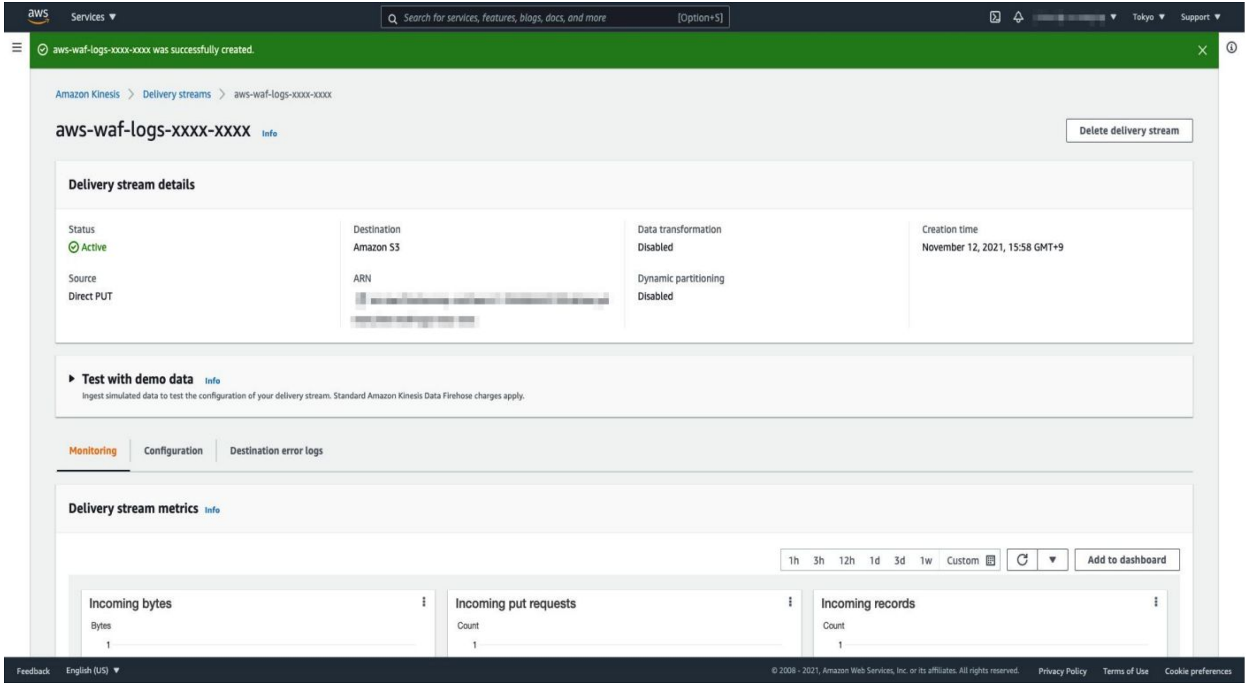
Creation time
November 12, 2021, 15:58 GMT+9

▸ **Test with demo data** Info
Ingest simulated data to test the configuration of your delivery stream. Standard Amazon Kinesis Data Firehose charges apply.

Delivery stream metrics Info

Stand-by

1.8. Kinesis Firehose Setting


aws
Services ▼
Search for services, features, blogs, docs, and more [Option+S]
[redacted] ▼
Tokyo ▼
Support ▼

aws-waf-logs-xxxx-xxxx was successfully created.

Amazon Kinesis > Delivery streams > aws-waf-logs-xxxx-xxxx

aws-waf-logs-xxxx-xxxx Info

Delivery stream details

Status: Active

Source: Direct PUT

Destination: Amazon S3

ARN: [redacted]

Data transformation: Disabled

Dynamic partitioning: Disabled

Creation time: November 12, 2021, 15:58 GMT+9

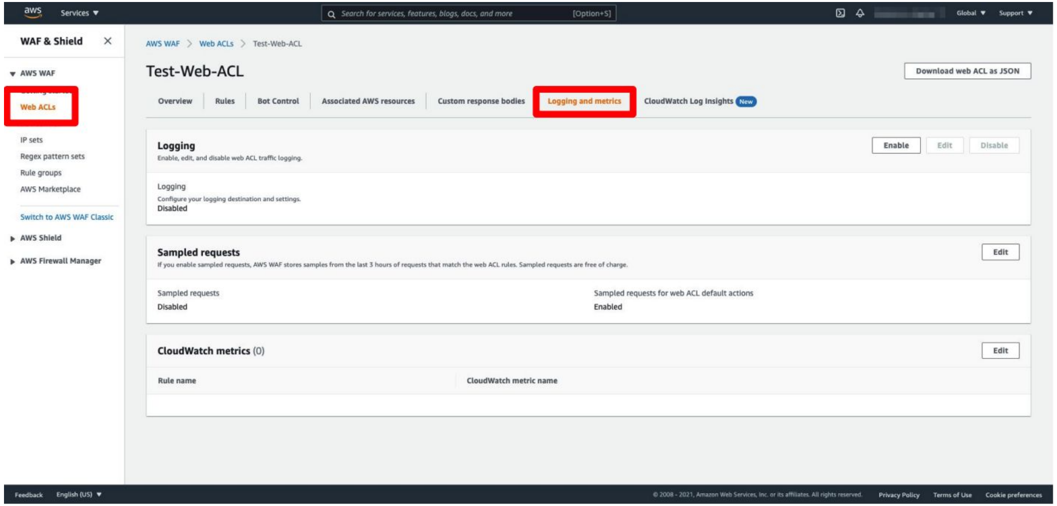
▸ **Test with demo data** Info

Ingest simulated data to test the configuration of your delivery stream. Standard Amazon Kinesis Data Firehose charges apply.

Delivery stream metrics Info

Complete

1.9. Configure Kinesis Firehose & AWS WAF integration



Test-Web-ACL

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

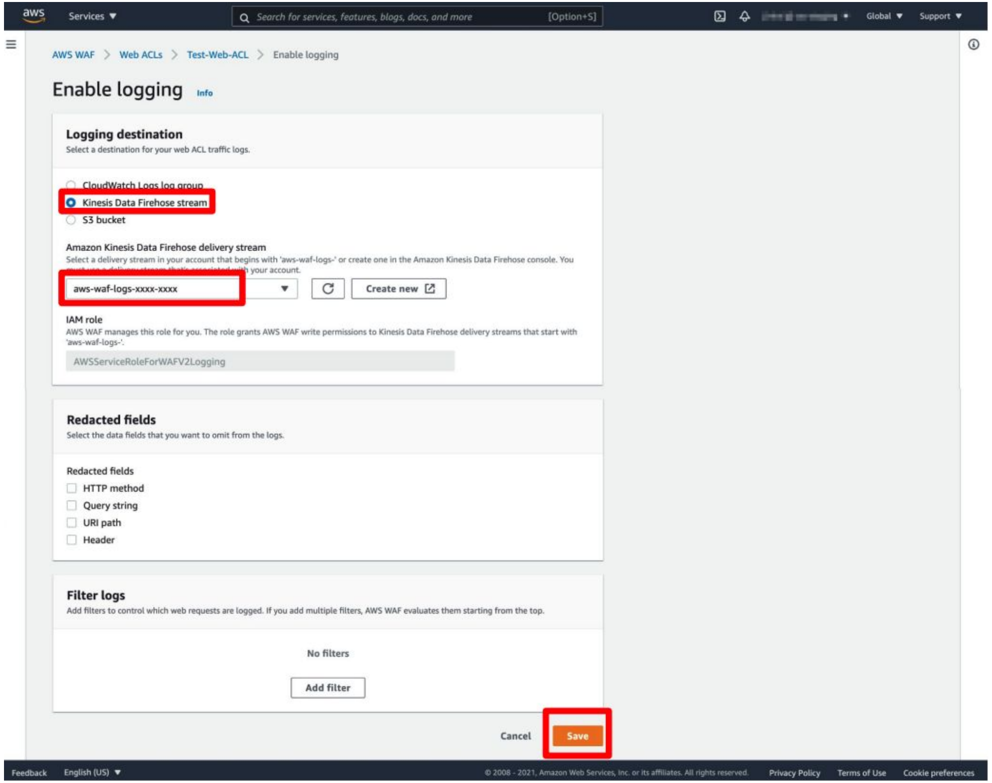
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Return to "AWS WAF" service

Select “Web ACLs” > “Logging and metrics”

「Enable Logging」

1.10. Configure Kinesis Firehose & AWS WAF integration


aws
Services ▼
Search for services, features, blogs, docs, and more [Option+S]
[redacted]
Global ▼
Support ▼
AWS WAF > Web ACLs > Test-Web-ACL > Enable logging
Info
Feedback
English (US) ▼
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences

Enable logging

Logging destination

Select a destination for your web ACL traffic logs.

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

Amazon Kinesis Data Firehose delivery stream

Select a delivery stream in your account that begins with 'aws-waf-logs-' or create one in the Amazon Kinesis Data Firehose console. You must use a delivery stream that's associated with your account.

aws-waf-logs-xxxx-xxxx ▼ | Create new

IAM role

AWS WAF manages this role for you. The role grants AWS WAF write permissions to Kinesis Data Firehose delivery streams that start with 'aws-waf-logs-'.

AWSServiceRoleForWAFV2Logging

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

Add filter

Cancel | Save

Logging destination:

Select the "Kinesis Data Firehose stream"

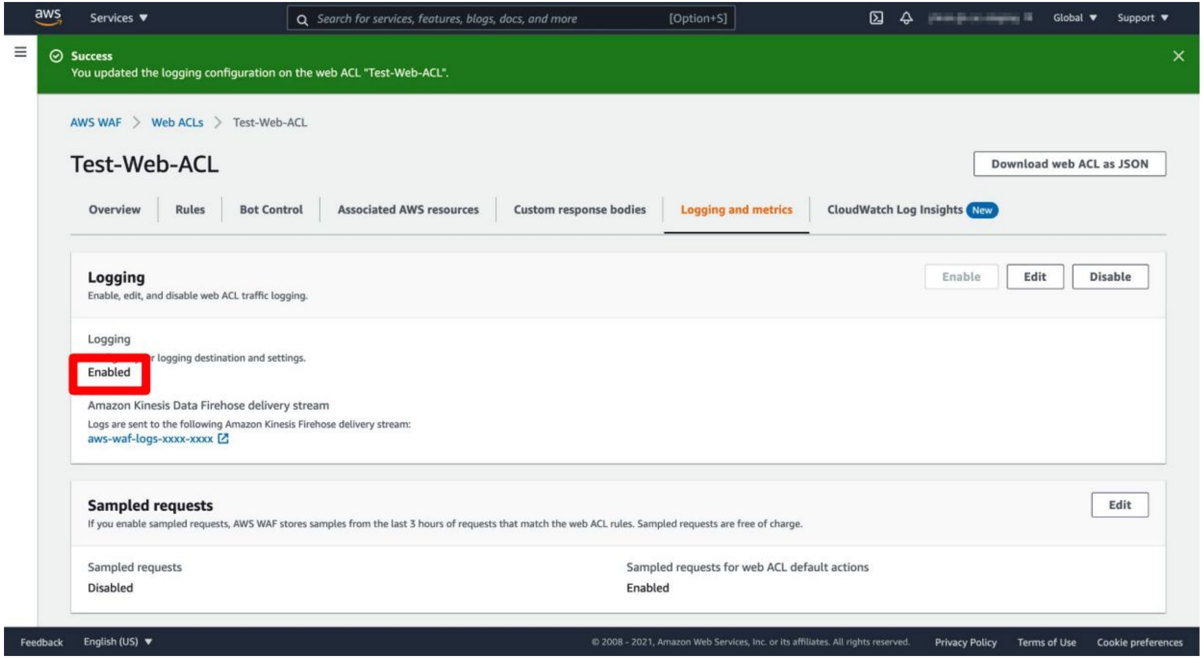
※ When using this report function/notification function, logging destination is only available at Kinesis Data Firehose.

Select the “Delivery Stream Name” you created.

※ Delivery Stream Name specified in Step 1.2.

Click「Save」

1.11. Configure Kinesis Firehose & AWS WAF integration



Success
You updated the logging configuration on the web ACL "Test-Web-ACL".

Test-Web-ACL

Logging
Enable, edit, and disable web ACL traffic logging.

Logging
r logging destination and settings.
Enabled

Amazon Kinesis Data Firehose delivery stream
Logs are sent to the following Amazon Kinesis Firehose delivery stream:
aws-waf-logs-xxxx-xxxx

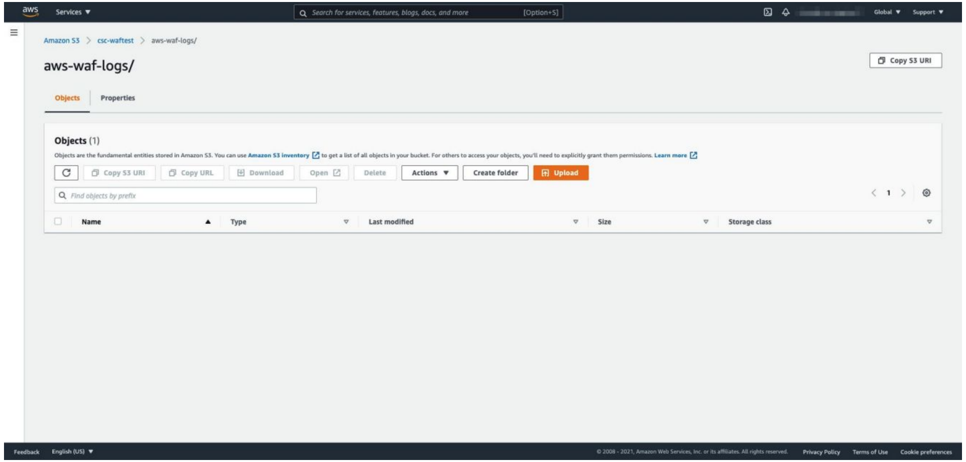
Sampled requests
If you enable sampled requests, AWS WAF stores samples from the last 3 hours of requests that match the web ACL rules. Sampled requests are free of charge.

Sampled requests	Sampled requests for web ACL default actions
Disabled	Enabled

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Confirm that Logging is “Enabled”.

1.12. Confirmation of completion of step 1



aws-waf-logs/

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

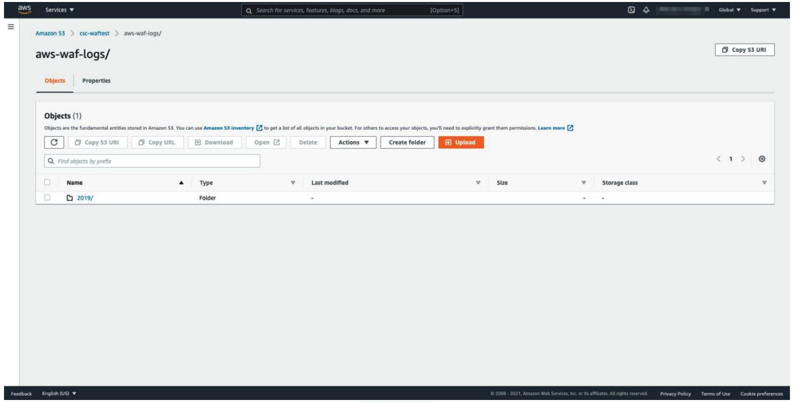
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Check if full log file is generated in S3

※ As specified in Step 1.4.

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

1.13. Confirmation of completion of step 1



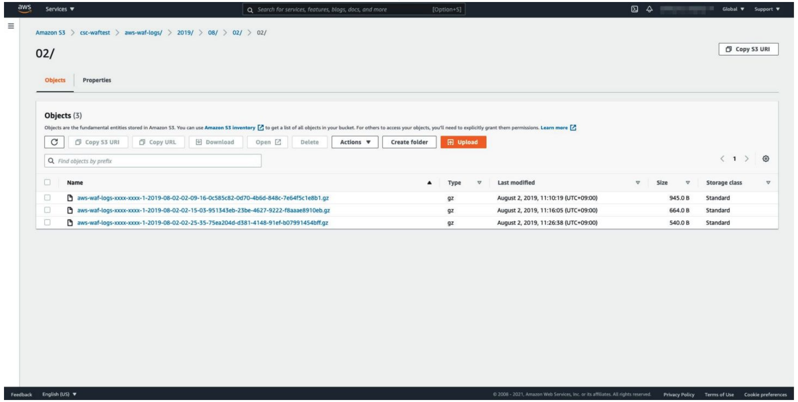
Amazon S3 > csc-waftest > aws-waf-logs/

aws-waf-logs/

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
2019/	Folder	-	-	-



Amazon S3 > csc-waftest > aws-waf-logs/ > 2019/ > 08/ > 02/ > 02/

02/

Objects (3)

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
aws-waf-logs-xxxx-xxxx-1-2019-08-02-02-09-16-0c585c82-0d70-4b6d-848c-7e64f5c1e8b1.gz	gz	August 2, 2019, 11:10:19 (UTC+09:00)	945.0 B	Standard
aws-waf-logs-xxxx-xxxx-1-2019-08-02-02-15-03-951343eb-23be-4627-9222-f8aaae8910eb.gz	gz	August 2, 2019, 11:16:05 (UTC+09:00)	664.0 B	Standard
aws-waf-logs-xxxx-xxxx-1-2019-08-02-02-25-35-75ea204d-d381-4148-91ef-b07991454bff.gz	gz	August 2, 2019, 11:26:38 (UTC+09:00)	540.0 B	Standard

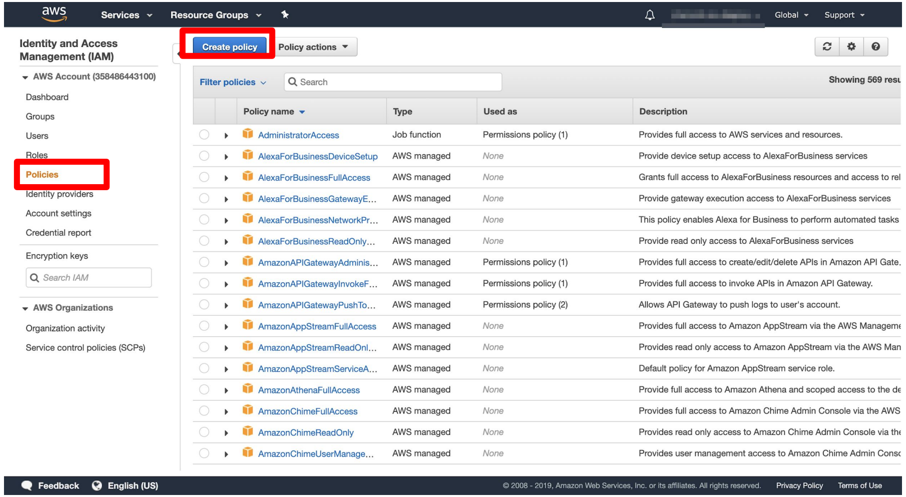
Once a file like the one on the left screen is generated, first chapter of the setup is complete.

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

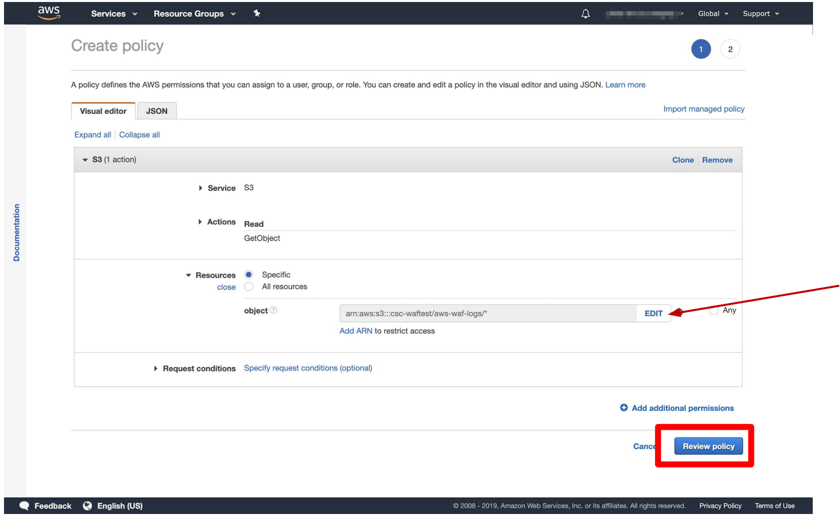


Policy name	Type	Used as	Description
AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and resources.
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to rel
AlexaForBusinessGatewayE...	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessNetworkPr...	AWS managed	None	This policy enables Alexa for Business to perform automated tasks
AlexaForBusinessReadOnly...	AWS managed	None	Provide read only access to AlexaForBusiness services
AmazonAPIGatewayAdminis...	AWS managed	Permissions policy (1)	Provides full access to create/edit/delete APIs in Amazon API Gate.
AmazonAPIGatewayInvokeF...	AWS managed	Permissions policy (1)	Provides full access to invoke APIs in Amazon API Gateway.
AmazonAPIGatewayPushTo...	AWS managed	Permissions policy (2)	Allows API Gateway to push logs to user's account.
AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppStream via the AWS Manageme
AmazonAppStreamReadOnl...	AWS managed	None	Provides read only access to Amazon AppStream via the AWS Man
AmazonAppStreamServiceA...	AWS managed	None	Default policy for Amazon AppStream service role.
AmazonAthenaFullAccess	AWS managed	None	Provide full access to Amazon Athena and scoped access to the de
AmazonChimeFullAccess	AWS managed	None	Provides full access to Amazon Chime Admin Console via the AWS
AmazonChimeReadOnly	AWS managed	None	Provides read only access to Amazon Chime Admin Console via the
AmazonChimeUserManage...	AWS managed	None	Provides user management access to Amazon Chime Admin Consc

From the “IAM” service,

Select “Policies” > “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

S3 (1 action)

Service S3

Actions Read
GetObject

Resources ● Specific
close ○ All resources

object arn:aws:s3:::csc-waftest/aws-waf-logs/* □ Any

Add ARN to restrict access

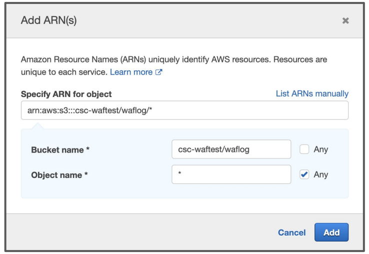
Request conditions Specify request conditions (optional)

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Service : S3

Action : GetObject

Resources :
arn:aws:s3:::csc-waftest/waflog/*
※ As setup in Step 1.4



Add ARN(s)

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

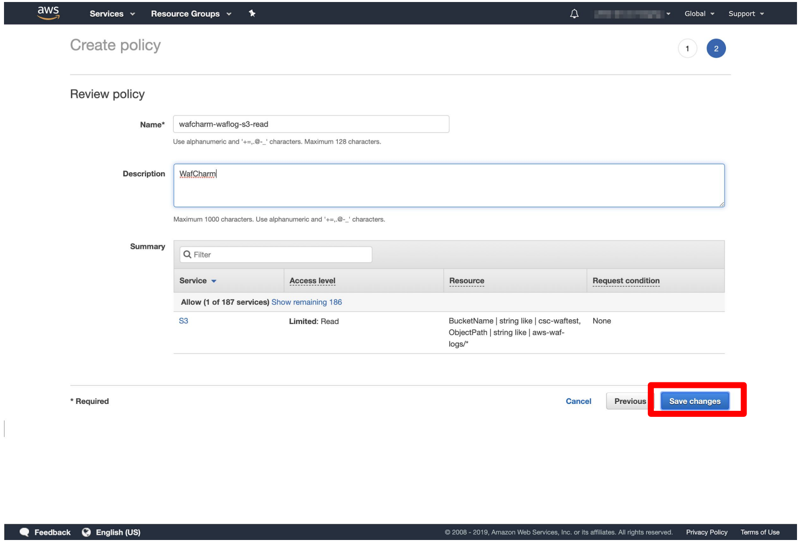
Specify ARN for object List ARNs manually
arn:aws:s3:::csc-waftest/waflog/*

Bucket name * csc-waftest/waflog □ Any
Object name * * ☑ Any

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

Click「Review policy」

2.3. Create read permission policy for WAFLog output destination S3



Create policy

1 2

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 187 services) Show remaining 186			
S3	Limited: Read	BucketName | string like | csc-waftest, ObjectPath | string like | aws-waf-logs/*	None

* Required

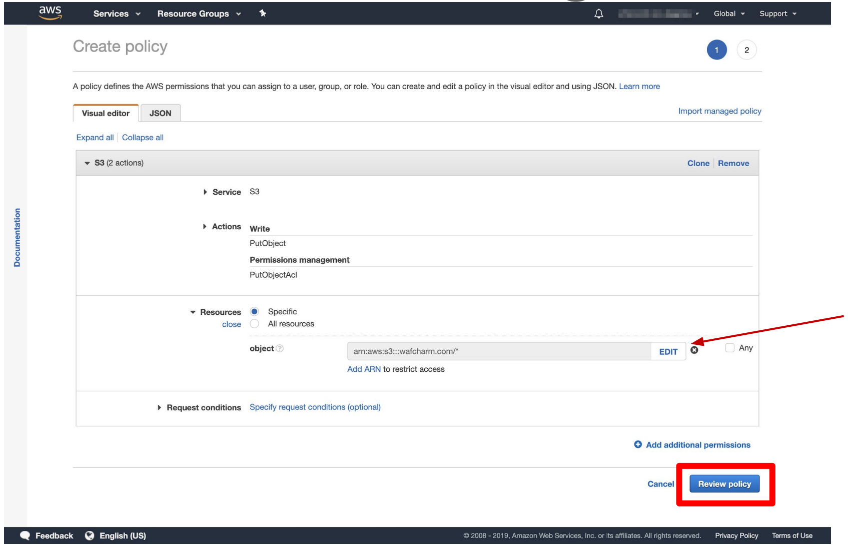
Filter
Cancel
Previous
Save changes
Feedback
English (US)
© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

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

Description : WafCharm (Arbitrary)

Click「Create policy」

2.4. Create put permission policy for WafCharm integration



[redacted] Global Support

Create policy

1 2

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

Visual editor | JSON | Import managed policy

Expand all | Collapse all

▾ S3 (2 actions) — Clone | Remove

- 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 additional permissions

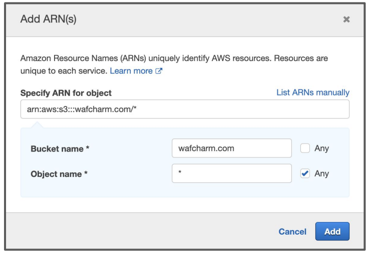
Cancel | Review policy

Documentation
Feedback
English (US)
© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Service : S3

Action : PutObject, PutObjectACL

Resources :
arn:aws:s3:::wafcharm.com/*
※ Access permission to S3 on CSC side



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

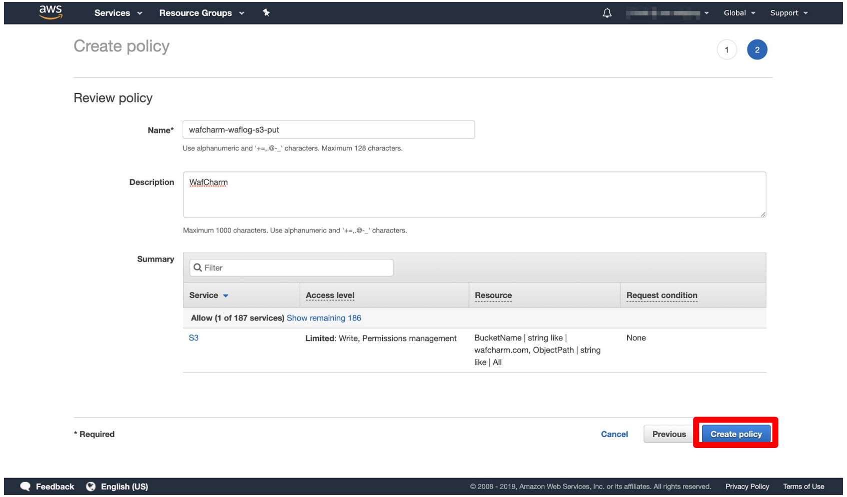
arn:aws:s3:::wafcharm.com/*

Bucket name *	wafcharm.com	□ Any
Object name *	*	☑ Any

Cancel | Add

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

Filter

Service	Access level	Resource	Request condition
Allow (1 of 187 services) Show remaining 186			
S3	**Limited**: Write, Permissions management	BucketName | string like | wafcharm.com, ObjectPath | string like | All	None

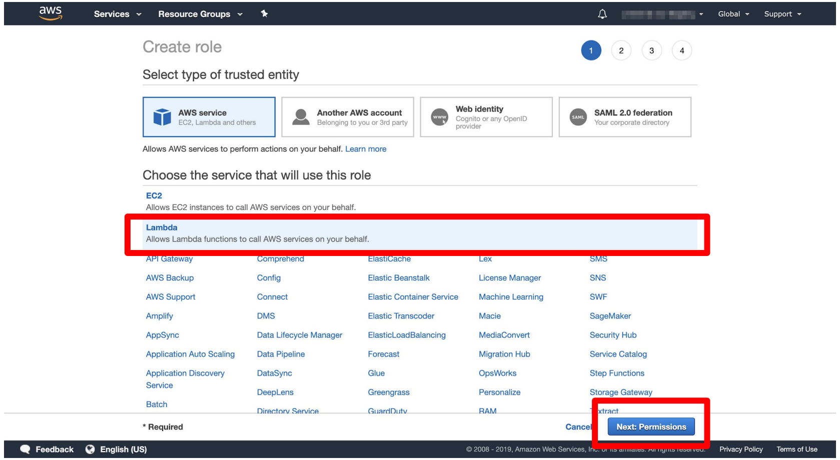
* Required

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

Description : WafCharm (Arbitrary)

Click「Create policy」

2.6. Create a role for Lambda to integrate with WafCharm



Create role

Select type of trusted entity

- AWS service — EC2, Lambda and others
- Another AWS account — Belonging to you or 3rd party
- Web identity — Cognito or any OpenID provider
- SAML 2.0 federation — Your corporate directory

Allows AWS services to perform actions on your behalf. Learn more

Choose the service that will use this role

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

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

API Gateway
AWS Backup
AWS Support
Amplify
AppSync
Application Auto Scaling
Application Discovery Service
Batch

Comprehend
Config
Connect
DMS
Data Lifecycle Manager
Data Pipeline
DataSync
DeepLens
Directory Service

ElastiCache
Elastic Beanstalk
Elastic Container Service
Elastic Transcoder
ElasticLoadBalancing
Forecast
Glue
Greengrass
GuardDuty

Lex
License Manager
Machine Learning
Macie
MediaConvert
Migration Hub
OpsWorks
Personalize
RAM

SMS
SNS
SWF
SageMaker
Security Hub
Service Catalog
Step Functions
Storage Gateway
Textract

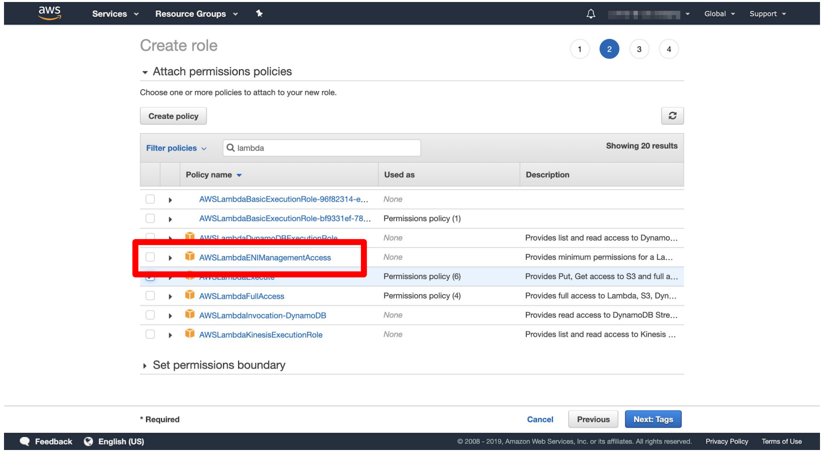
* Required

Cancel
Next: Permissions
Feedback
English (US)
© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Select a service to use this role : Lambda

Click「Next: Permissions」

2.7. Create a role for Lambda to integrate with WafCharm



Create role

Attach permissions policies

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

Filter policies: lambda

Showing 20 results

		Policy name	Used as	Description
□	▸	AWSLambdaBasicExecutionRole-96f82314-e...	None	
□	▸	AWSLambdaBasicExecutionRole-bf9331ef-78...	Permissions policy (1)	
□	▸	AWSLambdaDynamoDBExecutionRole	None	Provides list and read access to Dynamo...
□	▸	AWSLambdaENIManagementAccess	None	Provides minimum permissions for a La...
☑	▸	AWSLambdaExecute	Permissions policy (6)	Provides Put, Get access to S3 and full a...
□	▸	AWSLambdaFullAccess	Permissions policy (4)	Provides full access to Lambda, S3, Dyn...
□	▸	AWSLambdaInvocation-DynamoDB	None	Provides read access to DynamoDB Stre...
□	▸	AWSLambdaKinesisExecutionRole	None	Provides list and read access to Kinesis ...

Set permissions boundary

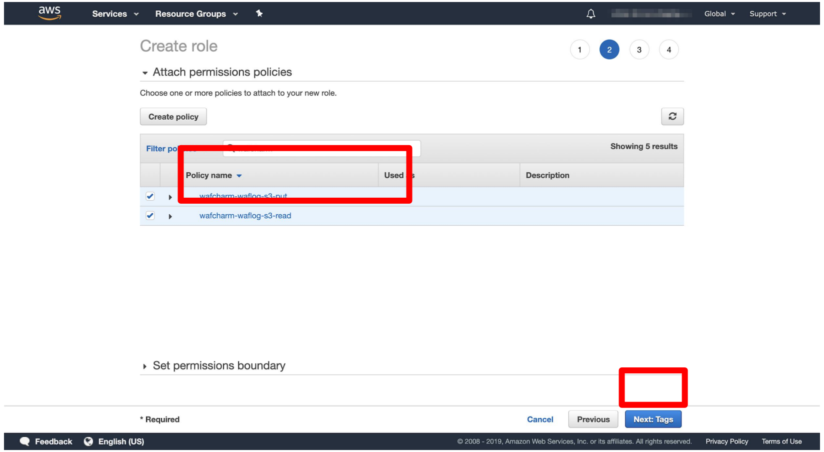
* Required

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enter「lambda」in Filter policies and

Select「AWSLambdaExecute」from the list.

2.8. Create a role for Lambda to integrate with WafCharm



Create role

Attach permissions policies

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

Filter po

Showing 5 results

	Policy name	Used s	Description
☑	wafcharm-waflog-s3-put		
☑	wafcharm-waflog-s3-read		

Set permissions boundary

* Required

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

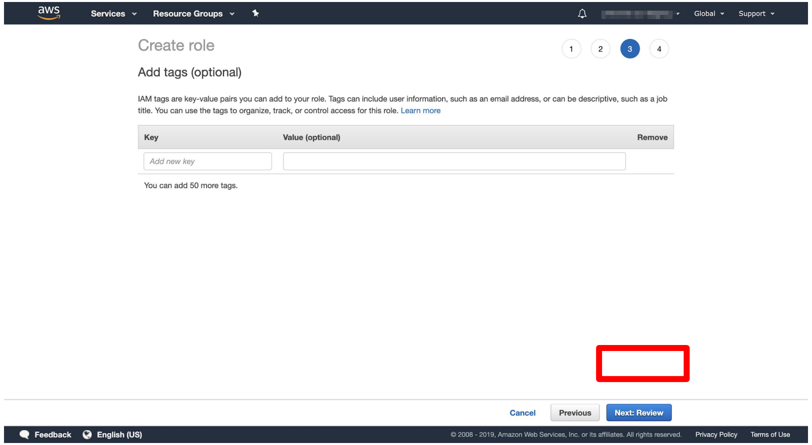
Enter「wafcharm」in Filter policies and select the following from the list.

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

※ Policies created in Step 2.3. and Step 2.5.

Click「Next: Tags」

2.9. Create a role for Lambda to integrate with WafCharm



Create role

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. Learn more

Key	Value (optional)	Remove
Add new key		

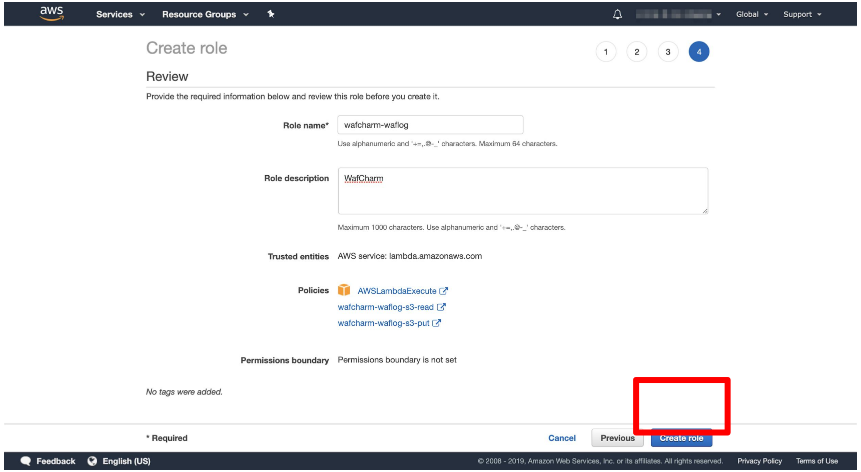
You can add 50 more tags.

Cancel
Previous
Next: Review
Feedback
English (US)
© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Adding tags is optional.

Click「Next: Review」

2.10. Create a role for Lambda to integrate with WafCharm



Create role

Review

Provide the required information below and review this role before you create it.

Role name* wafcharm-waflog

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description WafCharm

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

Trusted entities AWS service: lambda.amazonaws.com

Policies AWSLambdaExecute
wafcharm-waflog-s3-read
wafcharm-waflog-s3-put

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

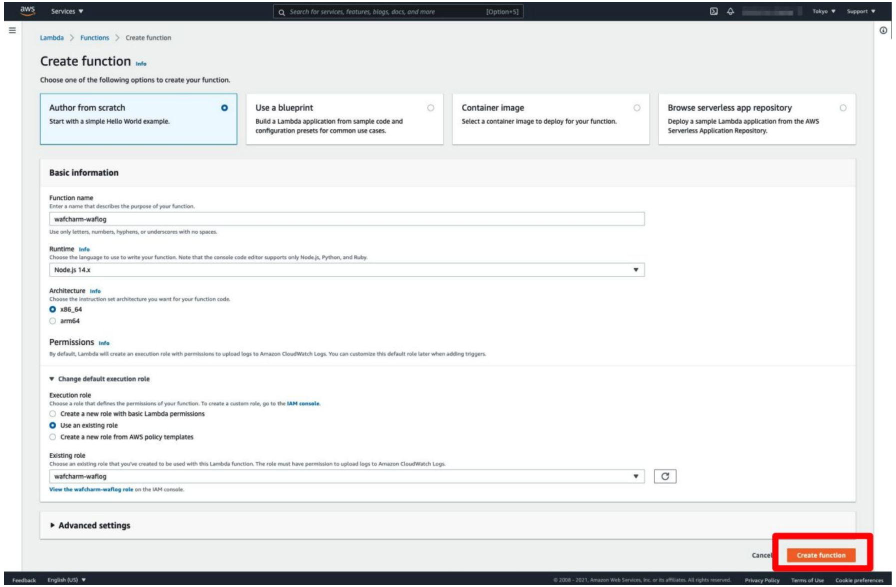
© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Role name:
wafcharm-waflog (Arbitrary)

Role description :
WafCharm (Arbitrary)

Click「Create role」

2.11. Create Lambda


aws
Services ▼
Search for services, features, blogs, docs, and more
[Option+S]
[redacted]
Tokyo ▼
Support ▼
Lambda > Functions > Create function
Info
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

Create function

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

Permissions
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

Function name : wafcharm-waflog (Arbitrary)

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

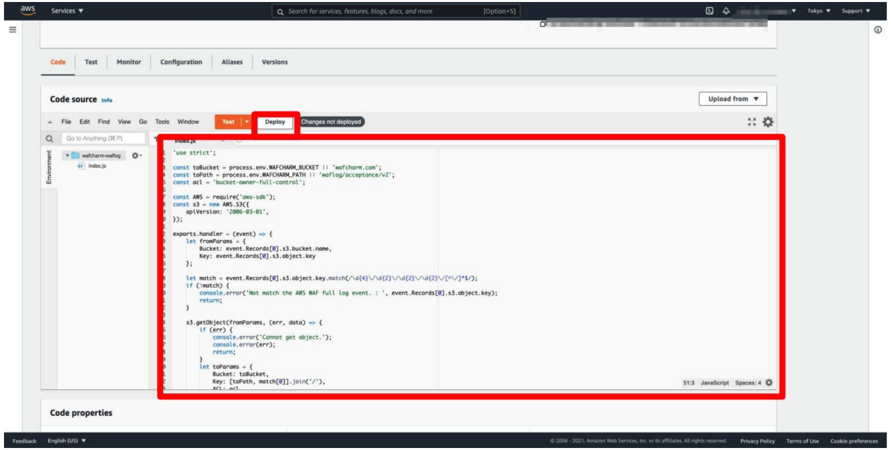
Execution Role : Use an existing role

Existing Role : wafcharm-waflog
※ Created in Step 2.10.

※ Make sure to create it in the same region as the S3 bucket specified in Step 1.4.

Click「Create function」

2.12. Create Lambda（Code Source)



```
'use strict';

const toBucket = process.env.WAFCHARM_BUCKET || 'wafcharm.com';
const toPath = process.env.WAFCHARM_PATH || 'waflog/acceptance/v2';
const acl = 'bucket-owner-full-control';

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

exports.handler = (event) => {
    let fromParams = {
        Bucket: event.Records[0].s3.bucket.name,
        Key: event.Records[0].s3.object.key
    };

    let match = event.Records[0].s3.object.key.match(/\d{4}\/\d{2}\/\d{2}\/\d{2}\/[^\/]*$/);
    if (!match) {
        console.error('Not match the AWS WAF full log event. : ', event.Records[0].s3.object.key);
        return;
    }

    s3.getObject(fromParams, (err, data) => {
        if (err) {
            console.error('Cannot get object.');
            console.error(err);
            return;
        }
        let toParams = {
            Bucket: toBucket,
            Key: [toPath, match[0]].join('/'),
            ACL: acl
```

Code source :

Paste the following source code

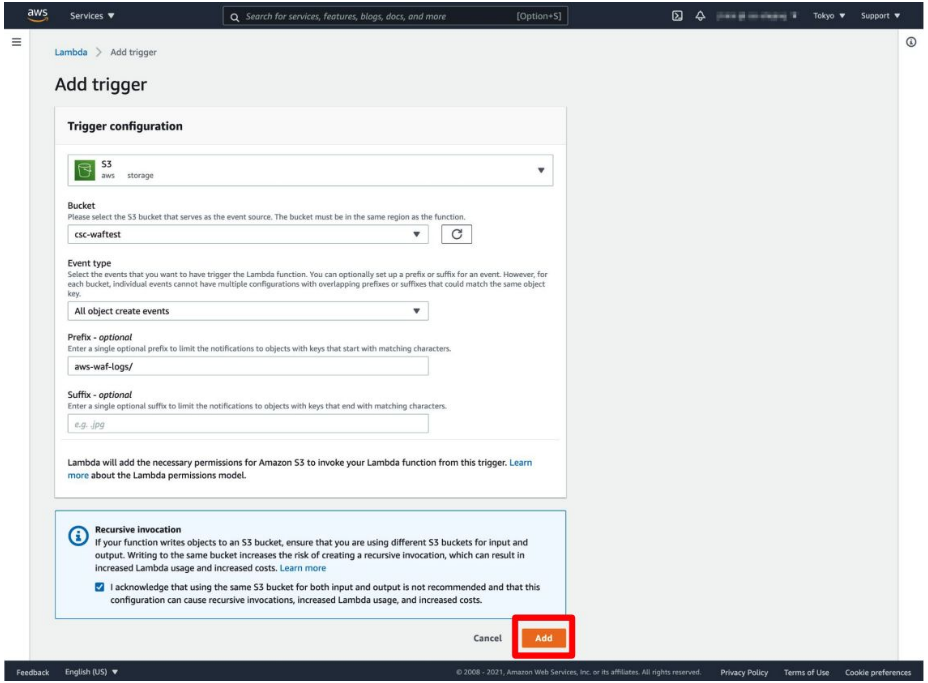
http://docs.wafcharm.com/manual/new_aws_waf/index.js

※ 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」

2.13. 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.
csc-waftest

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.
aws-waf-logs/

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

Trigger configuration:

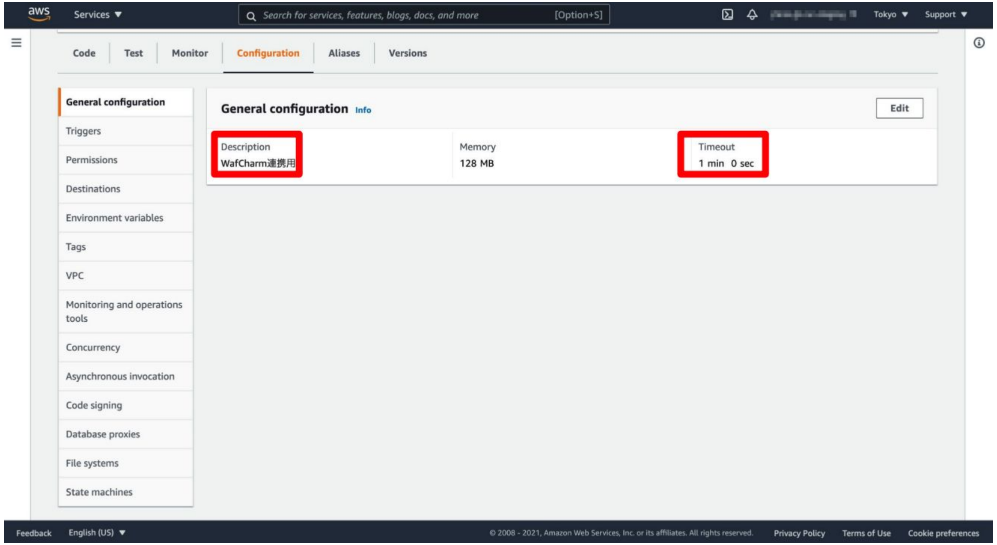
Bucket: Select the S3 bucket setup in Step 1.4.

Event Type: Select “All object create events”

Prefix : Enter the prefix setup in Step 1.4.

Click「Add」

2.14. Create Lambda



General configuration

Description
WafCharm連携用

Memory
128 MB

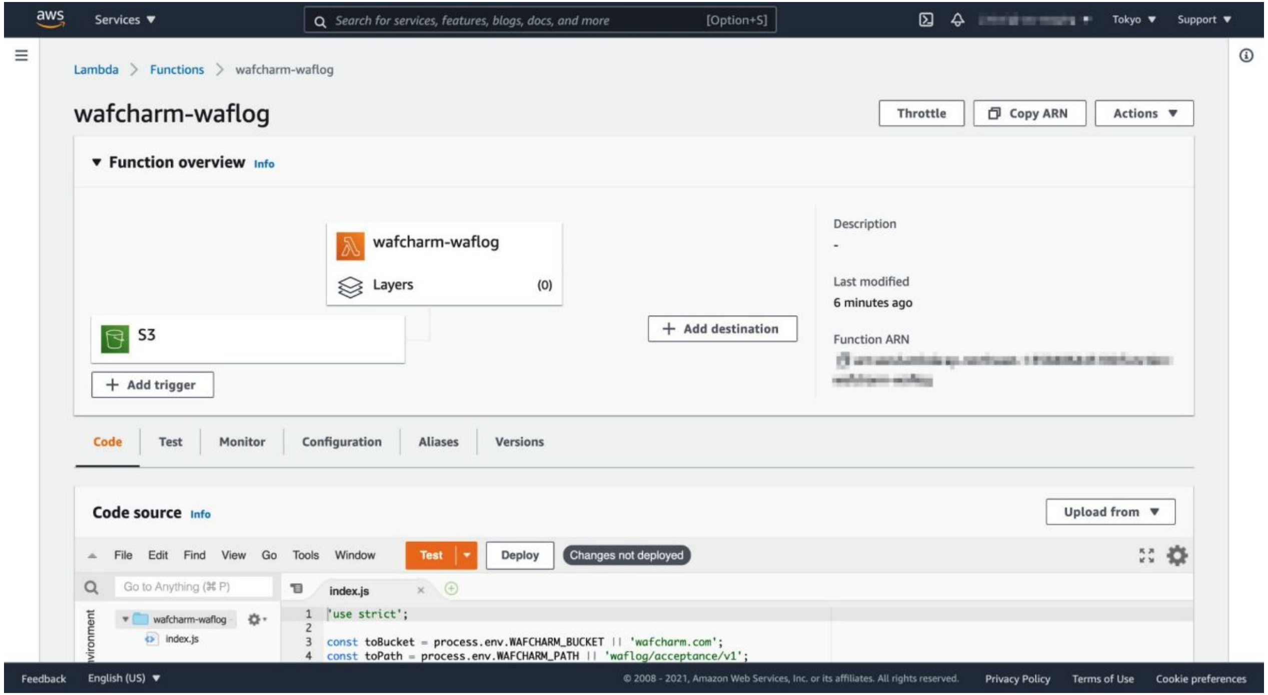
Timeout
1 min 0 sec

General configuration

Description : For WafCharm integration (Arbitrary)

Timeout : 1 min.

2.15. Create Lambda



wafcharm-waflog

Description
-

Last modified
6 minutes ago

Function ARN
[redacted]

```
'use strict';

const toBucket = process.env.WAFCHARM_BUCKET || 'wafcharm.com';
const toPath = process.env.WAFCHARM_PATH || 'waflog/acceptance/v1';
```

Complete

2.16. 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.

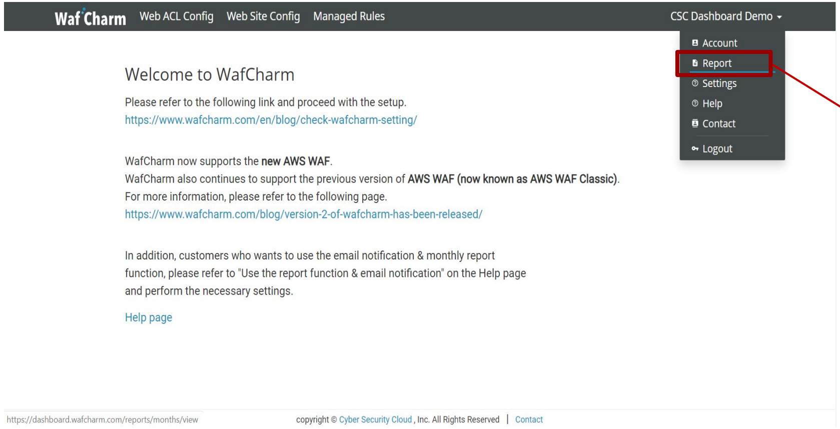
2. Detection in the previous month.

※ 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/

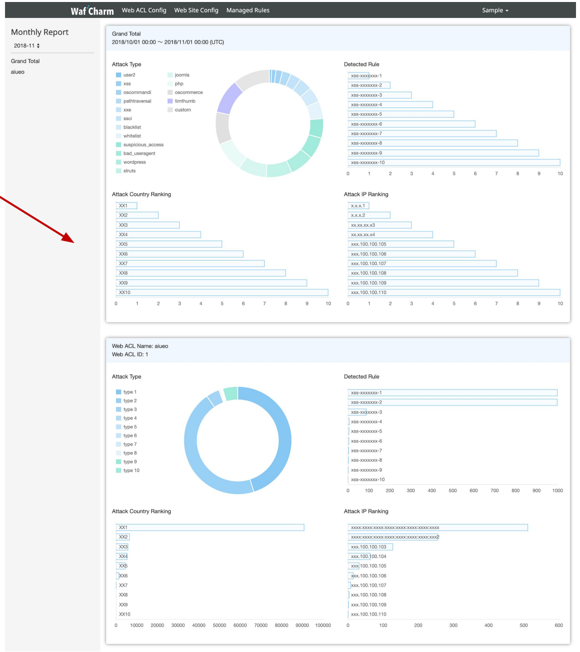
WafCharm now supports the **new AWS WAF**.
WafCharm also continues to support the previous version of **AWS WAF (now known as AWS WAF Classic)**.
For more information, please refer to the following page.
https://www.wafcharm.com/blog/version-2-of-wafcharm-has-been-released/

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.

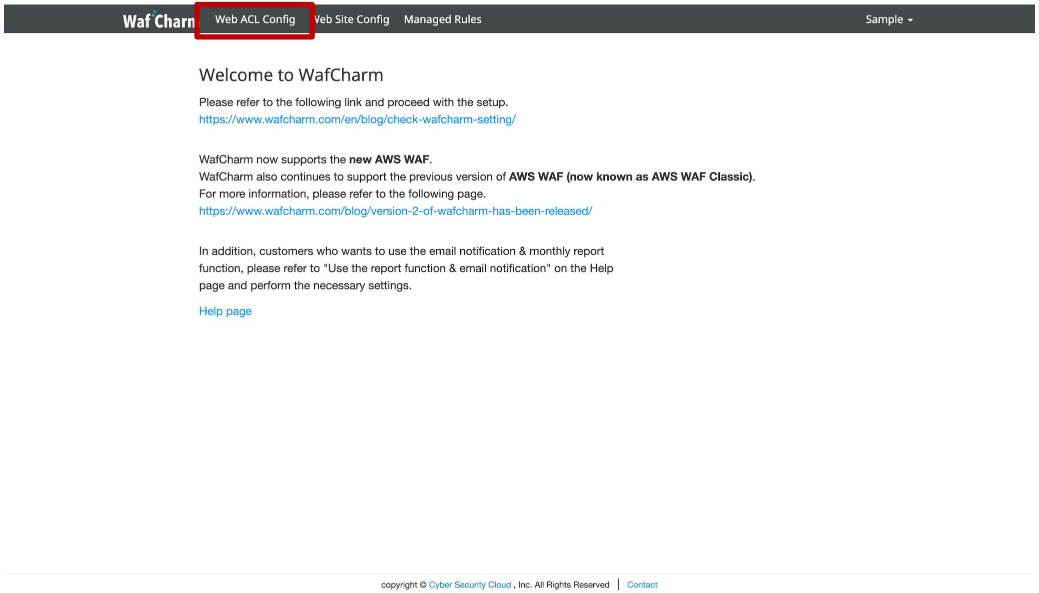
※ The above report is an image only

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.

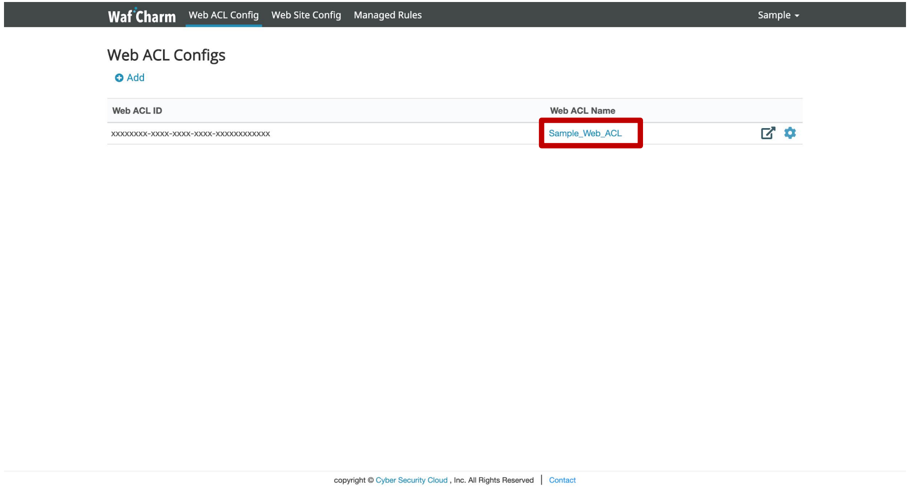
Help page

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

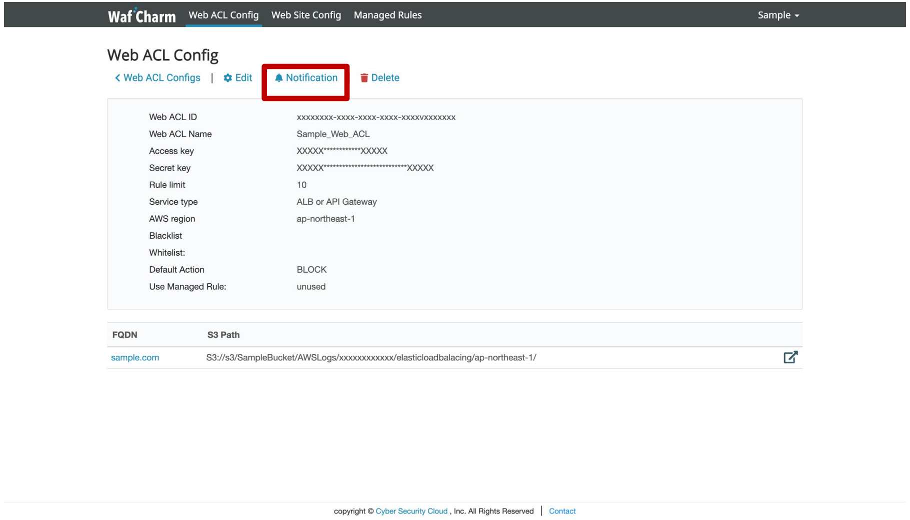
⊕ Add

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

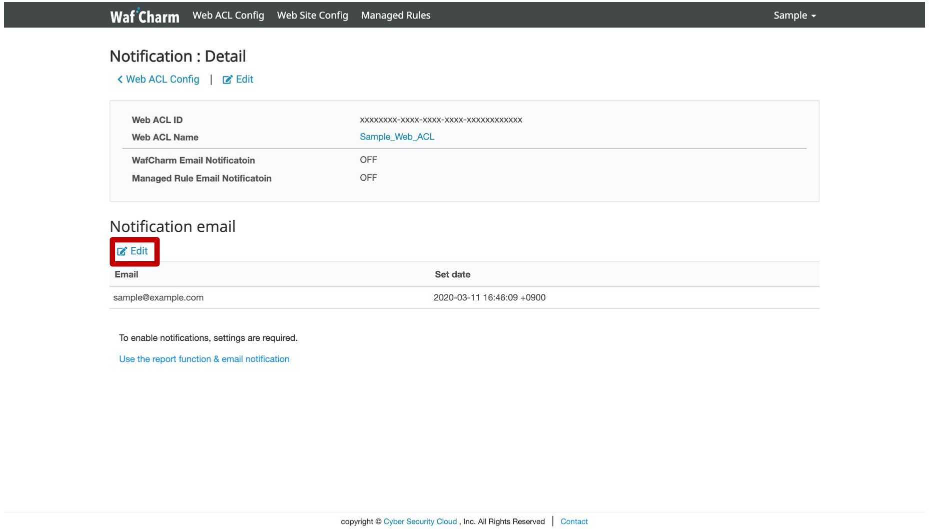
Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxvxxxxxxx
Web ACL Name	Sample_Web_ACL
Access key	XXXXX************XXXXX
Secret key	XXXXX**************************XXXXX
Rule limit	10
Service type	ALB or API Gateway
AWS region	ap-northeast-1
Blacklist	
Whitelist:	
Default Action	BLOCK
Use Managed Rule:	unused

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.

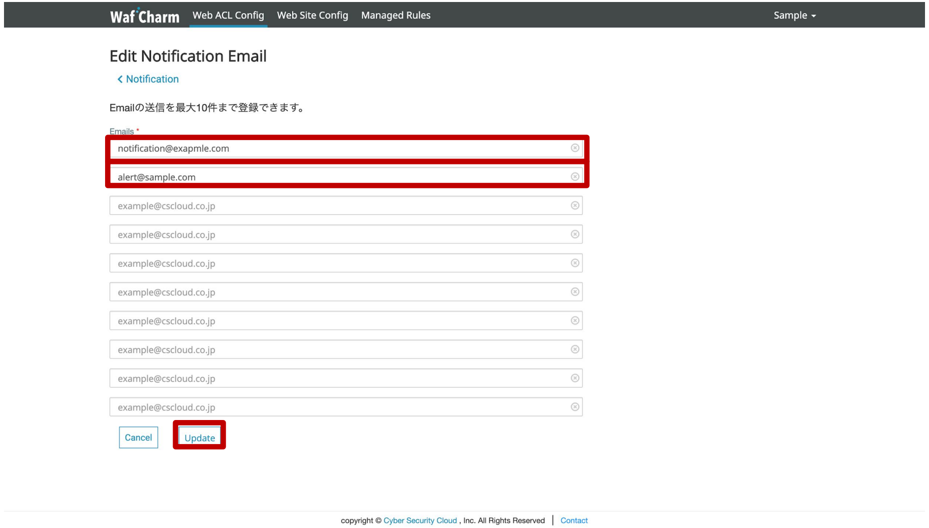
Use the report function & email notification

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

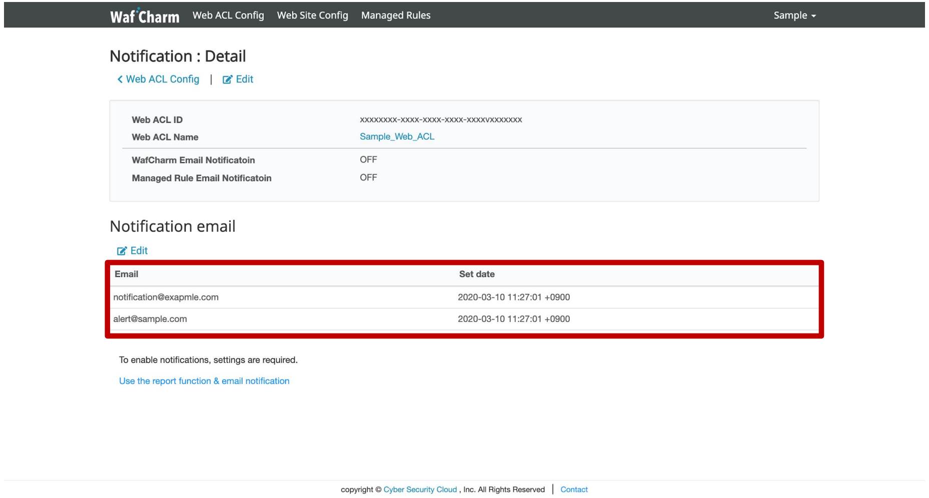
example@cscloud.co.jp

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

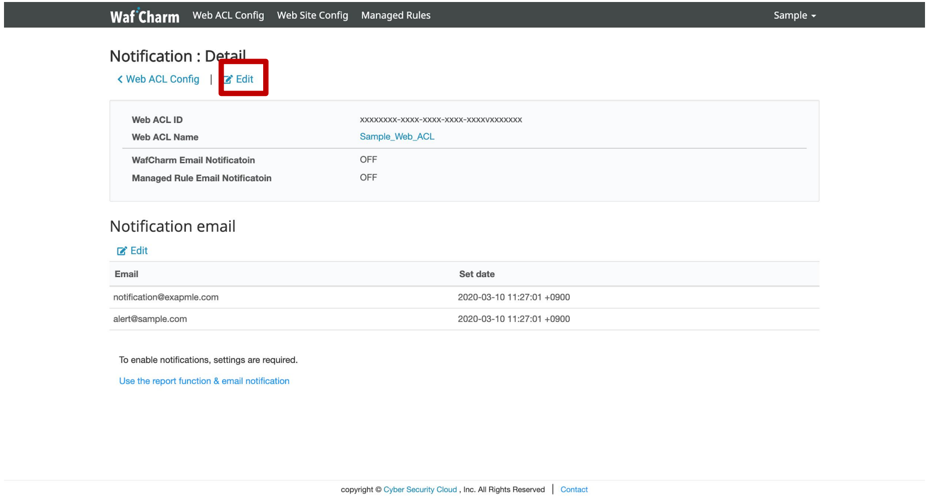
To enable notifications, settings are required.

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

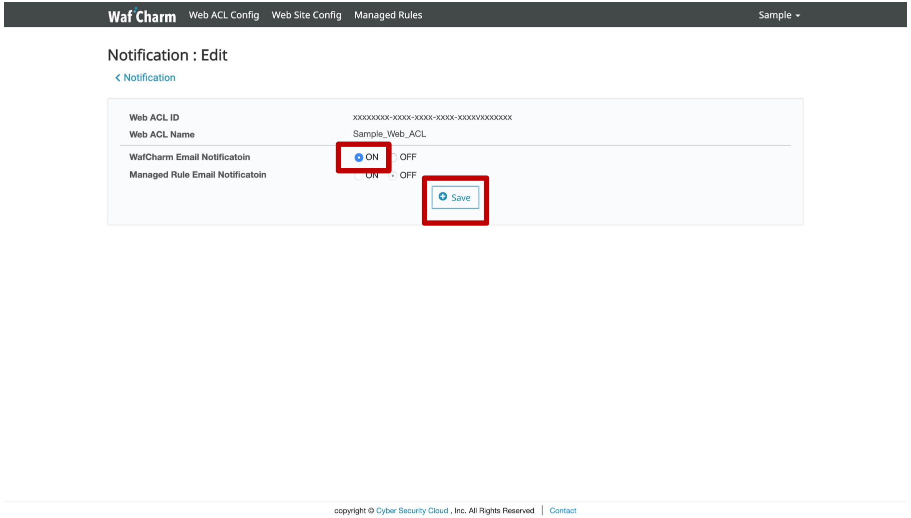
To enable notifications, settings are required.

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

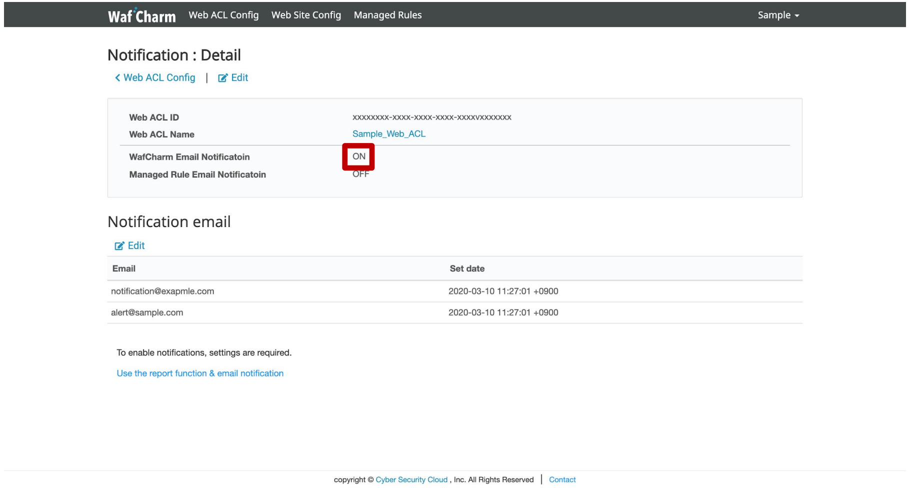
Web ACL ID xxxxxxxx-xxxx-xxxx-xxxx-xxxxvxxxxxxx
Web ACL Name Sample_Web_ACL

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

Notification email

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 varies according to the values set in the “Buffer intervals” and “Buffer size” in the Step 1.5. Kinesis Firehose Setting.

- 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 "Delivery Stream Name" that you set in Step 1.2.
  - 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.

- If you register a Web ACL with a different version of AWS WAF in WafCharm and use this feature in each Web ACL, please create Kinesis Data Firehose and Lambda for each version.
  - If the version is same, it is possible to share Kinesis Data Firehose and Lambda.

- 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.

6. Other additional information

- This reporting/notification function is available only when Logging destination (1.10) is Kinesis Data Firehose (as of 2021/11)