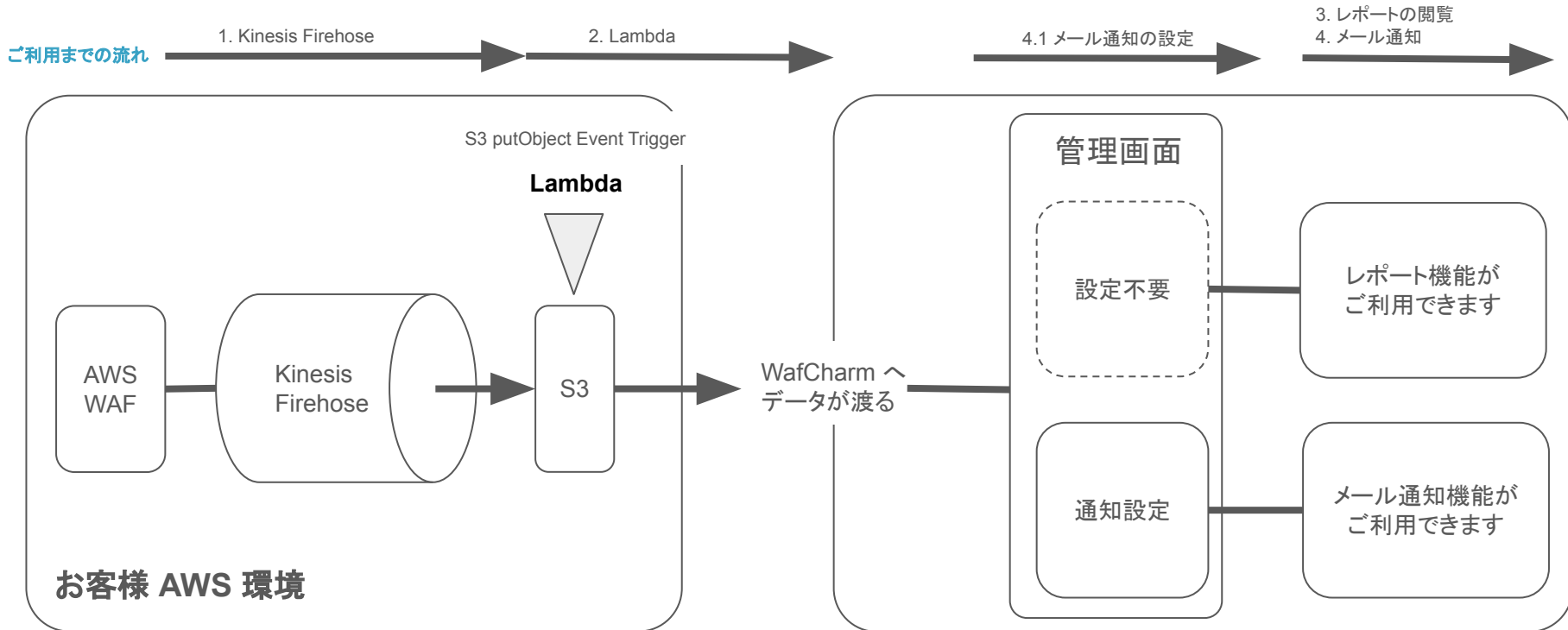


レポート機能/通知機能 利用マニュアル
new AWS WAF
Ver 1.6

レポート機能/通知機能のアーキテクチャ概要



本手順を実施頂く上で必要な権限

AWSにおいてデフォルトで用意されている権限ポリシーをご利用される場合の例となります

Permissions

Groups (2)

Tags

Security credentials

Access Advisor

▼ Permissions policies (18 policies applied)

Add permissions

+ Add inline policy

Policy name ▼	Policy type ▼	
Attached directly		
▶  AWSLambdaFullAccess	AWS managed policy	✕
▶  IAMFullAccess	AWS managed policy	✕
▶  CloudWatchFullAccess	AWS managed policy	✕
▶  AmazonKinesisFirehoseFullAccess	AWS managed policy	✕

レポート機能/通知機能の作業概要 (1/2)

レポート機能、および通知機能をご利用されたい場合には、まずはお客様 AWS環境にて下記 1 と 2 の作業を完了させる必要があります

1. Kinesis Firehose

- Kinesis Firehose の構築/設定
- Kinesis Firehose 実行用の role 設定
- Kinesis Firehose と AWS WAF との連携設定
- 1 章の完了確認

2. Lambda

- WAFLog 出力先 S3 の read 権限 policy 作成
- WafCharm 連携用 S3 の put 権限 policy 作成
- WafCharm 連携用 Lambda の role 作成
- Lambda 構築/設定

3. レポート機能をご利用される場合

- WafCharm 管理画面にて、月次レポートの閲覧

レポート機能/通知機能の作業概要 (2/2)

1 と 2 の作業が完了しましたら、ご利用されたい機能別に設定すべき事項が異なりますので、本マニュアルに沿って機能をご利用ください

4. メール通知機能をご利用される場合

- メール通知先の設定
- メール通知の設定
- メール通知内容

5. 通知機能に関する補足事項

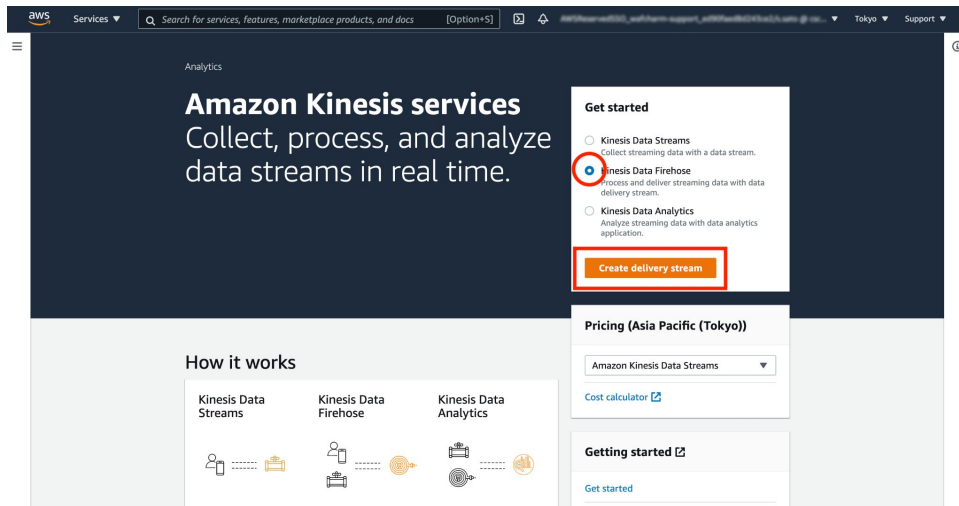
6. その他補足事項

1. Kinesis Firehose

WAF ログを S3 に転送する Kinesis Firehose を設定

- Kinesis Firehose の構築/設定
- Kinesis Firehose 実行用の Role 設定
- Kinesis Firehose と AWS WAF との連携設定
- 1 章の完了確認

1.1. Kinesis Firehose 設定



「Get started」より「Kinesis Data Firehose」を選択し、「Create delivery Stream」をクリックします

適用予定のAWS WAF(Web ACL)と同じリージョンで作成

※ CloudFront でのご利用の方はリージョンを「バージニア」にして作業を進めてください

1.2. Kinesis Firehose 設定

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

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 Info
Direct PUT

Destination Info
Amazon S3

Delivery stream name

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

Transform and convert records - optional
Configure Kinesis Data Firehose to transform and convert your record data.

「Choose source and destination」

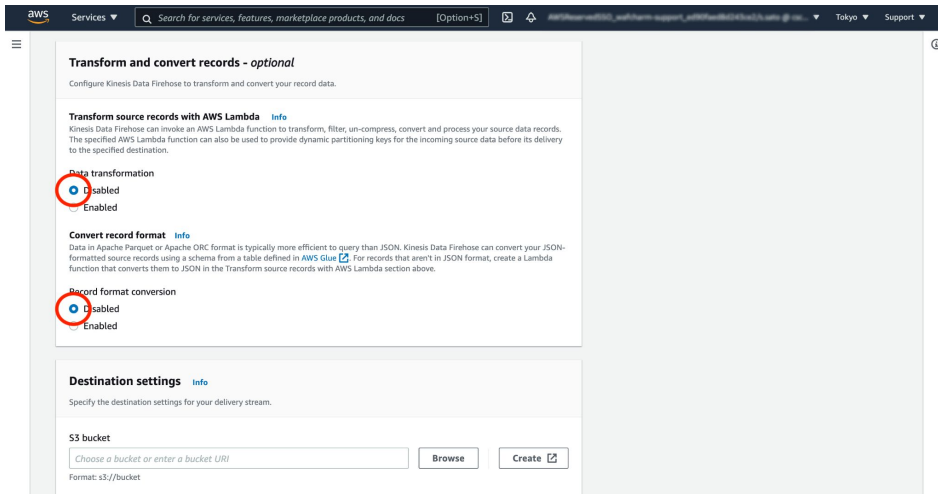
Source : Direct PUT

Destination : Amazon S3

Delivery Stream Name :
aws-waf-logs-＜任意の文字列＞

※ Delivery Stream Name は、先頭に "aws-waf-logs-" を付けるという制限がありますので、ご注意ください

1.3. Kinesis Firehose 設定



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

Format: s3://bucket

下記は使用しません (Disabled)

- Transform source records with AWS Lambda
- Convert record format

1.4. Kinesis Firehose 設定

Destination settings [Info](#)

Specify the destination settings for your delivery stream.

S3 bucket

csc-waf-test

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 GB of partitioned data. For more information, see [Kinesis Data Firehose pricing](#).

☒ Enabled
☐ Disabled

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 :

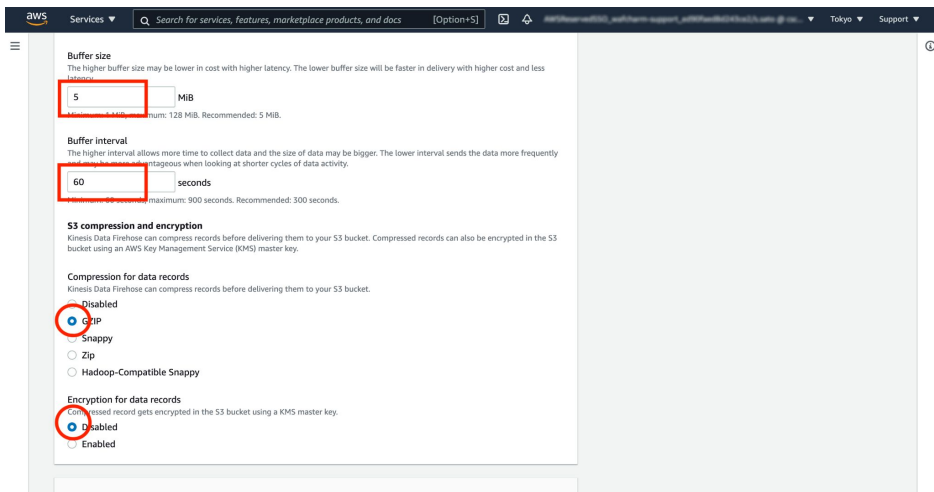
任意の S3bucket を指定 (ex : csc-waf-test)

Prefix :

任意の Prefix を指定 (ex : waflog/)

※ Prefix は、「 waflog/ 」というように必ず「 / 」を付けるようにしてください

1.5. Kinesis Firehose 設定



Buffer intervals :
推奨は 60 seconds

Buffer size :
推奨は 5 MB

※ Buffer intervals、またはBuffer size に達した時点で S3 にログが作成されます

S3 compression :
GZIP

S3 encryption :
Disable

1.6. IAM role 設定

aws Services Search for services, features, marketplace products, and docs [Option+S] 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** [KinesisFirehoseServiceRole-PUT-S3-K-ap-northeast-1-1635830651175](#)
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.

[Add new tag](#)
You can add up to 50 more tags.

Cancel [Create delivery stream](#)

IAM Role : 新しいIAM ロールの作成 or 選択

「Create delivery stream」

1.7. Kinesis Firehose 設定

The screenshot displays the AWS Management Console interface for configuring a Kinesis Firehose delivery stream. The top navigation bar includes the AWS logo, 'Services' dropdown, a search bar, and regional settings for Tokyo. A blue banner at the top indicates the stream is in a 'Creating' state, with a note that it may take up to 5 minutes for the status to update.

The main content area shows the 'aws-waf-logs-xxxx-xxxx' delivery stream details. A 'Delete delivery stream' button is located in the top right corner. The 'Delivery stream details' section contains the following information:

Delivery stream details	
Status	Creating
Destination	Amazon S3
Data transformation	Disabled
Creation time	November 12, 2021, 15:58 GMT+9
Source	Direct PUT
ARN	arn:aws:kinesis:ap-northeast-1:123456789012:delivery-stream/xxxx-xxxx-xxxx-xxxx
Dynamic partitioning	Disabled

Below the details, there is a 'Test with demo data' section with a link to 'Test with demo data' and a note about standard Amazon Kinesis Data Firehose charges.

The 'Monitoring' tab is selected, showing 'Delivery stream metrics'. The metrics section includes a time range selector (1h, 3h, 12h, 1d, 3d, 1w, Custom) and a chart area with three panels: 'Incoming bytes' (Byes), 'Incoming put requests' (Count), and 'Incoming records' (Count). The bottom of the console shows the footer with 'Feedback', 'English (US)', and copyright information.

待機

1.8. Kinesis Firehose 設定

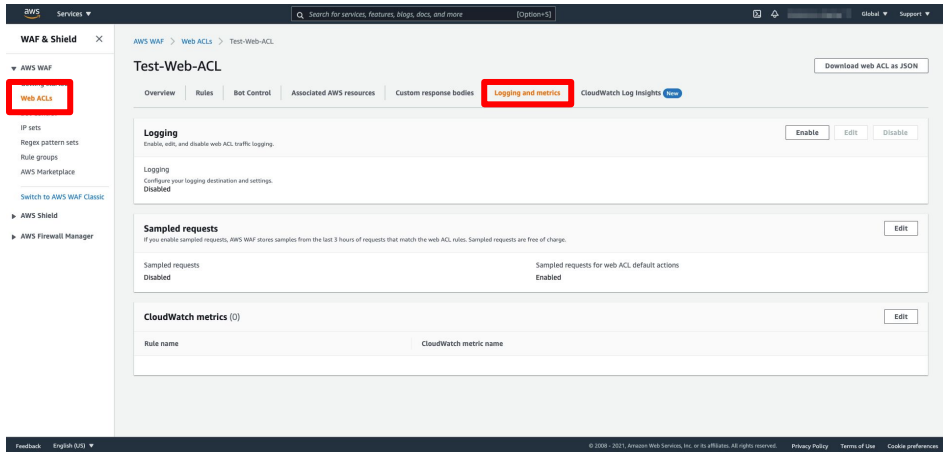
The screenshot displays the AWS Management Console interface for an Amazon Kinesis Firehose delivery stream. At the top, a green banner indicates that the stream 'aws-waf-logs-xxxx-xxxx' was successfully created. The main content area is titled 'aws-waf-logs-xxxx-xxxx' and includes a 'Delete delivery stream' button. Below this, the 'Delivery stream details' section shows the following information:

Property	Value
Status	Active
Source	Direct PUT
Destination	Amazon S3
ARN	arn:aws:kinesis:us-east-1:123456789012:stream/aws-waf-logs-xxxx-xxxx
Data transformation	Disabled
Dynamic partitioning	Disabled
Creation time	November 12, 2021, 15:58 GMT+9

Below the details, there is a section for 'Test with demo data' with an 'Info' link. The 'Monitoring' tab is selected, showing 'Delivery stream metrics'. The metrics section includes three cards: 'Incoming bytes' (1 Bytes), 'Incoming put requests' (1 Count), and 'Incoming records' (1 Count). The bottom of the console shows the footer with 'Feedback', 'English (US)', and copyright information for 2008-2021 Amazon Web Services, Inc.

完了

1.9. Kinesis Firehose と AWS WAF との連携設定



サービス “AWS WAF” に戻り

“Web ACLs” > “Logging and metrics”
を選択

「Enable Logging」

1.10. Kinesis Firehose と AWS WAFとの連携設定

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

AWS WAF > Web ACLs > Test-Web-ACL > 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 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 create a delivery stream before you can enable logging.

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](#)

Feedback English [US]

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

Logging destination:

Kinesis Data Firehose stream を選択

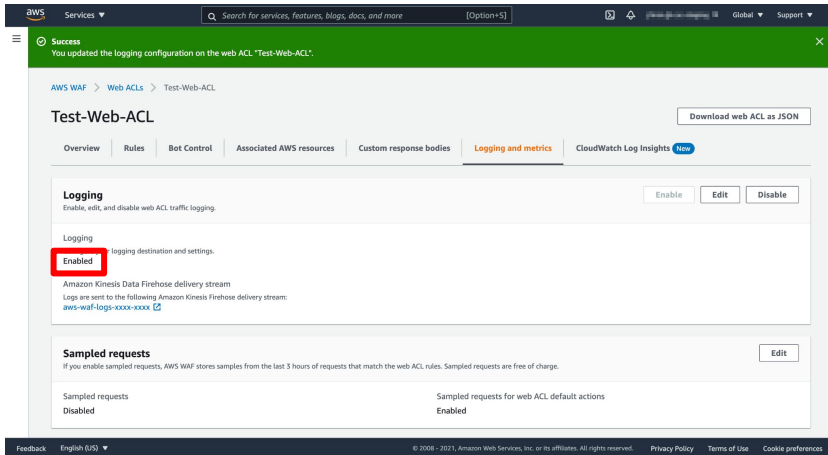
※本レポート機能/通知機能をご利用の場合、Logging destination は Kinesis Data Firehose のみ対応となります。

Amazon Kinesis Data Firehose delivery streams には自身で命名した Delivery Stream Name を選択

※ 1.2 で指定したもの

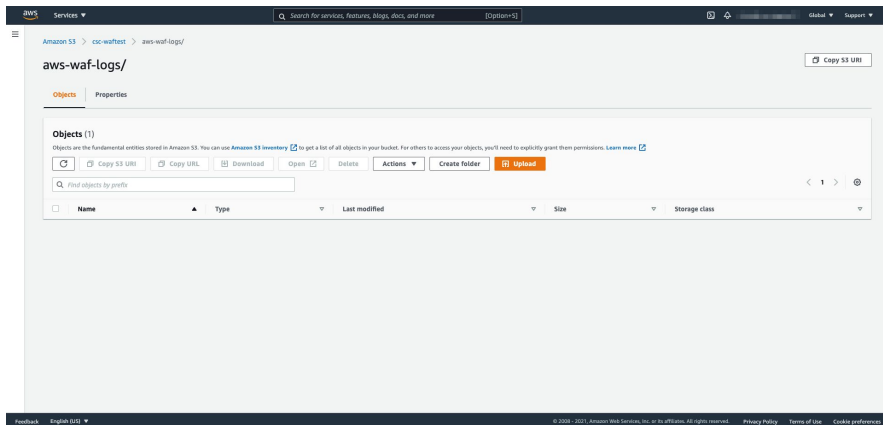
「Save」

1.11. Kinesis Firehose と AWS WAF との連携設定



Logging が、“Enabled” になっていることを確認

1.12. 1 章の完了確認

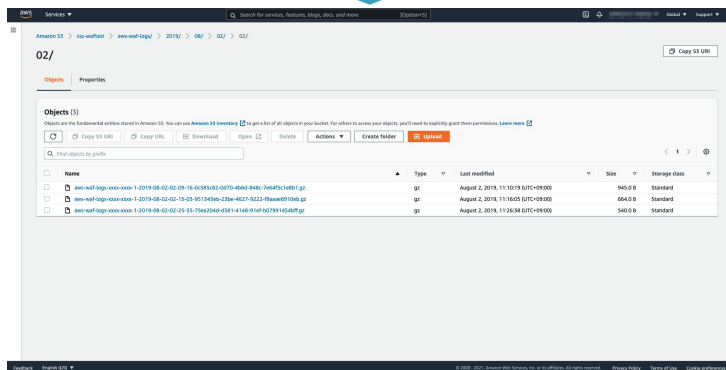
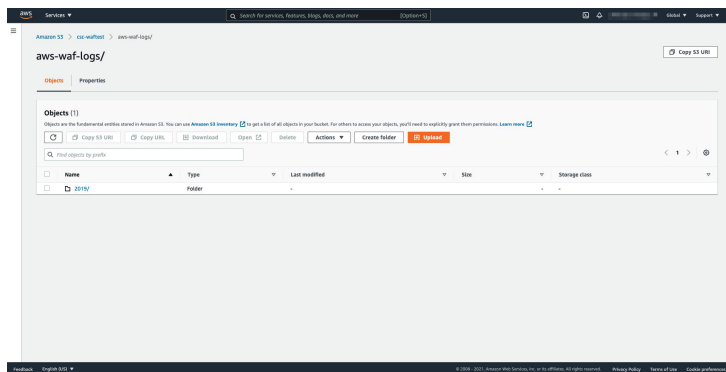


S3 にフルログファイルが生成されているか確認

※ 1.4 で指定したもの

左記の状態ではまだ検知がされておらず、ファイルが生成されていない状態

1.13. 1 章の完了確認



左記のようなファイルが生成されれば

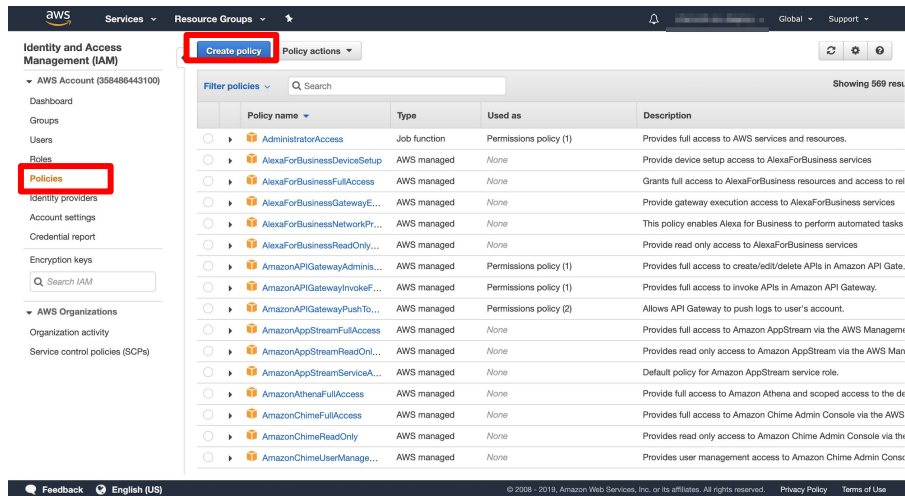
1 章の作業は完了

2. Lambda

顧客側の S3 に出力されたファイルを CSC 側の S3 に転送する設定

- WAFLog 出力先 (顧客側 S3) の read 権限 policy 作成
- WafCharm 連携用 (CSC 側 S3) の put 権限 policy 作成
- WafCharm 連携 Lambda 用の role 作成
- Lambda 構築
- CloudWatch ログ設定変更(Lambda 出力ログ) ※任意

2.1. WAFLog 出力先 read 権限 policy 作成



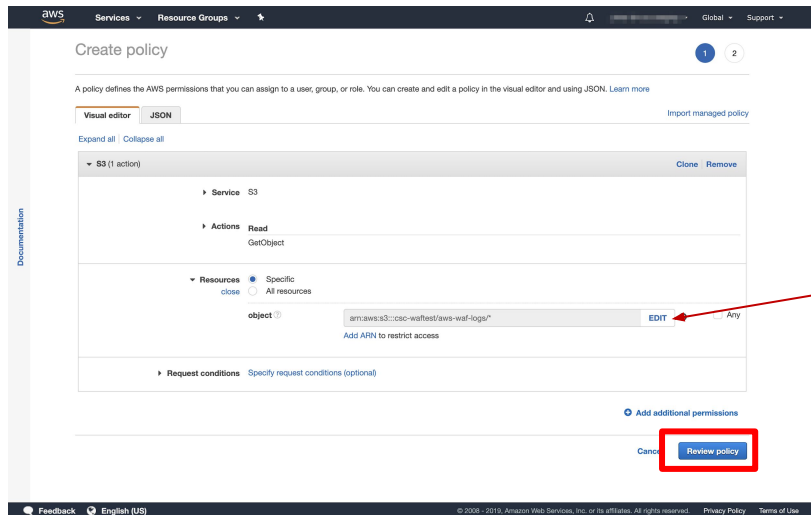
The screenshot shows the AWS IAM console interface. In the top navigation bar, the 'Create policy' button is highlighted with a red box. In the left sidebar, the 'Policies' link is also highlighted with a red box. The main content area displays a table of existing policies.

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 Managem
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 Cons

サービス “IAM” より

“Policy” > “Create policy” を選択

2.2. WAFLog 出力先 read 権限 policy 作成



Service : S3

Action : GetObject

Resources :

arn:aws:s3::csc-waftest/waflog/*

※ 1.4 で設定した内容



※ Resources に指定するパスには必ず “/*” を付けること

「Review policy」

2.3. WAFLog 出力先 read 権限 policy 作成

The screenshot shows the 'Create policy' wizard in the AWS IAM console, specifically the 'Review policy' step. The 'Name' field is 'wafcharm-waflog-s3-read' and the 'Description' field is 'WafCharm'. A summary table is displayed below, showing permissions for S3. At the bottom, the 'Save changes' button is highlighted with a red box.

Create policy

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-waf-test, None ObjectPath string like aws-waf-logs*	

* Required

Cancel Previous **Save changes**

Name:

wafcharm-waflog-s3-read (任意の名前)

Description : WafCharm (任意)

「Create policy」

2.4. WafCharm 連携用 put 権限 policy 作成

aws Services Resource Groups

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](#)

Visual editor JSON Import managed policy

Expand all Collapse all

S3 (2 actions) Clone Remove

Service S3

Actions Write
PutObject
Permissions management
PutObjectAcl

Resources 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

Service : S3

Action : PutObject, PutObjectACL

Resources :

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

※ CSC 側の S3 に対する権限

ARN の追加

Amazon リソースネーム (ARN) は、AWS リソースを一意に識別します。リソースは各サービスに固有です。 [詳細はこちら](#)

S3_object の ARN の指定 ARN を手動でリスト

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

Bucket name * wafcharm.com すべて

Object name * * すべて

キャンセル 追加

「Review policy」

2.5. WafCharm 連携用 put 権限 policy 作成

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 187 services) Show remaining 186			
S3	Limited: Write, Permissions management	BucketName string like wafcharm.com, ObjectPath string like All	None

* Required

Cancel Previous **Create policy**

Name :
wafcharm-waflog-s3-put (任意の名前)

Description : WafCharm (任意)

「Create policy」

2.6. WafCharm 連携 Lambda 用 role 作成

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	Comprehend	ElasticCache	Lex	SMS
AWS Backup	Config	Elastic Beanstalk	License Manager	SNS
AWS Support	Connect	Elastic Container Service	Machine Learning	SWF
Amplify	DMS	Elastic Transcoder	Macie	SageMaker
AppSync	Data Lifecycle Manager	ElasticLoadBalancing	MediaConvert	Security Hub
Application Auto Scaling	Data Pipeline	Forecast	Migration Hub	Service Catalog
Application Discovery Service	DataSync	Glue	OpsWorks	Step Functions
Batch	DeepLens	Greengrass	Personalize	Storage Gateway
	Directory Service	GuardDuty	RAM	

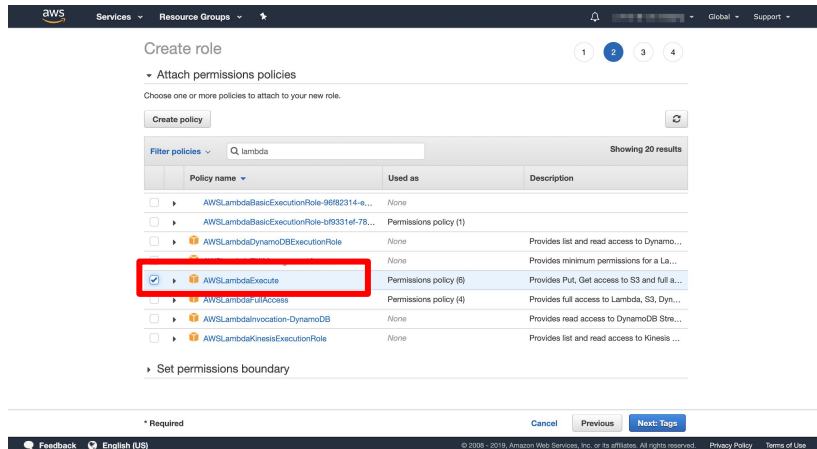
* Required

[Next: Permissions](#)

このロールを使用するサービスを選択 : Lambda

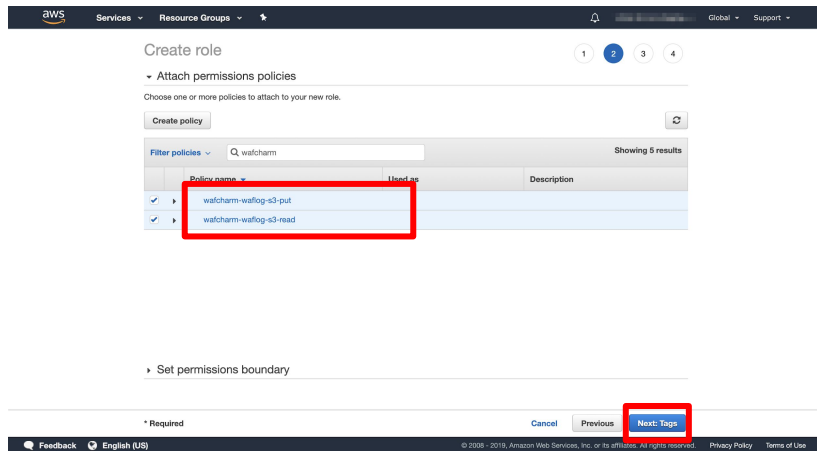
「Next: Permissions」

2.7. WafCharm 連携 Lambda 用 role 作成



フィルターに「lambda」を入力し、一覧の中から
「AWSLambdaExecute」を選択

2.8. WafCharm 連携 Lambda 用 role 作成



フィルターに「wafcharm」を入力し、一覧の中から

「wafcharm-waflog-s3-put」

「wafcharm-waflog-s3-read」

を選択

※ 2.3, 2.5 で作成した policy

「Next: Tags」

2.9. WafCharm 連携 Lambda 用 role 作成

aws Services Resource Groups

Create role 1 2 3 4

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

タグの追加は任意

「Next: Review」

2.10. WafCharm 連携 Lambda 用 role 作成

The screenshot shows the AWS IAM console 'Create role' page, step 4 (Review). The role name is 'wafcharm-waflog', the role description is 'WafCharm', and the trusted entity is 'AWS service: lambda.amazonaws.com'. Policies include 'AWSLambdaExecute', 'wafcharm-waflog-s3-read', and 'wafcharm-waflog-s3-put'. The 'Create role' button is highlighted with a red box.

aws Services Resource Groups

Create role

1 2 3 4

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 Cancel Previous **Create role**

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

Role name:
wafcharm-waflog (任意)

Role description :
WafCharm (任意)

「Create role」

2.11. Lambda 構築

AWS Services ▾ Search for services, features, blogs, docs, and more [Options+] Tokyo ▾ Support ▾

Lambda > Functions > Create function

Create function info

Choose one of the following options to create your function.

Author from scratch info
Start with a simple Hello World example.

Use a blueprint info
Build a Lambda application from sample code and configuration presets for common use cases.

Container image info
Select a container image to deploy for your function.

Browse serverless app repository info
Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

Function name info
Enter a name that describes the purpose of your function.
wafcharm-waflog

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 info
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 info
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

Cancel **Create function**

Feedback English (US) ▾ © 2018 - 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

名前 : wafcharm-waflog (任意)

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

Execution Role : Use an existing role

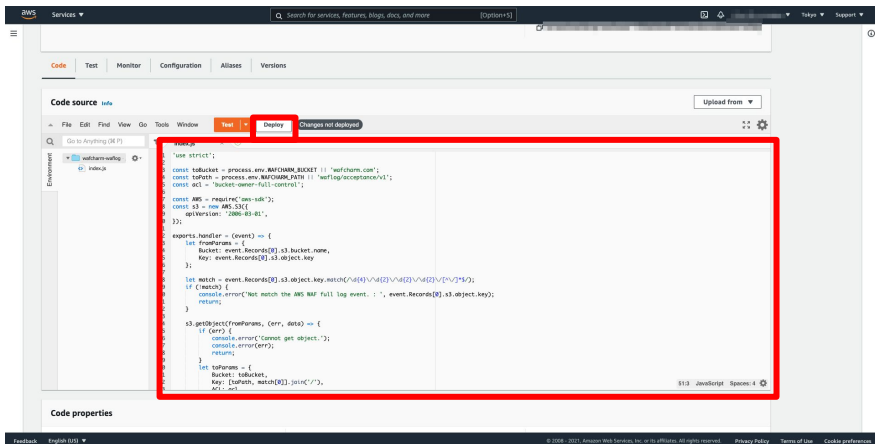
既存のロール : wafcharm-waflog

※ 2.10 で作成したもの

※ 1.4 で指定した S3 のバケットと同じリージョンで作成してください

「Create function」

2.12. Lambda 構築 (関数コード)



Code source:

以下のソースを貼り付け

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

※ ソースは AWS WAF のバージョンで異なりますのでご注意ください

※ Node.js 18.xをご利用頂く場合にはファイル名をindex.mjs から index.js へ変更してください。

「Deploy」

2.13. Lambda 構築 (トリガー)

Lambda > Add trigger

Add trigger

Trigger configuration

S3 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-waf-test

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.
.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.

Cancel **Add**

Add trigger :

トリガーに S3 を選択

トリガーの設定

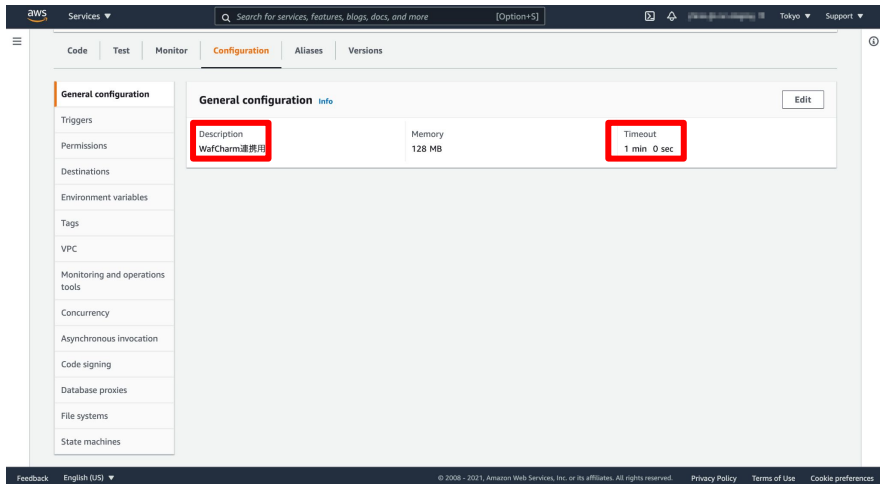
バケット: 1.4 で設定した S3 bucket

イベントタイプ : オブジェクトの作成 (すべて)

プレフィックス : 1.4 で設定した prefix

「Add」

2.14. Lambda 構築

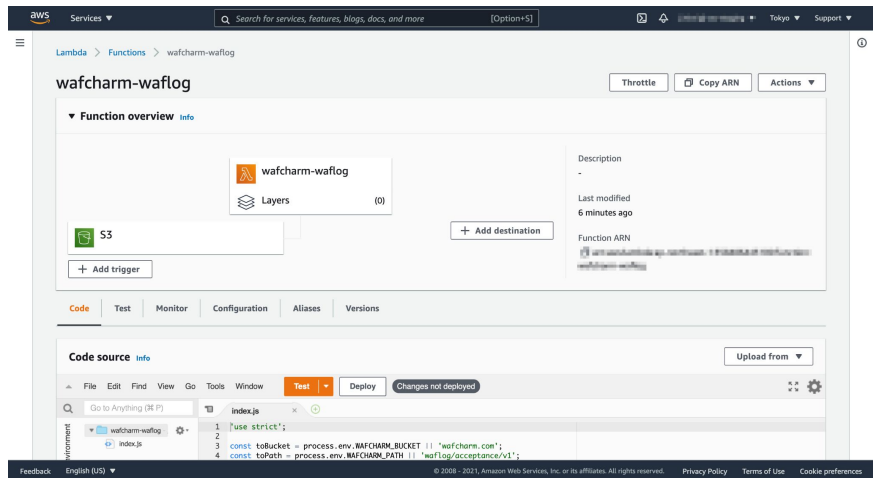


General configuration:

Timeout : 1 分

Description : WafCharm 連携用 (任意)

2.15. Lambda 構築



完了

2.16. CloudWatch

Lambda 関数実行後でないと作成されません

AWS コンソール > CloudWatch > ログを選択

“次の期間経過後にイベントを失効” “カラムの値が

デフォルト値: “失効しない”

となっているため

必要に応じてログの保存期間を変更してください

3. レポート機能をご利用される場合

レポート機能をご利用頂くには、以下の条件が満たされる必要があります

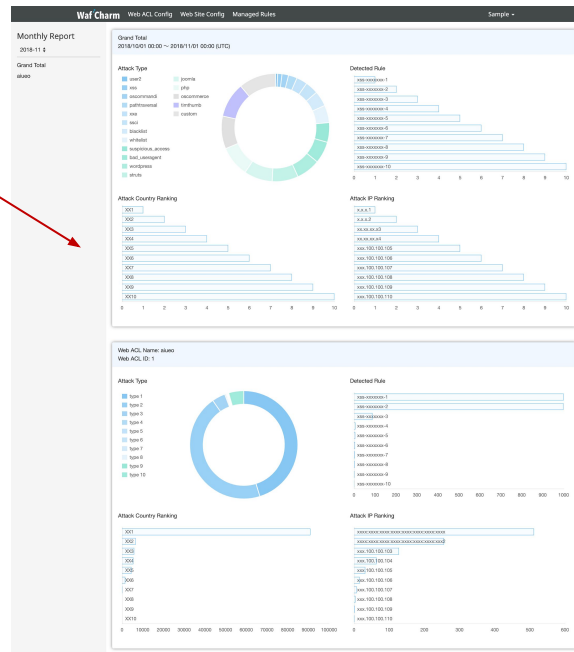
1. 1 ～ 2 章までの設定が完了している
2. 前月に検知があった

※ 前月に検知がなかった方 -> 月次レポートが作成されません

3.1. WafCharm 管理画面にて月次レポートの閲覧

WafCharm 管理画面

右上のメニューより、「Report」を選択



※ レポートは、毎月初旬に前月分が閲覧可能

※ 上記レポートはイメージです

4. メール通知機能をご利用される場合

1 ～ 2 章までの設定が完了し、さらに WafCharm 管理画面にて通知先の設定、通知 ON にするとメールによる検知内容の通知が開始されます

- メール通知先の設定
- メール通知の設定
- メール通知内容

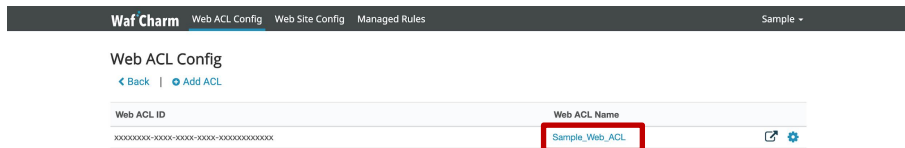
4.1. メール通知先の設定



WafCharm 管理画面

上部メニューより、「Web ACL Config」を選択

4.2. メール通知先の設定



対象の「Web ACL Name」を選択

4.3. メール通知先の設定

WafCharm Web ACL Config Web Site Config Managed Rules Sample ▾

Web ACL Config - Detail

[Back](#) | [Edit](#) | [Notification](#) | [Delete](#)

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

FDQN	S3 Path
sample.com	S3://s3/SampleBucket/AWSLogs/xxxxxxxxxx/elasticloadbalancing/ap-northeast-1/

「Notification」を選択

4.4. メール通知先の設定

WafCharm

Web ACL ConfigWeb Site ConfigManaged Rules

Sample

Notification : Detail

[< Web ACL Config](#) | [Edit](#)

Web ACL ID	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificatoin	OFF
Managed Rule Email Notificatoin	OFF

Notification email

[Edit](#)

Email	Set date
sample@example.com	2020-03-10 11:19:06 +0900

通知を有効にするためには設定が必要です。

[レポート機能/通知機能を利用する](#)

「Notification email」の「Edit」を選択

※ デフォルトは WafCharm 管理画面へのログイン
用メールアドレスが設定されています

4.5. メール通知先の設定

WafCharm Web ACL Config Web Site Config Managed Rules Sample ▾

Edit Notification Email

[← Notification](#)

Emailの送信を最大10件まで登録できます。

Emails *

notification@exapmie.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	⊗

「Emails」に任意のメールアドレスを設定し、
「Update」

※ 最大 10 件まで登録可

4.6. メール通知先の設定

WafCharm Web ACL Config Web Site Config Managed Rules Sample ▾

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

Get info

Email	Set date
notification@example.com	
alert@sample.com	

通知を有効にするためには設定が必要です。
[レポート機能/通知機能を利用する](#)

「Notification email」が設定したメールアドレスに更新されていることを確認

4.7. メール通知の設定

Waf Charm Web ACL Config Web Site Config Managed Rules Sample ▾

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
notification@example.com	
alert@sample.com	

通知を有効にするためには設定が必要です。

[レポート機能/通知機能を利用する](#)

「Edit」を選択

4.8. メール通知の設定

WafCharm Web ACL Config Web Site Config Managed Rules Sample ▾

Notification : Edit
[← Notification](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
Email Address	sample@example.com
WafCharm Email Notification	☒ ON OFF
Managed Rule Email Notification	☐ ON OFF

「WafCharm Email Notification」を「ON」
に変更し、「save」

4.9. メール通知の設定

Waf Charm Web ACL Config Web Site Config Managed Rules Sample ▾

Notification : Detail

[Web ACL Config](#) | [Edit](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificaiton	ON
Managed Rule Email Notificaiton	Off

Notification email

[Edit](#)

Email	Set date
notification@example.com	
alert@sample.com	

通知を有効にするためには設定が必要です。

[レポート機能/通知機能を利用する](#)

「WafCharm Email Notificaiton」が「ON」になっていることを確認

4.10. メール通知内容

検知 (BLOCK/COUNT) された場合、下記のメールが送信されます

- メールタイトル: WafCharm Attack Detected.
- メール差出人: WafCharm Notification wafcharm-notification@cscloud.co.jp
- メール宛先: WafCharm Notification wafcharm-notification@cscloud.co.jp
- メールBCC先: 「Notification email」に登録されているメールアドレス ([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): < お客様 のWeb ACL Name> (< お客様 のWeb ACL ID>)

Matches Rule Name: wafcharm-blacklist-XXX

Time(UTC): Thu, 01 Apr 2020 20:20:00 GMT

Source IP: XXX.XXX.XXX.XXX

Source Country: JP

Action: BLOCK

URI: /

5. 通知機能に関する補足事項

- 1 メール (ログファイル) につき最大 10 件まで検知内容が記載されます
- 通知間隔は、[1.5 Kinesis Firehose 設定](#) の Buffer intervals、Buffer size で設定した値に応じて変化します
- new AWS WAF 仕様の WafCharm では CSC マネージドルールとの連携機能はないため、AWS WAF Classic 仕様で利用可能な CSC マネージドルール専用の通知機能はありません
- お客様作成のルールグループを使用していないルールでの COUNT 検知は通知されません

6. その他補足事項

- お客様の S3 に出力されたログファイルは必要に応じてライフサイクル機能等を用いて定期的 (1ヶ月毎等) に S3 Glacier への退避や削除することを推奨します
- AWS にて対象の IP アドレスの地域を特定できていない場合、月次レポートの国名に「 - 」と出力されることがあります
- 弊社への WAF ログ転送確認をご希望の際は、事前に下記 2 点をご確認の上、[1.2](#) にて設定した「Delivery Stream Name」と対象の Web ACL ID を共有ください
 - Kinesis Data Firehose にて指定した S3 に WAF ログが出力されていること
 - CloudWatch のイベントログに ERROR が出力されていないこと (START/END/REPORTの3行は都度出力されている)
 - ERROR の確認方法
CloudWatch -> Log groups -> /aws/lambda/Lambda 関数名 (マニュアルの場合 : wafcharm-waflog)
-> 最新(一番上)の Log Stream を選択 -> ERROR のメッセージ有無確認

6. その他補足事項

- Lambda 起動後にロール(ポリシー)の権限を編集した場合、動作中の Lambda に変更点が反映されない可能性があるため、index.js の最終行に空白行の追加等を行い、再度デプロイを実施してください
- WafCharm に AWS WAF のバージョンが異なる Web ACL を登録し、各 Web ACL にて本機能を利用する場合、Kinesis Data Firehose、及び Lambda はバージョン毎に作成してください
 - 同じバージョンの場合、Kinesis Data Firehose、及び Lambda を共有することは可能です
- AWS より提供されているログフィルタリング機能の設定については基本的に **非推奨**となります
 - action: Block のみ保存するフィルタリングを設定した場合：
 - BLOCK したログのみ作成されるため、通知機能と月次レポートは BLOCK のログをベースに作成されます
 - action: Count のみ保存するフィルタリングを設定した場合：
 - WafCharm の Count は AWS が定義している Count とは異なるため、通知と月次レポートが正しく機能しません

6. その他補足事項

- WafCharm では Logging destination([1.10](#)) が Kinesis Data Firehose の場合のみ本レポート機能 / 通知機能をご利用いただけます (2021/11 時点)