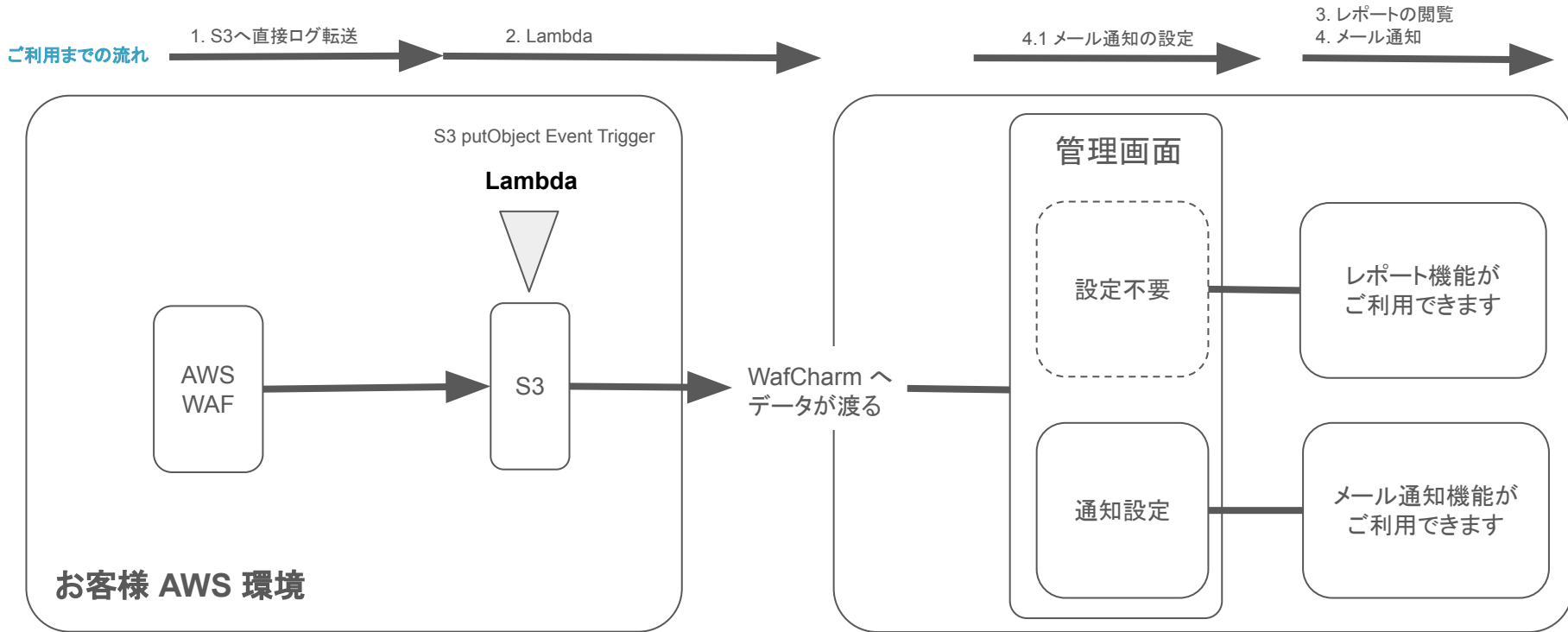


レポート機能/通知機能 利用マニュアル
new AWS WAF (S3)
Ver 1.2

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	×

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. S3へ直接ログ転送

- Web ACLの Logging and metrics設定
- S3 bucket登録
- 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

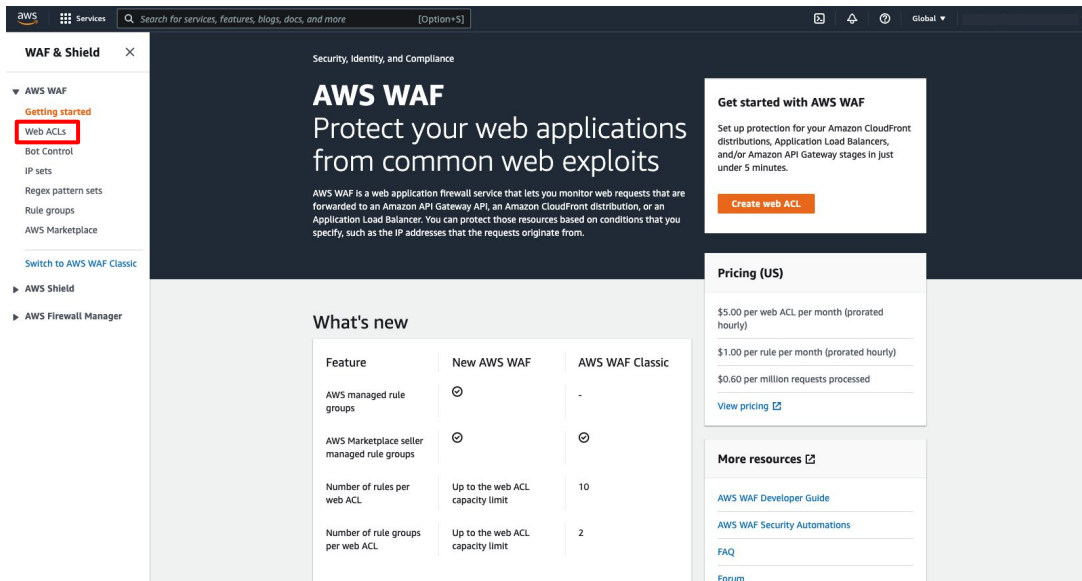
6. その他補足事項

1. S3へ直接ログ転送

WAF ログを S3 に転送するWeb ACL の Logging and metrics を設定

- Web ACLの Logging and metrics設定
- S3 bucket登録
- 1 章の完了確認

1.1. Web ACLの Logging and metrics設定



The screenshot shows the AWS WAF console interface. In the left-hand navigation menu, under the 'AWS WAF' section, the 'Web ACLs' link is highlighted with a red rectangle. The main content area displays the 'AWS WAF' header, a description of the service, a 'Get started with AWS WAF' section with a 'Create web ACL' button, a 'Pricing (US)' section with a table of costs, and a 'What's new' section with a table of features.

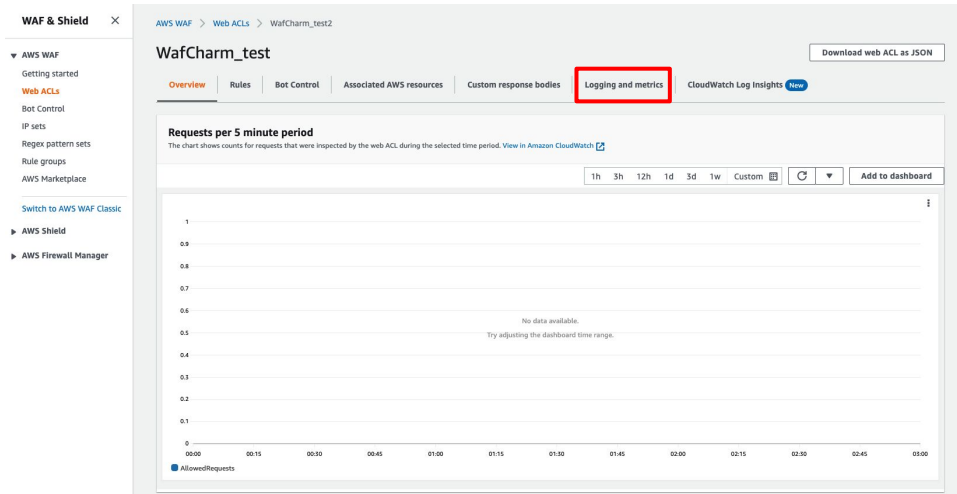
What's new

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

「WAF & Shield」より

「Web ACLs」をクリックします

1.2. Web ACLの Logging and metrics設定



設定をしたい Web ACLを開き

「Logging and metrics」をクリック

1.3. Web ACLの Logging and metrics設定

The screenshot shows the AWS WAF console interface. On the left is a navigation menu with 'WAF & Shield' selected. The main content area is titled 'WafCharm_test' and has a breadcrumb trail 'AWS WAF > Web ACLs > WafCharm_test2'. Below the title are tabs for 'Overview', 'Rules', 'Bot Control', 'Associated AWS resources', 'Custom response bodies', 'Logging and metrics' (which is active), and 'CloudWatch Log Insights'. A 'Download web ACL as JSON' button is in the top right. The 'Logging and metrics' section contains three sub-sections: 'Logging' with an 'Enable' button highlighted by a red box, 'Sampled requests' with an 'Edit' button, and 'CloudWatch metrics (0)' with an 'Edit' button. The 'Logging' sub-section shows 'Logging' is currently 'Disabled'.

Logging の項目の
「Enable」をクリック

※ 既に適用された設定がある場合は、
「Edit」をクリック

1.4. Web ACLの Logging and metrics設定

☰ 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.

Select an S3 bucket ▼  **Create new** [↗](#)

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:

「S3 bucket」を選択

Amazon S3 bucket:

「Create new」をクリック

1.5. S3 bucket 登録

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

aws-waf-logs-xxxxxx

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.

Choose bucket

Bucket name:

aws-waf-logs-**<任意の文字列>**

※ Bucket 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

1.6. S3 bucket 登録

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

Enable logging の編集画面に戻り、
作成した S3 Bucket を選択します

1.7. S3 bucket 登録

≡ 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

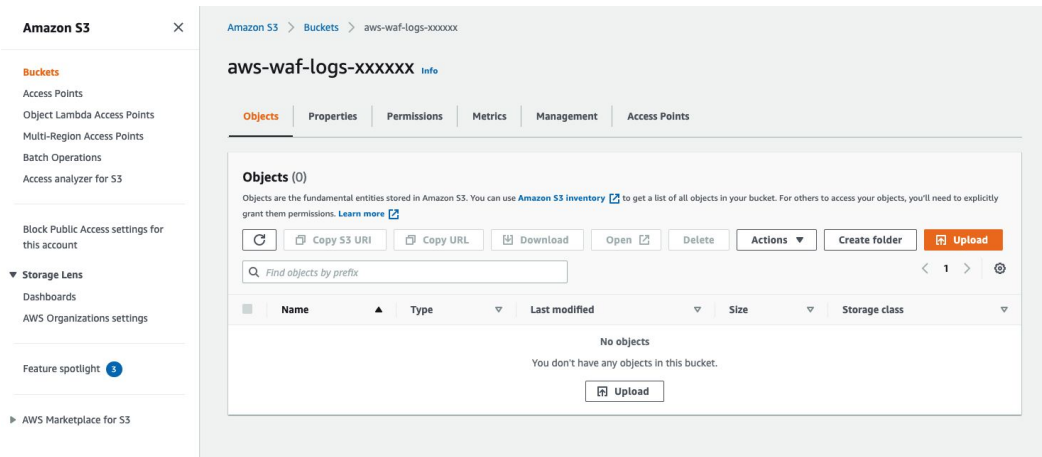
Filter logs
Add filters to control which web requests are logged. If you add multiple filters, AWS WAF evaluates them starting from the top.

No filters

「Save」をクリックすることで、

S3へ直接ログを転送する設定は完了です

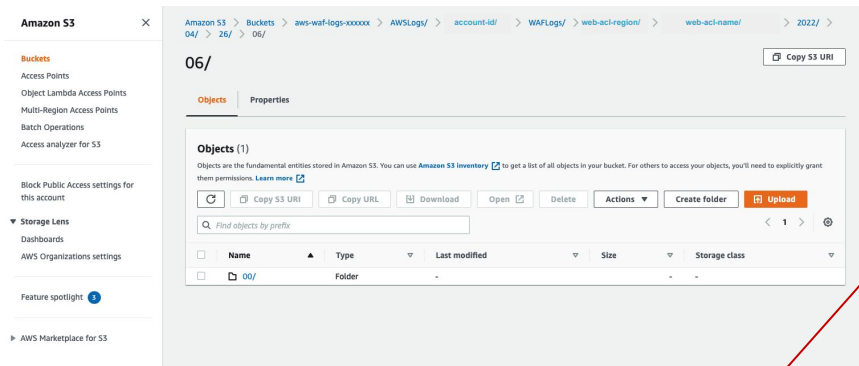
1.8. 1 章の完了確認



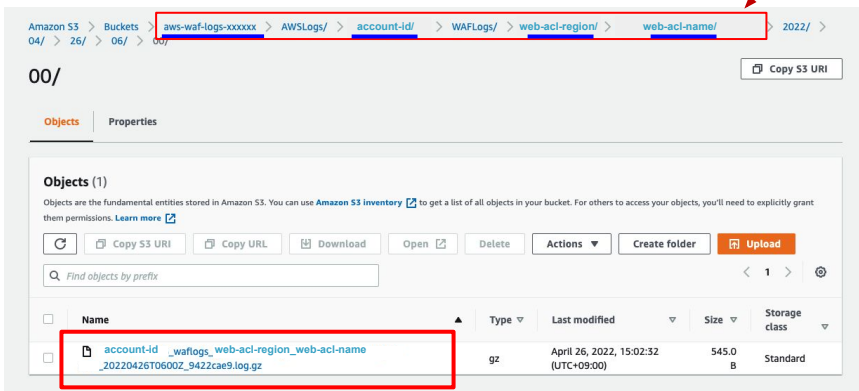
S3 にログファイルが生成されているか確認

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

1.9. 1 章の完了確認



※ こちらの情報を [2.2](#)、[2.11](#)で使います
青線の箇所はお客様の環境によって異なります



左記のようなファイルが生成されれば

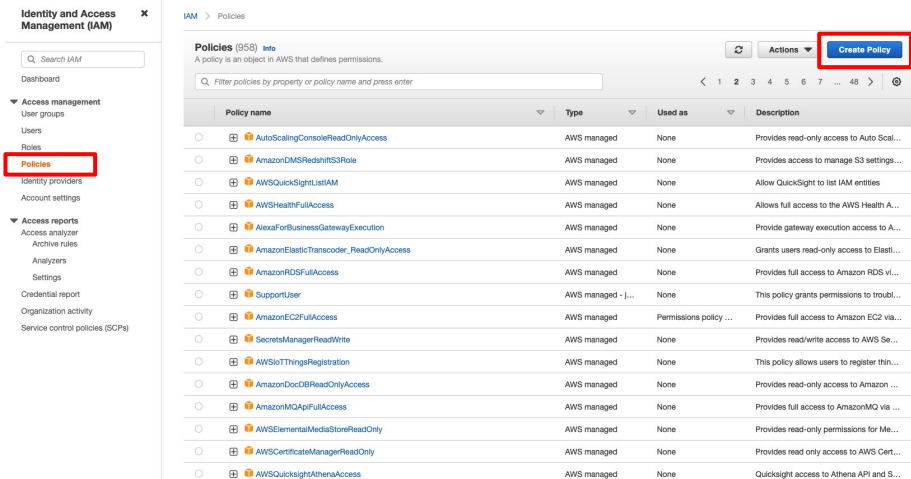
1 章の作業は完了

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. On the left sidebar, under 'Access management', the 'Policies' link is highlighted with a red box. The main content area shows the 'Policies (958)' page. At the top right of this page, the 'Create Policy' button is highlighted with a red box. Below the header, there is a table listing various AWS managed policies. The table has columns for 'Policy name', 'Type', 'Used as', and 'Description'.

Policy name	Type	Used as	Description
AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only access to Auto Scal...
AmazonDMSReadOnlyS3Role	AWS managed	None	Provides access to manage S3 settings...
AWSQuickSightIAM	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 Eli...
AmazonRDSFullAccess	AWS managed	None	Provides full access to Amazon RDS vl...
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 ...
AWS ElementalMediaStoreReadOnly	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...

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

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 (1 action) Clone Remove

Service S3

Actions Read
GetObject

Resources ☒ Specific
☐ All resources

object [Add ARN to restrict access](#) EDIT ☐ Any

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

Request conditions Specify request conditions (optional)

Add additional permissions

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:::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

Cancel Add

Service : S3

Action : GetObject

Resources :

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

※ 1.9 で確認した S3 Bucket 情報

※ 青色の箇所を環境に合わせて編集してください

※ Resources に指定するパスには必ず “/*” を付けること

「Add」

「Next: Tags」→「Review policy」

2.3. WAFLog 出力先 read 権限 policy 作成

Create policy

1 2 3

Review policy

Name*

wafcharm-waflog-s3-read

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 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.

Name :

wafcharm-waflog-s3-read (任意の名前)

Description : WafCharm (任意)

「Create policy」

* Required

Cancel

Previous

Create policy

2.4. WafCharm 連携用 put 権限 policy 作成

Create policy

1 2 3

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 restrict access

Request conditions Specify request conditions (optional)

Add additional permissions

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

Service : S3

Action : PutObject, PutObjectACL

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

※ CSC 側の S3 に対する権限

「Add」

「Next: Tags」→「Review policy」

2.5. WafCharm 連携用 put 権限 policy 作成

Create policy

1 2 3

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 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.

Name :

wafcharm-waflog-s3-put (任意の名前)

Description : WafCharm (任意)

「Create policy」

* Required

Cancel

Previous

Create policy

2.6. WafCharm 連携 Lambda 用 role 作成

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

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

Cancel Next

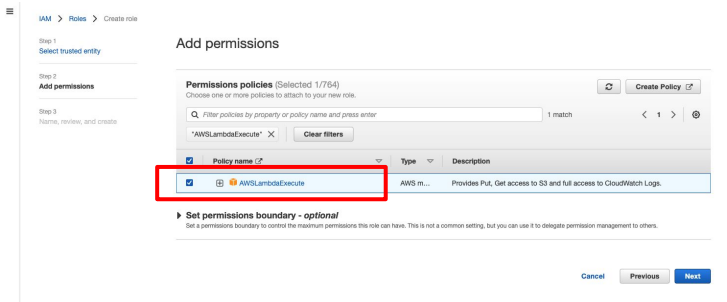
サービス “IAM” より

“Roles” > “Create role” を選択

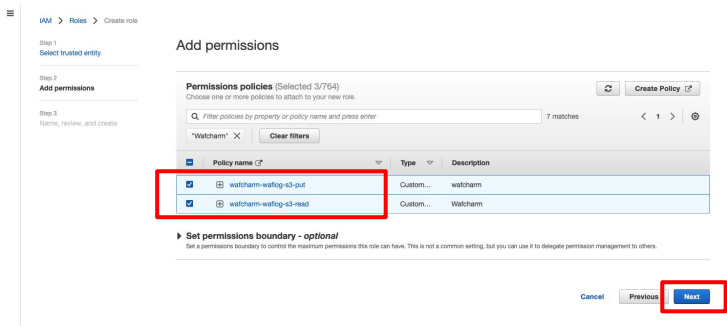
Use case: 「Lambda」を選択

「Next」

2.7. WafCharm 連携 Lambda 用 role 作成



フィルターに「AWSLambdaExecute」を入力し、
「AWSLambdaExecute」を選択



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」

2.8. WafCharm 連携 Lambda 用 role 作成

The screenshot shows the AWS IAM console 'Create role' wizard at Step 3: Name, review, and create. The left sidebar shows the progress: Step 1: Select trusted entity, Step 2: Add permissions, and Step 3: Name, review, and create. The main content area is titled 'Name, review, and create' and contains the following sections:

- Role details**:
 - Role name**: A text input field containing 'wafcharm-waflog'. Below it, a note states: 'Maximum 128 characters. Use alphanumeric and "+, @, _" characters.'
 - Description**: A text input field containing 'WafCharm'. Below it, a note states: 'Maximum 1000 characters. Use alphanumeric and "+, @, _" characters.'
- Step 1: Select trusted entities**: A code editor showing the JSON policy document for the role. The policy allows the role to assume the 'LambdaExecutionRole' on the 'aws:lambda' service.
- Step 2: Add permissions**: A table showing the permissions policy summary. The table has three columns: Policy name, Type, and Attached as.
- Tags**: A section titled 'Add tags (Optional)' with a note: 'Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.' Below this, it says 'No tags associated with the resource.' and there is an 'Add tag' button.

At the bottom of the page, there are three buttons: 'Cancel', 'Previous', and 'Create role'. The 'Create role' button is highlighted with a red rectangle.

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

Role name:
wafcharm-waflog (任意)

Description :
WafCharm (任意)

タグの追加は任意

「Create role」

2.9. Lambda 構築

The screenshot shows the AWS Lambda 'Create function' page. The 'Author from scratch' tab is active. The 'Function name' field contains 'wafcharm-waflog'. The 'Runtime' dropdown is set to 'Node.js 14.x'. The 'Architecture' dropdown is set to 'x86_64'. In the 'Permissions' section, the 'Change default execution role' dropdown is set to 'Use an existing role', and the 'Existing role' dropdown shows 'wafcharm-waflog'. The 'Create Function' button is highlighted with a red box at the bottom right.

名前 : wafcharm-waflog (任意)

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

Execution Role : Use an existing role

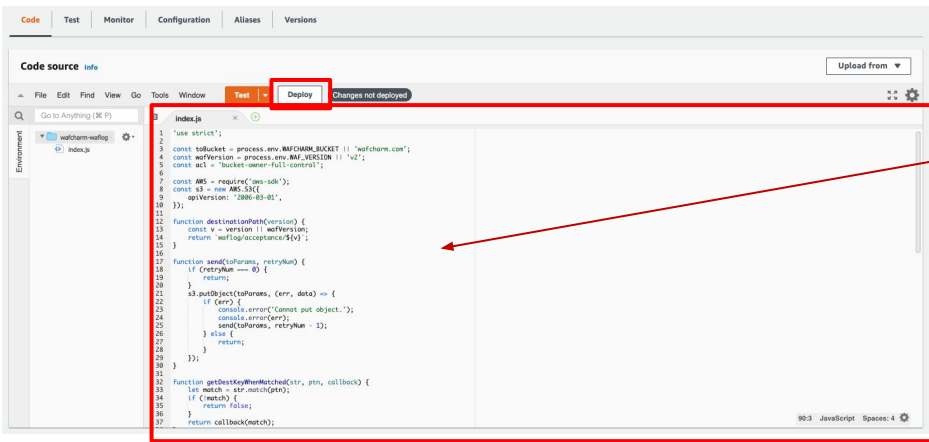
既存のロール : wafcharm-waflog

※ [2.8](#) で作成したもの

※ [1.6](#) 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」

2.10. 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.js

※ 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」

2.11. Lambda 構築 (トリガー)

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

Lambda > Add 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.

Cancel Add

Add trigger :

トリガーに S3 を選択

バケット: [1.6](#) 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)

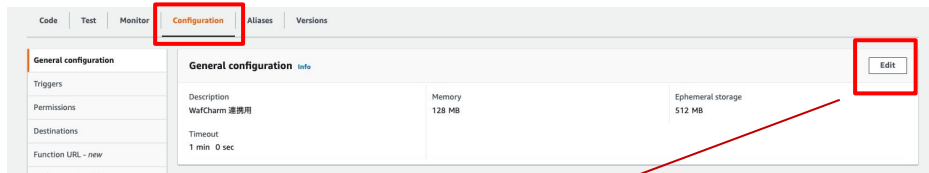
プレフィックス : [1.9](#) で確認した経路

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

※ 青色の箇所を環境に合わせて編集してください

「Add」

2.12. Lambda 構築



「Configuration」

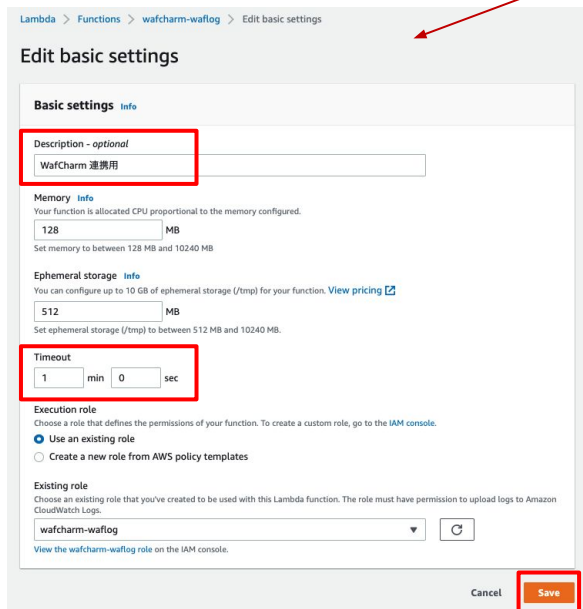
「General configuration」

「Edit」

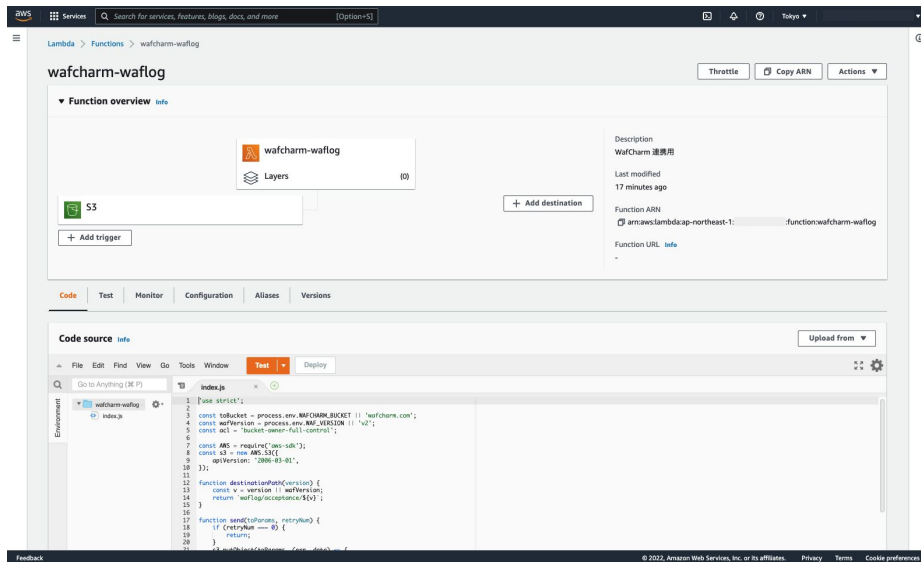
Description : WafCharm 連携用 (任意)

Timeout : 1 分

「Save」



2.13. Lambda 構築



完了

2.14. 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

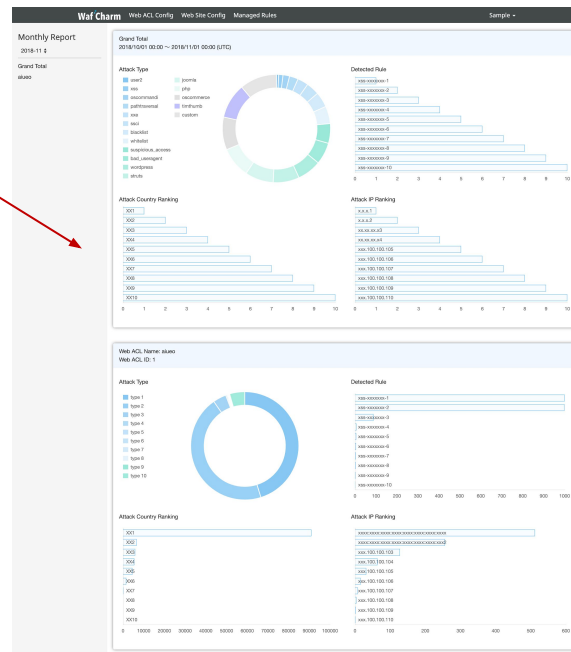
1. 1 ～ 2 章までの設定が完了している
2. 前月に検知があった

※ 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

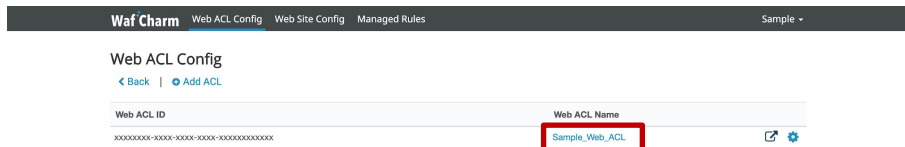
4.1. メール通知先の設定



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

Save

「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	☐
Managed Rule Email Notificaiton	☐

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、Web ACLからS3への直接出力間隔である 5 分となります
- 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、ログファイルのプレフィックス (<account-id>_waflogs_<Region>_<web-acl-name>) と対象の Web ACL ID を共有ください
 - 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
- 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