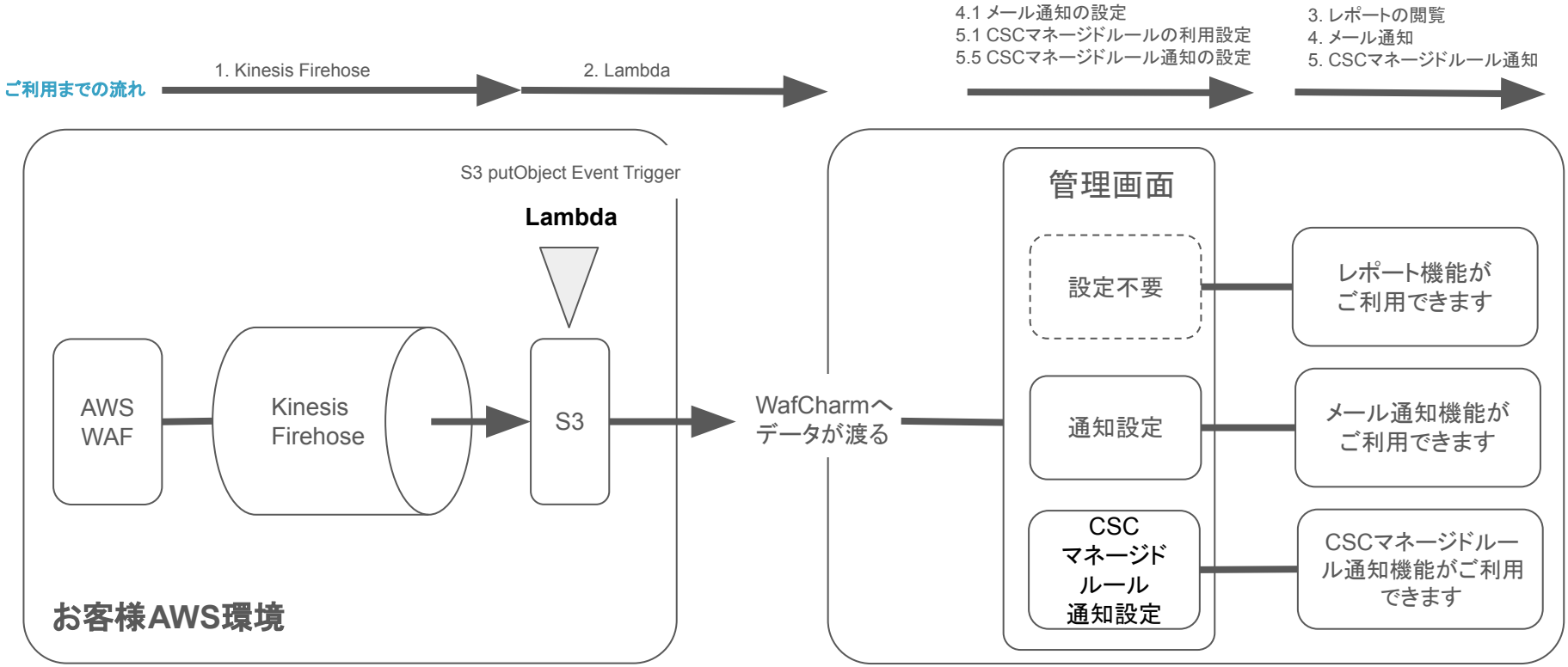
レポート機能/通知機能 利用マニュアル
Ver 1.5

Waf Charm

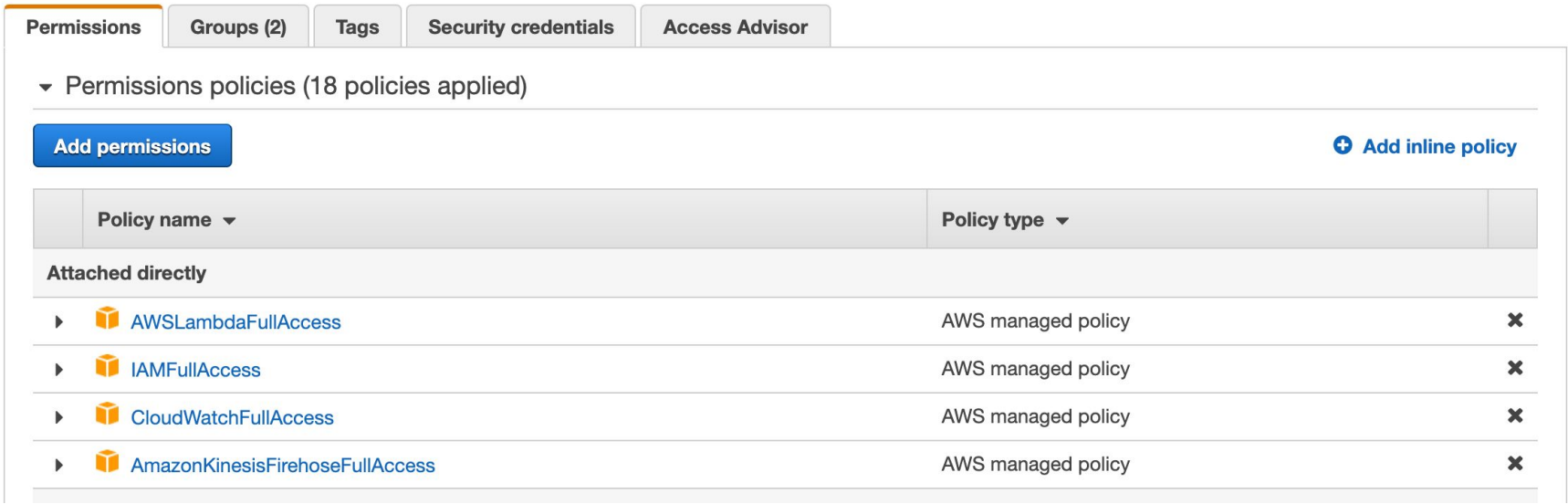
レポート機能/通知機能のアーキテクチャ概要



Waf Charm

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



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 full 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

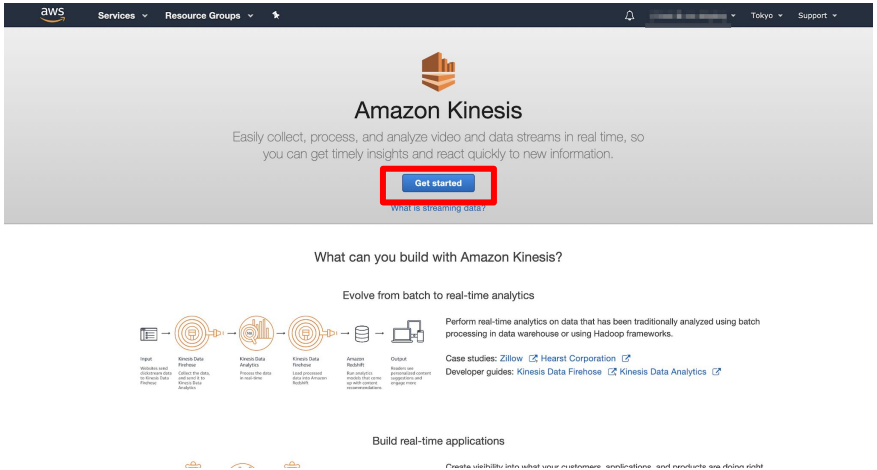
4. メール通知機能をご利用される場合
    - WafCharm管理画面にて、メール通知の設定
    - メール通知内容
5. CSCマネージドルール通知機能をご利用される場合
    - WafCharm管理画面にて、CSCマネージドルールの利用設定
    - CSCマネージドルール通知の設定
    - メール通知内容
6. 通知機能に関する補足事項
7. その他補足事項

1. Kinesis Firehose

WAFログをS3に転送するKinesis Firehoseを設定

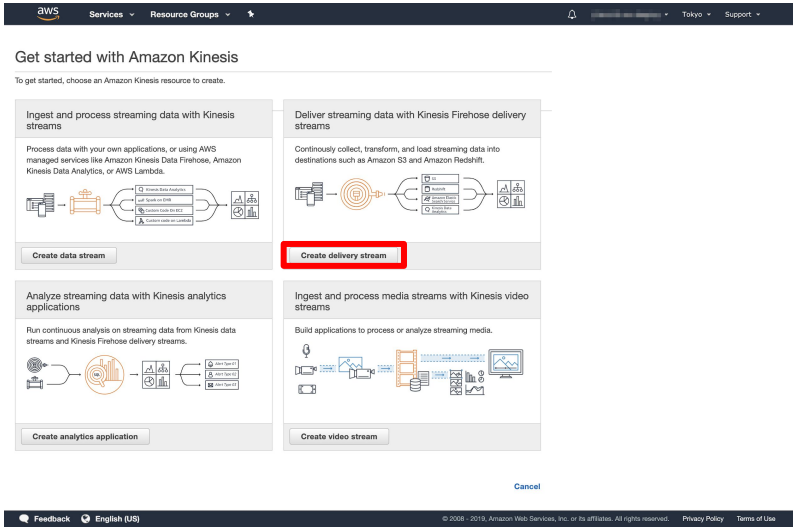
- Kinesis Firehose の構築/設定
- Kinesis Firehose 実行用の Role 設定
- Kinesis FirehoseとAWS WAFとの連携設定
- 1章の完了確認

1.1. Kinesis Firehose設定



「Get started」をクリックしします

1.2. Kinesis Firehose設定

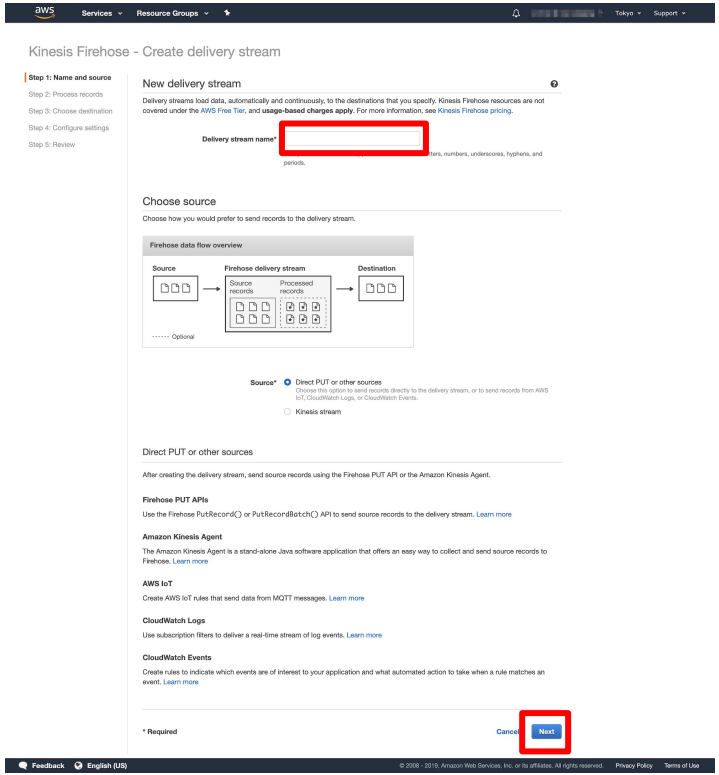


「Create delivery stream」

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

1.3. Kinesis Firehose設定

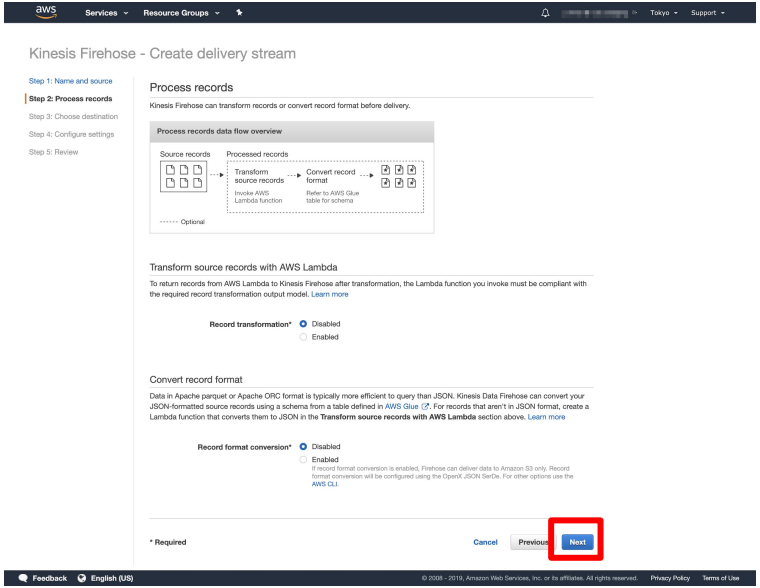


Delivery Stream Name :
aws-waf-logs-<任意の文字列>

「Next」

※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

1.4. Kinesis Firehose設定

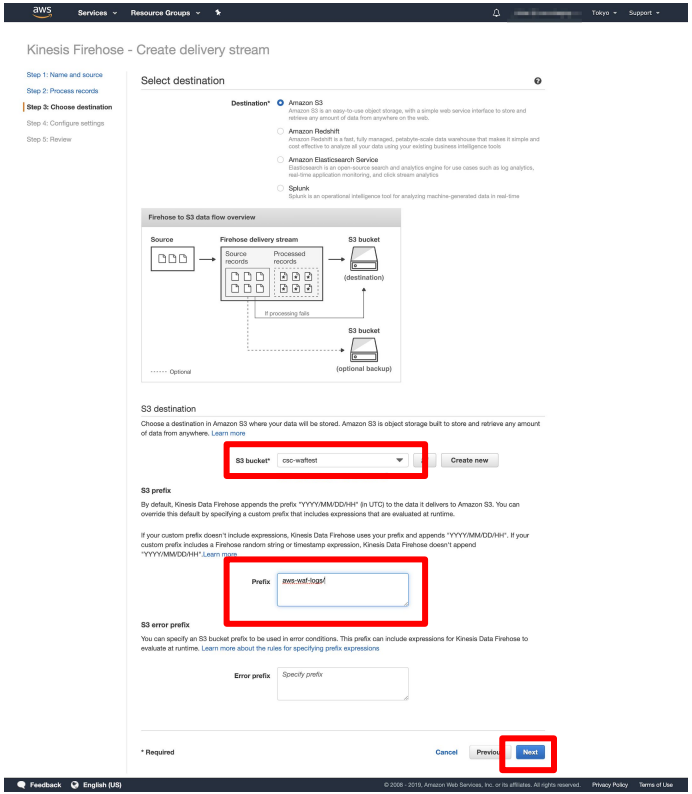


「Next」

下記は使用しません

- Transform source records with AWS Lambda
- Convert record format

1.5. Kinesis Firehose設定



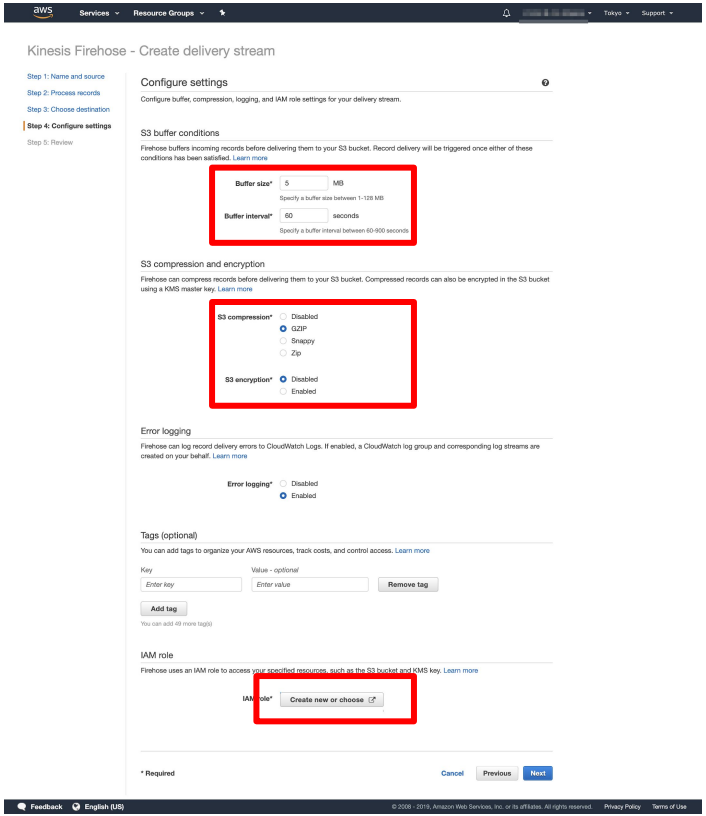
S3 bucket :
任意のS3bucketを指定(ex: csc-waftest)

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

「Next」

1.6. Kinesis Firehose設定



Buffer intervals :
推奨は 60 seconds

※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

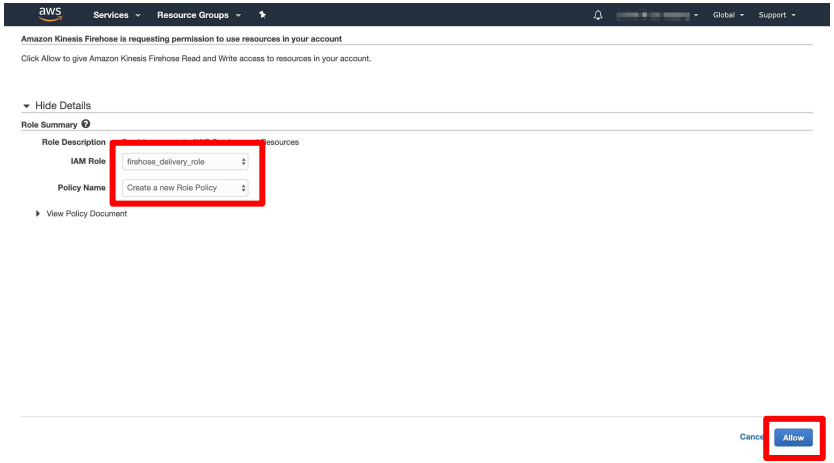
Buffer size :
推奨は 5 MB

S3 compression :
GZIP

S3 encryption :
Disable

「Create new or choose」

1.7. IAM role設定



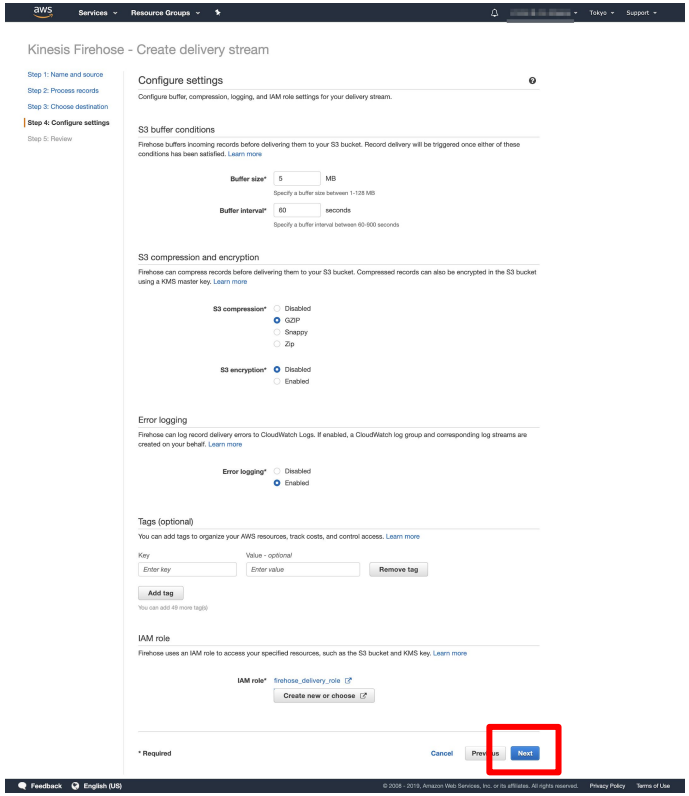
Role Description:
任意

IAM Role :
新しいIAM ロールの作成 or 選択

Policy Name :
新しいロールポリシーの作成 or 選択

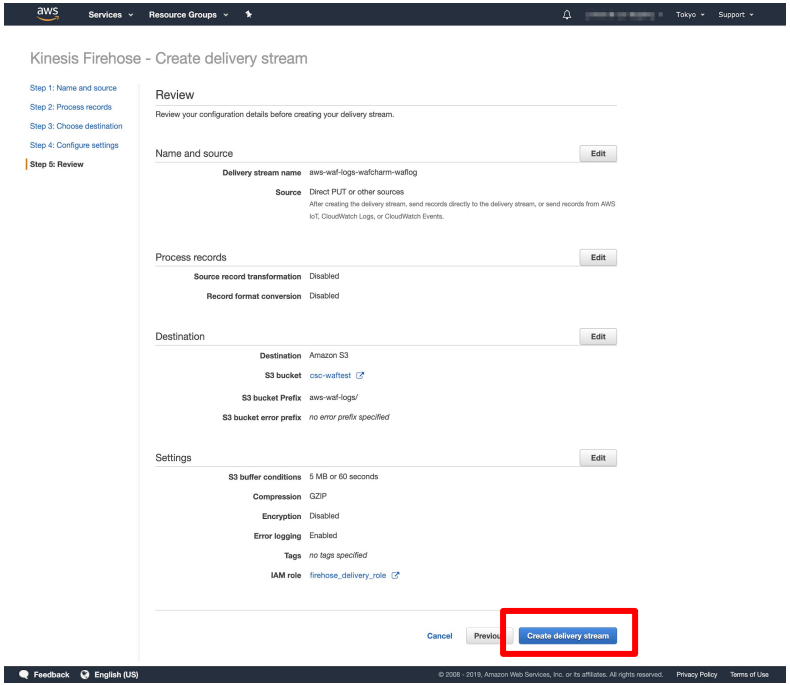
「Allow」

1.8. Kinesis Firehose設定



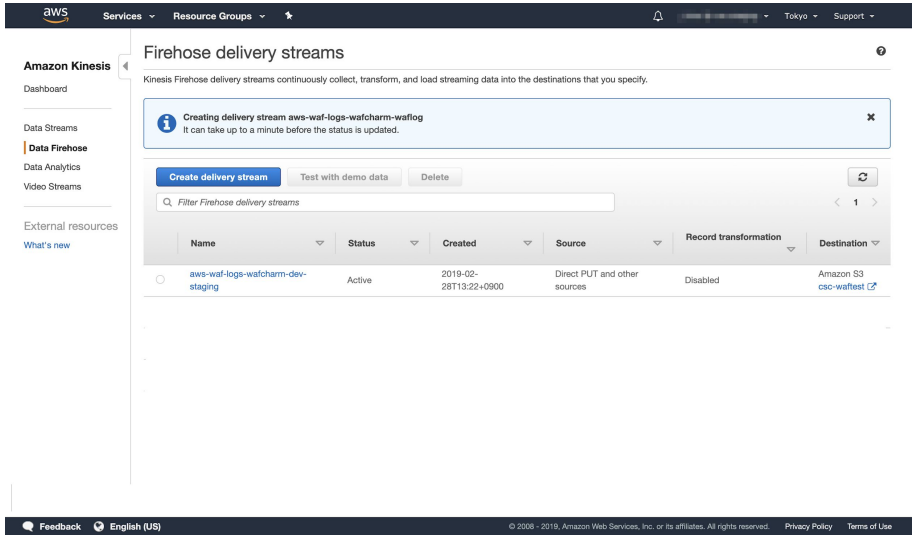
「Next」

1.9. Kinesis Firehose設定



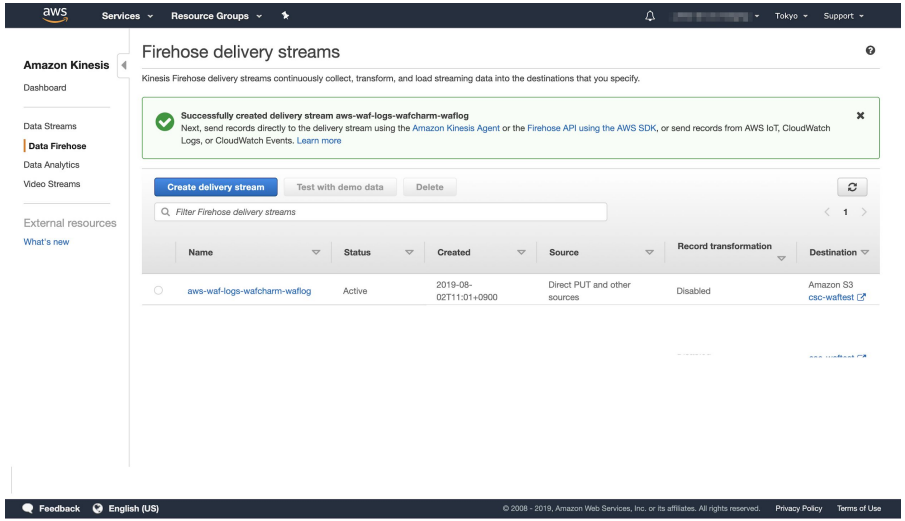
「Create delivery stream」

1.10. Kinesis Firehose設定



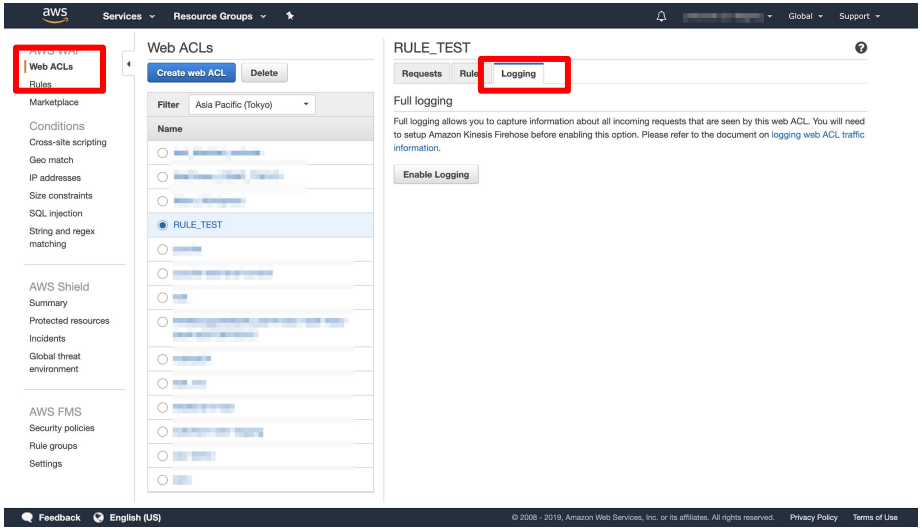
待機

1.11. Kinesis Firehose設定



完了

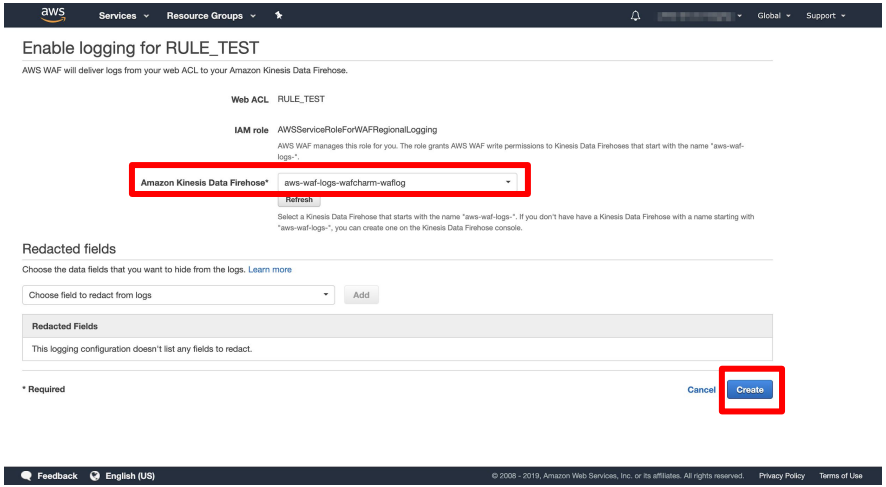
1.12. Kinesis FirehoseとAWS WAFとの連携設定



サービス “AWS WAF”に戻り

“Web ACLs” > “Logging” を選択

1.13. Kinesis FirehoseとAWS WAFとの連携設定



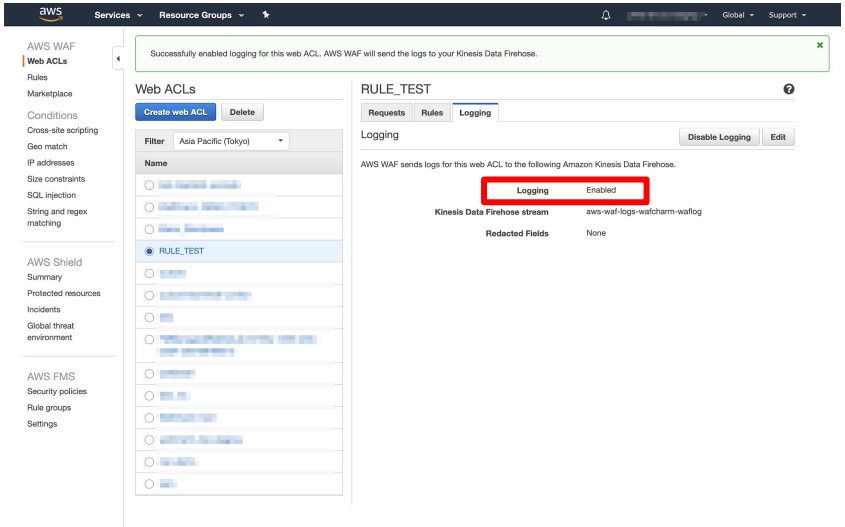
Amazon Kinesis Data Firehoseには

自身で命名したDelivery Stream Nameを選択

※ 1.3.で指定したもの

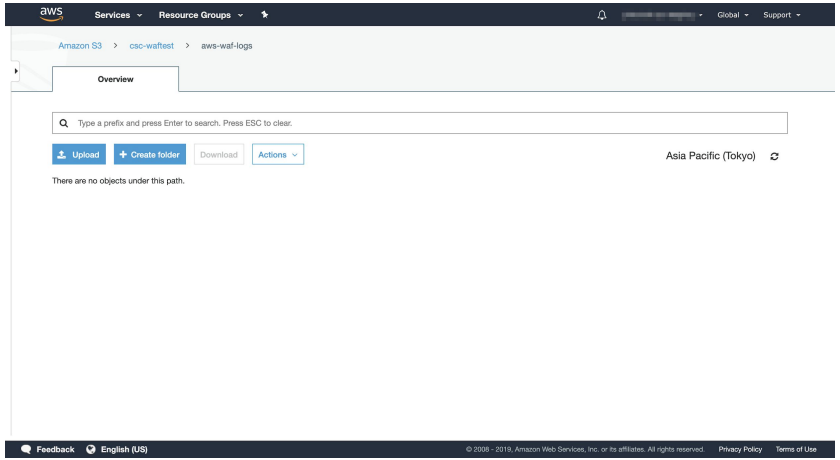
「Create」

1.14. 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

1.15. 1章の完了確認

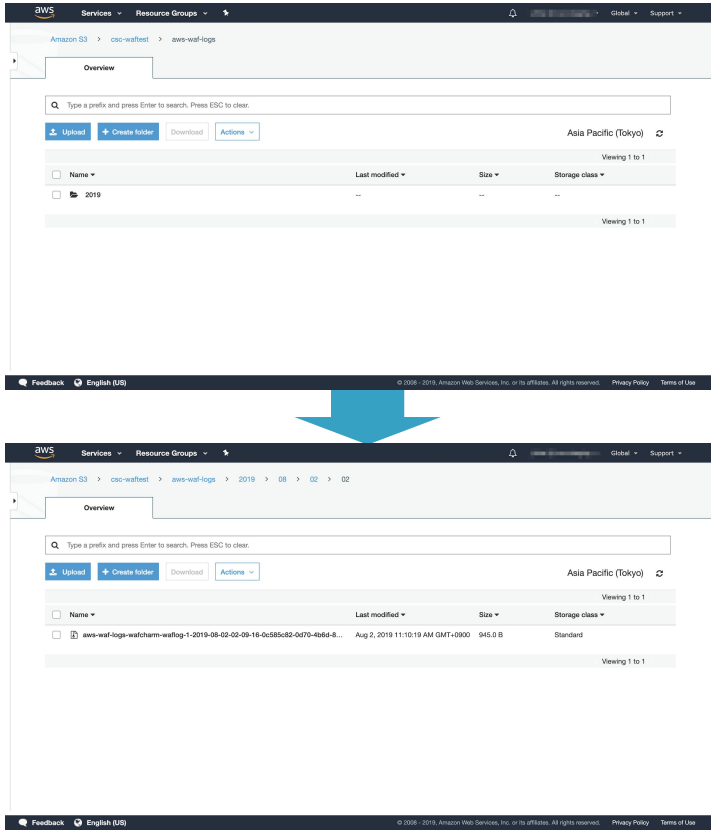


S3にフルログファイルが生成されているか確認

※ 1.5.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

1.16. 1章の完了確認



左記のようなファイルが生成されれば

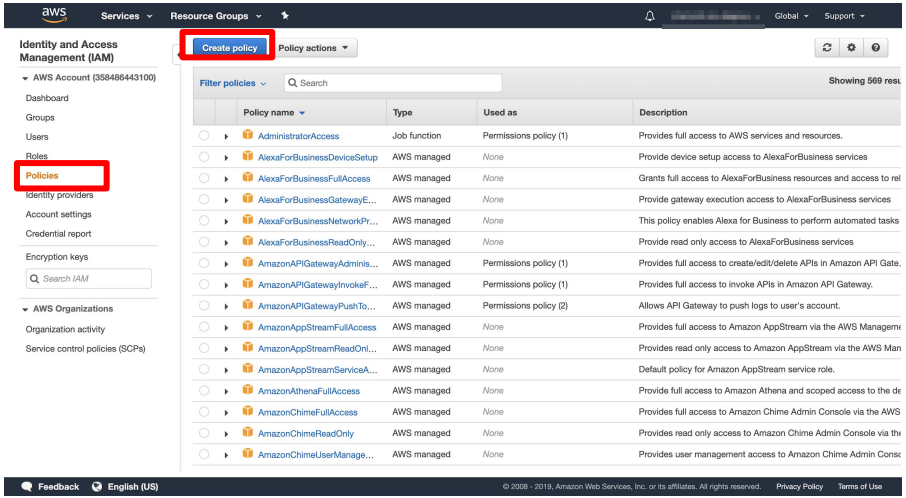
1章の作業は完了

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full権限policy作成
- WacCharm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

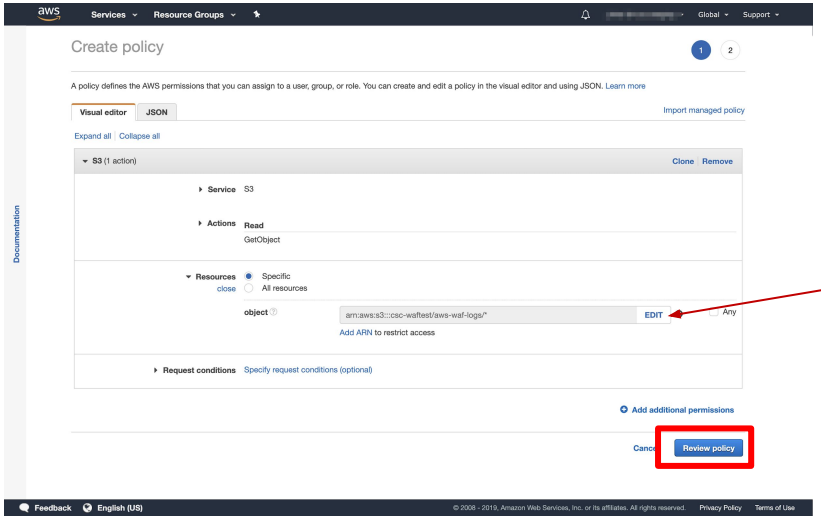
2.1. WAFLog出力先read権限policy作成



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

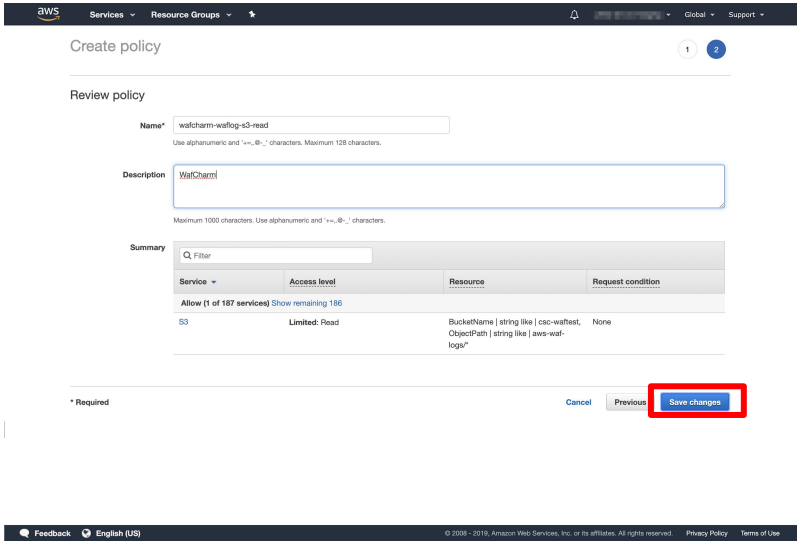
Action : GetObject

Resources :
arn:aws:s3:::csc-waftest/waflog/*
※ 1.5.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

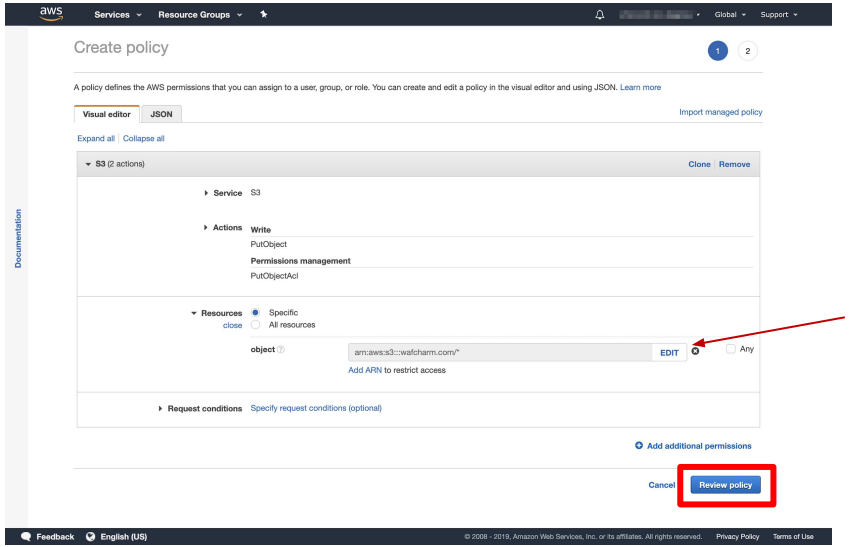


Name:
wafcharm-waflog-s3-read (任意の名前)

Description : WafCharm (任意)

「Create policy」

2.4. WafCharm連携用full権限policy作成



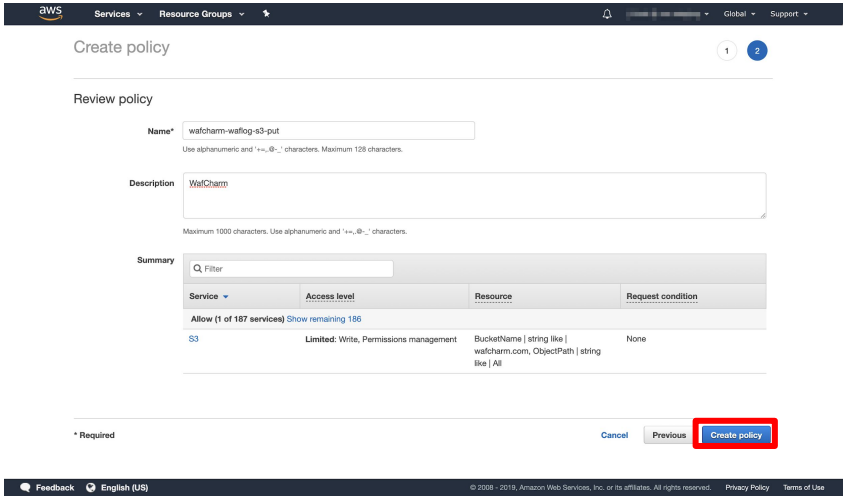
Service : S3

Action : PutObject, PutObjectACL

Resources :
arn:aws:s3:::wafcharm.com/*
※CSC側のS3に対する権限

「Review policy」

2.5. WafCharm連携用full権限policy作成

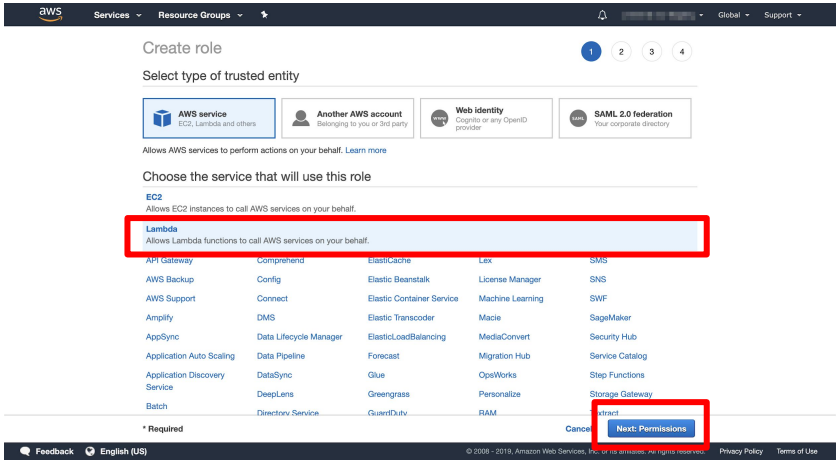


Name :
wafcharm-waflog-s3-put (任意の名前)

Description : WafCharm (任意)

「Create policy」

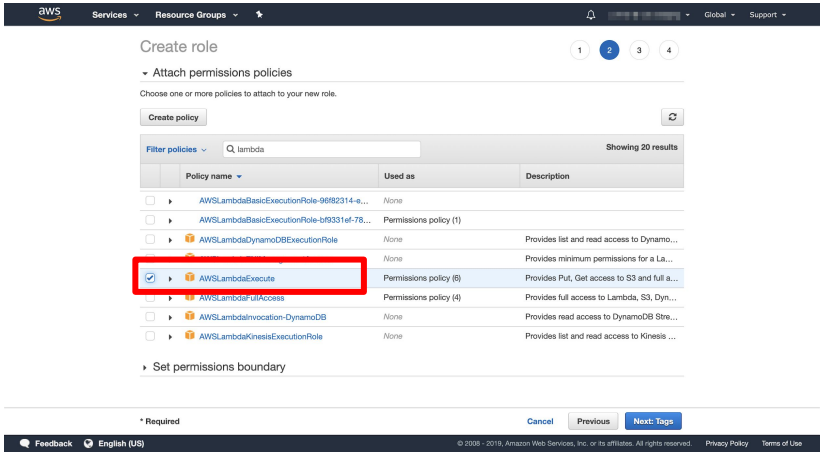
2.6. WafCharm連携Lambda用role作成



このロールを使用するサービスを選択 :Lambda

「Next: Permissions」

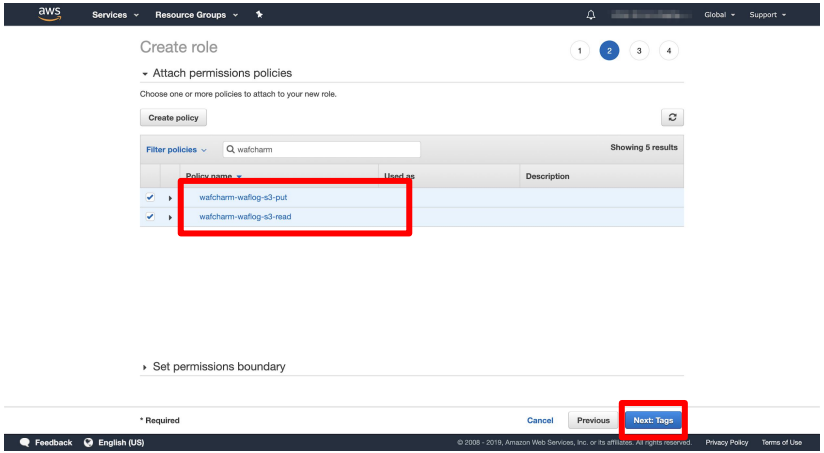
2.7. WafCharm連携Lambda用role作成



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

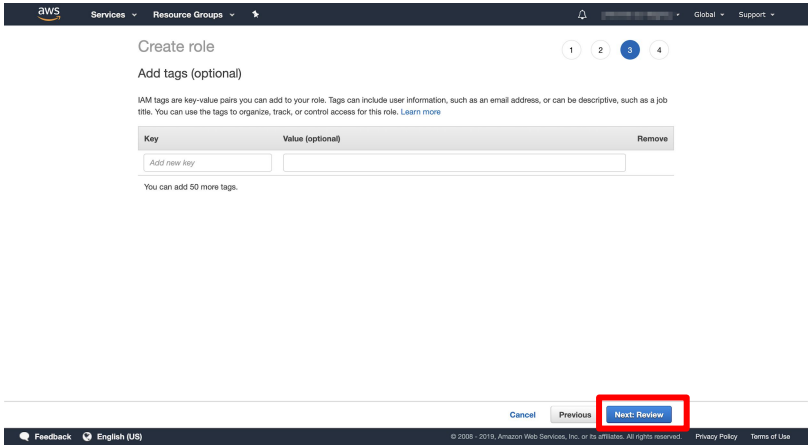
「wafcharm-waflog-s3-put」
「wafcharm-waflog-s3-read」

を選択

※2.2., 2.4.で作成したpolicy

「次のステップ：タグ」

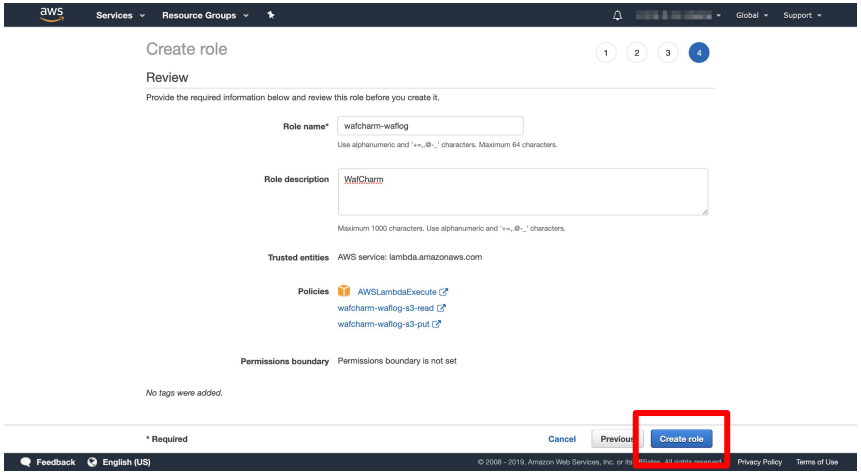
2.9. WafCharm連携Lambda用role作成



タグの追加は任意

「Next: Review」

2.10. WafCharm連携Lambda用role作成

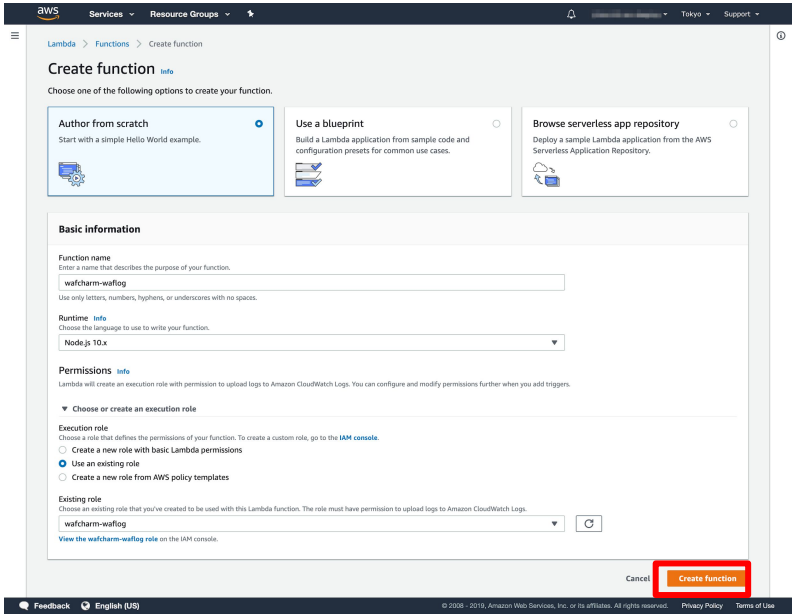


Role name:
wafcharm-waflog (任意)

Role description :
WafCharm (任意)

「Create role」

2.11. Lambda構築



名前：wafcharm-waflog (任意)

Runtime : Node.js 10.x 以上

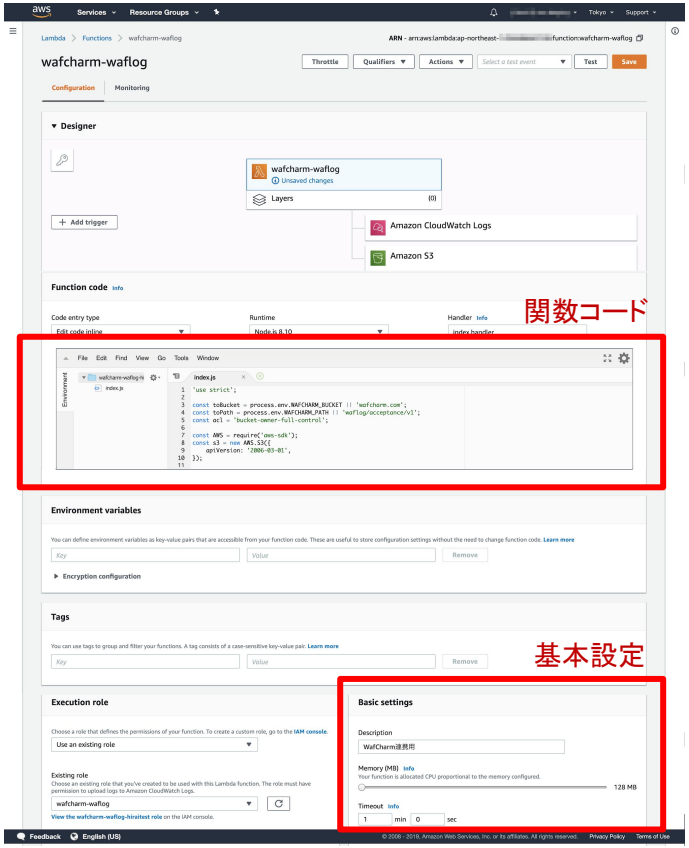
Role : Use an existing role

既存のロール：wafcharm-waflog
※ 2.8.で作成したもの

※1.5.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)



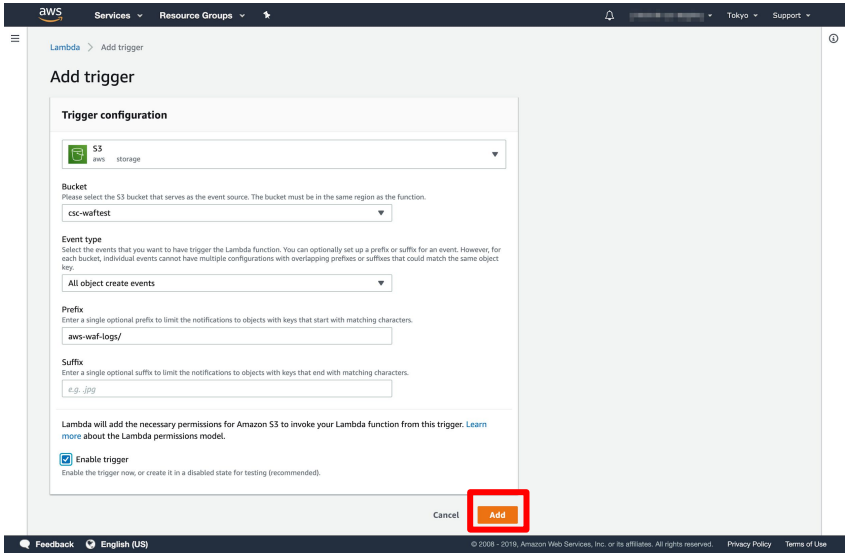
Function code :
以下のソースを貼り付け
http://docs.wafcharm.com/manual/index.js

Basic settings

Description : WafCharm連携用 (任意)

Timeout : 1分

2.13. Lambda構築 (トリガー)



Designer :
トリガーにS3を選択

トリガーの設定

バケット: 1.5. で設定したS3 bucket

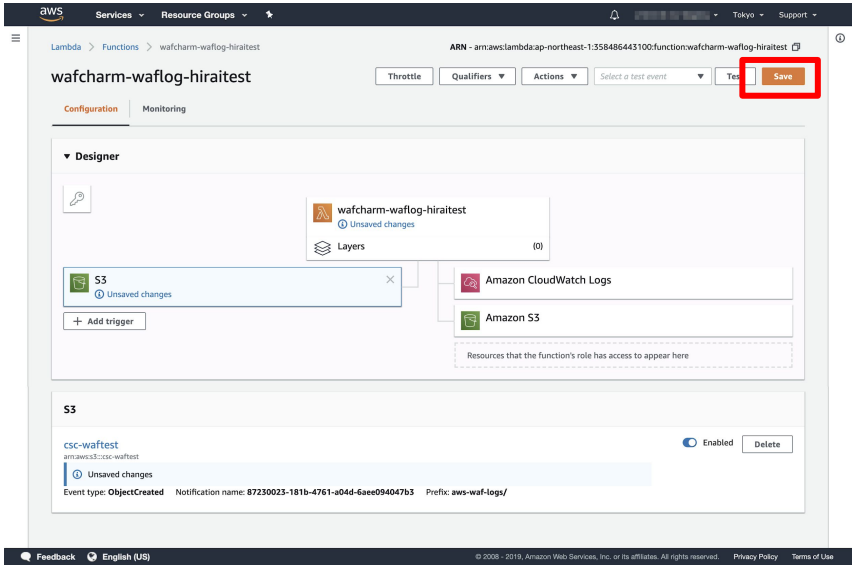
イベントタイプ：オブジェクトの作成 (すべて)

プレフィックス：1.5.で設定したprefix

トリガーの有効化：check

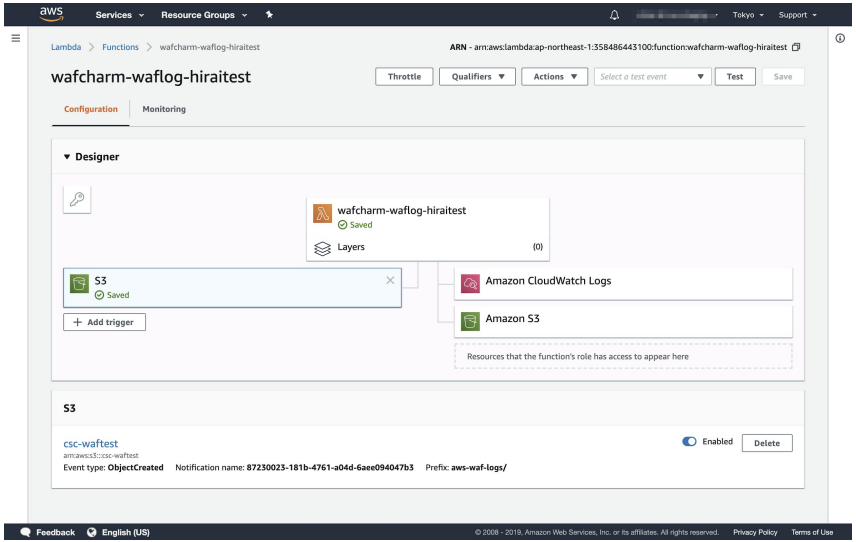
「追加」

2.14. Lambda構築



「保存」

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

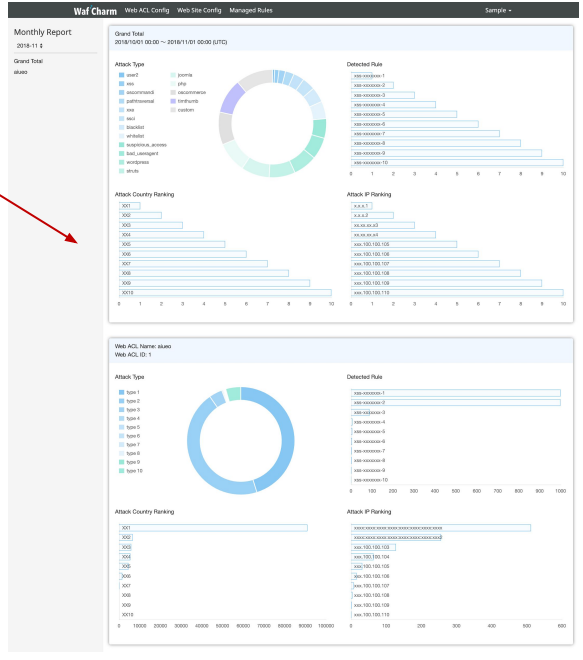
※前月に検知がなかった方 -> 月次レポートが作成されません

3.1. WafCharm管理画面にて月次レポートの閲覧

※レポートは、毎月初旬に前月分が閲覧可能

WafCharm管理画面

右上のメニューより、「Report」を選択



※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

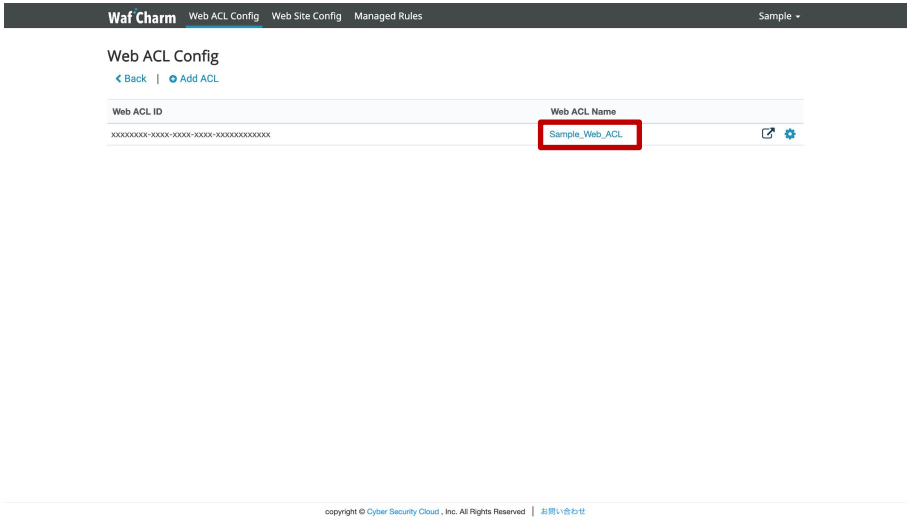
- WafCharm管理画面にて、メール通知の設定
- メール通知内容

4.1. メール通知の設定

WafCharm管理画面

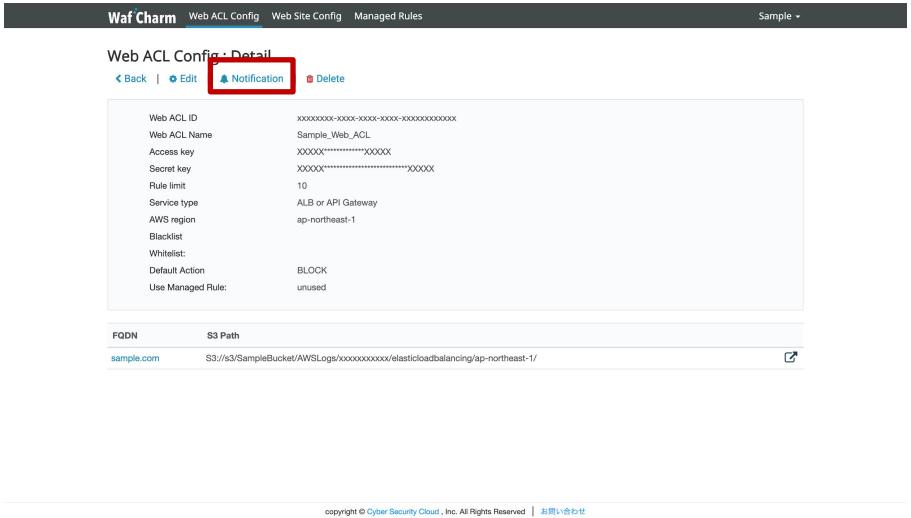
上部メニューより、「WebACL Config」を選択

4.2. メール通知の設定



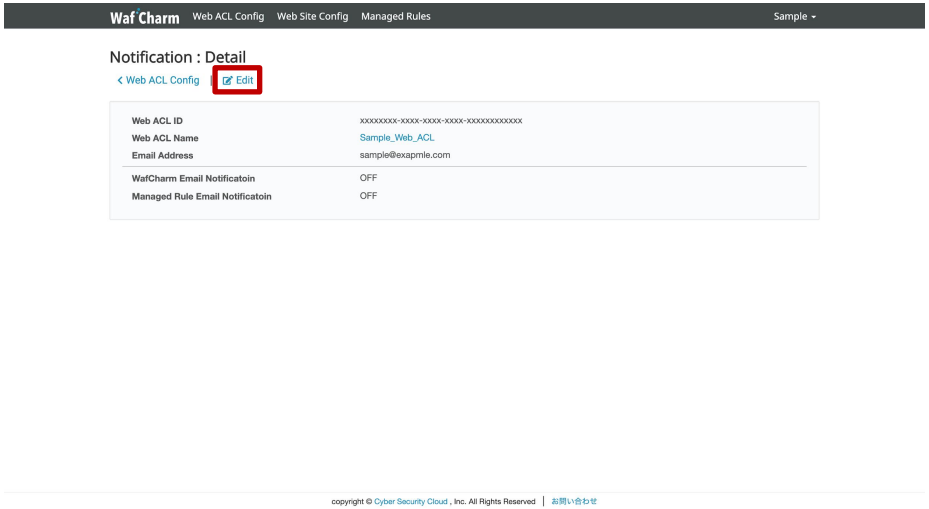
対象の「Web ACL Name」を選択

4.3. メール通知の設定



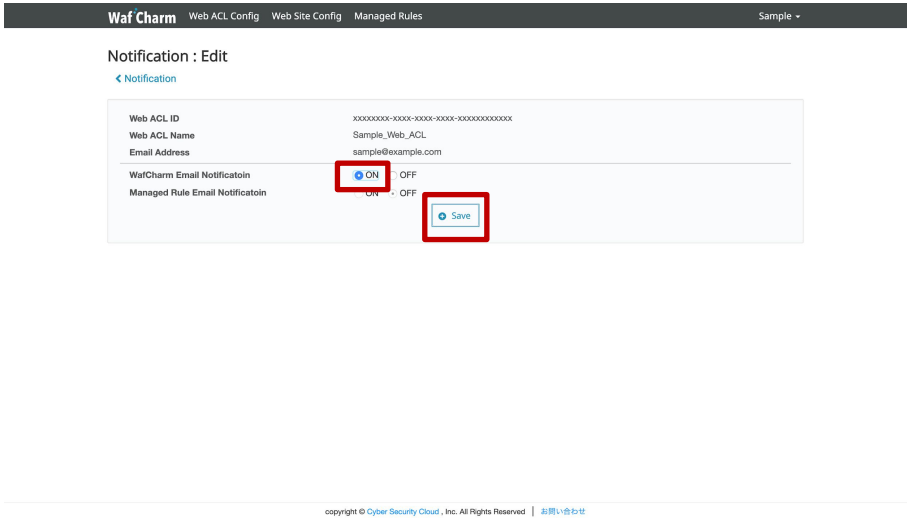
「Notification」を選択

4.4. メール通知の設定



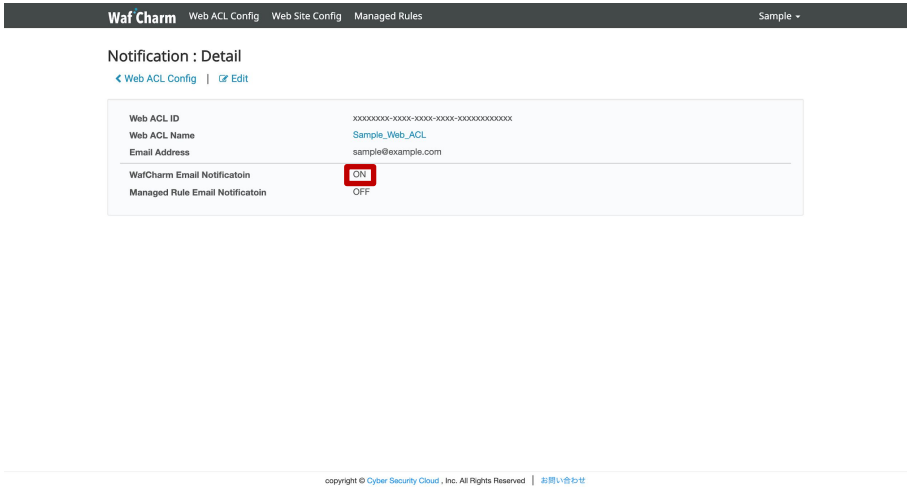
「Edit」を選択

4.5. メール通知の設定



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

4.6. メール通知の設定



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

4.7. メール通知内容

検知されると、下記メールが WafCharm管理画面アカウントのメールアドレス宛てに通知されます

- 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管理画面アカウントのメールアドレス

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(WebACL ID): <お客様のWeb ACL Name> (<お客様のWeb ACL ID>)
Matches Rule: wafcharm-blacklist-010090004-07 (<Rule ID>)
Time(UTC): Thu, 01 Aug 2019 09:21:03 GMT
Source IP: 192.0.2.0
Source Country: JP
URI: /

5. CSCマネージドルール通知機能をご利用される場合

1章(Kinesis Firehose)、2章(Lambda) の設定が完了し、CSCのマネージドルール(Cyber Security Cloud Managed Rules for AWS WAF HighSecurity OWASP Set)をご利用頂いている場合、WafCharm管理画面にて、設定及び、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

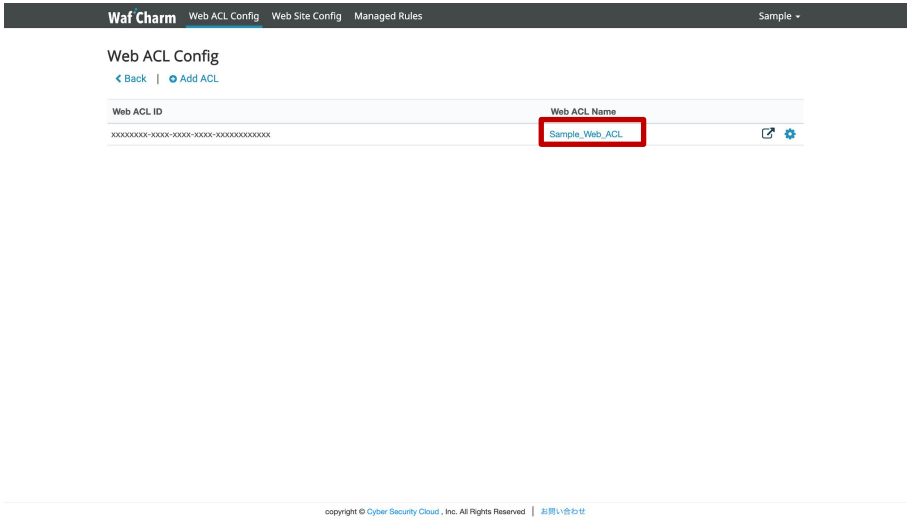
- WafCharm管理画面上でのCSCマネージドルールの設定
    - AWS WAF Managed Rules ルールグループの例外機能マニュアル（p4)
- CSCマネージドルール通知の設定
- 通知内容

5.1. CSCマネージドルールの利用設定

WafCharm管理画面

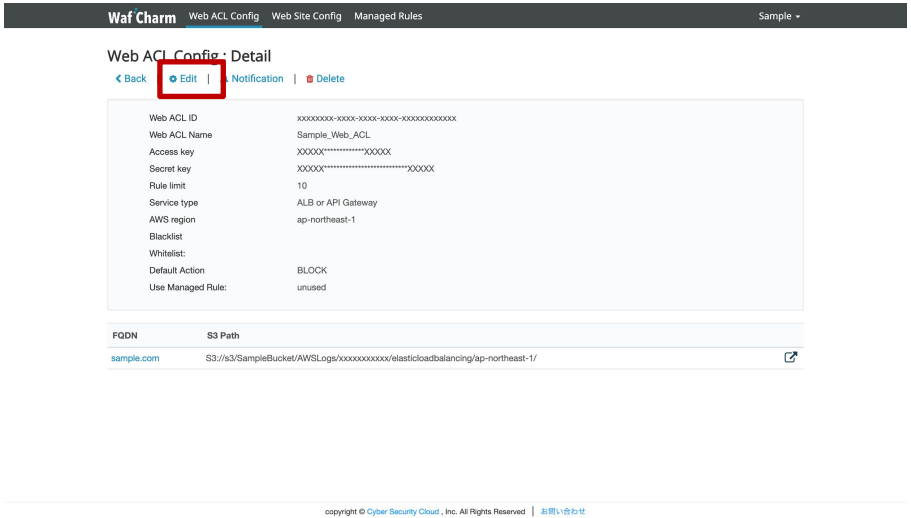
上部メニューより、「Web ACL Config」を選択

5.2. CSCマネージドルールの利用設定



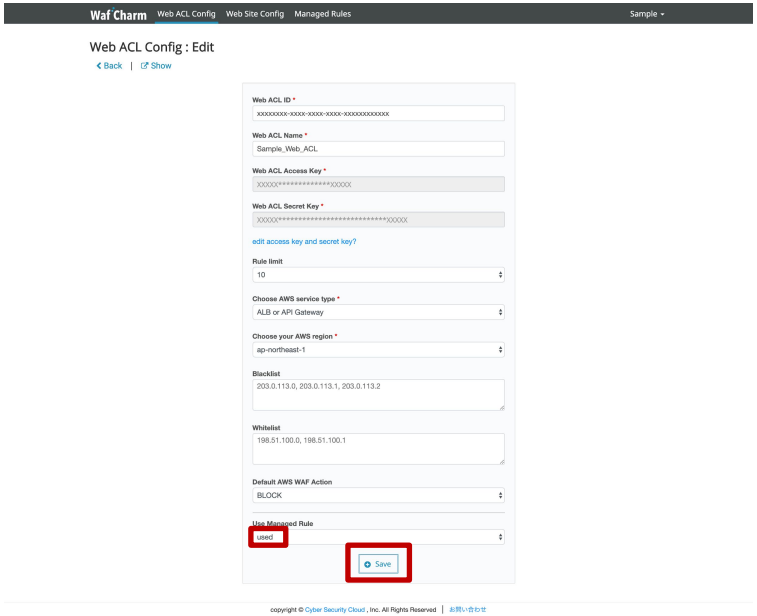
対象の「Web ACL Name」を選択

5.3. CSCマネージドルールの利用設定



「Edit」を選択

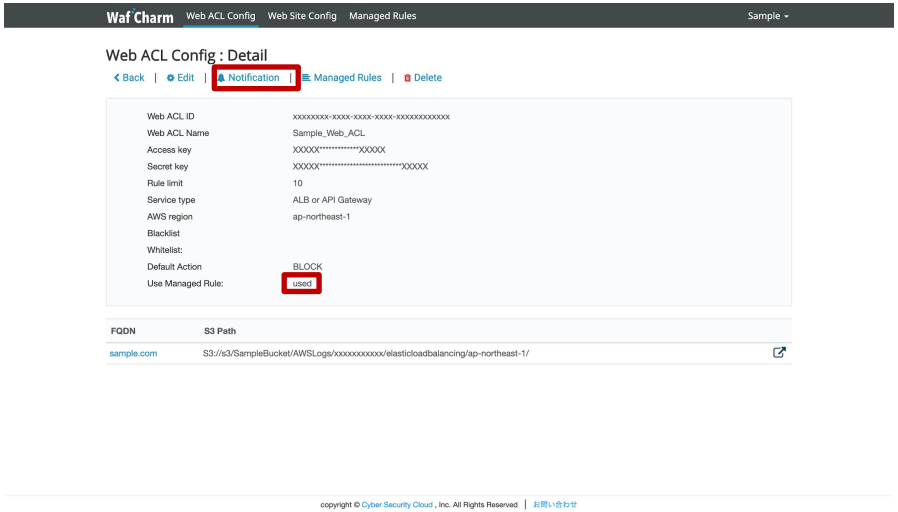
5.4. CSCマネージドルールの利用設定



「Use Managed Rule」を「used」へ変更し、

「Save」をクリック

5.5. CSCマネージドルール通知機能の設定



「Use Managed Rule」が「used」になっている
ことを確認

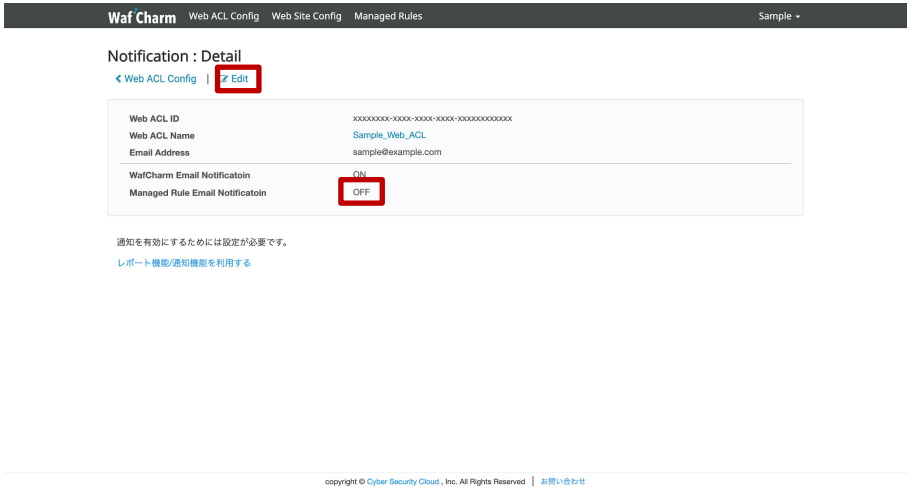
※お客様のCSCマネージドルールの利用確認に
5 ~ 10分程度かかります

設定反映確認には以下ページ参照

AWS WAF Managed Rules ルールグループの例外機能マニュアル (p11 ~ 13)

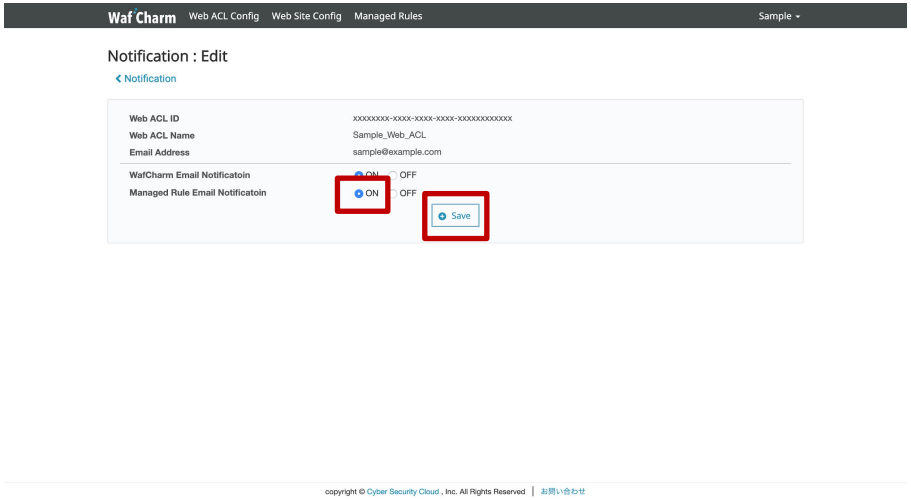
設定反映確認後、メニュー上部の「 Notification」を選択

5.6. CSCマネージドルール通知機能の設定



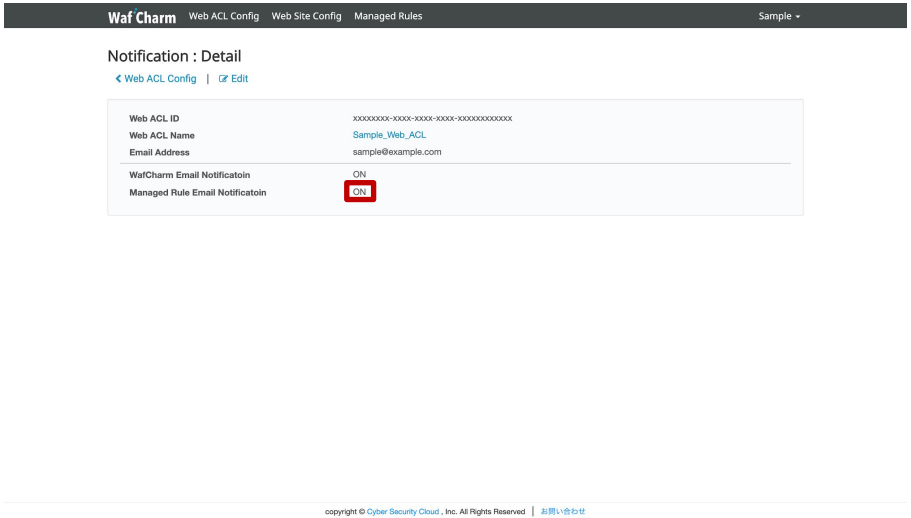
「Edit」を選択

5.7. CSCマネージドルール通知機能の設定



「Managed Rule Email Notificaition」を「ON」に変更し、「save」

5.8. CSCマネージドルール通知機能の設定



「Managed Rule Email Notificaition」が「ON」になっていることを確認

5.9. CSCマネージドルール通知内容

検知されると、下記メールが WafCharm管理画面アカウントのメールアドレス宛てに通知されます

- メールタイトル： CSC Managed Rules Attack Detected.
- メール差出人：WafCharm Notification wafcharm-notification@cscloud.co.jp
- メール宛先：WafCharm管理画面アカウントのメールアドレス

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(WebACL ID): <お客様のWeb ACL Name> (<お客様のWeb ACL ID>)
Managed Rule: Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-
Attack Type: suspicious_access
Field Type: url
Matches Rule Name: sample_suspicious_access-url-001
Matches Rule ID:<Rule ID>
Time(UTC): Tue, 19 Feb 2019 02:09:35 GMT
Source IP: 192.0.2.0
Source Country: JP
URI: /

6. 通知機能に関する補足事項

- 以下条件が揃った場合、WafCharm の通知機能は対象の Web ACL Config における通知機能　の ON / OFF に関わらず検知内容を通知します
  - 本マニュアルにて作成した 1 つの Kinesis Firehose を複数の Web ACL に連携している
  - 上記連携をしている Web ACL を 2 つ以上 WafCharm に登録している
  - 上記 Web ACL の内 1 つでも WafCharm の通知機能を ON にしている

- 以下条件が揃った場合、WafCharm の通知機能は「CSC管理外のルールグループによる検知」として通知します
  - CSCマネージドルール (Cyber Security Cloud Managed Rules for AWS WAF HighSecurity OWASP Set) を利用している
  - メール通知機能:ON
  - CSCマネージドルール通知機能 : OFF
  - CSCマネージドルールで検知

6. 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、1.6 Kinesis Firehose 設定 の Buffer intervals、Buffer size で設定した値に応じて変化します

- アカウントに登録されているメールアドレス以外に通知することはできません
  - 現在、機能拡張検討中

7. 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