SRA の技術情報誌
GS LetterNeo
Vol.183　2023 年 10 月

AWS VPC Flowlogs の サーバレス確認ツール

坂本 伊武暉

アドバンストクラウドエンジニアリング事業部

はじめに

AWS でマルチアカウントを使用している事例はとても多いと思います。中でも管理アカウントに各種ログを集約する使い方は多いのではないでしょうか。

その中でも課題となるのが、ログの可視化です。S3 バケットに出力しているログを手作業で確認すると、例えば，ファイルを一つずつダウンロードしては必要な検索を実行しなければならないなど、かなり手間が掛かります。

本記事ではサーバレスで可視化ツールを作成することで、サーバの運用コストを抑えつつ、ログを手軽に確認するツールのアーキテクチャを紹介します。

用語説明

本稿で使用する用語の説明を記載します。
詳細は AWS 公式ドキュメントを確認してください。

VPC:AWS で使用できる仮想ネットワークを構築できるサービス

AWS VPC Flowlog: VPC 間の通信のログを記録できるサービス

Lambda: ソースコードを記載することで、そのまま AWS 上でプログラムを動かすことのできるサービス

S3: ストレージサービス

API Gateway: 簡単に API の作成ができるサービス

Athena: サーバレスなデータ分析サービス

Cognito: サインイン機能をウェブなどに追加できるサービス

IAM Identity Center: 認証基盤を使用して認証を行うサービス

要件

今回作成を行った確認ツールは様々な制約の中で作成しています。そのため、条件によっては別なアーキテクチャが最適解の可能性がありますので、ご承知おきください。

要件：

- ✓ 社内向けに提供(社内とは DirectConnect の専用線で接続されている環境)
- ✓ サーバの新たな運用コストは発生したくない
- ✓ グローバル IP アドレスでサービス展開は NG
- ✓ 認証は SSO を使用(AD Connector でオンプレミス AD と接続)
- ✓ 特別なツールを必要とせず、簡単に確認できること

一番課題となるのがグローバル IP アドレスを持たせないサービス展開です。AWS では簡単に Web ページを公開できるように CloudFront、Amplify などが存在し、AWS WAF を使用すればアクセス制御を行うことは可能ですが、サービスエンドポイントがグローバル IP アドレスを持ってしまいます。

要件では、サービスエンドポイントがプライベート IP アドレスである必要がありました。そのため、VPC エンドポイントを使用したデプロイが必要ですが、それができるものが API Gateway の REST API でプライベート型です。

アーキテクチャ

今まで運用していた図が以下です。

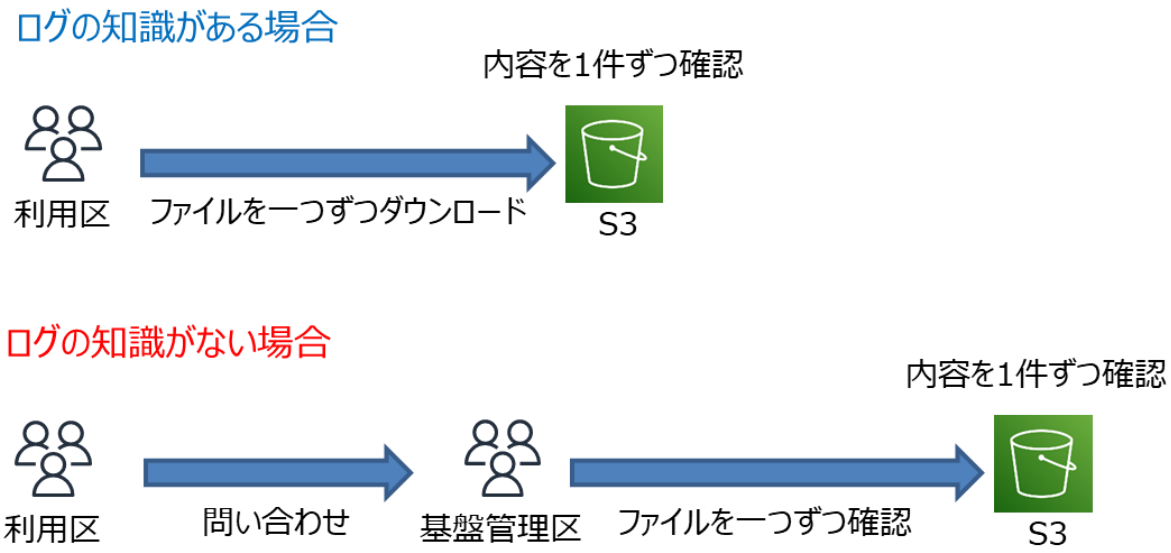

図 1.今までの運用

公式ドキュメントに書かれているログについての知識やネットワークの知識がないと、エンドユーザはログの内容を読み解くことができません。また，それらの知識があったとしても、ログファイルの内容は綺麗に読みやすい形式でまとまっている訳ではないため、ネットワークの知識がある人でも確認が一苦労という課題がありました。

ログの知識がない場合には、問い合わせ窓口に確認依頼の連絡が来ていました。直ぐ確認できるものではなく、問い合わせのあった対象アカウント、送信元 IP アドレス、送信先 IP アドレス、ポート番号、送信日時など多くの情報をヒアリングした後でないと確認できません。

1 件の問い合わせ回答時間はおおよそ 1 時間程掛かっており、ヒアリング状況によっては回答までに数日要したものもあります。

そのため、今回ログを簡単に分かりやすく確認できるツールを構成します。そのアーキテクチャの図が以下です。

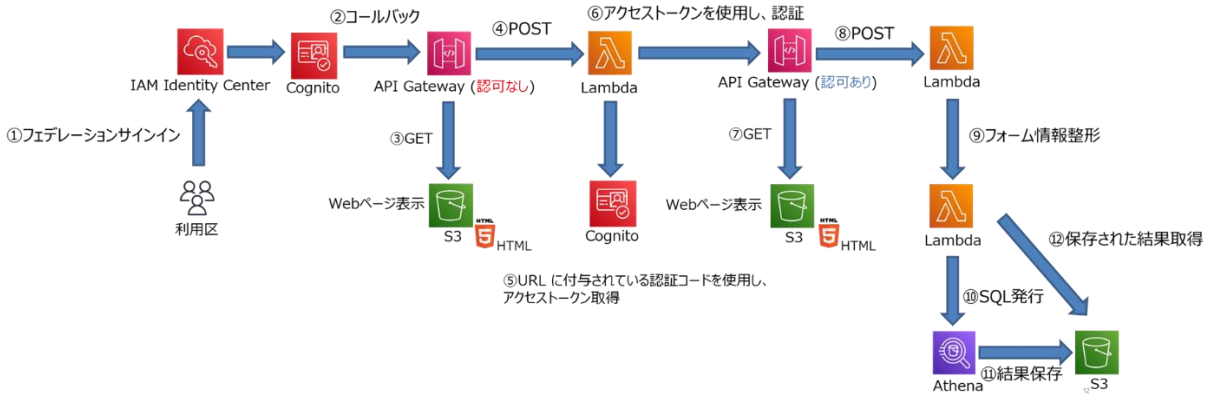

図 1.VPC Flowlogs 確認ツール構成

この構成では，API Gateway と S3 に保存した HTML などを使用して VPC Flowlog の検索ページを表示させています。実際のログ検索では，Lambda を通してログが集約されているアカウントの Athena でデータベーステーブルを作成しています。その内容を S3 に格納し、Lambda から検索結果を読み取る構成です。

図では省略していますが VPC エンドポイント経由で API Gateway にアクセスしています。そうすることによりオンプレミス内からプライベート IP アドレスでの接続が実現できます。

動作の流れ

詳細な動作の流れを説明します。各ステップは図 1 内の番号と連動しています。

1. AWS アクセスポータルへフェデレーションサインインを実施
2. アプリケーション一覧からツールを選択し、コールバック URL に遷移
3. 認可なし API Gateway は認証コード取得用ページを GET
4. ブラウザが JavaScript を実行し、認証コードをアクセストークン取得 Lambda に送信
5. Lambda は認証コードを使用し、アクセストークンを引き換えて Cookie に保存
6. 認可あり API Gateway にリダイレクト
7. 認可あり API Gateway は VPC Flowlogs 検索ツールのページを GET
8. ブラウザで必要な情報を入力し、フォームを送信
9. Lambda がブラウザからリクエストを受け取り、情報を整形し、Athena 実行 Lambda の呼び出し
10. Lambda は SQL を作成し、Athena を実行
11. 実行結果を S3 に格納

12. Lambda は S3 の結果を読み込み検索結果として Web ページ内に表示させる

以下は実際に検索した画面です。

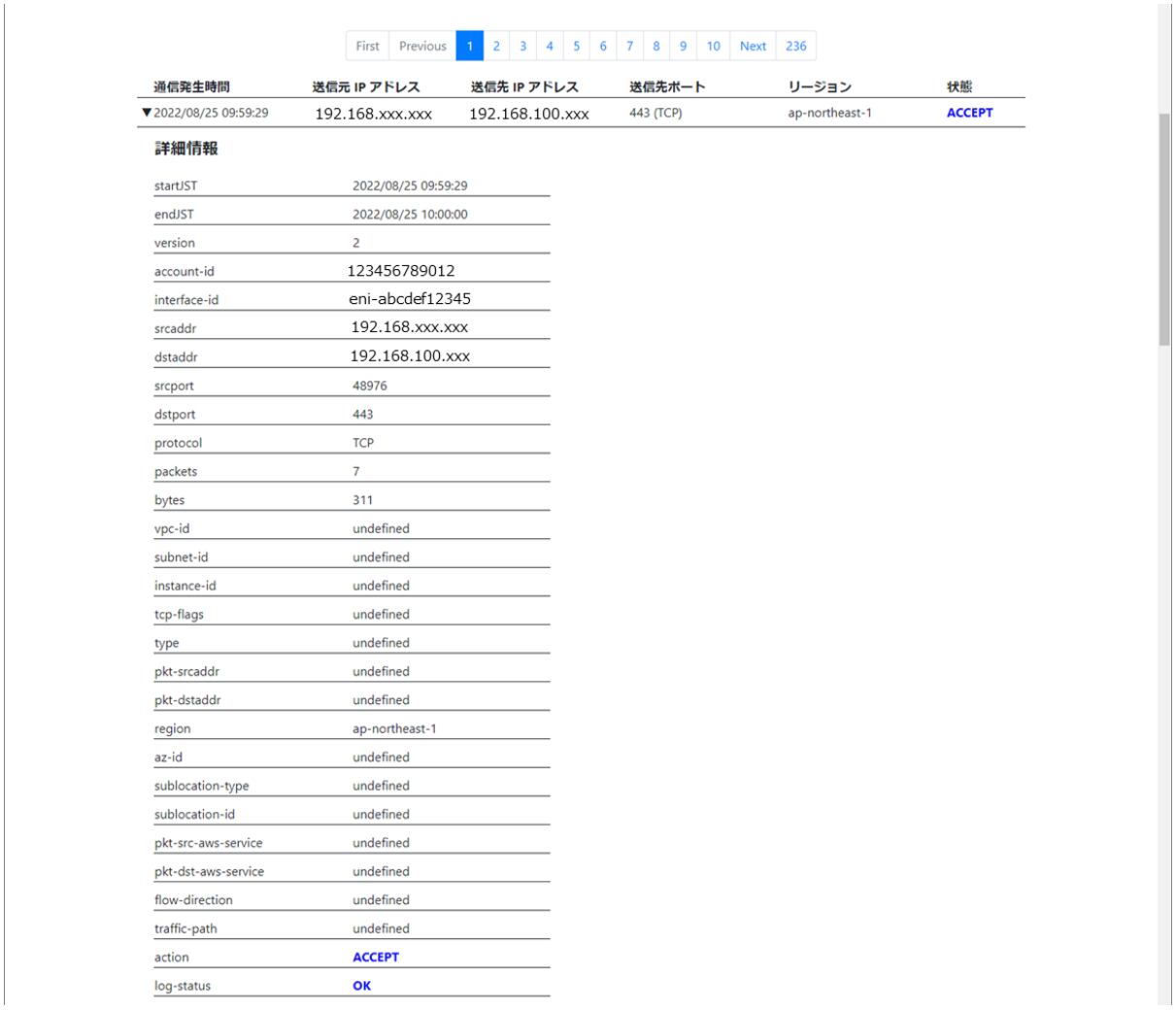

図 3.ログ検索結果(詳細表示)

検索時間は約 15 秒で完了し、確認することができます。ログの情報は膨大のため、各項目は最低限必要な日時、送信元 IP アドレス、送信先 IP アドレス、送信先ポート番号、リージョン、通信が実際に通っているかを示す状態のみを表示し、必要に応じて全ての状態が確認できる仕組みです。

手作業で確認する場合には以下のログからそれぞれの値がなんの項目かドキュメントと照らし合わせながら確認しなければならず、管理基盤側であっても直ぐには判断することが難しいです。

```
2 123456789012 eni-abcdef12345 192.168.xxx.xxx 192.168.100.xxx 1521 443 6 1 40 1696292447
1696292449 vpc-xxx subnet-xxx 192.168.xxx.xxx 192.168.100.xxx ap-northeast-1 - - egress 1 ACCEPT OK
```

ツールの詳細情報

✓ フロントエンド

HTML、CSS、JavaScript で構成しています。バックエンドの API Gateway とは XMLHttpRequest を使用し、通信しています。

✓ バックエンド

Lambda は全て Python で構成しています。図 1 では，認可あり API Gateway の先に Lambda が 2 つありますが、VPC Flowlogs の確認だけであれば 1 つにまとめてしまっても問題ありません。2 つで構成している意味としては、VPC Flowlogs のログだけではなく、オンプレミス内の Firewall のログ確認機能も持っているため、機能振り分け用として挟んでいます。

構築時の注意ポイント

構築する上で躓いたポイントを解説します。

✓ API Gateway のタイムアウト時間

Lambda の実行時間が最長 15 分なのは皆さんご存じかと思いますが、API Gateway にもタイムアウトの時間が存在します。Lambda と同じく 15 分程に設定できるかと思いきや、最長 30 秒です。負荷テストなどで判明することが多いのではないかと思います。構築後に判明してしまうと設計見直しやソースコードの改修でパフォーマンスを上げなければいけないので、考慮した上で設計を行いましょう。

✓ API Gateway の認可の設定

Cognito の設定と API Gateway 側でオーソライザーの設定を行えば、API Gateway が認可の設定を行ってくれると勘違いしていましたが、実際はリソース内のメソッドでオーソライザーを指定しないと設定されません。認可の設定をしないと，URL を直接打ちこむことで認証をクリアしていないにも関わらず、検索ページへアクセスできてしまいます。限ら

れた人のみにアクセス権を付与してアクセス制限を行っていますが、これではアクセス権がなくとも URL を知っているだけでアクセスが可能です。

✓　アクセストークンの付与

Lambda で認証コードを使用してアクセストークンを引き換え Cookie に保存していますが、ヘッダーに Authorization を埋め込むようにするエンジニアが多いのではないでしょうか。ツールの構成上，ヘッダーに Authorization を埋め込んでしまうと，ステータスコード 300 番台でのリダイレクトを行った際、ヘッダーの情報が欠落してしまい、認証が通りません。そのため、Cookie にアクセストークンを保存しています。

おわりに

以上、AWS VPC Flowlogs のサーバレス確認ツールの紹介でした。今回は様々な制約の元での作成であったため、選択の幅はかなり狭かったと思います。また、API Gateway と Lambda の間で 30 秒を超える処理はエラーが起きてしまうので、処理を更に最適化する，別のサービスと組み合わせるなどまだまだ改善点はあると思います。

社内向けアプリケーションであれば今回のように VPC エンドポイントを使用することでプライベート IP アドレスでのアクセスに限定できるので、セキュリティ面を考えるとかなりよいものではないかと思います。

GSLetterNeo Vol.183
2023 年 10 月 20 日発行
発行者　株式会社 SRA 技術本部 先端技術研究室

編集者　熊澤努　方 学芬
バックナンバー https://www.sra.co.jp/public/sra/gsletter/
お問い合わせ　gsneo@sra.co.jp

株式会社SRA
〒171-8513 東京都豊島区南池袋 2-32-8