Amazon EKSでFluent Bitを使って Amazon Kinesis Data Firehose へログ転送する際のポイント

Kubernetes Meetup Tokyo #22 LT (5min)

August 28, 2019

Isao Shimizu @isaoshimizu

About me

清水 勲 @isaoshimizu

株式会社ミクシィ
Vantageスタジオ みてね事業部 開発グループ

- 2011年8月 中途入社、SNS mixi アプリ運用チーム
- 2014年4月 モンスターストライク サーバーエンジニア、SRE
- 2018年2月〜現在 「家族アルバム みてね」 SRE

登壇歴: AWS Summit Tokyo 2014/2019, hbstudy, Internet Week, TechLION ほか

関わっているサービス

- 「家族アルバム みてね」 https://mitene.us/
- 世界に向けてサービス展開中
  - 海外では FamilyAlbum という名称 https://family-album.com/
  - 現在日本語と英語のみ（対応言語拡大予定）
- 2019 THE WEBBY AWARDS 受賞
- 2019 NATIONAL Parenting Product(NAPPA) AWARDS 受賞
- 2019年6月12日 **500**万人突破

今日お伝えしたいこと

- Amazon EKS上で、複数のログを Fluent Bitを経由して Amazon Kinesis Data Firehose へログ転送する際のポイント
- Kubernetes環境におけるFluent Bitの良さ

どういうシステムか

- Ruby on Railsアプリ
- AWS OpsWorksからAmazon EKSへ移行中
  - AWS Summit Tokyo 2019で発表したスライド
    https://speakerdeck.com/isaoshimizu/container-migration-in-familyalbum
- いままではRailsアプリ（fluent-logger-ruby）からlocalhostのFluentdにアクセスして、Amazon Kinesis Data Firehoseにログを転送し、S3へログを保存（ログ解析用途として使う）という流れ
- Nginxのログをtailして同様に転送

何をしたいか

- Kubernetes環境におけるログ転送
- Railsアプリのログ転送（従来通りfluent-logger-rubyを使いたい）
- 標準出力のログ転送
  - Kubernetesのシステムログ
  - Unicornログ
  - Nginxログ
- 極力ログをファイルに出力しない
  - ログファイルサイズのケア、ローテーションを運用したくない
- 転送されたログはログの分析基盤で使えるように

どうやって実現するか

Fluent Bit
https://fluentbit.io/

> Fluent Bit is a lightweight and extensible Log Processor that comes with full support for Kubernetes:

https://docs.fluentbit.io/manual/installation/kubernetes

Fluent Bit による集中コンテナロギング（AWSブログ）
https://aws.amazon.com/jp/blogs/news/centralized-container-logging-fluent-bit/

Fluent Bitはとても軽量

- Fluentd
  - ruby製
  - プロセスメモリ使用量 237MB（実測値）
  - Plugin豊富、できることが多い
- **Fluent Bit**
  - C言語製（組み込み機器やIoT向けと言われることも多い）
  - プロセスメモリ使用量 **28**MB（実測値）
  - Fluentdの設定ファイルはそのまま使えない（記法が全く違う）
  - 軽量。省コストにつながるというメリットがある

Fluent Bit でAmazon Kinesis Data Firehoseへ転送する

https://github.com/aws/amazon-kinesis-firehose-for-fluent-bit

Dockerイメージは amazon/aws-for-fluent-bit:**1.2.2** を利用

AWSのブログで解説されているイメージバージョンは1.2.0で古いので1.2.2以降を使いましょう

参考: 1.2.2で複数Pluginがサポートされた
https://github.com/aws/amazon-kinesis-firehose-for-fluent-bit/pull/4

設定ファイル（INPUT）

ConfigMapに記述します。
Fluentdと同様にPort 24224での待受と、Kubernetesのログtailを併用

```
    [INPUT]
        Name forward
        Listen 0.0.0.0
        Port 24224
        Buffer 512000
        Tag mitene.*

    [INPUT]
        Name tail
        Tag kube.*
        Path /var/log/containers/*.log
        Parser docker
        DB /var/log/flb_kube.db
        Mem_Buf_Limit 5MB
        Skip_Long_Lines On
        Refresh_Interval 10
```

設定ファイル（PARSER）

NginxログとDockerログのパース設定

```
    [PARSER]
        Name   nginx
        Format regex
        Regex ^(?<remote>[^ ]*) (?<host>[^ ]*) (?<user>[^ ]*) \[(?<time>[^\]]*)\] ...
        Time_Key time
        Time_Keep On
        Time_Format %d/%b/%Y:%H:%M:%S %z

    [PARSER]
        Name         docker
        Format       json
        Time_Key     time
        Time_Format %Y-%m-%dT%H:%M:%S.%L
        Time_Keep   On
```

設定ファイル（FILTER）

NginxログとKubernetesログのフィルタ設定

```
    [FILTER]
        Name parser
        Match kube.*
        Parser nginx
        Key_Name log

    [FILTER]
        Name                kubernetes
        Match               kube.*
        Kube_URL            https://kubernetes.default.svc:443
        Kube_CA_File        /var/run/secrets/kubernetes.io/serviceaccount/ca.crt
        Kube_Token_File     /var/run/secrets/kubernetes.io/serviceaccount/token
        Kube_Tag_Prefix     kube.var.log.containers.
        Merge_Log           On
        Merge_Log_Key       log_processed
        K8S-Logging.Parser  On
        K8S-Logging.Exclude Off
```

設定ファイル（OUTPUT）

Amazon Kinesis Data Firehoseへの転送設定。**タグごとに転送先を変えられる。**

```
    [OUTPUT]
        Name firehose
        Match kube.*
        delivery_stream mitene-kube
        region ap-northeast-1

    [OUTPUT]
        Name firehose
        Match mitene.log.*
        delivery_stream mitene-log
        region ap-northeast-1
```

これによって、タグごとにS3バケット/ディレクトリに格納できる

まとめ

- Kubernetesにおけるログ転送の一例を紹介
- Fluent Bit
  - 軽量でとてもよい（スループットも良い）
  - Kubernetesとの相性が良い（Kubernetes Filterが使える）
  - Amazon Kinesis Data Firehoseにも対応（Plugin）
  - 最新のDockerイメージ（1.2.2以降）を使うのがオススメ
- Fluentd利用を前提としていてKubernetesに移行する場合にオススメ
  - AWSかつFluentd前提でなければCloudWatch Logsも良い