aws DEV DAY
ONLINE JAPAN

B - 5

Deep Dive on DevOps for Serverless Applications

Keiichi Nakayama
Vice General Manager
Cloud Partner Group
CHARA-WEB Co., Ltd.

In Partnership with intel

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

自己紹介

- 中山　桂一 (@k1nakayama)
- 株式会社キャラウェブ
  クラウドパートナーグループ 副部長
- クラウドパートナー事業をリード
- 2020 APN AWS Top Engineers
- サーバーレス界隈に多く出没

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with intel

会社概要

会社名：株式会社キャラウェブ

所在地：東京都台東区東上野４−１２−１

資本金：7,161万円

主な事業内容：

- コンテンツ事業
  - 電子書籍のライセンスおよび管理，電子書籍販売
- クラウドパートナー事業
  - サーバーレスアプリケーション構築にフォーカスした
    アジャイルチーム提供サービス 他

当社はAWSパートナーネットワーク の
コンサルティングパートナーです

ISO/IEC 27001:2013 & JIS Q 27001:2014
クラウドに関するコンサルティング、設
計、構築、運用、管理 における認証

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with

本セッションについて

◆ 想定される聴講者

- DevOpsに取り組んでいる、またはこれから取り組もうとしている方
- サーバーレスアプリケーション開発に興味がある方
- 開発プロセスの改善を検討されている方

◆ ゴール

- AWSを活用した、サーバーレスアプリケーション開発のDevOpsにおけるポイントなどを知っていただく

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws DEV DAY
ONLINE JAPAN

Working on DevOps

In Partnership with intel

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DevOpsに取り組む上でのポイント

- ✓ 自動化

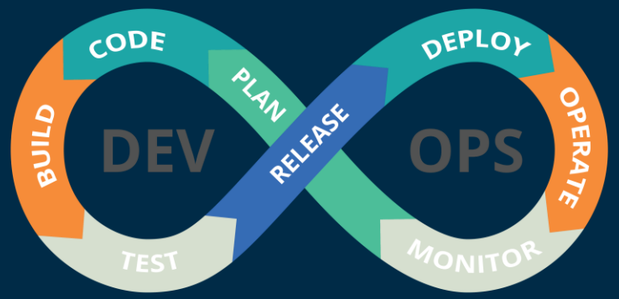
  原則としてすべてのプロセスにおいて属人性を排除し、自動的な流れで進む環境を作る

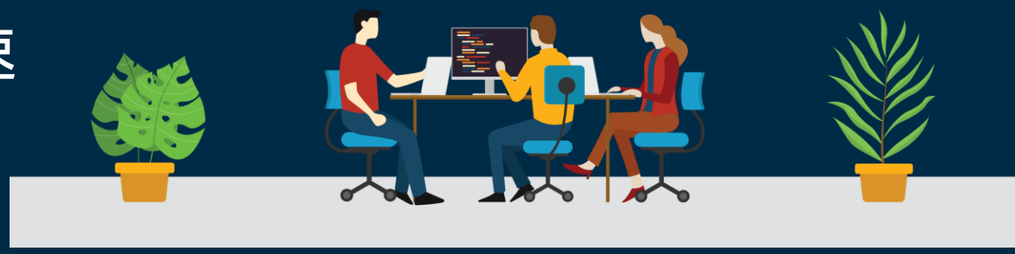
- ✓ 計測可能

  感覚値ではなく、数値化された指標やルールを用いることで、品質やコスト、その他すべてについて改善を行うことができる

- ✓ 高速な繰り返し

  一連のプロセスを価値ある最小限の単位で、高速に行い、そのプロセスを繰り返す





© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with

各プロセスでの考慮点

- Planning
  - マイクロサービス
  - AWSアカウント
- Code
  - ローカル環境でのユニットテスト
- Build
  - OS依存ライブラリ
  - 承認されたライブラリ
- Test
  - ユニットテスト
  - インテグレーションテスト
  - 脆弱性検査
- Release
  - リリース承認
- Deploy
  - Infrastructure as Code
- Operate
  - スケーリング
  - 障害復旧
  - ユーザーからのフィードバック
- Monitor
  - インシデントの検知
  - イベント追跡
  - コスト

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws DEV DAY
ONLINE JAPAN

Account Strategy

In Partnership with intel

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

プロダクト作成時の考慮点

- 環境の複製可能性
  開発・検証・商用等の各ステージを、1ソースのIaCで管理
- アカウント毎のクォータ
  アカウント毎に作成できるリソース数や実行上限等の制限がある
- アクセス権限管理
  ステージ毎のアクセス権限と、アカウント間の権限管理など
- コスト管理
  コスト管理を行う単位の明確化と計測方法

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

アカウント分割によるPros/Cons

Pros

- 原則として同一名称のリソースをアカウント毎に作成可能
- クォータ制約のコントロールがしやすい
- 明確な権限分離が可能
- アカウント単位でコストの把握が行える

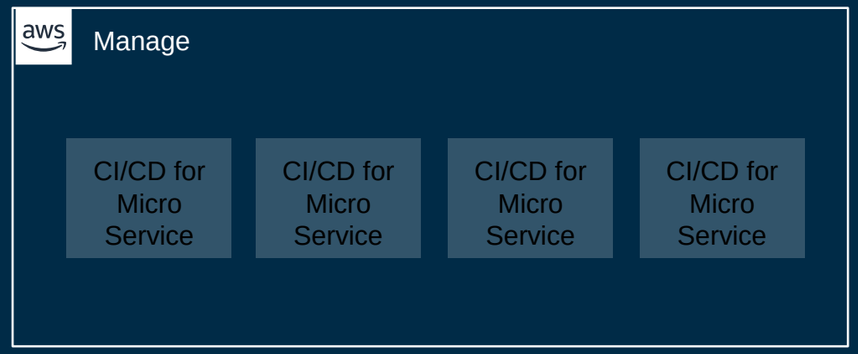
Cons

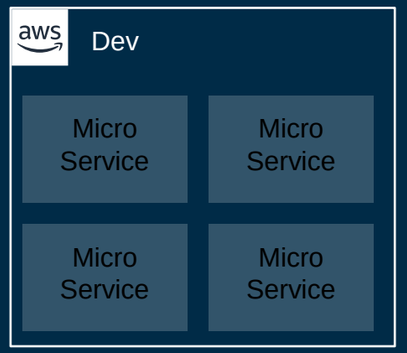
- アカウント間の権限管理が複雑
- アカウント横断でのデータ収集・分析が複雑
- CI/CD パイプラインにて複数アカウントに跨る場合、複雑化する
- マネジメントコンソールの切り替えが面倒

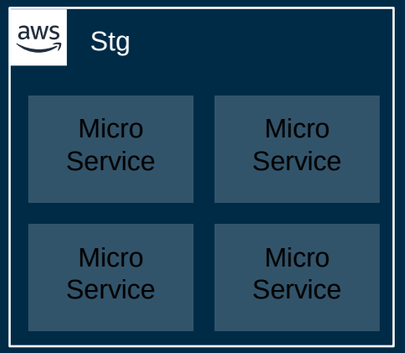
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

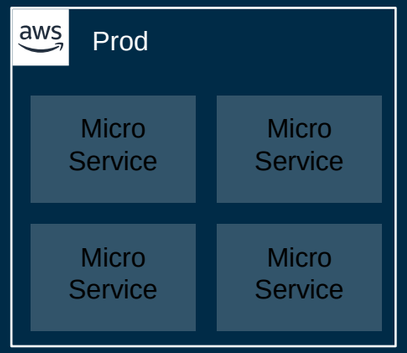
ステージ毎のアカウント分割

- 開発用
  新機能の開発を進めていくためのステージ
- 検証用
  商用にリリースする前の検証用ステージ
- 商用
  エンドユーザーへ実際に提供を行うステージ
- 管理用
  CI/CDパイプラインやソースコードリポジトリを配置したり、各アカウントを中央管理する









ステージ毎の権限分離やコストの把握が行いやすい

比較的中小規模なプロダクトにオススメ

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with intel

マイクロサービス毎のアカウント分割

- マイクロサービス毎ステージ毎

  ステージ毎のアカウント分割の4アカウントを、更にマイクロサービス毎に分割する

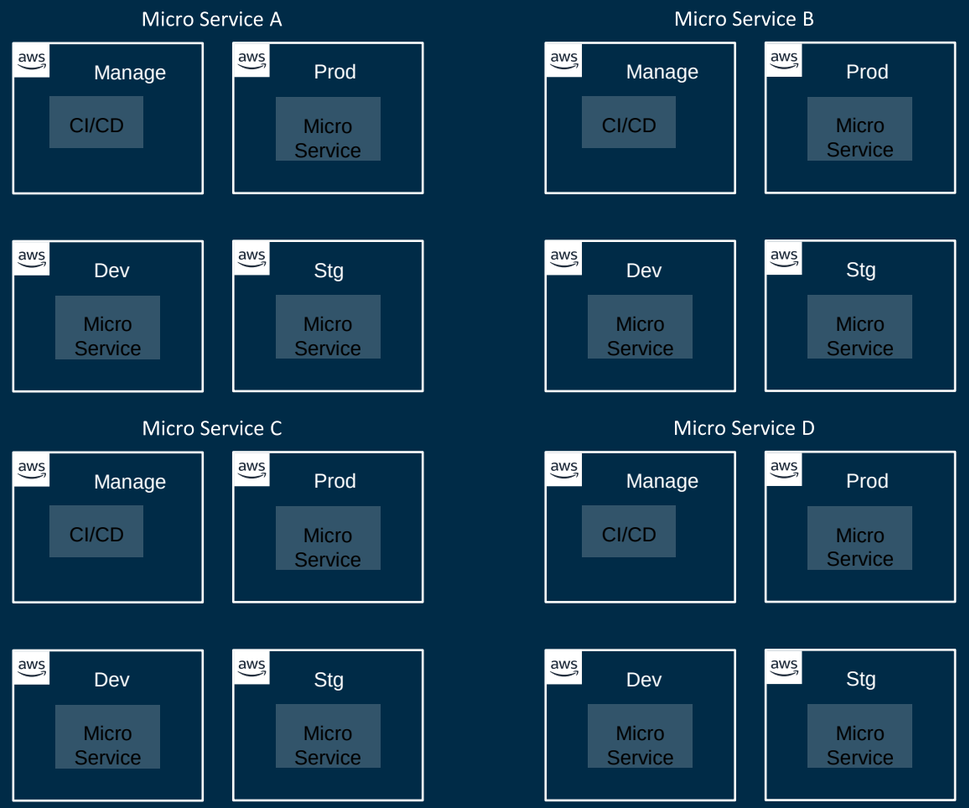
  マイクロサービス本来のポリシーが担保しやすく、きめ細やかな管理が実現できる

- マイクロサービス毎

  マイクロサービス毎に単一のアカウントを設け、アカウント内にCI/CDや各ステージを含む形で運用する

  マイクロサービス毎にDevOpsチームが分割されている組織などでは扱いやすい

マイクロサービス毎の権限分離やコストの把握が行いやすい



大規模なプロダクトにオススメ

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with

(宣伝) Cloud Partner Billing

日本円・請求書払

初期設定・証跡管理設定

サイバー攻撃の損害
保険による補償

AWS利用料について、全リージョン・全サービス※3%割引にてご提供いたします

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

※一部対象外となるサービスや利用タイプがあります。詳しくはお問い合わせください。

aws DEV DAY
ONLINE JAPAN

CI/CD Pipelines

In Partnership with intel

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CI/CD Pipelineの役割

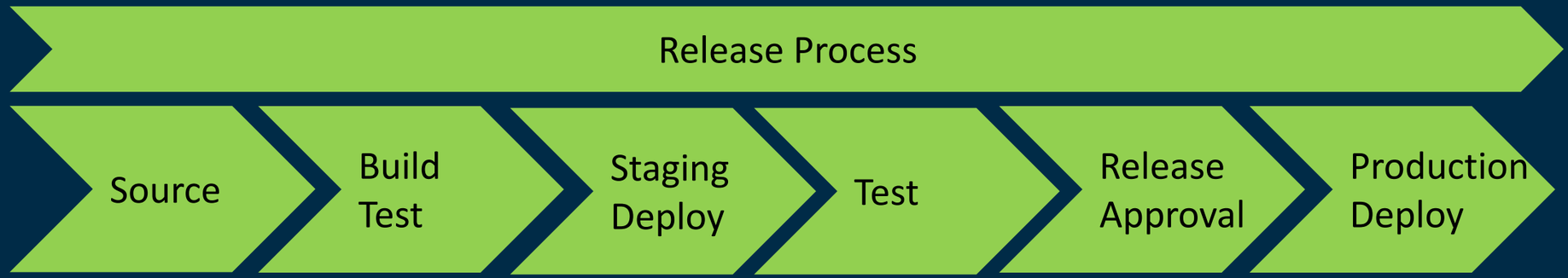
- リリースプロセスの自動化

  全てのコミットはリリース対象として扱い、特定のブランチへのプッシュにより自動的にリリースプロセスが稼働し、ターゲットステージへのデプロイまでが自動的に行われる。

  これにより、プロダクトの価値を素早く頻繁にエンドユーザーへデリバリーする
- 品質の安定化

  リリースターゲットに対するユニットテストのカバレッジや、静的コード解析を自動的に実行することで、一定基準の品質を保った安定したプロダクトをリリースする
- 統制管理

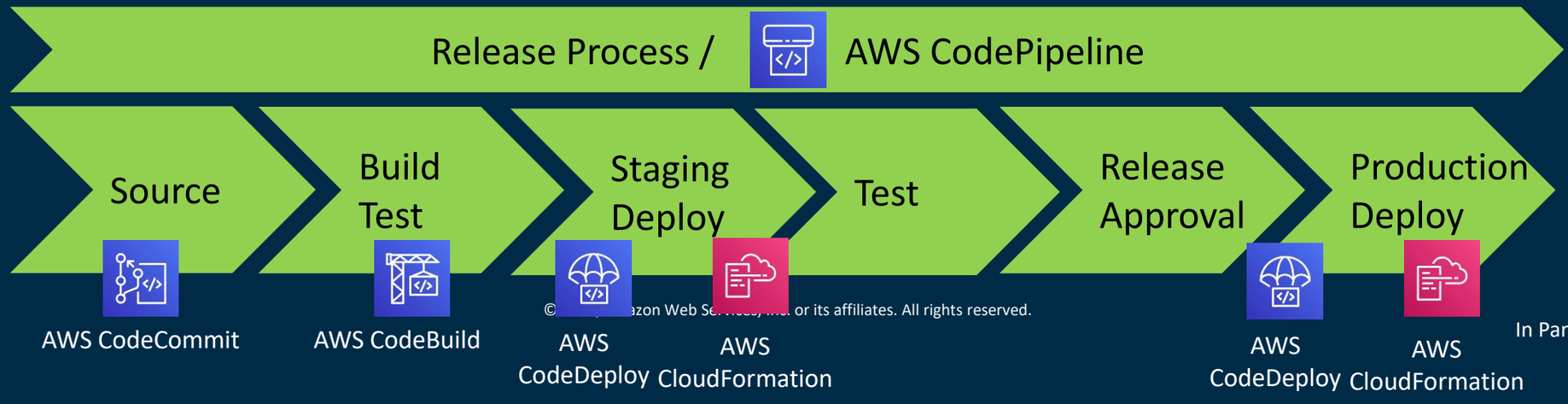
  組織のルールに則ったリリース承認フローや、使用されるライブラリのチェック、脆弱性検査等を強制する



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CI/CDを構成するサービス

- Pipeline
  - AWS CodePipeline
- Source
  - AWS CodeCommit
  - GitHub
- Build / Test
  - AWS CodeBuild
  - AWS CodeArtifact
- Deploy
  - AWS CloudFormation
  - AWS CodeDeploy
  - AWS Cloud Development Kit (CDK)
- Notification
  - Amazon Simple Notification Service (SNS)
  - AWS Chatbot
  - AWS CodeStar Nortifications



© Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with

AWS CodeArtifact

- 安全かつスケーラブルなアーティファクト管理サービス
- npmやPyPi、Maven等のパブリックリポジトリに対応
- 独自パッケージの管理も可能
- パッケージ、バージョンの利用を管理し、承認することができる
- Amazon EventBridgeと組み合わせることで、依存パッケージの更新を検知し、AWS CodePipelineのパイプライン実行を自動化可能

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with intel

静的解析（SAST）

- Bandit
  - Python用SASTツール
  - コード解析により様々な脆弱性を解析
  - CodeBuildで自動テストを実行
  - 指摘の意図と異なるコードについて、ライン単位での除外設定なども可能

https://pypi.org/project/bandit/

```
$ bandit -r functions/src
[main]  INFO    profile include tests: None
[main]  INFO    profile exclude tests: None
[main]  INFO    cli include tests: None
[main]  INFO    cli exclude tests: None
[main]  INFO    running on Python 3.7.6
Run started:2020-05-23 01:14:30.682260


Test results:

>> Issue: [B311:blacklist] Standard pseudo-random generators are not suitable for security/cryptographic purposes.
   Severity: Low   Confidence: High
   Location: functions/src/manager/manager.py:120
   More Info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

119                 self.__check_mail_addr()
120                 self.id = str(random.randint(1000000, 9000000))
121                 self.created_at = int(datetime.timestamp(datetime.now()))

--------------------------------------------------

>> Issue: [B311:blacklist] Standard pseudo-random generators are not suitable for security/cryptographic purposes.
   Severity: Low   Confidence: High
   Location: functions/src/organization/organization.py:77
   More Info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

76                  # 新規登録
77                  self.id = str(random.randint(1000000, 9000000))
78                  self.created_at = int(datetime.timestamp(datetime.now()))

--------------------------------------------------


Code scanned:
        Total lines of code: 1951
        Total lines skipped (#nosec): 0

Run metrics:
        Total issues (by severity):
                Undefined: 0.0
                Low: 2.0
                Medium: 0.0
                High: 0.0

        Total issues (by confidence):
                Undefined: 0.0
                Low: 0.0
                Medium: 0.0
                High: 2.0

Files skipped (0):
```

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with intel

パイプラインの実行状況管理

- CI/CDパイプラインの実行は比較的長時間かかる
- チームメンバー全員が随時パイプラインの実行状況を把握できるようにする
- Slackへの通知を行い、リアルタイムな状況把握を行う
- CodeStar NotificationやEventBridgeによりCodeCommitやCodePipelineのイベントを検知し、SNSへの通知を行いChatbotにより通知

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws DEV DAY
ONLINE JAPAN

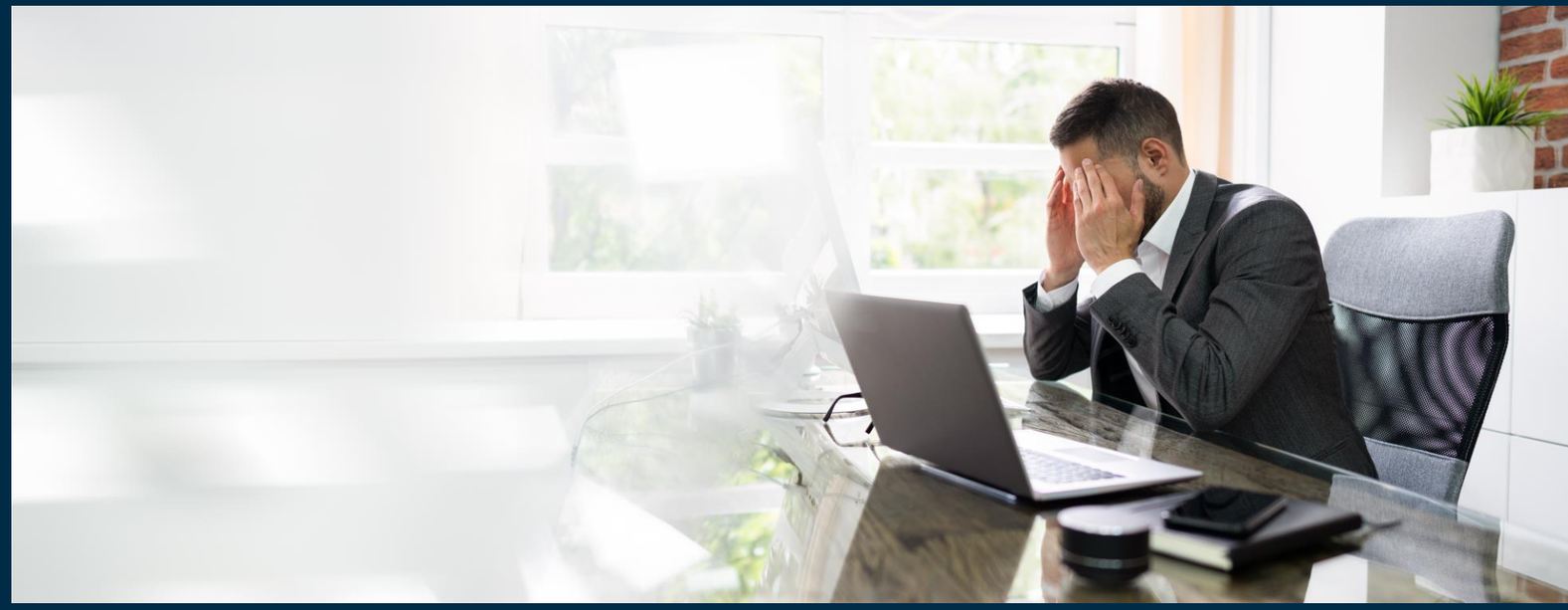
CDK Pipelines

In Partnership with intel

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CI/CD Pipeline構築時の課題

- クロスアカウントデプロイが複雑
- アプリケーションの構成変化に伴うPipelineの更新が必要
- CI/CD Pipeline自体のデプロイ管理



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with

CDK Pipelines **Developer Preview**

- CI/CD Pipelineとアプリケーションの構成を1つのAWS CDKアプリケーションでまとめて構成
- 簡単な初期設定とPipeline定義内のステージ指定に対し、アカウント番号を指定するだけで、クロスアカウントデプロイが定義できる
- アプリケーションの構成に合わせて自動的にパイプラインを更新

https://docs.aws.amazon.com/cdk/api/latest/docs/pipelines-readme.html

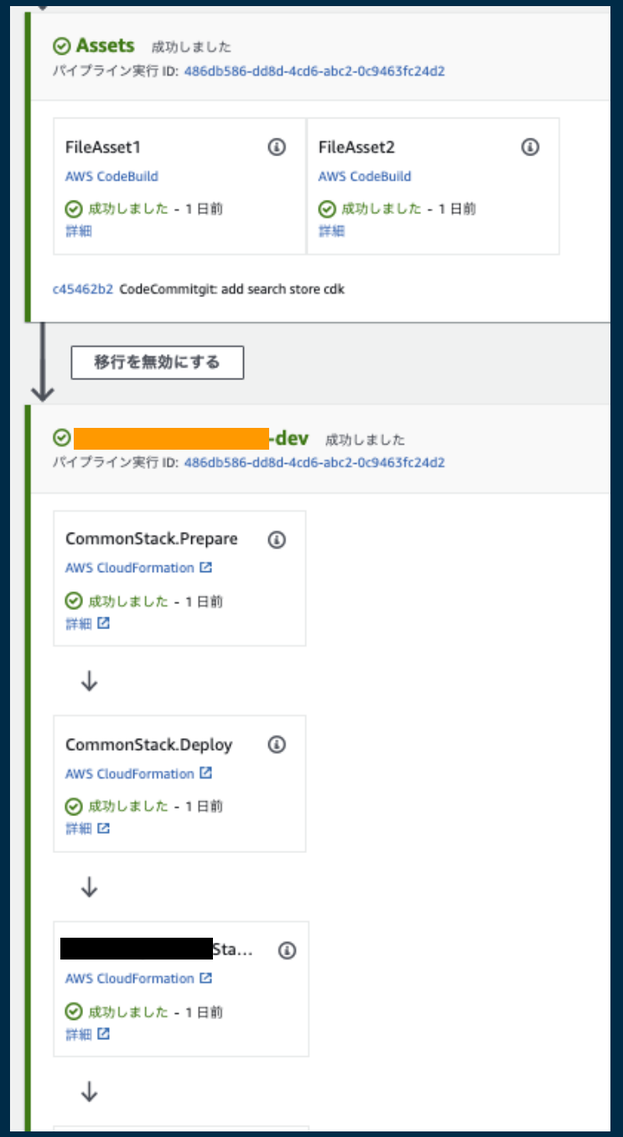
```
# CDKのbootstrap (アカウント間の信頼関係の設定）
$ cdk bootstrap --profile manage --cloudformation-execution-policies
arn:aws:iam::aws:policy/AdministratorAccess
aws://999999999999/ap-northeast-1

$ cdk bootstrap --profile dev --trust 999999999999
--cloudformation-execution-policies
arn:aws:iam::aws:policy/AdministratorAccess
aws://123456789012/ap-northeast-1

# CDK Pilelinesによるステージ定義
dev = PipelineStage(self,
self.node.try_get_context('repository_name') + "-dev",
env={
'region': "ap-northeast-1", 'account': ”123456789012"}
)
dev_stage = pipeline.add_application_stage(dev)
```

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with intel

Self Mutation

- CDK Pipelinesは、自身のパイプライン構成をアプリケーション構成の変化に合わせて自動的に更新
- Lambda Functionが追加された場合のアセットのアップロードアクションは平行実行が行われるように構成
- スタック間の依存関係を考慮しデプロイアクションが自動的に構成される



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with intel

aws DEV DAY
ONLINE JAPAN

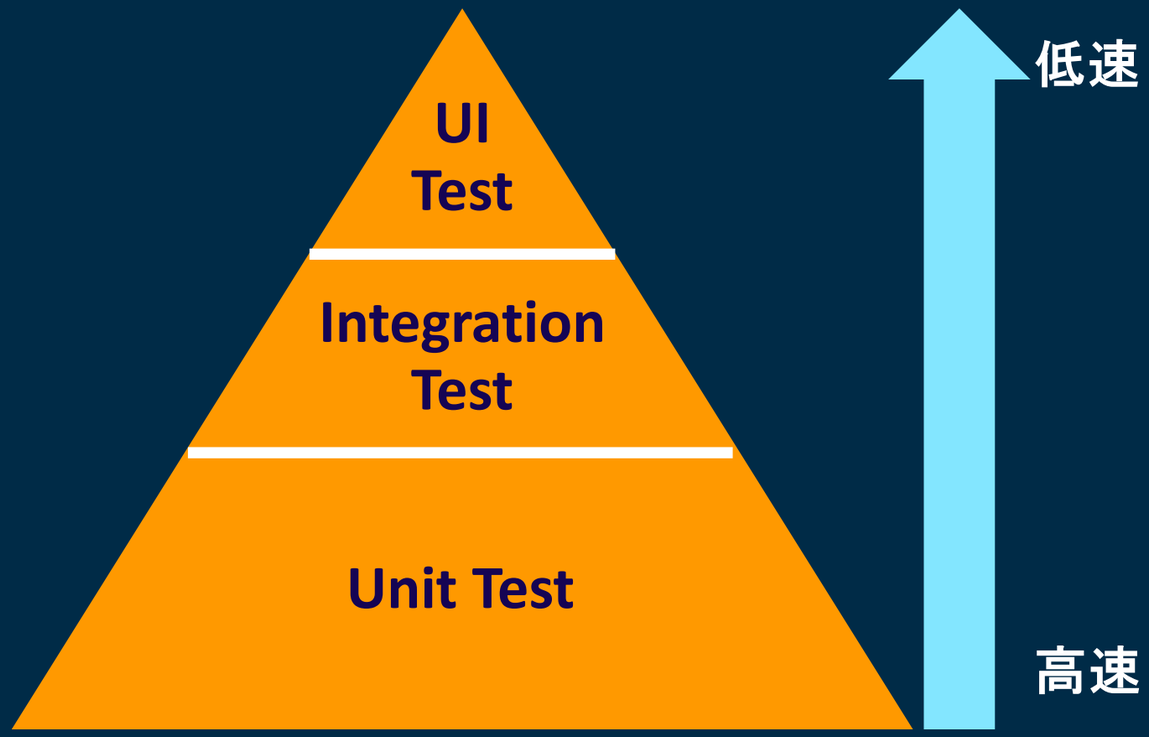
Unit Testing

In Partnership with intel

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ユニットテストのポイント

- ✓ ローカル環境でユニットテストを行いながら開発を進める
- ✓ 各メソッドをピュアに保ち、テスト可能なメソッドにする
- ✓ UIテストやインテグレーションテストではテストを行いにくい例外処理についても網羅的にテストを実行できる
- ✓ カバレッジを計測し一定基準を保ったテストが行われていることを担保する



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with

モックの活用

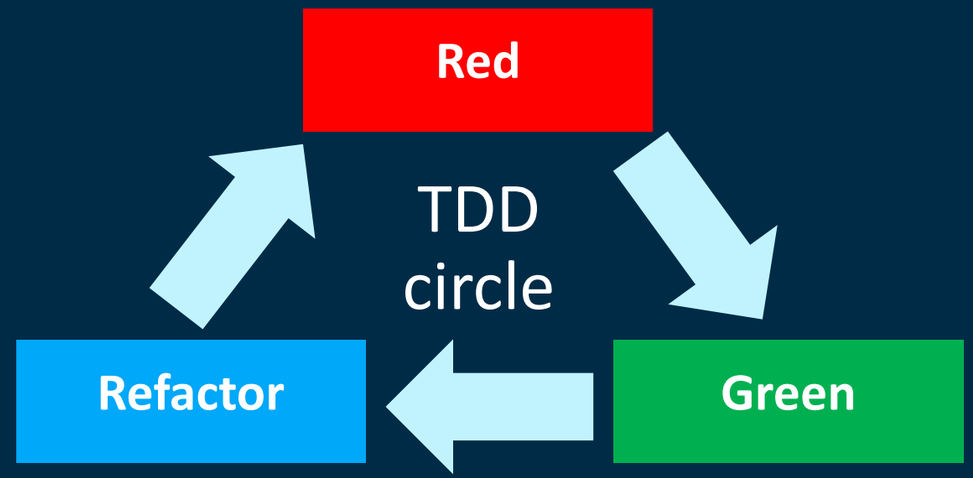
- moto (https://github.com/spulec/moto)
  Python用モックライブラリ
  Boto3の多くのAPIをモック化できる
  予めテスト開始時に前提とする状態を定義しておき、テスト結果が想定したとおりのレスポンスになるか、DynamoDB等のAWSリソースの状態についても想定通りかをテストする

- LocalStack (https://github.com/localstack/localstack)
  ローカル環境にAWS環境を再現できるツール
  AWS SDKの接続先エンドポイントをLocalStack環境に変更してテストを行う
  AWS SDKをモック化してはいないため、比較的正確な結果を得ることができる

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Test Driven Development

- TDDは下記のサイクルで行う
  - Red
    1つのテストを追加し、テストが失敗することを確認する
  - Green
    テストが成功するための最低限のコードを追加する
  - Refactor
    コードをリファクタリングする
- TDDにより小さくインクリメンタルに開発を進める
- 常にカバレッジが高く質の高いコードになりやすい



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with

aws DEV DAY
ONLINE JAPAN

Integration Testing

In Partnership with intel

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

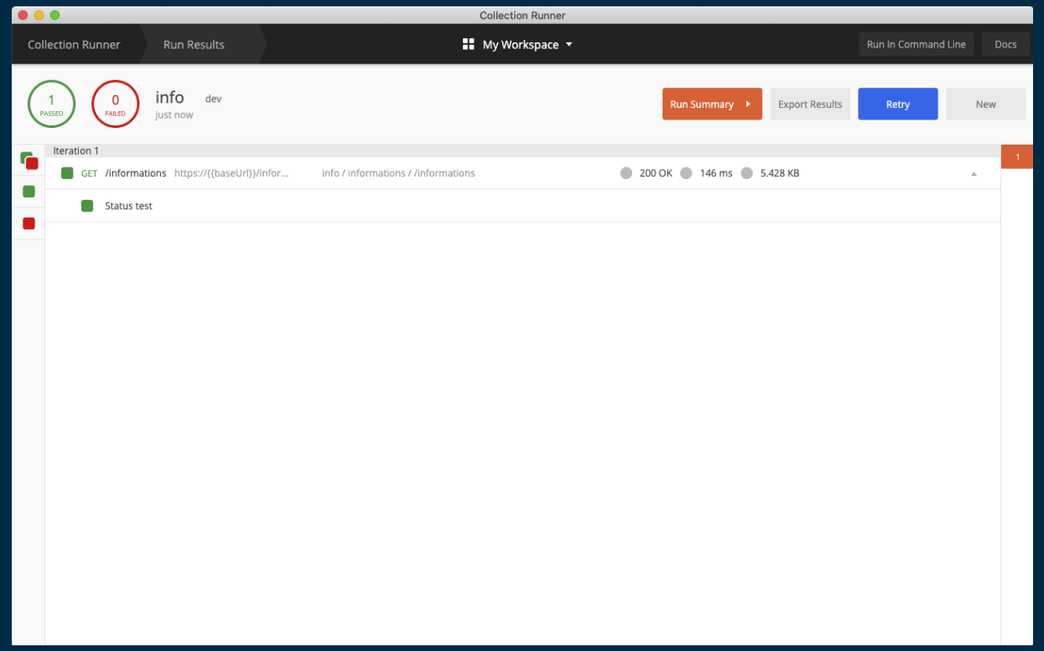
APIテスト

◆ APIテストの目的

- デプロイ後に実際のAPIを使用し、想定通りの動作が行われるかをテスト
- 権限不足、モックとの挙動差異、マッピングテンプレートの誤り等による問題を早期発見

◆ Postman + Newman

- PostmanによりTestの定義を作成
- CI/CDのデプロイ後のアクションにNewmanを使用した自動APIテストを行う
- Postmanを使用しAPIのモックを作成することも可能
- AWS Signature V4認証(IAM認証)にも対応




```
(cwknakayama@localhost:(master*) $ /Users/cwknakayama/.nodenv/versions/12.12.0/bin/newman run -e dev.postman_environment.json info.postman_colle
ction.json
newman

info

❑ informations
↳ /informations
  GET https://information.apidev.chara-web.net/v1/informations?platform=web [200 OK, 5.3KB, 7s]
  ✓  Status test
```

	executed	failed
iterations	1	0
requests	1	0
test-scripts	1	0
prerequest-scripts	0	0
assertions	1	0
total run duration: 7.1s		
total data received: 4.96KB (approx)		
average response time: 7s [min: 7s, max: 7s, s.d.: 0µs]		

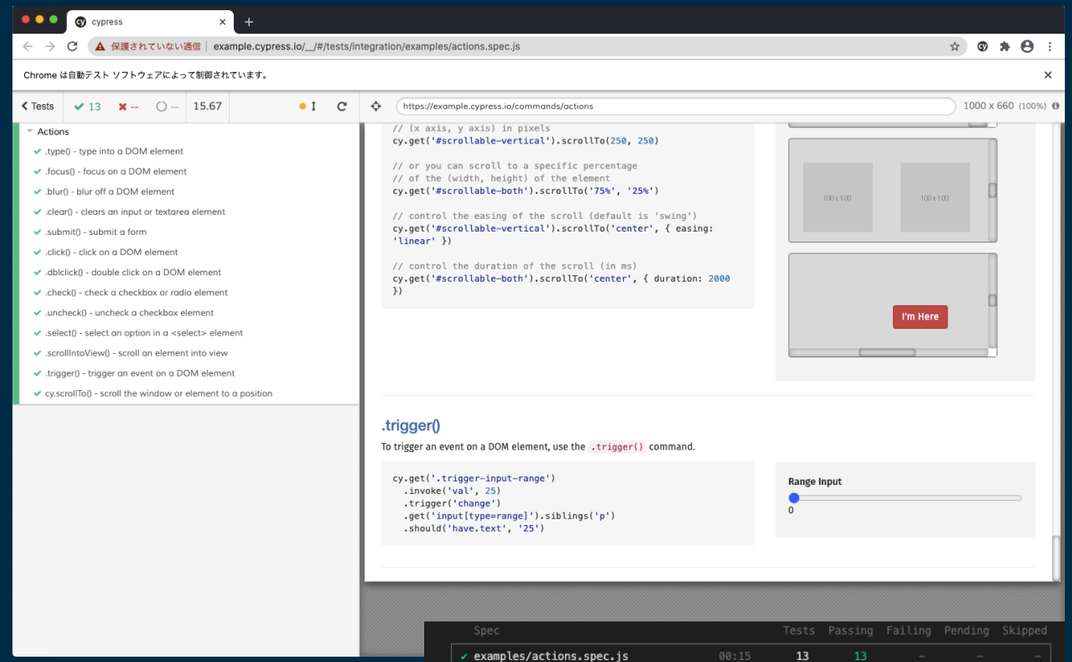
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

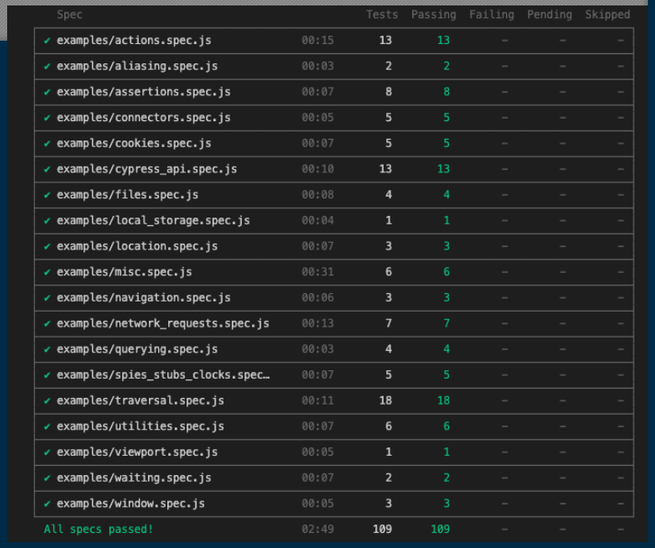
In Partnership with

UIテスト(E2Eテスト)

◆ UIテストの目的

- 実際のUIを通じて一気通貫で想定した挙動になっているかを確認する
- プロダクト全体を俯瞰的にテストする
- 機能改修により想定していない範囲への影響が発生していないかを確認する





◆ Cypress (https://cypress.io)

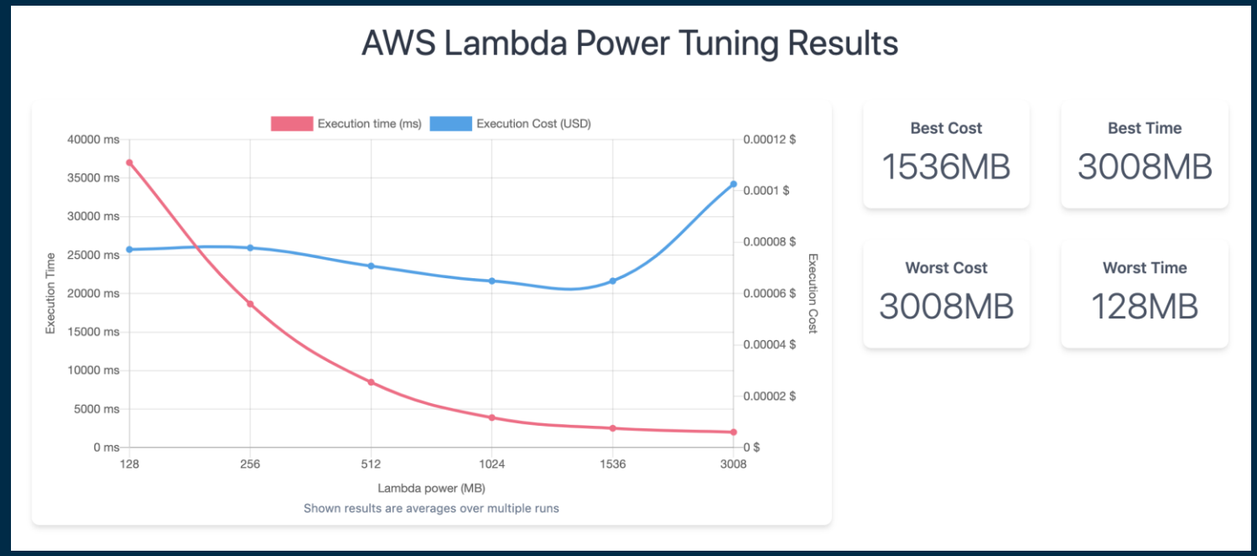
- Web UIテストツール
- JavaScriptにてテストを記述
- 簡単に各テストにおけるエビデンス用キャプチャを取得できる
- CI/CDにて自動テスト実行可能
- テストの一連の状況を動画で取得可能

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with

AWS Lambda Power Tuning

- Lambda Functionのメモリ割り当てを最適化するためのツール
- 複数のメモリ量で複数回実行を行い、最もコストが安いメモリ量や最も実行時間が短いメモリ量の測定を自動的に行う
- 右図のような結果を確認できるUIが提供される
- CI/CDに組み込み自動最適化可能
- テスト実行前後の処理を行うLambda Functionを指定可能



※公式GitHubより引用

https://github.com/alexcasalboni/aws-lambda-power-tuning

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with

aws DEV DAY
ONLINE JAPAN

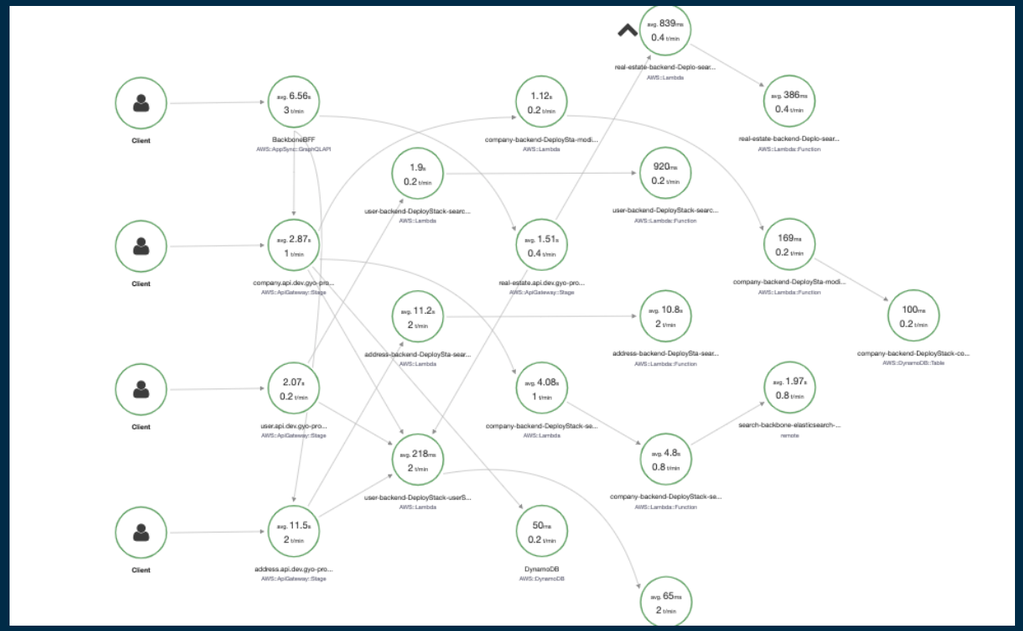
Monitoring

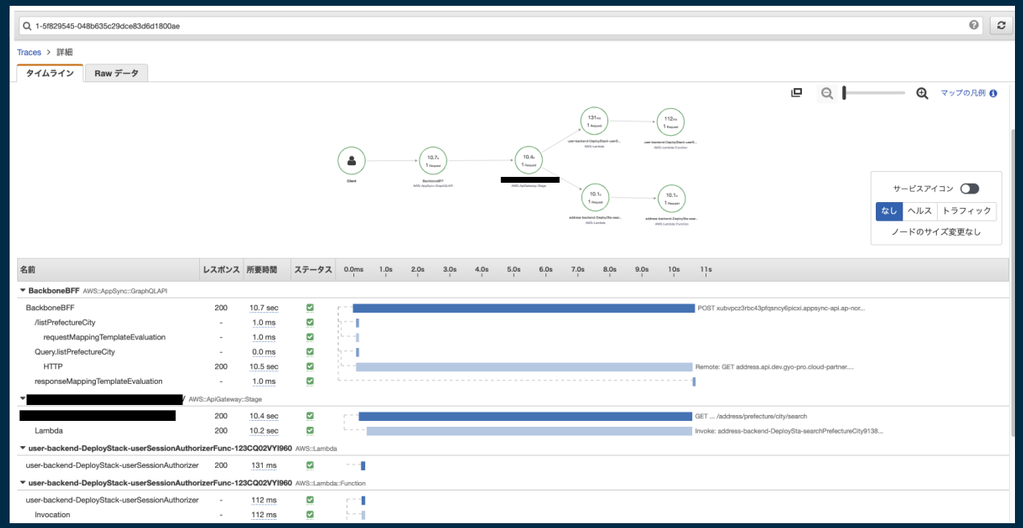
In Partnership with intel

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS X-Ray

- 分散アプリケーションの解析・デバッグツール
- イベントの追跡を視覚的に簡単に行える
- 基本的にサービス毎のTracing設定を有効化するだけ
- 運用効率化のために、様々なイベントによるデータの格納時にTracingIDを一緒に保管すると便利
- 応用的な活用でコード内のどこに時間が掛かっているかなど、パフォーマンス向上に役立てる



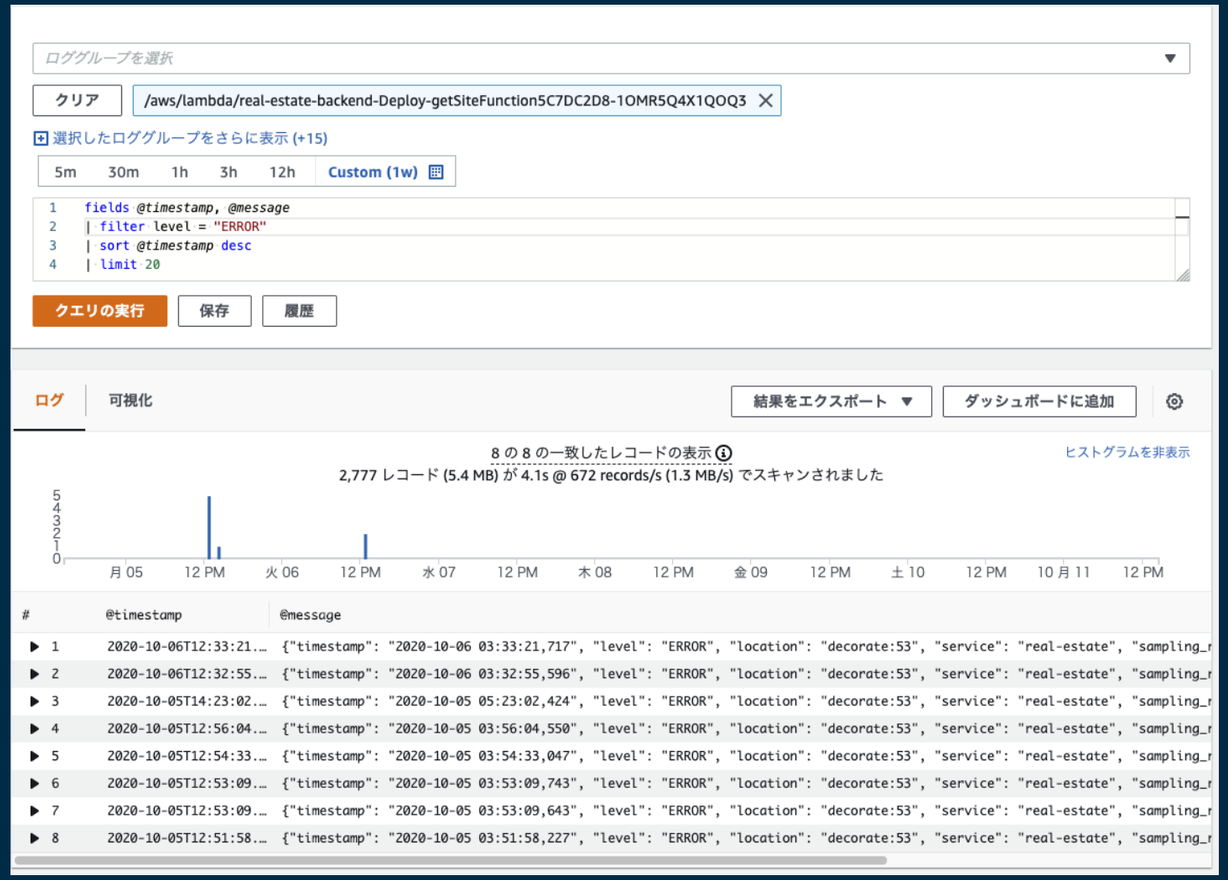


© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with intel

ログ監視

- インシデントが発生した際、ログへ詳細を出力することにより、通知を受ける仕組みを構築する
- Lambdaからのログについて、構造化されたログ出力を行う
- CloudWatch Logs Insightにより、必要に応じた効率的なログ解析を行うことができる



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with intel

AWS Lambda Powertools

- Lambda Functionにおけるロギング、トレース、メトリクス送信を簡単に行うことができるライブラリ
- 自動的に構造化ログ形式で出力が行われる
- Lambda FunctionのContext情報を自動的にログに含める機能や、コールドスタートか否かを判別しログに記録する機能などが使える
- メソッド毎に掛かった時間などをX-Rayで確認することが容易に行える

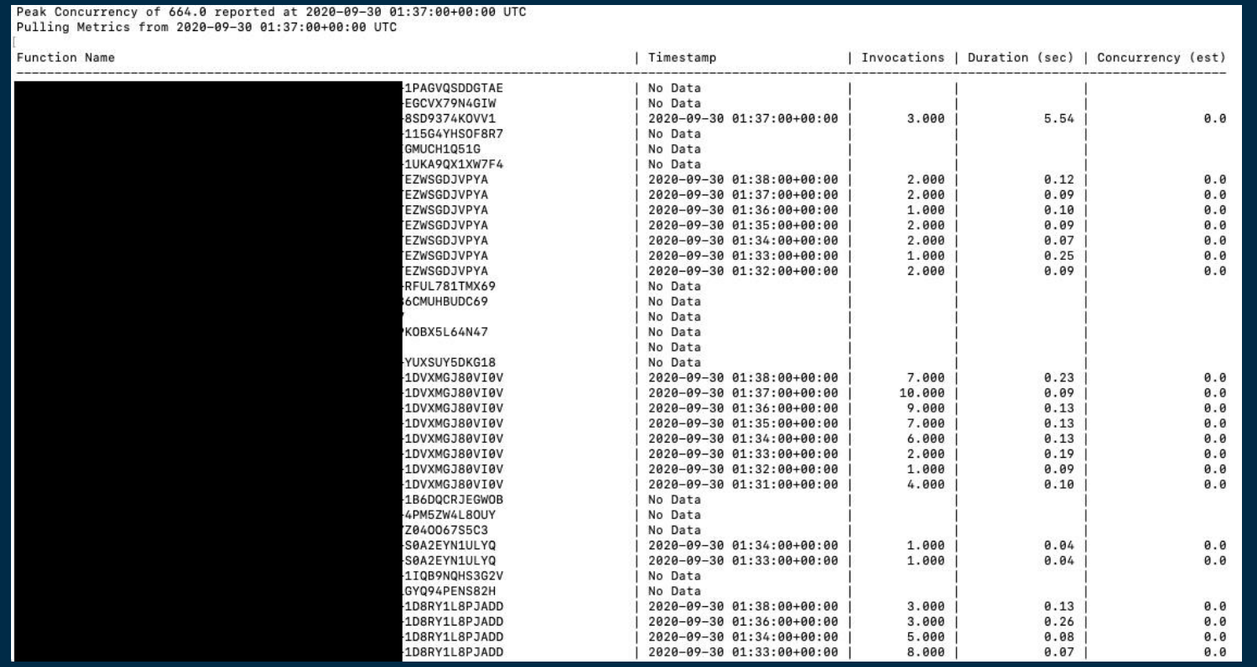
Python: https://github.com/awslabs/aws-lambda-powertools-python
Java: https://github.com/awslabs/aws-lambda-powertools-java
詳しくは：https://speakerdeck.com/_kensh/aws-lambda-powertools

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with

Lambda Concurrency Hunt

- 過去2週間の中でLambda Function毎に最も同時実行数が多かった時間を見つけ、関数の呼び出し回数、平均実行時間、同時実行数をレポートする
- Lambdaはリージョン毎に同時実行数の制限がある
- 不要なスパイクを見つけ、意図しないスロットリング等の対策を行う助けとなる



```
Peak Concurrency of 664.0 reported at 2020-09-30 01:37:00+00:00 UTC
Pulling Metrics from 2020-09-30 01:37:00+00:00 UTC
[
Function Name                                                    | Timestamp                 | Invocations | Duration (sec) | Concurrency (est)
-----------------------------------------------------------------------------------------------------------------------------------------------------
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | 2020-09-30 01:37:00+00:00 |       3.000 |           5.54 |              0.0
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | 2020-09-30 01:38:00+00:00 |       2.000 |           0.12 |              0.0
                                                                 | 2020-09-30 01:37:00+00:00 |       2.000 |           0.09 |              0.0
                                                                 | 2020-09-30 01:36:00+00:00 |       1.000 |           0.10 |              0.0
                                                                 | 2020-09-30 01:35:00+00:00 |       2.000 |           0.09 |              0.0
                                                                 | 2020-09-30 01:34:00+00:00 |       2.000 |           0.07 |              0.0
                                                                 | 2020-09-30 01:33:00+00:00 |       1.000 |           0.25 |              0.0
                                                                 | 2020-09-30 01:32:00+00:00 |       2.000 |           0.09 |              0.0
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | 2020-09-30 01:38:00+00:00 |       7.000 |           0.23 |              0.0
                                                                 | 2020-09-30 01:37:00+00:00 |      10.000 |           0.09 |              0.0
                                                                 | 2020-09-30 01:36:00+00:00 |       9.000 |           0.13 |              0.0
                                                                 | 2020-09-30 01:35:00+00:00 |       7.000 |           0.13 |              0.0
                                                                 | 2020-09-30 01:34:00+00:00 |       6.000 |           0.13 |              0.0
                                                                 | 2020-09-30 01:33:00+00:00 |       2.000 |           0.19 |              0.0
                                                                 | 2020-09-30 01:32:00+00:00 |       1.000 |           0.09 |              0.0
                                                                 | 2020-09-30 01:31:00+00:00 |       4.000 |           0.10 |              0.0
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | 2020-09-30 01:34:00+00:00 |       1.000 |           0.04 |              0.0
                                                                 | 2020-09-30 01:33:00+00:00 |       1.000 |           0.04 |              0.0
                                                                 | No Data                   |             |                |
                                                                 | No Data                   |             |                |
                                                                 | 2020-09-30 01:38:00+00:00 |       3.000 |           0.13 |              0.0
                                                                 | 2020-09-30 01:36:00+00:00 |       3.000 |           0.26 |              0.0
                                                                 | 2020-09-30 01:34:00+00:00 |       5.000 |           0.08 |              0.0
                                                                 | 2020-09-30 01:33:00+00:00 |       8.000 |           0.07 |              0.0
```

https://github.com/aws-samples/aws-lambda-concurrency-hunt

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

In Partnership with intel

aws DEV DAY
ONLINE JAPAN

まとめ

In Partnership with intel

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

まとめ

- 一連の流れを自動化し、計測可能にし高速に繰り返すことが重要である
- 適切なアカウント戦略を行う
- 様々なAWSサービスとサードパーティツールを活用し、CI/CDパイプラインの構築を行う
- テストの手法やツールも豊富にあるため、組織やチームの求めるプロダクトの品質に合わせて取り入れていく
- 構築時の設定や、ライブラリの活用により、運用時の効率化を図ることができる

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws DEV DAY
ONLINE JAPAN

Thank you!

サーバーレスアプリケーションやAWSを活用したDevOpsについてのご相談は、下記までお気軽にお問い合わせください。

Keiichi Nakayama
@k1nakayama

株式会社キャラウェブ
クラウドパートナーグループ

TEL: 03-6670-2560
Mail: inquiry@cloud-partner.jp

In Partnership with intel

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.