

ごった煮

ctrl + F → サービス名で必要な情報拾えるかも？

Amazon Macie

セキュリティリスクを発見し保護する機械学習のセキュリティサービス

Amazon GuardDuty

脅威検出サービス

管理者がメンバーに招待を送ることで一元管理が可能になる

AWS Config

AWSリソースの設定を評価するサービス

AWS Configアグリタ：最小の運用管理、**Config設定とコンプライアンスデータを収集**

- 1.AWS Configに設定ルールを定義
- 2.リージョンとアカウント全体のデータを収集
- 3.S3に保存→SNSで通知

Amazon EventBridge

Amazon CloudWatch Events

リソースのイベントをターゲットにして設定することでトリガーの問題を評価して通知できる

リアルタイムトラッキングを提供し、変更の監視や復旧を同時に行える

開始/停止アクションのためにスケジュールされたイベントをトリガーするために使用できる

CloudWatch Logsサブスクリプション

マネージドサービスは連携できない

ログインを追跡できる

Lambdaを使ってタグ付けが可能

例：CloudWatchLogsサブスクリプションでログインを追跡→ログインが検知されたインスタンスにLambdaでタグ付け→Eventbridgeでタグをトリガーに削除

Amazon KinesisとAWS Lambdaとの統合が可能

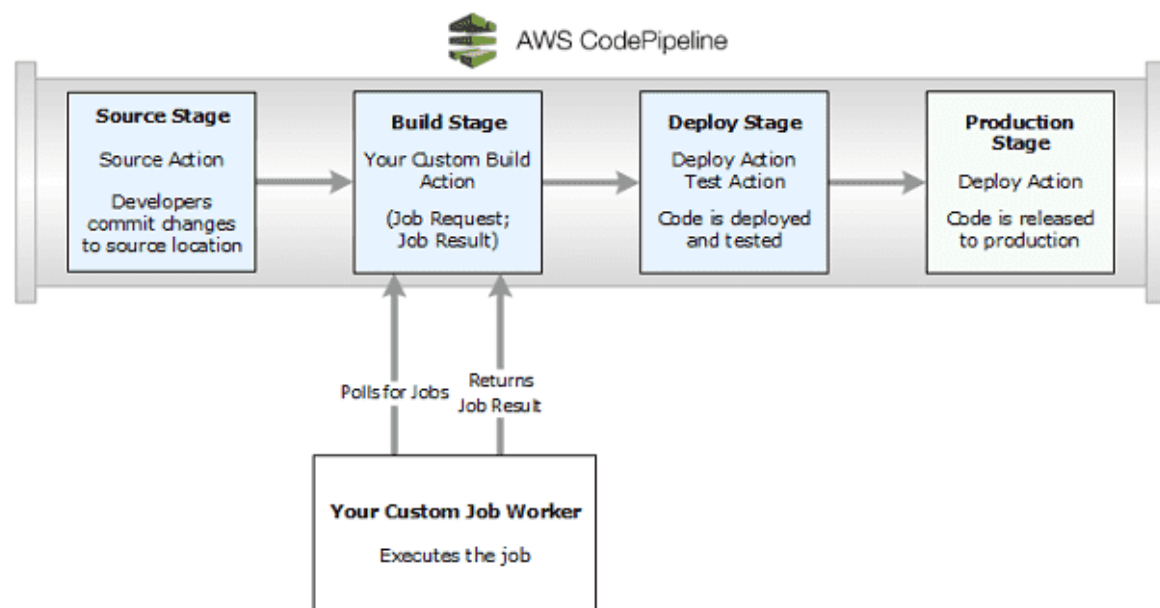
Lambda

インスタンスのスナップショット、コピー、復元に使用可能

CodePipeline

オンプレのソースコード分析ツールとやり取りして結果を返すことができるカスタムアクションを定義できる

速度向上させるには：runOrder属性を定義して、並行して実行できるシーケンスを指定する



CodeDeploy

CodeDeployの環境変数はログレベルの決定を行う環境を示すように構成できる

デプロイ設定としてCodeDeployDefault.HalfAtTimeを使用することでインスタンスの半分へのデプロイを制御し、デプロイを成功を確認してから続行できる。
Blue/Greenデプロイは新しいインスタンスでデプロイが実行される
デプロイ失敗時に自動的にロールバックを設定できる

Amazon CloudFront

単一のリージョンでホストすることで格納場所を特定できる
グローバルに最小限のレイテンシーでデータの配信が可能

S3

クロスリージョンレプリケーション

デフォルトではマルチAZで高可用だが、さらに遠く離れたリージョンにレプリケートしてデータを保護できる

静的Webホスティング

S3→Lambda@EdgeでHTTPレスポンスにセキュリティヘッダを追加する
配信にCloudFrontを使用

EC2 Systems Manager(SSM)

Amazon EC2 Run Command：既存のインスタンスでコマンドを発行してダウンタイムなしでパッチを適用したり、パッチが適用されたAMIに更新できる

サービスロール：EC2とSSMの統合に使う

SSMエージェント：オンプレ環境でのインスタンスの登録を許可する

「Amazon System Managerインベントリ」を使用してEC2やオンプレのコンピューティング環境の可視性を提供する(OSの種類やバージョン、インストールされたアプリケーション、ネットワーク構成図、EC2のAMI IDやAMIプロファイルなど)

SSM オートメーション：ソフトウェアをインストールしてAMIを事前に設定できる

AutoScaling

ライフサイクルフックを使うと一時的にインスタンスを保留にできるためトラブルシューティングに使える

Route53

加重ルーティング(A 20%,B 80%)は段階的なデプロイを実現することでBlue/Greenデプロイが可能になる

VPCフローログ

許可・拒否されたトラフィックの調査に役立つ

VPCエンドポイント

インターネットへのアクセスや接続なしでインスタンスをプライベートに保つのに役立つ

CloudFormation

パラメータとマッピングを使って動的、汎用的、かつ再利用的なデプロイが可能
マッピング：条件パラメータ値の指定に利用できる。キーと関連する値のマッピング。

クロススタック：他のスタックからの出力を参照して使用できる

変更セット：変更適用前にリソースに与える影響を確認できる

IAMアクセスアドバイザー

ユーザアクセスと最後にアクセスした情報に関する詳細なレポートを提供

Fn::ImportValueは同リージョンでエクスポートされた値をインポートできる。
Resourceセクションで利用

AWS Application Discovery Service

サーバの仕様、パフォーマンスデータ、実行中のプロセス、ネットワークの詳細情報が収集される

AWS X-Rayデーモン

アプリケーションをインストールし

X-Rayデーモンを有効化することでデータを公開できる

→これによって問題を診断するためのトレースデータをRDSなどから収集できる

Amazon Kinesis Data Streams

ログのリアルタイム分析

保持期間が1d~7dのため、7日間のログを分析できる

DynamoDB

グローバルテーブル：リージョン間でデータが複製され、1つのリージョンで障害が発生してももう1つのリージョンでデータの保護が可能

AWS Service Catlog

CloudFormationテンプレートを使用してプロビジョニングされた製品を作成するのに使用したり、運用上の負担を軽減できる

カスタムAMI

フレームワークがインストールされたカスタムAMIを作成することでフレームワークのインストール速度向上が期待できる

例：ユーザデータを使用してインストールしている→インストール済みのカスタムAMIを使用する

Secrets Manager

データベースの認証情報やAPIキーなどのシークレットを容易にローテーション、管理、取得できるようになっている

Trusted Advisor

AWS環境をモニタリングし、コスト、パフォーマンス、セキュリティ、フォールトトレランスの観点から、AWSのベストプラクティスと比較して、改善の

提案をしてくれるサービス

ECS

ECSにはアクセスログ機能がない

awslogsドライバーを使用してコンテナログをCloudWatchLogsに直接送信する

DynamoDB

DynamoDBAccelerator：DynamoDBのキャッシュ機能を提供する

DynamoDBストリーム：DynamoDBに加えられた情報を別のリソースにストリーミングしてログに書き込める

ElastiCache

RDSとともに使われるキャッシュ機能

Elastic beanstalk

GoイメージのDockerを作成→Gitをインストールしてアプリケーションを渡す
→Elastic beanstalkでデプロイ

OpsWorks

ChefやPuppetを使って運用を自動化するサービス

EC2インスタンスやオンプレの環境でのサーバ設定やデプロイ、管理を自動化できる

スタック：全インスタンスの構成を管理する

レイヤー：インストールするパッケージを選択する

App：アプリケーションサーバにデプロイされるもの

サーバレスアプリケーション

ELBは必要ない

API Gateway

Canaryリリース：新しいAPIバージョンのテストデプロイに使用できる。本稼働リリースとテスト(Canary)リリースに割合を分散できる

Cloudtrail

ログはアカウント関わらず単一のs3バケットに配信できる
AWSへのアクセス情報のみを提供する

Data Pipeline

MySQLからDynamoDBへの移行の際などに使用
RDSからデータをエクスポートしてDynamoDBにインポートする

RDS Oracle

クロスリージョンリードレプリカをサポートしていないAmazon Kinesis Data Streams

ログのリアルタイム分析

保持期間が1d~7dのため、7日間のログを分析できる

DynamoDB

グローバルテーブル：リージョン間でデータが複製され、1つのリージョンで障害が発生してももう1つのリージョンでデータの保護が可能

AWS Service Catlog

CloudFormationテンプレートを使用してプロビジョニングされた製品を作成するのに使用したり、運用上の負担を軽減できる

カスタムAMI

フレームワークがインストールされたカスタムAMIを作成することでフレームワークのインストール速度向上が期待できる

例：ユーザデータを使用してインストールしている→インストール済みのカスタムAMIを使用する

Secrets Manager

データベースの認証情報やAPIキーなどのシークレットを容易にローテーション、管理、取得できるようになっている

Trusted Advisor

AWS環境をモニタリングし、コスト、パフォーマンス、セキュリティ、フォールトトレランスの観点から、AWSのベストプラクティスと比較して、改善の提案をしてくれるサービス

ECS

ECSにはアクセスログ機能がない

awslogsドライバーを使用してコンテナログをCloudWatchLogsに直接送信する

DynamoDB

DynamoDBAccelerator：DynamoDBのキャッシュ機能を提供する

DynamoDbストリーム：DynamoDBに加えられた情報を別のリソースにストリーミングしてログに書き込める

ElastiCache

RDSとともに使われるキャッシュ機能

Elastic beanstalk

GoイメージのDockerを作成→Gitをインストールしてアプリケーションを渡す
→Elastic beanstalkでデプロイ

OpsWorks

ChefやPuppetを使って運用を自動化するサービス

EC2インスタンスやオンプレの環境でのサーバ設定やデプロイ、管理を自動化できる

スタック：全インスタンスの構成を管理する

レイヤー：インストールするパッケージを選択する

App：アプリケーションサーバにデプロイされるもの

サーバレスアプリケーション

ELBは必要ない

API Gateway

Canaryリリース：新しいAPIバージョンのテストデプロイに使用できる。本稼働リリースとテスト(Canary)リリースに割合を分散できる

Cloudtrail

ログはアカウント関わらず単一のs3バケットに配信できる

AWSへのアクセス情報のみを提供する

Data Pipeline

MySQLからDynamoDBへの移行の際などに使用

RDSからデータをエクスポートしてDynamoDBにインポートする

RDS Oracle

クロスリージョンリードレプリカをサポートしていない

CFnとOpsWorksはDockerをホストできない

TrustedAdvisor

リソースの作成上限に近づいたときにアラームするときに役立つ機能

Amazon Artifact

AWSのコンプライアンスやセキュリティドキュメントを提供するサービス

Amazon EMR

ビッグデータ処理・分析用リソース

Immutable

最小限のダウンタイム

BrueGreenデプロイと違うところはDNSがかわるかどうか

→ URLスワップ、CNAME入れ替えなどがImmutableでは発生しない

Amazon GuardDuty

IAMアクセス情報の漏洩などのセキュリティサービス

Amazon Macie

データの機密性や個人情報の保護に焦点をあてたセキュリティサービス

ElasticBeanStalk

デプロイ後、元のインスタンスを終了させることはできない

→ CodeDeployのオプションを使用する

ebextentionの設定ファイルでMeasureNameに設定した値をトリガーにスケーリングできる

Amazon X-Ray

Amazon X-Rayは、アプリケーションのバグやパフォーマンスの問題を特定することができる。特に、マイクロサービスのモニタリングが複雑な場合でも、マップで可視化してトレースで分析することができる

CloudWatchLogs

CloudWatchLogsサブスクリプションフィルターが連携できるサービス

→ AmazonKinesis,KinesisDataFirehose,Lambda

CodeDeployでデプロイが失敗し、特定のイベントがスキップされて終了する

→ インスタンスに権限がないorネットワーク設定がおかしい

S3TransferAcceleration

→ アプリケーションを介さずクライアントがS3に直接データを書き込める

OpsWorks

→ クックブックはS3からコードを引っ張ってくる

AmazonInspector

脆弱性を検出するために使用できる

Amazon CloudSearch

ウェブサイトまたはアプリケーション向けの検索ソリューションを容易かつコスト効率良く設定、管理、スケールできる

ElasticBeanStalk

DockerコンテナをElasticBeanStalkを使ってデプロイする流れをおぼえる

オンプレからのアクセスにはSSMエージェントを使用する

CFnのカスタムリソースにはSNSを利用して連携できる