

運用上の優秀性

Operational Excellence : 運用上の優秀性

運用の優秀性とは計画変更が起こった場合や予期せぬイベントの発生時において、自動化された運用実務及び文書化されテストされレビューされた手順があること

- ✓ コード化された運用実行（環境自動化）
- ✓ ビジネス目的に沿った運用手順
- ✓ 定期的かつ小規模で増加的な変更管理
- ✓ 予期せぬイベントへの対応テストの実施
- ✓ モニタリングにより障害を予測する
- ✓ 運用上の失敗やイベントから学習する
- ✓ 運用手順を繰り返しアップデートする

運用上の優秀性の主要サービス

準備	Cloud Formation Code シリーズ Runbook Playbook
運用	System Manager Service Catalog CloudTrail AWS Artifact AWS GuardDuty Cloud Watch AWS Config API Gateway
進化	継続的かつ段階的な改善のために時間とリソースを割り当て、運用の有効性と効率性を向上させる

CloudWatch

AWSリソースとAWSで実行するアプリケーションのモニタリングサービスで、様々なログやメトリクスを監視できる

CloudWatch

AWS上で稼働するシステム監視サービスで、死活監視、性能監視、キャパシティ監視を実施
有料枠では確認内容や設定の柔軟性が充実化する

CloudWatch Logs

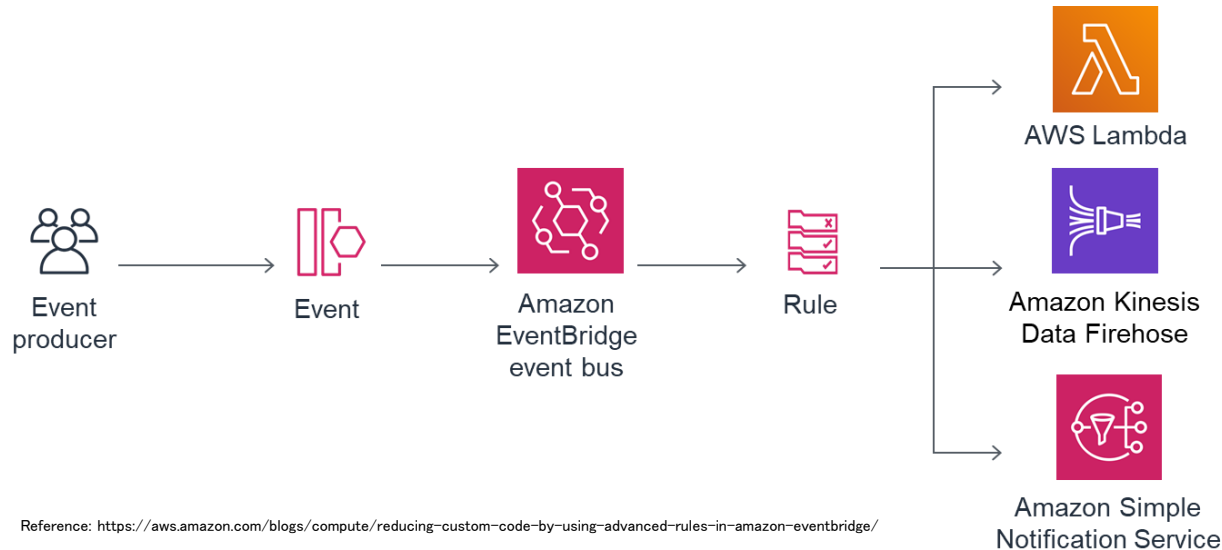
CloudWatchと連動したログ管理プラットフォームサービス。EC2上のOS・アプリケーションのログやAWSマネージドサービスのログを取得する

CloudWatch Events

CloudWatchはAWSリソースに対するイベントをトリガーにアクションを実行。オペレーションの変更に応答し、応答メッセージ送信、機能のアクティブ化。変更、状態情報収集による修正アクションを実行する

Amazon EventBridge

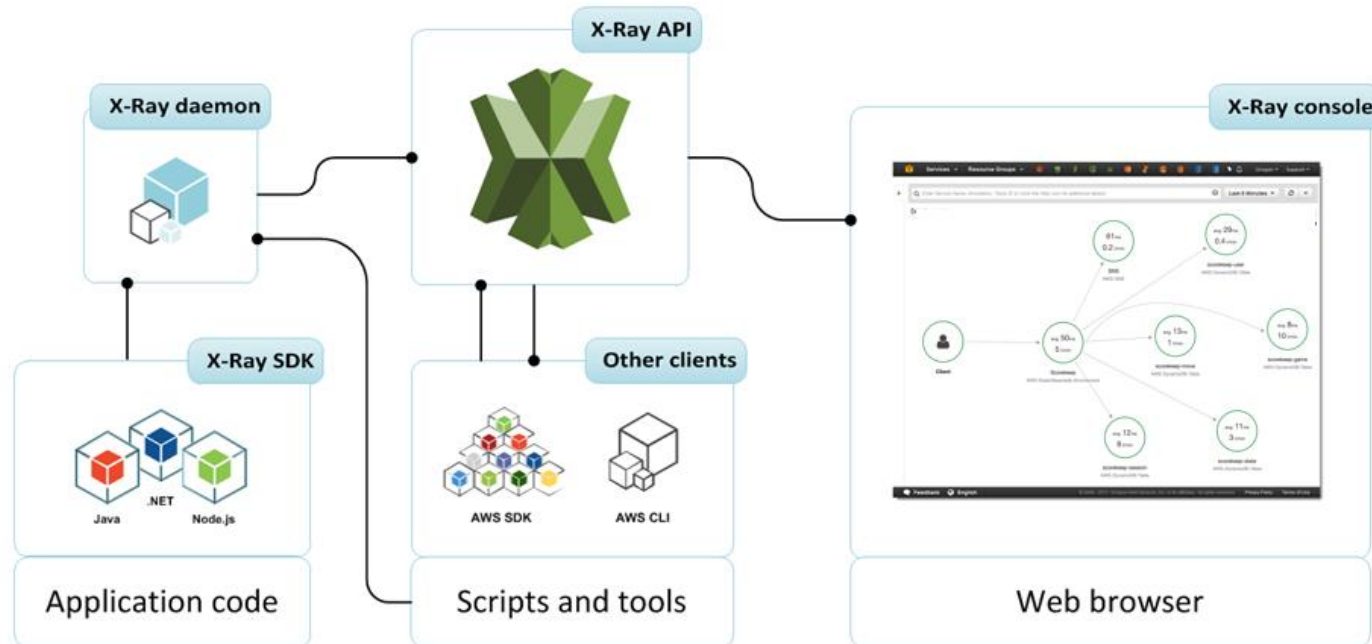
AWSサービスやアプリケーションに連携するイベント駆動型アプリケーションを大規模に構築するサービス



- ✓ CloudWatchイベントの進化版
- ✓ イベント駆動型のアプリケーションを容易に作成するサービス
- ✓ EventBridge Pipesにより、追加のコードなしにイベントプロデューサーとイベントコンシューマーを統合するイベントフローを作成する。
- ✓ EventBridge スケジューラにより、何百万ものイベントやタスクを1つのソースから作成、起動、管理する。
- ✓ スキーマレジストリにより、イベントのスキーマを自動的に検出格納し、簡単に検索してアクセスできるようになる。

AWS X-ray

AWS X-Ray はアプリケーションのリクエストデータをトレースして、アプリケーションを解析するサービス



Reference: https://docs.aws.amazon.com/ja_jp/xray/latest/devguide/aws-xray.html

- ✓ 分散アプリケーションやサーバレスアプリケーションのデバックと改善を支援
- ✓ ボトルネックを特定し、高レイテンシが発生している場所を特定して、アプリケーションのパフォーマンスを向上させる。
- ✓ ペイロード、関数、トレース、サービス、API などのビジュアルデータをノーコードおよびローコードモーションでフィルタリングして可視化する。
- ✓ 根本原因を分析するために、さまざまな条件でトレースセットを比較できる

















AWS Systems Manager

利用中のAWSサービスやリソースをモニタリングして、運用タスクを自動化する統合監視サービス

問題検出の時間短縮	EC2などをリソースグループごとに運用データを確認できるため、アプリケーションに影響を与えるリソースの問題をすばやく特定可能
運用の自動化	EC2のパッチ、更新、設定変更・削除・停止およびデプロイなどを自動化
可視化と制御	各リソースグループの最新状態を簡単に可視化して制御できる
ハイブリッド管理	AWSサーバーとオンプレミスのサーバーとを1つのインターフェイスで管理可能

AWS Personal Health Dashboard

AWS のサービス状態のパーソナライズされた状況をダッシュボード形式で確認できる。

Current Status	Details	RSS
 Amazon Elastic Compute Cloud (API)	Service is operating normally.	
 Amazon Elastic Compute Cloud (Instances)	Service is operating normally.	
 Amazon Flexible Payments Service	Service is operating normally.	
 Amazon Mechanical Turk (Requester)	Service is operating normally.	
 Amazon Mechanical Turk (Worker)	Service is operating normally.	
 Amazon SimpleDB	Service is operating normally.	
 Amazon Simple Storage Service (EU)	Service is operating normally.	
 Amazon Simple Storage Service (US)	Service is operating normally.	
 Amazon Simple Queue Service	Service is operating normally.	

AWS Config

AWSリソースのレポジトリ情報からリソース変更履歴や構成変更を管理するサービス

- AWSリソースの構成変更をロギングして保存する
(30日から7年)
- 履歴も定期的に構成情報スナップショットとして取得し、
S3に保存
- 構成情報に基づきシステム構成があるべき状態になっているかを評価
- 評価基準にはAWSルールまたは独自ルールを適用

AWS Config

AWS Configには構成変更を管理するストリームと履歴管理するヒストリーと構成要素を保存するスナップショットがある

Configuration Stream	Configuration History	Configuration Snapshot
<ul style="list-style-type: none">□ リソースが作成・変更・削除に対して作成され、構成ストリームに追加される□ SNSトピック連携して通知設定が可能	<ul style="list-style-type: none">□ 任意の期間における各リソースタイプの構成要素を履歴として蓄積□ S3バケットに保存	<ul style="list-style-type: none">□ ある時点での構成要素の集合□ 自動で定期的あるいは変更トリガーで作成□ S3バケットに保存

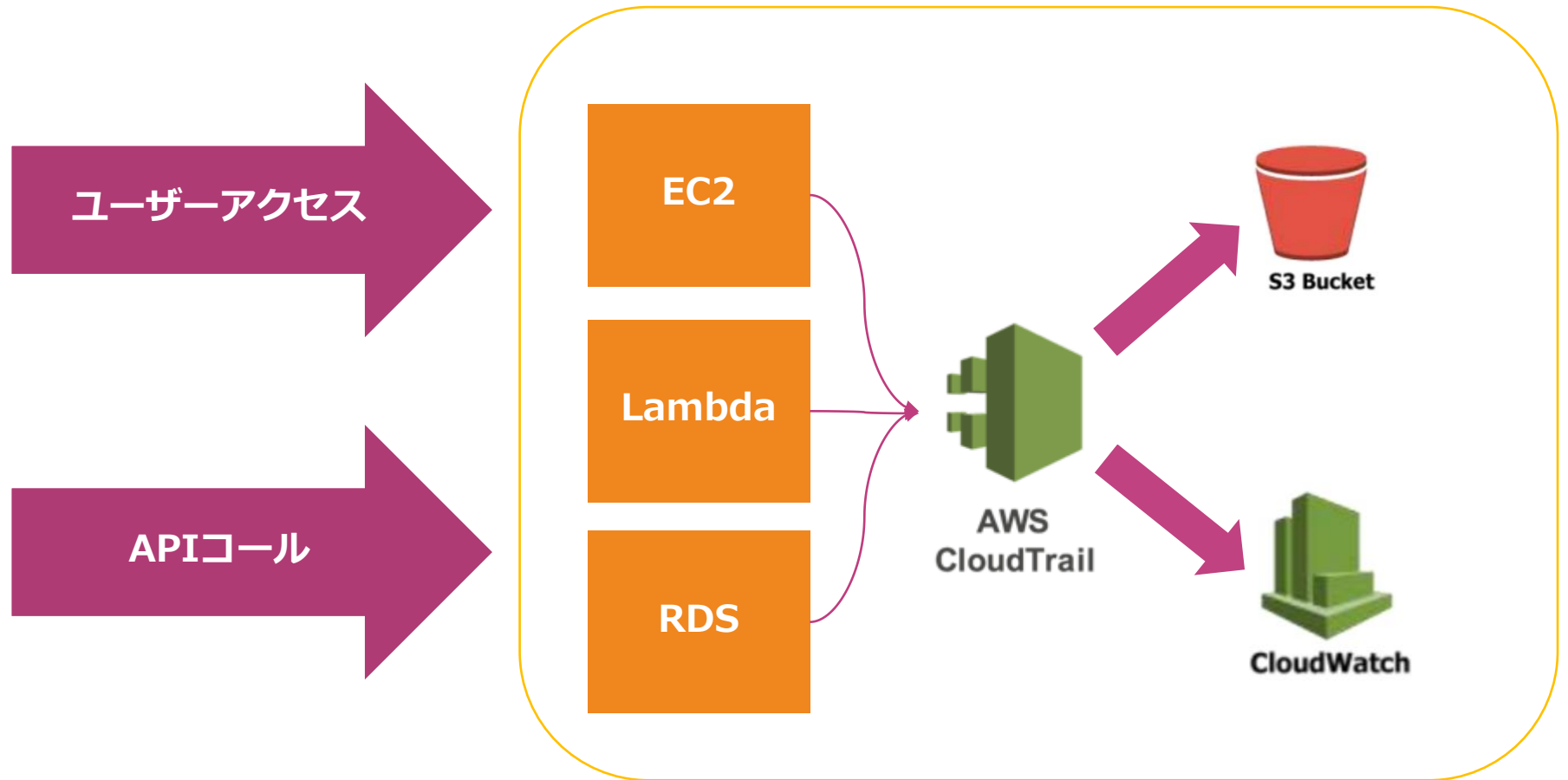
AWS CloudTrail

AWSユーザの操作（API操作やユーザのサインインアクティビティ）をロギングするサービス

- ❑ ルートアカウント／IAMユーザのオペレーションをトラッキングしてログを取得するサービス
- ❑ CloudTrail ログファイルは暗号化されてS3に保存
- ❑ KMSによる暗号化もサポート
- ❑ 無料

AWS CloudTrail

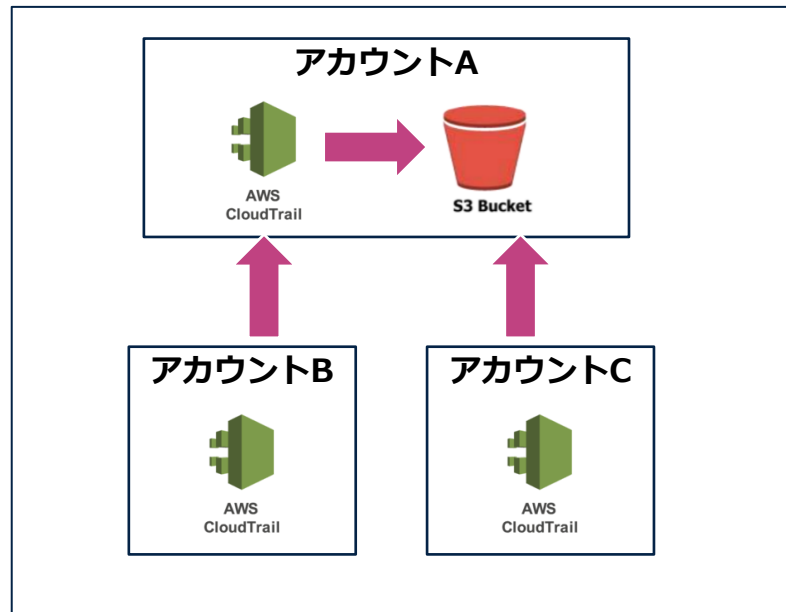
ユーザーアクセスとAPIコールのログ情報をS3バケットに保存し、CloudWatch上で解析できる。



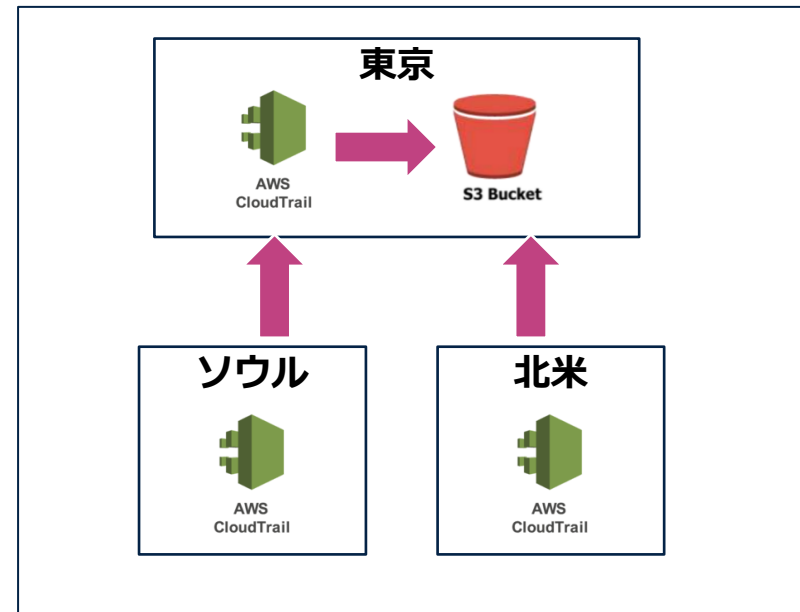
AWS CloudTrail

マルチアカウントで利用可能で、複数AWSアカウントの情報を集約可能

マルチアカウント

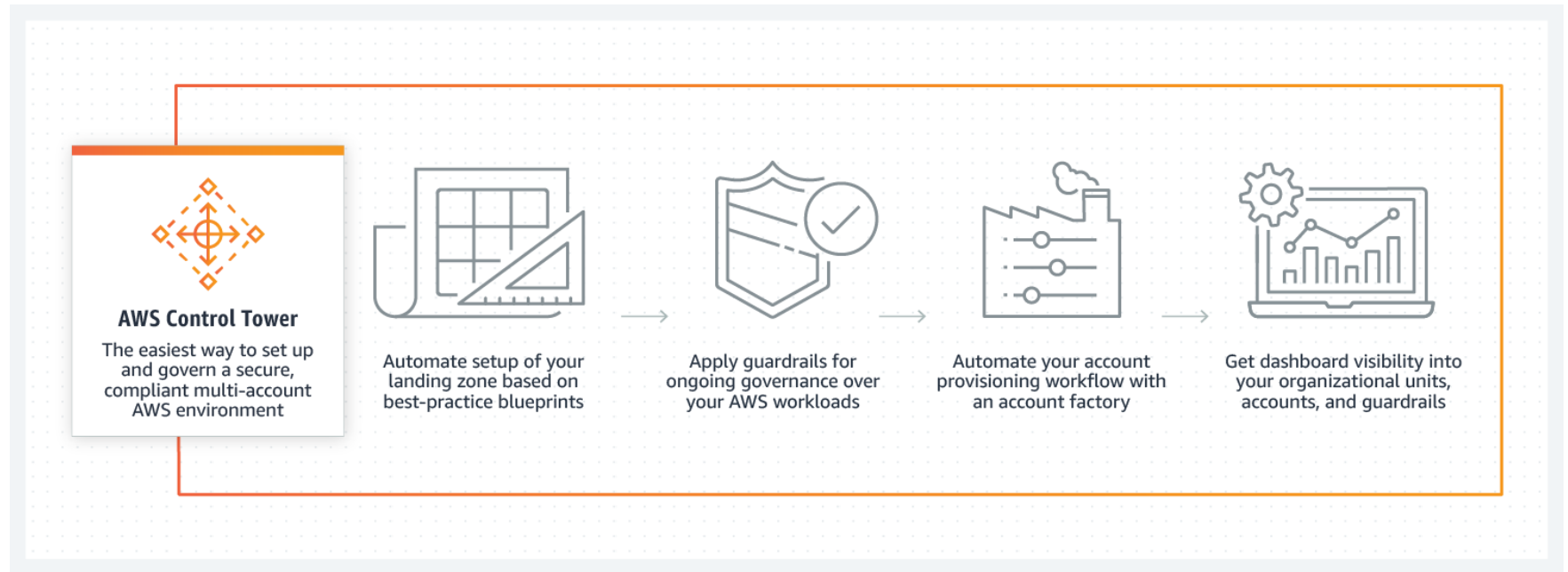


マルチリージョン



AWS Control Tower

ベストプラクティスに基づき安全性と適合性を備えた、複数アカウントの AWS 環境を設定および管理するサービス



AWS Service Catalog

AWSで承認されたITサービスのカタログを作成および管理する
支援サービス

IT運用管理者

CloudFormationのテンプレートを利用して、管理されるAWSリソース定義や、これらの利用権限をカタログとして一元管理する機能を提供

ユーザ部門

IT運用管理者が作成したカタログより、権限がなくとも求める機能に応じたAWS環境を必要に応じて起動が可能になる

AWS License Manager

ソフトウェアベンダーからのソフトウェアライセンスを簡単に管理するサービス

- ライセンスの利用数やライセンスの利用条件を登録
- ライセンスの利用状況を追跡して管理することが可能
- コンプライアンス違反などのライセンスルールに反する利用状況を可視化する。
- 既存ライセンスを自動検出するなどの一元的な管理を実現
- ダッシュボードを利用して可視化して、管理可能

AWS Artifact

重要なコンプライアンス関連情報の頼りになる一元管理型のリソース

AWS Artifact Reports

世界各地にある監査機関の指定する基準や規制を遵守状況をテストおよび確認したコンプライアンスレポートを提供

AWS Artifact Agreements

AWSアカウントとの契約の確認・受諾・管理を実施

AWS Trusted Advisor

コスト最適化とセキュリティと対障害性とパフォーマンス向上
についてアドバイスを提供するサービス

Cost Optimization



0  9  0 

\$7,516.85

Potential monthly savings

Performance



3  7  0 

Security



2  4  11 

Fault Tolerance



0  15  5 

Service Limits



37  0  1 

AWSサポート

AWSによる人的なオペレーターによる問い合わせや不具合サポートプラン

	ベーシック	開発者	ビジネス	エンタープライズ On-Ramp	エンタープライズ
ケース		各種サービスをお試しの方、テスト環境向け	本番環境のワークロード向け	プロダクション・ビジネスクリティカルなワークロード向け	ビジネスおよび/またはミッションクリティカルなワークロード向け
事前対応型支援・トレーニング	なし	サポートオートメーションワークフロー（SAWF）の利用	SAWFの利用。追加料金でインフラストラクチャイベント管理を利用	SAWFの利用。インフラストラクチャイベント管理を利用	SAWFの利用。インフラストラクチャイベント管理/事前対応型の評価、ワークショップ、ディープダイブ/トレーニングラボの利用
アカウント支援	-			コンシェルジュサポート	
Trusted Advisor	ベーシックチェックのみ		全項目チェックの利用		
技術サポートへのアクセス	サポート画面からの問い合わせ	メール対応（平日9時～18時）	電話／チャット／メール（24時間365日）、ライブ共有画面	ビジネスの内容に加えて、プロアクティブなガイダンス提供、TAMプールの利用/ Well-Architected対応支援	ビジネスの内容に加えて、TAMが環境を事前に監視して支援／Well-Architected対応支援
技術サポート対応ユーザー数		1	無制限	無制限	無制限
緊急度／初回応答時間		システム障害に対して12時間以内	本番システムのダウンに最短1時間以内	ビジネスクリティカルなシステムのダウンに最短30分以内	ビジネスクリティカルなシステムのダウンに最短15分以内

CloudWatchの概要

CloudWatch

AWSリソースとAWSで実行するアプリケーションのモニタリングサービスで、様々なログやメトリクスを監視できる

モニタリング

監視の集約化

トラブル
シューティング

ログ解析

自動アクション

運用状況の確認

CloudWatchの機能

AWSリソースとAWSで実行するアプリケーションのモニタリングサービスで、様々なログやメトリクスを監視できる

CloudWatch アラーム

CloudWatch メトリクスに基づく数式の結果を監視するメトリクスアラームを作成する。また、他のアラームのアラーム状態を考慮したルール式が含まれる複合アラームが作成できる。

CloudWatch メトリクス

EC2などのAWSリソースの監視サービスであり、死活監視、性能監視、キャパシティ監視を実施する。
有料枠では確認内容や設定の柔軟性が充実化する

CloudWatch Logs

CloudWatchと連動したログを収集・可視化する機能。
EC2上のOS・アプリケーションのログやAWSマネージドサービスのログを取得する

CloudWatch Events →Amazon Event Bridgeに統合

CloudWatchはAWSリソースに対するイベントをトリガーにアクションを実行する。オペレーションの変更に応答し、応答メッセージ送信、機能のアクティブなどを実施する。

CloudWatchの機能

AWSリソースとAWSで実行するアプリケーションのモニタリングサービスで、様々なログやメトリクスを監視できる

X-Rayトレース

AWS X-Rayはアプリケーションが処理するリクエストに関するデータを収集するサービス。X-RayトレースではX-RayのデータをCloudWatch上で可視化する。

CloudWatch アプリケーション モニタリング

CloudWatch ServiceLensやRUMを利用して、アプリケーションのヘルスのモニタリングを実施する

CloudWatch インサイト

Insights を使用して、Lambda関数、Logs、Containerアプリケーションなどのメトリクスとログを収集、集計、要約する。

CloudWatchアプリケーションモニタリング

CloudWatch ServiceLensとRUMを利用してアプリケーションのモニタリングを実施する。

CloudWatch ServiceLens

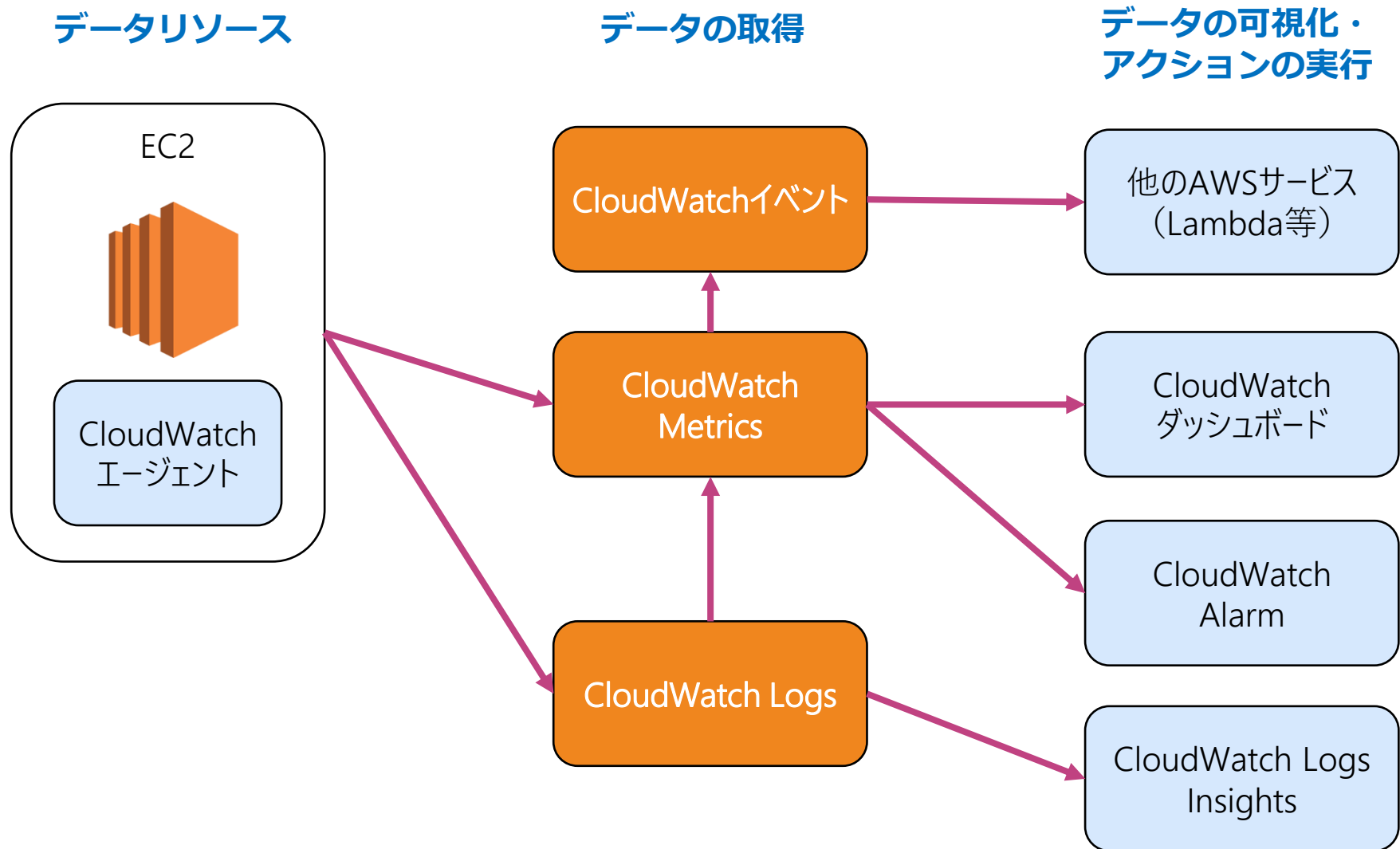
AWS X-Rayと統合して、トレース、メトリクス、ログ、アラーム、および他のリソースヘルス情報を 1 か所に統合して、サービスとアプリケーションの監視性する。
サービスマップには、サービスエンドポイントとリソースの各ノードとその接続のトラフィック、レイテンシー、およびエラーがハイライトされる。

CloudWatch RUM

リアルユーザーモニタリング (RUM)はアプリケーションの信頼性、パフォーマンス、エンドユーザー満足度を可視化する。アプリケーションにスニペットをインストールすることで、ユーザーがアプリケーションの各ページにアクセスする際に統合と分析のためにデータを RUM に送信する。

CloudWatch

データを取得・表示・アクションの実行までを集中管理



CloudWatch

CloudWatchメトリクスを利用して、多くのメトリクスを取得することが可能

標準メトリクス

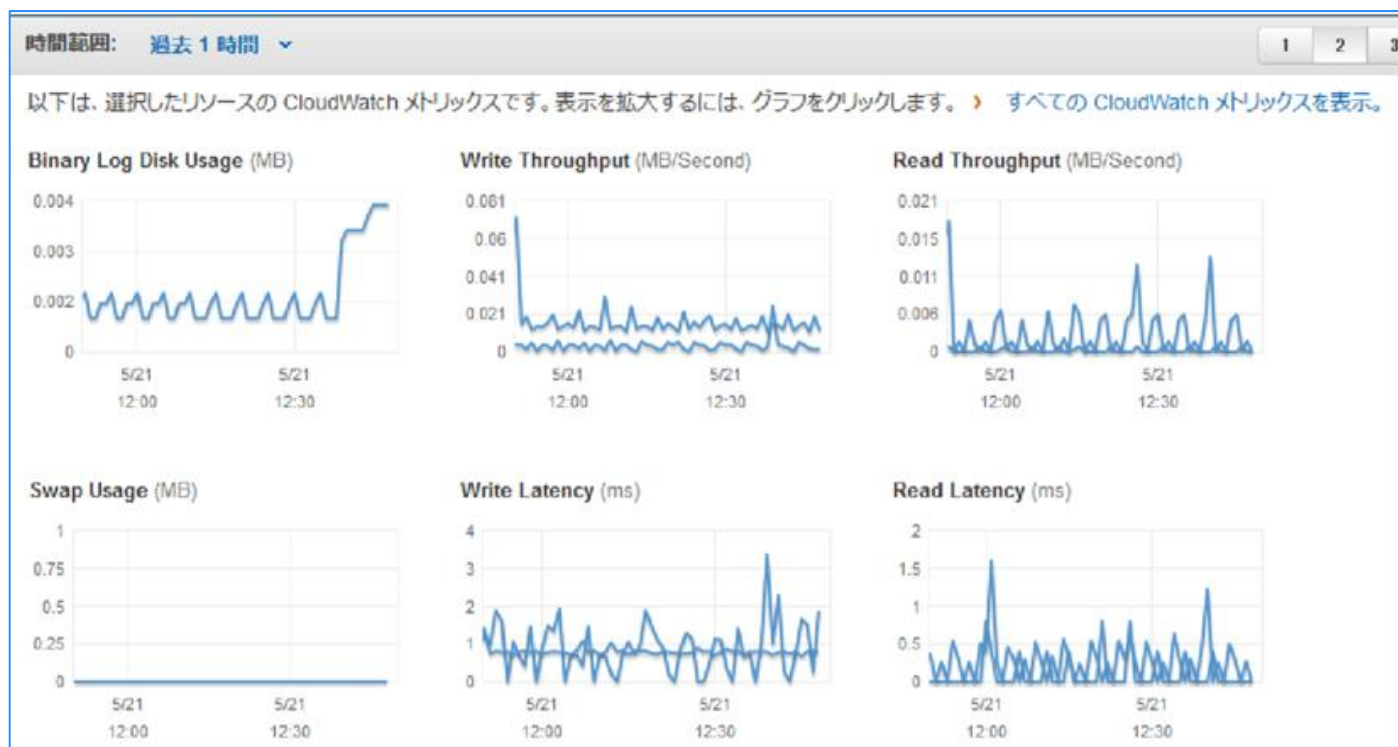
- CPUUtilization／ディスク利用率／読み込みIOPSなど 一般的なメトリクスの多くが取得可能
- 5分間隔でのメトリクス取得

カスタムメトリクス

- 標準では取得できないメトリクス
- 高解像度で1秒から60秒のリアルタイムでのメトリクス取得

CloudWatchダッシュボード

必要なRDSのメトリクスを選択してダッシュボードで可視化することが可能



拡張モニタリングの実施

DB インスタンスが実行されているオペレーティングシステム (OS) のリアルタイムのメトリクスを取得できる。

- ✓ 50種類以上のOSメトリクスを利用可能
- ✓ 1秒から60秒間隔でメトリクスを取得可能（標準は5分）
- ✓ 取得したメトリクスはCloudWatch Logs に保存される。
- ✓ 料金は、Amazon CloudWatch Logs に示された無料利用枠を超えた拡張モニタリングに対してのみ発生
- ✓ 拡張モニタリングはdb.m1.small を除くすべての DB インスタンスクラスに使用できます。
- ✓ APIコール時のスロットリング対策

CloudWatchアラーム

CloudWatchアラームにより、特定のメトリクスのしきい値に応じたアラーム通知や自動アクションを実行可能

メトリクス	CloudWatchに発行された時系列のデータポイントをセットのこと リージョンごとのメトリクスを取得
名前空間	CloudWatchメトリクスのコンテナのこと 異なる名前空間のメトリクスは相互に分離される。
ディメンション	メトリクスを一意に識別する名前／値のペア (例 : Instanceid = i-123948576)

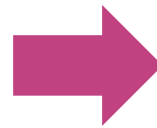
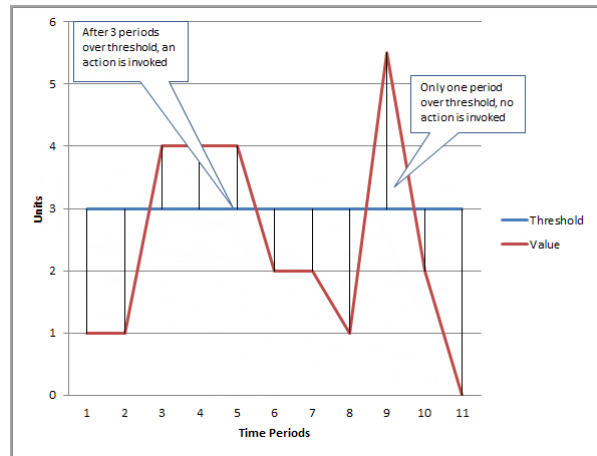
CloudWatchアラーム

CloudWatchアラームにより、特定のメトリクスのしきい値に応じたアラーム通知や自動アクションを実行可能

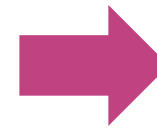
正常値 OK	定義されたしきい値を下回っている。
異常値 ALARM	定義されたしきい値を上回っている。
判定不能 INSUFFICIENT _DATA	データ不足のため状態を判定できない。 CloudWatch特有の状態

CloudWatchアラーム

モニタリング値を閾値にアラームを設定して、担当者に周知することが可能



Amazon
SNS



メール
通知

CloudWatch logs

CloudWatch Logsはログを管理しつつ、可視化・分析を実施できるサービスで、RDSのログに対応している。

- ✓ AWSサービスのログの保存して、可視化・分析する仕組みを提供
- ✓ EC2インスタンスの場合はエージェント経由でログメッセージをCloudWatchエンドポイントに転送する
- ✓ ログデータは1日から永久に保存期間を設定可能
- ✓ Amazon S3にログデータをエクスポートできる。
- ✓ サブスク립ションフィルタによってログのフィルタリングパターンによって、リアルタイムにKinesisやLambdaにログを送付するアクションを実施

CloudWatch logs

CloudWatch Logsはロググループ>ログストリーム>ログイベントという3つのレイヤーで構成されている。

ロググループ

- ログを保存・管理するための設定を共有するグループの定義
- 複数のログストリームで構成される。

ログストリーム

- モニタリングしているリソースのタイムスタンプ順でイベントを表す。
- 複数のログイベントで構成される。

ログイベント

- モニタリングしているリソースによって記録されたアクティビティレコード
- イベント発生時のタイムスタンプとイベントメッセージによって構成

CloudWatch logs Insights

CloudWatch Logs Insightsはログデータをインタラクティブに検索して分析

- ✓ クエリによってログを可視化・分析することが可能
- ✓ 3つのフィールドを生成
 - ✓ @message: 生の未解決のログイベント
 - ✓ @timestamp: ログイベントがCloudWatch Logsに追加された時間
 - ✓ @logStream: ログイベントの追加先のログストリームの名前
- ✓ 時間軸に沿ってトレンドやパターンを可視化することが可能
- ✓ 可視化されたグラフをダッシュボードに追加可能

CloudWatch Logsとの連携

AWS上のリソースの変更を示すシステムイベントをトリガーとして、ターゲットがイベントを処理する。

