

これで完璧、AWSの運用監視

初心者向けWebinarシリーズ

アマゾン ウェブ サービス ジャパン株式会社
パートナー ソリューション アーキテクト
酒徳 知明

2015.12.25

自己紹介

酒徳 知明(さかとく ともあき)

エコシステム ソリューション部

パートナー ソリューション アーキテクト

- エンタープライズ SIパートナー様のご支援
- ISVパートナー様のご支援

好きなAWSサービス

- 運用監視系サービス

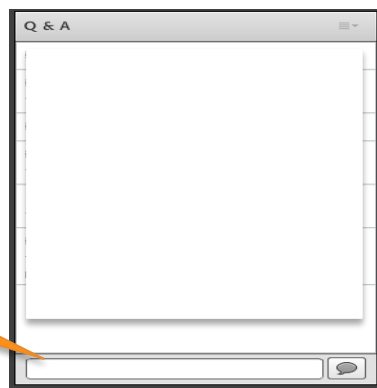


ご質問を受け付け致します！

📦 質問を投稿することができます！

- Adobe Connectのチャット機能を使って、質問を書き込んでください。（書き込んだ質問は、主催者にしか見えません）
- Webinarの最後に、可能な限り回答させていただきます。
- 終了時刻となった際は、割愛させていただく場合がございます。

①画面右下のチャットボックスに質問を書き込んでください



②吹き出しマークで送信してください

初心者向けWebinarのご紹介

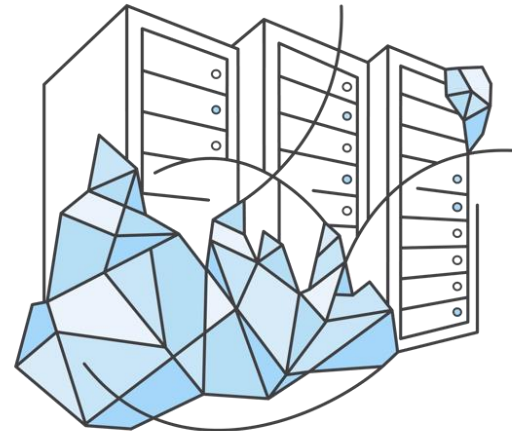
- AWSについてこれから学ぶ方向けのWebinarです。
- 過去のWebinar資料
 - AWSクラウドサービス活用資料集ページにて公開
<http://aws.amazon.com/jp/aws-jp-introduction/>
- イベントの告知
 - 国内のイベント・セミナースケジュールページにて告知
<http://aws.amazon.com/jp/about-aws/events/>
(オンラインセミナー枠)

Introduction

- 今回のAWS初心者向けWebinarでは、AWS上に構築されたシステムの運用監視についてご紹介します。
- 運用監視に必要なとなるAWSサービスを中心に基本設定方法含めみていきます。

AWSの運用監視

- 今までのシステム監視と然程変わらない
 - オンプレミス時の運用ノウハウを最大限活用
 - AWSサービスをうまく活用したシンプルな監視
 - 多くの監視ツールがAWSに対応
- クラウドならではの運用監視
 - コスト監視
 - AWSマネジドサービスの監視
 - 運用軽減を手伝うAWSサービス

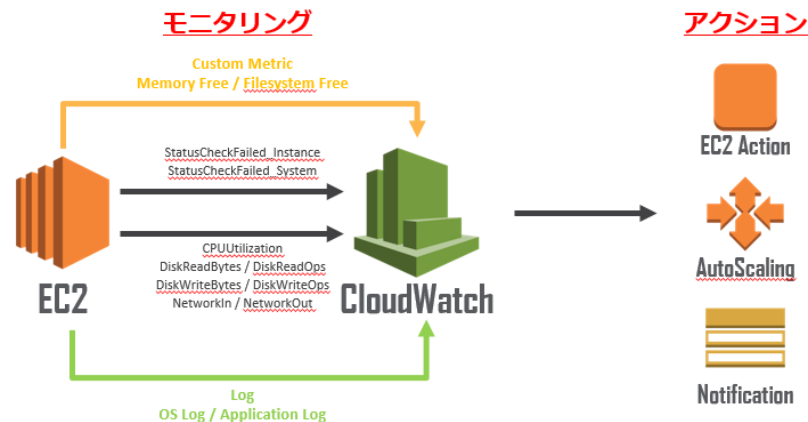


Q. AWSの監視はどうすればいい？

Amazon CloudWatchとは



- AWSの各種リソースを監視する マネージドサービス
 - AWSリソースの死活、性能、キャパシティ
 - 取得メトリックスのグラフ化 (可視化)
 - 各メトリックスをベースとしたアラーム(通知)、アクションの設定が可能
- 多くのAWSサービスの監視が可能
 - Amazon EC2
 - Amazon EBS
 - Amazon RDS
 - Elastic Load Balancing など



Amazon EC2のモニタリングタイプ

基本モニタリング

無料

**データは5分間隔で
自動的に取得**

詳細モニタリング

追加料金が必要

**データは1分間隔
で取得可能**

Amazon CloudWatchのメトリックス (EC2)

標準メトリックス

CPUUtilization
CPUCreditBalance
CPUCreditUsage
DiskReadBytes
DiskWriteBytes
DiskWriteOps
NetworkOut
NetworkIn
StatusCheckFailed_Instance
StatusCheckFailed
StatusCheckFailed_System

カスタムメトリックス

標準メトリックスでは
取得できないメトリックス



Amazon CloudWatch カスタムメトリックス

- 標準メトリックス以外の独自メトリックスも監視可能
 - AWS CLIの“put-metric-data”、API Toolsの“mon-put-data”、もしくは“PutMetricData” APIでデータを登録
 - サイズ制限として、HTTP GETは8KB、HTTP POSTは40KB、1つのPutMetricDataリクエストに20データ

```
$ aws cloudwatch put-metric-data --metric-name RequestLatency\  
  --namespace "GetStarted"\  
  --timestamp 2014-10-28T12:30:00\  
  --value 87 \  
  --unit Milliseconds\  

```

```
$ aws cloudwatch put-metric-data --metric-name RequestLatency¥  
  --namespace "GetStarted"¥  
  --timestamp 2014-10-28T12:30:00\  
  --statistic-value Sum=60,Minimum=15,Maximum=105,SampleCount=5
```

CloudWatchのメトリックス値

- CloudWatchで取得される情報は統計情報
 - メトリックスデータを指定した期間で集約したもの
 - それぞれのメトリックスについて適切な統計情報を見る必要がある

統計	説明
Minimum	指定された期間に認められた最小値です。この値を用いて、アプリケーションの低ボリュームのアクティビティを判断できます。
Maximum	指定された期間に認められた最大値です。この値を用いて、アプリケーションの高ボリュームのアクティビティを判断できます。
Sum	該当するメトリックスで加算されたすべての合計値です。この統計は、メトリックスの合計ボリュームを判断するのに役立ちます。
Average	指定した期間の Sum/SampleCount の値です。この統計を Minimum および Maximum と比較することで、メトリックスの全容、および平均使用量がどれくらい Minimum と Maximum に近いかを判断できます。この比較は、必要に応じてリソースを増減させるべきかを知るのに役立ちます。
SampleCount	統計計算で使用するデータポイントのカウント(数)です。

- メトリックスデータの保管は2週間まで
 - 2週間以上保存する場合は、get-metric-statisticsでデータを取得し別の場所に保管しておく
- データ保管粒度は最短で1分間隔
 - 多くのサービスで1分間隔、5分間隔のものもある

http://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

CloudWatch の始め方

アマゾン ウェブ サービス

コンピューティング

- EC2
クラウド内の仮想サーバー
- Lambda
イベント発生時にコードを実行
- EC2 Container Service
Docker コンテナの実行と管理

ストレージ & コンテンツ配信

- S3
スケーラブルなクラウドストレージ
- Storage Gateway
オンプレミス IT 環境とクラウドストレージの統合
- Glacier
クラウド内のアーカイブストレージ
- CloudFront
グローバルなコンテンツ配信ネットワーク

データベース

- RDS
マネージド型のリレーショナルデータベースサービス
- DynamoDB
予測可能でスケーラブルな NoSQL データストア
- ElastiCache
インメモリアリキャッシュ
- Redshift
マネージド型のペタバイトスケールのデータウェアハウスサービス

ネットワークング

管理およびセキュリティ

- Directory Service
クラウド上の管理型ディレクトリ
- Identity & Access Management
アクセスコントロールとキー管理
- Trusted Advisor
AWS クラウド最適化エキスパート
- CloudTrail
ユーザーアクティビティと変更の追跡
- Config
リソース設定およびイベントトリ
- CloudWatch
リソースとアプリケーションのモニタリング

デプロイ & マネジメント

- Elastic Beanstalk
AWS アプリケーションコンテナ
- OpsWorks
DevOps アプリケーション管理サービス
- CloudFormation
テンプレートによる AWS リソース作成
- CodeDeploy
自動デプロイ

分析

- Elastic MapReduce
マネージド型 Hadoop フレームワーク
- Kinesis
ビッグデータストリームのリアルタイム処理
- Data Pipeline

アプリケーションサービス

- SQS
メッセージキューサービス
- SWF
アプリケーションコンポーネントを連携させるワークフローサービス
- AppStream
低レイテンシーのアプリケーションストリーミング
- Elastic Transcoder
使いやすいスケーラブルなメディア変換サービス
- SES
E メール送信サービス
- CloudSearch
マネージド型検索サービス

モバイルサービス

- Cognito
ユーザー ID およびアプリケーションデータの同期
- Mobile Analytics
大規模なアプリケーションの使用状況データの把握
- SNS
プッシュ通知サービス

エンタープライズアプリケーション

- WorkSpaces
クラウド内のデスクトップ
- WorkDocs
セキュアなエンタープライズ向けストレージおよび共有サービス
- WorkMail プレビュー
サボリリテック保護された E メールとカレンダーサービス

リソースグループ

リソースグループは、1 つ以上のタグを共有するリソースのコレクションです。お客様のアカウントの各プロジェクトのグループ、アプリケーション、環境の作成

グループの作成

タグエディター

その他のリソース

はじめに

サービスを初めて使用する手順やさらに詳しい使用方法については、ドキュメントを参照してください。

AWS Console モバイルアプリ

Amazon アプリストア、Google Play、または iTunes から入手可能な AWS コンソールモバイルアプリを使用して、出先でリソースを表示します。

AWS Marketplace

ソフトウェアを検索して購入し、1-Click で起動し、時間単位で料金を支払えます。

AWS Summit - サンフランシスコ

詳細については、サンフランシスコで開催される AWS Summit で発表予定のエンジニアリングの新規リリースや機能をお

CloudWatch利用イメージ 標準メトリックス監視

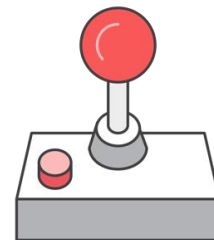
The screenshot displays the AWS CloudWatch console interface. At the top, the navigation bar includes 'AWS', 'サービス', 'EC2', 'CloudWatch', 'CloudTrail', 'Config', 'S3', and '編集'. On the left sidebar, the 'ダッシュボード' menu is expanded to show 'アラーム', 'アラーム 不足', 'OK', '請求', 'ログ', 'メトリックス', '選択されたメトリックス', '請求', 'DynamoDB', 'EBS', 'EC2', 'Lambda', 'Redshift', 'SNS', and 'SQS'. A 'カスタムメトリックス...' dropdown is also visible.

The main content area is titled 'EC2 インスタンス別メトリックス'. A search bar at the top of this section contains 'EC2' and 'i-cbe78721', highlighted with a red box and labeled '対象インスタンス検索ウィンドウ'. Below the search bar, a table lists metrics for the instance 'i-cbe78721'. The table has two columns: 'インスタンス ID (InstanceID)' and 'メトリックス名'. The 'メトリックス名' column is highlighted with a red box and labeled '標準メトリックス一覧'. The listed metrics are: CPUUtilization (CPUUtilization), DiskReadBytes (DiskReadBytes), DiskReadOps (DiskReadOps), DiskWriteBytes (DiskWriteBytes), DiskWriteOps (DiskWriteOps), NetworkIn (NetworkIn), NetworkOut (NetworkOut), StatusCheckFailed (StatusCheckFailed), StatusCheckFailed_Instance (StatusCheckFailed_Instance), and StatusCheckFailed_System (StatusCheckFailed_System).

Below the table, a line graph titled 'CPUUtilization (Percent)' is displayed. The graph shows CPU utilization over time, with the x-axis ranging from 13:00 on 4/27 to 00:00 on 4/28. The y-axis represents the percentage of CPU utilization, ranging from 5 to 30. The graph is labeled '平均' (Average) and '5 分間' (5 minutes). The left axis is labeled '左軸の単位: Percent'. A red box highlights the graph area, and a dashed orange box is present in the bottom right corner of the graph area.

On the right side of the graph, there are controls for 'グラフの更新' (Refresh graph), '時間範囲' (Time range), and '相対値' (Relative value) / '絶対値' (Absolute value) options. The '時間範囲' section includes '開始' (Start) and '終了' (End) time pickers, and a 'ズーム' (Zoom) dropdown.

Amazon CloudWatchを使った死活監視



- EC2の死活監視

- CloudWatch標準メトリックスを利用可能

- StatusCheckFailed System

- ハイパーバイザーレイヤから見た正常性確認
 - 最近 1 分間にインスタンスが EC2 システムステータスチェックに成功したかどうかを報告

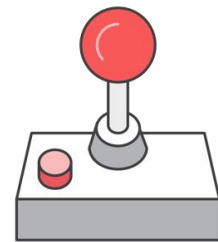
- StatusCheckFailed Instance

- OSレイヤの正常性確認
 - 最近 1 分間にインスタンスが EC2 インスタンスステータスチェックに成功したかどうかを報告

- StatusCheckFailed

- StatusCheckFailed Instance と StatusCheckFailed System の組み合わせで評価を行い、どちらかのステータスチェックが失敗したら報告
 - 1分間隔でモニタリング可能

Amazon EC2 Auto Recovery



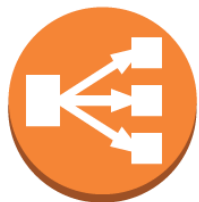
- EC2の自動復旧
 - EC2インスタンスが稼働しているAWSシステムに障害が発生した場合に、自動的にEC2インスタンス復旧する機能。
 - ネットワーク接続喪失
 - システム電源喪失
 - 物理ホストの障害
- 対応するインスタンスタイプ
 - C3, C4, M3, R3, T2インスタンス
- VPC内のインスタンス
 - EC2クラシックは未対応
 - ハードウェア専有インスタンスは未対応
- EBS-Backedインスタンスのみ



http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2-instance-recover.html

CloudWatchを使ったマネージドサービスの監視

• AWSマネージドサービスの監視



ELB

- Latency
- BackendConnectionErrors
- HealthyHostCount
- UnHealthyHostCount
- RequestCount
- HTTPCode_ELB_5XX
- HTTPCode_Backend_4XX



**Amazon
RDS**

- CPUUtilization
- FreeableMemory
- SwapUsage
- FreeStorageSpace
- DiskQueueDepth
- ReadIOPS
- ReadThroughput
- ReadLatency
- NetworkReceiveThroughput
- NetworkTransmitThroughput
- WriteIOPS
- WriteThroughput
- WriteLatency
- DatabaseConnections
- BinLogDiskUsage

http://docs.aws.amazon.com/ja_jp/ElasticLoadBalancing/latest/DeveloperGuide/US_MonitoringLoadBalancerWithCW.html

http://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/DeveloperGuide/rds-metricscollected.html

RDSの拡張モニタリング(MySQL 5.6, MariaDB, Aurora)

- CPU、メモリ、ファイルシステムやディスクI/Oなどの50を超えるメトリクスが取得可能
- 対応しているDB
 - MySQL 5.6
 - MariaDB
 - Aurora
- 拡張モニタリングのデータはCloudWatch Logsにパブリッシュ

New

Manage Graphs

CPU utilization <ul style="list-style-type: none"><input checked="" type="checkbox"/> User<input checked="" type="checkbox"/> Total<input type="checkbox"/> System<input type="checkbox"/> Guest<input type="checkbox"/> IRQ<input type="checkbox"/> Wait<input type="checkbox"/> Idle<input type="checkbox"/> Nice<input type="checkbox"/> Steal	Load average <ul style="list-style-type: none"><input checked="" type="checkbox"/> 1 min<input checked="" type="checkbox"/> 5 min<input checked="" type="checkbox"/> 15 min	Memory <ul style="list-style-type: none"><input checked="" type="checkbox"/> Free<input type="checkbox"/> Cached<input type="checkbox"/> Buffered<input type="checkbox"/> Total<input type="checkbox"/> Writeback<input type="checkbox"/> Inactive<input type="checkbox"/> Dirty<input type="checkbox"/> Mapped<input checked="" type="checkbox"/> Active<input type="checkbox"/> Slab<input type="checkbox"/> Huge Pages Free<input type="checkbox"/> Huge Pages Rsvd<input type="checkbox"/> Huge Pages Surp<input type="checkbox"/> Huge Pages Size<input type="checkbox"/> Huge Pages Total<input type="checkbox"/> Page Tables	Swap <ul style="list-style-type: none"><input type="checkbox"/> Swap<input type="checkbox"/> Free<input type="checkbox"/> Committed
Processes <ul style="list-style-type: none"><input type="checkbox"/> Sleeping<input checked="" type="checkbox"/> Running<input type="checkbox"/> Total<input type="checkbox"/> Stopped<input type="checkbox"/> Blocked<input type="checkbox"/> Zombie	Disk I/O <ul style="list-style-type: none"><input type="checkbox"/> TPS<input type="checkbox"/> Read Kb/s<input type="checkbox"/> Write Kb/s<input type="checkbox"/> Read IO/s<input type="checkbox"/> Write IO/s<input type="checkbox"/> Rrqms<input type="checkbox"/> Wrqms<input type="checkbox"/> Avg Queue Size<input type="checkbox"/> Avg Request Size<input type="checkbox"/> Await<input type="checkbox"/> Util<input type="checkbox"/> Read Total<input type="checkbox"/> Write Total	File system <ul style="list-style-type: none"><input checked="" type="checkbox"/> Used<input type="checkbox"/> Total<input type="checkbox"/> Used Inodes<input type="checkbox"/> Max Inodes<input type="checkbox"/> Used %<input type="checkbox"/> Used Inodes %	

Cancel Save

CloudWatch利用イメージ 標準メトリックス監視

The screenshot displays the AWS CloudWatch console interface. At the top, the navigation bar includes 'AWS', 'サービス', 'EC2', 'CloudWatch', 'CloudTrail', 'Config', 'S3', and '編集'. The left-hand navigation menu is highlighted with a red box and contains the following items: 'ダッシュボード', 'アラーム', 'アラーム' (with a notification badge of 11), '不足' (with a notification badge of 2), 'OK', '請求', 'ログ', 'メトリックス', '選択されたメトリックス' (with a notification badge of 1), '請求', 'DynamoDB', 'EBS', 'EC2', 'Lambda', 'Redshift', 'SNS', 'SQS', and 'カスタムメトリックス...'. The main content area shows the 'EC2 > インスタンス別メトリックス' view for instance 'i-cbe78721'. A table lists various metrics with checkboxes for selection. The 'CPUUtilization (CPUUtilization)' metric is selected. Below the table, a line graph displays 'CPUUtilization (Percent)' over time, with a '5 分間' (5-minute) interval and '平均' (Average) aggregation. The graph shows a fluctuating blue line between 5% and 25% utilization. The x-axis is labeled with dates and times from 13:00 on 4/27 to 00:00 on 4/28. The y-axis is labeled '左軸の単位: Percent' and ranges from 5 to 30. A dashed orange box highlights the legend area at the bottom of the graph, which contains the label 'CPUUtilization'. On the right side of the graph, there are controls for 'グラフの更新', '時間範囲' (set to '相対値'), '開始' (12 時間前), '終了' (0 分前), and 'ズーム' (1 時間, 3 時間, 6 時間, 12 時間, 1 日間, 3).

インスタンス ID (InstanceID)	メトリックス名
<input checked="" type="checkbox"/>	CPUUtilization (CPUUtilization)
<input type="checkbox"/>	DiskReadBytes (DiskReadBytes)
<input type="checkbox"/>	DiskReadOps (DiskReadOps)
<input type="checkbox"/>	DiskWriteBytes (DiskWriteBytes)
<input type="checkbox"/>	DiskWriteOps (DiskWriteOps)
<input type="checkbox"/>	NetworkIn (NetworkIn)
<input type="checkbox"/>	NetworkOut (NetworkOut)
<input type="checkbox"/>	StatusCheckFailed (StatusCheckFailed)
<input type="checkbox"/>	StatusCheckFailed_Instance (StatusCheckFailed_Instance)
<input type="checkbox"/>	StatusCheckFailed_System (StatusCheckFailed_System)

Amazon CloudWatchを使ったアラーム設定

OK

定義された閾値を
下回っている
(正常値)

アラーム
(Alarm)

定義された閾値を
上回っている
(異常値)

不足
(INSUFFICIENT)

データが不足のため、
状態を判定できない
(判定不能)

CloudWatch特有のステータス

INSUFFICIENT_DATAの考え方

- CloudWatchはデータポイントを基準にステータスを判断
 - データポイントとはCloudWatchに送信される値(CPU値など)
 - OK / アラーム時は入力されたデータポイントを基準に状態評価
 - INSUFFICIENT時はCloudWatchにデータポイントの入力が無い状態

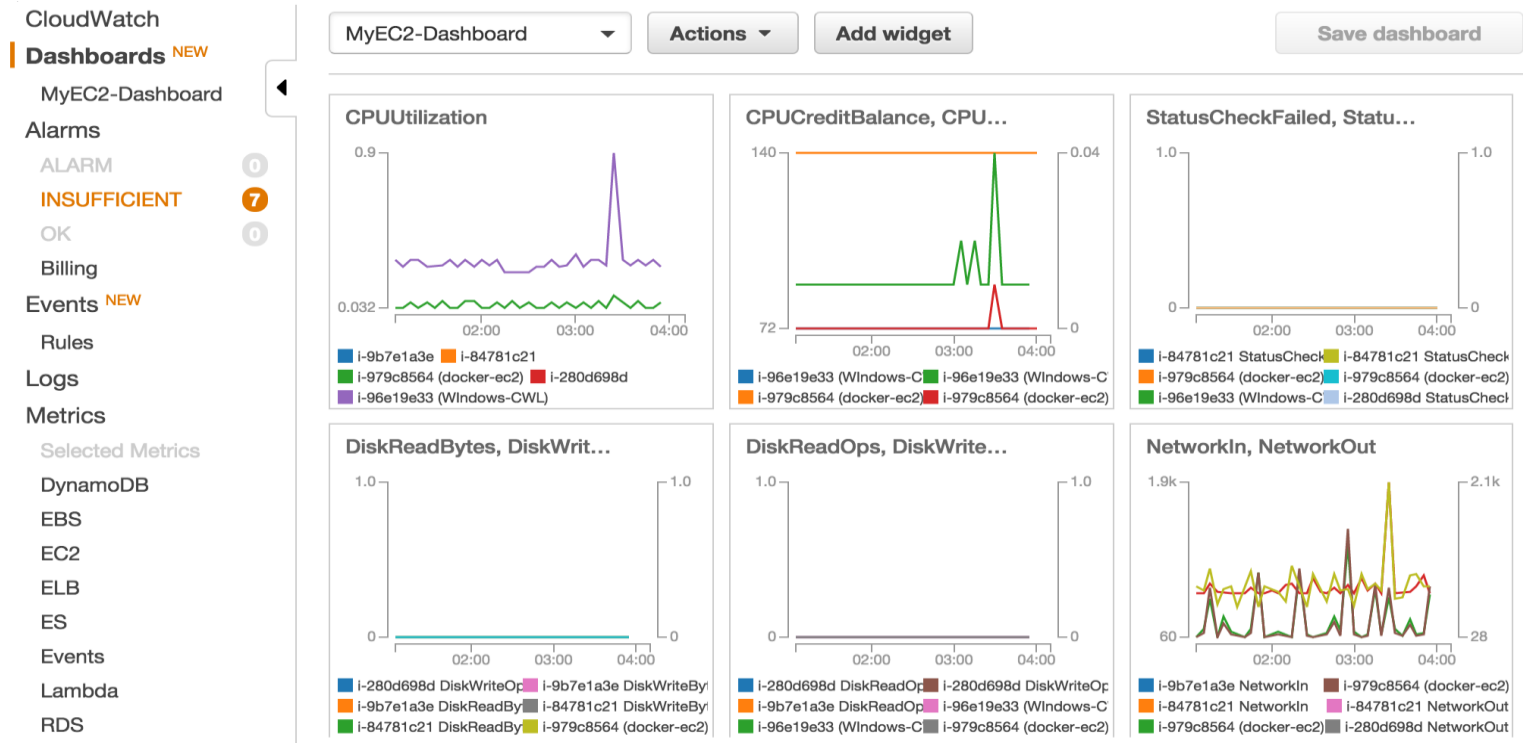
→ “INSUFFICIENT”は必ずしも障害を表すステータスではない



CloudWatch Dashboard

New

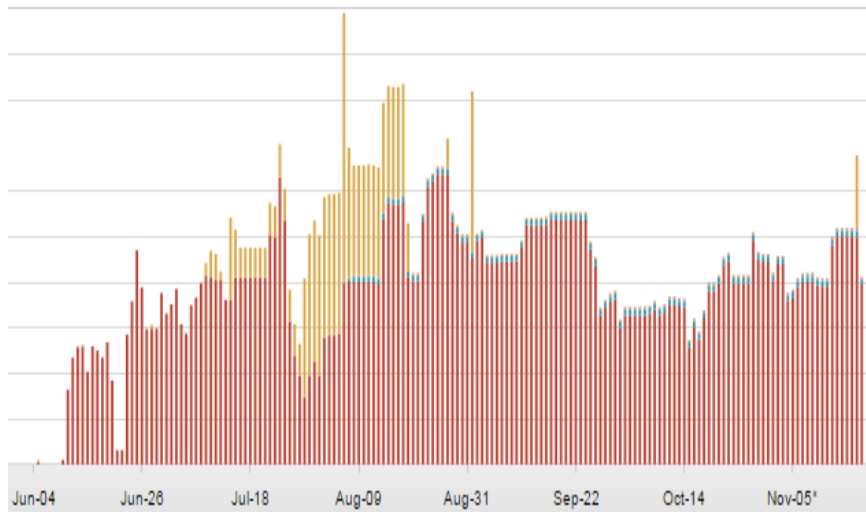
- 運用にあったメトリックス ダッシュボードが利用可能



Amazon CloudWatchによるコストの監視

• Billingアラーム設定

- 課金状況をCloudWatch監視
- 一定金額を超えるとアラームメール通知が可能



Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name:

Description:

Whenever charges for: EstimatedCharges

is:

Actions

Define what actions are taken when your alarm changes state.

Notification Delete

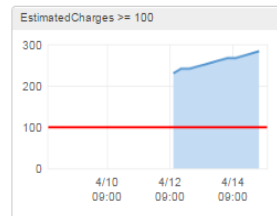
Whenever this alarm:

Send notification to: [New list](#) [Enter list](#) ⓘ

[+ Notification](#) [+ Auto Scaling Action](#) [+ EC2 Action](#)

Alarm Preview

This alarm will trigger when the blue line goes up to or above the red line



Namespace: AWS/Billing

Currency:

Metric Name:

メンテナンスイベントの監視

- AWSが予定するメンテナンス情報は事前にお客様にご連絡させていただきます。

マネジメントコンソールへの通知

The screenshot shows the AWS Management Console interface for an EC2 instance. At the top, there is a table listing instances. Below it, a yellow warning banner indicates a scheduled maintenance event: "リタイア: このインスタンスは 2015年7月01日 9:00:00 UTC+9 後にリタイアが予定されています。" Below the banner, there are tabs for "説明", "ステータスチェック", "モニタリング", and "タグ". The "説明" tab is active, showing instance details such as ID, status (running), type (t2.micro), DNS, and security groups. A red box highlights the "予定されているイベント" (Scheduled events) section, which shows one event: "AMI ID: amzn-ami-hvm-2015.03.0.x86_64-gp2".

Name	インスタンス名	インスタンスタイプ	アベイラビリティゾーン	インスタンスの状態	ステータスチェック	アラームのステータス	パブリック DNS
Server 1	i-xxxxxxx	t2.micro	ap-northeast-1c	running	2/2のチェック済み	なし	
Server 2	i-xxxxxxx	t2.micro	ap-northeast-1a	running	2/2のチェック済み	なし	

インスタンス: i-xxxxxxx (Server 1) パブリック DNS: ec2-xx-xx-xx-xx.ap-northeast-1.compute.amazonaws.com

リタイア: このインスタンスは 2015年7月01日 9:00:00 UTC+9 後にリタイアが予定されています。

説明 ステータスチェック モニタリング タグ

インスタンス ID: i-xxxxxxx パブリック DNS: ec2-xx-xx-xx-xx.ap-northeast-1.compute.amazonaws.com

インスタンスの状態: running パブリック IP: -

インスタンスタイプ: t2.micro Elastic IP: -

プライベート DNS: ip-xxx-xxx-xx-xx.ap-northeast-1.compute.internal アベイラビリティゾーン: ap-northeast-1c

プライベート IP: - セキュリティグループ: . ルールの表示

セカンダリプライベート IP: - **予定されているイベント: 予定されているイベントが 1 件あります**

AMI ID: amzn-ami-hvm-2015.03.0.x86_64-gp2

メールでの通知

Dear Amazon EC2 Customer,

We have important news about your account. EC2 has detected degradation of the underlying hardware hosting one or more of your Amazon EC2 instances in the ap-northeast-1 region. Due to this degradation, your instance(s) could already be unreachable. Running instances will be stopped or terminated after XX:XX AM UTC on YYYY-MM-DD. The affected instances are listed below:

i-XXXXXXXX

You can see more information on your instances that are scheduled for retirement in the AWS Management Console (<https://console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#Events>)

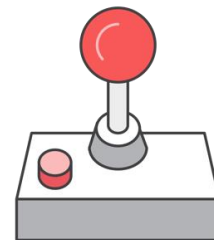
メンテナンスイベントの監視

- メンテナンスイベント取得にはCLI/APIが便利
 - EC2
 - describe-instance-status (CLI)
 - DescribeInstanceStatus (API)
 - RDS
 - describe-pending-maintenance-actions (CLI)
 - DescribePendingMaintenanceActions (API)

```
aws ec2 describe-instance-status --instance-ids i-15a4417c
```

```
{
  "InstanceStatuses": [
    {
      "InstanceStatus": {
        "Status": "ok",
        "Details": [
          {
            "Status": "passed",
            "Name": "reachability"
          }
        ]
      },
      "AvailabilityZone": "us-west-2a",
      "InstanceId": "i-1a2b3c4d",
      "InstanceState": {
        "Code": 16,
        "Name": "running"
      },
      "SystemStatus": {
        "Status": "ok",
        "Details": [
          {
            "Status": "passed",
            "Name": "reachability"
          }
        ]
      },
      "Events": [
        {
          "Code": "instance-stop",
          "Description": "The instance is running on degraded hardware",
          "NotBefore": "2015-05-23T00:00:00.000Z"
        }
      ]
    }
  ]
}
```

AWSサービス毎の監視



• AWS Service Health Dashboard

- AWSサービス全体の利用可能確認
- 各リージョン毎、サービス毎にサービス提供状態
- RSSフィードを使ったモニタリング

North America	South America	Europe	Asia Pacific									
				<<	Apr 29	Apr 28	Apr 27	Apr 26	Apr 25	Apr 24	Apr 23	>>
Amazon CloudFront					✓	✓	✓	✓	✓	✓	✓	
Amazon CloudSearch (Singapore)					✓	✓	✓	✓	✓	✓	✓	
Amazon CloudSearch (Sydney)					✓	✓	✓	✓	✓	✓	✓	
Amazon CloudSearch (Tokyo)					✓	✓	✓	✓	✓	✓	✓	
Amazon CloudWatch (Singapore)					✓	✓	✓	✓	✓	✓	✓	
Amazon CloudWatch (Sydney)					✓	✓	✓	✓	✓	✓	✓	
Amazon CloudWatch (Tokyo)					✓	✓	✓	✓	✓	✓	✓	
Amazon DynamoDB (Singapore)					✓	✓	✓	✓	✓	✓	✓	



Amazon Web Services > Service Health Dashboard

Current Status - Apr 16, 2015 PDT

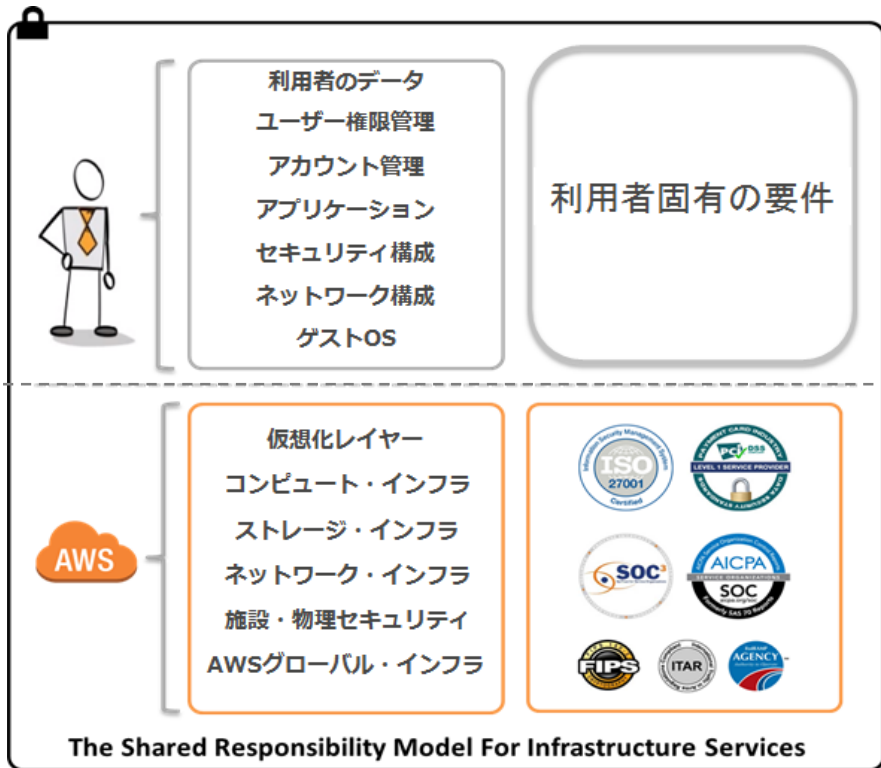
Amazon Web Services publishes our most up-to-the-minute information on service availability in the table below. Check back here any time to get current status information, or subscribe to an RSS feed to be notified of interruptions to each individual service. If you are experiencing a real-time operational issue with one of our services that is not described below, please inform us by clicking on the "Contact Us" link to submit a service issue report. All dates and times are in Pacific Time (PST/UTC).

North America	South America	Europe	Asia Pacific	Contact Us
Current Status			Details	RSS
✓ Amazon CloudFront			Service is operating normally	53
✓ Amazon CloudSearch (Singapore)			Service is operating normally	53
✓ Amazon CloudSearch (Sydney)			Service is operating normally	53
✓ Amazon CloudSearch (Tokyo)			Service is operating normally	53
✓ Amazon CloudWatch (Singapore)			Service is operating normally	53
✓ Amazon CloudWatch (Sydney)			Service is operating normally	53
✓ Amazon CloudWatch (Tokyo)			Service is operating normally	53
✓ Amazon DynamoDB (Singapore)			Service is operating normally	53
✓ Amazon DynamoDB (Sydney)			Service is operating normally	53
✓ Amazon DynamoDB (Tokyo)			Service is operating normally	53
✓ Amazon EC2 Container Service (Tokyo)			Service is operating normally	53
✓ Amazon Elastic Compute Cloud (Singapore)			Service is operating normally	53
✓ Amazon Elastic Compute Cloud (Sydney)			Service is operating normally	53
✓ Amazon Elastic Compute Cloud (Tokyo)			Service is operating normally	53
✓ Amazon Elastic Load Balancing (Singapore)			Service is operating normally	53
✓ Amazon Elastic Load Balancing (Sydney)			Service is operating normally	53
✓ Amazon Elastic Load Balancing (Tokyo)			Service is operating normally	53

<http://status.aws.amazon.com/>

Q. 監視はCloudWatchだけで十分？

監視システムとのAmazon CloudWatch連携



3rd Party 監視ツール



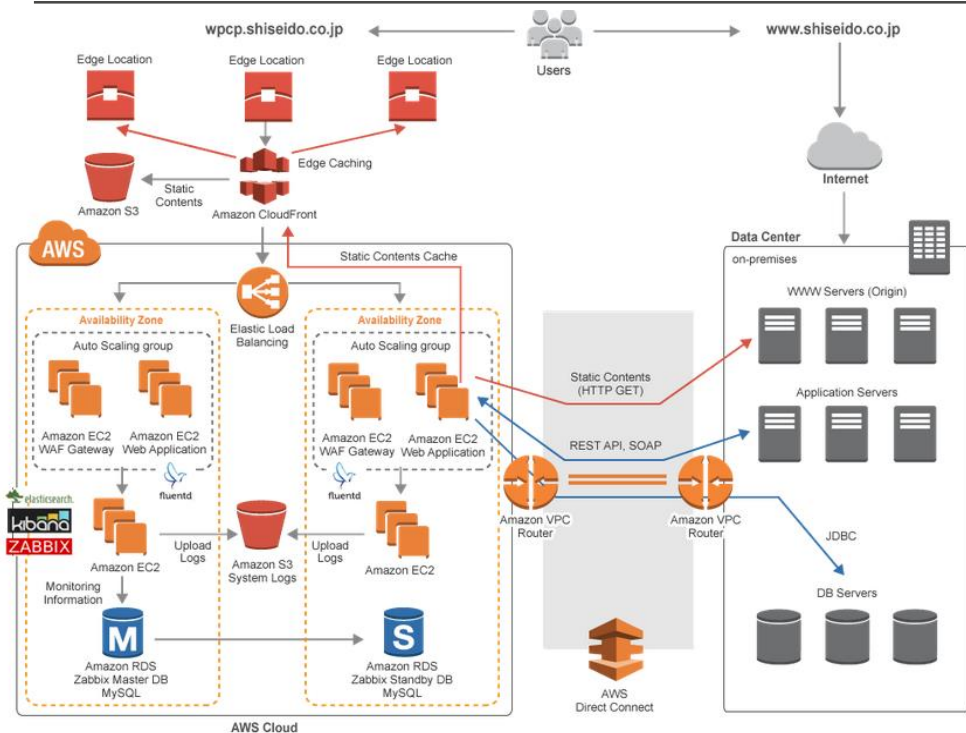
監視ツール連携の必要性

- 監視対象の制限
 - ハイブリッド環境の監視
- データ保存期間(2週間の保存)
- データ保管粒度は最短で1分間隔
- アラートの制限
 - 複合アラートの設定
 - メンテナンス ウィンドウの設定
 - 重要度の設定
- アクション機能
- 通知フォーマット



監視システムとのAmazon CloudWatch連携

監視システムでのCloudWatch活用イメージ



サードパーティ監視ツールの確認ポイント

- AWSに対応しているか
- CloudWatchとの連携機能の有無
- CloudWatchカスタムメトリックスに対応しているか
- Auto Scaling対応しているか
- EC2インスタンス自動検出・自動削除が可能か

ZABBIX

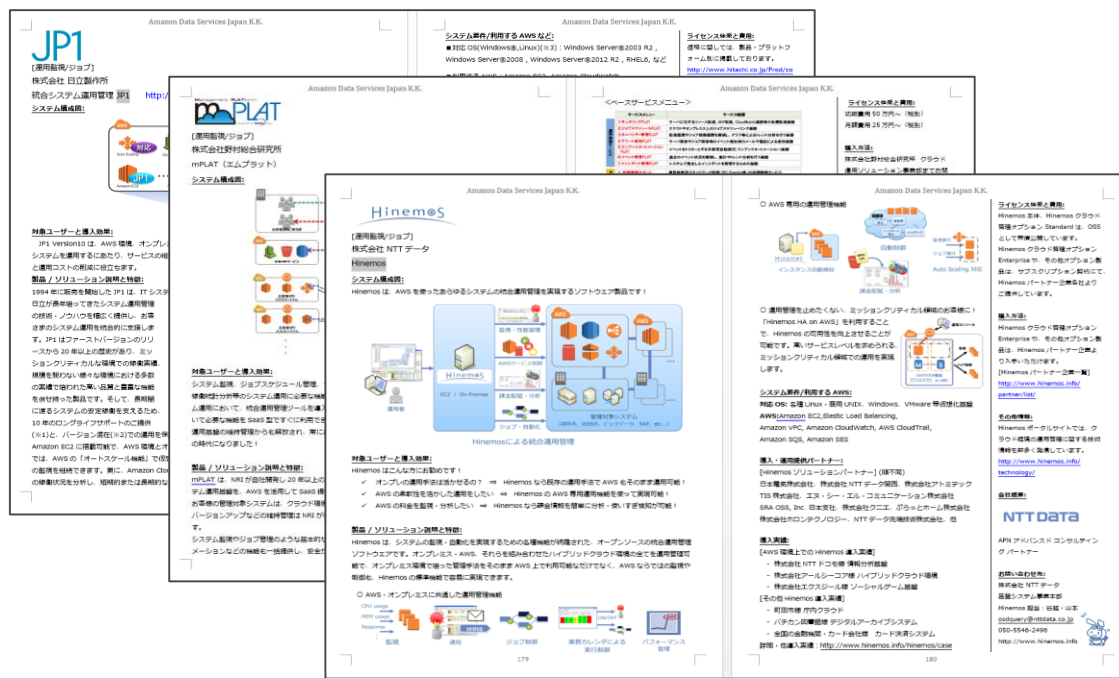
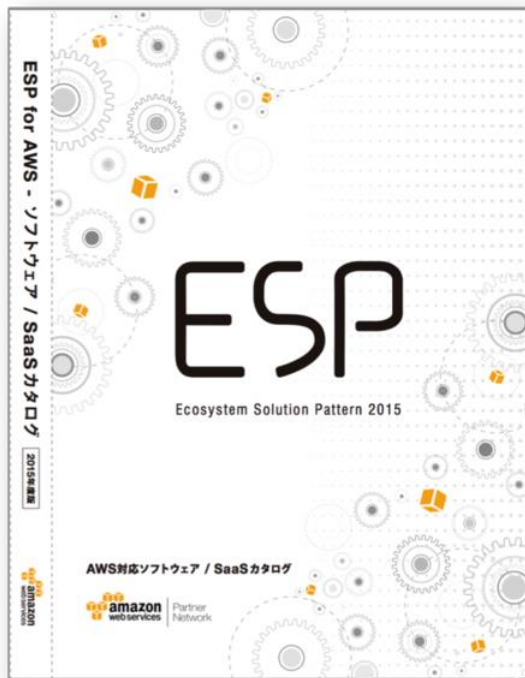
HinemOS

Management PLATform
powered by Senjū only

mackerel JP1

ESP(Ecosystem Solution Pattern)カタログ 無料配布

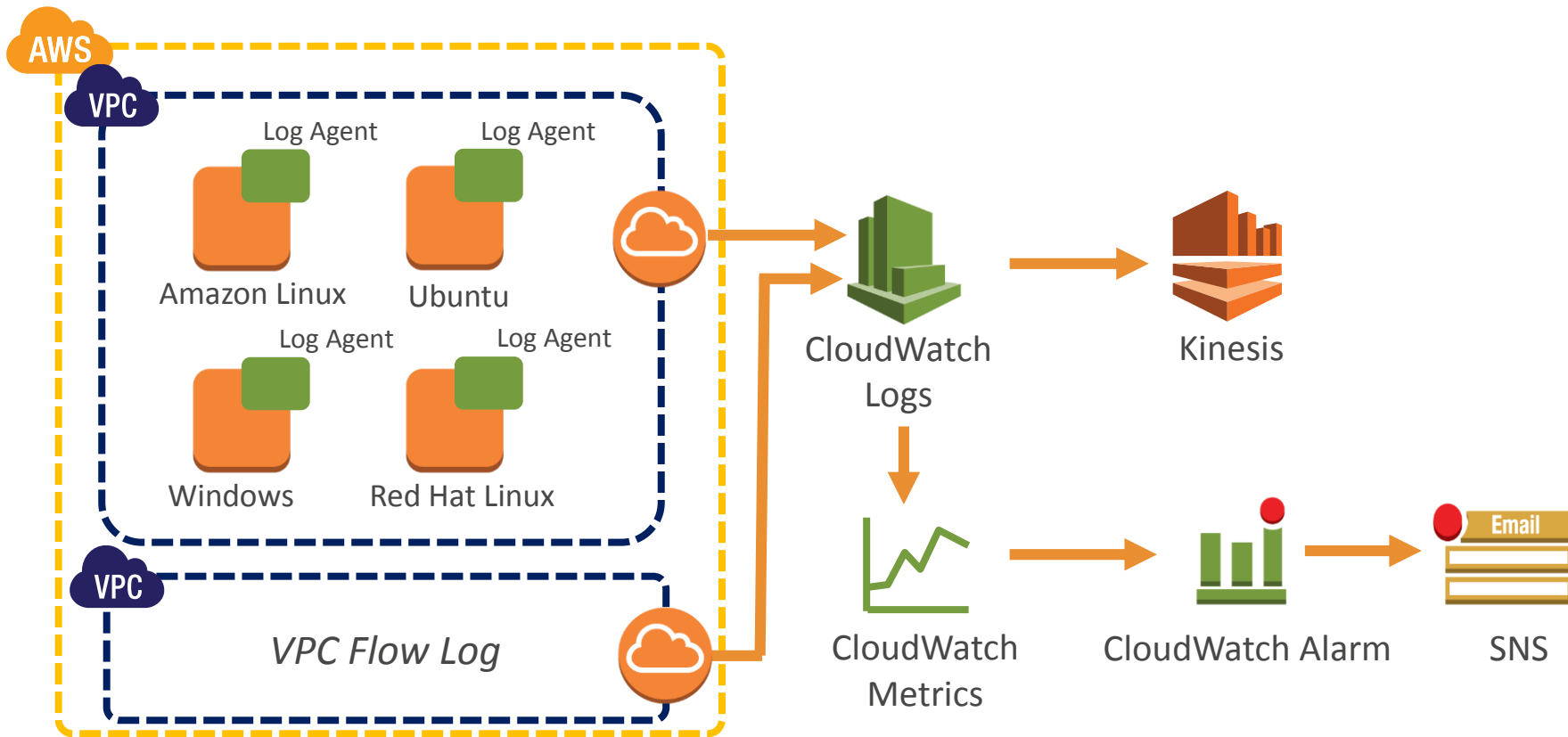
2015年度版 AWS対応ソフトウェア/SaaSガイド



<https://aws.amazon.com/jp/solutions/partner-central/esp-catalog/>

Q. ログの管理はどうしたらいい？

CloudWatch Logs を使ったログ監視



ログモニタリングイメージ

- ログ内容はタイムスタンプとログメッセージ（UTF-8）で構成

The screenshot shows the AWS CloudWatch console interface. At the top, there are navigation tabs for AWS, サービス, EC2, CloudWatch, CloudTrail, Config, S3, and 編集. The main content area displays the breadcrumb path: ロググループ > Windows-Log-Group のストリーム > i-cbe78721 のイベント. Below this, there is a filter bar with '日付/時刻' set to '2015/04/27 06:02:37' and 'ローカル (GMT+09:00)'. The '作成時刻' column is visible. A table of log events is shown, with the 'イベントデータ' column highlighted by a red box. The table contains multiple rows of log entries, each starting with a timestamp and followed by a detailed message in Japanese.

作成時刻	イベントデータ
2015-04-27 06:02:37 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [Windows Modules Installer サービスは 実行中 状態に移行しました。]
2015-04-27 06:04:42 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [Windows Modules Installer サービスは 停止 状態に移行しました。]
2015-04-27 06:04:42 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [Windows Modules Installer サービスは 停止 状態に移行しました。]
2015-04-27 06:06:35 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [Windows Modules Installer サービスは 実行中 状態に移行しました。]
2015-04-27 06:06:35 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [Windows Modules Installer サービスは 実行中 状態に移行しました。]
2015-04-27 06:10:05 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [Windows Modules Installer サービスは 停止 状態に移行しました。]
2015-04-27 06:10:05 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [Windows Modules Installer サービスは 停止 状態に移行しました。]
2015-04-27 06:38:28 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [WinHTTP Web Proxy Auto-Discovery Service サービスは 停止 状態に移行しまし…]
2015-04-27 06:57:57 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [WinHTTP Web Proxy Auto-Discovery Service サービスは 実行中 状態に移行しま…]
2015-04-27 07:25:00 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [WinHTTP Web Proxy Auto-Discovery Service サービスは 停止 状態に移行しまし…]
2015-04-27 07:25:00 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [WinHTTP Web Proxy Auto-Discovery Service サービスは 停止 状態に移行しまし…]
2015-04-27 08:02:45 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [WinHTTP Web Proxy Auto-Discovery Service サービスは 実行中 状態に移行しま…]
2015-04-27 08:23:38 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [Windows Modules Installer サービスは 実行中 状態に移行しました。]
2015-04-27 08:25:39 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [Windows Modules Installer サービスは 停止 状態に移行しました。]
2015-04-27 08:31:17 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [WinHTTP Web Proxy Auto-Discovery Service サービスは 停止 状態に移行しまし…]
2015-04-27 09:05:23 UTC+9	[System] [Information] [7036] [Service Control Manager] [WIN-BHGRATORDMN] [WinHTTP Web Proxy Auto-Discovery Service サービスは 実行中 状態に移行しま…]

CloudWatch Logsのディレクトリ階層

Log Group



Web Server

Log Stream



i-1234501



i-1234502



i-1234503

Log Event

```
04 kernel: initlog 5.8.10, log source = /proc/kmsg started.
04 rsyslogd: [origin software"rsyslogd" swftversion:"3.8.10" xpid:"1391" v-info:"https://www.rs-
04 kernel: [ 0.000000] Initializing cpufreq subsystem
04 kernel: [ 0.000000] Initializing cpufreq subsystem
04 kernel: [ 0.000000] Initializing cpufreq subsystem
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] Linux version 3.10.42-52.145.amzn1.x86_64 (ec2-user@ip-10-0-10-104) (~
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] Command line: root=LABEL=/ console=tty0
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] e820: BIOS-provided physical RAM map:
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] usable
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] reserved
```

```
04 kernel: initlog 5.8.10, log source = /proc/kmsg started.
04 rsyslogd: [origin software"rsyslogd" swftversion:"3.8.10" xpid:"1391" v-info:"https://www.rs-
04 kernel: [ 0.000000] Initializing cpufreq subsystem
04 kernel: [ 0.000000] Initializing cpufreq subsystem
04 kernel: [ 0.000000] Initializing cpufreq subsystem
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] Linux version 3.10.42-52.145.amzn1.x86_64 (ec2-user@ip-10-0-10-104) (~
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] Command line: root=LABEL=/ console=tty0
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] e820: BIOS-provided physical RAM map:
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] usable
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] reserved
```

```
04 kernel: initlog 5.8.10, log source = /proc/kmsg started.
04 rsyslogd: [origin software"rsyslogd" swftversion:"3.8.10" xpid:"1391" v-info:"https://www.rs-
04 kernel: [ 0.000000] Initializing cpufreq subsystem
04 kernel: [ 0.000000] Initializing cpufreq subsystem
04 kernel: [ 0.000000] Initializing cpufreq subsystem
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] Linux version 3.10.42-52.145.amzn1.x86_64 (ec2-user@ip-10-0-10-104) (~
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] Command line: root=LABEL=/ console=tty0
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] e820: BIOS-provided physical RAM map:
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] usable
2014-07-24 17:20:56 UTC+9 *Jul 24 08:37:00 i-10-0-10-104 kernel: [ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] reserved
```

ログの保存期間

- CloudWatch Logsはログを永久保存可能

Log Groups

Create Metric Filter Create Log Group Delete Log Group

Log Groups	Expire Events After	Metric Filters
<input type="checkbox"/> CloudTrail-Virginia	Never Expire	1 filter
<input type="checkbox"/> Linux-Secure-Logs	Never Expire	0 filters
<input type="checkbox"/> Linux-Sysytem-Logs	Never Expire	1 filter
<input type="checkbox"/> Windows-Log-Group	Never Expire	0 filters
<input type="checkbox"/> Windows-SQL-Logs	Never Expire	0 filters

Never Expire ▾

- Never Expire
- 1 day
- 3 days
- 5 days
- 1 week (7 days)
- 2 weeks (14 days)
- 1 month (30 days)
- 2 months (60 days)
- 3 months (90 days)
- 4 months (120 days)
- 5 months (150 days)
- 6 months (180 days)
- 1 year (365 days)
- 13 months (400 days)
- 18 months (545 days)
- 2 years (731 days)
- 5 years (1827 days)
- 10 years (3653 days)

CloudWatch Logs Metric Filter

- 特定文字列の出現回数によりアラーム作成が可能
- “error”という文字列が出現するとアラーム上げる

Create Metric Filter and Assign a Metric

Filter for Log Group: /var/log/messages

Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.

Filter Name: error

Filter Pattern: error

“error”という文字列を監視

Metric Details

Metric Namespace: LogMetrics **i** Select existing namespace

Metric Name: error **i**

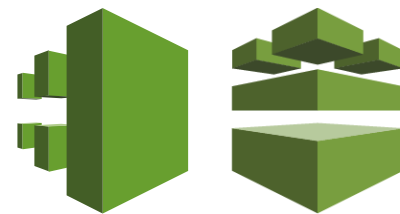
Metric Value: 1

“error”という文字列の出現回数

AWS監視のまとめ

1. AWS上のシステム運用監視の際は、まずCloudWatchでどこまで対応可するかを検討
 - まずどのレイヤまでを監視するのか決定する
 - 必要に応じて3rd Partyの利用も検討
2. AWSならではの監視項目も合わせて監視対象メトリック스에組み込む
3. CloudWatch Logsを利用することで、AWSプラットフォームのログを一元的に集約できる

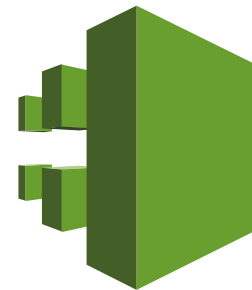
Q. AWSの運用監視をより安全にするには？



AWS CloudTrailとは

- 概要

- AWSアカウント/ユーザの操作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
- S3にロギングデータを保存
 - CloudTrail ログファイルは暗号化されS3に保存 (SSE)
 - gz形式で圧縮
- CloudTrail 自体は無料
 - Amazon S3/SNSの使用料金が必要



The screenshot shows the AWS console interface for an S3 bucket named 'fmrinc-cloudtrail-bucket'. The breadcrumb path is 'All Buckets / fmrinc-cloudtrail-bucket / AWSLogs / 123456789012 / CloudTrail / us-west-2 / 2013 / 11 / 03'. A table lists several log files with their names, storage classes, and sizes.

Name	Storage Class	Size
123456789012_CloudTrail_us-west-2_2013-11-03T21:40Z_63QlcV3Qp2609sCL.json.gz	Standard	1 KB
123456789012_CloudTrail_us-west-2_2013-11-03T21:45Z_EseusVU7TNEe8jS.json.gz	Standard	1.2 KB
123456789012_CloudTrail_us-west-2_2013-11-03T21:50Z_7CC05rQj5YDGf78.json.gz	Standard	1.1 KB
123456789012_CloudTrail_us-west-2_2013-11-03T23:00Z_sGNVF0fjbKfip0rh.json.gz	Standard	1.1 KB

API call の発生状況



Amazon S3

API call の発生状況
SNS設定の有無



Amazon SNS

AWS CloudTrailによりロギングされるイベント

API call Event



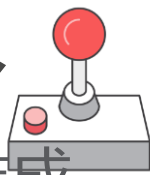
- サポート サービスから発行されるAPI
 - ❖ StartInstances
 - ❖ CreateKeyPair

Non-API call Event



- ユーザのサインイン アクティビティ
 - ❖ AWS マネジメント コンソール
 - ❖ AWS ディスカッション フォーラム

CloudWatchアラーム CloudFormationテンプレート



CloudFormationをつかったメトリック フィルタの自動作成

```
1 {
2   "AWSTemplateFormatVersion" : "2010-09-09",
3   "Description" : "AWS CloudTrail API Activity Alarm Template for
CloudWatch Logs",
4   "Parameters" : {
5     "LogGroupName" : {
6       "Type" : "String",
7       "Default" : "CloudTrail/DefaultLogGroup",
8       "Description" : "Enter CloudWatch Logs log group name. Default
is CloudTrail/DefaultLogGroup"
9     },
10    "Email" : {
11      "Type" : "String",
12      "Description" : "Email address to notify when an API activity
has triggered an alarm"
13    }
14  },
15  "Resources" : {
16    "SecurityGroupChangesMetricFilter" : {
17      "Type" : "AWS::Logs::MetricFilter",
18      "Properties" : {
19        "LogGroup" : { "Ref": "LogGroup" },
```

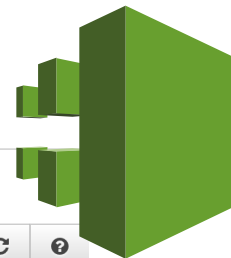
Filter Name: CloudWatchAlarm-CloudTrail-APIActivity-ConsoleSignInFailuresMetric Filter-35PVKU305SE3
Filter Pattern: { (\$.\$eventSource = ConsoleLogin) && (\$.\$errorMessage = "Failed authentication") }
Metric: CloudTrailMetrics / ConsoleSignInFailureCount
Metric Value: 1
Alarm: CloudTrailConsoleSignInFailures

Filter Name: CloudWatchAlarm-CloudTrail-APIActivity-EC2InstanceChangesMetric Filter-1Q1TJK84379GF
Filter Pattern: { (\$.\$eventName = RunInstances) || (\$.\$eventName = RebootInstances) || (\$.\$eventName = StartInstances) || (\$.\$eventName = StopInstances) || (\$.\$eventName = TerminateInstances) }
Metric: CloudTrailMetrics / EC2InstanceEventCount
Metric Value: 1
Alarm: CloudTrailEC2InstanceChanges

Filter Name: CloudWatchAlarm-CloudTrail-APIActivity-EC2LargeInstanceChangesMetric Filter-r-V2DOYX90SA20
Filter Pattern: { ((\$.\$eventName = RunInstances) || (\$.\$eventName = RebootInstances) || (\$.\$eventName = StartInstances) || (\$.\$eventName = StopInstances) || (\$.\$eventName = TerminateInstances)) && ((\$.\$requestParameters.instanceType = *.8xlarge) || (\$.\$requestParameters.instanceType = *.4xlarge)) }
Metric: CloudTrailMetrics / EC2LargeInstanceEventCount
Metric Value: 1
Alarm: CloudTrailEC2LargeInstanceChanges

CloudTrail API lookup – マネジメントコンソール

- 直近7日間の情報はヒストリから確認可能



API activity history

Look up API activity related to creation, modification and deletion of resources in your AWS account in the last 7 days. Filter using one of the attributes to troubleshoot operational issues or security incidents.



Filter:	Select attribute	Enter lookup value	Time range:	Select time range	
	Event time	User name	Event name	Resource type	Resource name
▶	2015-12-21, 01:18:28 PM	sakatoku	CreateTags		i-6c19e33
▶	2015-12-21, 01:18:27 PM	sakatoku	RunInstances	Ami and 7 more	ami-t430b0f and 9 more
▶	2015-12-21, 01:17:03 PM	sakatoku	TerminateInstances	Instance	i-846628
▶	2015-12-21, 01:16:23 PM	sakatoku	ConsoleLogin		
▶	2015-12-20, 01:26:07 AM	sakatoku	RunInstances	Ami and 7 more	ami-83c1935 and 9 more
▶	2015-12-20, 01:26:07 AM	sakatoku	CreateTags		i-96b1238
▶	2015-12-20, 12:50:43 AM	sakatoku	DetachUserPolicy	Policy and 1 more	arn:aws:iam::97389731...
▶	2015-12-20, 12:46:34 AM	sakatoku	PutRolePolicy	Policy and 1 more	oneClick_CloudTrail_CI...
▶	2015-12-20, 12:40:39 AM	sakatoku	AttachUserPolicy	Policy and 1 more	arn:aws:iam::97389731...

CloudTrail API サンプル (RunInstance)

▼ 2015-12-21, 01:18:27 PM sakatoku RunInstances Instance and 7 more i-06a198c9 and 9 more

AWS access key ASIA3CAEM2YQW9PDDG6Y4

AWS region ap-northeast-1

Error code

Event ID 7c9f7210-a336-42bc-b94a-03cafacb0c61

Event name RunInstances

Event source ec2.amazonaws.com

Event time 2015-12-21, 01:18:27 PM

Request ID d1bb5747-dd13-48b1-a5e7-647bfb1d4ed7

Source IP address 27.0.3.145

User name sakatoku

Resources Referenced (10)

[ami-0435520](#)

Ami

[mysg4win](#)

SecurityGroup

[AIRA3OQRTU196QJ35UEWS](#)

InstanceProfile

[i-06a198c9](#)

Instance

[sg-0435520](#)

SecurityGroup

[arn:aws:iam::730973481507:instance-profile-](#)

[profile/AWS_Admin](#)

InstanceProfile

[my_0435520](#)

KeyPair

[subnet-0435520](#)

Subnet

[eni-0435520](#)

NetworkInterface

[vpc-0435520](#)

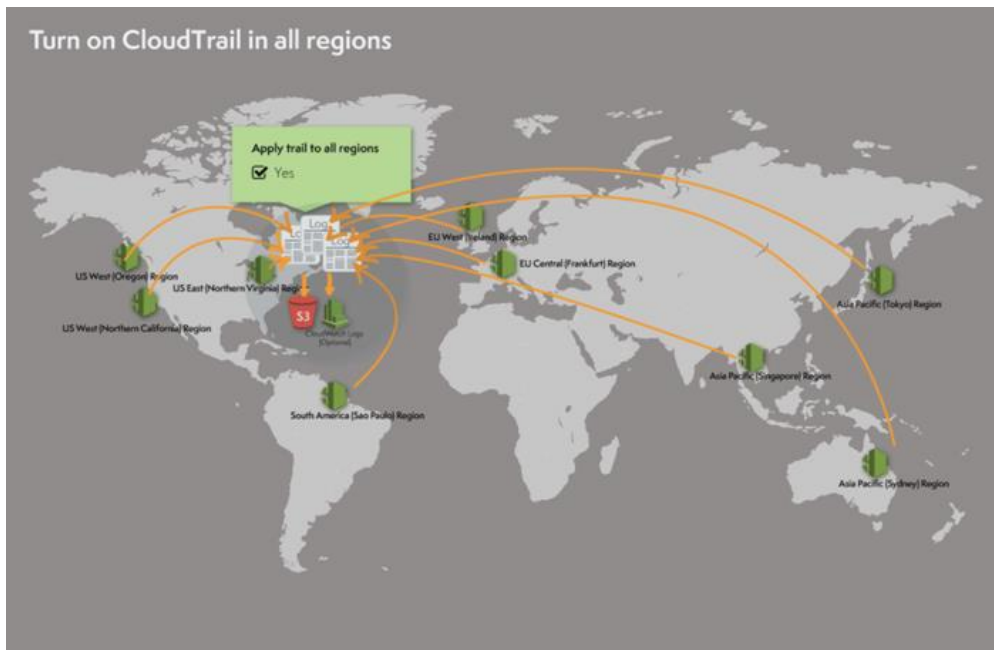
VPC

[View event](#)

CloudTrailの設定が簡単に！

New

- ご利用頂けるすべてのリージョンに数クリックで設定



Create Trail

Trail name* CloudTrail-All-Regions

Apply trail to all regions Yes No ⓘ

Create a new S3 bucket Yes No

S3 bucket* cloudtrail-all-region-bucket ⓘ


Log file prefix ⓘ

Location: /AWSLogs/675897846150/CloudTrail/us-west-2

Amazon Elasticsearch Service



- Elasticsearch クラスタを数分間で起動できるマネージドサービス
- Kibana が組み込まれており、即座にデータのビジュアライズに着手できる
- すでに東京リージョンでも利用可能
- **CloudWatch Logs インテグレーションがとっても簡単**

分析	
	Elastic MapReduce マネージド型 Hadoop フレームワーク
	Data Pipeline データ駆動型ワークフローに対するオーケストレーションサービス
	Elasticsearch Service Elasticsearch クラスタの実行とスケーリング
	Kinesis ビッグデータストリームのリアルタイム処理
	Machine Learning すばやく簡単にスマートアプリケーションを構築

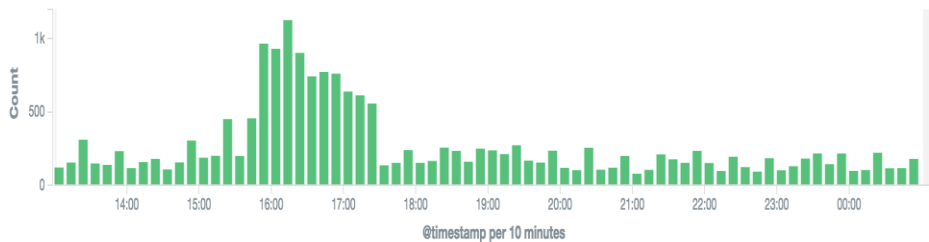


Kibanaを使ったログの可視化



December 24th 2015, 13:01:35.398 - December 25th 2015, 01:01:35.398

19,154 hits



Time

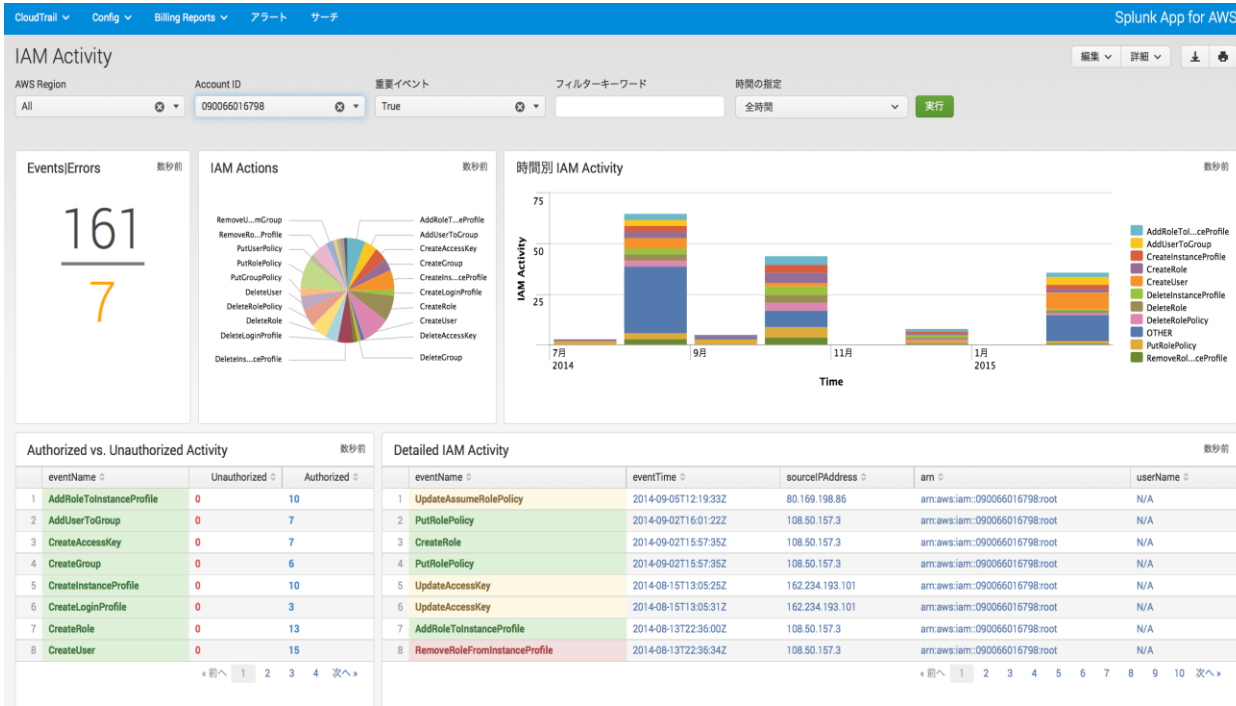
_source

December 25th 2015, 00:58:03.000
srcaddr: 172.31.8.175 dstport: 59250 start: 1450972683 dstaddr: 172.31.0.164 version: 2 packets: 1
protocol: 17 account_id: 675897846150 interface_id: eni-4e229939 log_status: OK bytes: 187 srcport: 53
action: ACCEPT end: 1450972737 @id: 32357772093611345919090088375315554887440576385533214764
@timestamp: December 25th 2015, 00:58:03.000 @message: 2 675897846150 eni-4e229939 172.31.8.175 172.31.0.164 53 59250 17 1 187 1450972683 1450972737 ACCEPT OK @owner: 675897846150 @log_group: defaultvpc-f

December 25th 2015, 00:58:03.000
srcaddr: 172.31.0.164 dstport: 389 start: 1450972683 dstaddr: 172.31.8.175 version: 2 packets: 1
protocol: 17 account_id: 675897846150 interface_id: eni-4e229939 log_status: OK bytes: 211 srcport: 63250
action: ACCEPT end: 1450972737 @id: 32357772093611345919090088375315554887440576385533214769
@timestamp: December 25th 2015, 00:58:03.000 @message: 2 675897846150 eni-4e229939 172.31.0.164 172.31.8.175 63250 389 17 1 211 1450972683 1450972737 ACCEPT OK @owner: 675897846150 @log_group: defaultvpc-



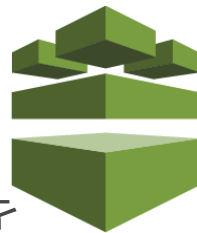
Splunk App for AWS



```
新規サーチ
host="ip-10-170-32-235" sourcetype="aws:cloudtrail" eventName=DeleteInstance*
79件のイベント (15/05/28 5:40:52.000 より前)
```

```
時間 イベント
15/02/03 15:18:26.000 { [-]
  awsRegion: us-east-1
  eventID: ecf14f7b-108a-4b8f-9533-ca08bd8b9eef
  eventName: DeleteInstanceProfile
  eventSource: iam.amazonaws.com
  eventTime: 2015-02-03T15:18:26Z
  eventType: AwsApiCall
  eventVersion: 1.02
  recipientAccountId: 090066016798
  requestID: e6654a76-abb7-11e4-b773-95f72f8c3d47
  requestParameters: { [+]}
  responseElements: null
  sourceIPAddress: 173.63.70.227
  userAgent: console.amazonaws.com
  userIdentity: { [+]}
}
```

AWS Configとは



- AWSリソースのレポジトリ情報を取得し、リソースの設定履歴を監査、リソース構成の変更を通知するフルマネージドサービス

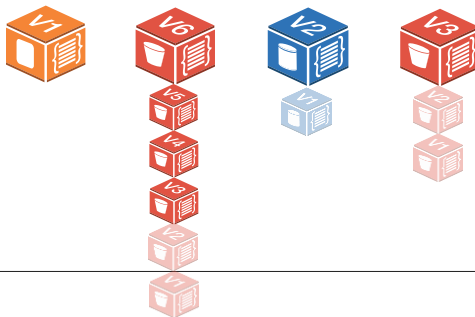
Configuration Stream

- リソースが作成、変更、または構成項目を削除されるたびに、作成され、構成ストリームに追加される
- SNSトピック連携可能



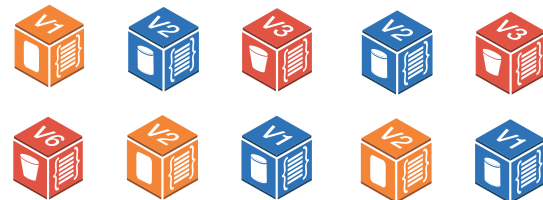
Configuration History

- 設定履歴は、任意の期間における各リソースタイプの構成要素の集合
- リソースの設定履歴を、指定したS3バケットに保存



Configuration Snapshot

- あるポイントでのコンフィグレーション アイテムの集合
- 自動で定期的あるいは変更トリガで作成され、Amazon S3にエクスポートされる



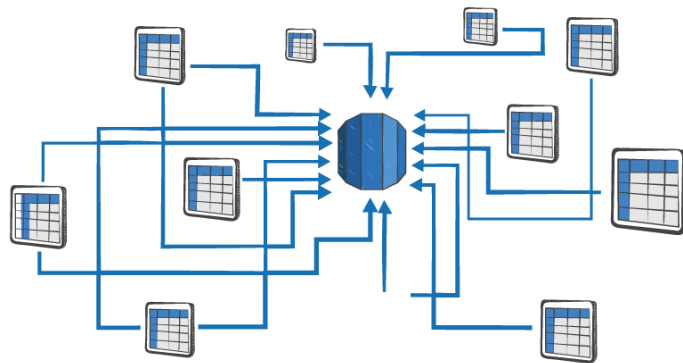
Snapshot @ 2014-11-12, 2:30pm

リレーションシップ

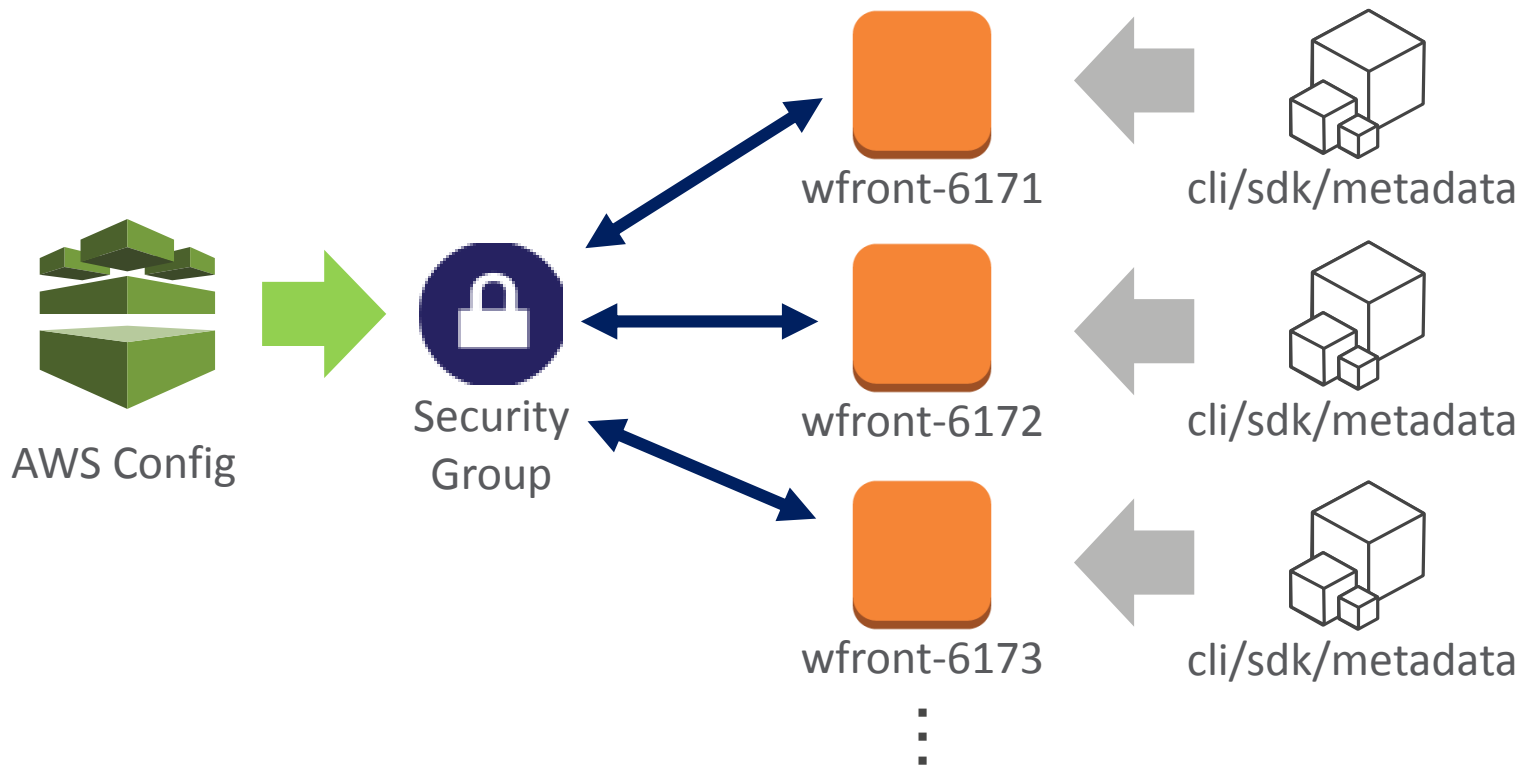
- アカウント内のAWSリソース間の関係
- 双方向の依存関係が自動的に割り当てられる

Example:

セキュリティ グループ“`sg-10dk8ej`” とEC2 インスタンス “`i-123a3d9`”
は互いに関連関係にあります



AWS Config リレーションシップ



AWS Configが対応しているAWSリソース

- 現在AWS Configが対応しているのは下記5サービス



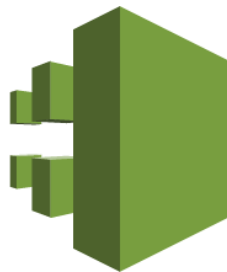
Amazon EC2
Instance, ENI...



Amazon VPC
VPC, Subnet...



Amazon EBS
Volumes



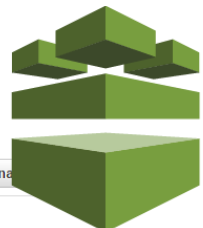
AWS CloudTrail



AWS IAM

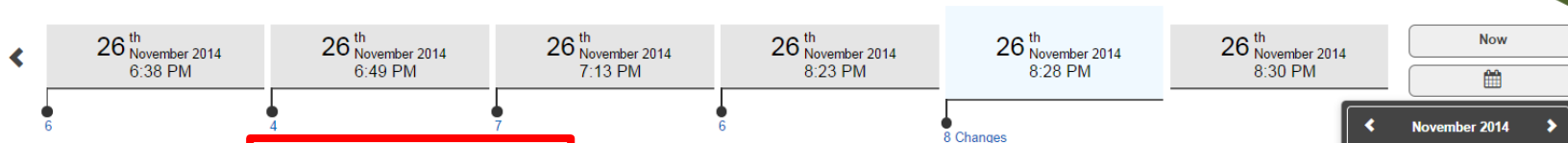
※2015年12月25日時点

現在の構成の確認



EC2 Instance i-cbe78721

Man...



構成詳細

Configuration Details

Amazon Resource Name am:aws:ec2:us-east-1: [redacted] instance/[redacted]
Resource type AWS::EC2::Instance
Resource ID [redacted]
Availability zone us-east-1c
Created at November 26, 2014 8:25 PM
Tags (1) Name:cwl...

Instance Type m3.medium
Instance state running
Private DNS [redacted]
Private Ips [redacted]
Public DNS [redacted]
AMI ID ami-5c17af34
Platform windows
Launch time 2014-11-26T11:25:36.000Z
Lifecycle null
Monitoring disabled

November 2014
Sun Mon Tue Wed Thu Fri Sat
26 27 28 29 30 31 01
02 03 04 05 06 07 08
09 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 01 02 03 04 05 06
08 : 06 PM
Apply

ew Details

リレーション

Relationships

変更

Changes (8)

Terminateしたインスタンスも確認可能

New

Status ?

Resource inventory

Look up existing and deleted resources recorded by AWS Config. View compliance details for each resource or choose the Config timeline icon to see how a particular resource's configuration has changed over time.





Resources EC2: Instance

Include deleted resources

Tag Tag key

[Look up](#)

Choose the  icon to see Config timeline for a resource.

	Resource type	Resource identifier	Compliance	Config timeline
▶	EC2 Instance	i-02368020	Noncompliant with 1 rule	
▶	EC2 Instance	i-72f08f38	Compliant	
▶	EC2 Instance	i-cb978721	Noncompliant with 1 rule	
▼	EC2 Instance	i-02b0cff2 (deleted)	--	



i-02b0cff2 Deleted

Resource i-02b0cff2 was deleted on March 21, 2015 at 11:58PM

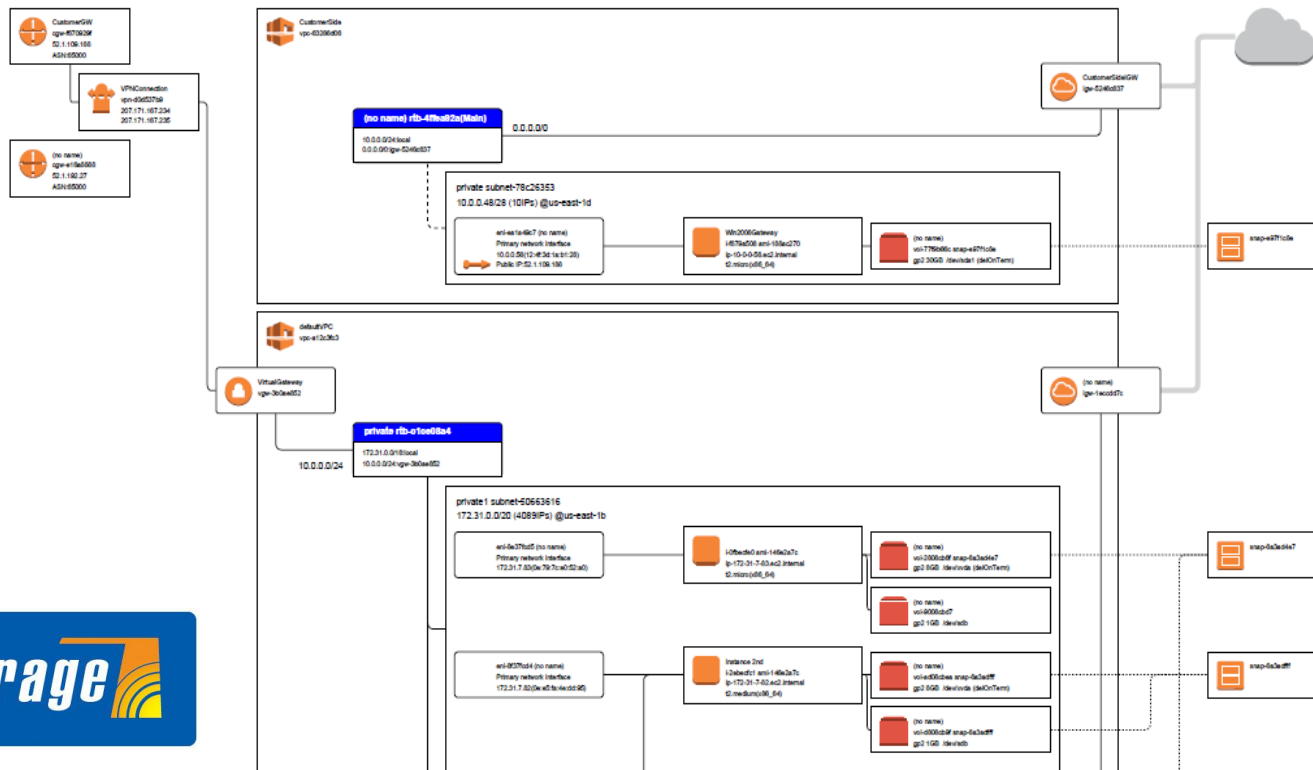
Logstorageによる可視化



AWS Config snapshot Report

Snapshot created:2015/05/19 10:25:08 +0900

data2



AWS Config Rules

New

COMPLIANCE GUIDELINE

All EBS volumes should be encrypted

Instances must be within a VPC

Instances must be tagged with environment type

ACTION

Encrypt volumes

Terminate instance

Page developer

AWS Config Rulesによるポリシー適合の評価

- AWS Config Rules

- 準拠すべきルールを事前に設定し、その内容に沿った構成変更が行われているかをルールに従い評価
 - ✓ 全てのEBCボリュームが暗号化されているか
 - ✓ EC2インスタンスが適切にタグ付されているか
 - ✓ Elastic IP address(EIP)がインスタンスにアタッチされているか

AWS Config Rules

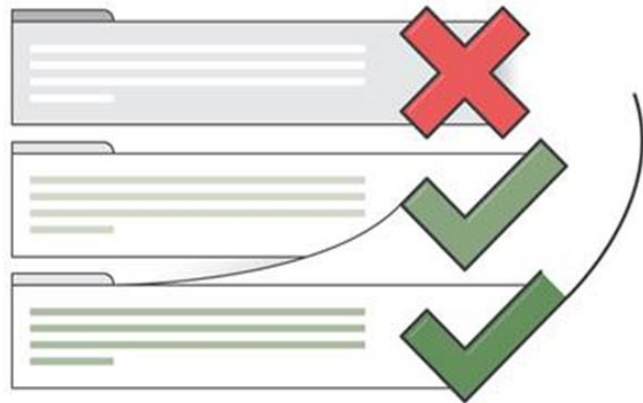
準拠すべきルールを事前に定義、評価を実施

AWS Managed Rules

- AWSにより定義・提供される
- AWSにより運用される
- 必要最低限のベーシック・ルール

Customer Managed Rules

- 自分でAWS Lambdaをベースにルールを作成可能
- 管理自体は作成者（自分）で実施



AWS Config Rules (AWS Managed Rules)

• Managed Rulesの種類

- ✓ ボリュームが暗号化されているか
- ✓ CloudTrail が有効になっているか
- ✓ EIP がアタッチされているか
- ✓ SSH の設定確認(SG)
- ✓ EC2がVPC内に作成されているか
- ✓ タグが付けられているか
- ✓ ポートが適切に設定されているか(SG)

<p>encrypted-volumes</p> <p>Checks whether EBS volumes that are in an attached state are encrypted. Optionally, you can specify the ID of a KMS key to use to encrypt the volume.</p>	<p>cloudtrail-enabled</p> <p>Checks whether AWS CloudTrail is enabled in your AWS account. Optionally, you can specify which S3 bucket, SNS topic, and Amazon CloudWatch Logs ARN to use.</p>	<p>eip-attached</p> <p>Checks whether Elastic IP addresses that are allocated for use in a VPC are attached to EC2 instances.</p>
<p>restricted-ssh</p> <p>Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.</p>	<p>ec2-instances-in-vpc</p> <p>Checks whether your EC2 instances belong to a virtual private cloud (VPC). Optionally, you can specify the VPC ID to associate with your instances.</p>	<p>required-tags</p> <p>Checks whether your resources have all of the tags you specify; for example, you can check whether the 'CostCenter' tag is present on your EC2 instances.</p>
<p>restricted-common-ports</p> <p>Checks whether security groups that are in use disallow unrestricted incoming TCP traffic to the specified ports.</p>		

AWS Config Rules (Customer Managed Rules)

• Customer Managed Rulesの種類

- ✓ Lambda functionを自分で作成
 - ✓ 自由にルールを設定することが可能
- ✓ 作成したLambda functionのarnをルールに紐付ける
- ✓ トリガーのタイミングを選択 (Configuration changes or Periodic)

AWS Lambda function ARN* ⓘ

[Create AWS Lambda function](#)

AWS Config will gain permission to invoke the function by updating the function's access policy.

Trigger

AWS Config evaluates resources when the trigger occurs.

Trigger type* Configuration changes Periodic ⓘ

Rule parameters

Rule parameters define attributes for which your resources are evaluated; for example, a required tag or S3 bucket.

Key	Value
<input type="text" value="Key"/>	<input type="text" value="Value"/>

AWS Config Rules マネジメントコンソール





Rules

Status 

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the results in the following table.

 Add rule



Rule name	Compliance	Edit rule
InstanceTypesAreT2micro	1 noncompliant resource(s)	 Customer Managed
required-tags	Compliant	 AWS Managed
cloudtrail-enabled	Compliant	 AWS Managed
AWSSuperUserPolicyChecks	Compliant	 Customer Managed

AWS Managed Rules サンプル

required-tags

Description Checks whether your resources have all the tags you specify. For example, all EC2 instances should have the CostCenter tag, is triggered by changes to EC2 instance resource type.

Trigger type Configuration changes

Scope of changes Resources

Resource types

Config rule ARN arn:aws:config:us-east-1:675897846150:config-rule/config-rule-vv6m6k

Parameters

Rule status Last successful invocation at Dec 24 5:23 AM

Last successful evaluation at Dec 24 5:23 AM

Resources evaluated

Click on the icon to view configuration details for the resource when it was last evaluated with this rule.

Resource type	Resource identifier	Compliance	Config timeline
EC2 Instance	i-78f0819375	Compliant	
EC2 Instance	i-4be7072175	Compliant	

ルールに違反したインスタンスの表示

Resource type	Resource identifier	Compliance	Config timeline
▼ EC2 Instance	i-cbe78721	Noncompliant with 1 rule	↶

Rules applying to i-cbe78721

Name	Compliance	Description	Last evaluated state
InstanceTypesAreT2micro	Noncompliant	Evaluates whether EC2 instances are the t2.micro type	↶
required-tags	Compliant	Checks whether your resources have all the tags you specify. For exa...	↶

▼ Configuration Details

Amazon Resource Name arn:aws:ec2:us-east-1:i-cbe78721:instance/i-cbe78721

Resource type AWS::EC2::Instance

Resource ID i-cbe78721

Availability zone us-east-1c

Created at November 26, 2014 8:25:36 PM

Tags (2) CostCenter:4005 Name:cwl-sqlserver

Instance Type m3.medium

Instance state stopped

Private DNS ip-10.0.2.230.internal

Private Ips 10.0.2.230

Public DNS null

AMI ID ami-5c17af34

Platform windows

Launch time 2014-11-26T11:25:36.000Z

Lifecycle null

Monitoring disabled

まとめ

- CloudWatchをうまくご利用頂くことで、クラウドで必要な監視を実装可能
- 必要に応じて3rd Party監視ツールとの連携
- ユーザ オペレーションのロギングはCloudTrailを有効かすることで対応可能
- システム全体の構成管理にはAWS Configを利用することで運用負荷軽減に結びつく
- ログの可視化に関してはAPNパートナー様のソリューションと連携する

OpsJAWSご紹介

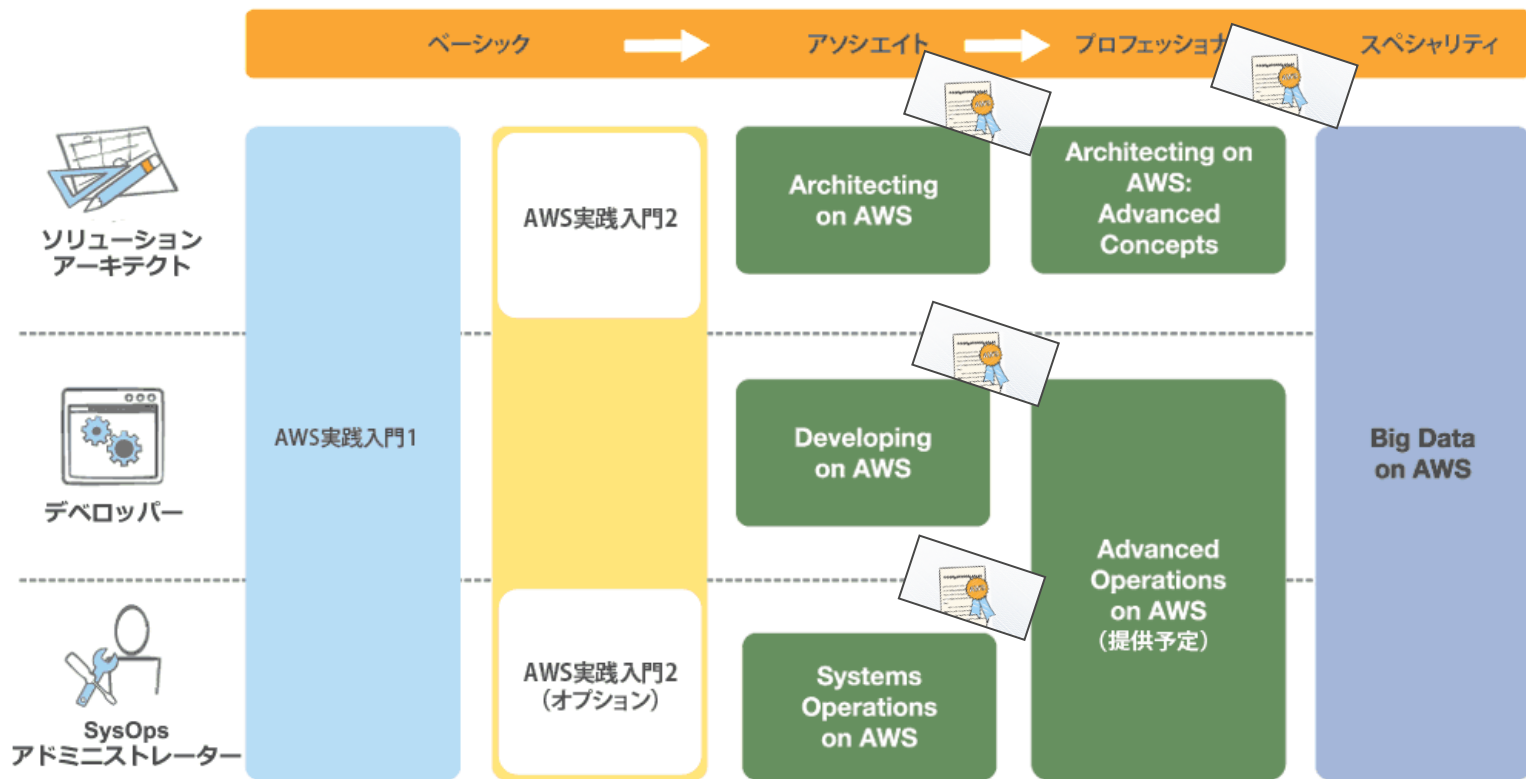
- AWS運用管理のノウハウを広く発信
- Partner SAブログに運用Tips記事を掲載中
 - http://aws.typepad.com/aws_partner_sa/2015/06/aws-ops.html
 - または、 で検索
- DoorKeeper: OpsJAWSコミュニティ
 - <https://opsjaws.doorkeeper.jp/>



Ops-JAWS

AWS User Group - Japan

AWSをより深く理解したい方向けに クラスルームトレーニングを提供しています。



公式Twitter/Facebook AWSの最新情報をお届けします



@awscloud_jp



もしくは <http://on.fb.me/1vR8yWm>

検索



最新技術情報、イベント情報、お役立ち情報、
お得なキャンペーン情報などを日々更新しています！



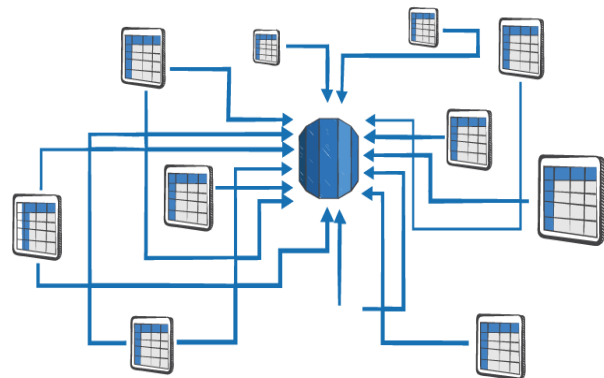
システム基盤運用で考えるポイント



Monitoring
監視



Logging
ロギング



Configuration
構成管理