

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

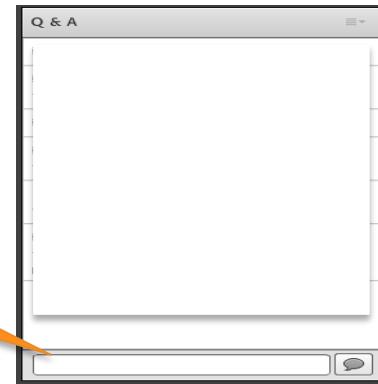
- ・ 運用監視系サービス

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

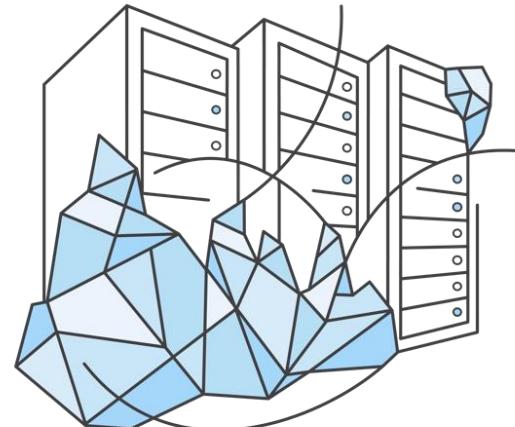
- AWSについてこれから学ぶ方向けのWebinarです。
- 過去のWebinar資料
 - AWSクラウドサービス活用資料集ページにて公開
<http://aws.amazon.com/jp/aws-jp-introduction/>
- イベントの告知
 - 国内のイベント・セミナースケジュールページにて告知
<http://aws.amazon.com/jp/about-aws/events/>
(オンラインセミナー枠)

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

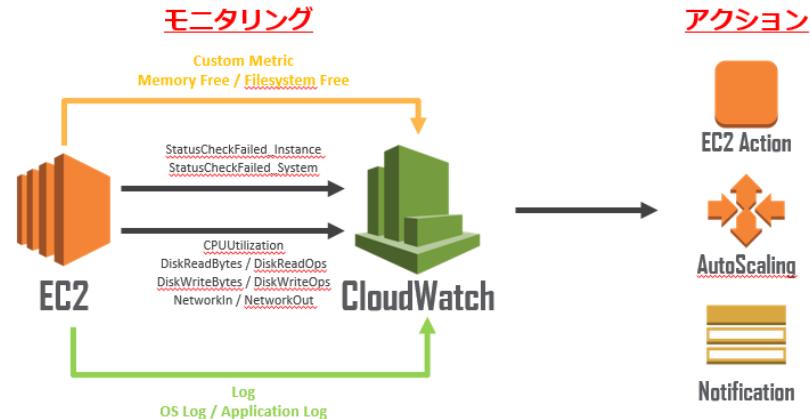


Q. AWSの監視はどうすればいい？

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



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

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 2014-10-28T12:30:00Z\  
  --value 87 \  
  --unit Milliseconds\
```

```
$ aws cloudwatch put-metric-data --metric-name RequestLatency\  
  --namespace "GetStarted"\  
  --timestamp 2014-10-28T12:30:00Z\  
  --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 $\text{Sum}/\text{SampleCount}$ の値です。この統計を <code>Minimum</code> および <code>Maximum</code> 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 <code>Minimum</code> と <code>Maximum</code> 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ために役立ちます。
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

AWS | サービス | EC2 | CloudWatch | CloudTrail | Config | S3 | 編集 | 東京 | サポート

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
- ネットワーキング

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ンベントリ
- 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

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

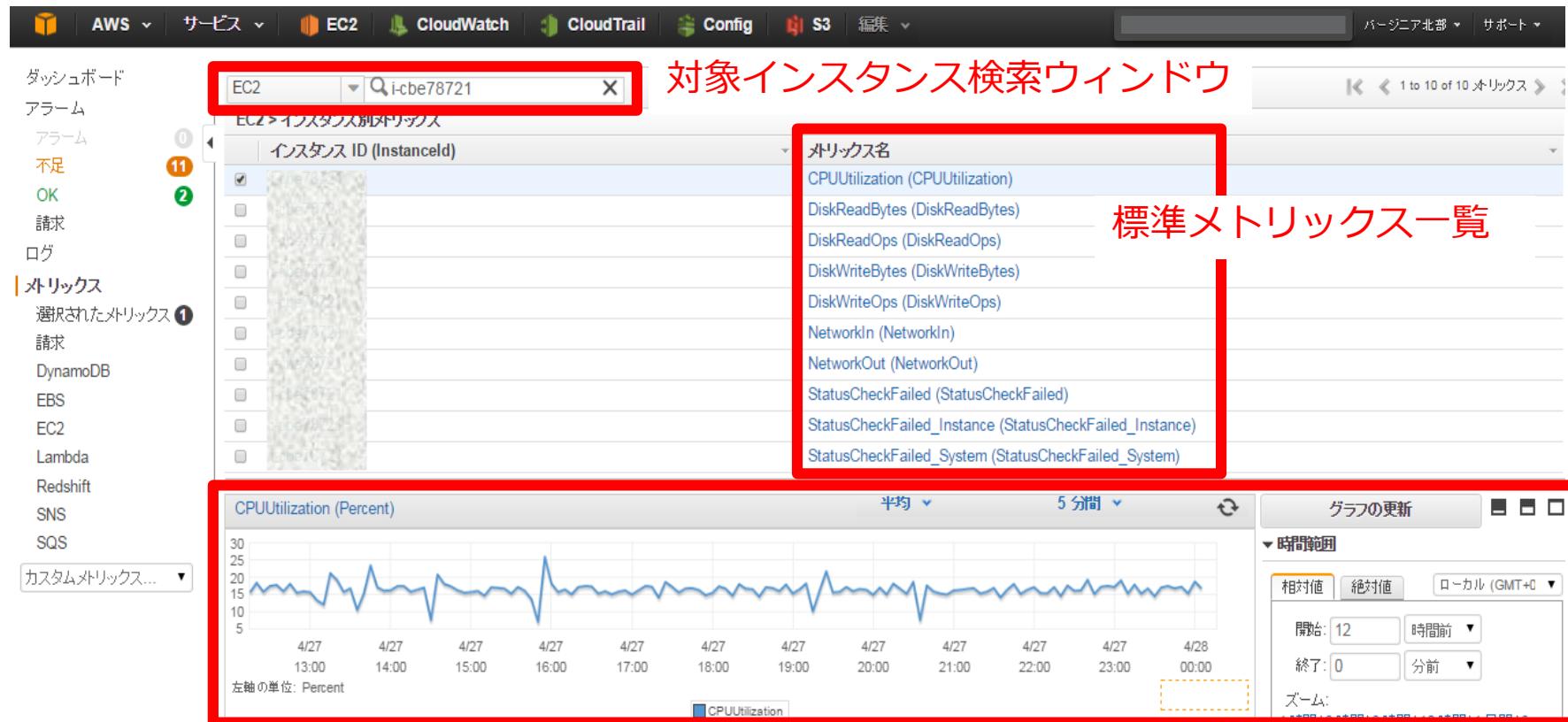
はじめに サービスを初めて使用する手順やさらに詳しい使用方法については、ドキュメントを参照してください。

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。

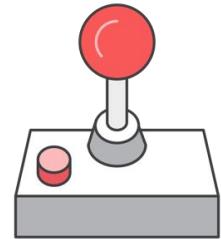
AWS Marketplace ソフトウェアを検索して購入し、1-Click で起動し、時間単位で料金を支払えます。

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 で発表予定のエキサイティングな新規サービスや機能をア

CloudWatch利用イメージ 標準メトリックス監視



Amazon CloudWatchを使った死活監視

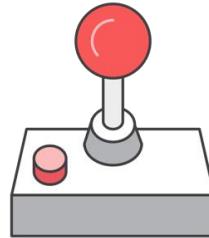


- EC2の死活監視
 - CloudWatch標準メトリックスを利用可能
 - StatusCheckFailed System
 - ハイパーバイザーレイヤから見た正常性確認
 - 最近 1 分間にインスタンスが EC2 システムステータスチェックに成功したかどうかを報告
 - StatusCheckFailed Instance
 - OSレイヤの正常性確認
 - 最近 1 分間にインスタンスが EC2 インスタンスステータスチェックに成功したかどうかを報告
 - StatusCheckFailed
 - StatusCheckFailed_Instance と StatusCheckFailed_System 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

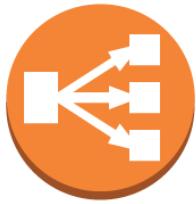
- EC2の自動復旧
 - EC2インスタンスが稼働しているAWSシステムに障害が発生した場合に、自動的にEC2インスタンス復旧する機能。
 - ネットワーク接続喪失
 - システム電源喪失
 - 物理ホストの障害
- 対応するインスタンスタイプ
 - C3, C4, M3, R3, T2インスタンス
- VPC内のインスタンス
 - EC2クラシックは未対応
 - ハードウェア専有インスタンスは未対応
- EBS-Backedインスタンスのみ

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



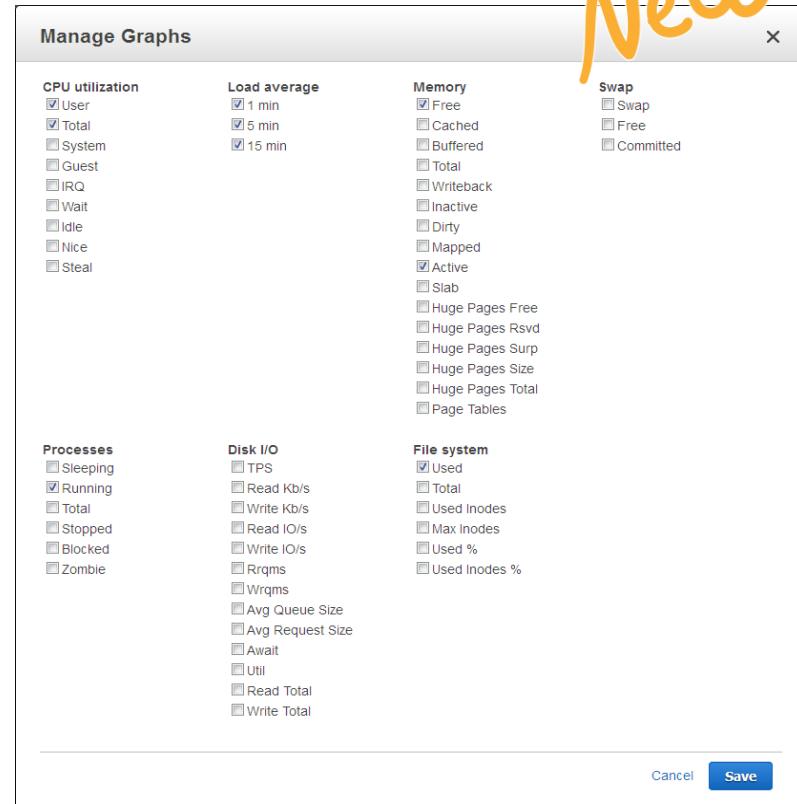
- CPUUtilization
- FreeableMemory
- SwapUsage
- FreeStorageSpace
- DiskQueueDepth
- ReadIOPS
- ReadThroughput
- ReadLatency
- NetworkReceiveThroughput
- NetworkTransmitThroughput
- WriteIOPS
- WriteThroughput
- WriteLatency
- DatabaseConnections
- BinLogDiskUsage

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)

New

- 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



http://aws.typepad.com/aws_japan/2015/12/new-enhanced-monitoring-for-amazon-rds-mysql-5-6-mariadb-and-aurora.html



CloudWatch利用イメージ 標準メトリックス監視

AWS | サービス | EC2 | CloudWatch | CloudTrail | Config | S3 | 編集 | バージニア北部 | サポート

ダッシュボード EC2 i-cbe78721

アラーム
アラーム
不足 11
OK 2
請求
ログ

選択されたメトリックス 1

EC2 > インスタンス別メトリックス

インスタンス ID (InstanceId) メトリックス名

- CPUUtilization (CPUUtilization)
- DiskReadBytes (DiskReadBytes)
- DiskReadOps (DiskReadOps)
- DiskWriteBytes (DiskWriteBytes)
- DiskWriteOps (DiskWriteOps)
- NetworkIn (NetworkIn)
- NetworkOut (NetworkOut)
- StatusCheckFailed (StatusCheckFailed)
- StatusCheckFailed_Instance (StatusCheckFailed_Instance)
- StatusCheckFailed_System (StatusCheckFailed_System)

CPUUtilization (Percent)

左軸の単位: Percent

4/27 13:00 4/27 14:00 4/27 15:00 4/27 16:00 4/27 17:00 4/27 18:00 4/27 19:00 4/27 20:00 4/27 21:00 4/27 22:00 4/27 23:00 4/28 00:00

CPUUtilization

平均 5 分間

グラフの更新

時間範囲

相対値 絶対値 ローカル (GMT+0)

開始: 12 時間前
終了: 0 分前

ズーム: 1時間 | 3時間 | 6時間 | 12時間 | 1日間 | 3

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

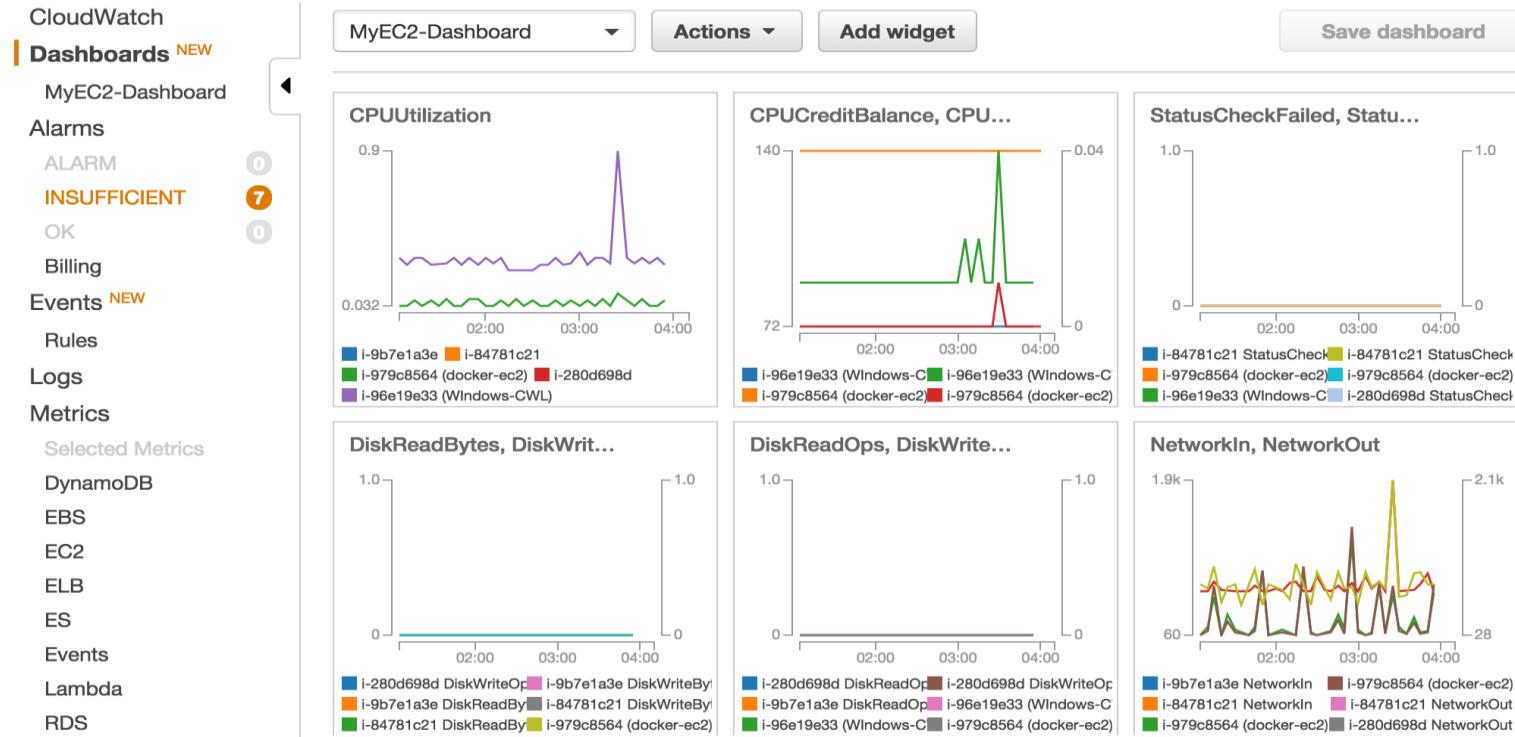
- CloudWatchはデータポイントを基準にステータスを判断
 - データポイントとはCloudWatchに送信される値(CPU値など)
 - OK / アラーム時は入力されたデータポイントを基準に状態評価
 - INSUFFICIENT時はCloudWatchにデータポイントの入力が無い状態
- “INSUFFICIENT”は必ずしも障害を表すステータスではない



CloudWatch Dashboard

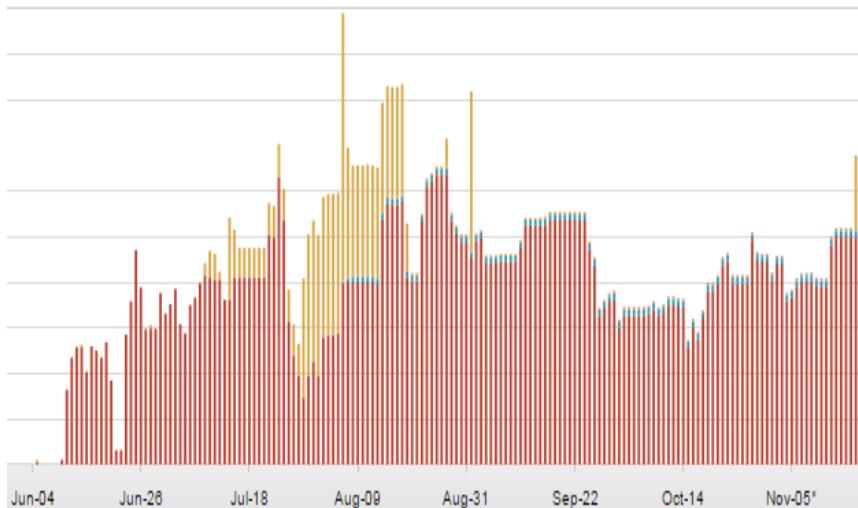
New

- 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: Billing Alarm

Description: AWS Billing Alarm

Whenever charges for: EstimatedCharges

is: \geq USD \$ 100

Actions

Define what actions are taken when your alarm changes state.

Notification

Delete

Whenever this alarm: State is ALARM

Send notification to: Select a notification list

New list Enter list

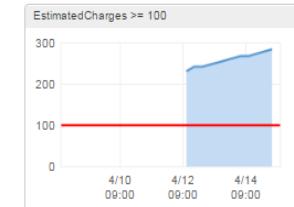
+ Notification

+ AutoScaling 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: USD

Metric Name: EstimatedCharges



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頂きます。

マネジメントコンソールへの通知

The screenshot shows the AWS Management Console interface for monitoring EC2 instances. At the top, a table lists two instances: 'Server 1' and 'Server 2'. Below the table, a message box indicates a scheduled retirement for 'Server 1'. The main content area displays detailed information for 'Server 1', including its instance ID, public DNS, and security group details. A red box highlights the '予定されているイベント' (Scheduled Events) section, which shows a single event: '予定されているイベント 1件あります' (1 scheduled event). At the bottom, a detailed view of the scheduled event is shown, including the event type ('instance-stop'), source ('ap-northeast-1c'), and description ('The instance is running on degraded hardware').

メールでの通知

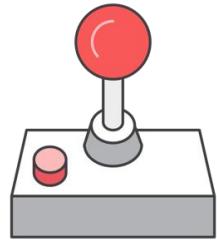
The screenshot shows an email message from AWS to the customer. The subject is 'Important: EC2 instance degradation detected'. The body of the email informs the customer about detected degradation in the underlying hardware and provides a list of affected instances. It also links to the AWS Management Console for more information. A red box highlights the '予定されているイベント 1件あります' (1 scheduled event) message, which corresponds to the event shown in the previous screenshot.

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)
 - DescribeInstanceState (API)
 - RDS
 - describe-pending-maintenance-actions (CLI)
 - DescribePendingMaintenanceActions (API)

```
aws ec2 describe-instance-status --instance-ids i-15a4417c
{
    "InstanceStatuses": [
        {
            "InstanceState": {
                "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

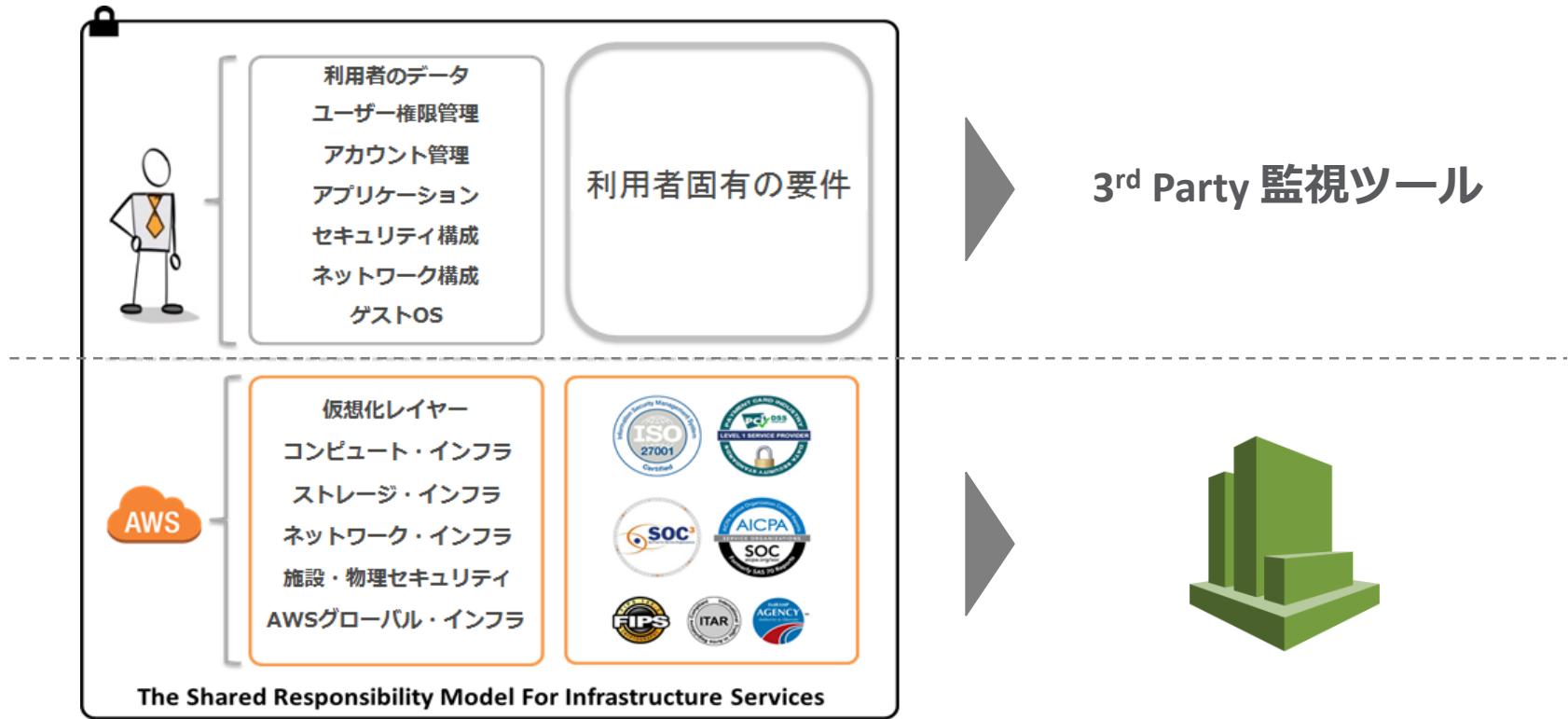
	◀◀	Apr 29	Apr 28	Apr 27	Apr 26	Apr 25	Apr 24	Apr 23	▶▶
	Region	Amazon CloudFront	Amazon CloudSearch (Singapore)	Amazon CloudSearch (Sydney)	Amazon CloudSearch (Tokyo)	Amazon CloudWatch (Singapore)	Amazon CloudWatch (Sydney)	Amazon CloudWatch (Tokyo)	Amazon DynamoDB (Singapore)
Amazon CloudFront	North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

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

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

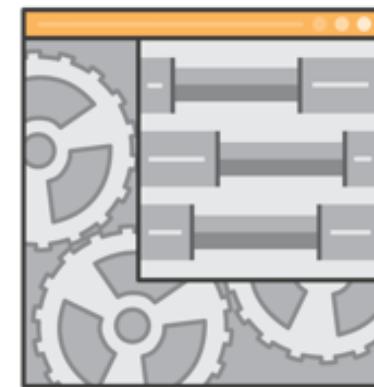
Q. 監視はCloudWatchだけで十分？

監視システムとのAmazon CloudWatch連携



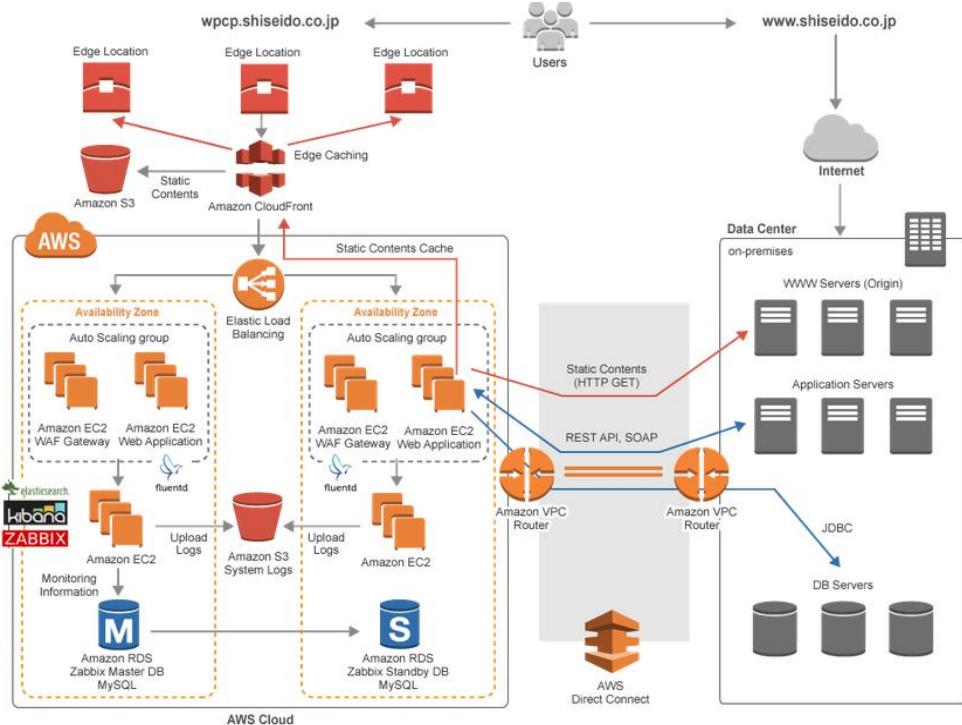
監視ツール連携の必要性

- 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

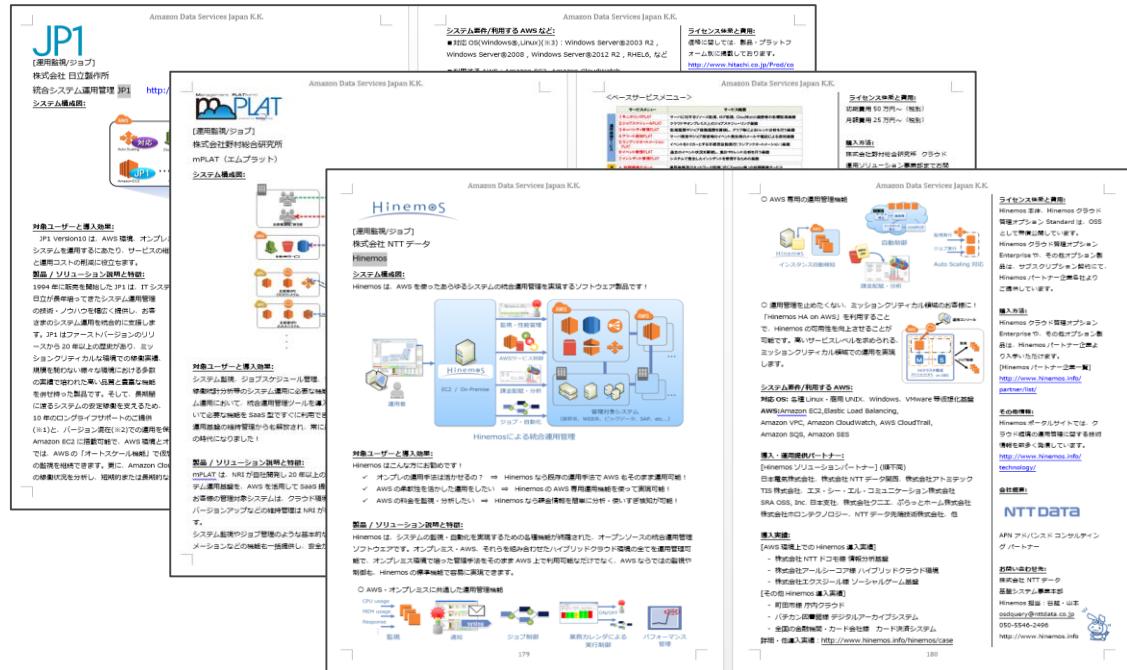
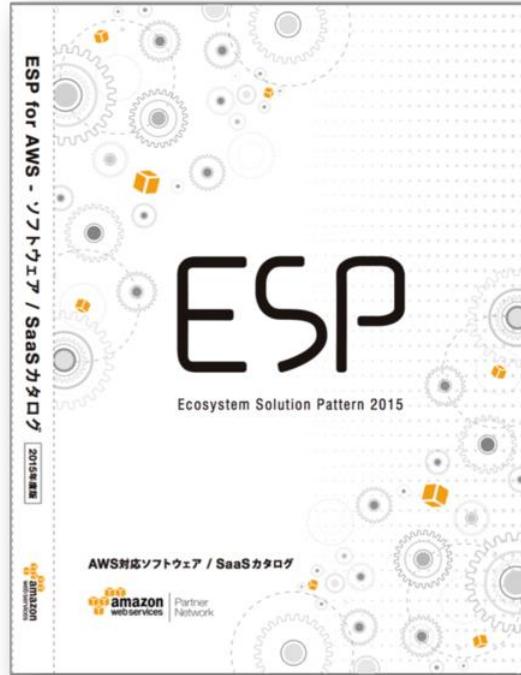
ZABBIX

Hinemos

Management PLATform
m PLAT
powered by Senju Technology

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

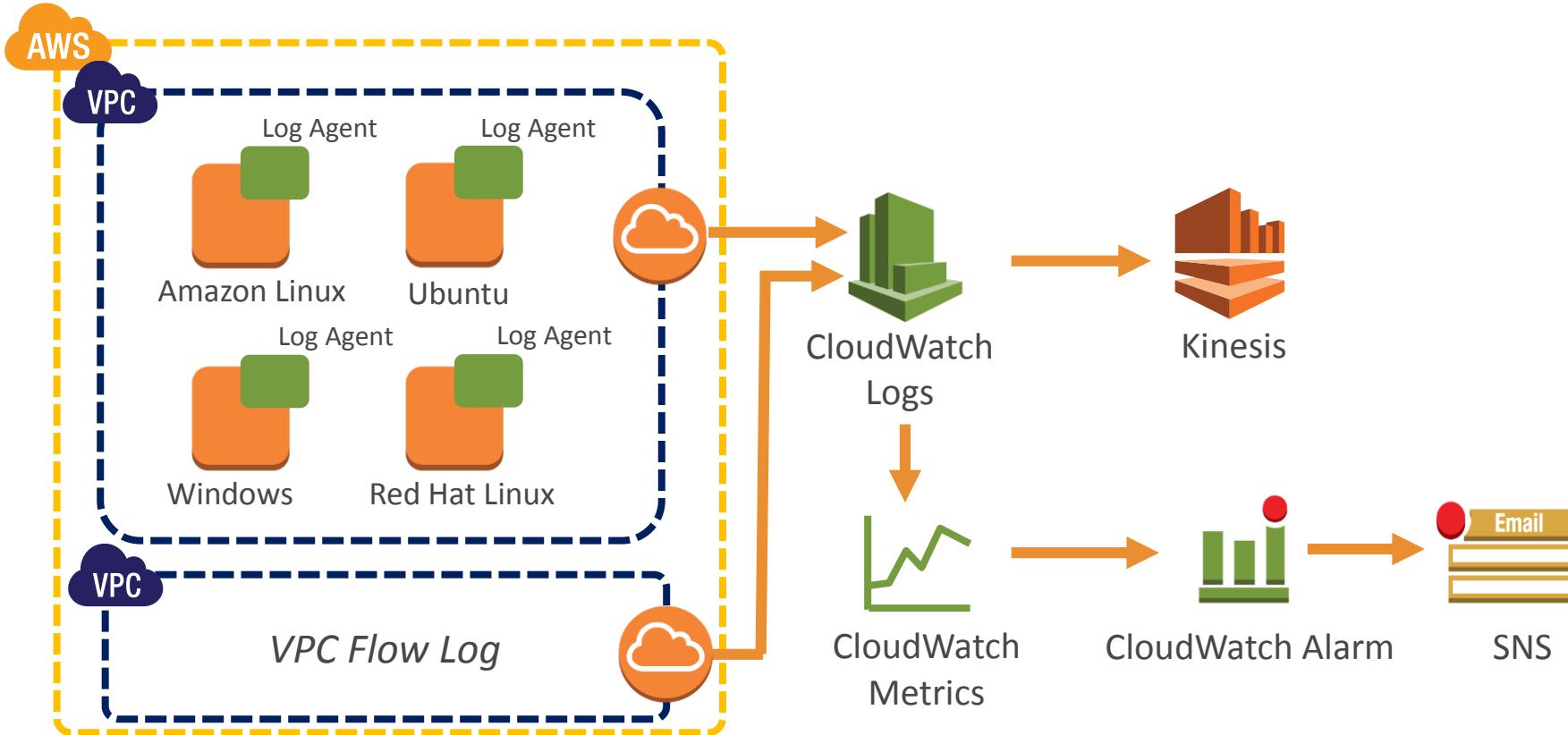


<https://aws.amazon.com/jp/solutions/partner-central/esp-catalog/>



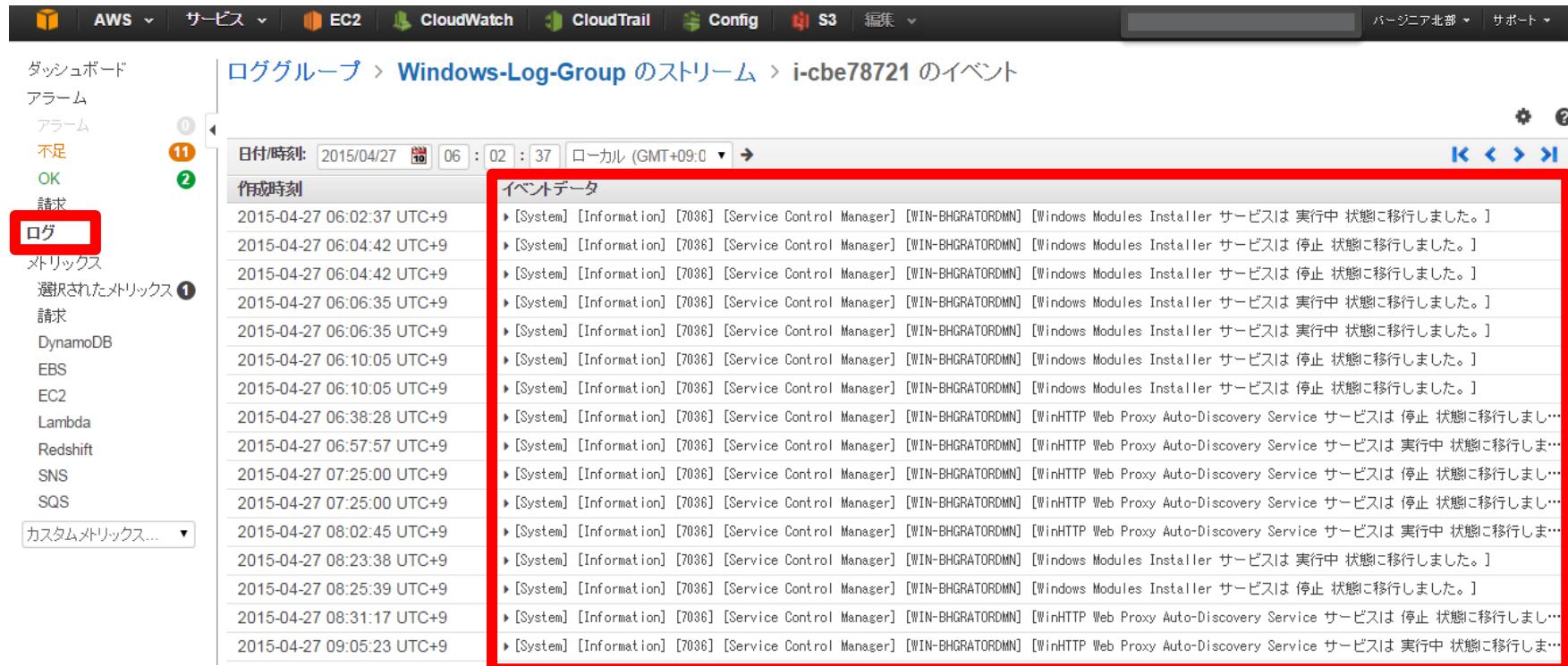
Q. ログの管理はどうしたらいい？

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 Logs interface. On the left, a sidebar lists various AWS services with 'Logs' selected. The main area shows a log group structure: 'ロググループ > Windows-Log-Group のストリーム > i-cbe78721 のイベント'. A red box highlights the list of log events on the right, which are timestamped and show service control manager activity. The log entries are as follows:

- 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 状態に移行しました。]
- 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 状態に移行しました。]
- 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 状態に移行しました。]
- 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 状態に移行しました。]
- 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 状態に移行しました。]
- 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 状態に移行しました。]
- 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 状態に移行しました。]

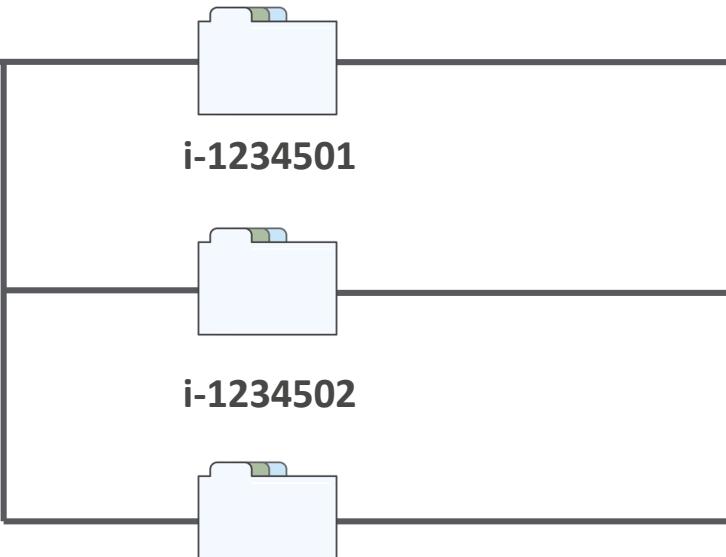
CloudWatch Logsのディレクトリ階層

Log Group



Web Server

Log Stream



i-1234503

Log Event



ログの保存期間

- CloudWatch Logsはログを永久保存可能

Log Groups

	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

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



“error”という文字列を監視

Filter Pattern: error

Metric Details

Metric Namespace: LogMetrics

[Select existing namespace](#)

Metric Name: error



Metric Value: 1

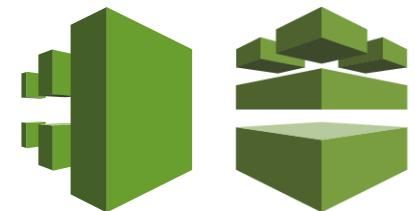


“error”という文字列の出現回数

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スに組み込む
3. CloudWatch Logsを利用してすることで、AWSプラットフォームのログを一元的に集約できる

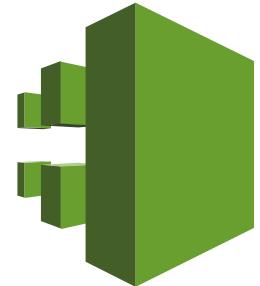
Q. AWSの運用監視をより安全にするには？



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



API call の発生状況 API call の発生状況
SNS設定の有無



The screenshot shows the AWS S3 console interface. A table lists CloudTrail log files in a bucket named 'fmrinc-cloudtrail-bucket'. The table columns are 'Name', 'Storage Class', and 'Size'. The log files are named with a timestamp and a unique identifier, such as '123456789012_CloudTrail_us-west-2_2013-11-03T21:40Z_63QlcV3Qp2609sCL.json.gz'. The storage class is 'Standard' and the size is 1 KB for the first file.

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_EseusVU7TNIeE8jS.json.gz	Standard	1.2 KB
123456789012_CloudTrail_us-west-2_2013-11-03T21:50Z_7CC05rQf5YDGf78.json.gz	Standard	1.1 KB
123456789012_CloudTrail_us-west-2_2013-11-03T23:00Z_sGNVF0FjbKfip0rh.json.gz	Standard	1.1 KB



Amazon S3



Amazon SNS

AWS CloudTrailによりロギングされるイベント

API call Event



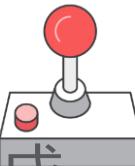
Non-API call Event



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

JSON形式での出力

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": { "Fn::GetLogGroup": "CloudWatchLogs" }
20             }
21         }
22     }
23 }
```

<p>Filter Name: CloudWatchAlarm-CloudTrail-APIActivity-ConsoleSignInFailuresMetric Filter-35PVKU305SE3</p> <p>Filter Pattern: { (\$.eventName = ConsoleLogin) & (\$.errorMessage = "Failed authentication") }</p> <p>Metric: CloudTrailMetrics / ConsoleSignInFailureCount</p> <p>Metric Value: 1</p> <p>Alarm: CloudTrailConsoleSignInFailures</p>
<p>Filter Name: CloudWatchAlarm-CloudTrail-APIActivity-EC2InstanceStateChangesMetric Filter-1Q1TJK84379GF</p> <p>Filter Pattern: { (\$.eventName = RunInstances) (\$.eventName = RebootInstances) (\$.eventName = StartInstances) (\$.eventName = StopInstances) (\$.eventName = TerminateInstances) }</p> <p>Metric: CloudTrailMetrics / EC2InstanceStateEventCount</p> <p>Metric Value: 1</p> <p>Alarm: CloudTrailEC2InstanceStateChanges</p>
<p>Filter Name: CloudWatchAlarm-CloudTrail-APIActivity-EC2LargeInstanceStateChangesMetric Filter-2V2DOYX90SA20</p> <p>Filter Pattern: { ((\$.eventName = RunInstances) (\$.eventName = RebootInstances) (\$.eventName = StartInstances) (\$.eventName = StopInstances) (\$.eventName = TerminateInstances)) && (\$.requestParameters.instanceType = *.8xlarge) (\$.requestParameters.instanceType = *.4xlarge) }</p> <p>Metric: CloudTrailMetrics / EC2LargeInstanceStateEventCount</p> <p>Metric Value: 1</p> <p>Alarm: CloudTrailEC2LargeInstanceStateChanges</p>

http://aws.typepad.com/aws_japan/2015/03/cloudtrail-integration-with-cloudwatch-in-four-more-regions.html

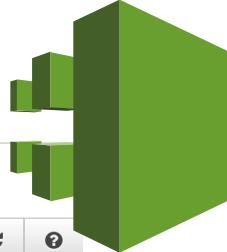


CloudTrail API lookup – マネジメントコンソール

- 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-06e19633
▶	2015-12-21, 01:18:27 PM	sakatoku	RunInstances	Ami and 7 more	ami- and 9 more
▶	2015-12-21, 01:17:03 PM	sakatoku	TerminateInstances	Instance	i-
▶	2015-12-21, 01:16:23 PM	sakatoku	ConsoleLogin		
▶	2015-12-20, 01:26:07 AM	sakatoku	RunInstances	Ami and 7 more	ami- and 9 more
▶	2015-12-20, 01:26:07 AM	sakatoku	CreateTags		i-
▶	2015-12-20, 12:50:43 AM	sakatoku	DetachUserPolicy	Policy and 1 more	arn:aws:iam::...
▶	2015-12-20, 12:46:34 AM	sakatoku	PutRolePolicy	Policy and 1 more	oneClick_CloudTrail_Cl...
▶	2015-12-20, 12:40:39 AM	sakatoku	AttachUserPolicy	Policy and 1 more	arn:aws:iam::...

CloudTrail API サンプル (RunInstances)

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

AWS access key 

Event source ec2.amazonaws.com

AWS region ap-northeast-1

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

Error code

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

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

Source IP address 27.0.3.145

Event name RunInstances

User name sakatoku

Resources Referenced (10)

ami-

Ami

i-

Instance

my_

KeyPair

eni-

NetworkInterface

mysg4win

SecurityGroup

sg-

SecurityGroup

subnet-

Subnet

vpc-

VPC

profile/AWS_Admin

InstanceProfile

arn:aws:iam::/InstanceProfiles/

profile/AWS_Admin

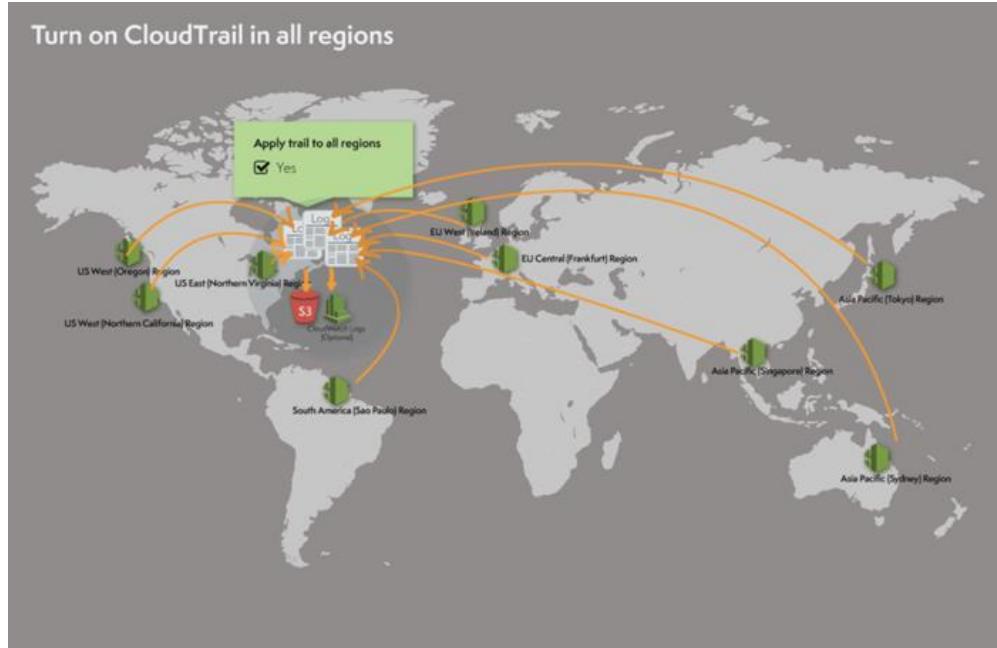
InstanceProfile

[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

http://aws.typepad.com/aws_japan/2015/12/aws-cloudtrail-update-turn-on-in-all-regions-use-multiple-trails.html

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ても簡単**



Kibanaを使ったログの可視化



Splunk App for AWS



The Splunk logo is displayed in a bold, lowercase sans-serif font. The word "splunk" is in black, with a registered trademark symbol (®) to the top right of the "k". A grey "greater than" symbol (>) is positioned to the right of the "k", partially overlapping it.

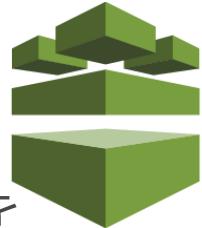
The screenshot shows the IAM Activity dashboard in the Splunk App for AWS. Key features include:

- Events|Errors:** A large display showing 161 Events and 7 Errors.
- IAM Actions:** A pie chart showing the distribution of IAM actions. The largest categories are AddRoleToInstanceProfile, RemoveRoleFromInstanceProfile, and PutRolePolicy.
- 時間別 IAM Activity:** A stacked bar chart showing IAM activity by month from July 2014 to January 2015. The total activity shows a peak in September 2014 and a smaller peak in January 2015.
- Authorized vs. Unauthorized Activity:** A table comparing the number of unauthorized and authorized events for various IAM actions.
- Detailed IAM Activity:** A table listing specific IAM events with details like event name, time, source IP, and user name.

新規サーチ		
host="ip-10-170-32-235" sourcetype="aws:cloudtrail" eventName=DeleteInstance*		
▼		
✓ 9件のイベント (15/05/28 5:40:52.000 より前)		
i	時間	イベント
>	15/02/03 15:18:26.000	<pre>{ [-] 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: { [+] }</pre>



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

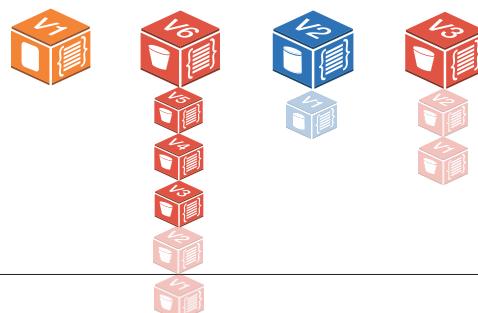
Configuration Stream

- 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



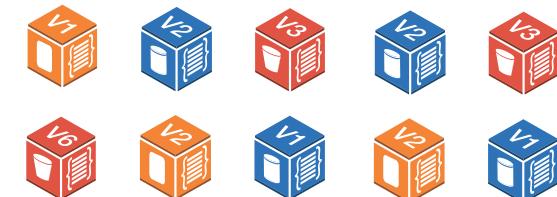
Configuration History

- 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ライガで作成され、Amazon S3 にエクスポートされる



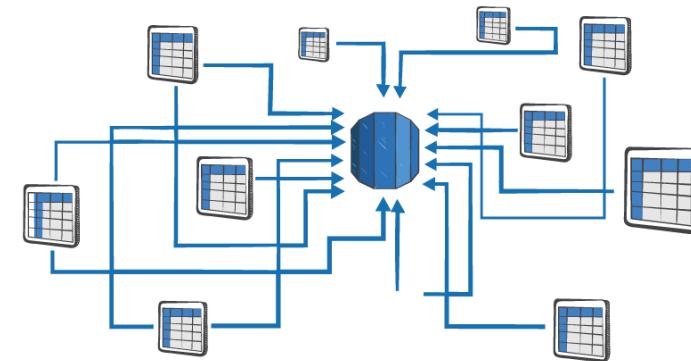
Snapshot @ 2014-11-12, 2:30pm

リレーションシップ

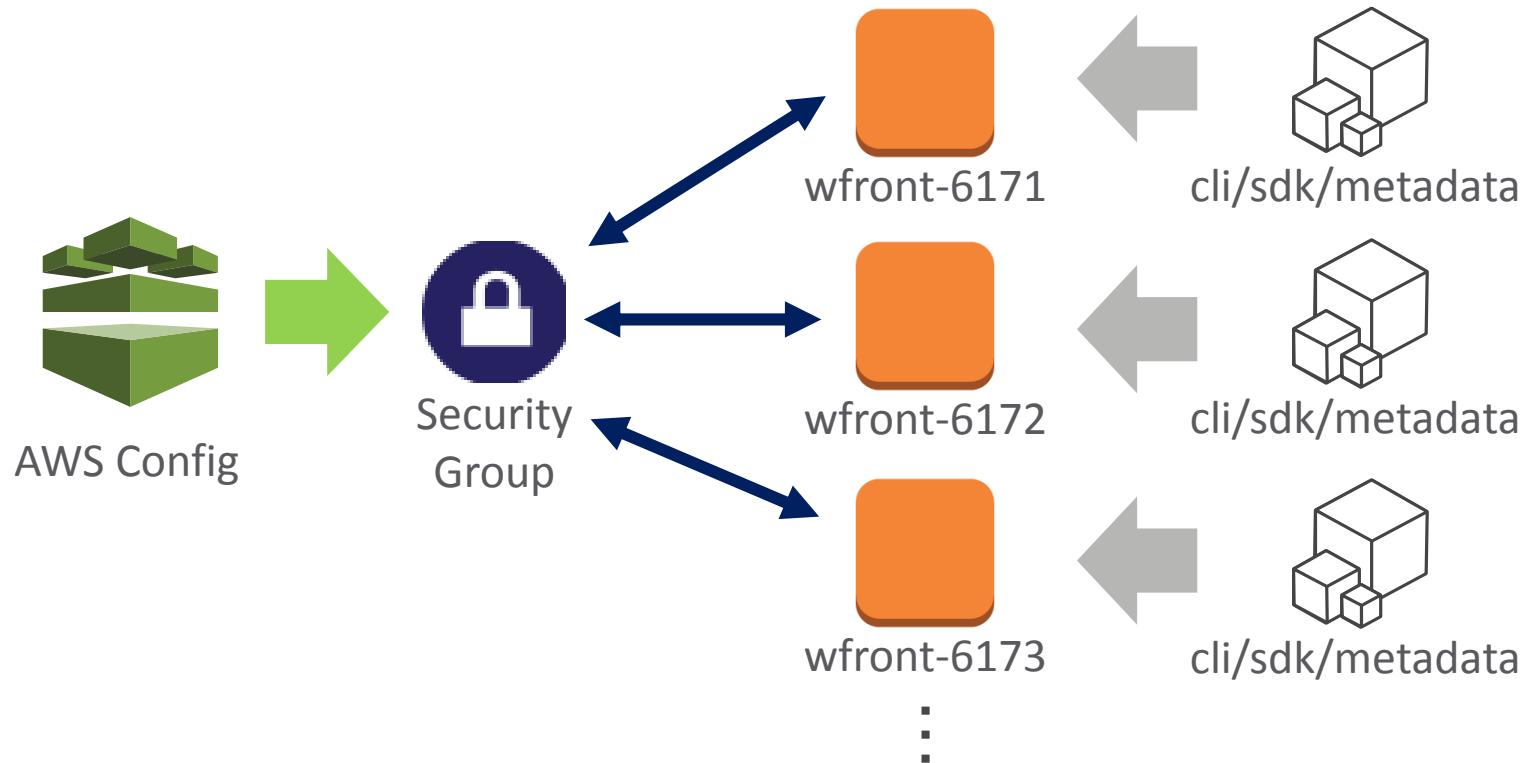
- アカウント内のAWSリソース間の関係
- 双方向の依存関係が自動的に割り当てられる

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

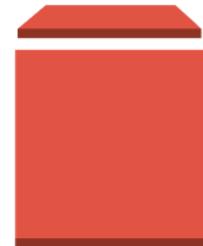
- 現在AWS Configが対応しているのは下記5サービス



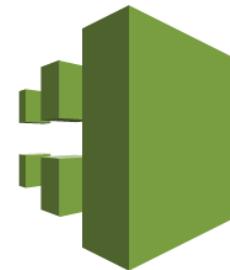
Amazon EC2
Instance, ENI...



Amazon VPC
VPC, Subnet...



Amazon EBS
Volumes



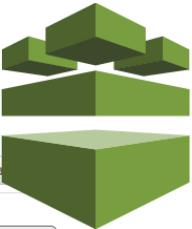
AWS CloudTrail



AWS IAM

※2015年12月25日時点

現在の構成の確認



EC2 Instance i-cbe78721

Manage

Timeline (6 changes):

- 26th November 2014 6:38 PM
- 26th November 2014 6:49 PM
- 26th November 2014 7:13 PM
- 26th November 2014 8:23 PM
- 26th November 2014 8:28 PM
- 26th November 2014 8:30 PM (Now)

Configuration Details (6 changes):

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

Resource type: AWS::EC2::Instance

Resource ID: ██████████

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: ██████████

Private Ips: ██████████

Public DNS: ██████████

AMI ID: ami-5c17af34

Platform: windows

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

Lifecycle: null

Monitoring: disabled

Now: November 26, 2014 8:30 PM

Apply

Relationships

Changes (8)

構成詳細 (highlighted in red box)

リレーション (highlighted in green box)

変更 (highlighted in blue box)

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 Resource identifier (optional)

Include deleted resources

Tag Tag key Tag value (optional)

Look up

Choose the  icon to see Config timeline for a resource.

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



i-02b0cff2 Deleted

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

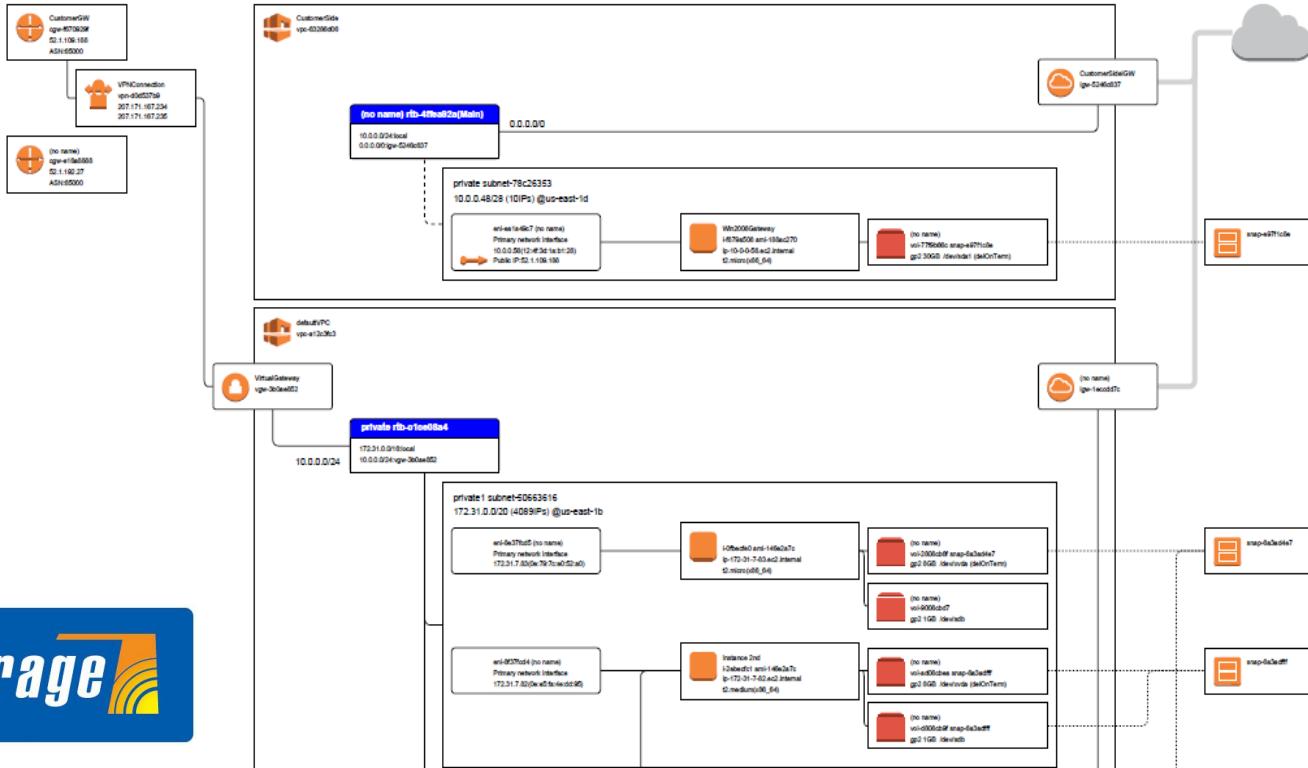
Logstorageによる可視化



AWS Config snapshot Report



Snapshot created: 2015/05/19 10:29:08 +0900
data2



Logstorage

amazon
web services

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

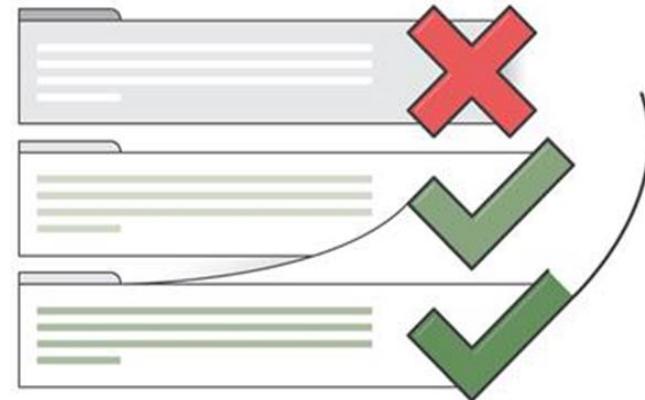
- AWS Config Rules
 - 準拠すべきルールを事前に設定し、その内容に沿った構成変更が行われているかをルールに従い評価
 - ✓ 全てのEBCボリュームが暗号化されているか
 - ✓ EC2インスタンスが適切にタグ付されているか
 - ✓ Elastic IP address(EIP)がインスタンスにアタッチされているか

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
- ✓ タグが付けられれているか
- ✓ ポートが適切に設定されているか(SG)

encrypted-volumes	cloudtrail-enabled	eip-attached
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.	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.	Checks whether Elastic IP addresses that are allocated for use in a VPC are attached to EC2 instances.
restricted-ssh	ec2-instances-in-vpc	required-tags
Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.	Checks whether your EC2 instances belong to a virtual private cloud (VPC). Optionally, you can specify the VPC ID to associate with your instances.	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.
restricted-common-ports		
Checks whether security groups that are in use disallow unrestricted incoming TCP traffic to the specified ports.		

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"/> Key	<input type="text"/> 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 EC2 Instance

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

Parameters

tag1Key: CostCenter

tag1Value: null

tag2Key: null

tag2Value: null

tag3Key: null

tag3Value: null

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- 	Compliant	
EC2 Instance	i- 	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-1:65897835: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-10-20-7-52.internal
Private IPs	10.0.20.72
Public DNS	null
AMI ID	ami-5c17af34
Platform	windows
Launch time	2014-11-26T11:25:36.000Z
Lifecycle	null
Monitoring	disabled

まとめ

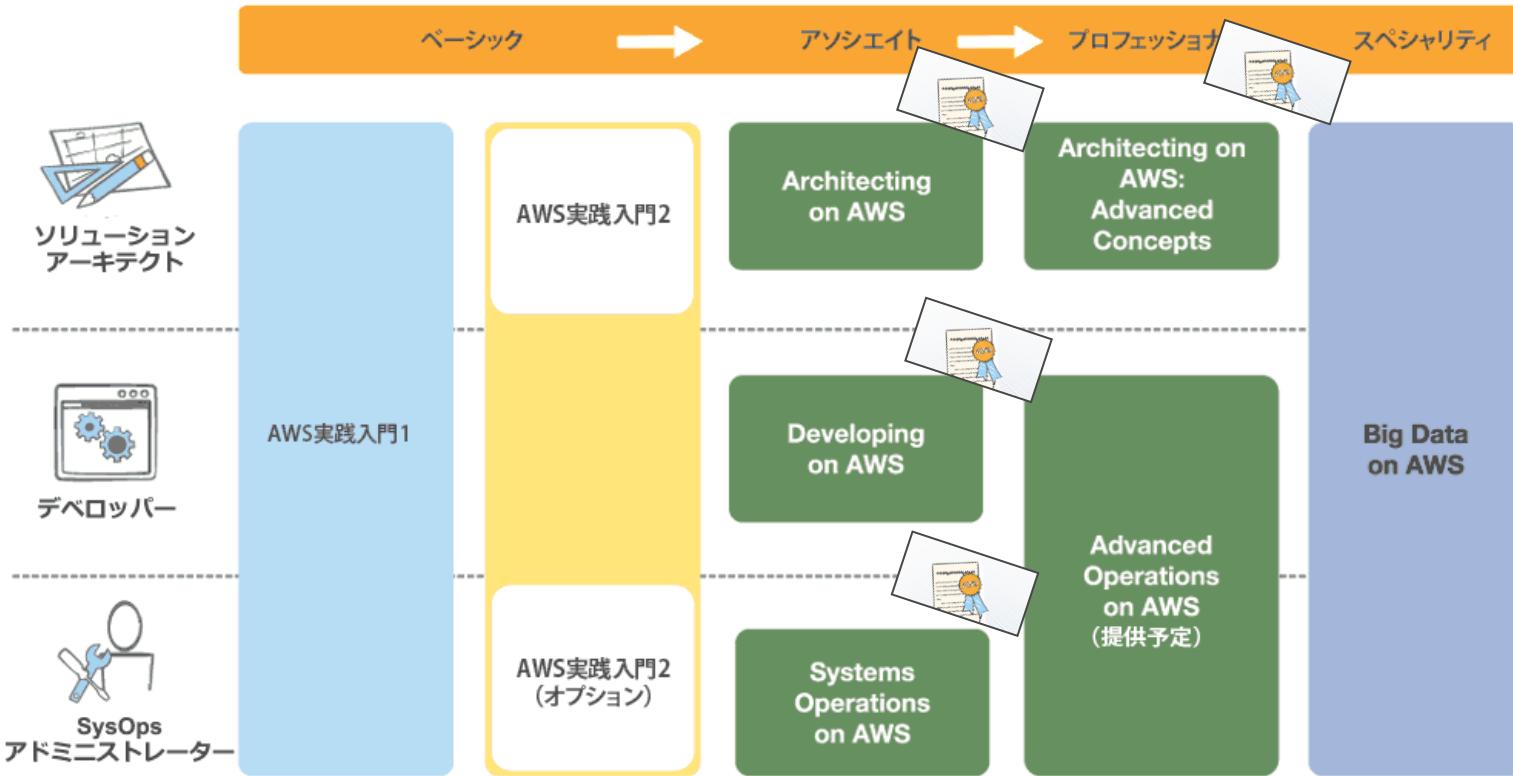
- CloudWatchをうまくご利用頂くことで、クラウドで必要な監視を実装可能
- 必要に応じて3rd Party監視ツールとの連携
- ユーザ オペレーションのロギングはCloudTrailを有効化することで対応可能
- システム全体の構成管理にはAWS Configを利用するこ
とで運用負荷軽減に結びつく
- ログの可視化に関してはAPNパートナー様のソリュー
ションと連携する

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、
- DoorKeeper: OpsJAWSコミュニティ
 - <https://opsjaws.doorkeeper.jp/>



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



検索

もしくは <http://on.fb.me/1vR8yWm>

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！



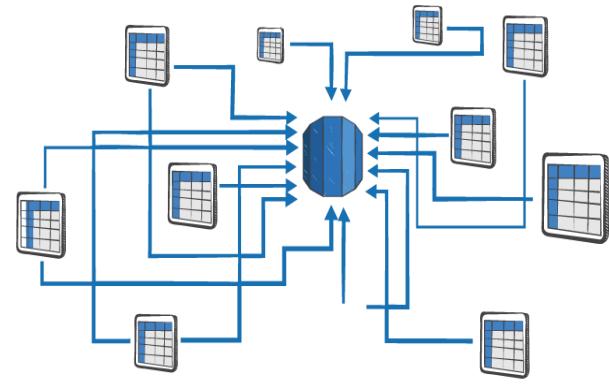
システム基盤運用で考えるポイント



Monitoring
監視



Logging
ロギング



Configuration
構成管理