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

amazon web services

自己紹介

酒徳 知明(さかとく ともあき)

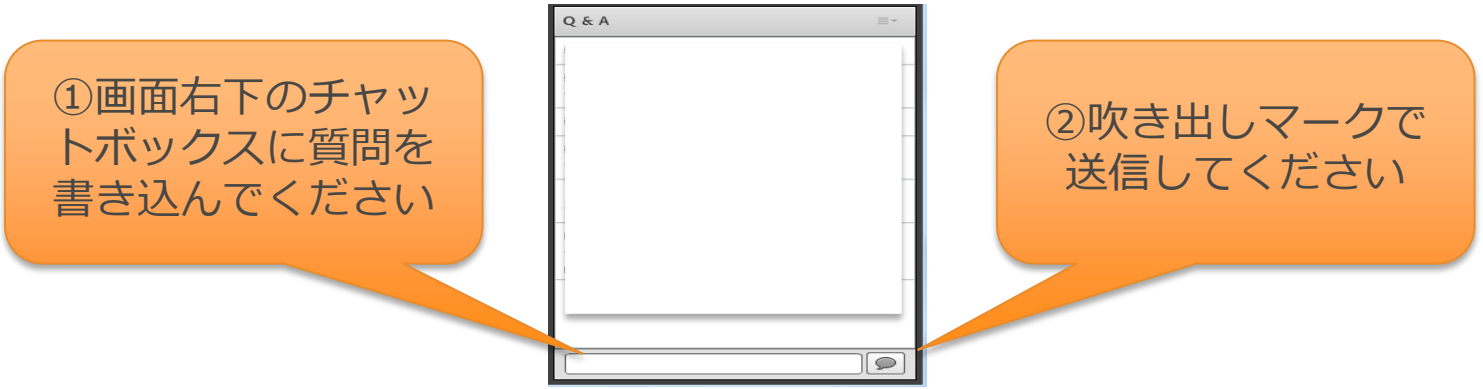
エコシステム ソリューション部
パートナー ソリューション アーキテクト

- 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。



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。

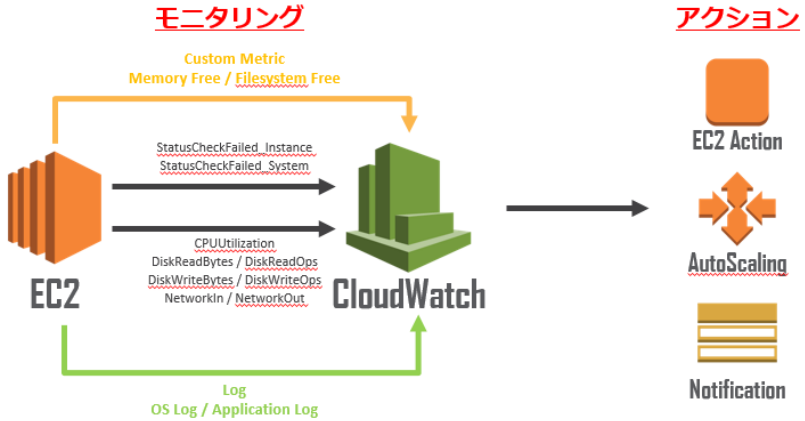
AWSの運用監視

- 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
```

https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/DeveloperGuide/publishingMetrics.html

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

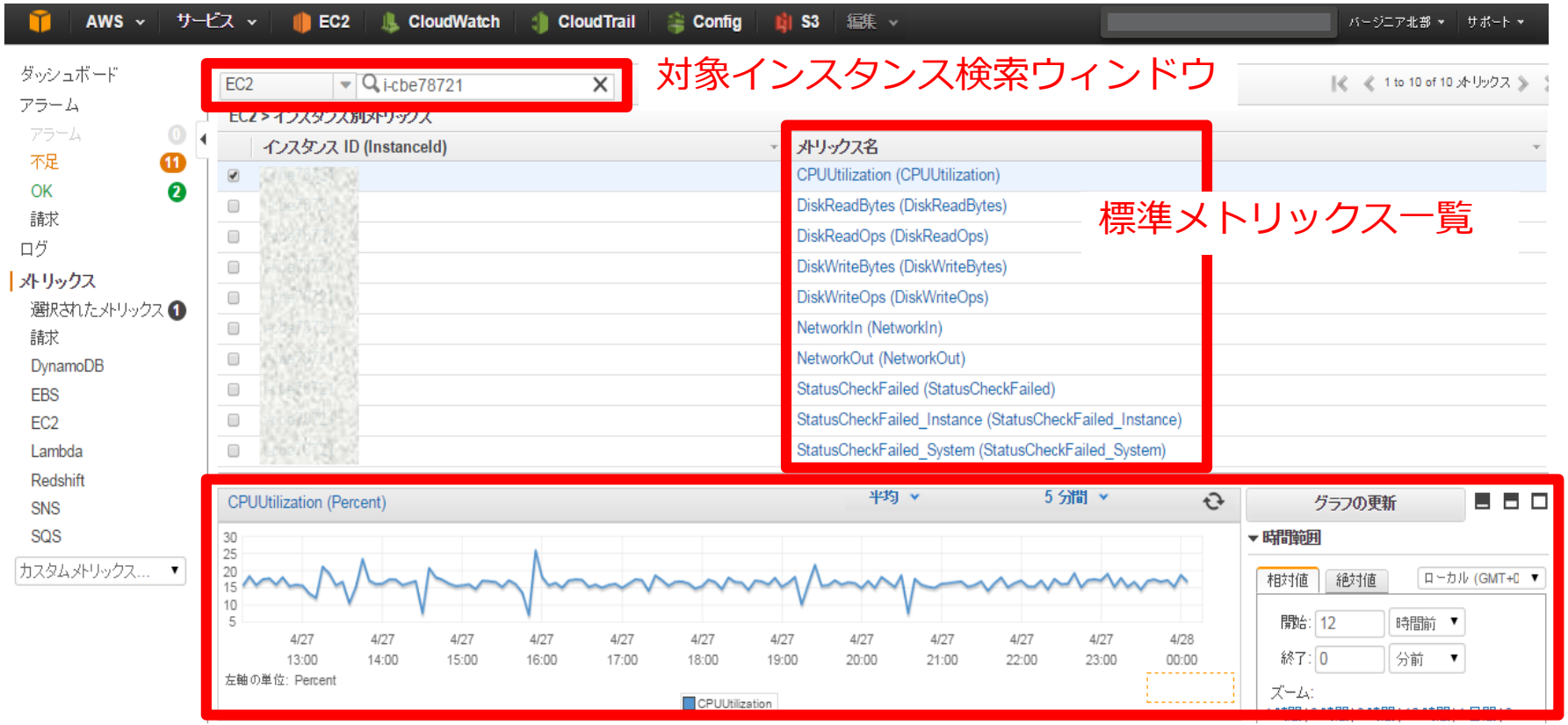
統計	説明
Minimum	指定された期間に認められた最小値です。この値を用いて、アプリケーションの低ボリュームのアクティビティを判断できます。
Maximum	指定された期間に認められた最大値です。この値を用いて、アプリケーションの高ボリュームのアクティビティを判断できます。
Sum	該当するメトリックスで加算されたすべての合計値です。この統計は、メトリックスの合計ボリュームを判断するのに役立ちます。
Average	指定した期間の Sum/SampleCount の値です。この統計を Minimum および Maximum と比較することで、メトリックスの全容、および平均使用量がどれくらい Minimum と Maximum に近いかを判断できます。この比較は、必要に応じていつ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

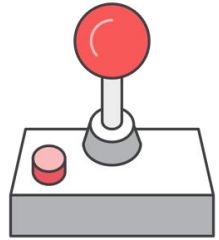
http://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

CloudWatch の始め方

CloudWatch利用イメージ 標準メトリックス監視

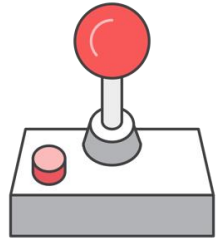


Amazon CloudWatchを使った死活監視



- 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

Amazon RDS

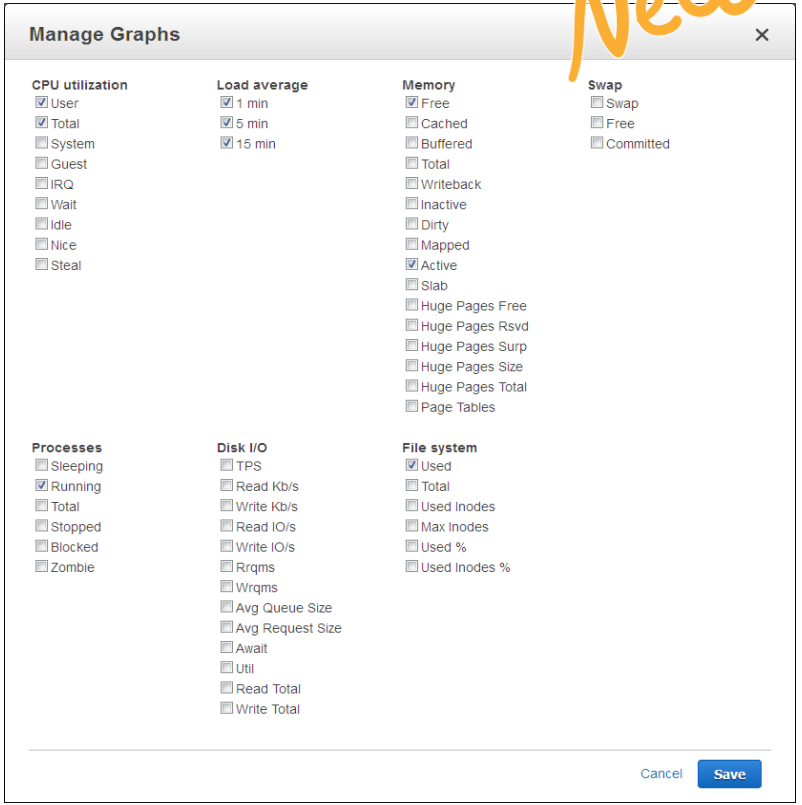
- CPUUtilization
- FreeableMemory
- SwapUsage
- FreeStorageSpace
- DiskQueueDepth
- ReadIOPS
- ReadThroughput
- ReadLatency
- NetworkReceiveThroughput
- NetworkTransmitThroughput
- WriteIOPS
- WriteThroughput
- WriteLatency
- DatabaseConnections
- BinLogDiskUsage

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

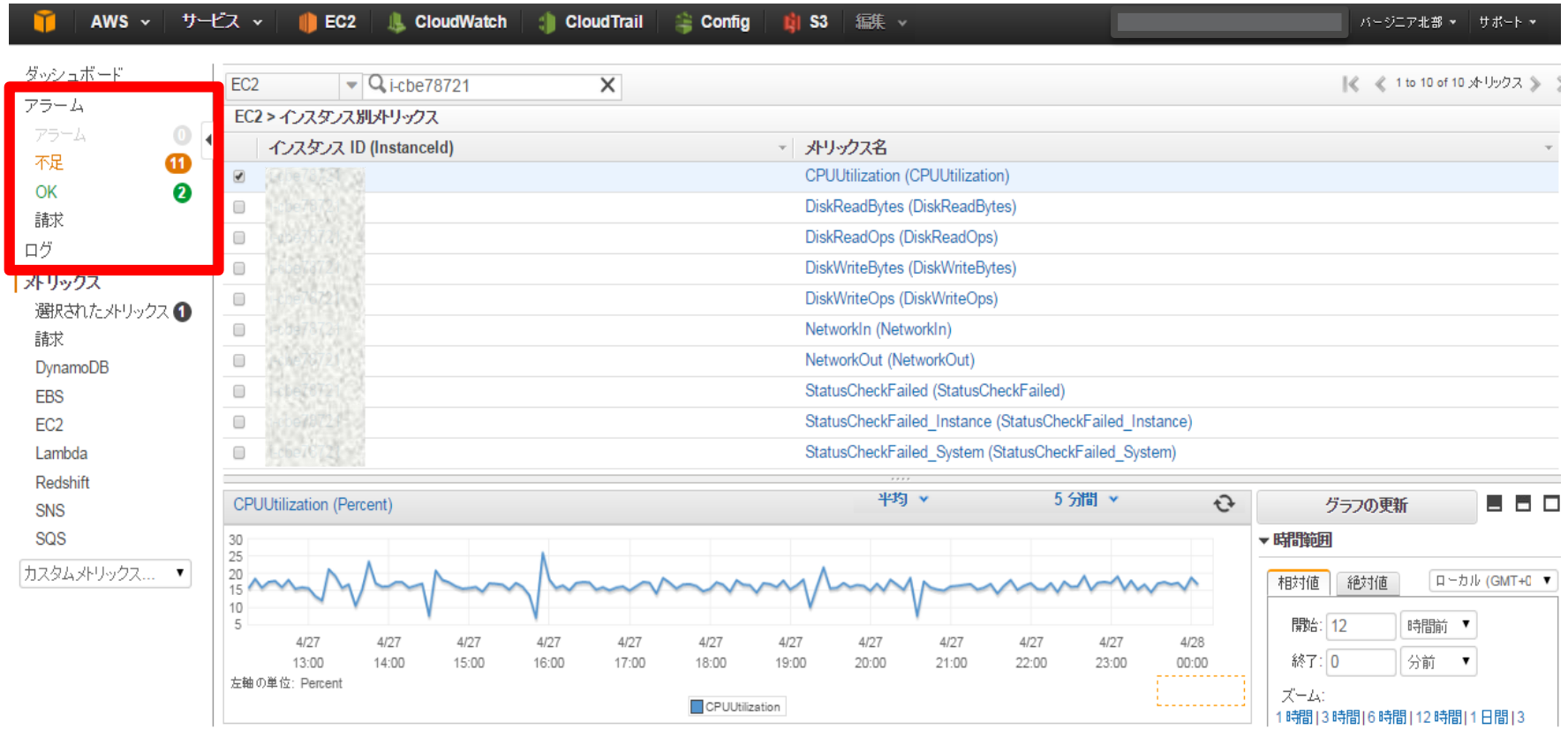
New



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

amazon web services

CloudWatch利用イメージ 標準メトリックス監視



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

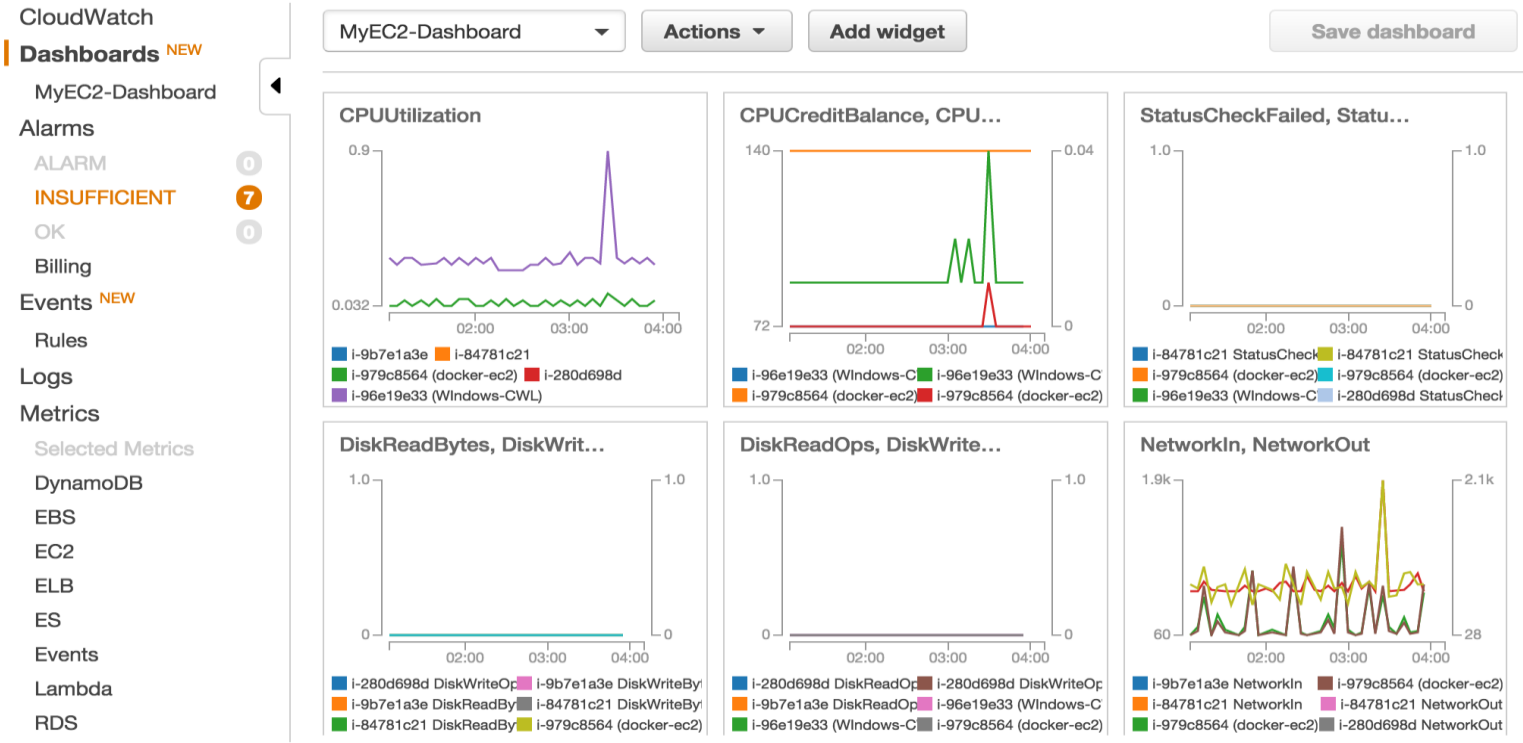
- CloudWatchはデータポイントを基準にステータスを判断
  - データポイントとはCloudWatchに送信される値(CPU値など)
  - OK / アラーム時は入力されたデータポイントを基準に状態評価
  - INSUFFIENT時は**CloudWatchにデータポイントの入力が無い状態**

→ **“INSUFFICIENT”は必ずしも障害を表すステータスではない**

CloudWatch Dashboard

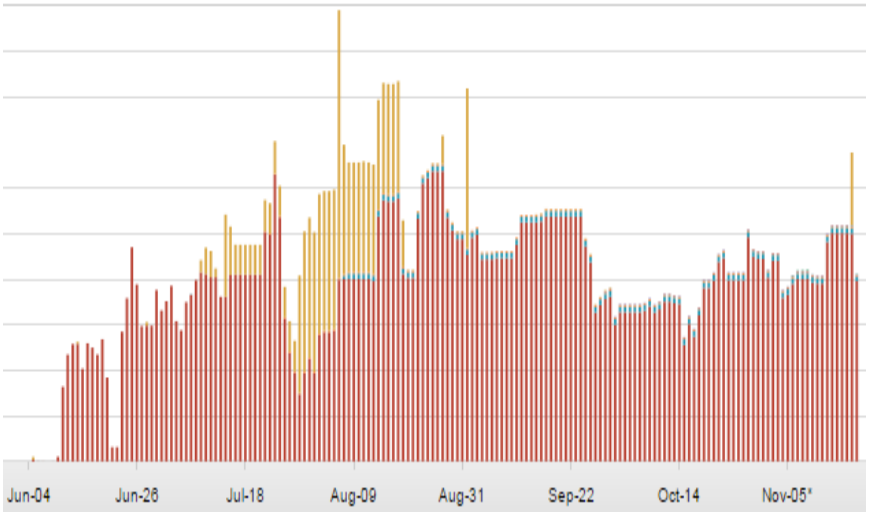
New

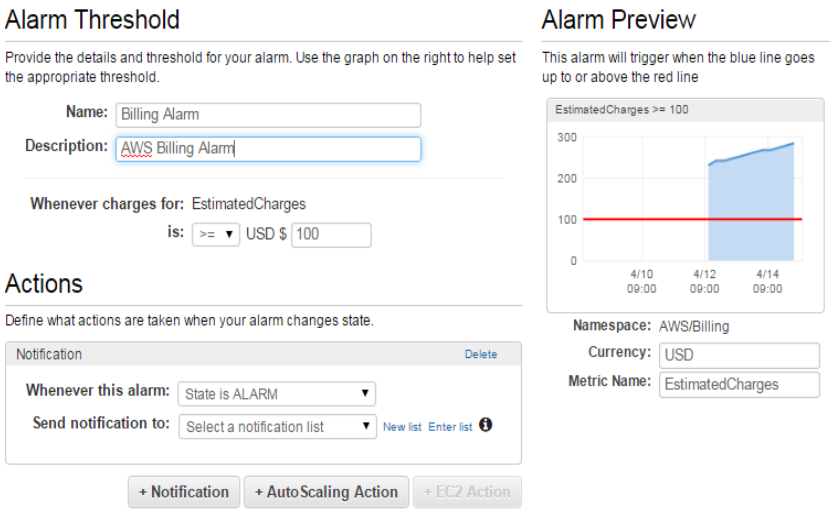
- 運用にあったメトリックス ダッシュボードが利用可能



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





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

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)

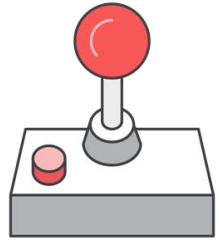
http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/monitoring-instances-status-check_sched.html

メンテナンスイベントの監視

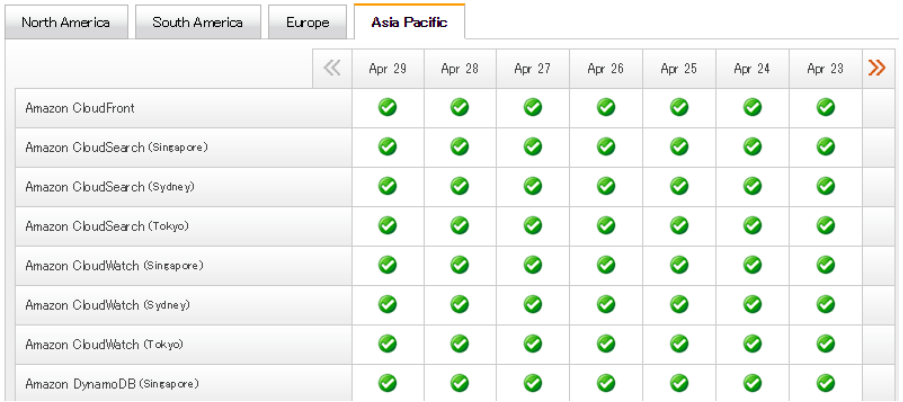
- メンテナンスイベント取得にはCLI/APIが便利
  - EC2
    - describe-instance-status (CLI)
    - DescribeInstanceStatus (API)
  - RDS
    - describe-pending-maintenance-actions (CLI)
    - DescribePendingMaintenanceActions (API)

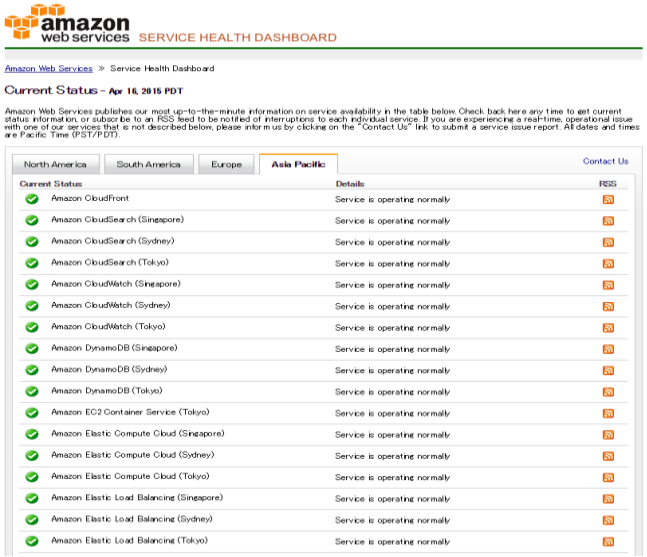
```
aws ec2 describe-instance-status --instance-ids i-15a4417c

{
    "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

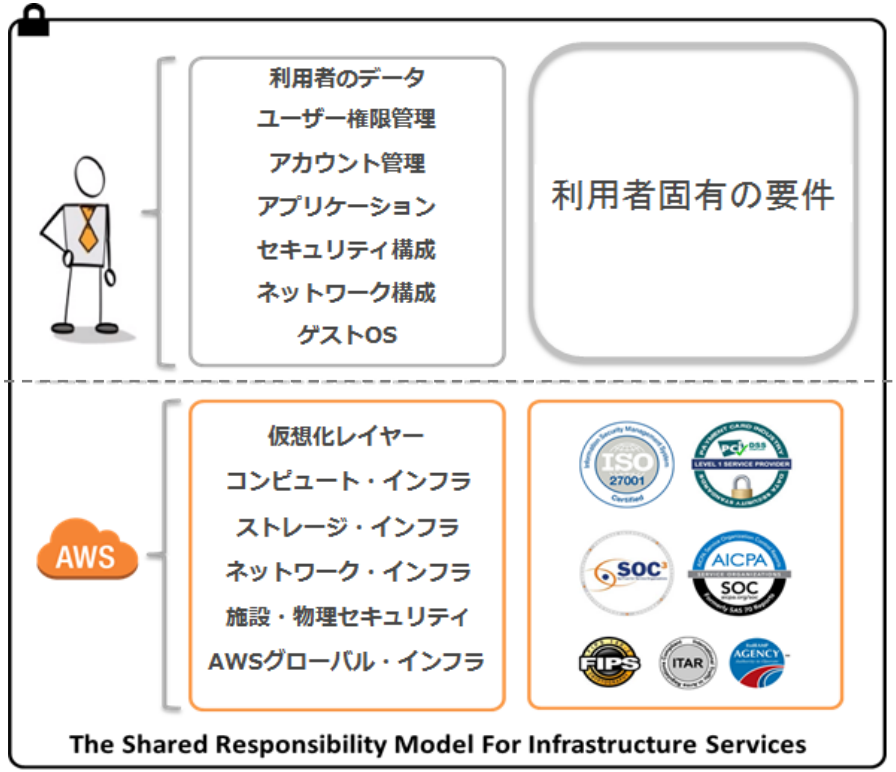




http://status.aws.amazon.com/

Q. 監視はCloudWatchだけで十分？

監視システムとのAmazon CloudWatch連携



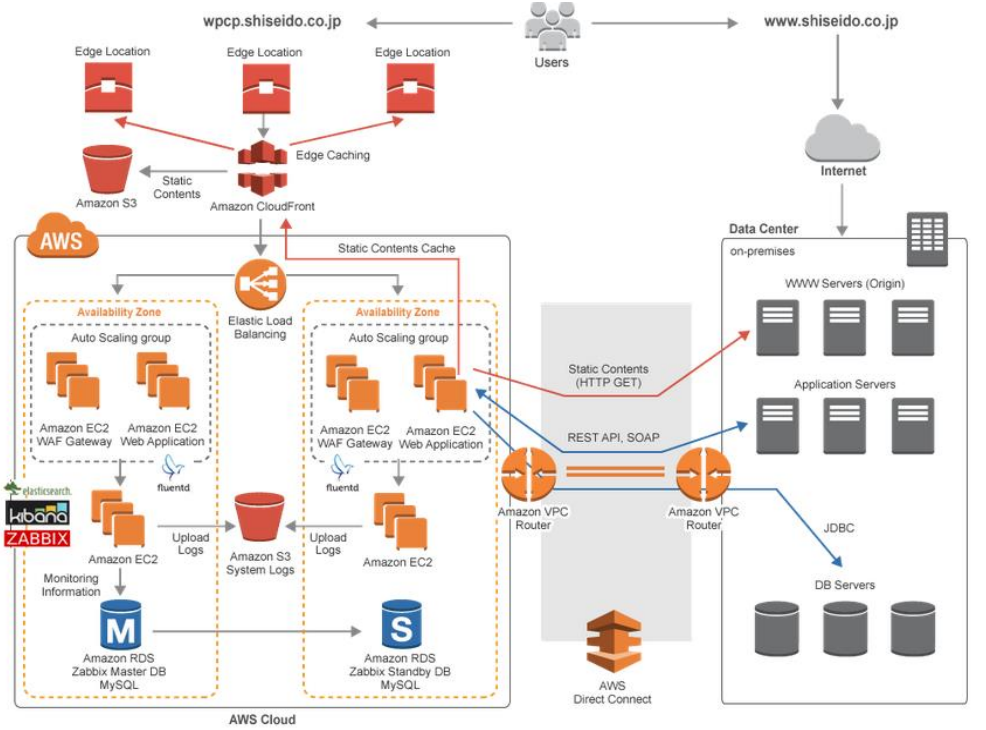
3rd Party 監視ツール

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

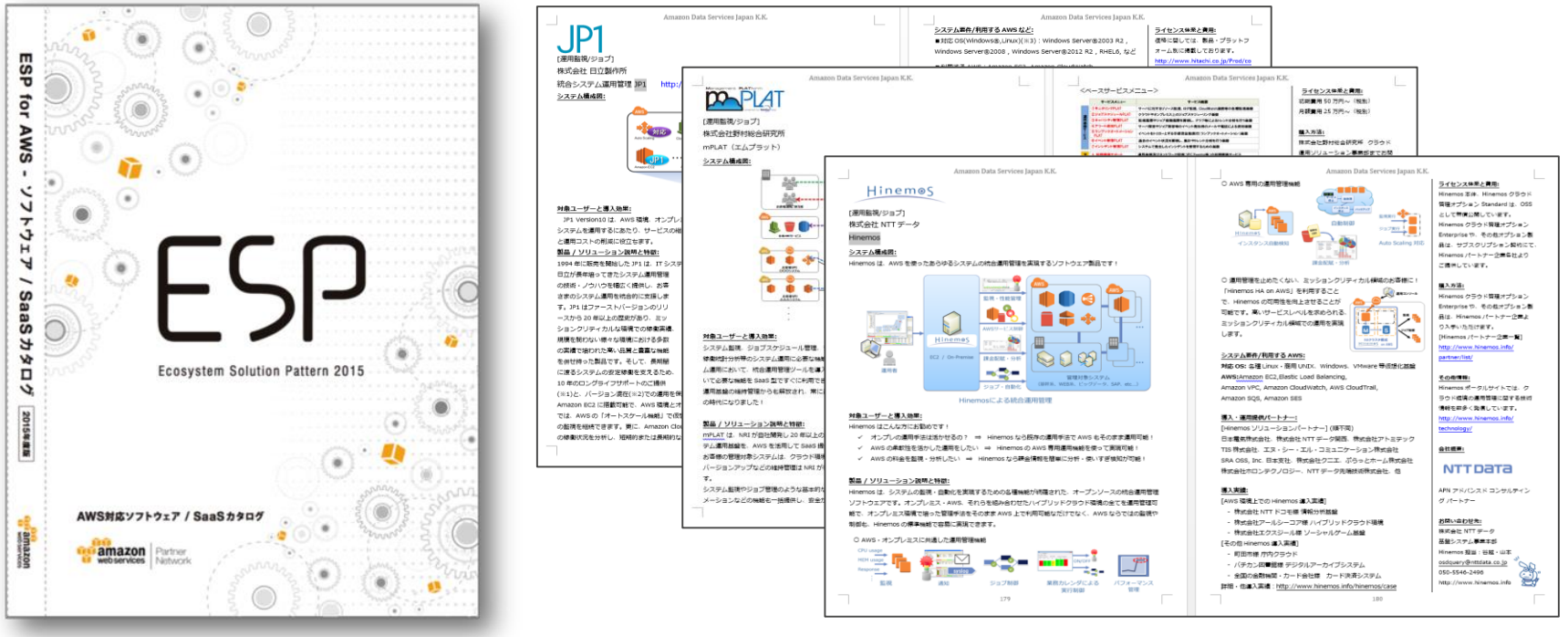
ZABBIX　Hinemos　mPLAT

mackerel　JP1

http://aws.amazon.com/jp/solutions/case-studies/shiseido/

amazon web services

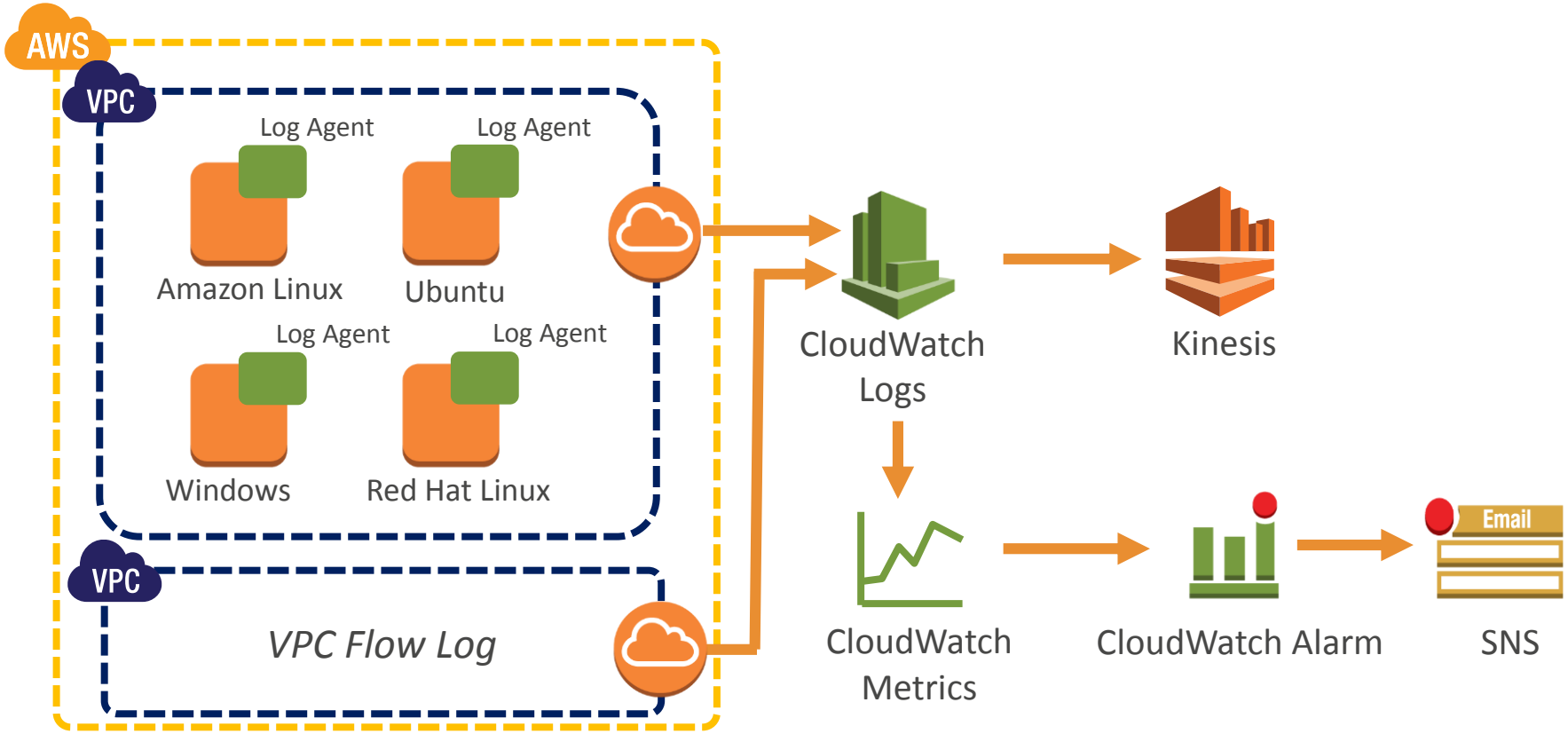
ESP(Ecosystem Solution Pattern)カタログ 無料配布
2015年度版 AWS対応ソフトウェア/SaaSガイド



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

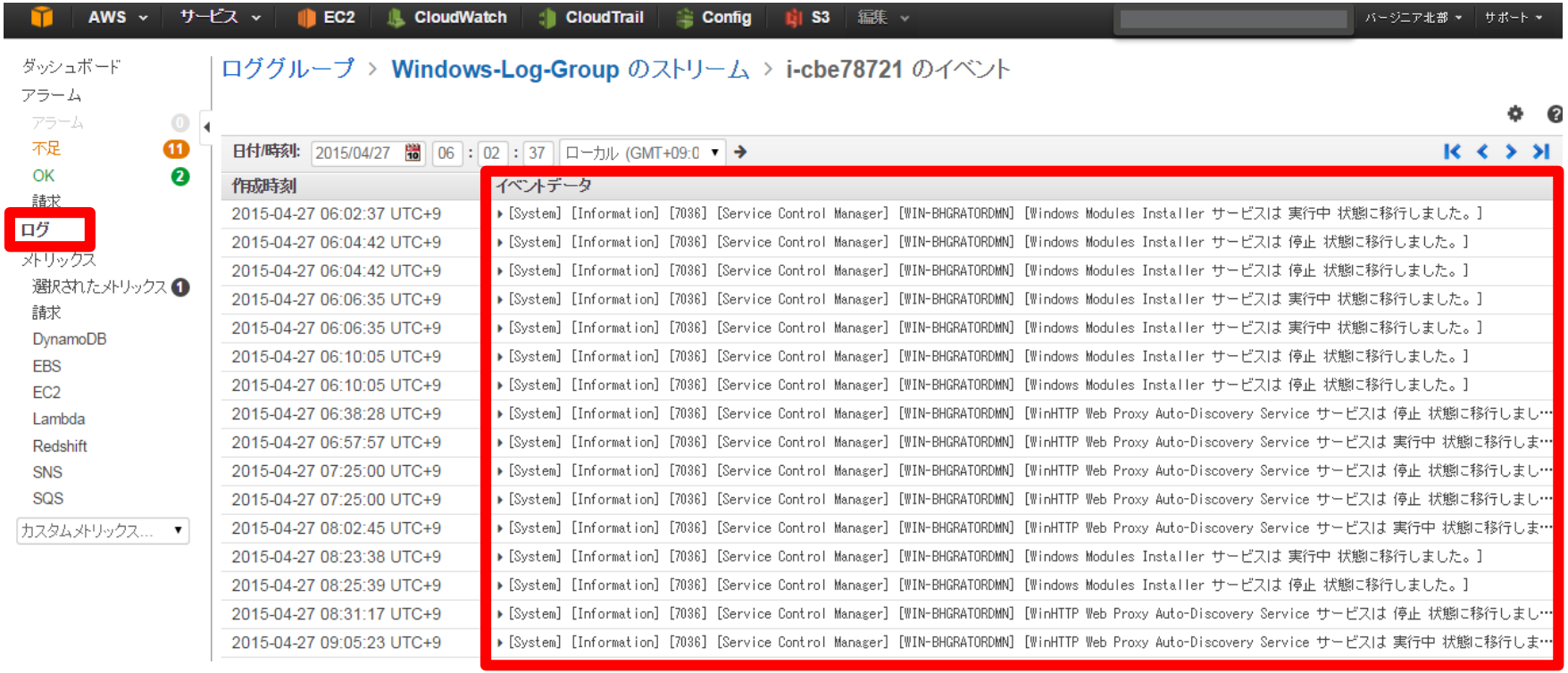
Q. ログの管理はどうしたらいい？

CloudWatch Logs を使ったログ監視

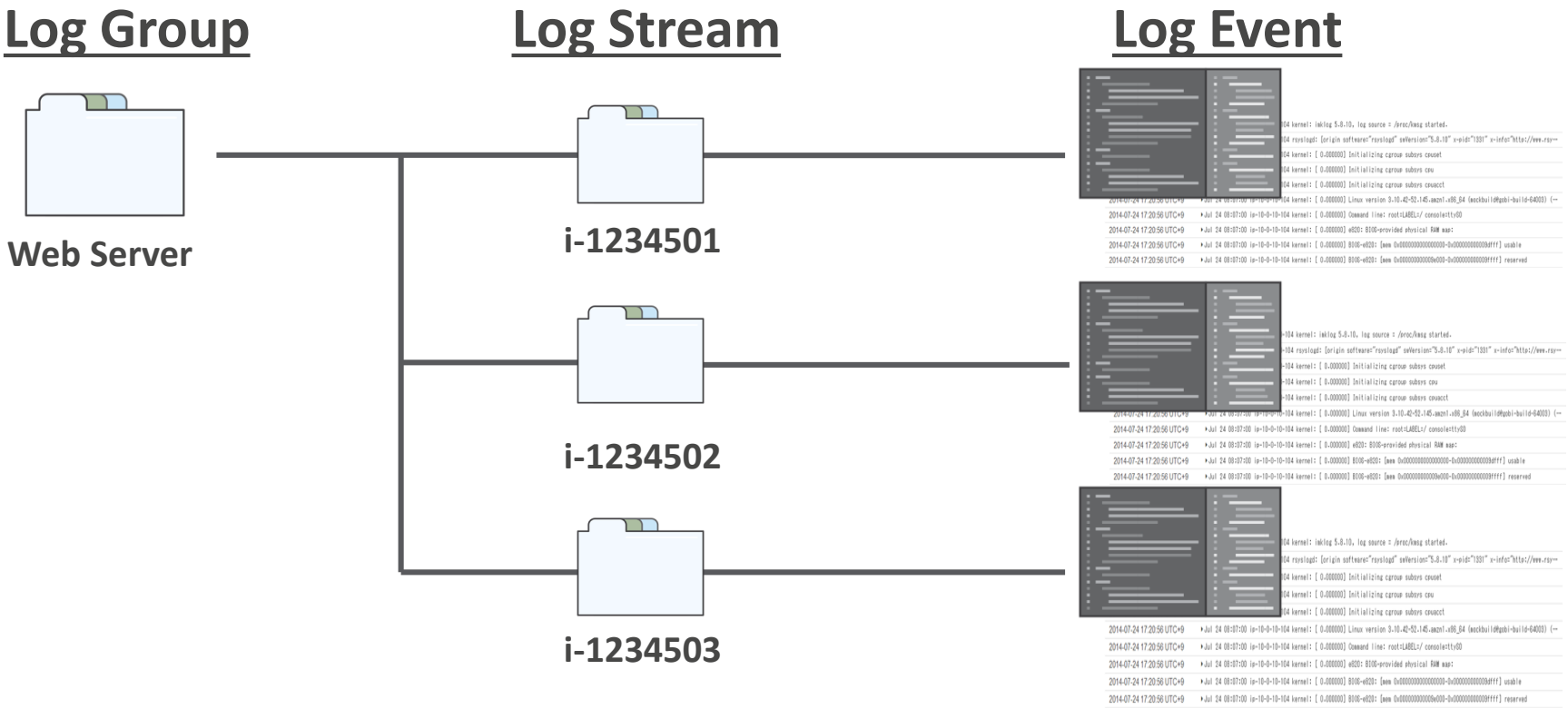


ログモニタリングイメージ

- 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

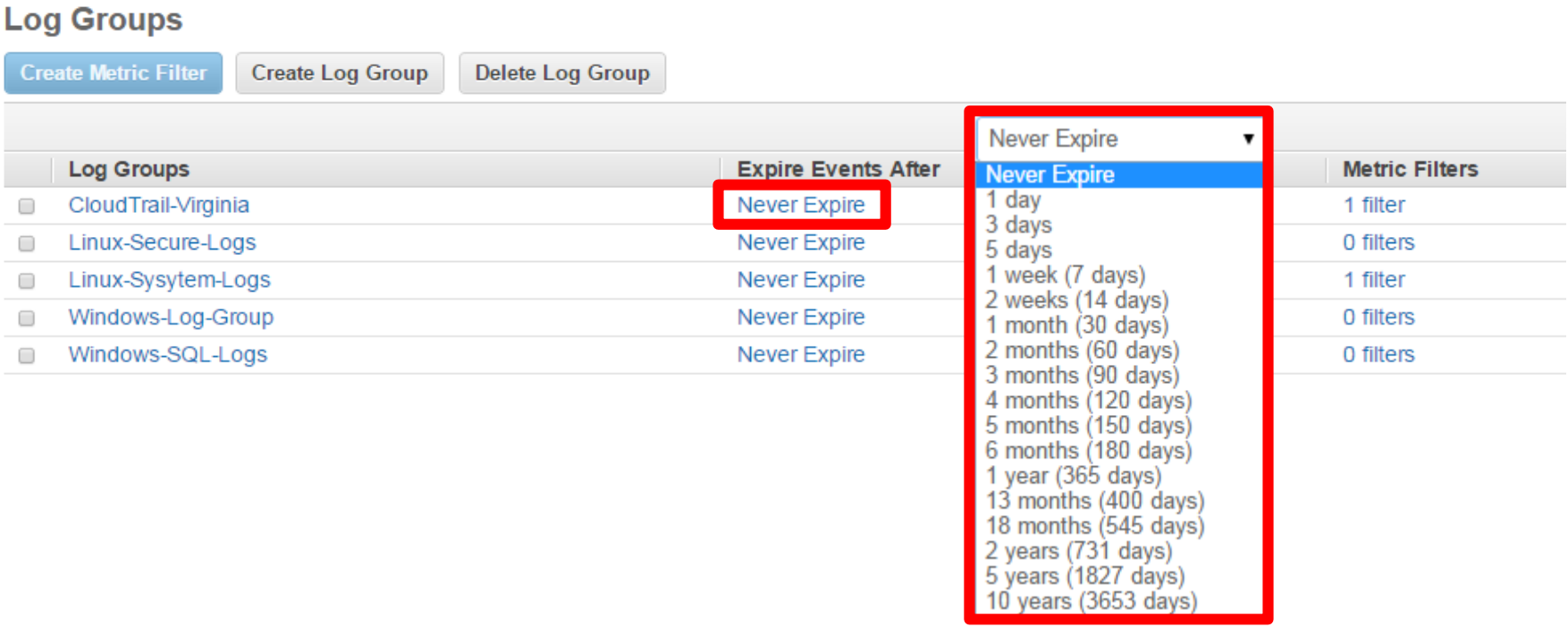


CloudWatch Logsのディレクトリ階層



ログの保存期間

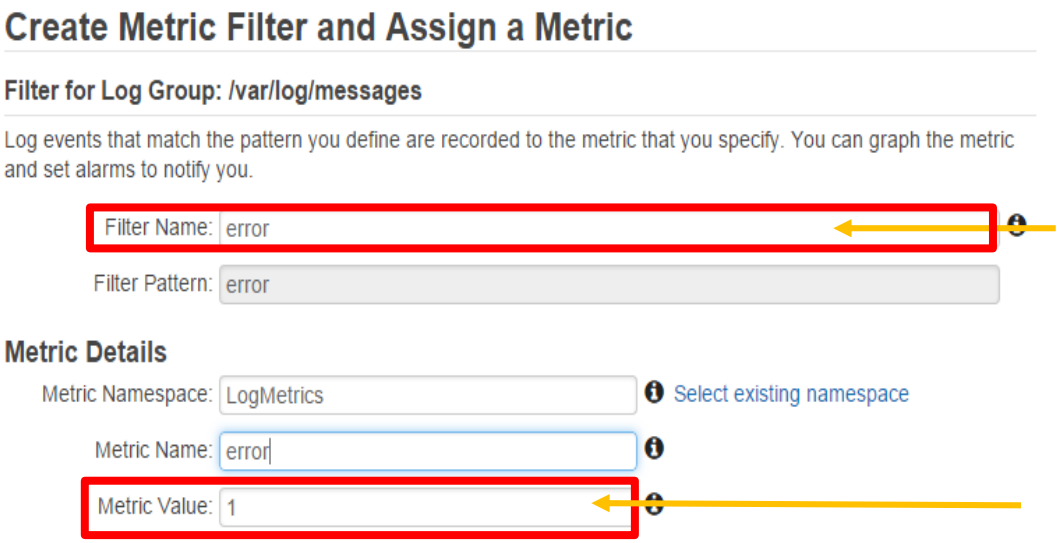
- CloudWatch Logsはログを永久保存可能



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**



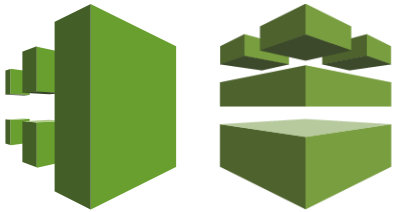
“error”という文字列を監視

“error”という文字列の出現回数

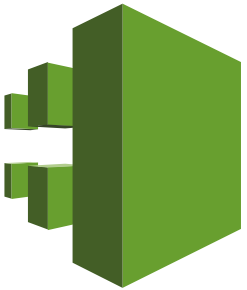
AWS監視のまとめ

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

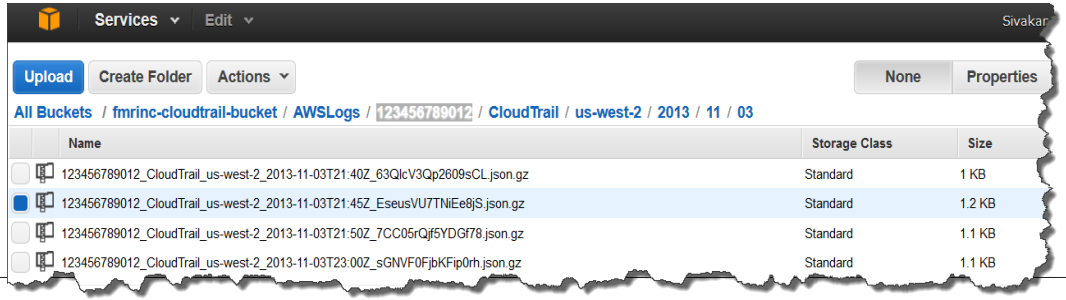
Q. AWSの運用監視をより安全にするには？



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

Amazon S3

API call の発生状況
SNS設定の有無

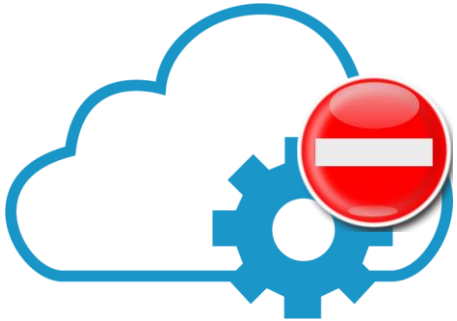
Amazon SNS

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

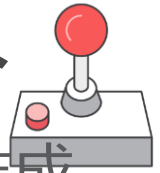
Non-API call Event



- 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


149022,
"type": "Organization",
"login": "atomicobject",
"starred_url": "https://api.github.com/
"gravatar_id": "bd869a731379aa8c867b1
"received_events_url": "https://api.github.com/
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

powered by ace

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Description" : "AWS CloudTrail API Activity Alarm Template for CloudWatch Logs",
  "Parameters" : {
      "LogGroupName" : {
          "Type" : "String",
          "Default" : "CloudTrail/DefaultLogGroup",
          "Description" : "Enter CloudWatch Logs log group name. Default is CloudTrail/DefaultLogGroup"
      },
      "Email" : {
          "Type" : "String",
          "Description" : "Email address to notify when an API activity has triggered an alarm"
      }
  },
  "Resources" : {
      "SecurityGroupChangesMetricFilter": {
          "Type": "AWS::Logs::MetricFilter",
          "Properties": {
```

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

Filter Name: CloudWatchAlarm-CloudTrail-APIActivity-EC2InstanceChangesMetricFilter-1Q1TJK84379GF — Create Alarm
Filter Pattern: { ($.eventName = RunInstances) || ($.eventName = RebootInstances) || ($.eventName = StartInstances) || ($.eventName = StopInstances) || ($.eventName = TerminateInstances) }
Metric: CloudTrailMetrics / EC2InstanceEventCount
Metric Value: 1
Alarm: CloudTrailEC2InstanceChanges

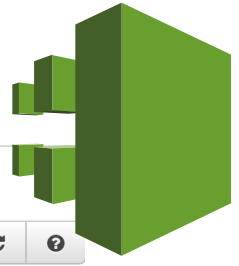
Filter Name: CloudWatchAlarm-CloudTrail-APIActivity-EC2LargeInstanceChangesMetricFilter-V2DOYX90SA20 — Create Alarm
Filter Pattern: { (($.eventName = RunInstances) || ($.eventName = RebootInstances) || ($.eventName = StartInstances) || ($.eventName = StopInstances) || ($.eventName = TerminateInstances)) && (($.requestParameters.instanceType = *.8xlarge) || ($.requestParameters.instanceType = *.4xlarge)) }
Metric: CloudTrailMetrics / EC2LargeInstanceEventCount
Metric Value: 1
Alarm: CloudTrailEC2LargeInstanceChanges

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

amazon web services

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-[redacted]
2015-12-21, 01:18:27 PM	sakatoku	RunInstances	Ami and 7 more	ami-[redacted] and 9 more
2015-12-21, 01:17:03 PM	sakatoku	TerminateInstances	Instance	i-[redacted]
2015-12-21, 01:16:23 PM	sakatoku	ConsoleLogin		
2015-12-20, 01:26:07 AM	sakatoku	RunInstances	Ami and 7 more	ami-[redacted] and 9 more
2015-12-20, 01:26:07 AM	sakatoku	CreateTags		i-[redacted]
2015-12-20, 12:50:43 AM	sakatoku	DetachUserPolicy	Policy and 1 more	arn:aws:iam::[redacted]...
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::[redacted]...

CloudTrail API サンプル (RunInstance)

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

AWS access key [redacted]
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-[redacted]
Ami

i-[redacted]
Instance

my_[redacted]
KeyPair

eni-[redacted]
NetworkInterface

mysg4win
SecurityGroup

sg-[redacted]
SecurityGroup

subnet-[redacted]
Subnet

vpc-[redacted]
VPC

[redacted]
InstanceProfile

arn:aws:iam::[redacted]
profile/AWS_Admin
InstanceProfile

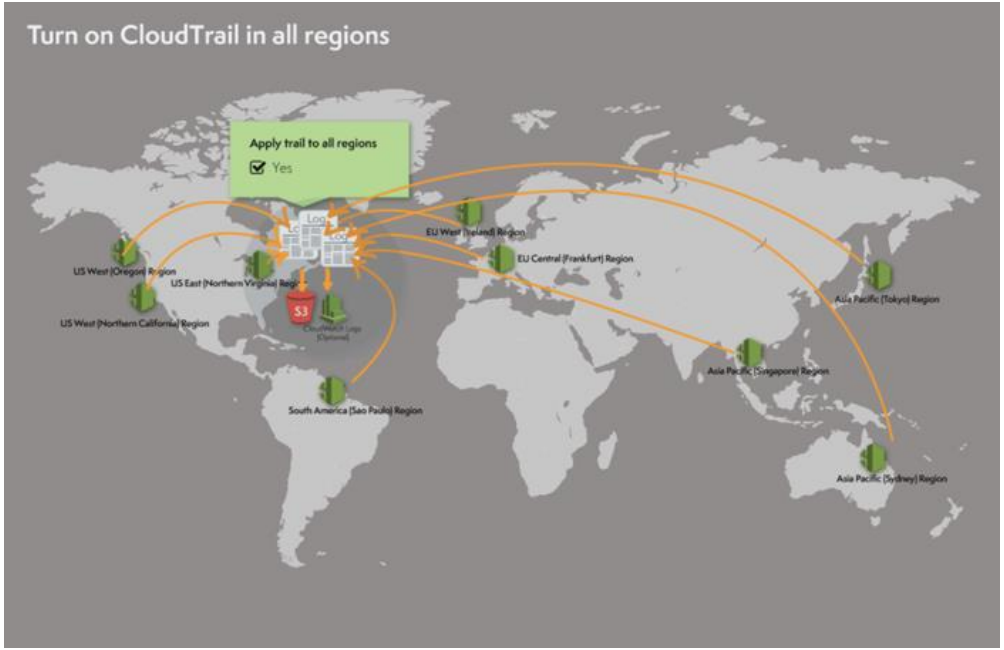
View event

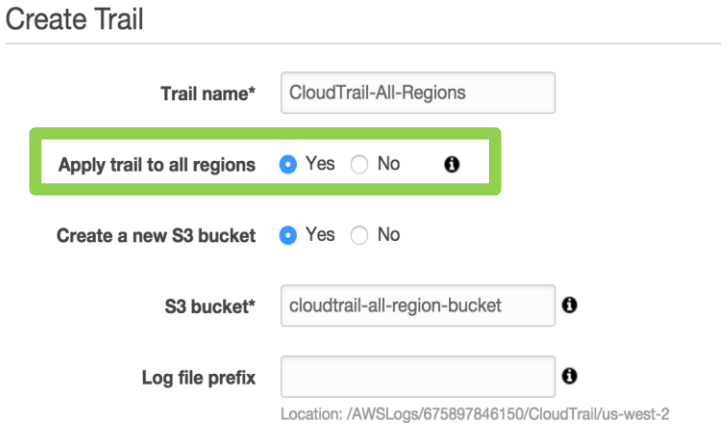
amazon web services

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





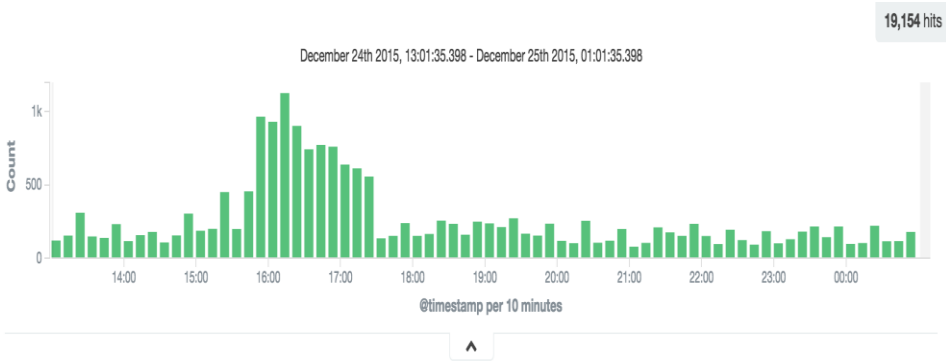
http://aws.typepad.com/aws_japan/2015/12/aws-cloudtrail-update-turn-on-in-all-regions-use-multiple-trails.html

amazon web services

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

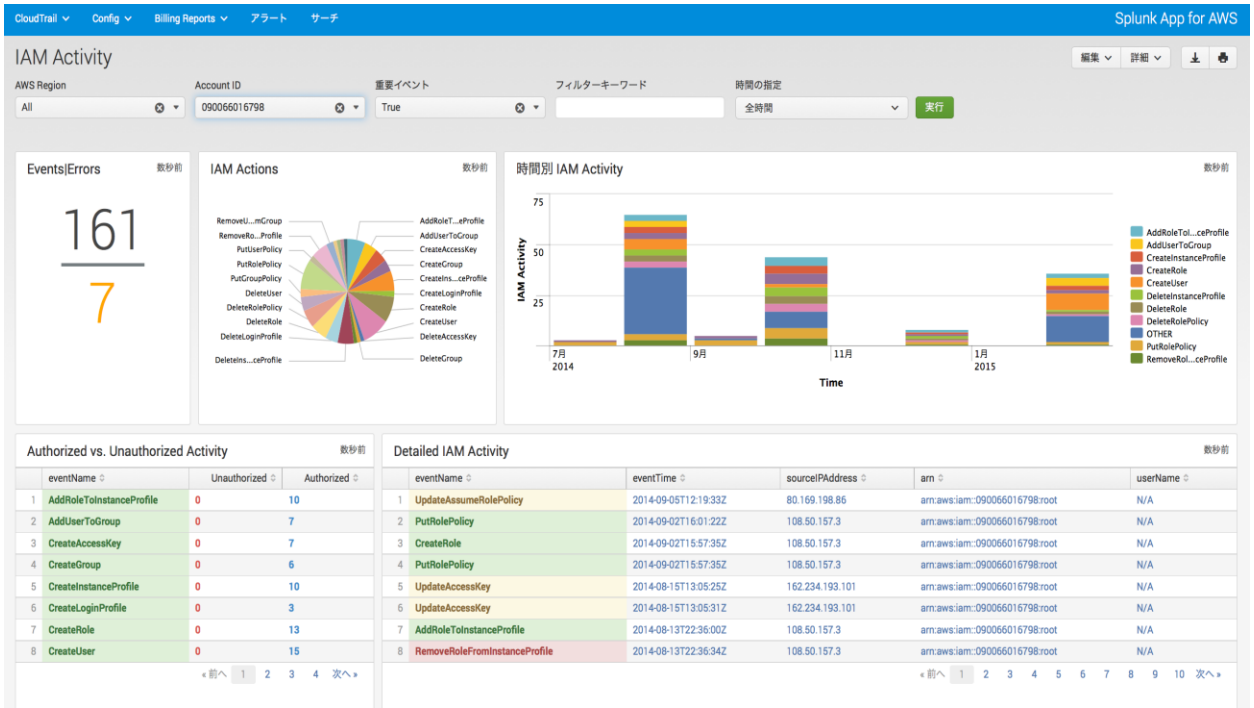


Time ▾ _source

▸ 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 172.31.8.175 172.3 1.0.164 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 172.31.0.164 172.3 1.8.175 63250 389 17 1 211 1450972683 1450972737 ACCEPT OK @owner: 675897846150 @log_group: defaultvpc-

Splunk App for AWS



splunk>

新規サーチ

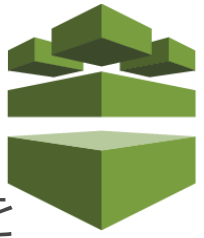
```
host="ip-10-170-32-235" sourcetype="aws:cloudtrail" eventName=DeleteInstance*
```

✓ 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	{ [-] 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: { [+] }

amazon web services

AWS Configとは



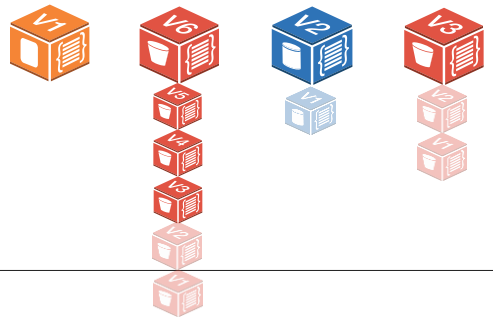
- AWSリソースのレポジトリ情報を取得し、リソースの設定履歴を監査、リソース構成の変更を通知するフルマネージドサービス

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

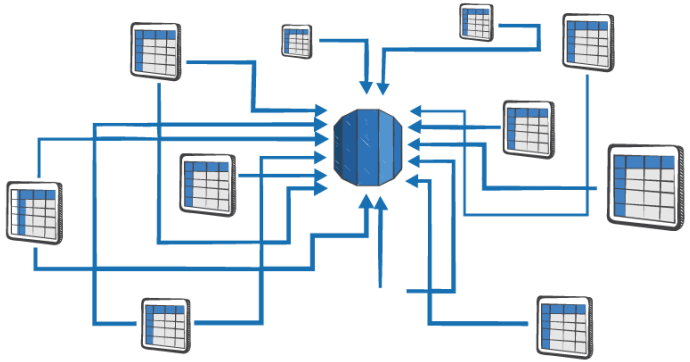
- あるポイントでのコンフィグレーション アイテムの集合
- 自動で定期的あるいは変更トリガで作成され、Amazon S3にエクスポートされる

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

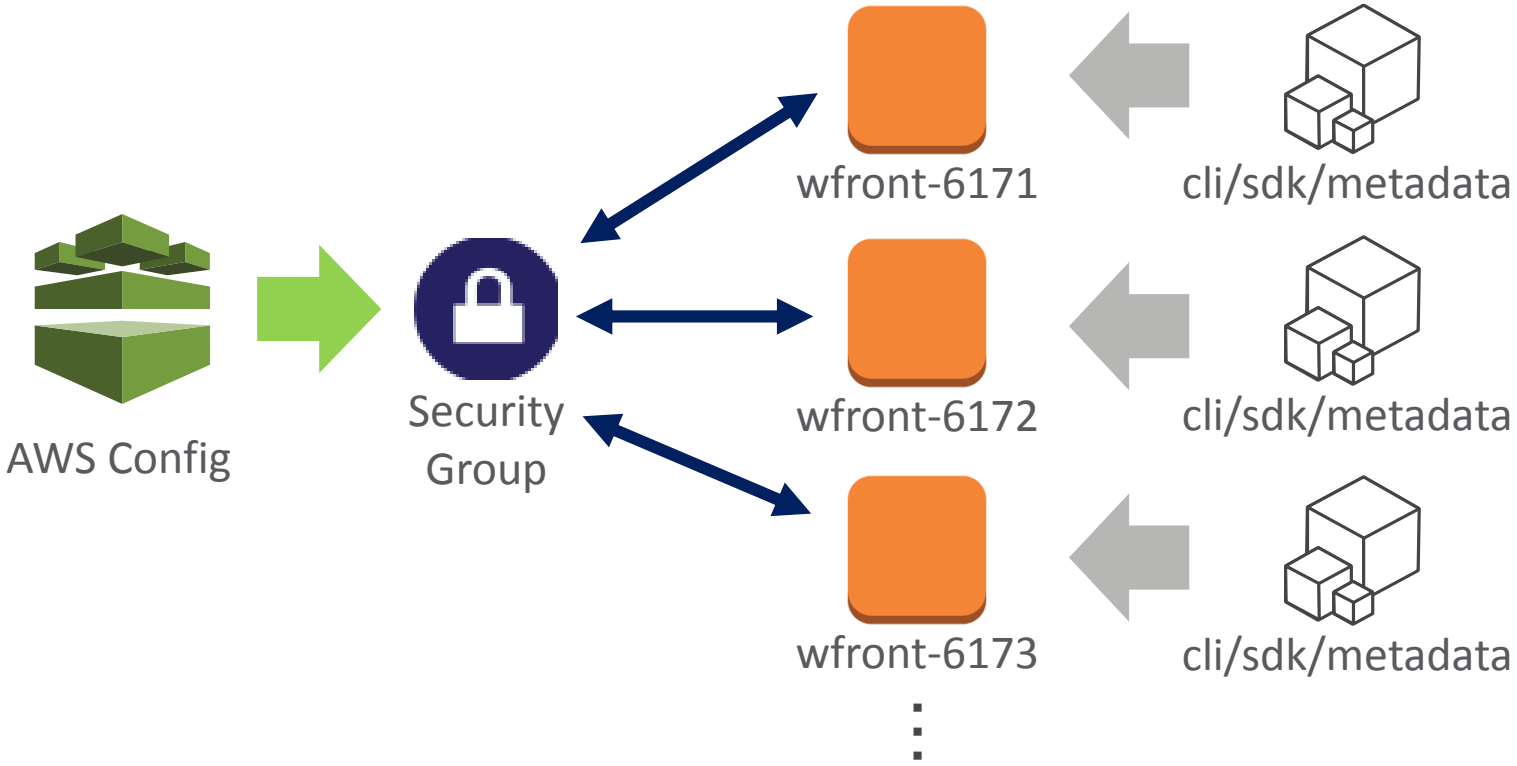
リレーションシップ

- 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



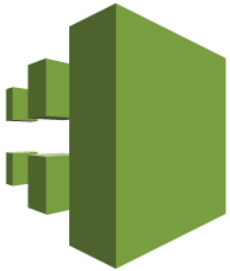
AWS Configが対応しているAWSリソース

- 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

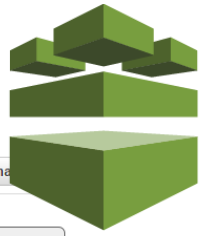


AWS CloudTrail

AWS IAM

※2015年12月25日時点

現在の構成の確認



EC2 Instance i-cbe78721

Mana

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

6 4 7 6 8 Changes

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

構成詳細

Configuration Details

ew Details

Amazon Resource Name	arn: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

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

Resource inventory

Status

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

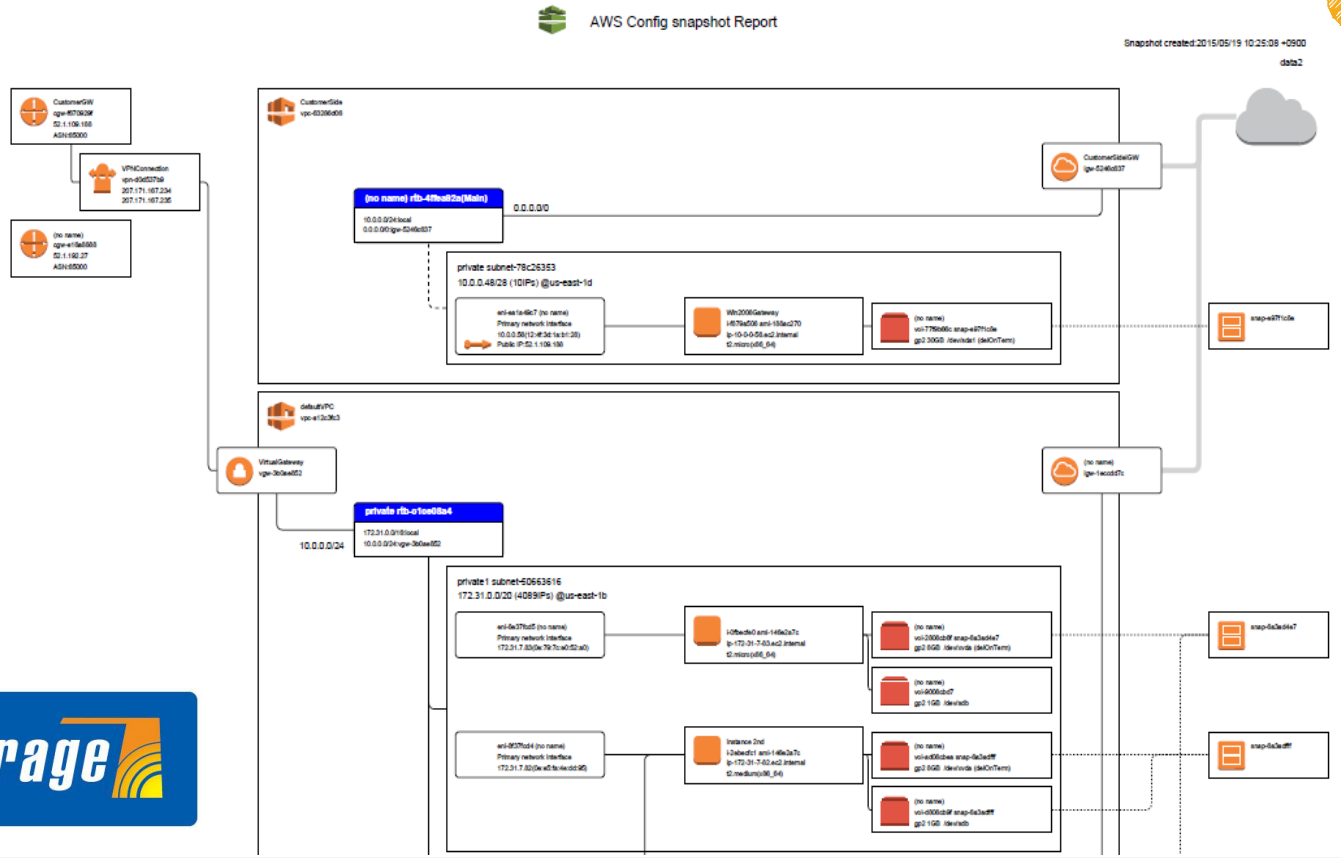
Choose the icon to see Config timeline for a resource.

Resource type	Resource identifier	Compliance	Config timeline
EC2 Instance	i-[redacted]	Noncompliant with 1 rule	
EC2 Instance	i-[redacted]	Compliant	
EC2 Instance	i-[redacted]	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



Logstorage

amazon web services

AWS Config Rules

New

COMPLIANCE GUIDELINE	ACTION
All EBS volumes should be encrypted	Encrypt volumes
Instances must be within a VPC	Terminate instance
Instances must be tagged with environment type	Page developer

AWS Config Rulesによるポリシー適合の評価

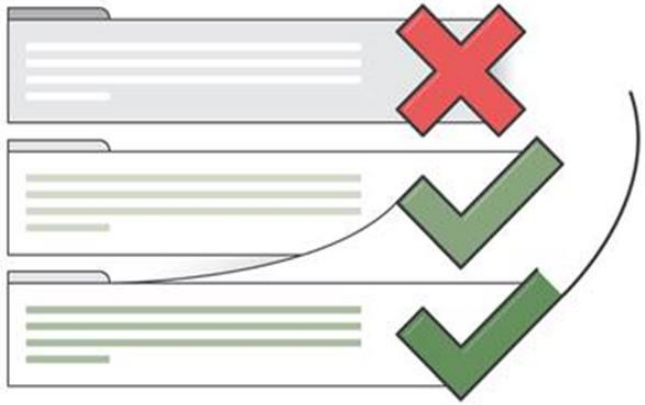
- AWS Config Rules
  - 準拠すべきルールを事前に設定し、その内容に沿った構成変更が行われているかをルールに従い評価
    - ✓ 全てのEBCボリュームが暗号化されているか
    - ✓ EC2インスタンスが適切にタグ付されているか
    - ✓ Elastic IP address(EIP)がインスタンスにアタッチされているか

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

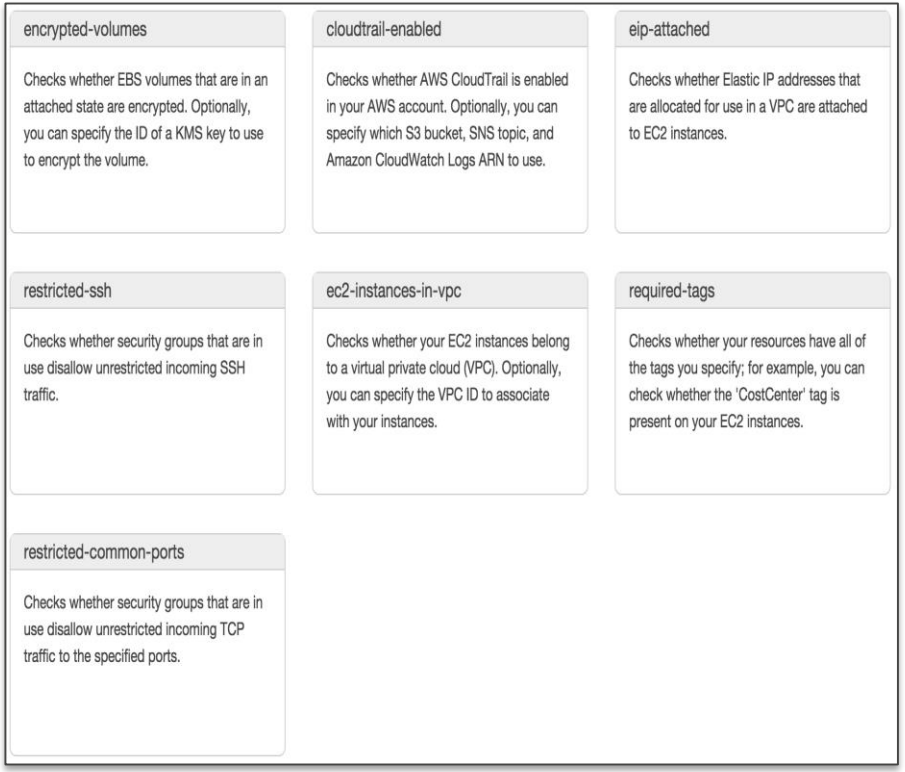


Customer Managed Rules

- 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

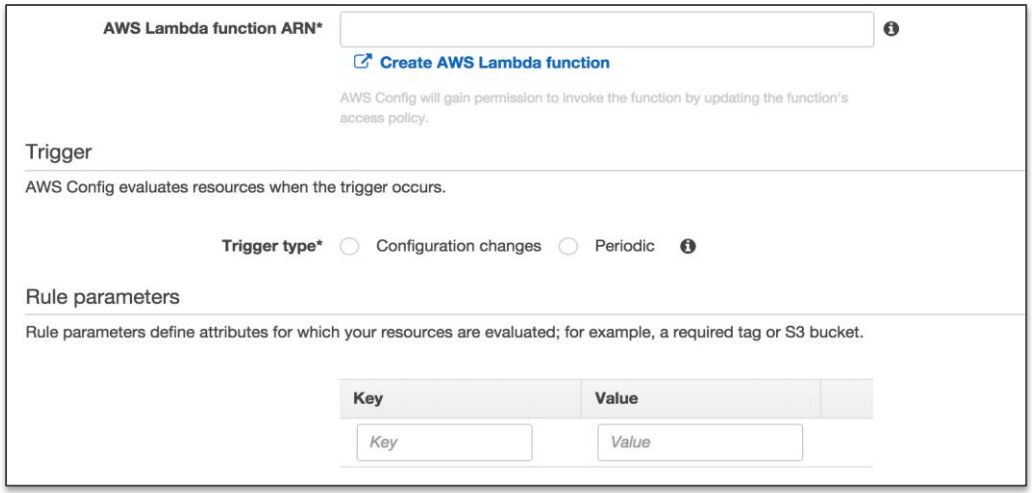
AWS Config Rules (AWS Managed Rules)

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



AWS Config Rules (Customer Managed Rules)

- Customer Managed Rulesの種類
  - ✓ Lambda functon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 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

amazon web services

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-[redacted]	Compliant	
EC2 Instance	i-[redacted]	Compliant	

amazon web services

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:[redacted]:instance/i-cbe78721	Instance Type	m3.medium
Resource type	AWS::EC2::Instance	Instance state	stopped
Resource ID	i-[redacted]	Private DNS	ip-[redacted].internal
Availability zone	us-east-1c	Private Ips	[redacted]
Created at	November 26, 2014 8:25:36 PM	Public DNS	*null*
Tags (2)	CostCenter:4005, Name:cwl-sqlserver	AMI ID	ami-5c17af34
		Platform	windows
		Launch time	2014-11-26T11:25:36.000Z
		Lifecycle	*null*
		Monitoring	disabled

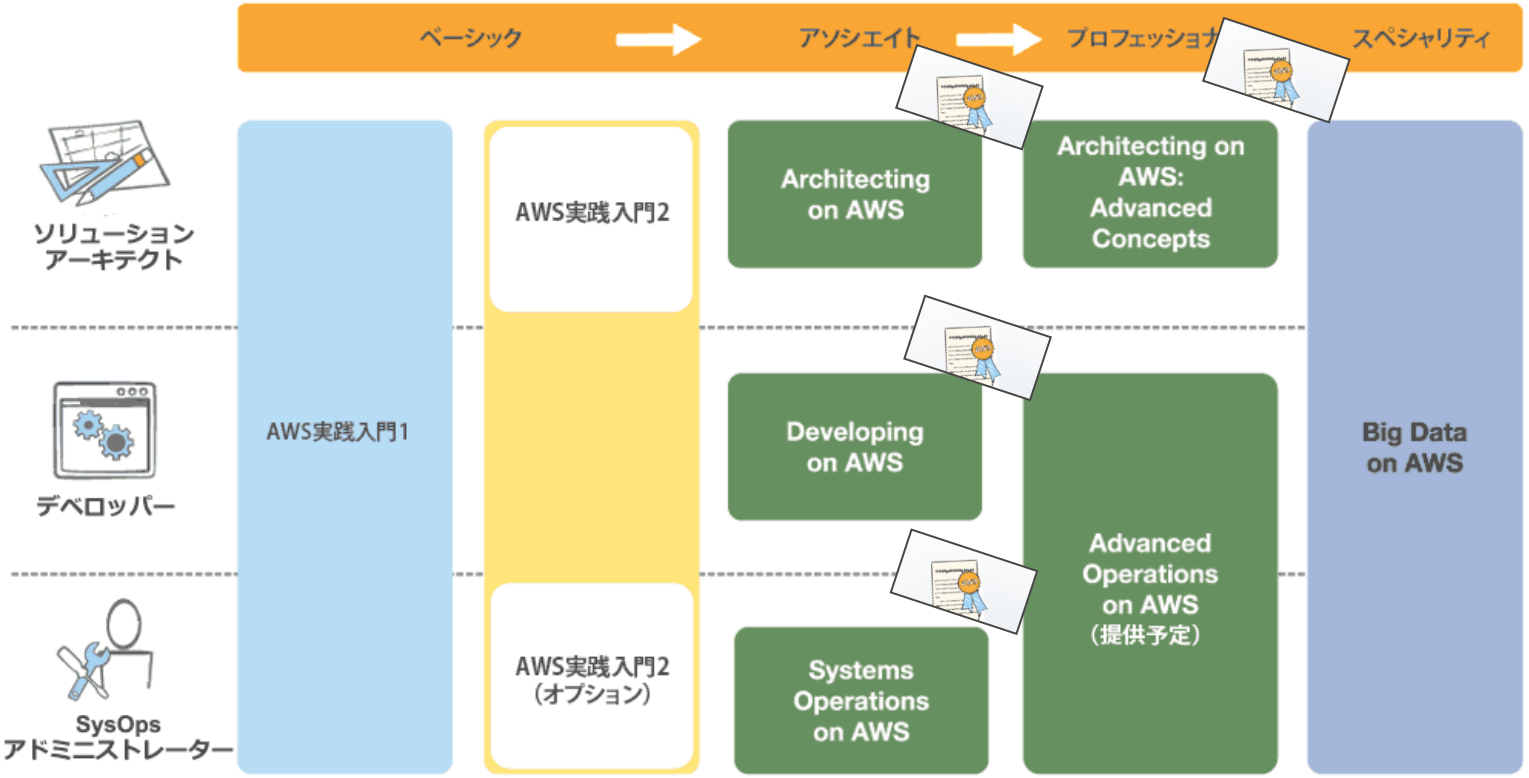
まとめ

- 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、AWS 運用管理コミュニティ で検索 Ops JAWS
- 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。



詳細： aws.amazon.com/training

認定資格試験

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

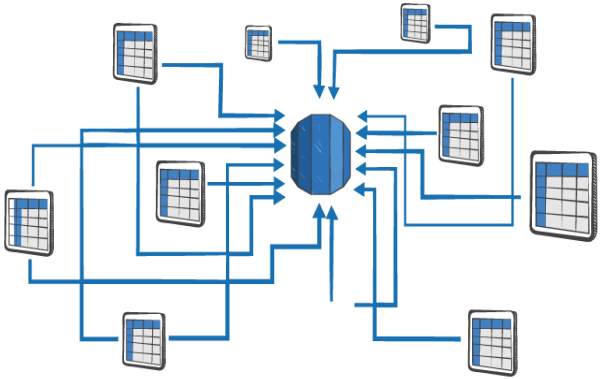
最新技術情報、イベント情報、お役立ち情報、
お得なキャンペーン情報などを日々更新しています！


amazon
web services

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