

AWS

S U M M I T

# AWS の運用監視入門

Amazon CloudWatch

技術統括本部 ソリューションアーキテクト  
藤倉 和明

2017年6月2日



# 本セッションのFeedbackをお願いします

受付でお配りしたアンケートに本セッションの満足度やご感想などをご記入ください  
アンケートをご提出いただきました方には、もれなく素敵なAWSオリジナルグッズを  
プレゼントさせていただきます



アンケートは受付、パミール3FのEXPO展示会場内にて回収させて頂きます

# 自己紹介

藤倉 和明 (ふじくら かずあき)

アマゾン ウェブ サービス ジャパン株式会社  
エンタープライズソリューション部  
ソリューションアーキテクト



好きなAWSサービス

- Amazon Virtual Private Cloud (VPC)
- Amazon CloudWatch

# 本日皆様にお持ち帰りして頂く内容



運用をもっと簡単に



夜ぐっすり眠れる運用体制へ



運用もスケーラブルに



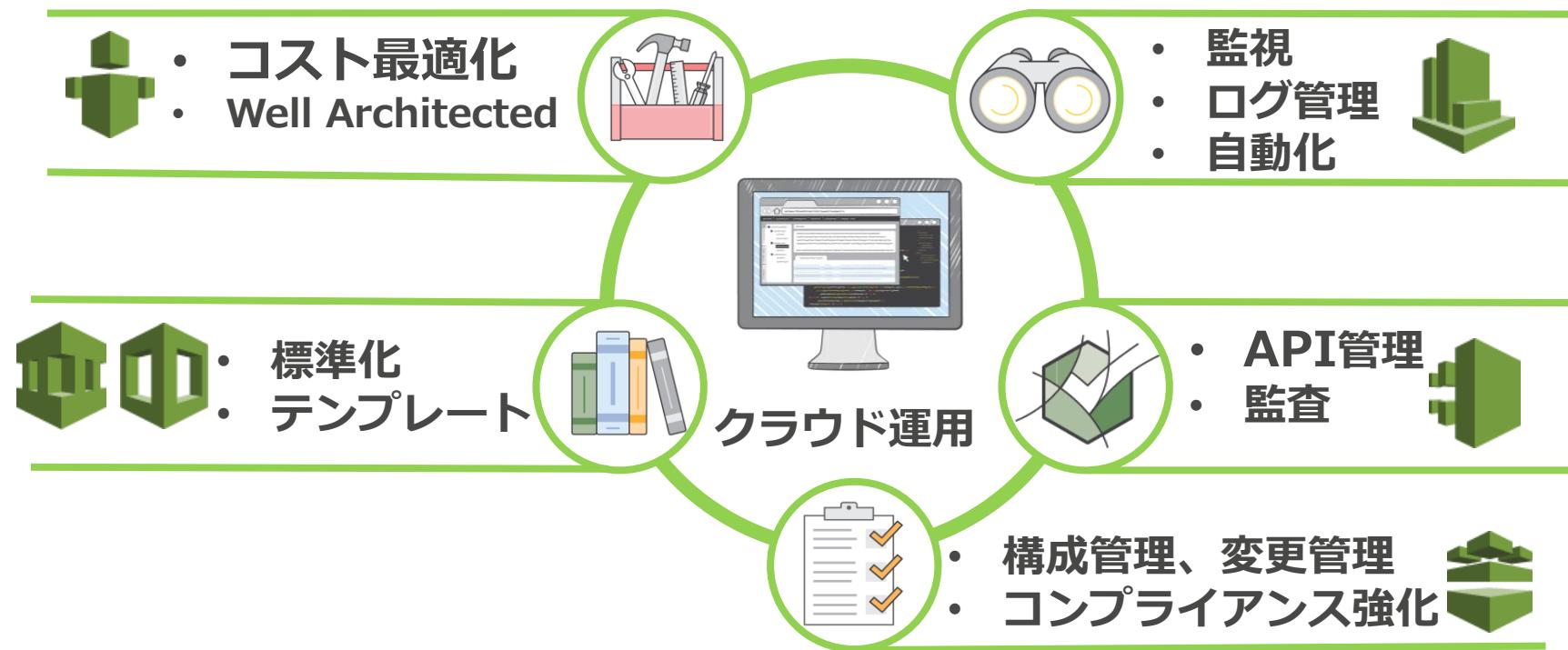
# 本セッションについて



- 想定するオーディエンス
  - オンプレミス、クラウド問わず**システム運用**をしている人
  - システム運用、監視に**課題を感じている人**
- セッションの概要
  - **フルマネージド運用監視サービス Amazon CloudWatch**を中心とした、**クラウドの運用**についてご紹介

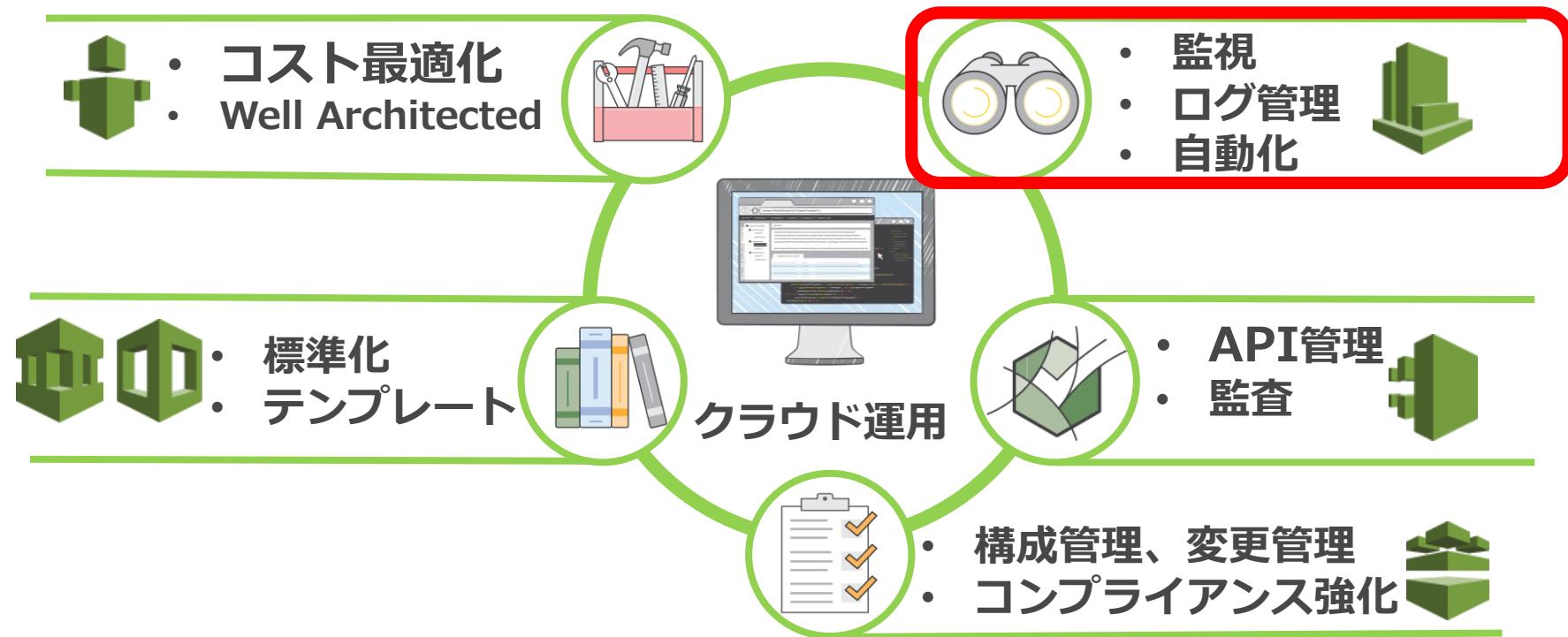
# クラウドの運用

# AWSのクラウド運用



# AWSのクラウド運用

今日はここを中心に



# システム監視とは



# システム監視とは

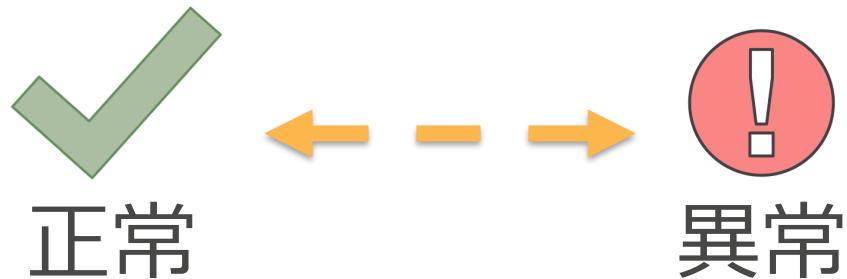


正常



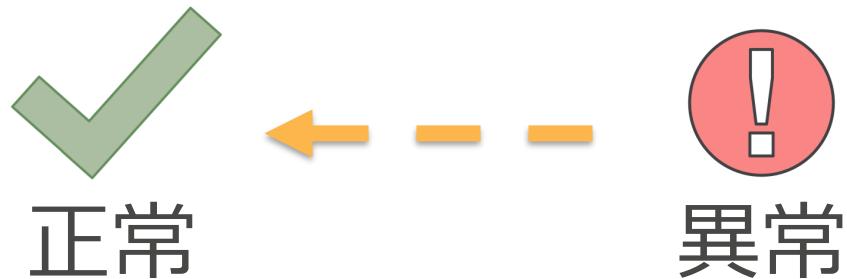
異常

# システム監視とは



- 「正常な状態」を定義
- 「異常な状態」を定義
- その状態の変化

# 障害対応：「異常な状態」を「正常な状態」へ



障害対応は重要な「運用」

- 予め決まっている対応
- 不測の事態
  - まずは落ち着いて
  - 一時復旧、根本対応
  - 再発防止

# クラウドにおける「正常」「異常」とは？



AWSクラウドにおけるシステム運用監視は  
CloudWatchが最適！



CloudWatch

# Amazon CloudWatchとは

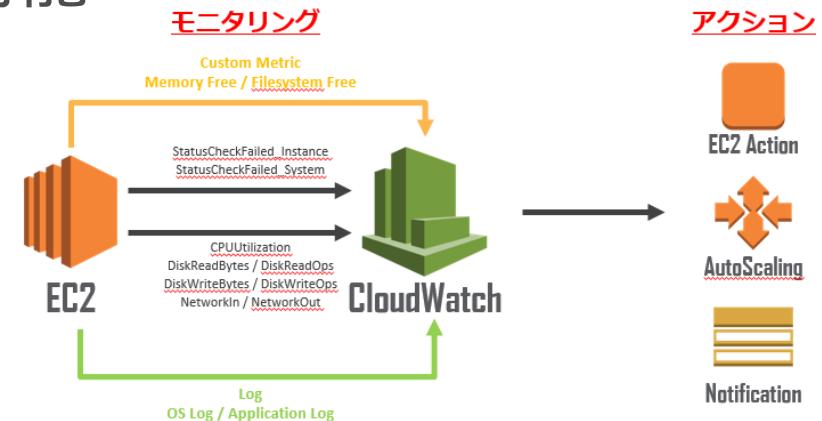


AWSの各種リソースを監視するマネージドサービス

- セットアップ不要
- 正常な状態を継続的に監視
- 異常な状態の検知と、自動的な復旧をサポート
- 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

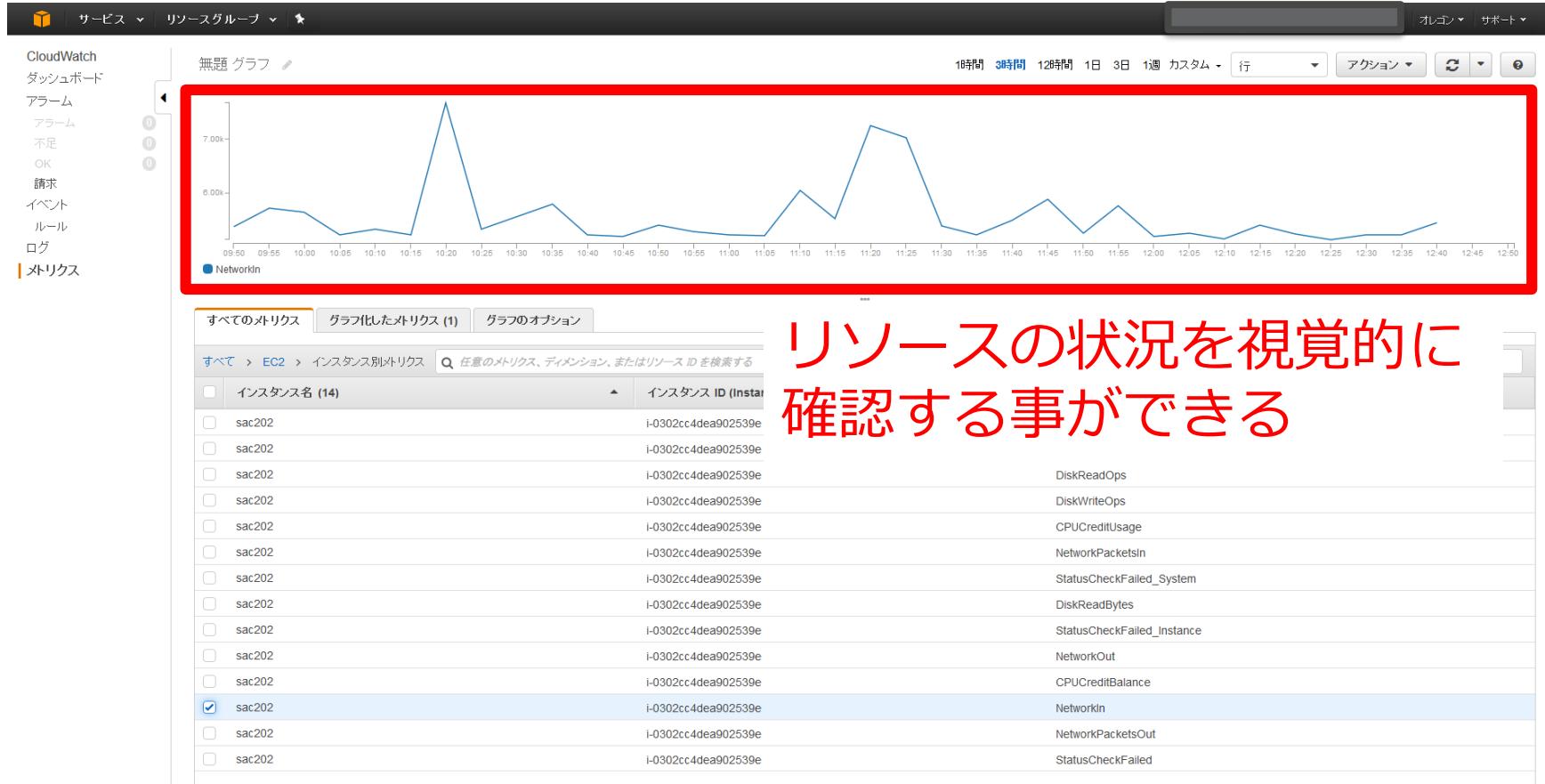


# Amazon CloudWatchのできる事



- CloudWatch
  - システム監視サービス
    - ✓ 死活監視 / 性能監視 / キャパシティ監視
- CloudWatch Logs
  - ログ管理プラットフォームサービス
    - ✓ EC2上のOS, APPのログ
    - ✓ AWSマネージド サービスのログ
- CloudWatch Events
  - AWS上リソースの状態監視サービス
  - AWSリソースに対する**イベントをトリガーにアクションを実行**する機能

# CloudWatch利用イメージ



# CloudWatchのメトリックス

## 標準メトリックス (EC2)

CPUUtilization  
CPUCreditBalance  
CPUCreditUsage  
DiskReadBytes  
DiskWriteBytes  
DiskReadOps  
DiskWriteOps  
NetworkOut  
NetworkIn  
NetworkPacketsIn  
NetworkPacketsOut  
StatusCheckFailed\_Instance  
StatusCheckFailed  
StatusCheckFailed\_System  
BurstBalance

## カスタムメトリックス

標準メトリックスでは  
収集できないメトリックス



# Amazon CloudWatch のアクション機能

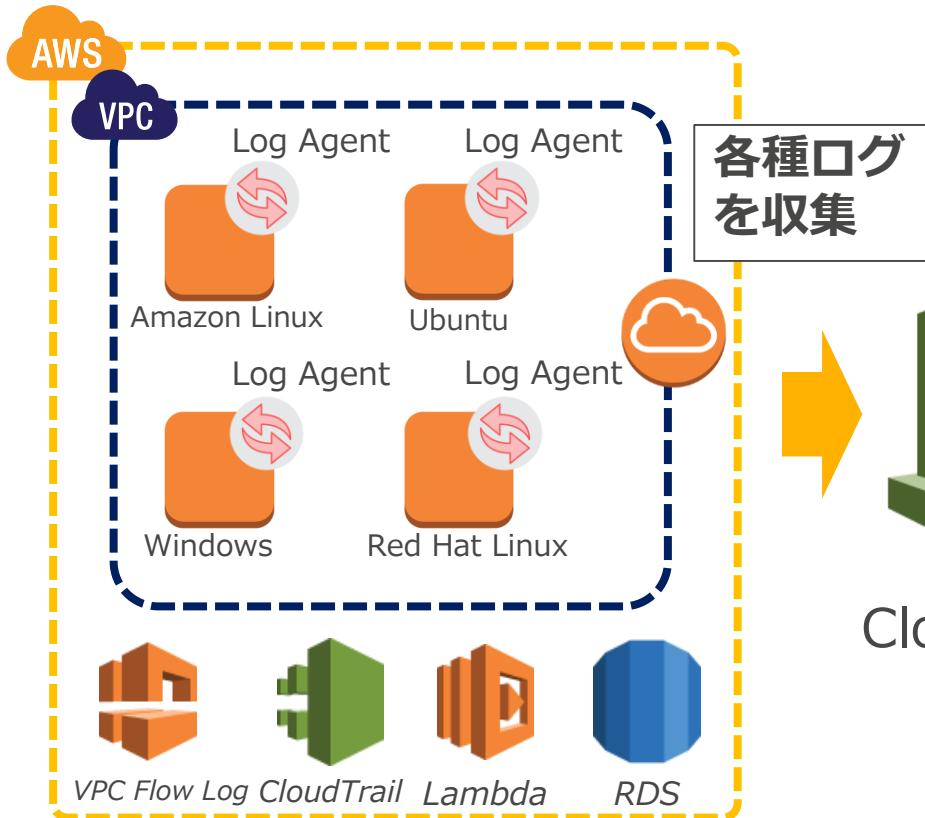
## モニタリング



## アクション



# CloudWatch Logs利用イメージ



CloudWatch  
Logs



通知:  
CloudWatch Alarm



エクスポート:  
Amazon Kinesis  
Firehose



可視化:  
Amazon Elasticsearch  
Service  
(Kibana)

# 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 ロググループ Default-Log-Group 0-0299505423feee84b

フィルター (検索)

すべて展開 行 テキスト

すべて 30秒 5分 1時間 6時間 1日 1週 カスタム

イベントのフィルター

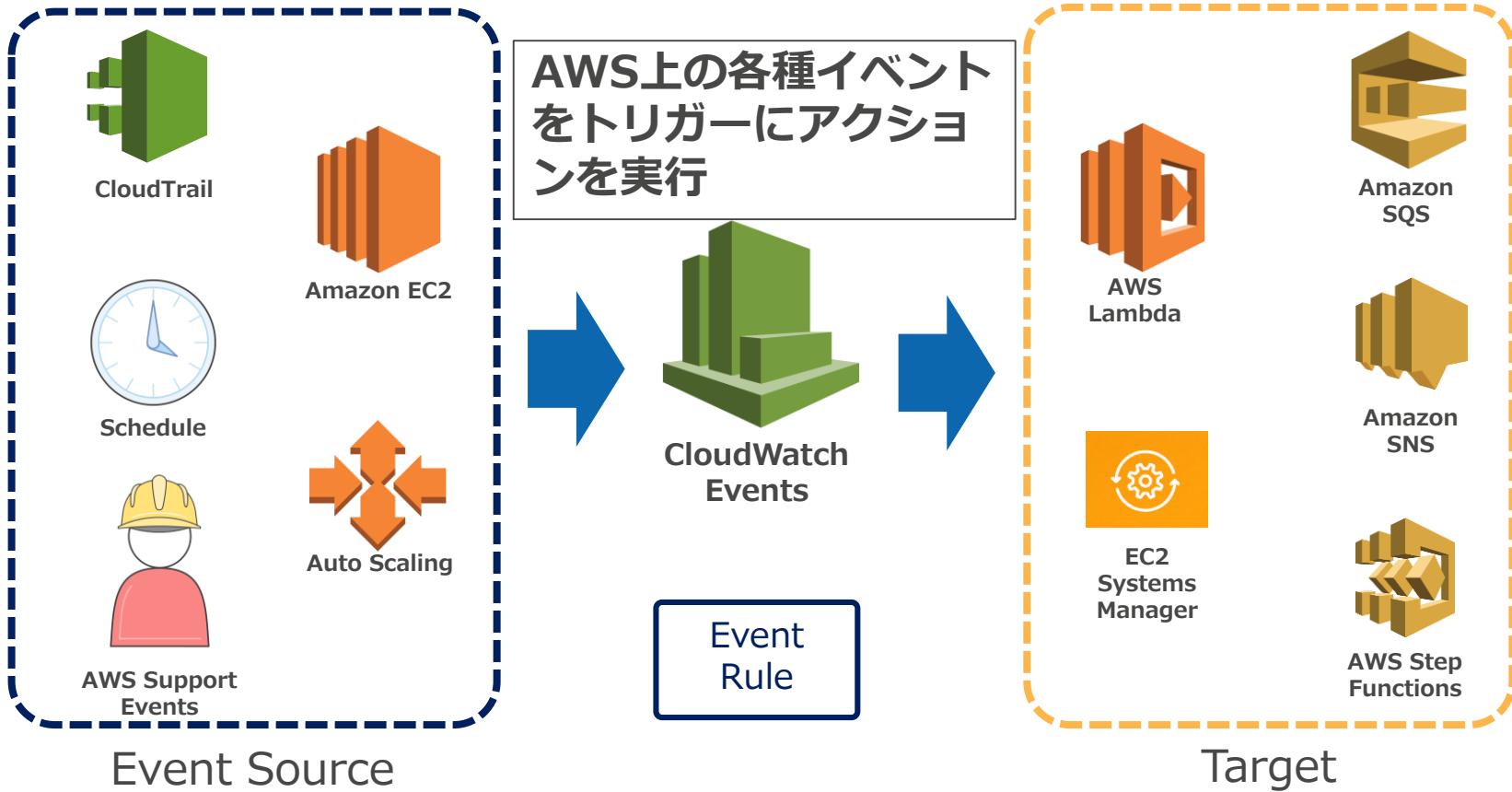
時間 (UTC +00:00) メッセージ

05-03

タイムスタンプ ログメッセージ

タイムスタンプ	ログメッセージ
14:57:16	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The Software Protection service entered the running state.]
15:17:32	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The Software Protection service entered the stopped state.]
15:17:33	[System] [Error] [1111] [Microsoft-Windows-TerminalServices-Printers] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [Driver Microsoft Print To PDF required for printer Microsoft Print to PDF.]
15:17:35	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The Device Setup Manager service entered the running state.]
15:19:35	[System] [Error] [1111] [Microsoft-Windows-TerminalServices-Printers] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [Driver Send to Microsoft OneNote 16 Driver required for printer Microsoft OneNote 16.]
15:21:30	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The Device Setup Manager service entered the stopped state.]
15:17:35	[System] [Error] [1111] [Microsoft-Windows-TerminalServices-Printers] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [Driver Send to Microsoft OneNote 16 Driver required for printer Microsoft OneNote 16.]
15:19:35	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The Device Setup Manager service entered the stopped state.]
15:21:09	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The WinHTTP Web Proxy Auto-Discovery Service service entered the stopped state.]
15:34:57	[System] [Error] [36888] [Schannel] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connection.]
15:34:57	[System] [Error] [36888] [Schannel] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connection.]
15:40:04	[System] [Error] [36888] [Schannel] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connection.]
15:40:04	[System] [Error] [36888] [Schannel] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connection.]
15:54:42	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The WinHTTP Web Proxy Auto-Discovery Service service entered the running state.]

# CloudWatch Events利用イメージ



# 例：コンソールサインイン時にアラートを飛ばす

## イベントソース

CloudTrail

イベントパターン  サインインイベント

サービス別のイベントにて

サービス名: AWS コンソールのサインイン

イベントタイプ: サインインイベント

任意のユーザー

ARN 別の特定のユーザー

arn:aws:iam::029845397858:user/kazuakf



## ターゲット

Amazon SNS

イベントがイベントパターンに一致します。

SNS トピック

トピック\*: alert-iam

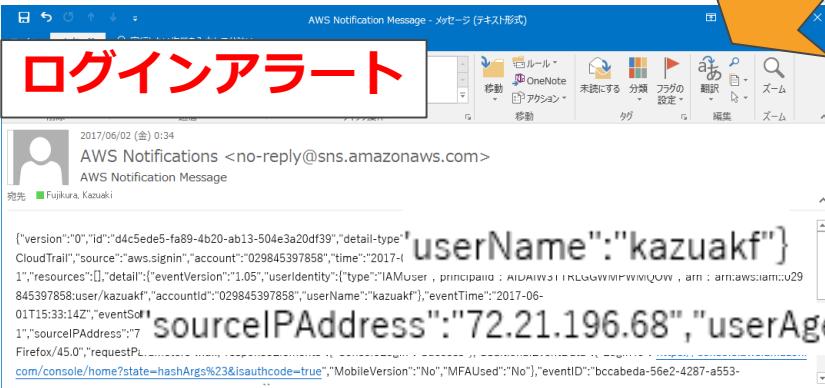
入力の設定

一致したイベント

一致したイベントの一部

定数 (JSON テキスト)

インプットトランスフォーマー



# Amazon CloudWatchのできる事



- CloudWatch
  - システム監視サービス
    - ✓ 死活監視 / 性能監視 / キャパシティ監視
- CloudWatch Logs
  - ログ管理プラットフォームサービス
    - ✓ EC2上のOS, APPのログ
    - ✓ AWSマネージド サービスのログ
- CloudWatch Events
  - AWS上リソースの状態監視サービス
  - AWSリソースに対する**イベントをトリガーにアクションを実行**する機能

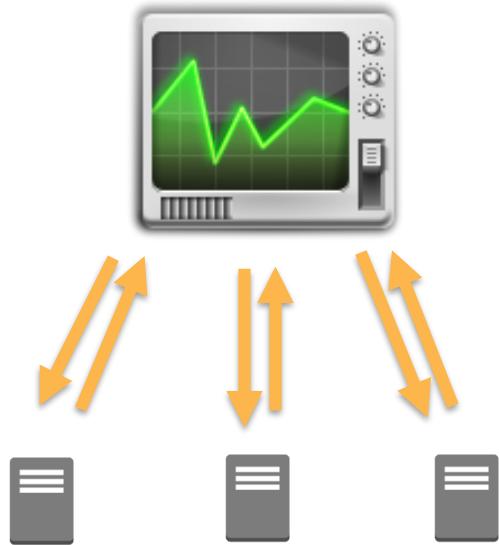
# Why CloudWatch

1. Pollingモデルから、 **Pushモデル**へ
2. サーバ中心の監視から、 **サービスの監視**へ
3. AWSサービスとの**連携**

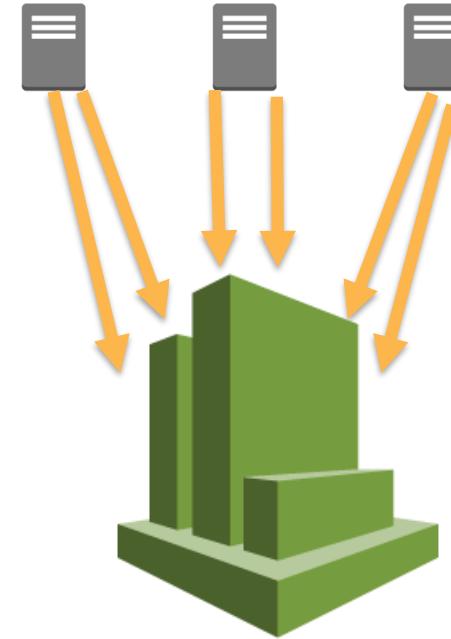
# Why CloudWatch

1. Pollingモデルから、 **Pushモデル**へ
2. サーバ中心の監視から、 **サービスの監視**へ
3. AWSサービスとの**連携**

# Polling / Push

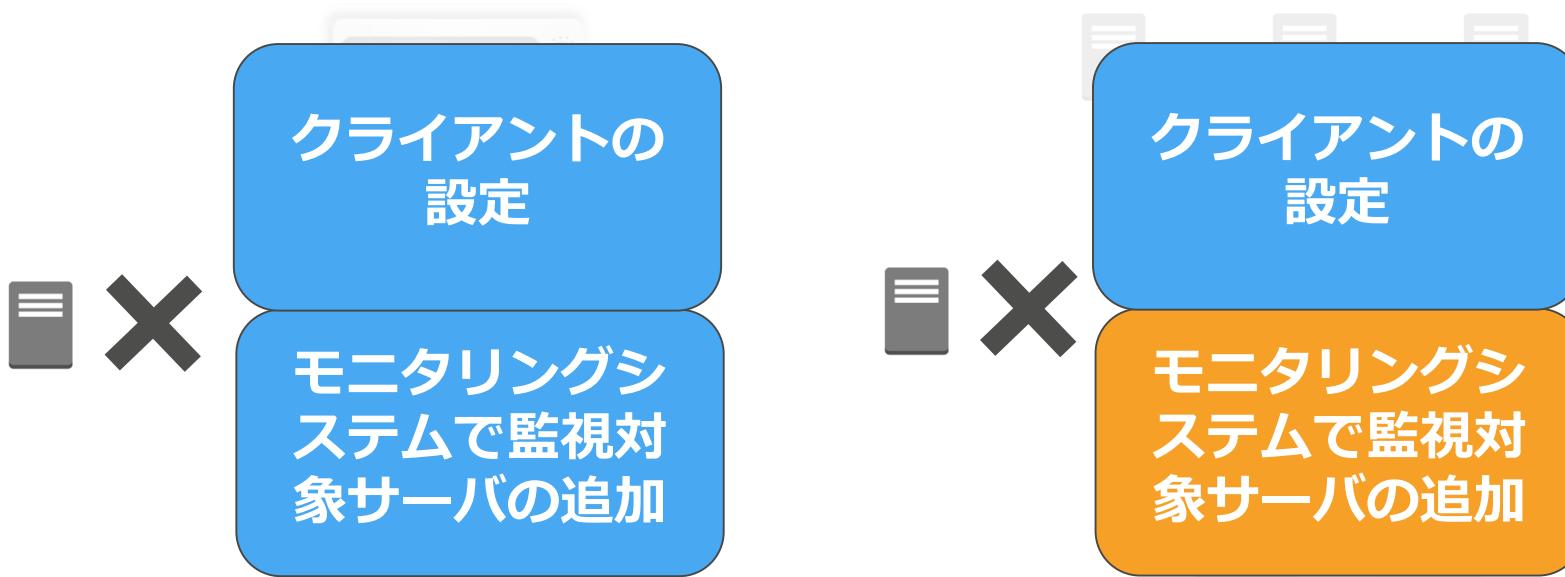


Before Cloud



Amazon CloudWatch

# Polling / Push



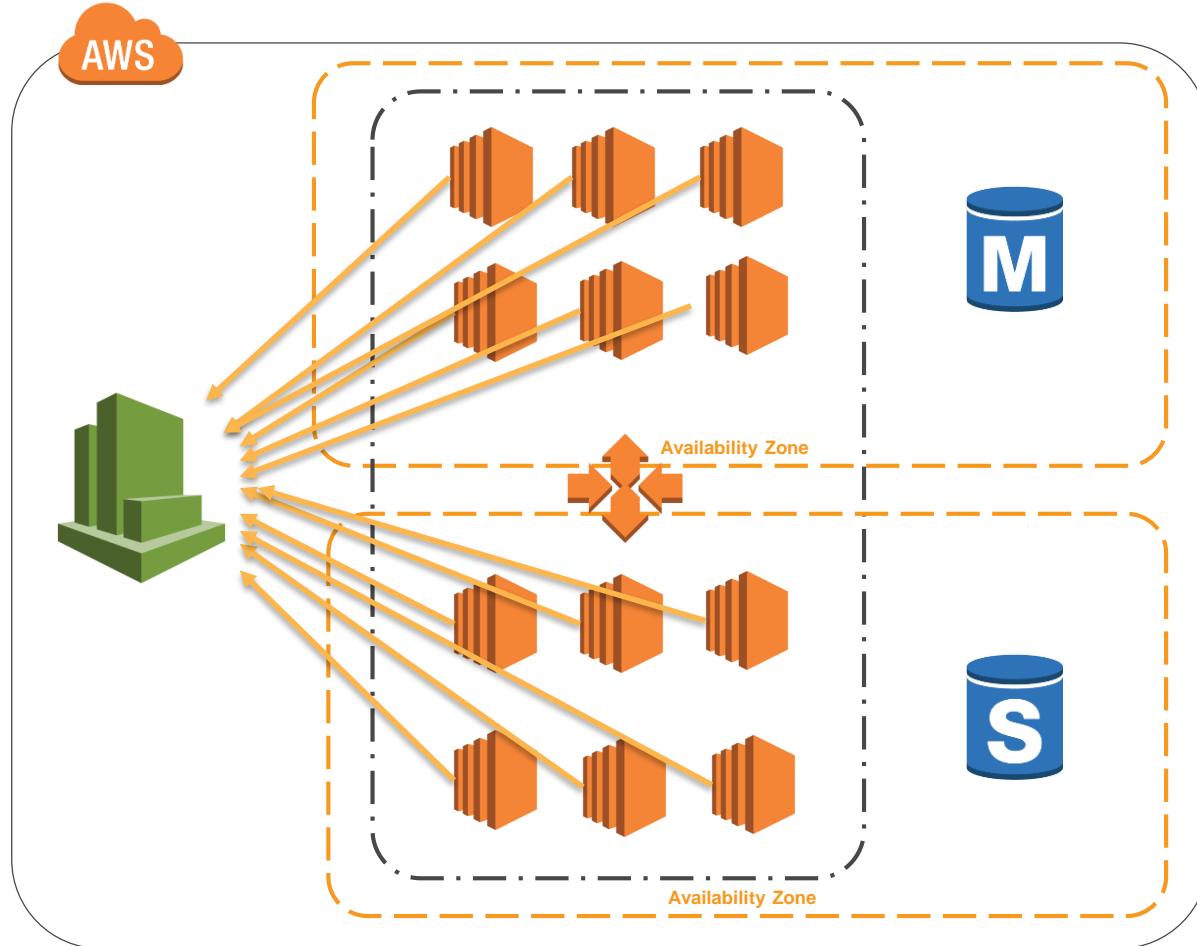
Before Cloud

監視を始めるまでに必要な作業

Amazon CloudWatch

CloudWatchを利用する  
と省略できる作業

# その監視、オートスケールに対応していますか？

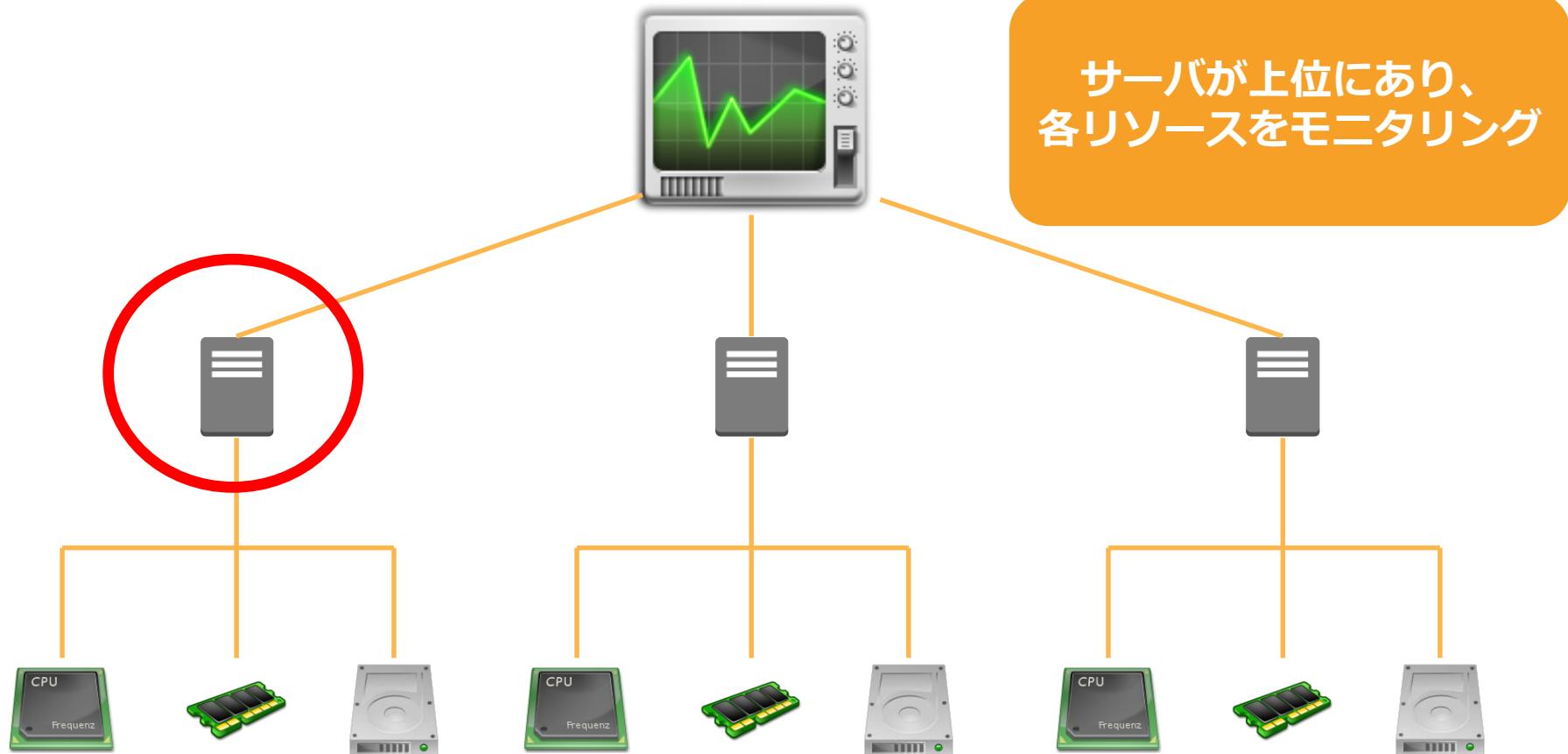


- ダイナミックに変化するサーバの監視は、従来のPollingモデルは難しかった
- Pushモデルの監視ソリューションでは、オートスケール等のダイナミックに増減するサーバにも対応可能

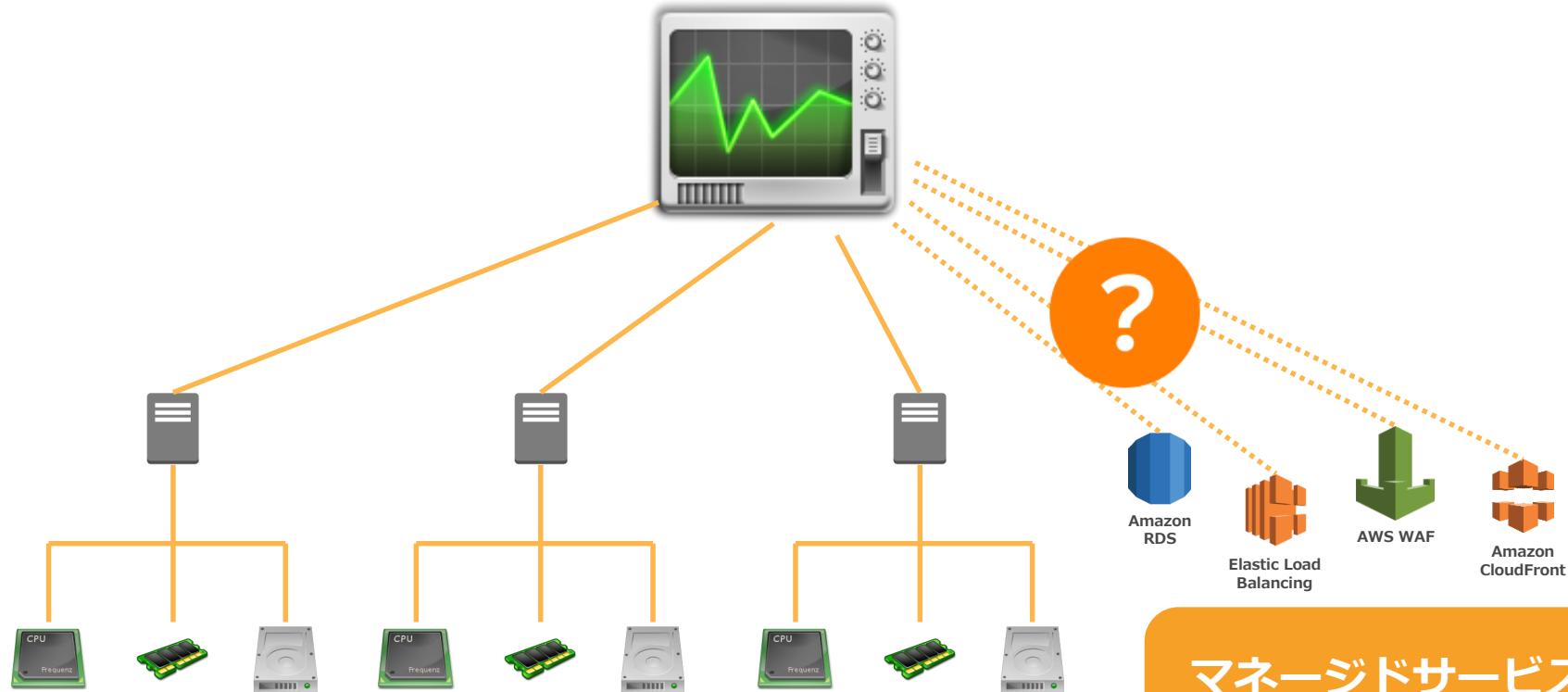
# Why CloudWatch

1. Pollingモデルから、Pushモデルへ
2. サーバ中心の監視から、**サービスの監視**へ
3. AWSサービスとの連携

# 従来のモニタリングシステム



# 従来のモニタリングシステム



マネージドサービス  
のモニタリングは?

# マネージドサービスの場合

アプリケーション最適化
スケール
高可用性
バックアップ
MW パッチ適用
MW インストール
OS パッチ適用
OS インストール
サーバー管理
ラッキング
電源, 空調, ネットワーク
オンプレミス

アプリケーション最適化
スケール
高可用性
バックアップ
MW パッチ適用
MW インストール
OS パッチ適用
OS インストール
サーバー管理
ラッキング
電源, 空調, ネットワーク
On EC2

アプリケーション最適化
スケール
高可用性
バックアップ
MW パッチ適用
MW インストール
OS パッチ適用
OS インストール
サーバー管理
ラッキング
電源, 空調, ネットワーク
マネージドサービス



# マネージドサービスの場合

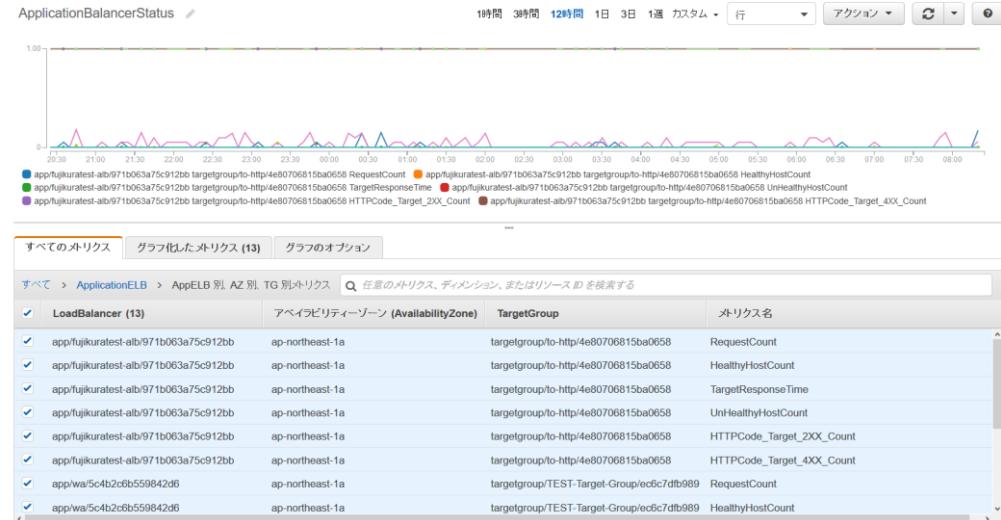
パッチ適用 / バックアップ / スケールまでお任せの  
マネージドサービスを活用する事で  
**より付加価値の高い仕事に集中**できる  
クラウドの運用にマネージドサービスの利用は不可欠



# マネージドサービスの活用にはCloudWatch



40を超えるマネージドサービスが追加の設定無くメトリクスの収集が可能  
サーバ中心の監視から**サービス中心の監視**へ  
シフトする事で運用もスケーラブルに



# CloudWatchに対応するAWSサービス

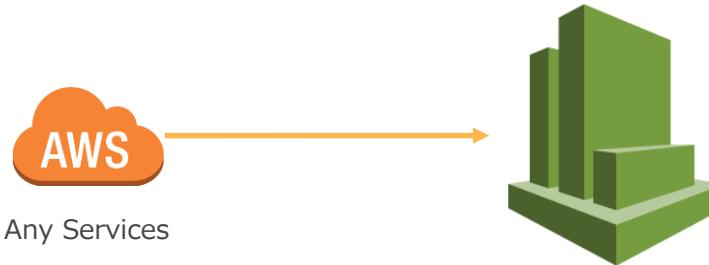
AWS サービス	名前空間	AWS サービス	名前空間
Amazon API Gateway	AWS/ApiGateway	Amazon EMR	AWS/ElasticMapReduce
Auto Scaling	AWS/AutoScaling	AWS IoT	AWS/IoT
AWS Billing	AWS/Billing	Amazon Kinesis	AWS/KMS
Amazon CloudFront	AWS/CloudFront	Amazon Kinesis Analytics	AWS/KinesisAnalytics
Amazon CloudSearch	AWS/CloudSearch	Amazon Kinesis Firehose	AWS/Firehose
Amazon CloudWatch Events	AWS/Events	Amazon Kinesis	AWS/Kinesis
Amazon CloudWatch Logs	AWS/Logs	Amazon Lambda	AWS/Lambda
AWS Database Migration Service		Amazon ML	AWS/ML
Amazon DynamoDB		Amazon OpsWorks	AWS/OpsWorks
Amazon EC2		Amazon Polly	AWS/Polly
Amazon EC2 Container Service		Amazon Redshift	AWS/Redshift
Amazon Elastic Beanstalk		AWS RDS	AWS/RDS
Amazon Elastic Block Store		AWS Route 53	AWS/Route53
Amazon Elastic File System		AWS DDoS Protection	AWS/DDoSProtection
Elastic Load Balancing		Amazon SES	AWS/SES
Elastic Load Balancing (Classic)		Amazon Simple Notification Service	AWS/SNS
Amazon Elastic Transcoder	AWS/ElasticTranscoder	Amazon Simple Queue Service	AWS/SQS
Amazon ElastiCache	AWS/ElastiCache	Amazon Simple Storage Service	AWS/S3
Amazon Elasticsearch Service	AWS/ES	Amazon Simple Workflow Service	AWS/SWF
		AWS Storage Gateway	AWS/StorageGateway
		AWS WAF	AWS/WAF
		Amazon WorkSpaces	AWS/WorkSpaces

40を超える  
AWSサービスに対応

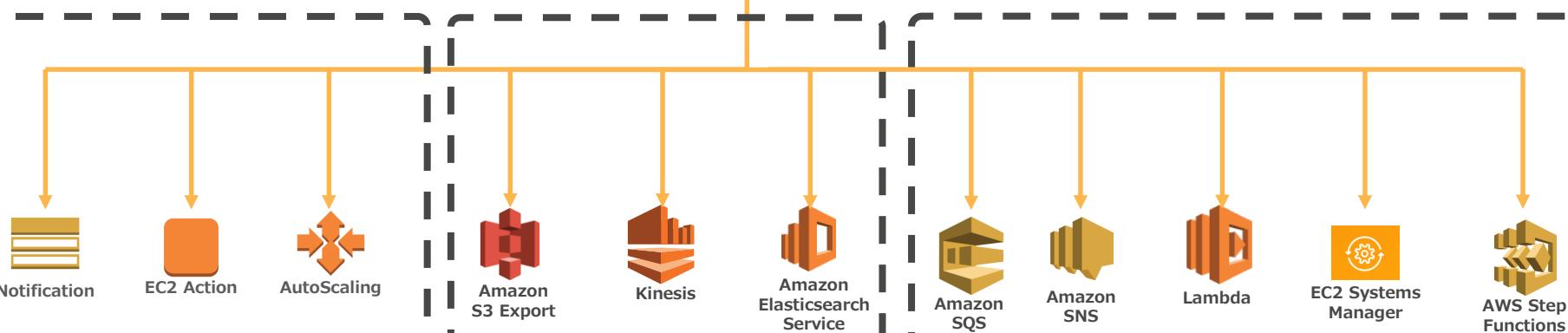
# Why CloudWatch

1. Pollingモデルから、Pushモデルへ
2. サーバ中心の監視から、サービスの監視へ
3. AWSサービスとの**連携**

# AWSサービスとの連携



予め定めてある障害対応手順は、サービス連携により  
**運用の自動化**が可能



CloudWatch

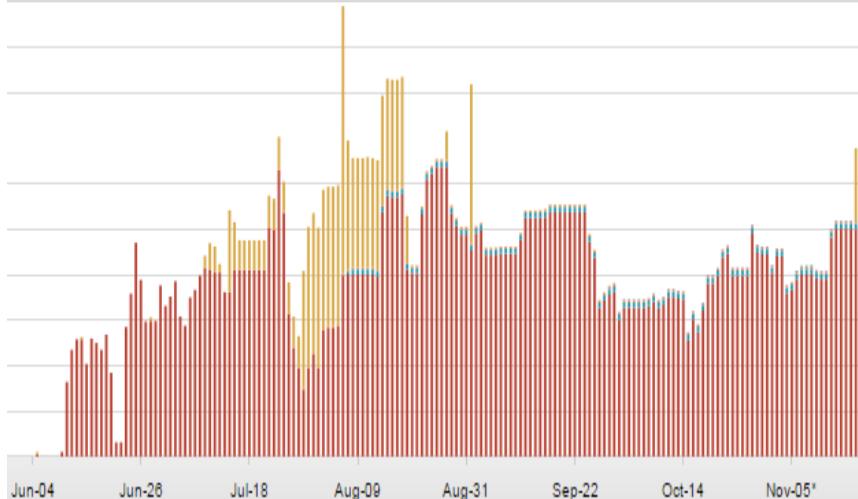
CloudWatch Logs

CloudWatch Events

# クラウドならではの監視も

## 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
- アラームの設定はVirginiaリージョンから設定



### 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

+ Notification

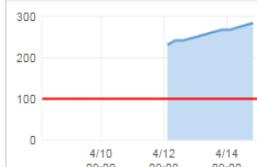
+ AutoScaling Action

+ EC2 Action

### Alarm Preview

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

EstimatedCharges  $\geq$  100



Namespace: AWS/Billing

Currency: USD

Metric Name: EstimatedCharges

# (再掲) Why CloudWatch

1. Pollingモデルから、**Pushモデルへ**
2. サーバ中心の監視から、**サービスの監視へ**
3. AWSサービスとの**連携**

# Dive Deep CloudWatch

# (再掲) Amazon CloudWatchのできる事



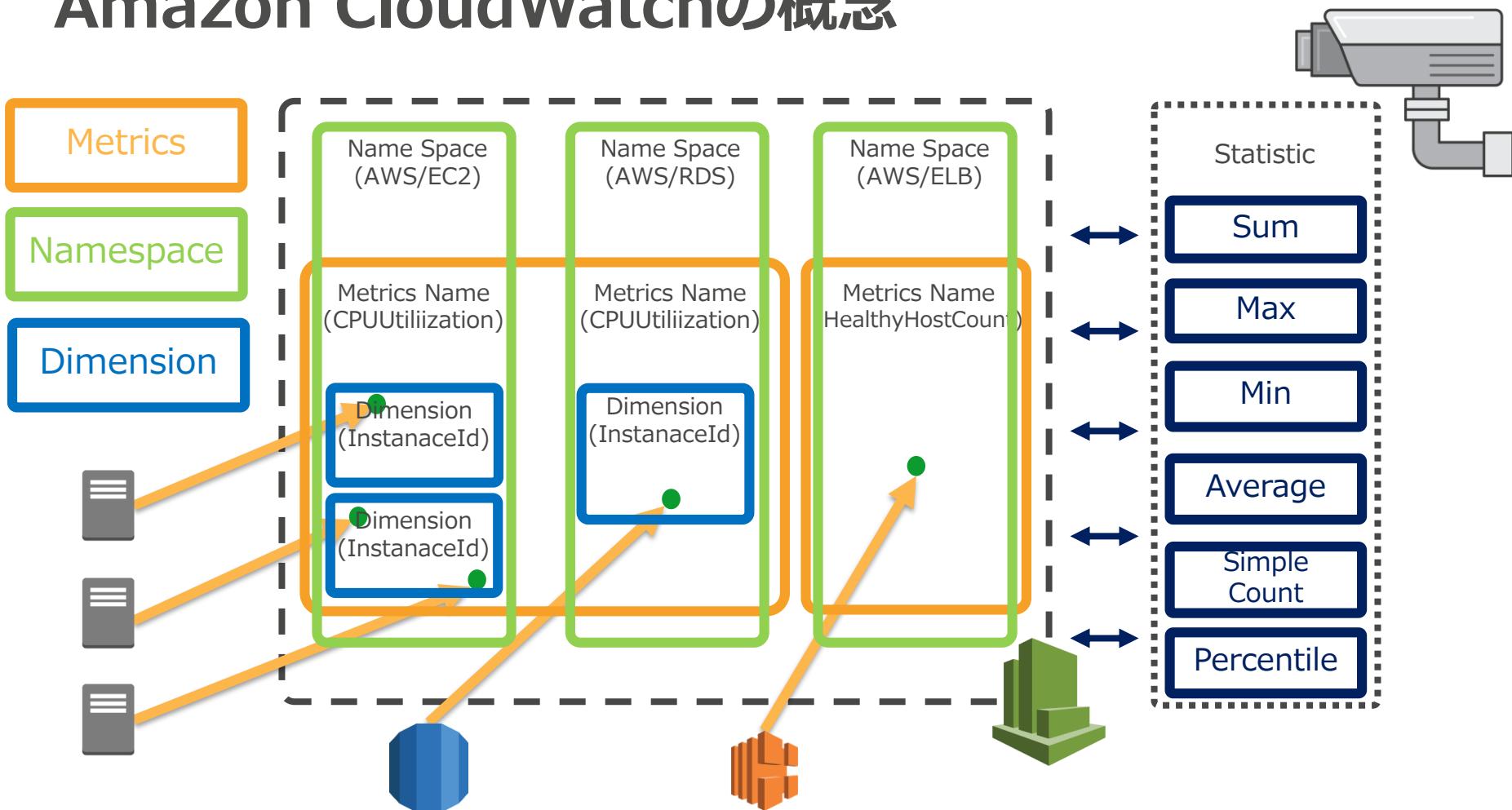
- CloudWatch
  - システム監視サービス
    - ✓ 死活監視 / 性能監視 / キャパシティ監視
- CloudWatch Logs
  - ログ管理プラットフォームサービス
    - ✓ EC2上のOS, APPのログ
    - ✓ AWSマネージド サービスのログ
- CloudWatch Events
  - AWS上リソースの状態監視サービス
  - AWSリソースに対する**イベントをトリガーにアクションを実行**する機能

# Amazon CloudWatch



- *CloudWatch*
  - システム監視サービス
    - ✓ 死活監視 / 性能監視 / キャパシティ監視
- *CloudWatch Logs*
  - ログ管理プラットフォーム サービス
    - ✓ EC2上のOS, APPのログ
    - ✓ AWSマネジドサービスのログ
- *CloudWatch Events*
  - AWS上リソースの状態監視サービス
  - AWSリソースに対するイベントをトリガーにアクションを実行する機能

# Amazon CloudWatchの概念



# CloudWatch利用イメージ 標準メトリックス監視

CloudWatch ダッシュボード

アラーム

不足

OK

請求

イベント

ルール

ログ

メトリクス

無題 グラフ

グラフ表示期間設定

時間 3時間 12時間 1日 3日 1週 カスタム

アクション

オレゴン サポート

Networkin

すべてのメトリクス グラフ化したメトリクス (1) グラフのオプション

すべて > EC2 > インスタンス別メトリクス

任意のメトリクス、ディメンション、またはリソース ID を検索する

インスタンス名 (14)

- sac202

インスタンス ID (InstanceId)

- i-0302cc4dea902539e

対象インスタンス検索ウィンドウ

ディメンション

標準メトリクス一覧

- DiskWriteBytes
- CPUUtilization
- DiskReadOps
- DiskWriteOps
- CPUCreditUsage
- NetworkPacketsIn
- StatusCheckFailed\_System
- DiskReadBytes
- StatusCheckFailed\_Instance
- NetworkOut
- CPUCreditBalance
- Networkin
- NetworkPacketsOut
- StatusCheckFailed

# CloudWatch利用イメージ 標準メトリックス監視



# 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

メトリックスデータの保管は**15ヶ月**まで

- 15ヶ月以上保存する場合は、APIでデータを取得し別の場所に保管しておく（サードパーティ製ツールとの連携も検討）

データの粒度によって遡って参照できる期間が異なる

- 1分毎のデータポイント : 15日間
- 5分毎のデータポイント : 63日間
- 1時間毎のデータポイント : 15ヶ月間

# Amazon CloudWatch を使ったアラーム設定

OK

アラーム  
(Alarm)

不足  
(INSUFFICIENT)

定義された閾値を  
下回っている  
(正常値)

定義された閾値を  
上回っている  
(異常値)

データが不足のため、  
状態を判定できない  
(判定不能)

# 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

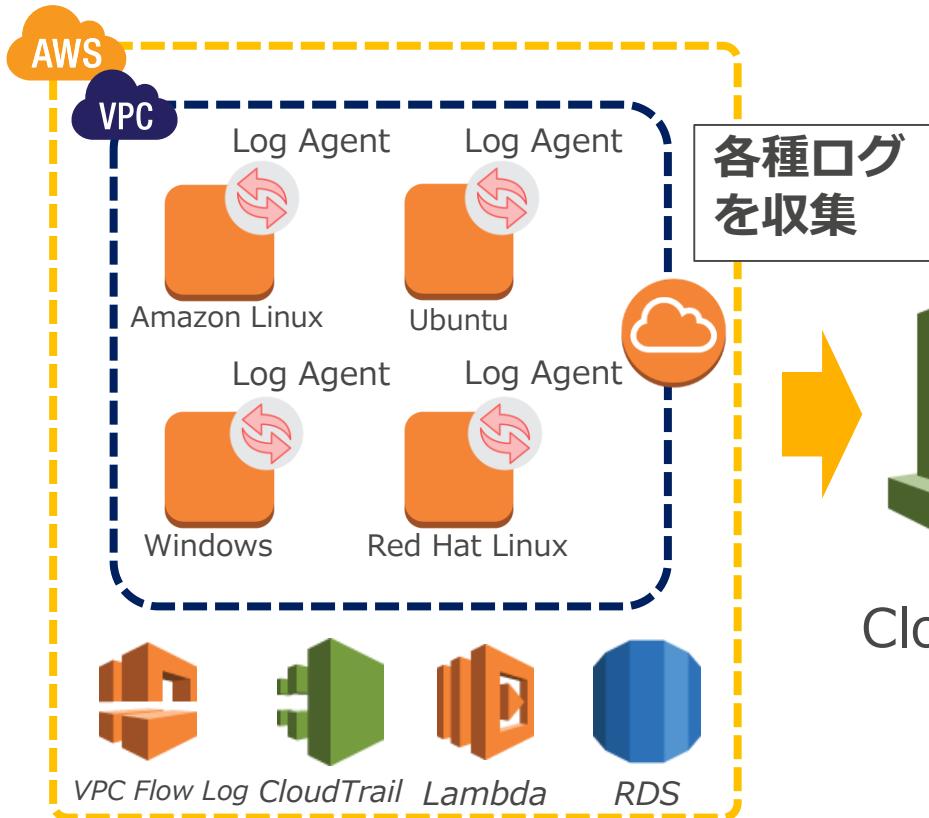


# Amazon CloudWatch Logs



- *CloudWatch*
  - AWS上で稼働するシステム監視サービス
    - ✓ 死活監視 / 性能監視 / キャパシティ監視
- *CloudWatch Logs*
  - **ログ管理**プラットフォームサービス
    - ✓ EC2上のOS, APPのログ
    - ✓ AWSマネジドサービスのログ
- *CloudWatch Events*
  - AWS上リソースの状態監視サービス
  - AWSリソースに対するイベントをトリガーにアクションを実行する機能

# CloudWatch Logs



通知:  
CloudWatch Alarm



エクスポート:  
Amazon Kinesis  
Firehose



可視化:  
Amazon Elasticsearch  
Service  
(Kibana)

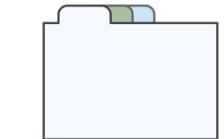
# Use cases

- ログの長期保存、ストレージの容量削減
- HTTP responsesのエラー、例外、性能の監視
- ホストにログインせずに障害調査
- セキュリティインシデント対応用の証跡ログとして



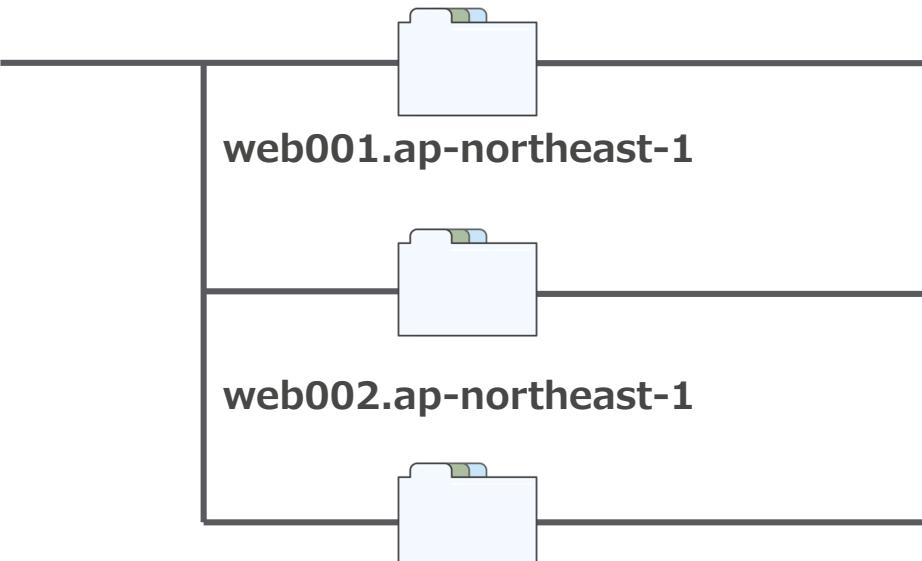
# CloudWatch Logsのログ管理

## Log Group



## Web Server

# Log Stream



## web003.ap-northeast-1

## Log Event



# ログの保存期間

CloudWatch Logsはログの保存期間を設定可能

## 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

A dropdown menu for 'Expire Events After' is open, showing a list of options. The 'Never Expire' option is selected and highlighted with a red box. A larger red box surrounds the entire dropdown menu, which lists the following options:

- 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)

# 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 ロググループ Default-Log-Group 0-0299505423feee84b

フィルター (検索)

すべて展開 行 テキスト

すべて 30秒 5分 1時間 6時間 1日 1週 カスタム

イベントのフィルター

時間 (UTC +00:00) メッセージ

05-03

タイムスタンプ ログメッセージ

タイムスタンプ	ログメッセージ
14:57:16	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The Software Protection service entered the running state.]
15:17:32	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The Software Protection service entered the stopped state.]
15:17:33	[System] [Error] [1111] [Microsoft-Windows-TerminalServices-Printers] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [Driver Microsoft Print To PDF required for printer Microsoft Print to PDF.]
15:17:35	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The Device Setup Manager service entered the running state.]
15:19:35	[System] [Error] [1111] [Microsoft-Windows-TerminalServices-Printers] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [Driver Send to Microsoft OneNote 16 Driver required for printer Microsoft OneNote 16.]
15:21:30	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The Device Setup Manager service entered the stopped state.]
▶ 15:17:35	[System] [Error] [1111] [Microsoft-Windows-TerminalServices-Printers] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [Driver Send to Microsoft OneNote 16 Driver required for printer Microsoft OneNote 16.]
▶ 15:19:35	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The Device Setup Manager service entered the stopped state.]
▶ 15:21:09	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The WinHTTP Web Proxy Auto-Discovery Service service entered the stopped state.]
▶ 15:34:57	[System] [Error] [36888] [Schannel] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connection.]
▶ 15:34:57	[System] [Error] [36888] [Schannel] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connection.]
▶ 15:40:04	[System] [Error] [36888] [Schannel] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connection.]
▶ 15:40:04	[System] [Error] [36888] [Schannel] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connection.]
▶ 15:44:42	[System] [Information] [7036] [Service Control Manager] [WIN-3AM8GUMMNLG.defaultvc-adtest2.local] [The WinHTTP Web Proxy Auto-Discovery Service service entered the running state.]

# CloudWatch Logs Metric Filter

ログイベントから特定の文字列のフィルタリングが可能

## ログメトリクスフィルタの定義

ロググループのフィルター: `/var/log/messages`

メトリクスフィルターを使用し、ロググループ内のイベントが CloudWatch ログに送信されるときに、それらのイベントを自動的にモニタリングできます。特定の用語のモニタリングやカウントを行ったり、ログイベントから値を抽出したりでき、その結果をメトリクスに関連付けることができます。[パターン構文の詳細を確認してください。](#)

フィルタパターン

DHCPREQUEST

[例の表示](#)

テストするログデータの選択

i-03c761920e378615b

クリア

[パターンのテスト](#)

Apr 28 10:22:06 ip-172-31-30-146 dhclient[2133]: XMT: Solicit on eth0, interval 125240ms.

Apr 28 10:24:12 ip-172-31-30-146 dhclient[2133]: XMT: Solicit on eth0, interval 109010ms.

Apr 28 10:24:36 ip-172-31-30-146 dhclient[2047]: DHCPREQUEST on eth0 to 172.31.16.1 f...

Apr 28 10:24:36 ip-172-31-30-146 dhclient[2047]: DHCPACK from 172.31.16.1 (xid=0xb30...

Apr 28 10:24:36 ip-172-31-30-146 dhclient[2047]: bound to 172.31.30.146 -- renewal in...

Metric Filterからアラーム作成、  
SNS連携が可能

結果

サンプルログの 50 イベントから 3 の一致が見つかりました

# CloudWatch Logs Metric filter syntax

- 文字列の一致
- Common log format
- JSON



# Metric filters – 文字列の一致

## Filter examples

- Error
- “Invalid user”
- NullReferenceException “main(”

## Notes

- AND検索
- 文字列のグループ化、英数字以外の検索は“ ” 囲む
- Metricは出現回数で評価される

# Metric filters – Common log format

## Log examples

[11/Nov/2014:02:00:14 +0000] 10.15.128.6 "GET HTTP/1.1" 200 108 33 "S3Console/0.4"  
127.0.0.1 user-identifier frank [10/Oct/2000:13:55:36 -0700] "GET /apache\_pb.gif HTTP/1.0"  
200 2326

## Filter example

[**Timestamp**, **IPAddress**, **Header**, **HTTPCode=4\***, ...]

## Notes

- ・ “” か [ ]で囲まれていない限り、空白文字が区切り文字となる
- ・ 値の抽出が可能

# Metric filters – JSON

## Filter examples

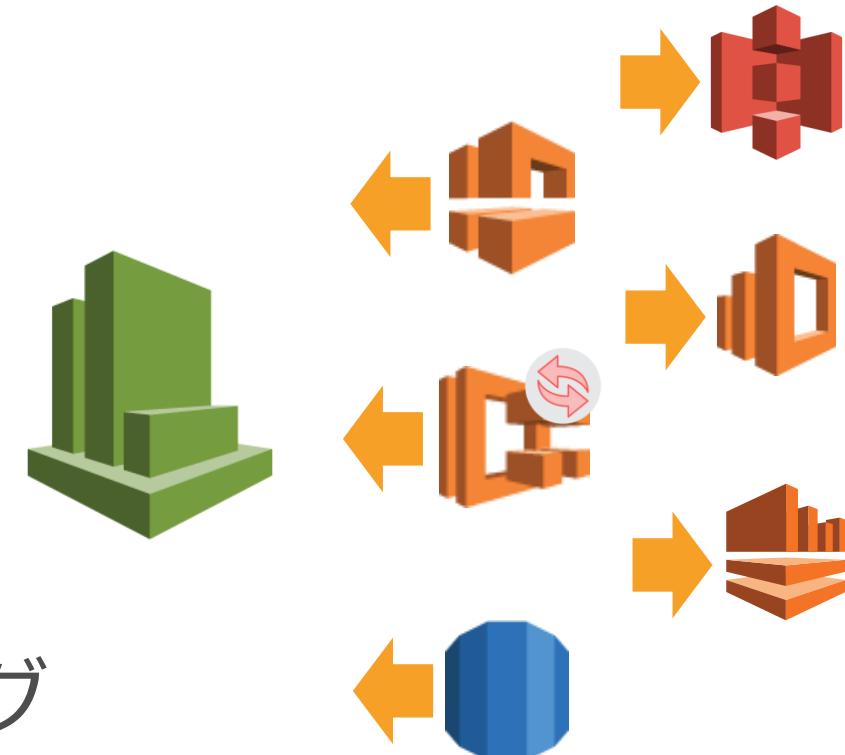
```
{$.errorCode = "AccessDenied" || $.errorCode = "UnauthorizedOperation"}  
{ $.eventType = "UpdateTrail" }  
{ $.sourceIpAdress != 123.123.* }  
{ $.arrayKey[0] = "value" }  
{ $.objectList[1].id = 2 }
```

## Notes

- {}で囲むとJSONとして評価される

# AWSサービスとの連携

- S3へのエクスポート
- VPC Flow Logs
- Elasticsearch
- ECS
- Kinesis
- RDS拡張モニタリング

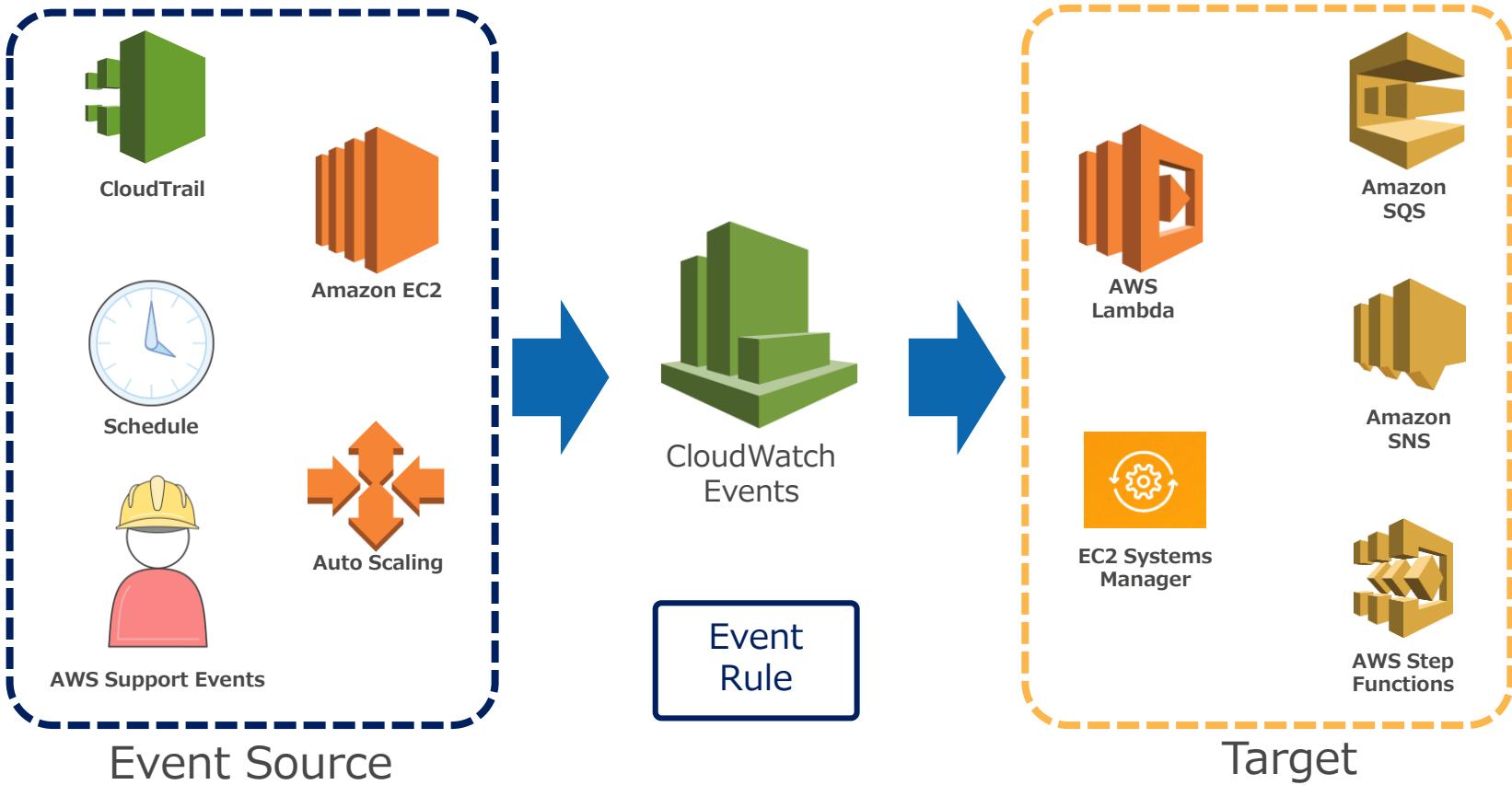


# Amazon CloudWatch Events



- *CloudWatch*
  - AWS上で稼働するシステム監視サービス
    - ✓ 死活監視 / 性能監視 / キャパシティ監視
- *CloudWatch Logs*
  - ログ管理プラットフォーム サービス
    - ✓ EC2上のOS, APPのログ
    - ✓ AWSマネジドサービスのログ
- *CloudWatch Events*
  - AWS上リソースの状態監視サービス
  - AWSリソースに対する**イベントをトリガーにアクションを実行**する機能

# CloudWatch Events



# イベントソースの選択

## EC2 Instance states change notification

- Pending/Running/Shutting down/Stopped/Stopping/Terminated

## Schedule

- 間隔：分(Minutes)/時間(Hours)/日(Days)
- クーロン表記

## AWS API call

- AWS CloudTrailにより発行されたイベント

## AWS console sign-in

## AWS SupportへのCase作成

## Auto Scaling

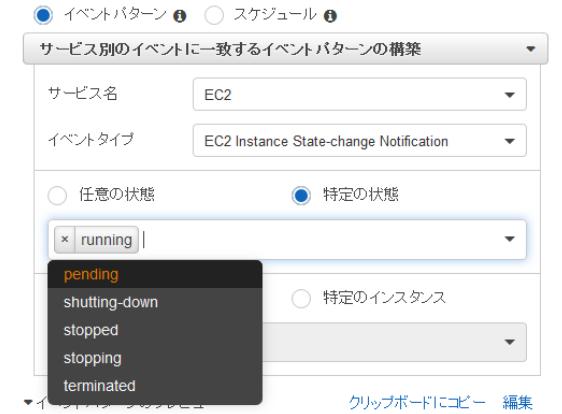
- Launch Successful / Launch Unsuccessful
- Terminate Successful / Terminate Unsuccessful

### ステップ 1: ルールの作成

AWS 環境で発生するイベントに基づいてターゲットを呼び出すためのルールを作成します。

#### イベントソース

イベントパターンを構築またはカスタマイズするか、スケジュールを設定してターゲットを呼び出します。



イベントパターン  イベントパターン  スケジュール

サービス別のイベントに一致するイベントパターンの構築

サービス名: EC2

イベントタイプ: EC2 Instance State-change Notification

任意の状態  特定の状態

running

pending

shutting-down

stopped

stopping

terminated

特定のインスタンス

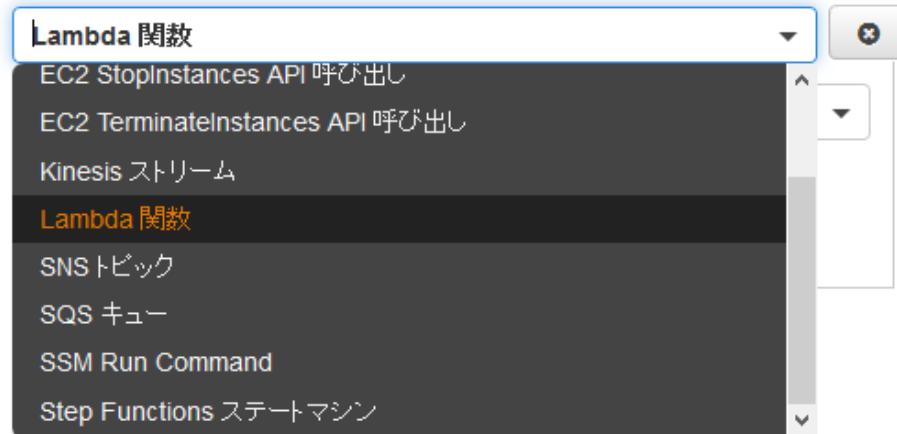
クリップボードにコピー 編集

# ターゲットの選択

- Lambda Function
- SNS Topic
- SQS Queue
- SSM Run Command
- Step Function StateMachine
- Kinesis Stream
- Built-in target
  - EC2インスタンスの再起動
  - EC2インスタンスの削除
  - EC2インスタンスの停止
  - EBSボリュームのスナップショット作成

## ターゲット

イベントがイベントパターンに一致するか、スケジュールがトリガーされたときに呼び出すターゲットを選択します。



# (再々掲) Amazon CloudWatchのできる事



- CloudWatch
  - システム監視サービス
    - ✓ 死活監視 / 性能監視 / キャパシティ監視
- CloudWatch Logs
  - ログ管理プラットフォームサービス
    - ✓ EC2上のOS, APPのログ
    - ✓ AWSマネージド サービスのログ
- CloudWatch Events
  - AWS上リソースの状態監視サービス
  - AWSリソースに対する**イベントをトリガーにアクションを実行**する機能

# まとめ



CloudWatch

- クラウドシステムの正常・異常を監視する事ができるマネージドサービス
- サービス間の連携により各種サービス、アプリケーションの運用の自動化が可能
- AWSクラウドにおける運用監視はCloudWatchが最適！

# 本セッションのFeedbackをお願いします

受付でお配りしたアンケートに本セッションの満足度やご感想などをご記入ください  
アンケートをご提出いただきました方には、もれなく素敵なAWSオリジナルグッズを  
プレゼントさせていただきます



アンケートは受付、パミール3FのEXPO展示会場内にて回収させて頂きます

AWS

S U M M I T

Thank you!

