AWS

SUMMIT

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

amazon web services

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

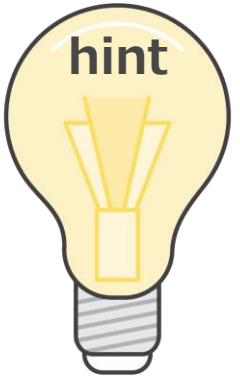
- Amazon Virtual Private Cloud（VPC）
- Amazon CloudWatch

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

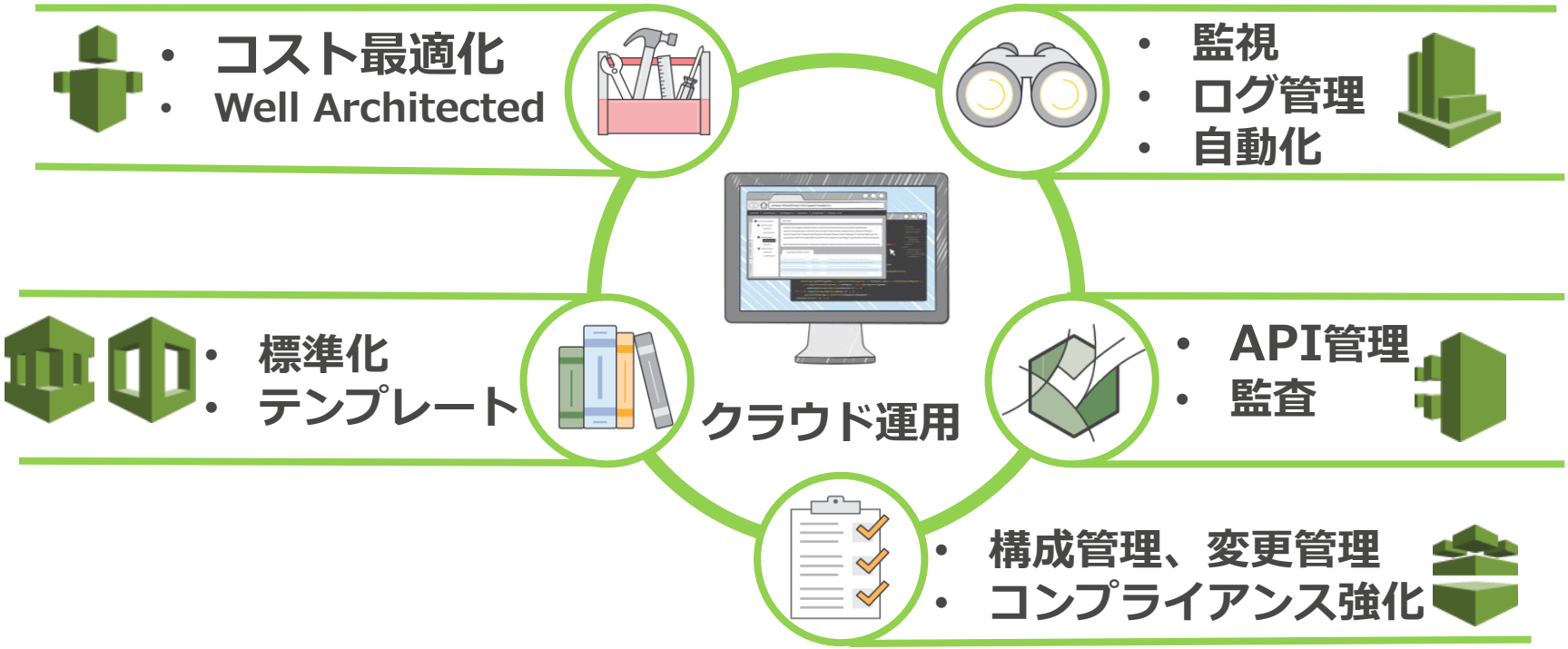


本セッションについて

- 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

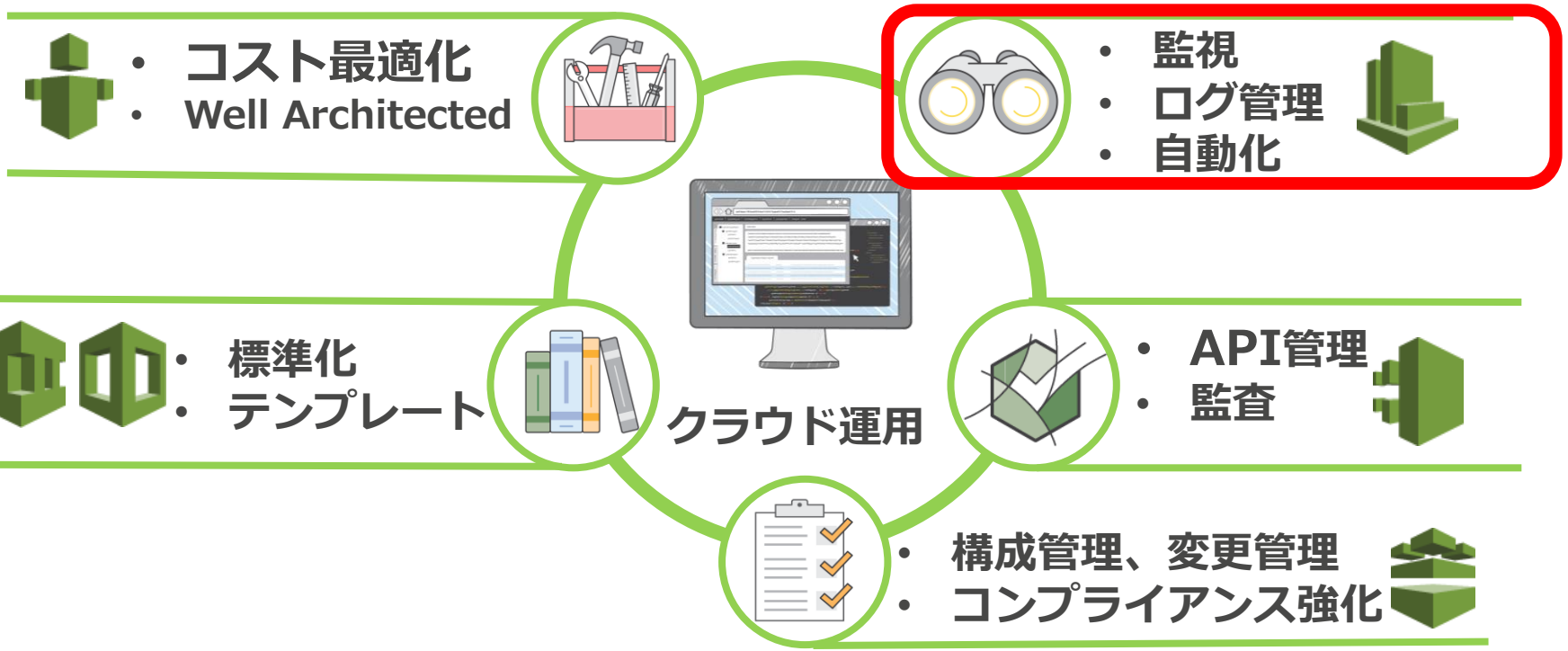
クラウドの運用

AWSのクラウド運用


• コスト最適化
• Well Architected
• 監視
• ログ管理
• 自動化
• 標準化
• テンプレート
クラウド運用
• API管理
• 監査
• 構成管理、変更管理
• コンプライアンス強化

AWSのクラウド運用

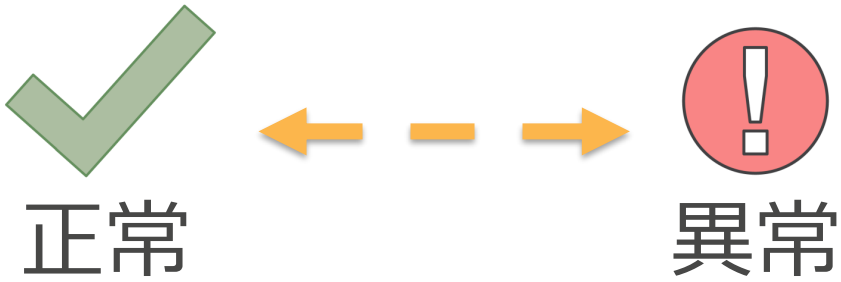
今日はここを中心に



システム監視とは

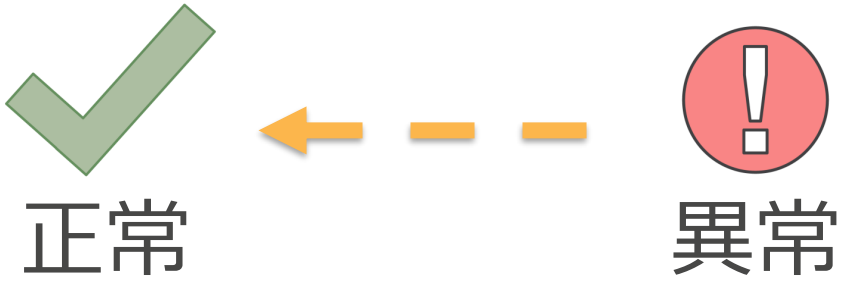
システム監視とは

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？

Serverless？

スケールアウト？

ビッグデータ？

データレイク？

マネージドサービス？

AWSクラウドにおけるシステム運用監視は CloudWatchが最適！

CloudWatch

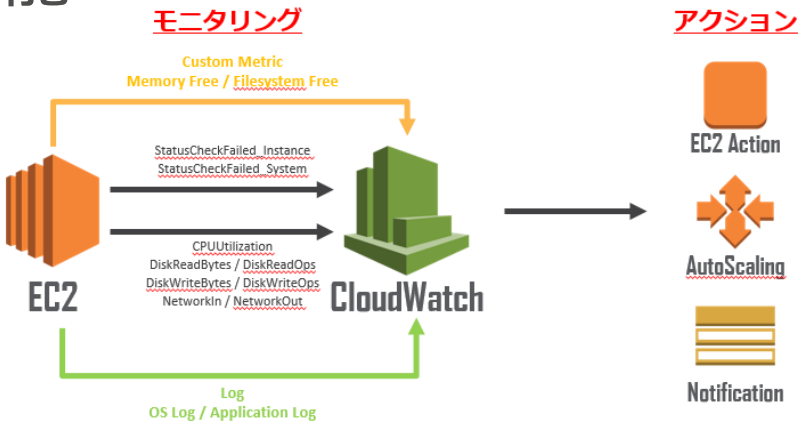
Amazon CloudWatchとは

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

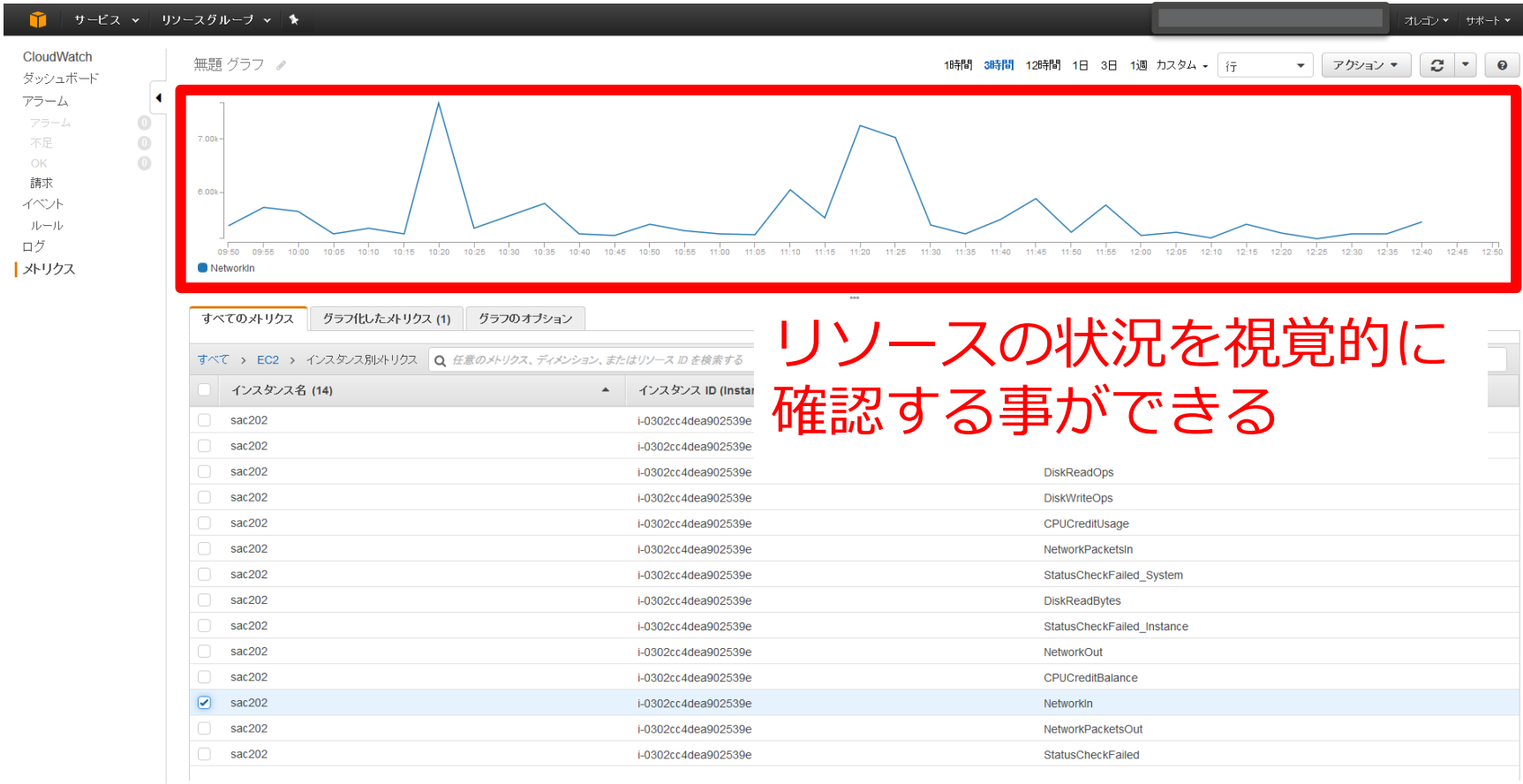


Amazon CloudWatchのできる事

CloudWatch

- ***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



リソースの状況を視覚的に
確認する事ができる

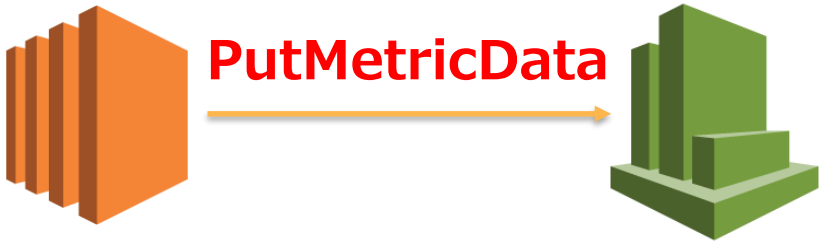
CloudWatchのメトリックス

標準メトリックス(EC2)

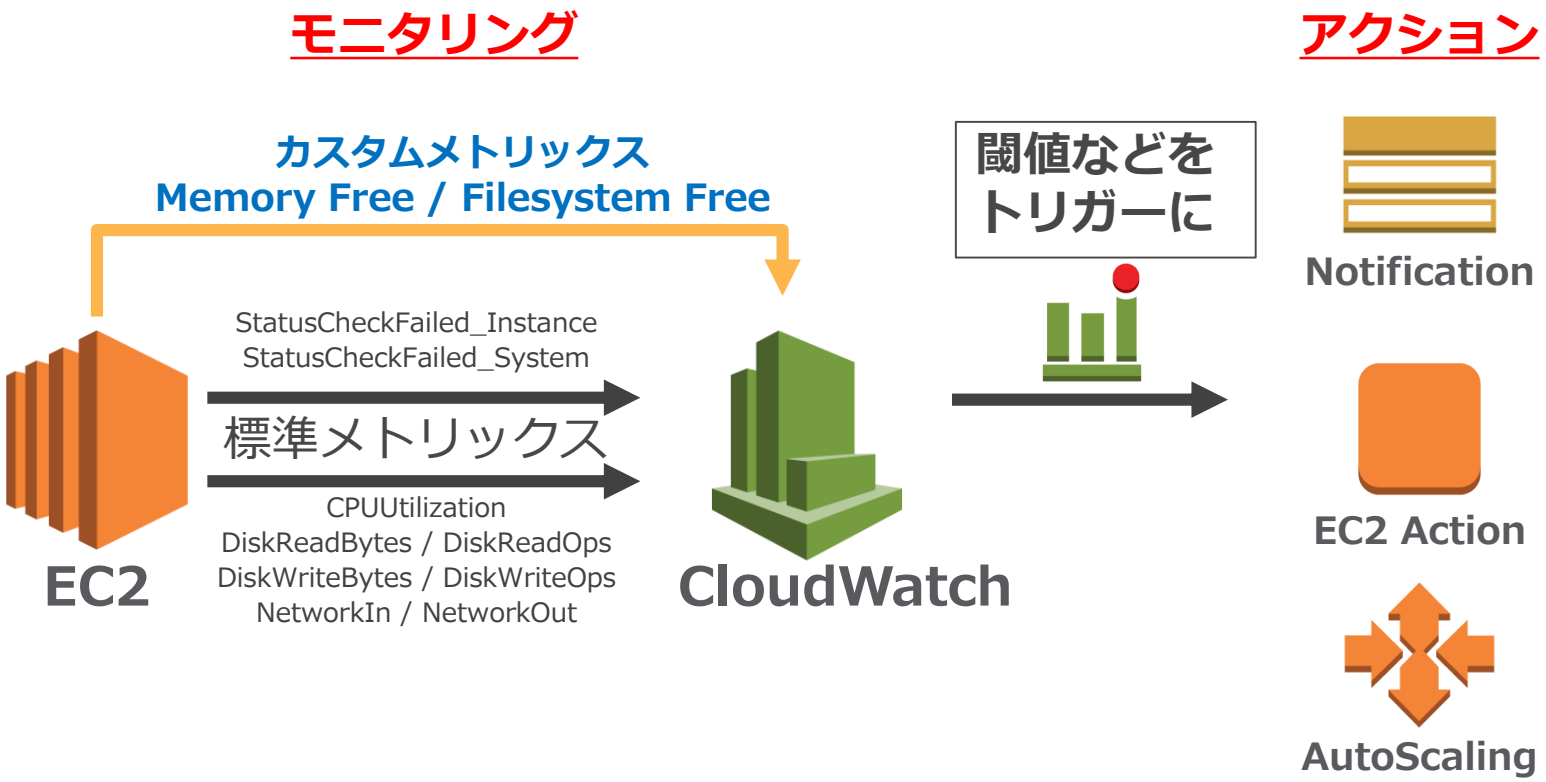
CPUUtilization
CPUCreditBalance
CPUCreditUsage
DiskReadBytes
DiskWriteBytes
DiskReadOps
DiskWriteOps
NetworkOut
NetworkIn
NetworkPacketsIn
NetworkPacketsOut
StatusCheckFailed_Instance
StatusCheckFailed
StatusCheckFailed_System
BurstBalance

カスタムメトリックス

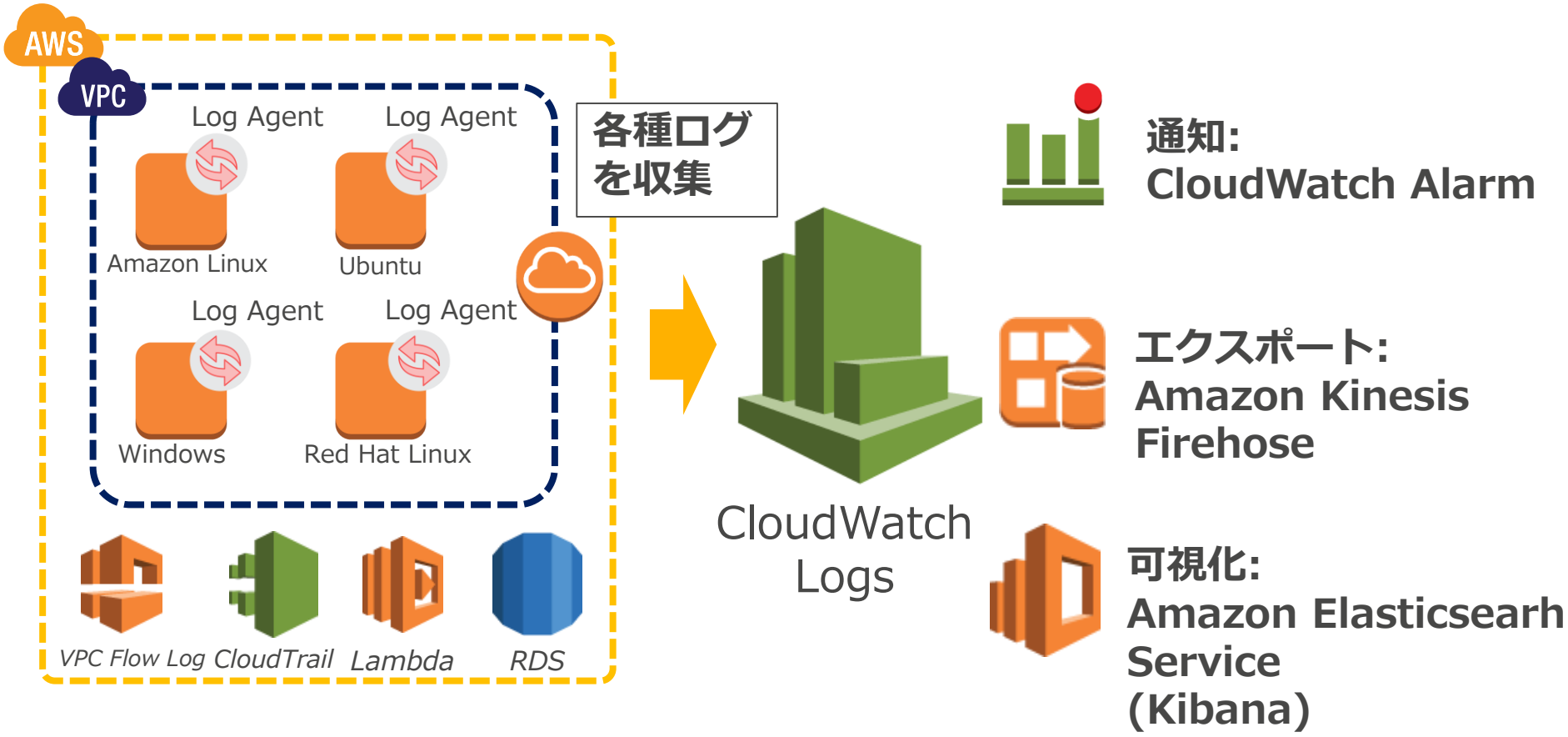
標準メトリックスでは
収集できないメトリックス



Amazon CloudWatch のアクション機能



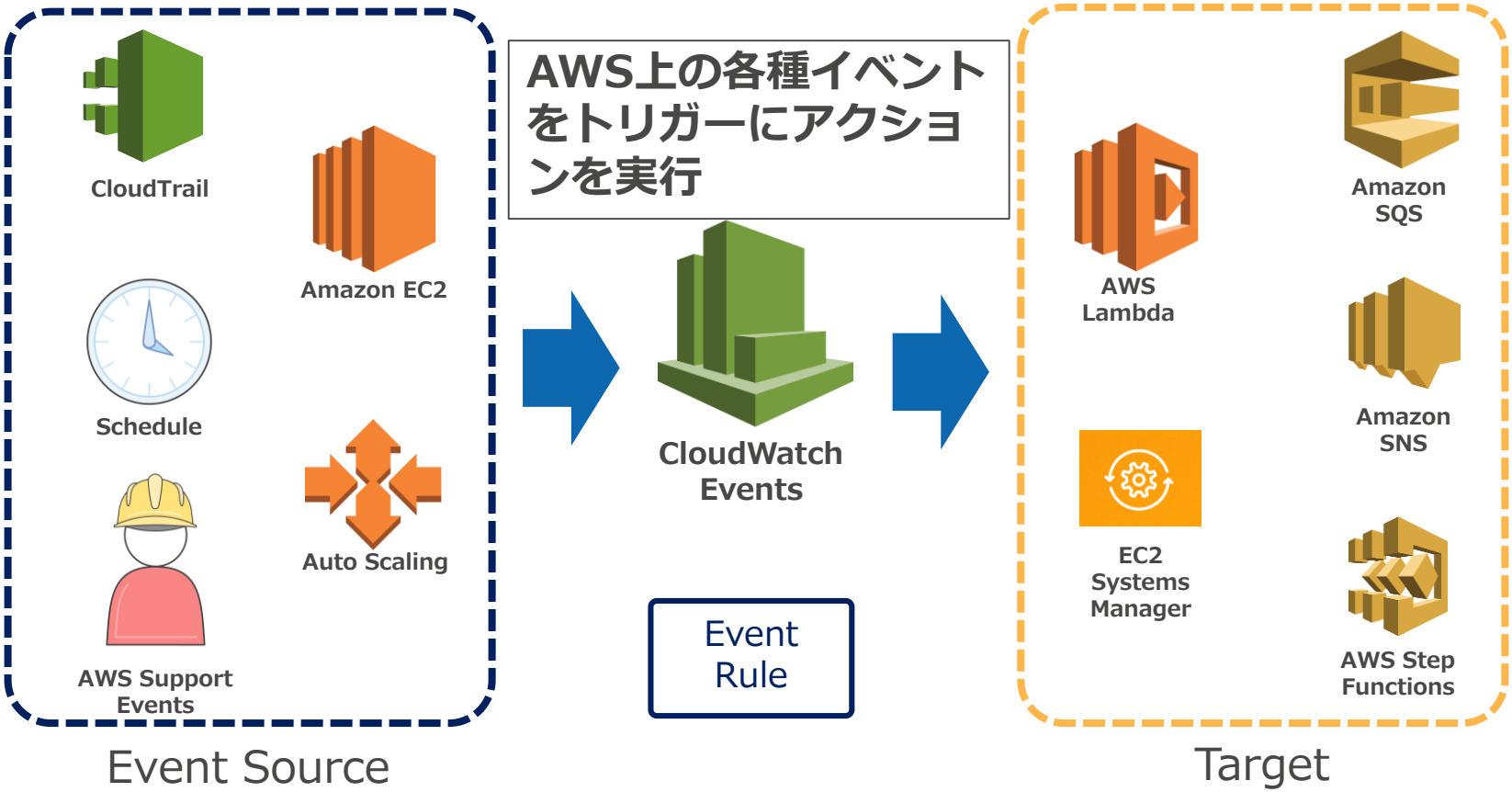
CloudWatch Logs利用イメージ



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 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

CloudTrail

イベントソース

サインインイベント

イベントパターン

サービス別のイベントに一

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

Amazon SNS

ターゲット

イベントがイベントパターン(　　)れたときに呼び出すターゲットを選択します。

SNSトピック

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

ログインアラート

AWS Notification Message - メッセージ (テキスト形式)

2017/06/02 (金) 0:34

AWS Notifications <no-reply@sns.amazonaws.com>

AWS Notification Message

宛先 Fujikura, Kazuaki

{"version":"0","id":"d4c5ede5-fa89-4b20-ab13-504e3a20df39","detail-type":"CloudTrail","source":"aws.signin","account":"029845397858","time":"2017-(　　)1","resources":[],"detail":{"eventVersion":"1.05","userIdentity":{"type":"IAMUser", principalId : AIDAIW3TREGGWMPWMQOW , arn : arn:aws:iam::029845397858:user/kazuakf","accountId":"029845397858","userName":"kazuakf"},"eventTime":"2017-06-01T15:33:14Z","eventSo(　　)1","sourceIPAddress":"7(　　)Firefox/45.0","requestPa(　　)com/console/home?state=hashArgs%23&isauthcode=true","MobileVersion":"No","MFAUsed":"No"},"eventID":"bccabeda-56e2-4287-a553-

"userName":"kazuakf"}

"sourceIPAddress":"72.21.196.68","userAgent":"Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0)

Amazon CloudWatchのできる事

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**

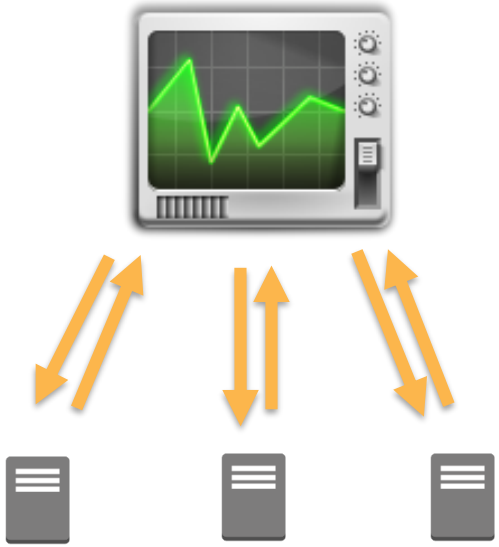
Why CloudWatch

1. Pollingモデルから、**Pushモデル**へ

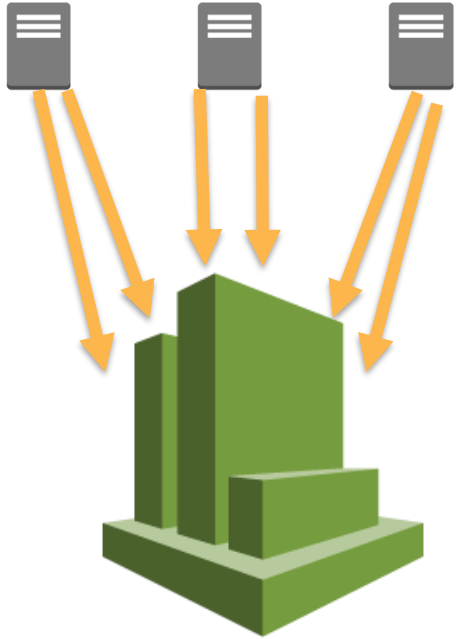
2. サーバ中心の監視から、**サービスの監視**へ

3. AWSサービスとの**連携**

Polling / Push

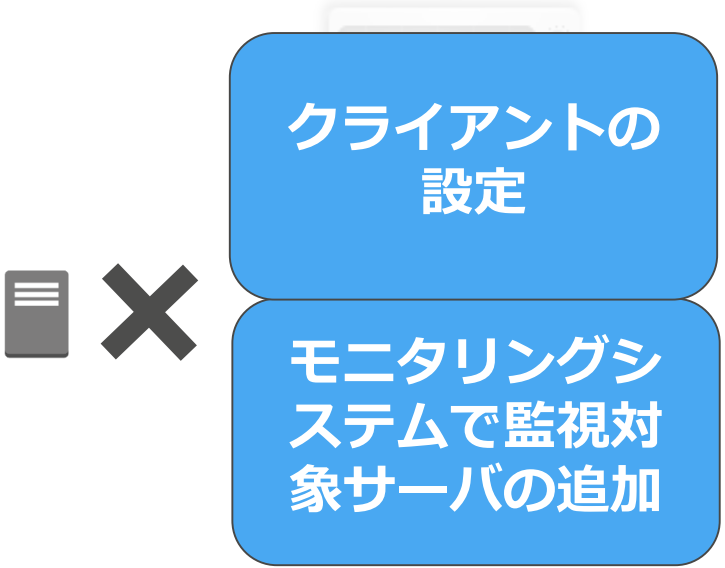


Before Cloud



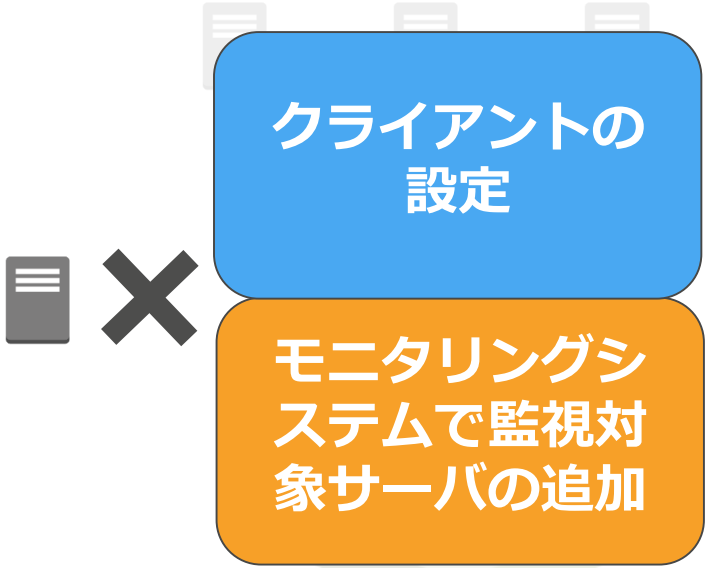
Amazon CloudWatch

Polling / Push



Before Cloud

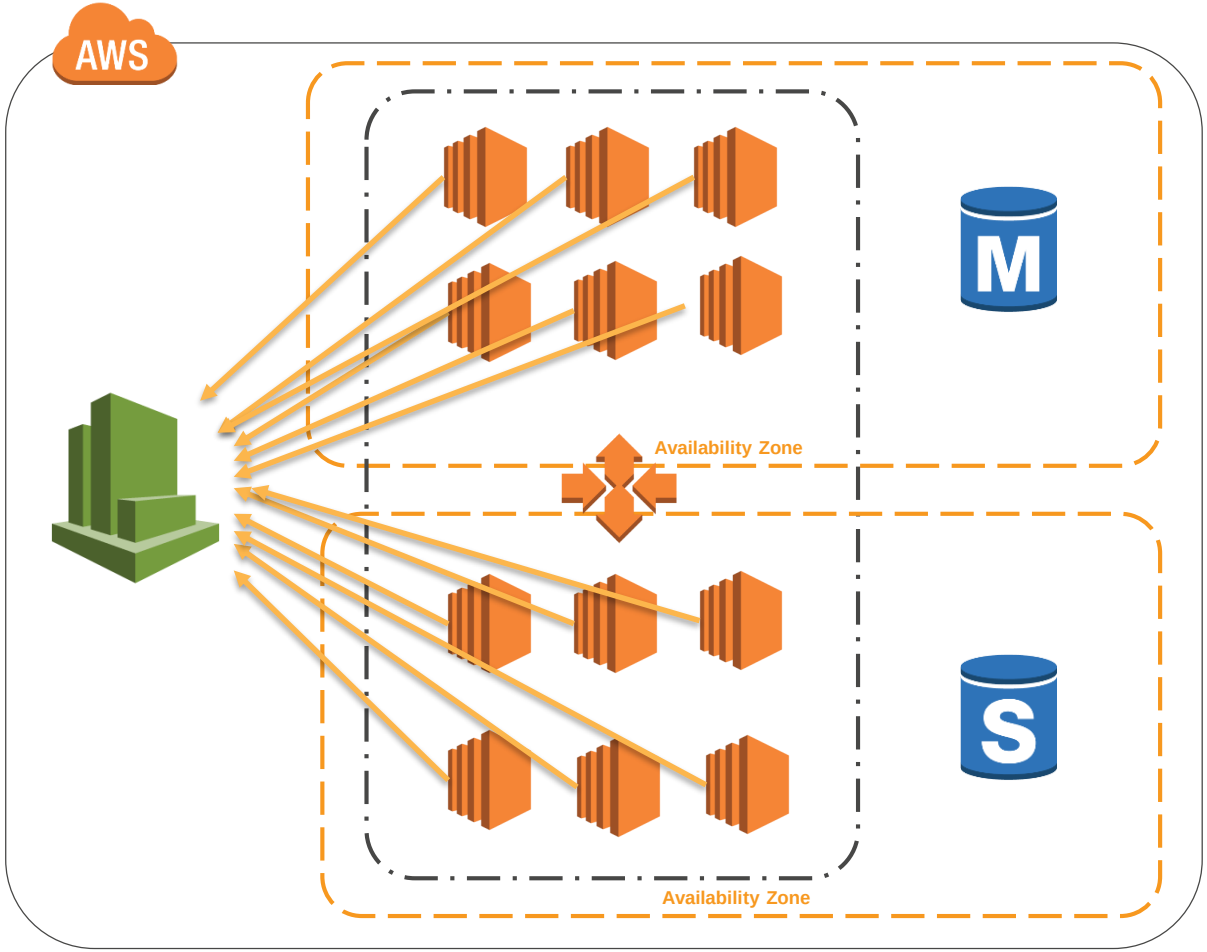
監視を始めるまでに必要な作業



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

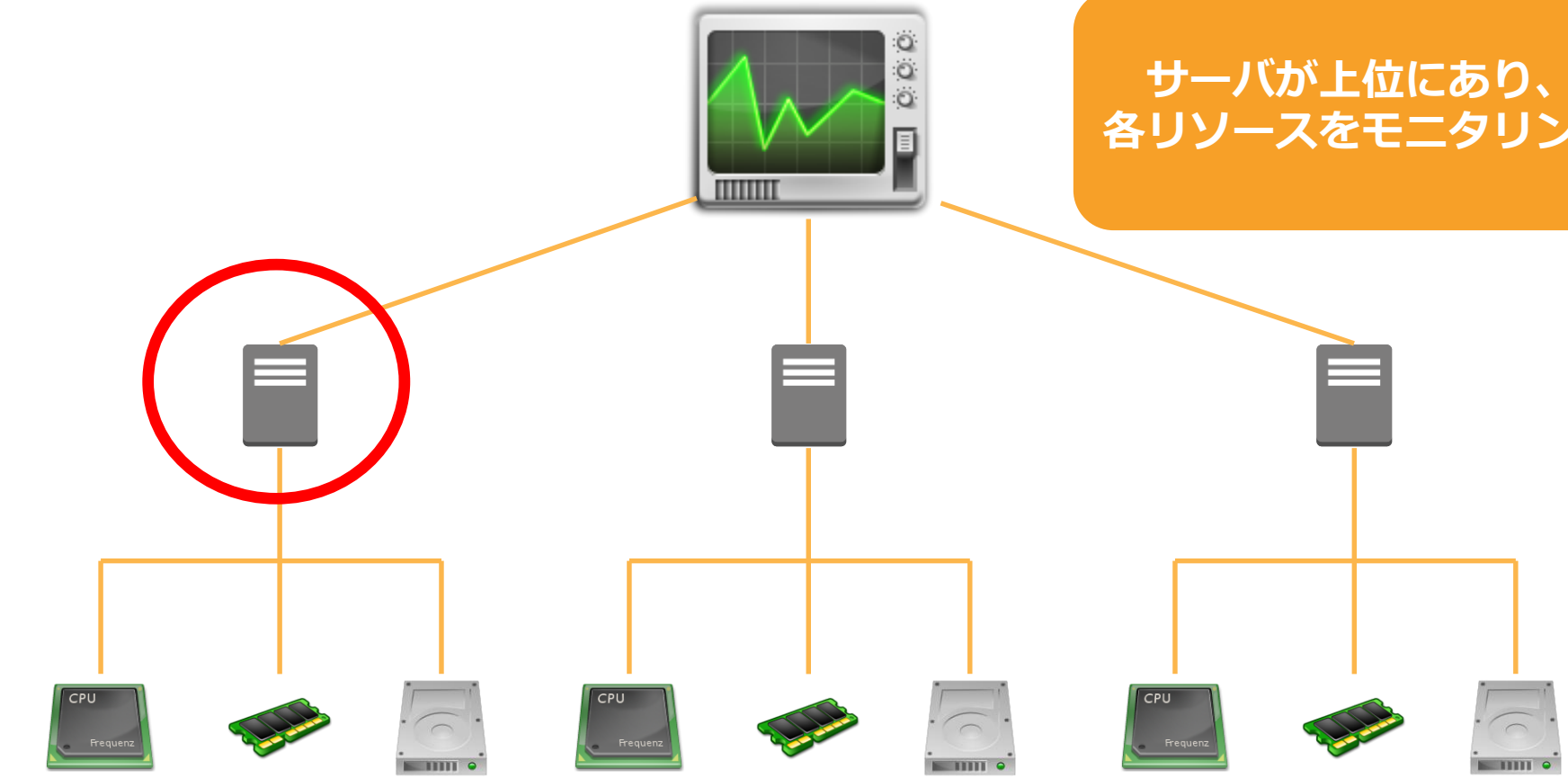
Why CloudWatch

1. Pollingモデルから、**Pushモデル**へ

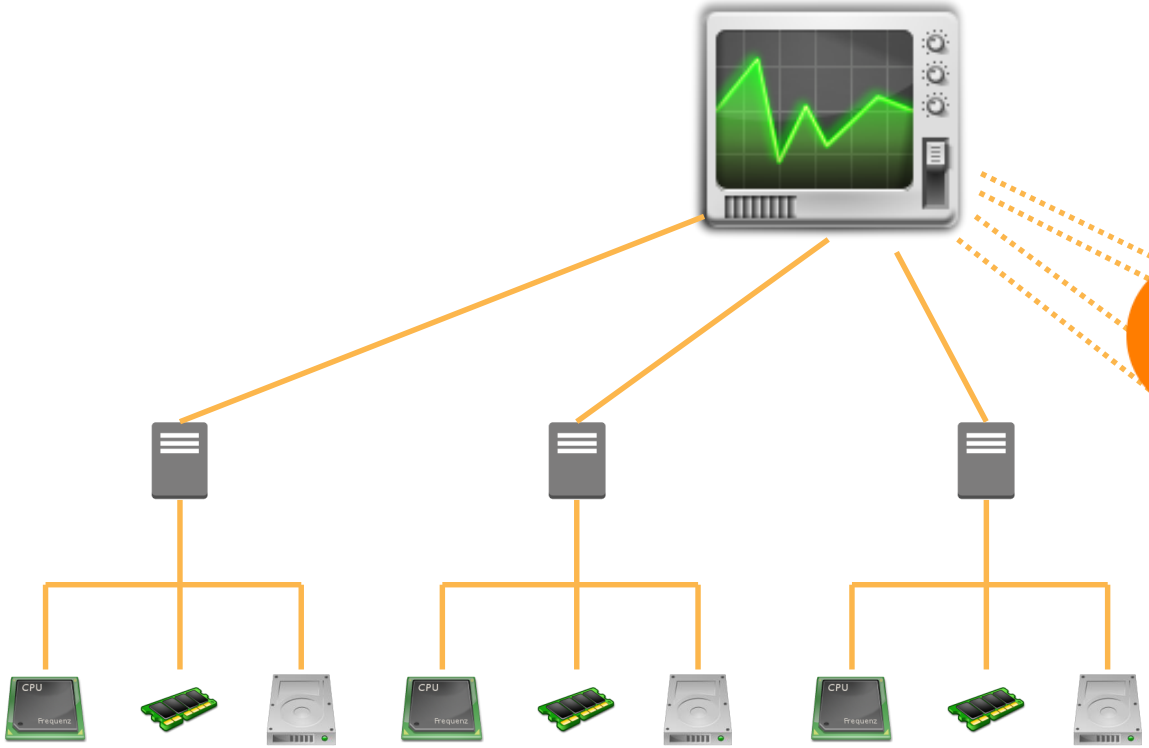
2. サーバ中心の監視から、**サービスの監視**へ

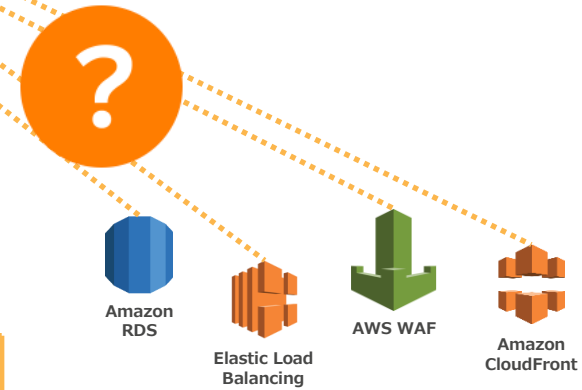
3. AWSサービスとの**連携**

従来のモニタリングシステム



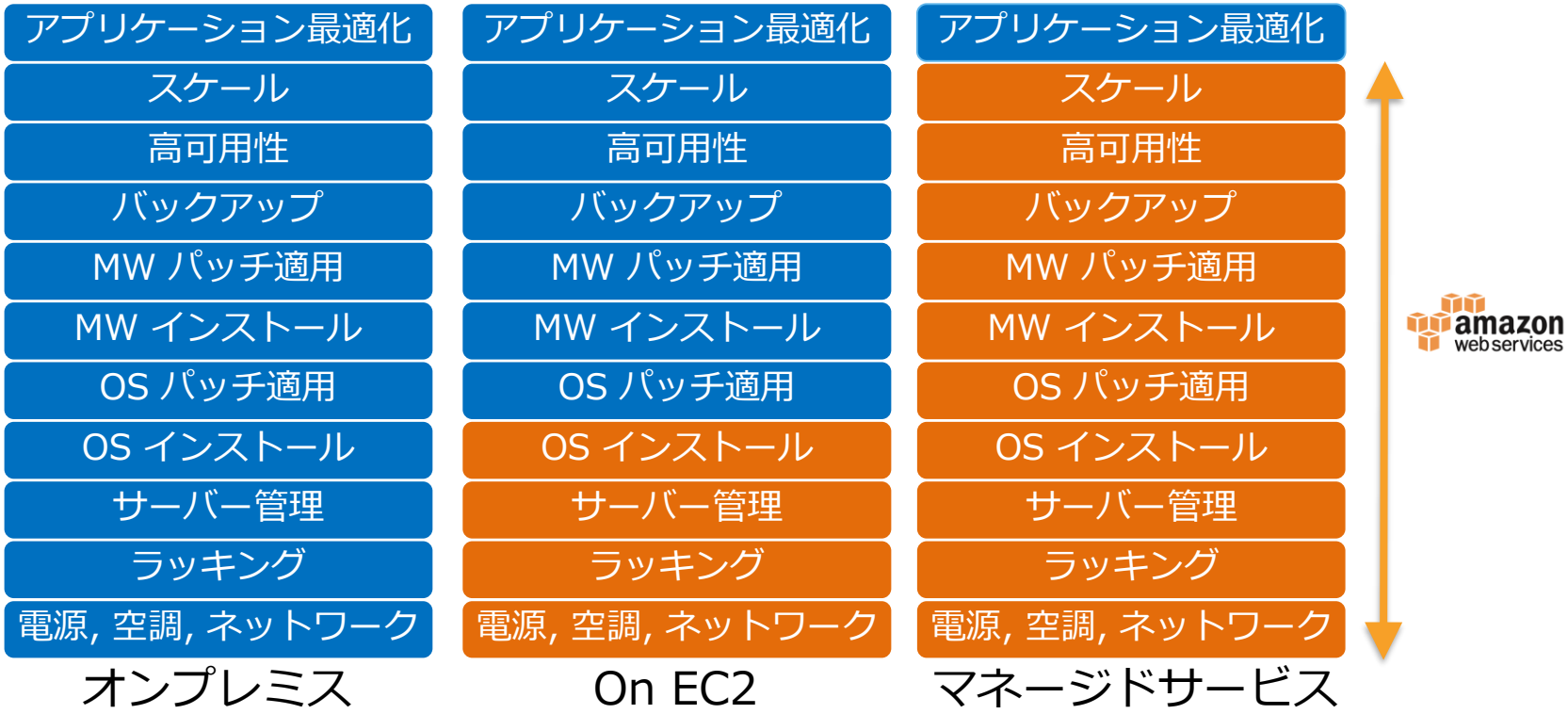
従来のモニタリングシステム



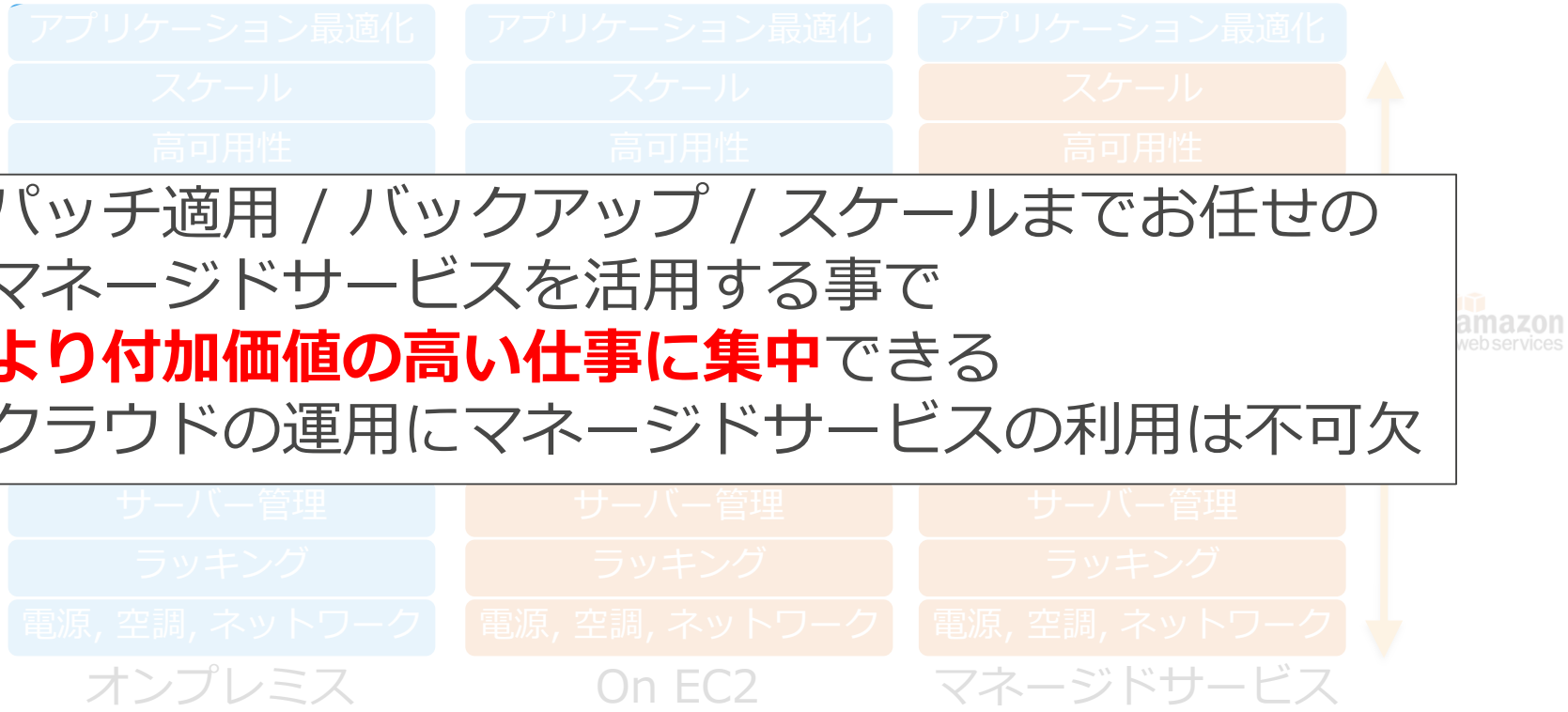


マネージドサービスのモニタリングは？

マネージドサービスの場合



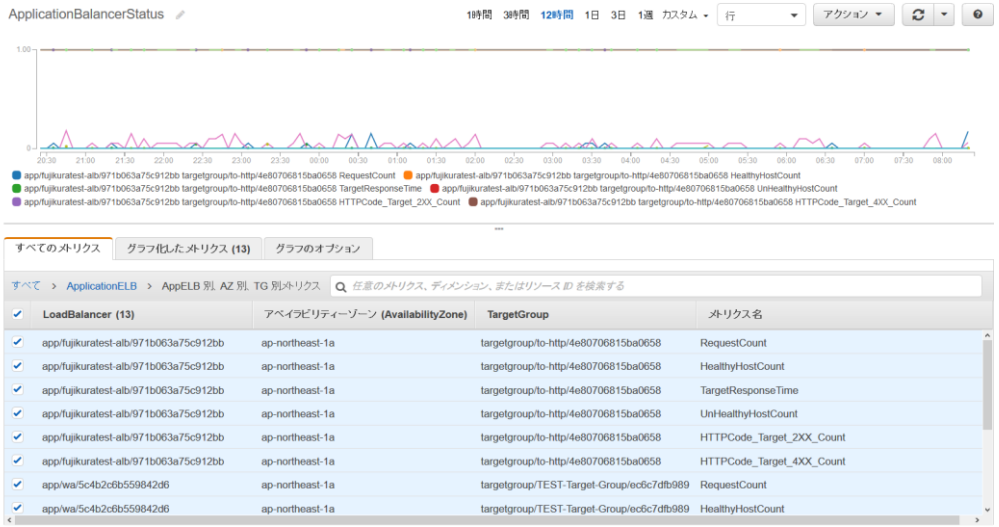
マネージドサービスの場合



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
Amazon API Gateway	AWS/ApiGateway
Auto Scaling	AWS/AutoScaling
AWS Billing	AWS/Billing
Amazon CloudFront	AWS/CloudFront
Amazon CloudSearch	AWS/CloudSearch
Amazon CloudWatch Events	AWS/Events
Amazon CloudWatch Logs	AWS/Logs
AWS Database Migration Service	
Amazon DynamoDB	
Amazon EC2	
Amazon EC2 Containe	
AWS Elastic Beanstalk	
Amazon Elastic Block Sto	
Amazon Elastic File Systen	
Elastic Load Balancing	
Elastic Load Balancing	(Application ancers)
Amazon Elastic Transcoder	/ElasticTranscoder
Amazon ElastiCache	AWS/ElastiCache
Amazon Elasticsearch Service	AWS/ES

AWS サービス	名前空間
Amazon EMR	AWS/ElasticMapReduce
AWS IoT	AWS/IoT
Service	AWS/KMS
cs	AWS/KinesisAnalytics
	AWS/Firehose
	AWS/Kinesis
	AWS/Lambda
	AWS/ML
	AWS/OpsWorks
	AWS/Polly
	AWS/Redshift
	AWS/RDS
	AWS/Route53
ield Advanced	AWS/DDoSProtection
azon Simple Email Service	AWS/SES
Amazon Simple Notification Service	AWS/SNS
Amazon Simple Queue Service	AWS/SQS
Amazon Simple Storage Service	AWS/S3
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

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

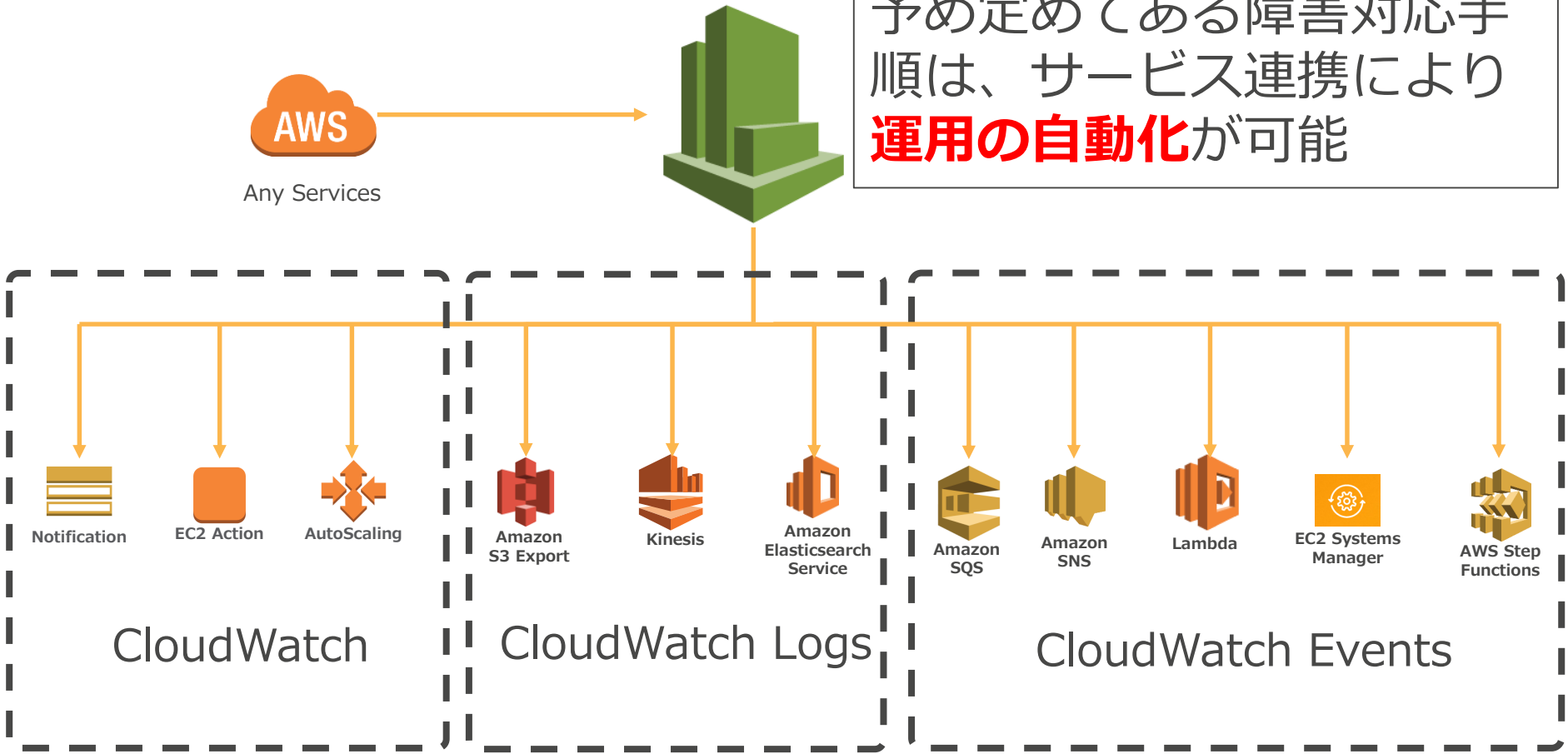
Why CloudWatch

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**

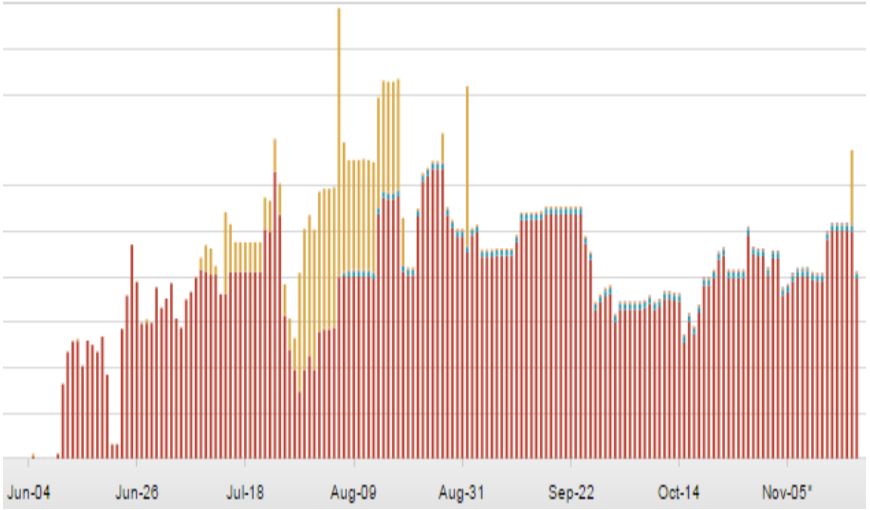
AWSサービスとの連携

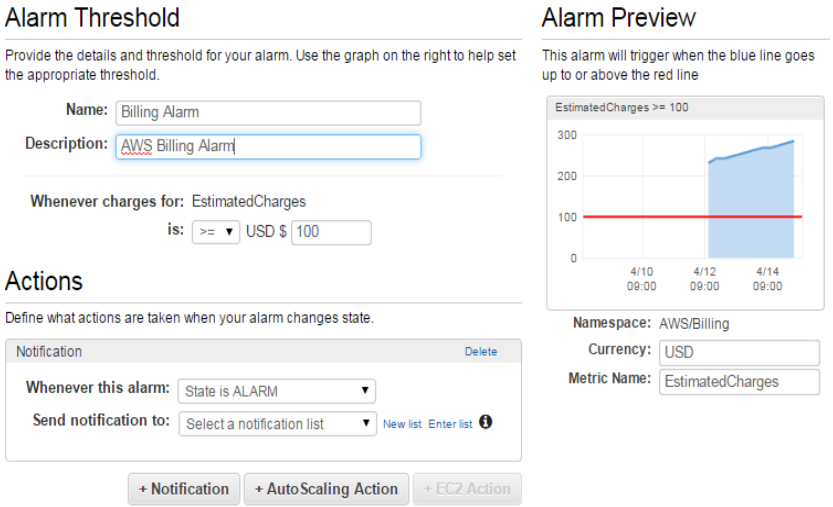


クラウドならではの監視も

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





（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

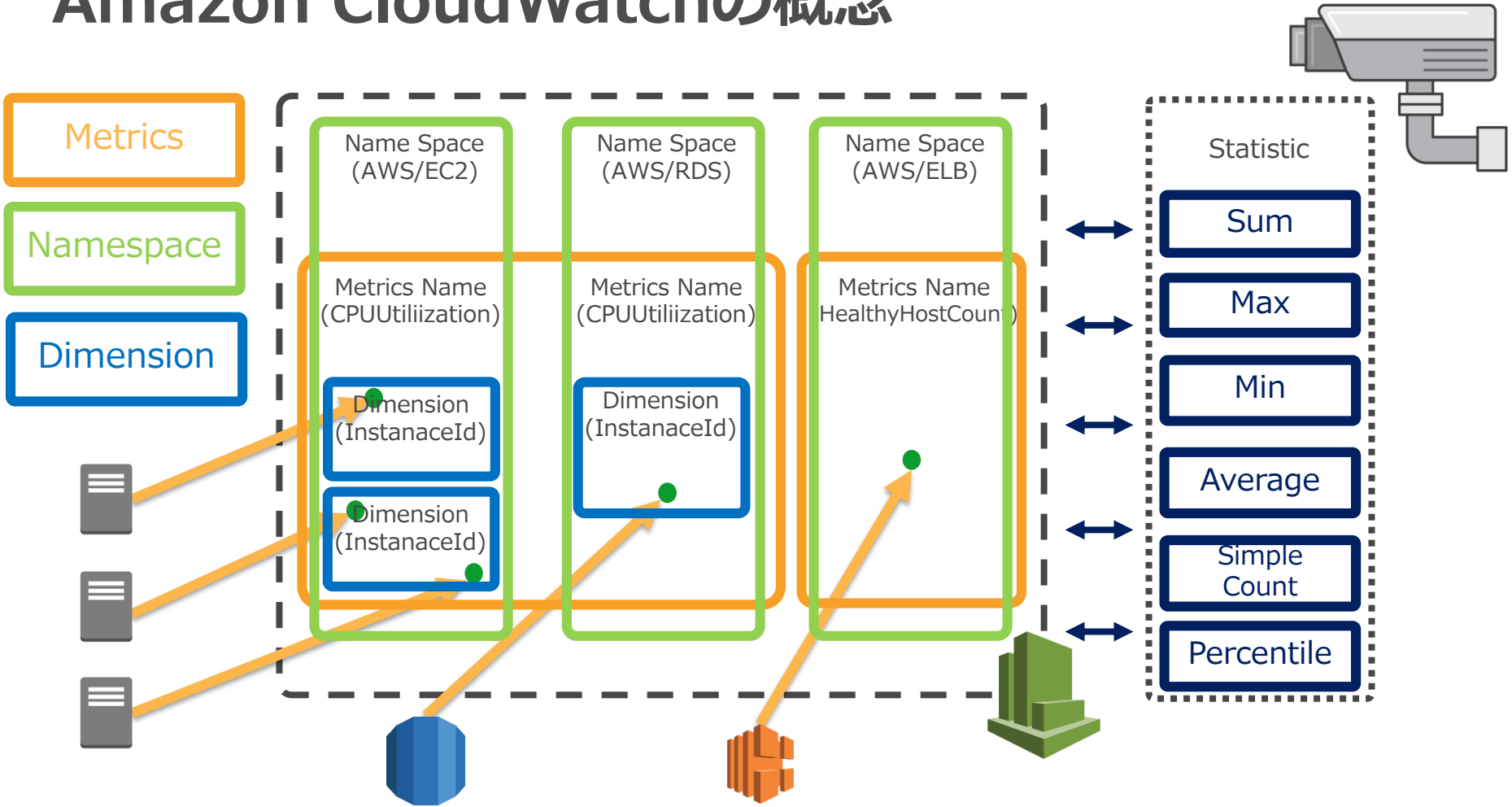
- ***CloudWatch***
  - **システム監視サービス**
    - ✓ 死活監視 / 性能監視 / キャパシティ監視
- ***CloudWatch Logs***
  - **ログ管理**プラットフォームサービス
    - ✓ EC2上のOS, APPのログ
    - ✓ AWSマネージド サービスのログ
- ***CloudWatch Events***
  - AWS上リソースの状態監視サービス
  - AWSリソースに対する**イベントをトリガーにアクションを実行**する機能

Amazon CloudWatch

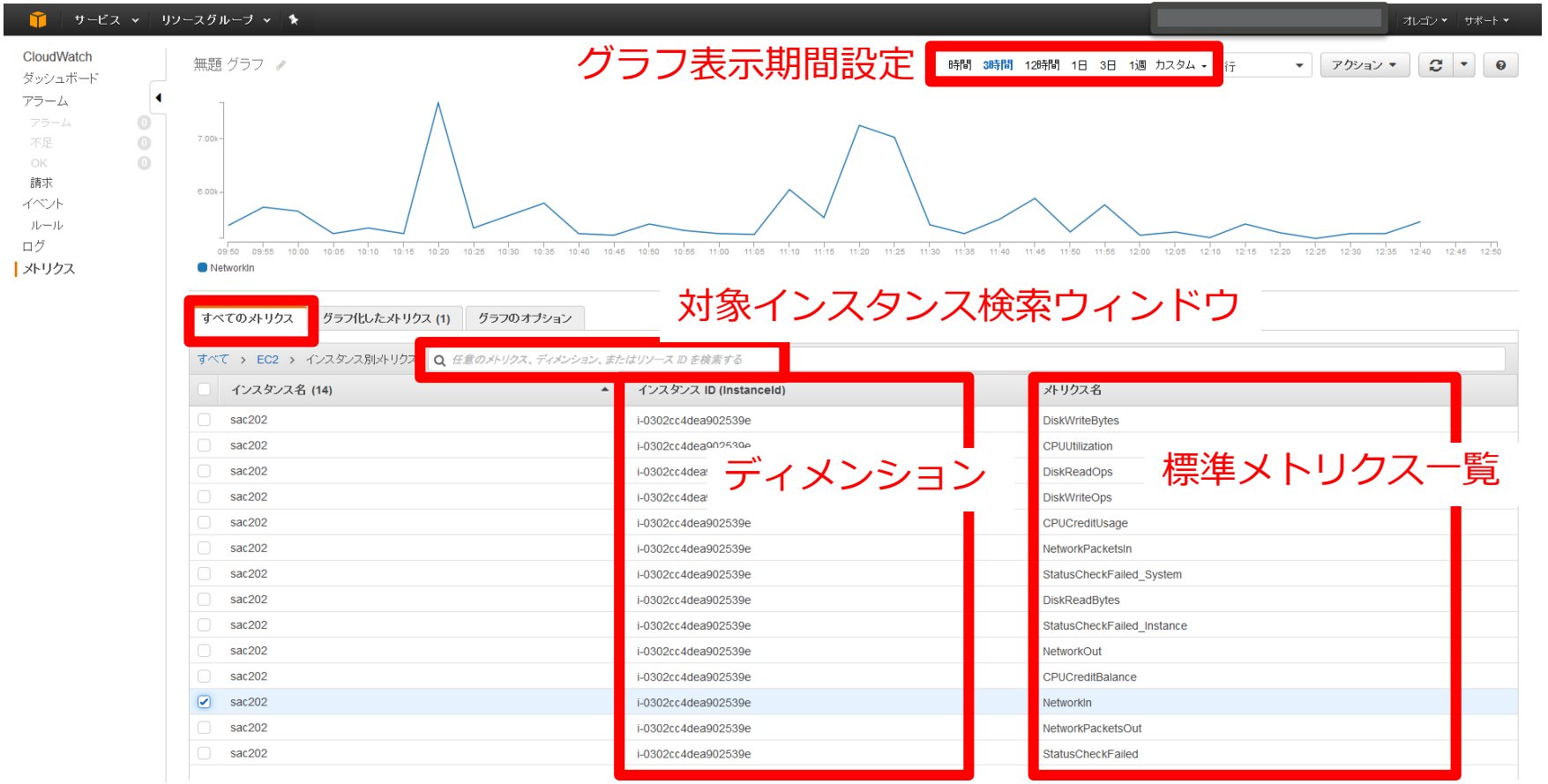
CloudWatch

- ***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

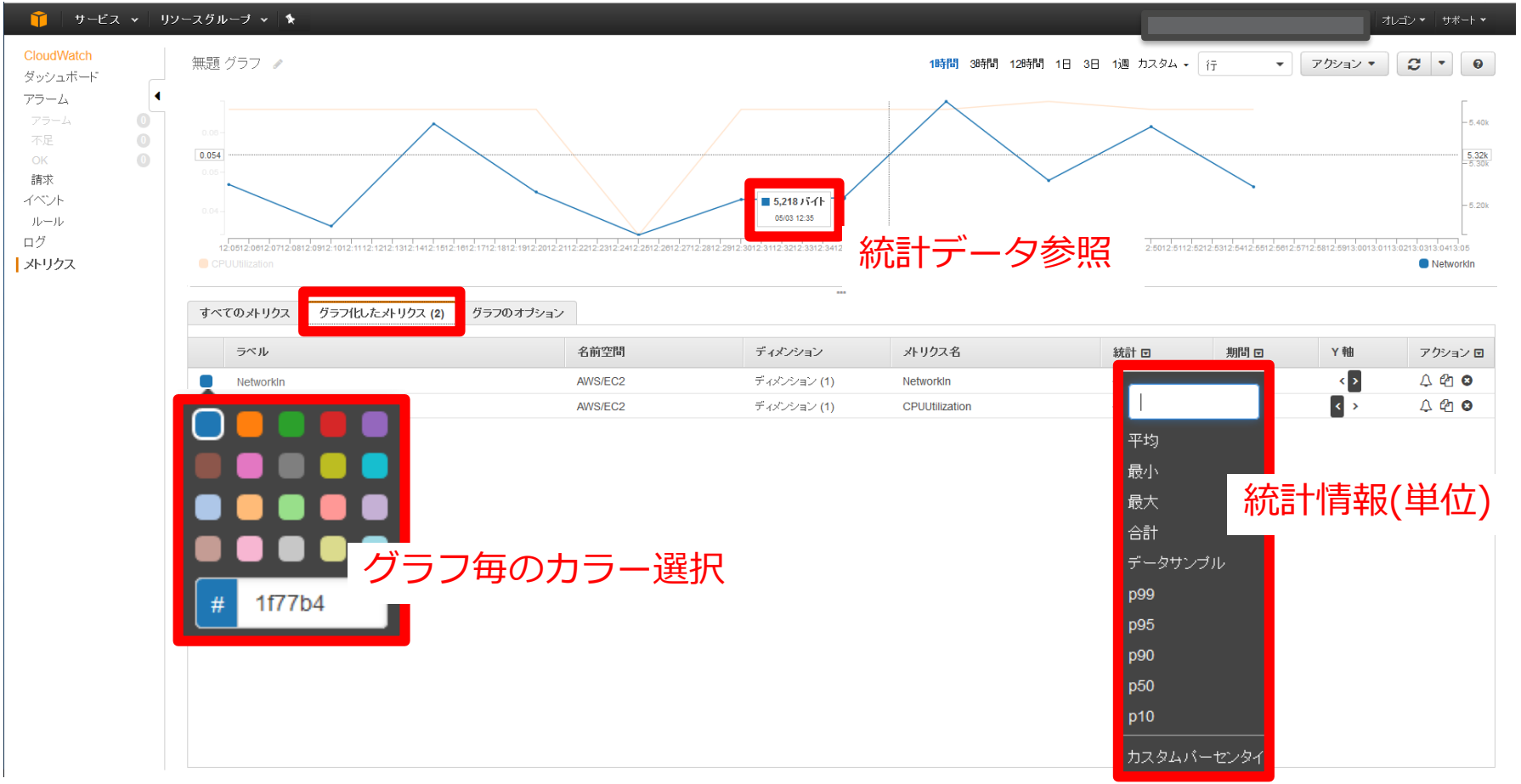
Amazon CloudWatchの概念



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

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

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
- 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**

Amazon CloudWatch Logs

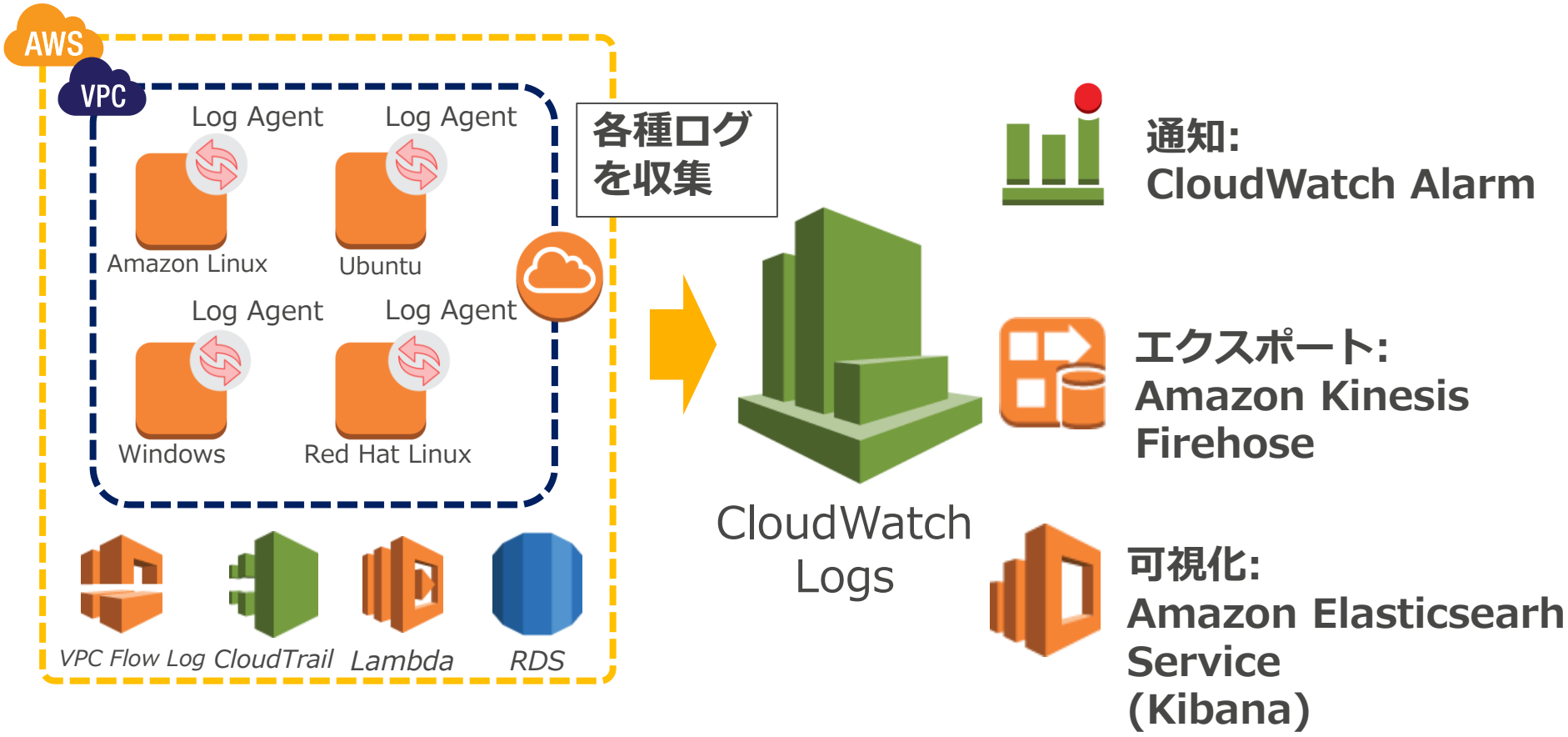
CloudWatch

- ***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



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

Log Stream

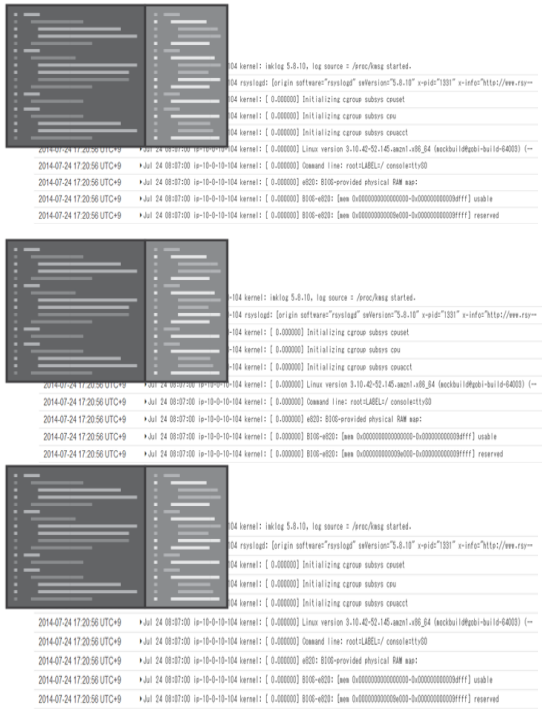
Log Event

Web Server

web001.ap-northeast-1

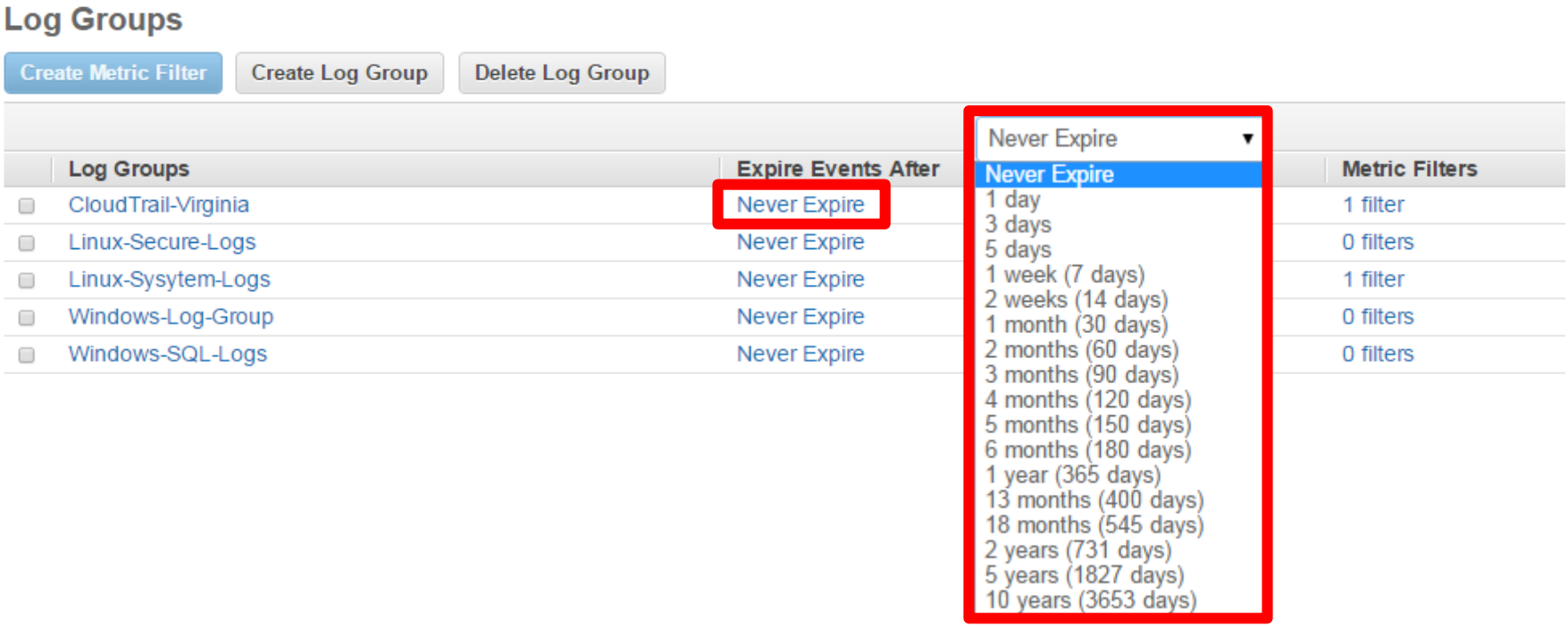
web002.ap-northeast-1

web003.ap-northeast-1



ログの保存期間

CloudWatch Logsはログの保存期間を設定可能



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 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

Metric Filterからアラーム作成、SNS連携が可能

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" }

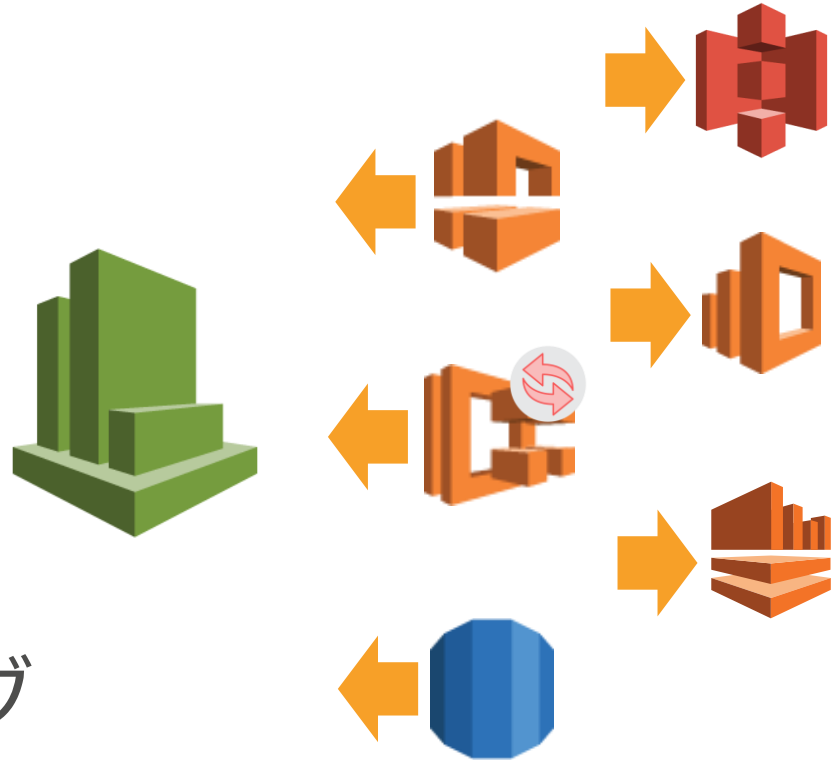
{ $.objectList[1].id = 2 }`

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

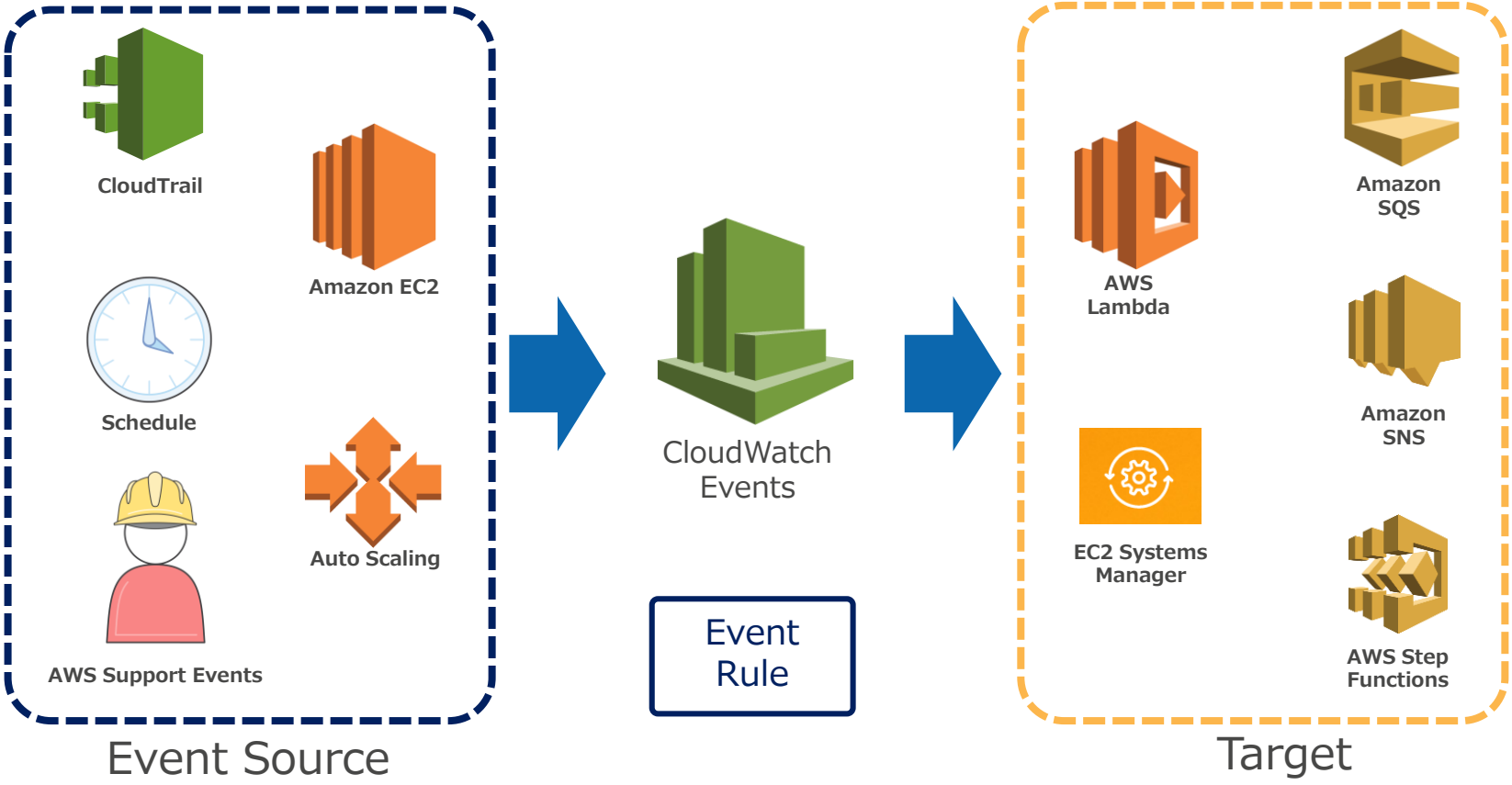


Amazon CloudWatch Events

CloudWatch

- ***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(Minites)/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

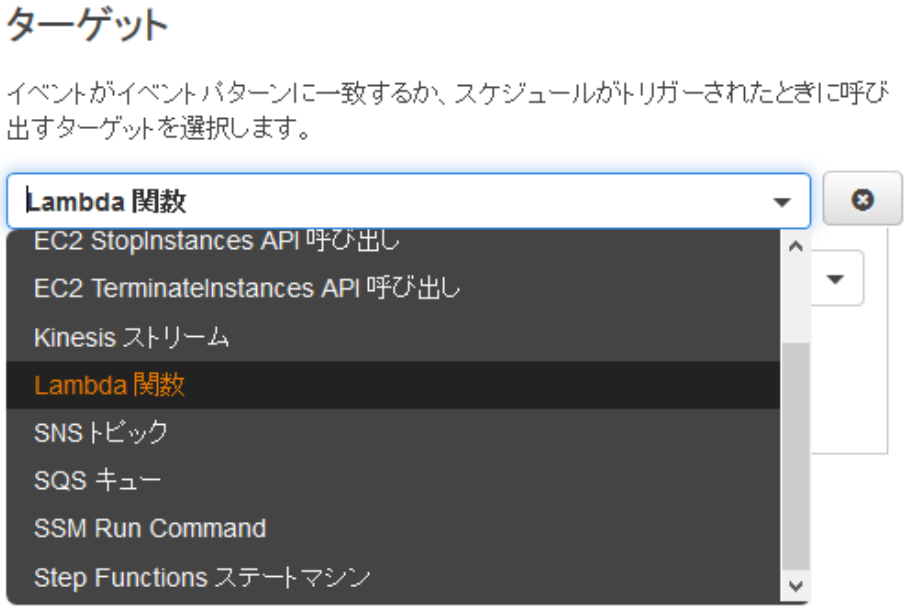
AWS SupportへのCase作成

Auto Scaling

- Launch Successful / Launch Unsuccessful
  Terminate Successful / Terminate Unsuccessful

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



（再々掲）Amazon CloudWatchのできる事

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

SUMMIT

Thank you!

amazon web services