Amazon CloudWatch / CloudWatch Logs

2015/07/01
AWS Black Belt Tech Webinar 2015
アマゾンデータサービスジャパン株式会社

プロフェッショナル サービス 山本 教仁
パートナー ソリューション アーキテクト 酒徳 知明

Agenda

- Amazon CloudWatch
- Amazon CloudWatch Logs
- AWSでの運用監視

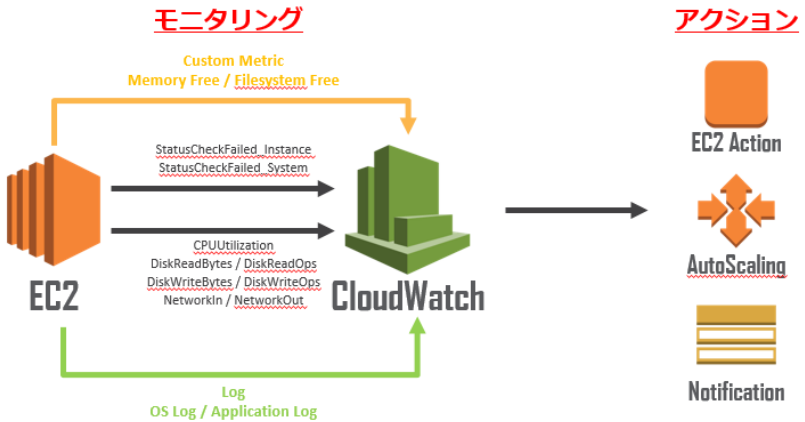
Amazon CloudWatch

CloudWatch

amazon web services

Amazon CloudWatchとは

- AWSの各種リソースを監視するサービス
  - AWSリソースの死活、性能、ログ監視 (監視)
  - 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



CloudWatchに対応するAWSサービス

AWS サービス	名前空間
Auto Scaling	AWS/AutoScaling
AWS Billing	AWS/Billing
Amazon CloudFront	AWS/CloudFront
Amazon CloudSearch	AWS/CloudSearch
Amazon DynamoDB	AWS/DynamoDB
Amazon ElastiCache	AWS/ElastiCache
Amazon Elastic Block Store	AWS/EBS
Amazon Elastic Compute Cloud	AWS/EC2
Elastic Load Balancing	AWS/ELB
Amazon Elastic MapReduce	AWS/ElasticMapReduce
Amazon Kinesis	AWS/Kinesis
Amazon Machine Learning	AWS/ML
AWS OpsWorks	AWS/OpsWorks
Amazon Redshift	AWS/Redshift

AWS の製品	名前空間
Amazon Relational Database Service	AWS/RDS
Amazon Route 53	AWS/Route53
Amazon Simple Notification Service	AWS/SNS
Amazon Simple Queue Service	AWS/SQS
Amazon Simple Workflow Service	AWS/SWF
AWS Storage Gateway	AWS/StorageGateway
Amazon WorkSpaces	AWS/WorkSpaces

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

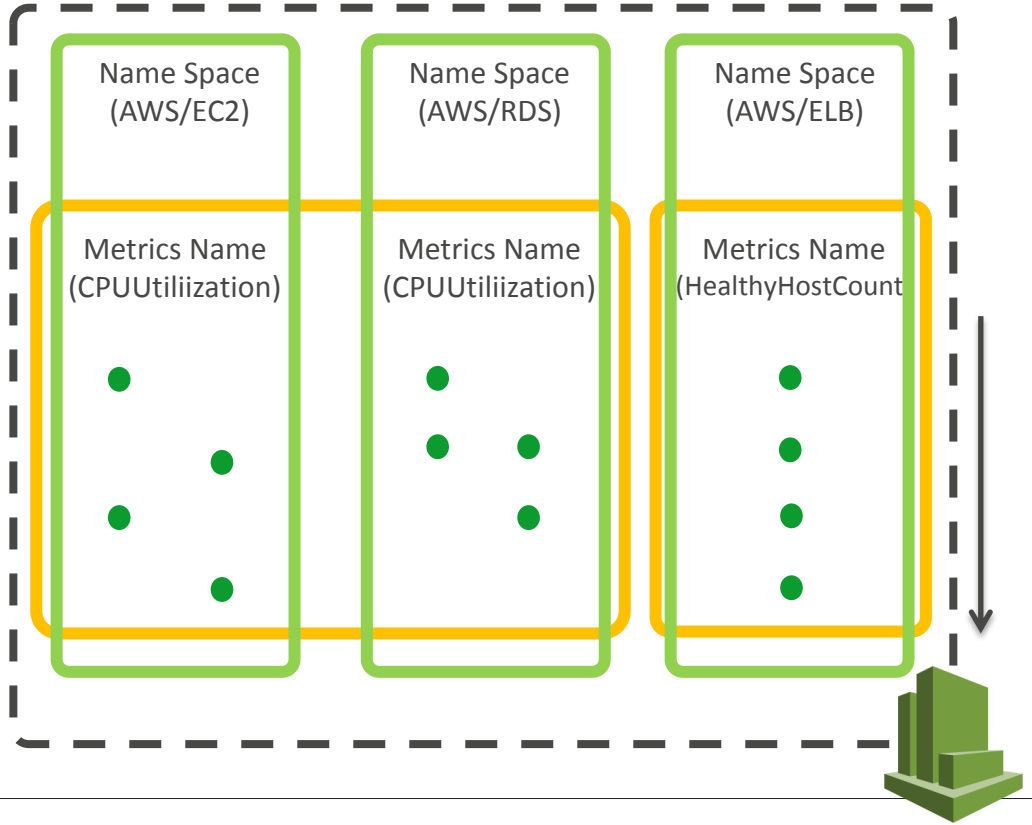
CloudWatchでの監視データ管理

Metrics

Namespace

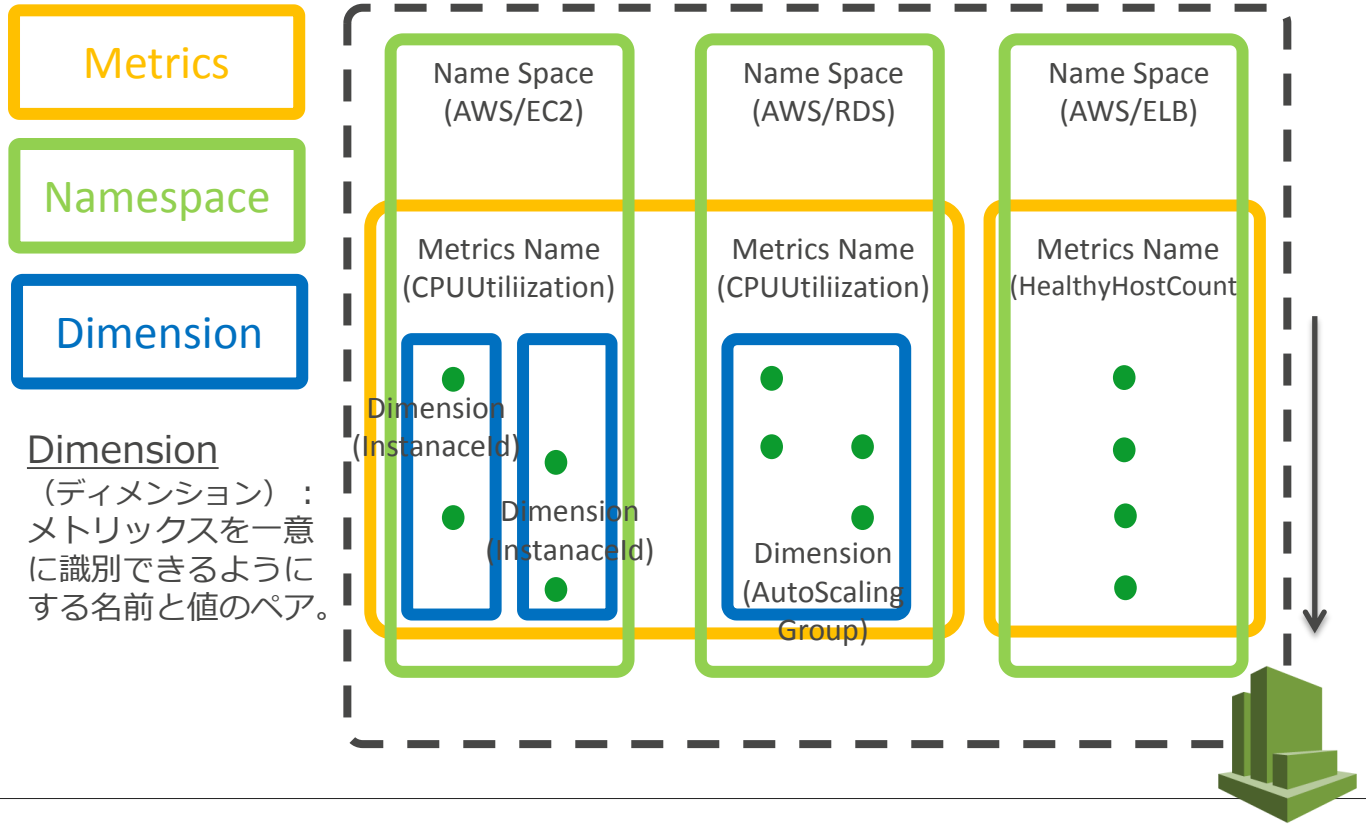
Metrics
（メトリックス）：
時系列で表わした
データポイント一式

Namespace
（名前空間）：
メトリックスの
コンテナ。標準では
AWSサービスごと。



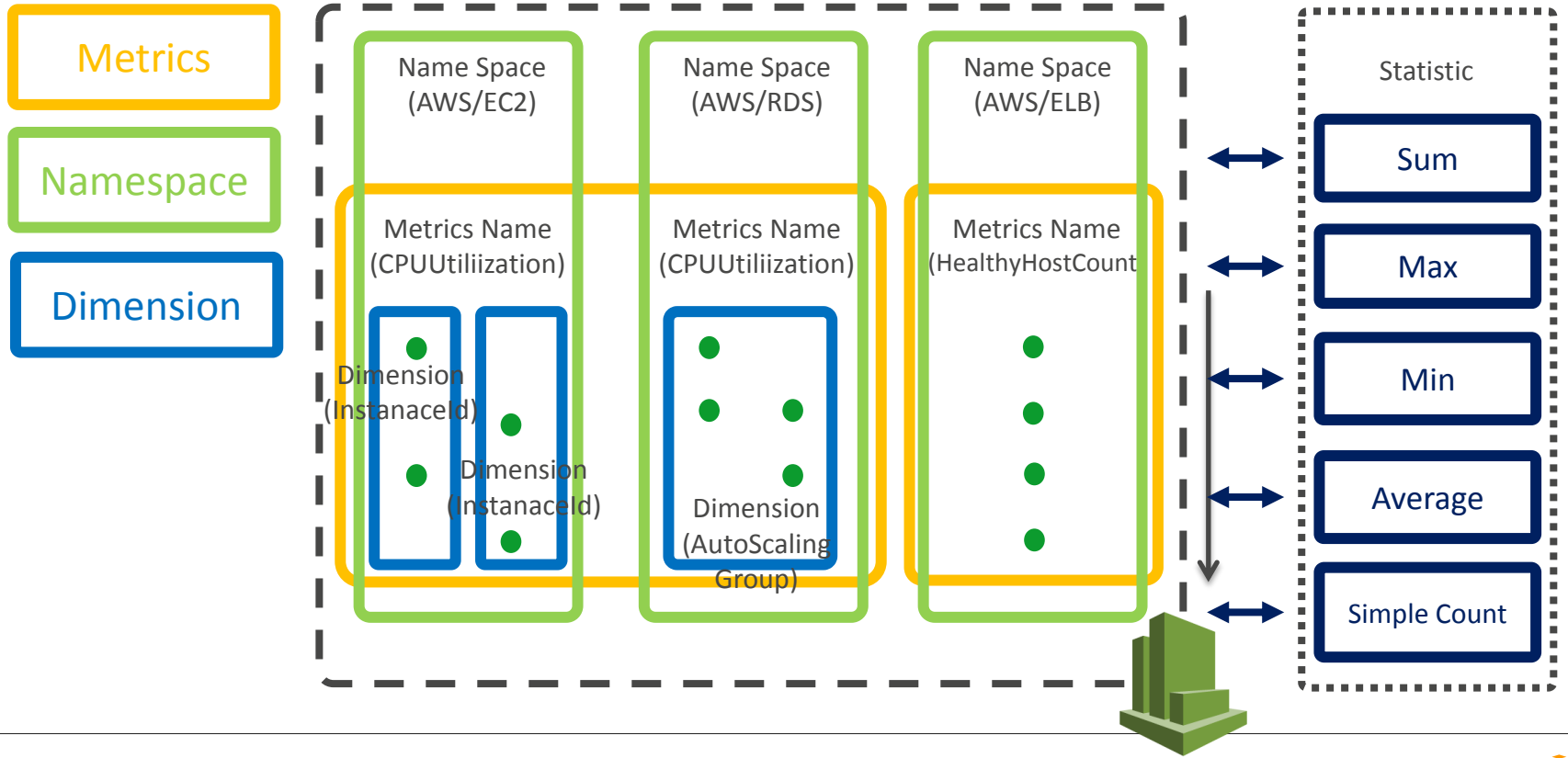
amazon web services

CloudWatchでの監視データ管理



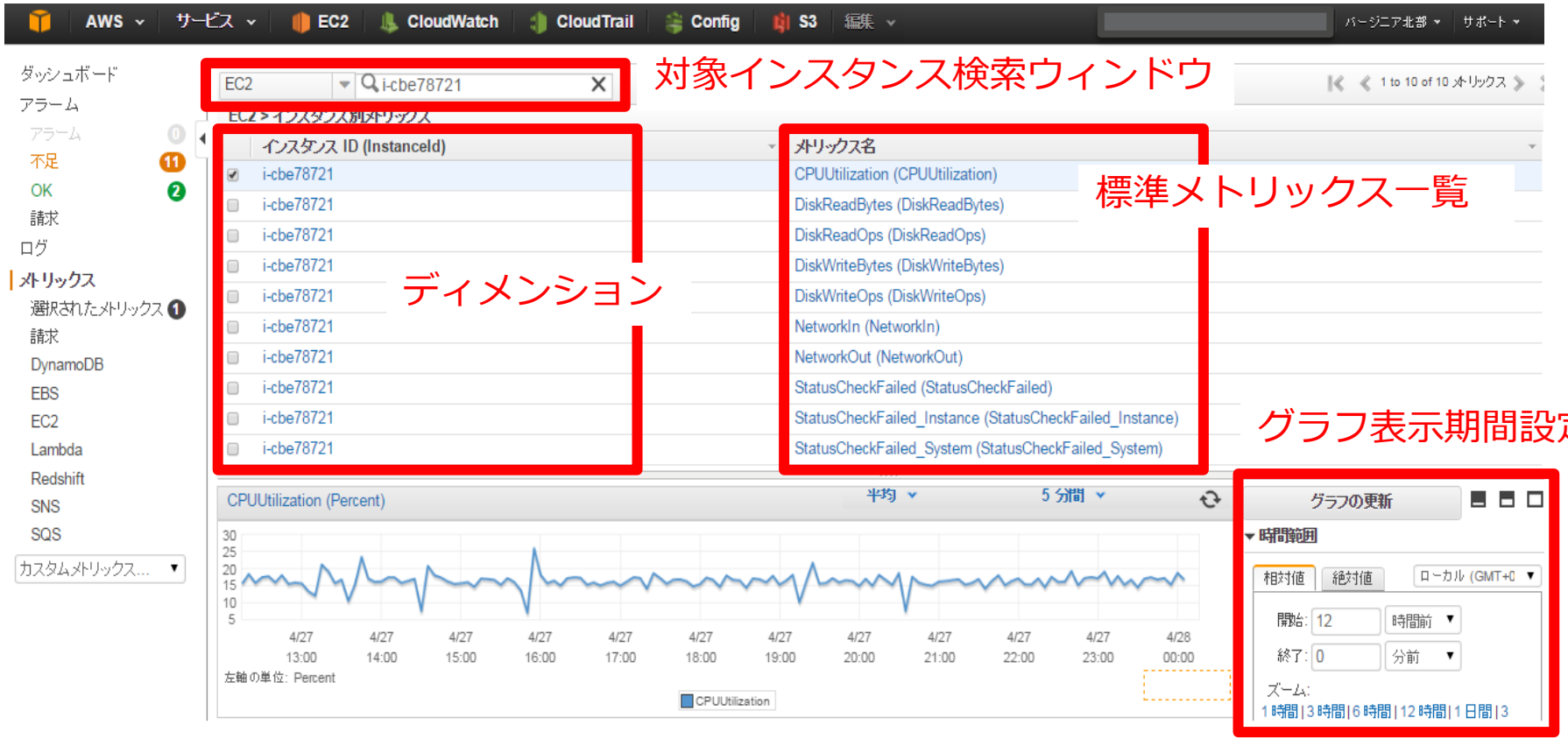
Dimension
（ディメンション）：メトリックスを一意に識別できるようにする名前と値のペア。

CloudWatchでの監視データ管理



amazon web services

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

標準メトリックス(EC2)

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
収集できないメトリックス

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\                                    ←単一値の登録

$ 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   ←統計セットの登録
```

- APIコールにスロットリングあり
  - カスタムメトリックスの頻繁な登録や頻度の高いデータ取得には注意

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

Amazon EC2のモニタリングタイプ

基本モニタリング

無料

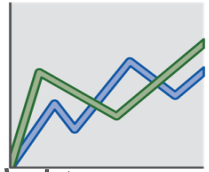
データは
5分間隔のものを
閲覧可能

詳細モニタリング

追加料金が必要

データは
1分間隔のものを
閲覧可能

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
  - サードパーティツールのエージェントをインストールできないため、CloudWatchでの監視が必須

ELB

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

Amazon RDS

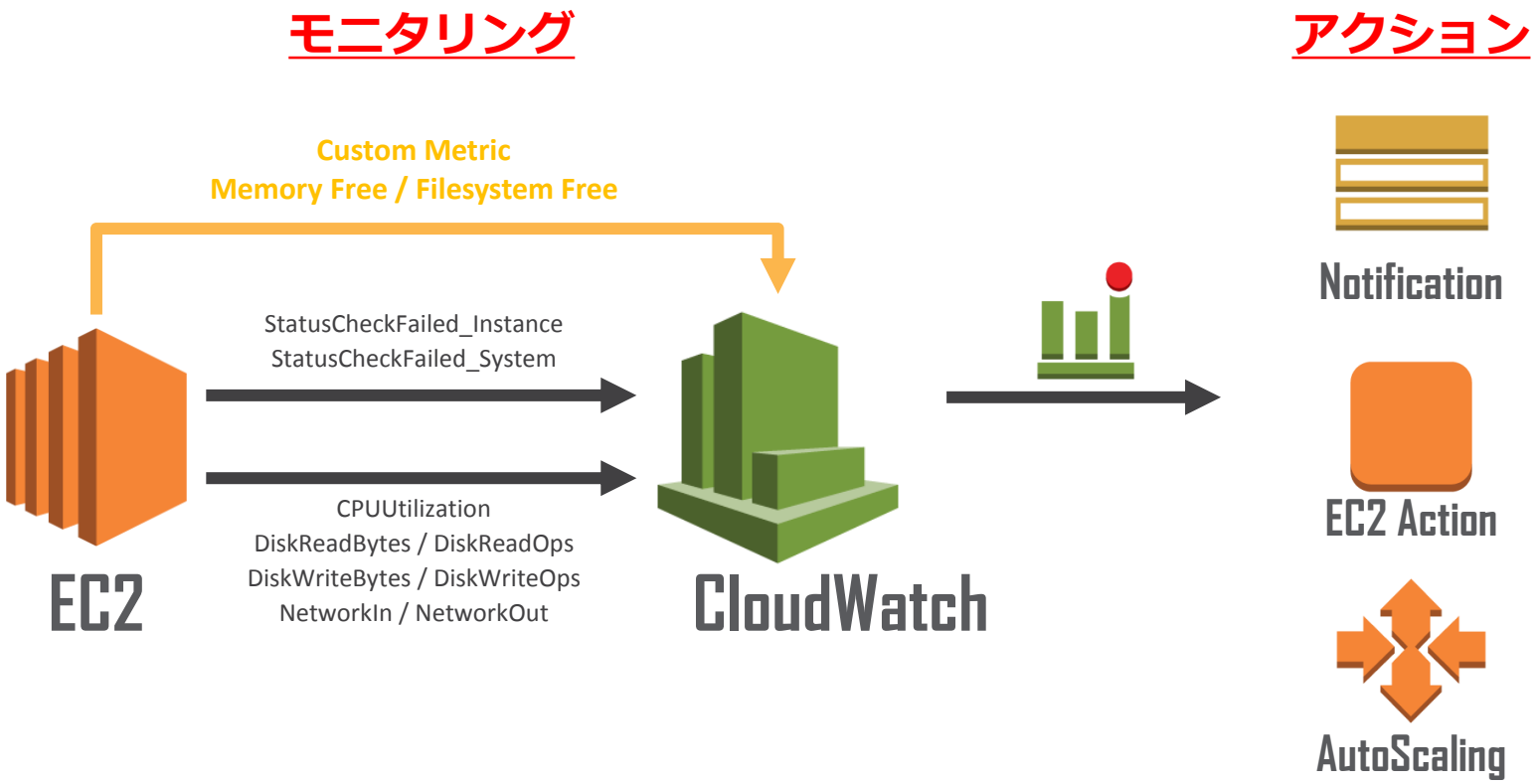
- CPUUtilization
- FreeableMemory
- SwapUsage
- FreeStorageSpace
- DiskQueueDepth
- ReadIOPS
- ReadThroughput
- ReadLatency
- NetworkReceiveThroughput
- NetworkTransmitThroughput
- WriteIOPS
- WriteThroughput
- WriteLatency
- DatabaseConnections
- BinLogDiskUsage

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

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）

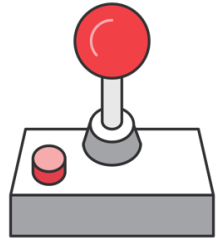
CloudWatchのアクション機能



CloudWatchのアクション機能

- 各アラーム状態に対してアクションを定義可能
  - 通知（Notification）
    - Amazon Simple Notification Service（SNS）を使って通知
    - メール送信やHTTP(S)送信、Amazon Simple Queue Service（SQS）への送信が可能
  - EC2アクション
    - EC2インスタンスの復元、停止および終了が実行可能
  - Auto Scalingアクション
    - Auto Scaling GroupのScaling Policyを指定し、インスタンスのスケールアウト／インが可能

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

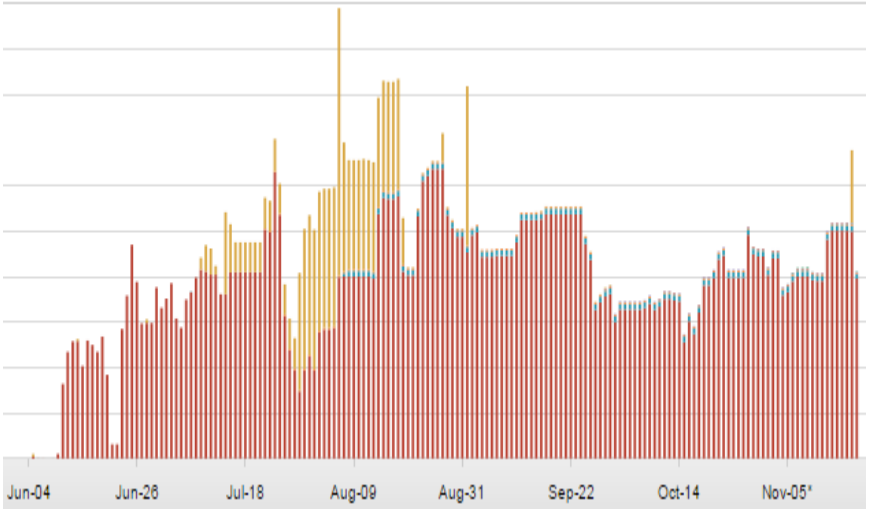
http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2-instance-recover.html

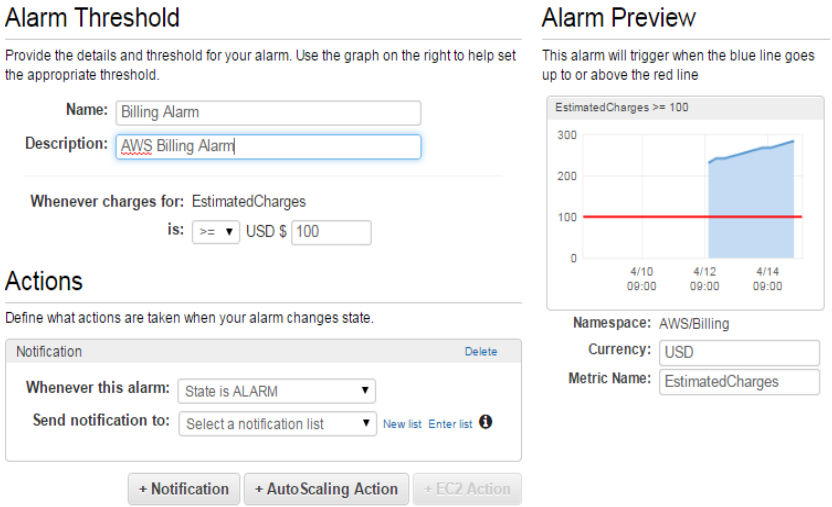
CloudWatchアラームの設定

CloudWatchアラームの設定

CloudWatchによるコストの監視

- Billingアラーム設定　※Virginiaリージョンから設定
  - 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





CloudWatchの料金

- 初期費用無しの従量課金
- 標準の監視は無料
  - EC2インスタンスの標準監視（5分間隔）
  - EBS、ELB、RDSは1分間隔が無料
- アラームやカスタムメトリックスは一定数まで無料
  - 10メトリックス、10 アラーム、および100万APIリクエスト
  - 1 か月あたり5GBのデータの取り込みおよび5GBのアーカイブされたストレージ
- 課金対象及び料金（2015年7月現在 Tokyoリージョン）
  - EC2詳細モニタリング1インスタンスにつき$3.50/月
  - カスタムメトリックス1つにつき$0.50/月
  - アラーム1つにつき$0.10/月
  - APIリクエスト1000回につき$0.01（Get, List, Putごとに）

http://aws.amazon.com/jp/cloudwatch/pricing/

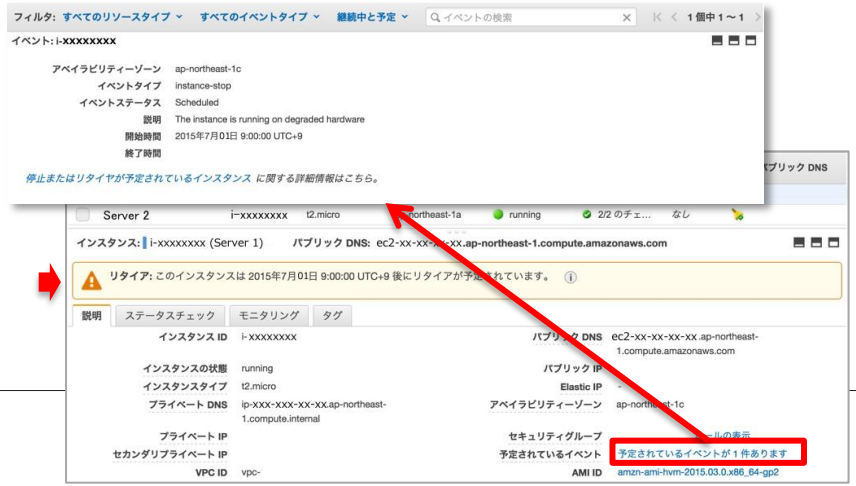
メンテナンスイベントの監視

- EC2やRDSのメンテナンスイベント（※）
  - AWSが予定する、再起動、停止/開始、またはリタイアなどのイベント
    - 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が予定されている場合メールで通知されますが、見逃さないようにコマンドラインでの確認をしておくことが有効
  - 管理コンソールからも確認可能

■コマンドラインによるイベントの確認例

```
$ aws ec2 describe-instance-status ¥
          --query "InstanceStatuses[?Events != null].[InstanceId,Events]"
[
   [
      "i-xxxxxxxx",
      [
         {
            "Code": "instance-stop",
            "Description": "The instance is running on degraded
hardware",
            "NotBefore": "2015-07-01T00:00:00.000Z"
         }
      ]
   ]
]
```

■管理コンソールでの確認

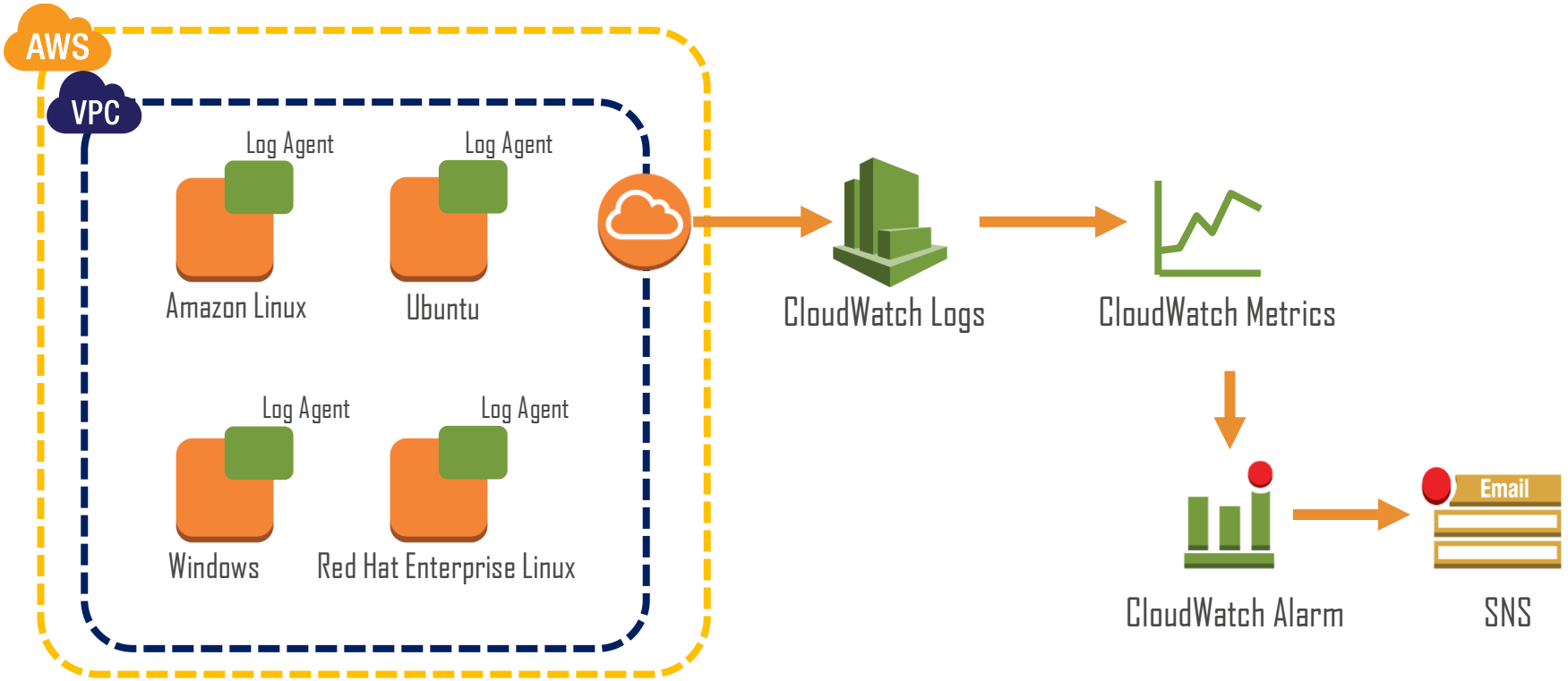


Amazon CloudWatch Logs

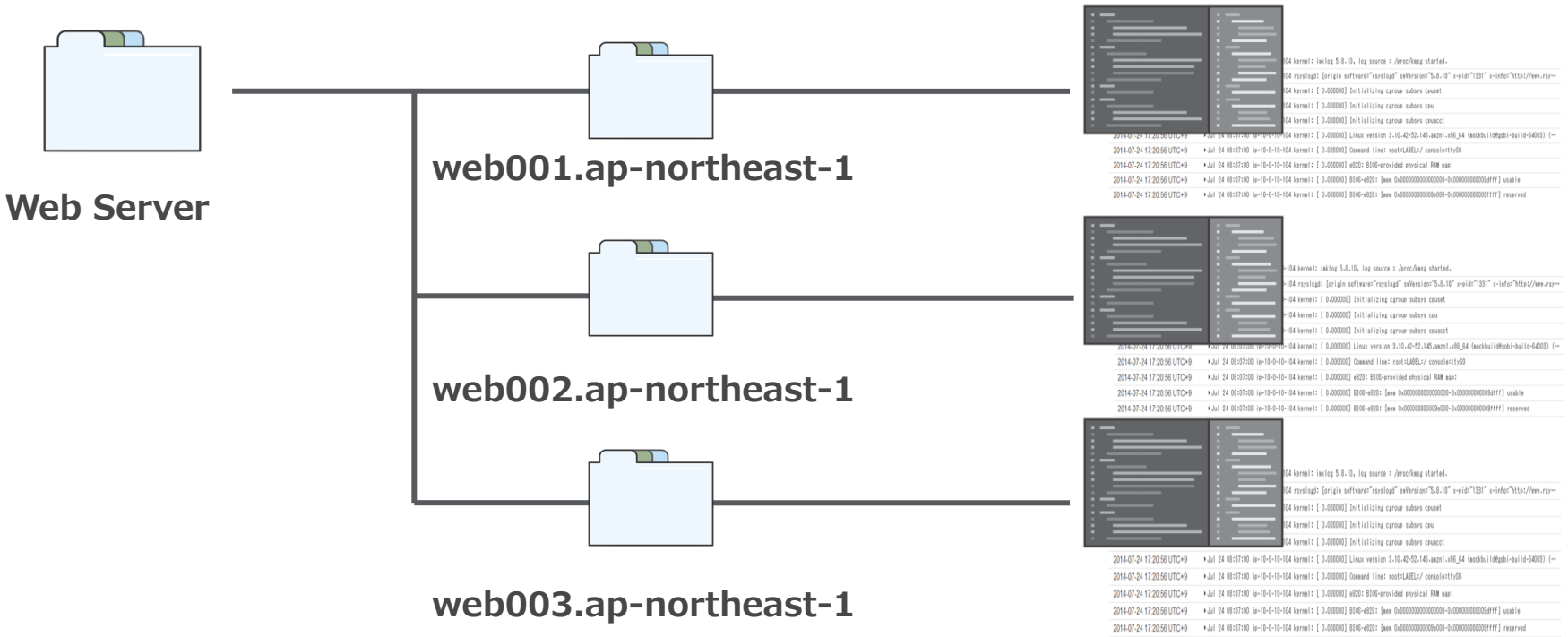
CloudWatchを使ったログ監視

- CloudWatch Logsを使ったログ監視
- OS、アプリケーション等のテキストログをモニタリング
- エージェント経由でログメッセージをCloudWatchエンドポイントに転送
- ログデータの保存期間は設定可能
  - 1日～永久保存で選択可能

CloudWatch Logsの利用イメージ

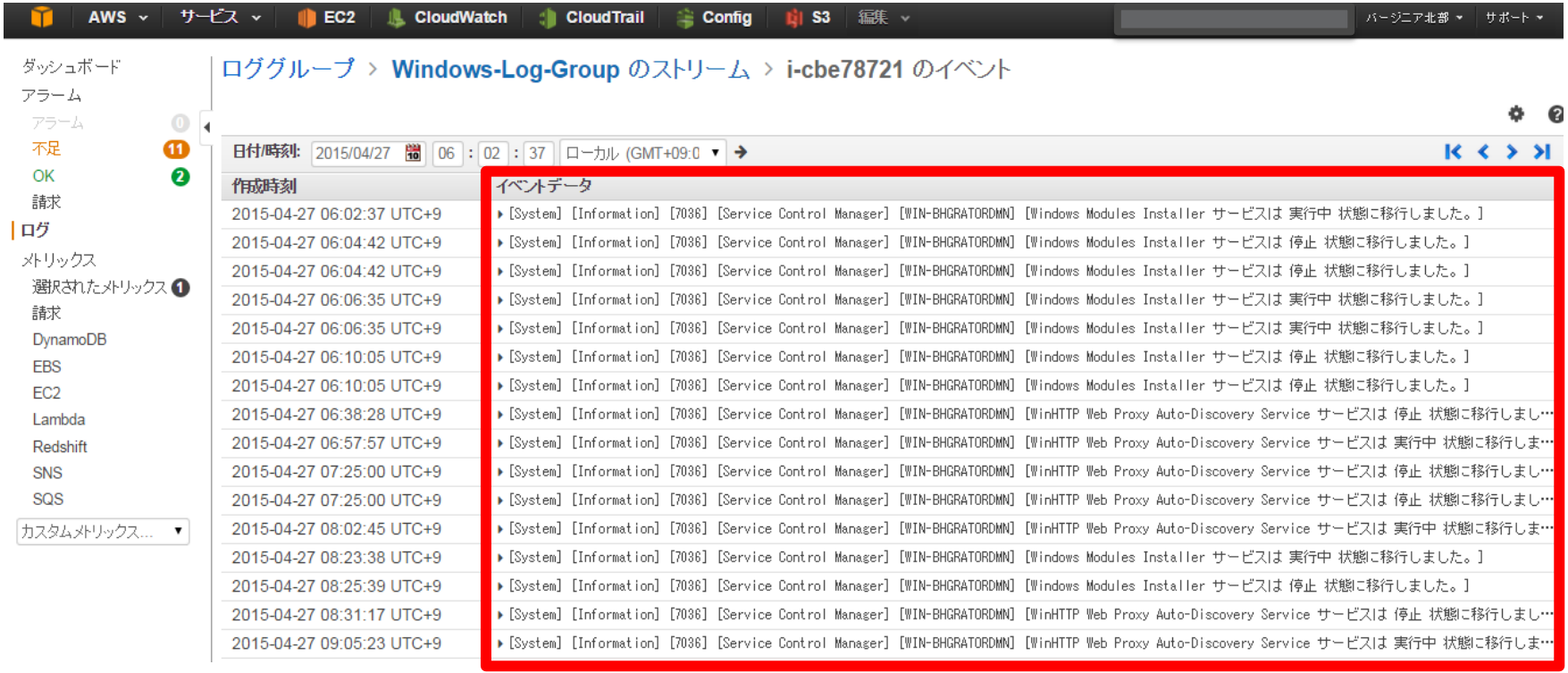


CloudWatch Logsのディレクトリ階層



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

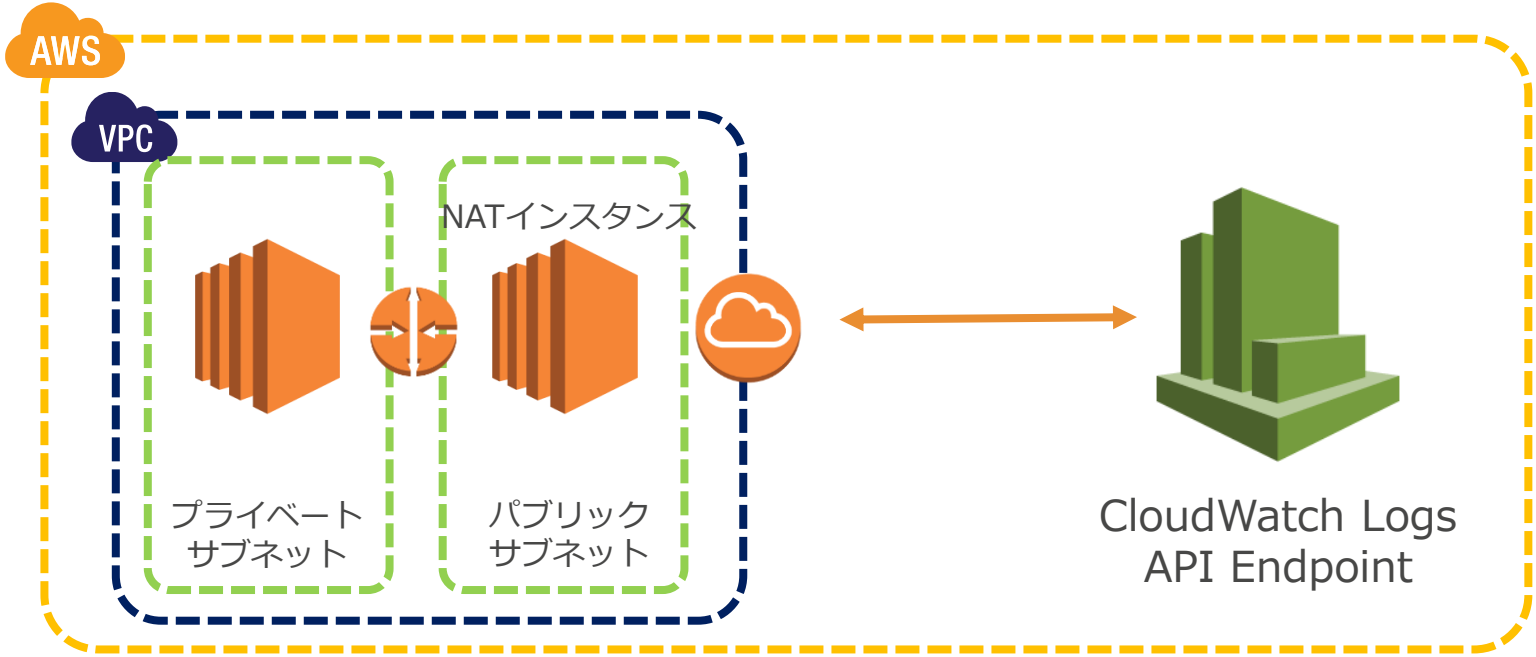


CloudWatch Logsのクライアント

- Linuxの場合: テキストログ
  - CloudWatch Logs Agent
- Windowsの場合: テキストログ,Windowsイベントログ、パフォーマンスカウンタ
  - EC2Config
- その他
  - AWS CLI
  - AWS SDK
  - サードパーティツール (fluentd など)

Log Agentの通信要件

- CloudWatch Logsエンドポイントに接続できること



Linux:CloudWatch Logs Agent

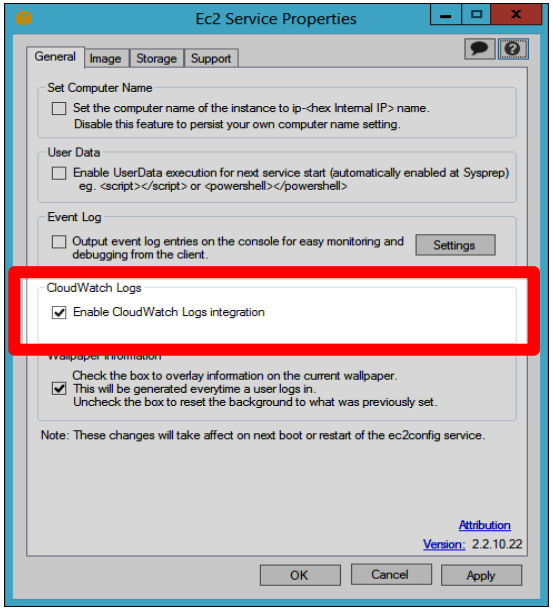
- CloudWatch Logs Agent
  - ログデータをCloudWatch Logsにプッシュするaws cliプラグイン
  - CloudWatch Logsにデータを送信するaws logs pushコマンドを実行するスクリプト（デーモン）
  - デーモンが常に実行中であることを確認するcronジョブ
  - インストールと構成が必要
  - 導入対象EC2インスタンスにはRoleをつける
- 対応プラットフォーム
  - Amazon Linux
  - Ubuntu Server
  - CentOS
  - Red Hat Enterprise Linux

CloudWatch Logs Agentの注意点

- 転送できるログメッセージの長さの制限
  - Agentが１回あたりプッシュできるログレコードサイズは最大32KB
  - 32KBを超えると、ログがトランケートされる
- 対応しているログローテーション
  - rename and re-create
    - 元のログにsuffix(数値)をつけてrenameし、空のログファイルを再作成
    - 例) /var/log/syslog.log が /var/log/syslog.log.1 に 変更される場合
  - copy and truncate
    - 元のログファイルをコピーしてからTRUNCATE
    - 例) /var/log/syslog.log が /var/log/syslog.log.1 に copy され、/var/log/syslog.log が TRUNCATE される場合
  - create common-patterned file
    - 共通のパターンを持つ新しいファイルを作成
    - 例) /var/log/syslog.log.2014-01-01 を残し、 /var/log/syslog.log.2014-01-02 が作成される 場合
    - ※access_log_80, access_log_443のような異なるファイルに交互に書き込まれるようなファイル監視は未対応

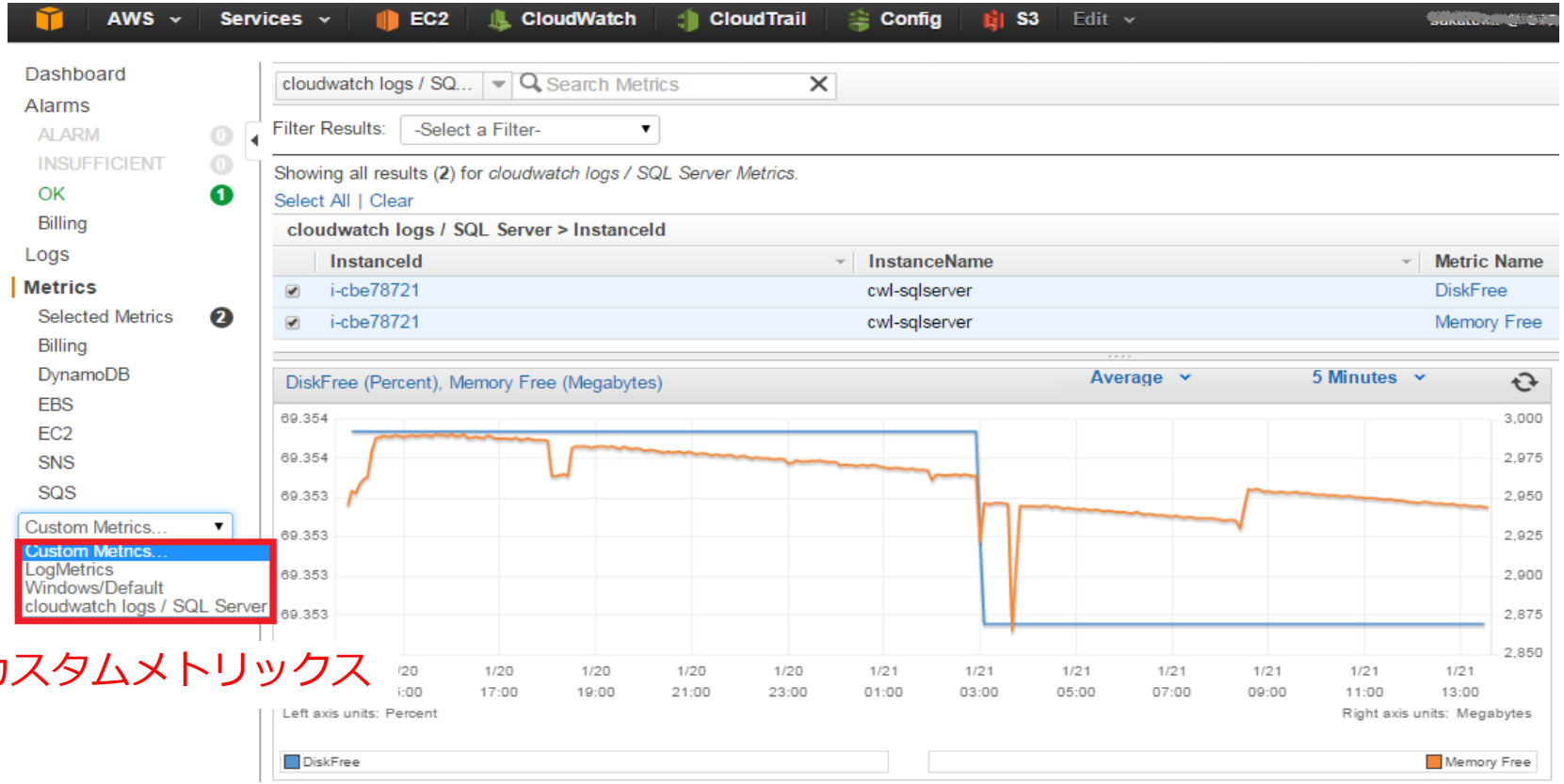
Windows:CloudWatch Logs設定

- ec2configでCloudWatch Logs設定
  - JSON設定ファイルを編集することで、監視するメトリックスを設定
    - “C:¥Program Files¥Amazon¥Ec2ConfigService¥Settings” に配置されている “AWS.EC2.Windows.CloudWatch.json“ ファイルを編集
- 収集するログを設定
  - Windowsイベントログ
  - Event Tracing for Windows
  - テキストベース ログ
  - IISログ
  - パフォーマンスカウンタ



チェックを入れるだけで利用可能

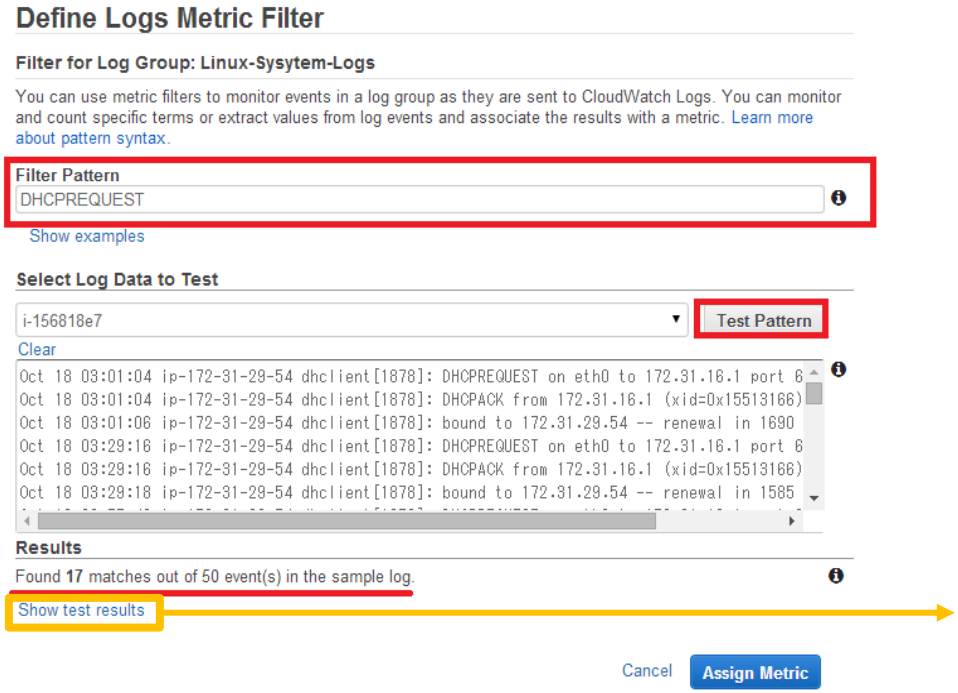
カスタムメトリックスの確認

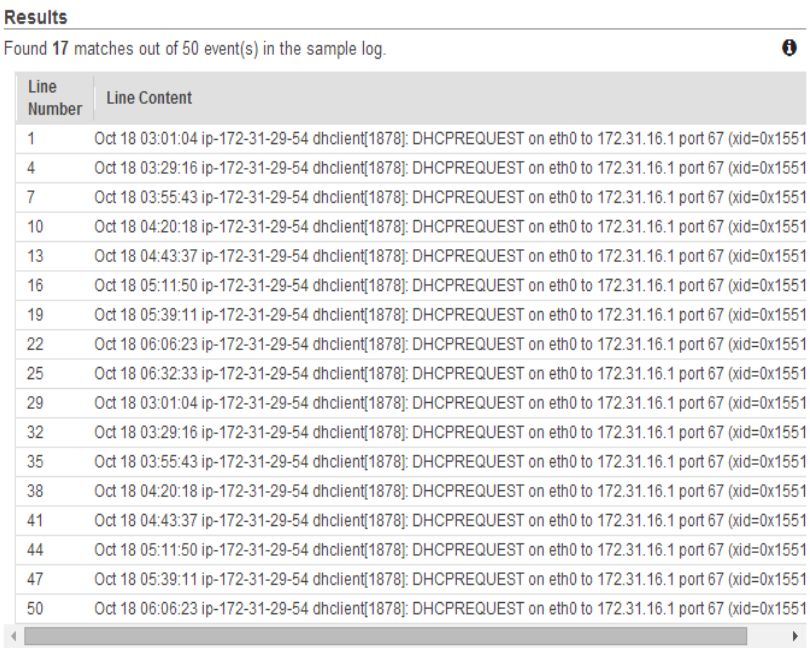


カスタムメトリックス

CloudWatch Logs Metric Filter（1/3）

- 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





amazon web services

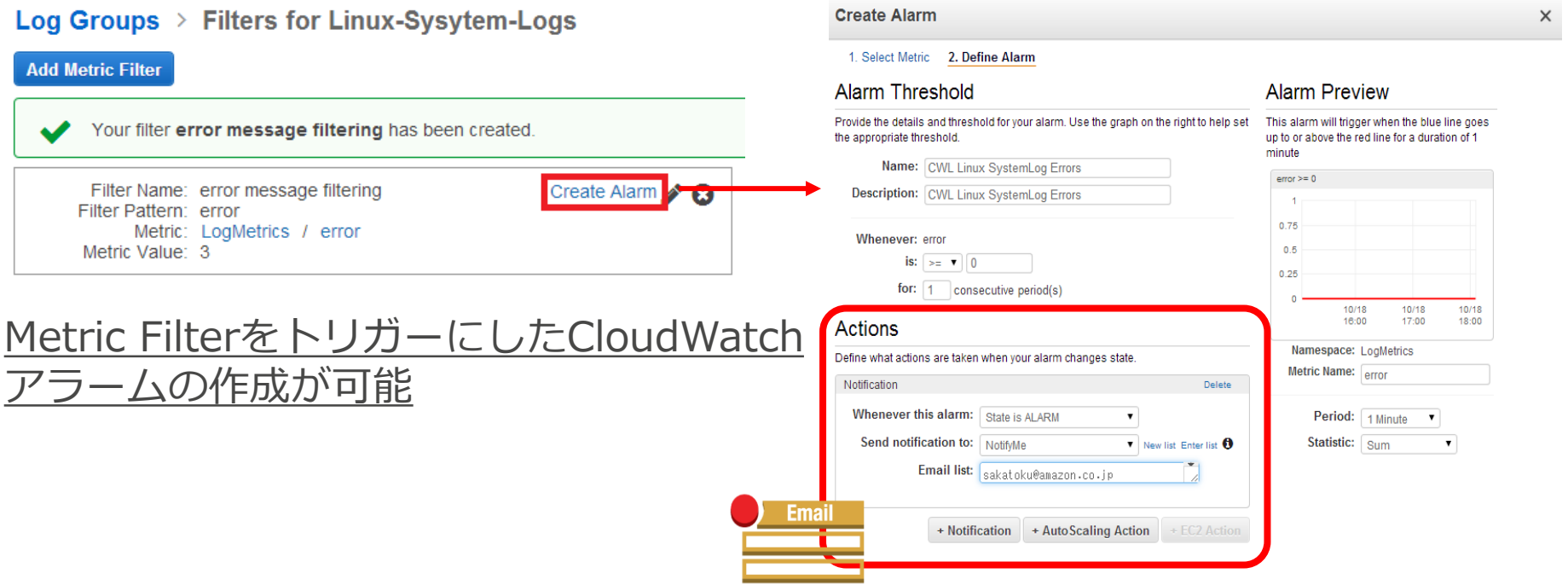
CloudWatch Logs Metric Filter（2/3）

- 特定文字列のエントリ頻度によりアラーム作成が可能

→ **コンソールへのログインが失敗するとアラーム警告**

CloudWatch Logs Metric Filter（3/3）

- Metric Filterからアラーム作成、SNS連携が可能



Metric FilterをトリガーにしたCloudWatchアラームの作成が可能

メトリックスフィルタ (一般的なログフォーマット)

```
127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] "GET /apache_pb.gif HTTP/1.0" 200 1534
127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] "GET /apache_pb.gif HTTP/1.0" 500 5324
127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] "GET /apache_pb.gif HTTP/1.0" 200 4355
```

- Filter example

  [ip, user, username, timestamp, request, status_code, bytes > 1000]

  [ip, user, username, timestamp, request, status_code = 200, bytes]

  [ip, user, username, timestamp, request, status_code = 4*, bytes]

  [ip, user, username, timestamp, request = *html*, status_code = 4*, bytes]

- Notes
  - 角括弧 [] または 2 個の二重引用符（""）で囲まれた文字は単一のフィールドとして扱われます
  - メトリックスフィルタは大文字と小文字を区別します

CloudWatch Logs料金体系

	無料枠 (1カ月あたり)	従量課金
インジェクション	5GB	$0.76 / GB
アーカイブ	5GB	$0.033 GB / 月

10メトリックス、10アラーム、および100万の API リクエストの無料利用枠を準備

http://aws.amazon.com/jp/cloudwatch/pricing/

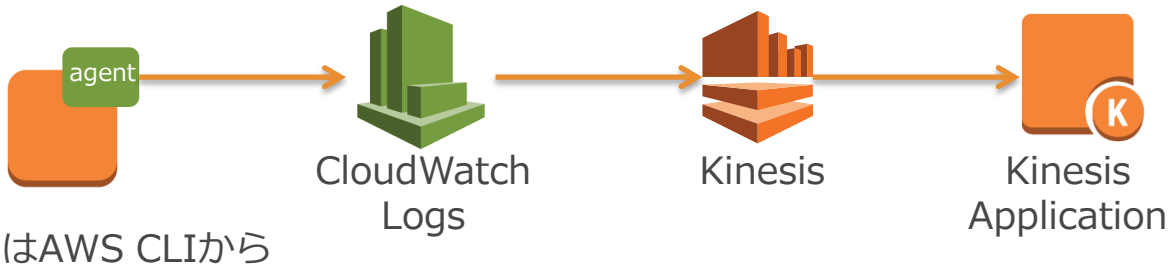
CloudWatch Logs検索機能の向上

- 複数のロググストリームにまたがってログを閲覧したり、
  キーワード検索が可能（1つのロググループ内）

ログストリームを複数選択し、
イベントを検索ボタンをクリック

CloudWatch Logs Subscription

- CloudWatch Logsに集めたログをリアルタイムにKinesisに転送可能に
  - Kinesis Applicationでログに対して／を受けてロジックを記述可能
  - CloudWatch Logsには指定した保管期間ログが保管される

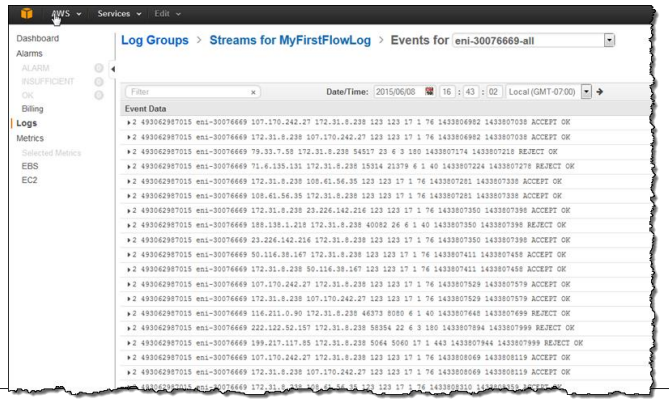


設定はAWS CLIから

```
aws logs put-subscription-filter ¥
    --log-group-name ”xxxxxxxx" ¥
    --filter-name ”xxxxxxxx" ¥
    --filter-pattern "{xxxxxxxx = xxxxxxxx}" ¥
    --destination-arn "arn:aws:kinesis:ap-northeast-1:123456789012:stream/xxxxxxxx" ¥
    --role-arn "arn:aws:iam::123456789012:role/xxxxxxxx"
```

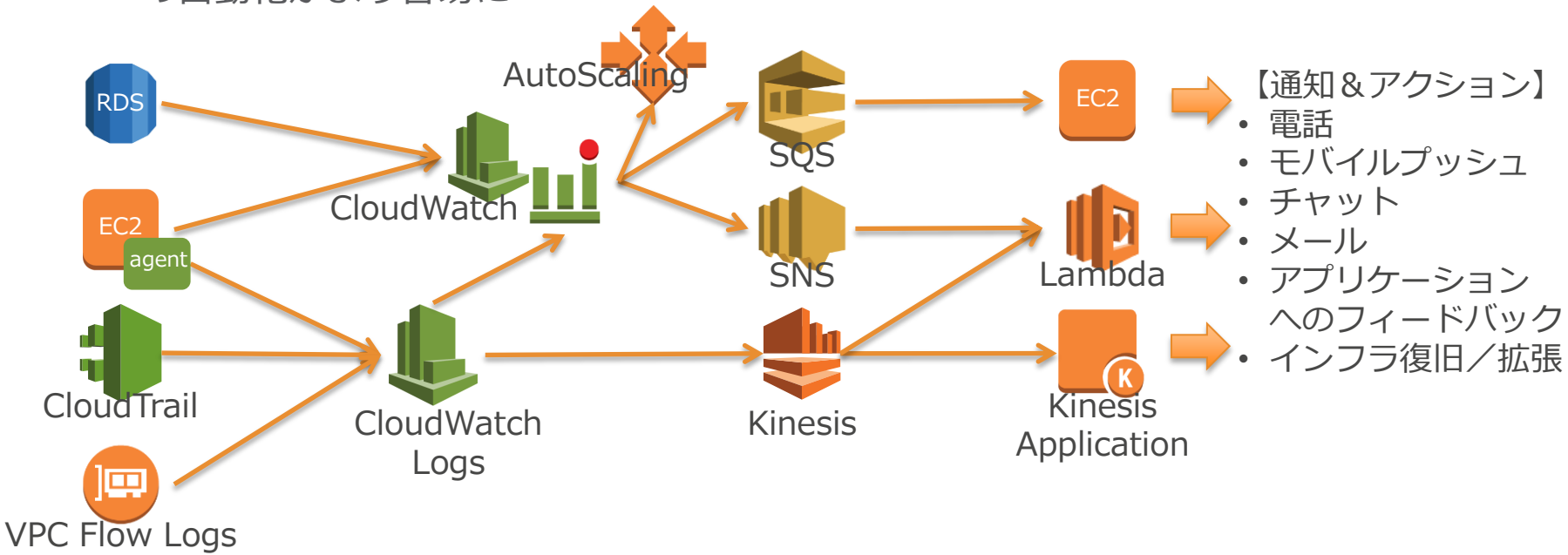
VPC Flow Logs

- VPC内ネットワーク・ログ
  - VPC内のネットワークのログが取得可能
  - Network ACLとSecurity Groupでの許可と禁止のトラフィックログ
  - VPC Flow Logsの設定は、VPC、Subnet、ENIに対して実施
  - ログは、ネットワークインタフェース（ENI）ごとに取得（ENIがログストリーム）
  - 特定の通信はログされない
    - Amazon Provided DNSへのDNS Lookup、Windowsライセンスアクティベーション、DHCP等



CloudWatchを介したシステム運用の自動化

- システム運用の自動化
  - CloudWatchおよびCloudWatch Logsの各種連携機能が登場し、システム運用の自動化がより容易に



CloudWatchを使った自動化例

- IAMの設定変更に関するアラートの受け取り方について
  - http://aws.typepad.com/aws_japan/2015/02/how-to-receive-alerts-when-your-iam-configuration-changes.html
- AWSアカウントのルートアクセスキーを使用した場合の通知方法
  - http://aws.typepad.com/aws_japan/2015/06/how-to-receive-notifications-when-your-aws-accounts-root-access-keys-are-used.html
- CloudWatch Logs Subscriptionsを利用したZabbixへのログ転送
- アラート発生時に AWS Lambda を使って音声電話をかける
- CloudWatchのAlertをAWS Lambda経由でSlackに飛ばす
- Auto Scalingによる自動復旧（AWS Lambda+SNS編）
- Amazon ECSのDockerコンテナをLambdaでAuto Scalingに連携させる
- VPC Flow LogsをElasticsearch + Kibana4で可視化する

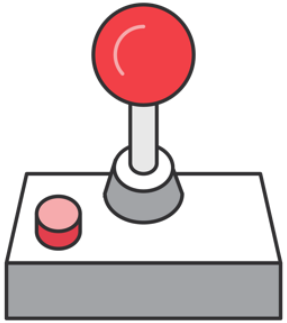
AWSでの運用監視

AWSの運用監視

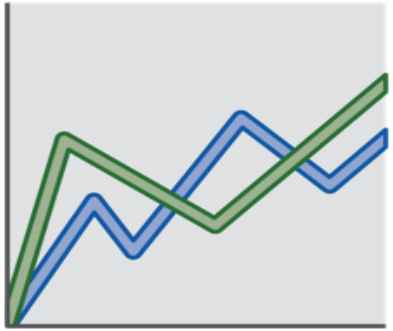
- 今までのシステム監視と変わらない
  - オンプレミス時の運用ノウハウを最大限活用
  - AWSサービスをうまく活用したシンプルな監視
  - 多くの監視ツールがAWSに対応
- クラウドならではの監視
  - スケール監視
  - コスト監視
  - コンプライアンス

基本となる運用監視

性能監視



死活監視

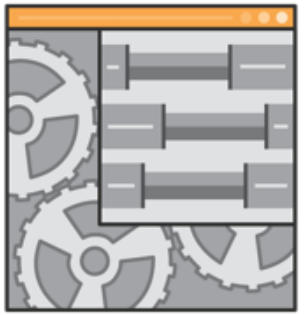


キャパシティ監視

オンプレミスでもクラウドでも基本的には同じ

監視ツール連携の必要性

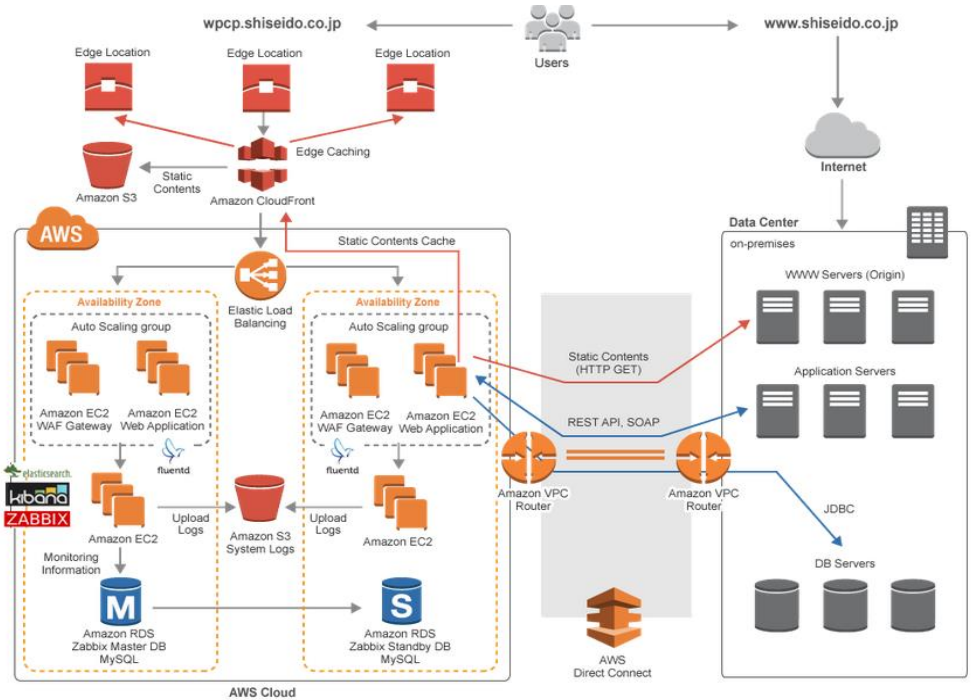
- サードパーティ監視ツールの必要性
  - ハイブリッド環境での統合監視
  - CloudWatch機能制限への対応
    - プロセス監視
    - ログ監視での柔軟な文字列マッチング
    - メンテナンスウィンドウの設定
    - 重要度の設定
    - 長期保管
- 環境と監視項目ごとのツール利用例



	AWS		オンプレミス
	EC2	ELB/RDS	サーバ
性能監視 （CPU使用率、DiskI/O他）	CloudWatch標準メトリックス or サードパーティツール	CloudWatch標準メトリックス	サードパーティツール
死活監視（ホスト）	CloudWatch標準メトリックス or サードパーティツール	CloudWatch標準メトリックス	サードパーティツール
死活監視（プロセス）	サードパーティツール	CloudWatch標準メトリックス	サードパーティツール
キャパシティ監視 （メモリ使用、ディスク使用量）	CloudWatchカスタムメトリックス or WindowsであればCloudWatch Logs or サードパーティツール	CloudWatch標準メトリックス	サードパーティツール

監視システムとのAmazon CloudWatch連携

監視システム利用イメージ

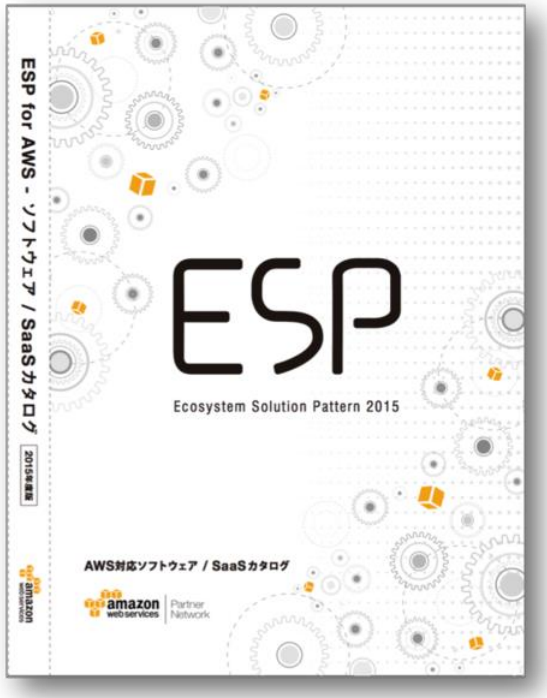


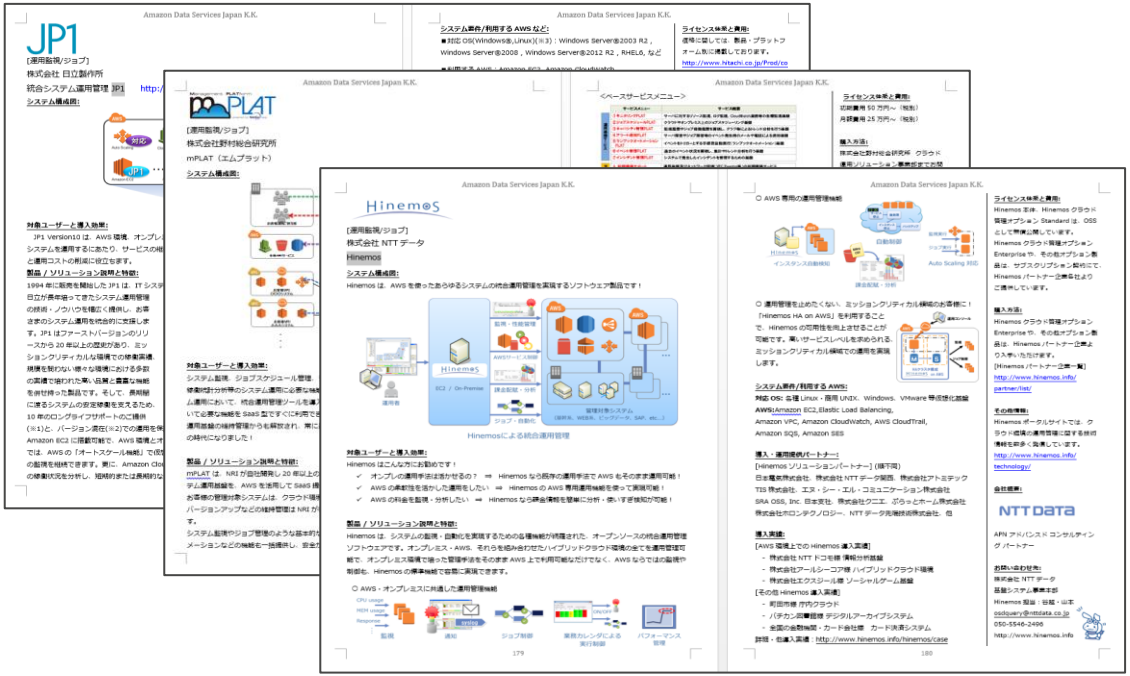
http://aws.amazon.com/jp/solutions/case-studies/shiseido/

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

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





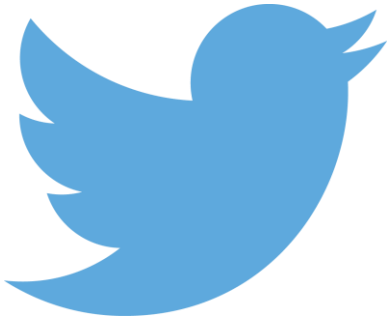
http://aws.typepad.com/aws_japan/2015/06/esp-catalog-pdf.html

amazon web services

AWS運用コミュニティ

～クラウドによる、クラウドのための、クラウド運用管理～

AWS上に構築されたシステムの
運用管理のベストプラクティスを集約！



@opsjaws

http://aws.typepad.com/aws_partner_sa/2015/06/aws-ops.html

amazon web services

Q&A

次回Webinarのお申し込み

http://aws.amazon.com/jp/event_schedule/

Webinar資料の配置場所

- AWS クラウドサービス活用資料集
  - http://aws.amazon.com/jp/aws-jp-introduction/

プロダクト別：				
Amazon S3		AWSマイスターシリーズ Re:Generate Amazon Simple Storage Service (S3)	Slideshare	PDF
Amazon Glacier		AWSマイスターシリーズ Reloaded Amazon Glacier Amazon Glacierのご紹介 機能編	Slideshare（Reloaded） Slideshare（機能編）	PDF（Reloaded） PDF（機能編）
Amazon Route 53		AWSマイスターシリーズ Re:Generate	Slideshare	PDF

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！

ご参加ありがとうございました。