

# ログからひも解く AWSのす・べ・て！！

アマゾン データ サービス ジャパン  
酒徳 知明・関山 宜孝

# 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  
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
- 運用監視サービス担当
  - AWS CloudTrail, AWS Config, Amazon CloudWatch



# 自己紹介

関山 宜孝(せきやま のりたか)

技術支援本部

クラウドサポート エンジニア

- AWSサポートをご利用いただいているお客様の技術支援を担当
- 好きなAWSサービス
  - CloudWatch, **CloudTrail**, EMR, Data Pipeline

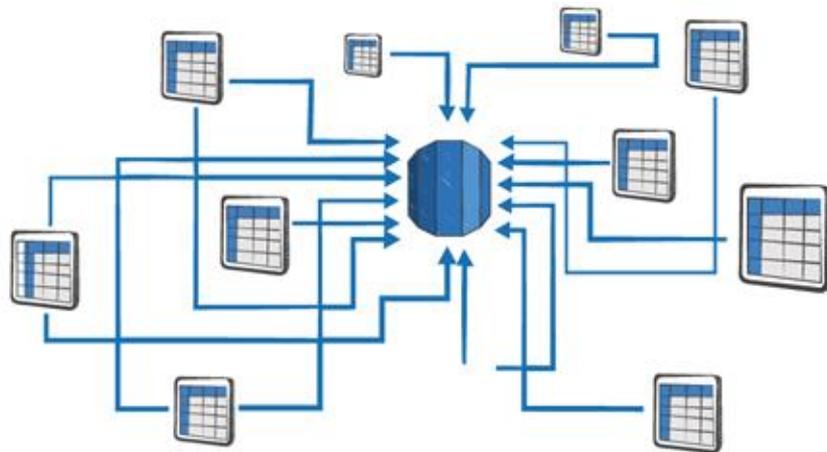


# クラウドならではの運用管理

## API管理

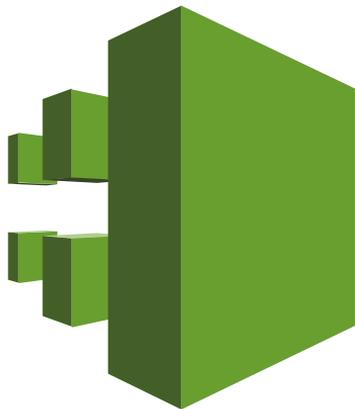


## リソース管理



# クラウドならでの運用管理

API管理

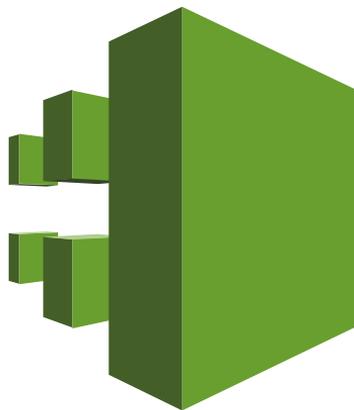


**AWS CloudTrail**

リソース管理



**AWS Config**



**AWS CloudTrail**

# 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

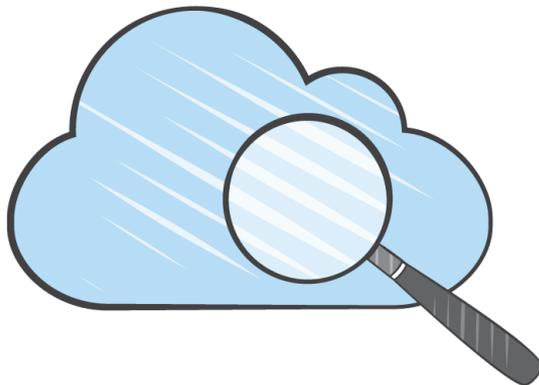


# 蓄積したJSONファイルをどう扱うか???

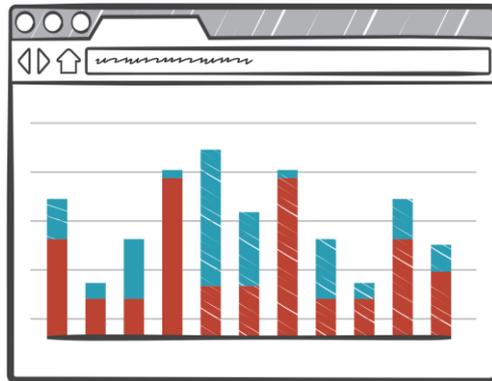
アラート



文字列検索



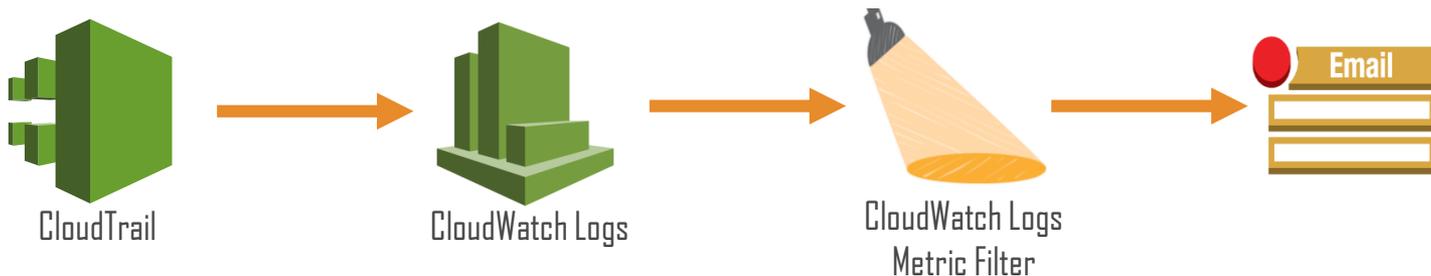
可視化



# CloudWatch Logs Metric Filter の利用



- CloudTrail と CloudWatch Logs の連携
  - アカウント内でコールされた特定のAPIを監視し、呼ばれたときに電子メール通知を受けることが可能



[http://aws.typepad.com/aws\\_japan/2015/03/cloudtrail-integration-with-cloudwatch-in-four-more-regions.html](http://aws.typepad.com/aws_japan/2015/03/cloudtrail-integration-with-cloudwatch-in-four-more-regions.html)

# CloudWatch logs Metric Filter (1/3)



- ログイベントから特定の文字列の検索が可能

## Define Logs Metric Filter

### Filter for Log Group: Linux-Sysytem-Logs

You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. [Learn more about pattern syntax.](#)

#### Filter Pattern



[Show examples](#)

#### Select Log Data to Test

[Clear](#)

```
Oct 18 03:01:04 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 6
Oct 18 03:01:04 ip-172-31-29-54 dhclient[1878]: DHCPACK from 172.31.16.1 (xid=0x15513166)
Oct 18 03:01:06 ip-172-31-29-54 dhclient[1878]: bound to 172.31.29.54 -- renewal in 1690
Oct 18 03:29:16 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 6
Oct 18 03:29:16 ip-172-31-29-54 dhclient[1878]: DHCPACK from 172.31.16.1 (xid=0x15513166)
Oct 18 03:29:18 ip-172-31-29-54 dhclient[1878]: bound to 172.31.29.54 -- renewal in 1585
```



#### Results

Found 17 matches out of 50 event(s) in the sample log.



[Show test results](#)

## Results

Found 17 matches out of 50 event(s) in the sample log.



Line Number	Line Content
1	Oct 18 03:01:04 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
4	Oct 18 03:29:16 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
7	Oct 18 03:55:43 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
10	Oct 18 04:20:18 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
13	Oct 18 04:43:37 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
16	Oct 18 05:11:50 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
19	Oct 18 05:39:11 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
22	Oct 18 06:06:23 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
25	Oct 18 06:32:33 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
29	Oct 18 03:01:04 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
32	Oct 18 03:29:16 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
35	Oct 18 03:55:43 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
38	Oct 18 04:20:18 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
41	Oct 18 04:43:37 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
44	Oct 18 05:11:50 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
47	Oct 18 05:39:11 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)
50	Oct 18 06:06:23 ip-172-31-29-54 dhclient[1878]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x1551)

# CloudWatch Logs Metric Filter (2/3)



- 特定文字列のエントリー頻度によりアラーム作成が可能
- “error”という文字列が3回以上エントリーされるとアラーム上げる

## Create Metric Filter and Assign a Metric

### Filter for Log Group: Linux-System-Logs

Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.

Filter Name: error message filtering ⓘ

Filter Pattern: error ⓘ

“error”という文字列を監視

### Metric Details

Metric Namespace: LogMetrics ⓘ

Metric Name: error ⓘ

Metric Value: 3 ⓘ

“error”という文字列のエントリー回数

Cancel

Back

Create Filter

# CloudWatch Logs Metric Filter (3/3)



- Metric Filterからアラーム作成、SNS連携が可能

Log Groups > Filters for Linux-Sysytem-Logs

Add Metric Filter

✓ Your filter **error message filtering** has been created.

Filter Name: error message filtering  
Filter Pattern: error  
Metric: LogMetrics / error  
Metric Value: 3

Create Alarm

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

Create Alarm

1. Select Metric 2. Define Alarm

Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name: CWL Linux SystemLog Errors

Description: CWL Linux SystemLog Errors

Whenever: error

is:  $\geq$  0

for: 1 consecutive period(s)

Actions

Define what actions are taken when your alarm changes state.

Notification

Whenever this alarm: State is ALARM

Send notification to: NotifyMe

Email list: sakatoku@amazon.co.jp

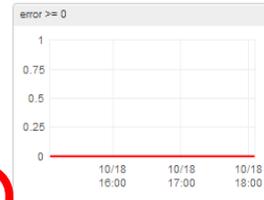
+ Notification

+ AutoScaling Action

+ EC2 Action

Alarm Preview

This alarm will trigger when the blue line goes up to or above the red line for a duration of 1 minute



Namespace: LogMetrics

Metric Name: error

Period: 1 Minute

Statistic: Sum



# Metric Filtersサンプル



- アカウントrootログインの監視

```
{ ($.eventName = "ConsoleLogin") && ($.userIdentity.type = "Root") }
```

- 認証失敗の監視

```
{$.errorCode = "AccessDenied" || $.errorCode =  
"UnauthorizedOperation"}
```

- 特定インスタンスタイプのEC2が作成されたかの監視

```
{$.eventName = "RunInstances" &&  
($.requestParameters.instanceType = "*.8xlarge" ||  
$.requestParameters.instanceType = "*.4xlarge")}
```

- セキュリティグループ変更の監視

```
{($.eventName = "AuthorizeSecurityGroupIngress") || ($.eventName =  
"AuthorizeSecurityGroupEgress") || ($.eventName =  
"RevokeSecurityGroupIngress" || ($.eventName =  
"RevokeSecurityGroupEgress") || ($.eventName =  
"CreateSecurityGroup") || ($.eventName = "DeleteSecurityGroup")}
```

# CloudWatchアラーム CloudFormationテンプレート



## CloudFormationをつかったメトリック フィルタの自動作成

```
1 {
2   "AWSTemplateFormatVersion" : "2010-09-09",
3   "Description" : "AWS CloudTrail API Activity Alarm Template for
  CloudWatch Logs",
4   "Parameters" : {
5     "LogGroupName" : {
6       "Type" : "String",
7       "Default" : "CloudTrail/DefaultLogGroup",
8       "Description" : "Enter CloudWatch Logs log group name. Default
  is CloudTrail/DefaultLogGroup"
9     },
10    "Email" : {
11      "Type" : "String",
12      "Description" : "Email address to notify when an API activity
  has triggered an alarm"
13    }
14  },
15  "Resources" : {
16    "SecurityGroupChangesMetricFilter" : {
17      "Type" : "AWS::Logs::MetricFilter",
18      "Properties" : {
19        "LogGroup" : { "Ref": "LogGroup" },
```

[http://aws.typepad.com/aws\\_japan/2015/03/cloudtrail-integration-with-cloudwatch-in-four-more-regions.html](http://aws.typepad.com/aws_japan/2015/03/cloudtrail-integration-with-cloudwatch-in-four-more-regions.html)

The screenshot displays three alarm configurations in the AWS CloudWatch console. Each configuration includes a filter name, filter pattern, metric, and metric value. The first alarm is for 'CloudTrailConsoleSignInFailures', the second for 'CloudTrailEC2InstanceChanges', and the third for 'CloudTrailEC2LargeInstanceChanges'. Each configuration has a 'Create Alarm' button and a 'new' badge.

Filter Name	Filter Pattern	Metric	Metric Value	Alarm Name
CloudWatchAlarm-CloudTrail-APIActivity-ConsoleSignInFailuresMetric Filter-35PVKU305SE3	{ (\$eventSource = ConsoleLogin) && (\$errorMessage = "Failed authentication") }	CloudTrailMetrics / ConsoleSignInFailureCount	1	CloudTrailConsoleSignInFailures
CloudWatchAlarm-CloudTrail-APIActivity-EC2InstanceChangesMetric Filter-1Q1TJK84379GF	{ (\$eventName = RunInstances)    (\$eventName = RebootInstances)    (\$eventName = StartInstances)    (\$eventName = StopInstances)    (\$eventName = TerminateInstances) }	CloudTrailMetrics / EC2InstanceEventCount	1	CloudTrailEC2InstanceChanges
CloudWatchAlarm-CloudTrail-APIActivity-EC2LargeInstanceChangesMetric Filter-r-V2DOYX90SA20	{ ((\$eventName = RunInstances)    (\$eventName = RebootInstances)    (\$eventName = StartInstances)    (\$eventName = StopInstances)    (\$eventName = TerminateInstances)) && ((\$requestParameters.instanceType = *.8xlarge)    (\$requestParameters.instanceType = *.4xlarge)) }	CloudTrailMetrics / EC2LargeInstanceEventCount	1	CloudTrailEC2LargeInstanceChanges



# AWS CloudTrail API Activity Lookup

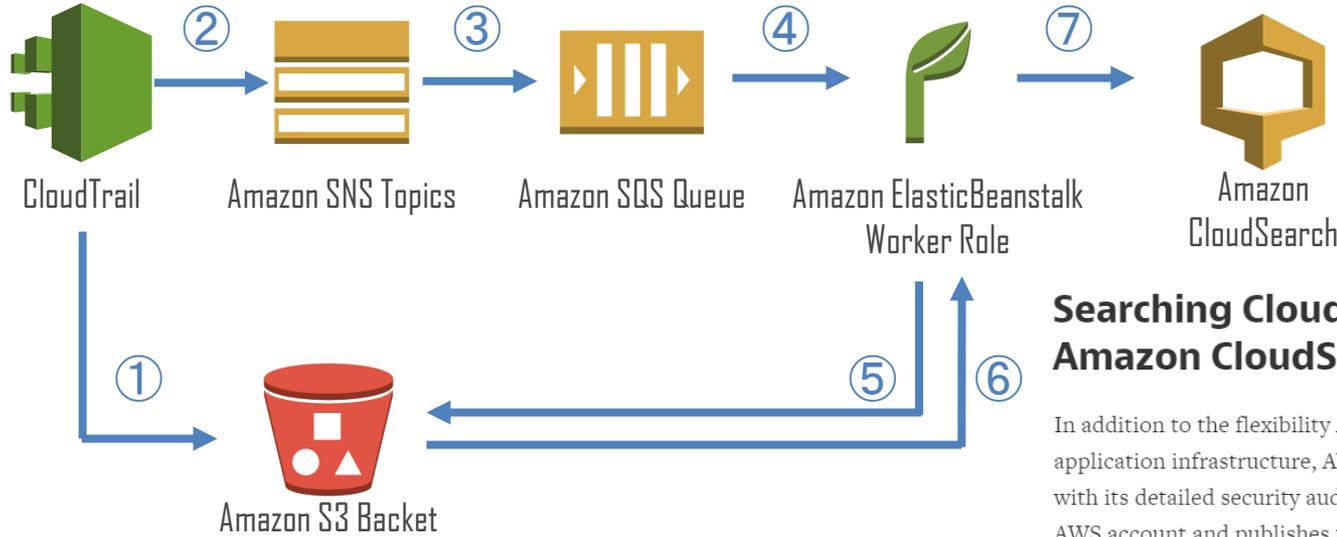


- CloudTrailコンソールまたはAWS SDK, AWS CLIからAPIアクティビティを検索する機能
- 東京リージョンでも利用可能
- CloudTrailが有効にするだけで自動で利用可能
- 最新の7日間のAPIアクティビティの検索



[http://aws.typepad.com/aws\\_japan/2015/03/new-aws-api-activity-lookup-in-cloudtrail.html](http://aws.typepad.com/aws_japan/2015/03/new-aws-api-activity-lookup-in-cloudtrail.html)

# Amazon CloudSearch, Amazon Elastic Beanstalk



## Searching CloudTrail Logs Easily with Amazon CloudSearch

In addition to the flexibility AWS provides startups in creating and deleting application infrastructure, AWS CloudTrail provides a key security service with its detailed security audit logs. It records the API calls made in your AWS account and publishes the resulting log files to an Amazon S3 bucket in JSON format. But without appropriate tooling, audit log review can be cumbersome. In today's post, you'll see how to set up a simple CloudTrail log analysis solution based on Amazon CloudSearch, a fully managed cloud-based search service.

<https://medium.com/aws-activate-startup-blog/searching-cloudtrail-logs-easily-with-amazon-cloudsearch-2d716e23efee>

# CloudTrail JSON to CloudSearch Table



## CloudTrail JSON

- **eventTime**
- eventVersion
- **userIdentity**
- **eventSource**
- **eventName**
- **awsRegion**
- **sourceIPAddress**
- userAgent
- errorCode
- errorMessage
- requestParameters
- responseElements
- **requestID**
- **eventID**
- eventType
- apiVersion
- recipientAccountID



## CloudSearch

LARGE SCREEN

KEY COLUMN			
mmmm			
mmmm			
mmmm			

# CloudTrail JSON "userIdentity"



```
"userIdentity": {  
  "type": "AssumedRole",  
  "principalId": "AROAI DPPEZS35WEXAMPLE:AssumedRoleSessionName",  
  "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",  
  "accountId": "123456789012",  
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
  "sessionContext": {  
    "attributes": {  
      "creationDate": " 20131102T010628Z ",  
      "mfaAuthenticated": "false"  
    },  
    "sessionIssuer": {  
      "type": "Role",  
      "principalId": "AROAI DPPEZS35WEXAMPLE",  
      "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",  
      "accountId": "123456789012",  
      "userName": "RoleToBeAssumed"  
    }  
  }  
}
```

## CloudTrail JSON

- Type
- arn
- accountId
- accessKeyId
- accountId
- userName

# CloudTrail JSON to CloudSearch Table



## CloudTrail JSON

- **eventTime**
- eventVersion
- **userIdentity**
  - **Type**
  - **arn**
  - **accountID**
  - **accessKeyId**
  - **accountId**
  - **userName**
- **eventSource**
- **eventName**
- **awsRegion**
- **sourceIPAddress**
- userAgent
- errorCode
- errorMessage
- requestParameters
- responseElements
- **requestID**
- **eventID**
- eventType
- apiVersion
- recipientAccountID

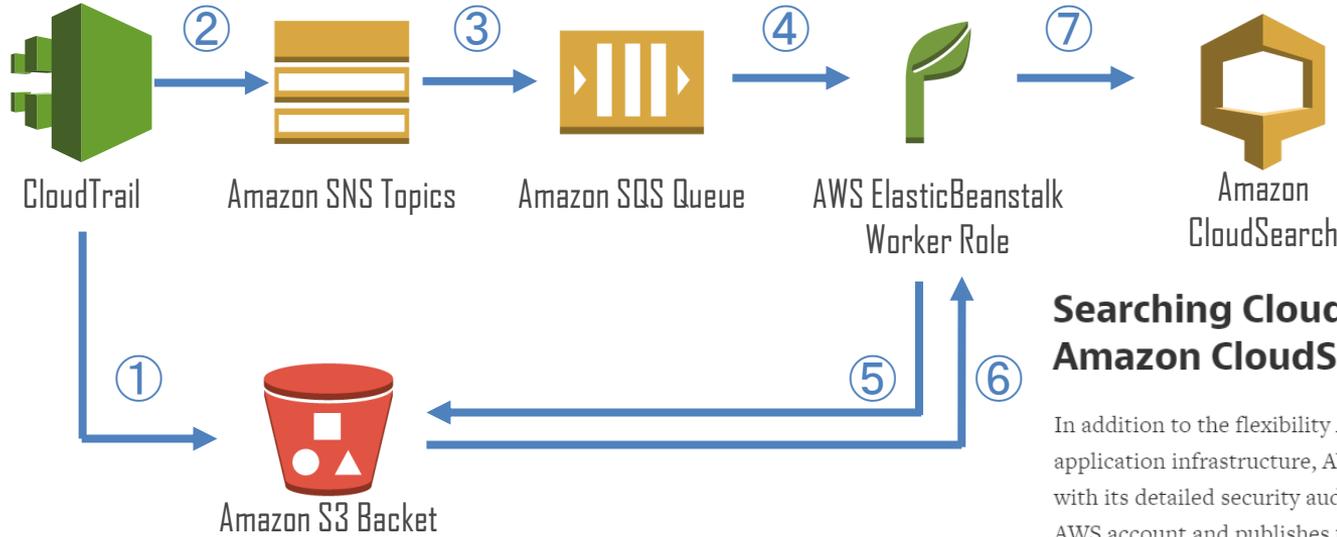


## CloudSearch

LARGE SCREEN

KEY COLUMN			
mmmm			
mmmm			
mmmm			

# Amazon CloudSearch, Amazon Elastic Beanstalk



## Searching CloudTrail Logs Easily with Amazon CloudSearch

In addition to the flexibility AWS provides startups in creating and deleting application infrastructure, AWS CloudTrail provides a key security service with its detailed security audit logs. It records the API calls made in your AWS account and publishes the resulting log files to an Amazon S3 bucket in JSON format. But without appropriate tooling, audit log review can be cumbersome. In today's post, you'll see how to set up a simple CloudTrail log analysis solution based on Amazon CloudSearch, a fully managed cloud-based search service.

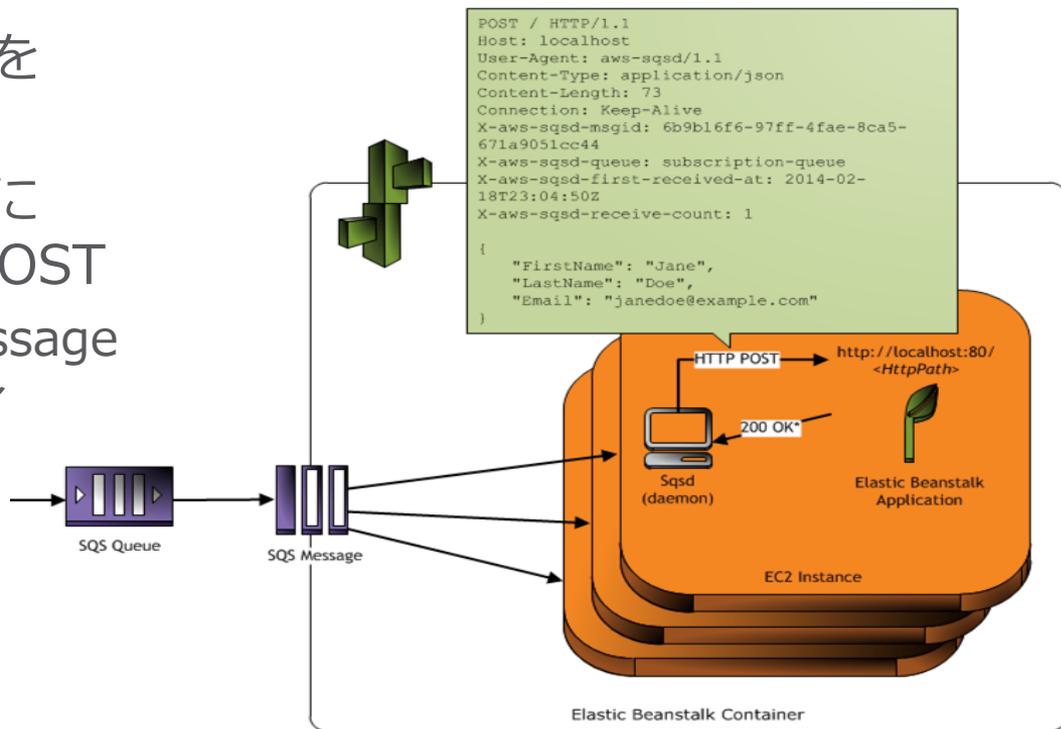
<https://medium.com/aws-activate-startup-blog/searching-cloudtrail-logs-easily-with-amazon-cloudsearch-2d716e23efee>

# AWS Elastic Beanstalk Worker Tier

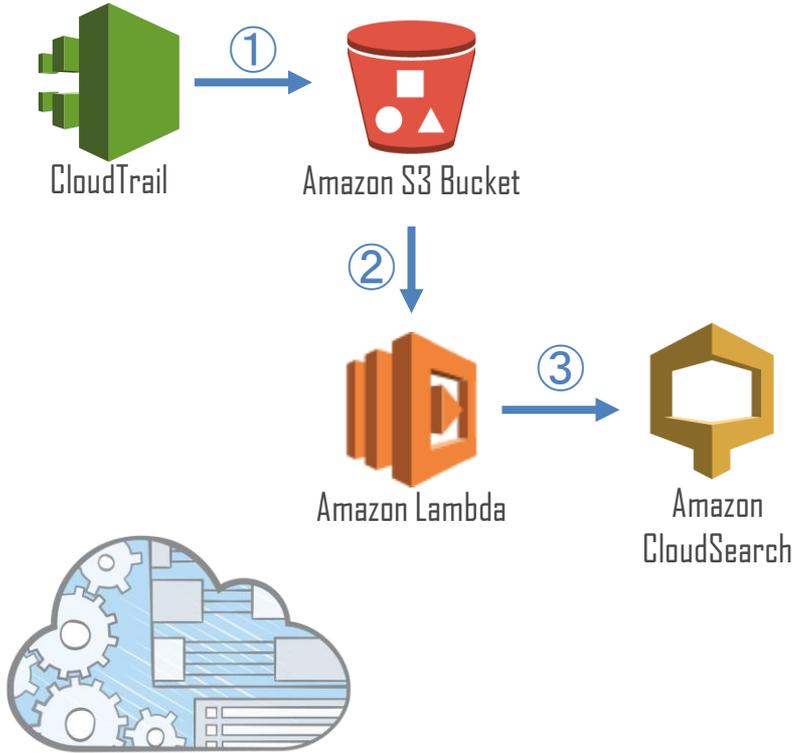


## Webアプリを実装するだけでSQSを使った非同期処理Workerを実装

- SQSに登録されたタスクを非同期処理するTier
- SQSメッセージは自動的にHTTPエンドポイントにPOST
  - 200 OKならDelete Message
  - エラー応答ならリトライ



# Amazon CloudSearch, Amazon Lambda



Search: event\_source:'sqs.amazonaws.com' Go Options No Suggester

Filter Query:

Query Parser: Structured Default Operator: and (default)

Search Fields: List of fields you want to search with optional boost. Example: title^5, description^2, summary

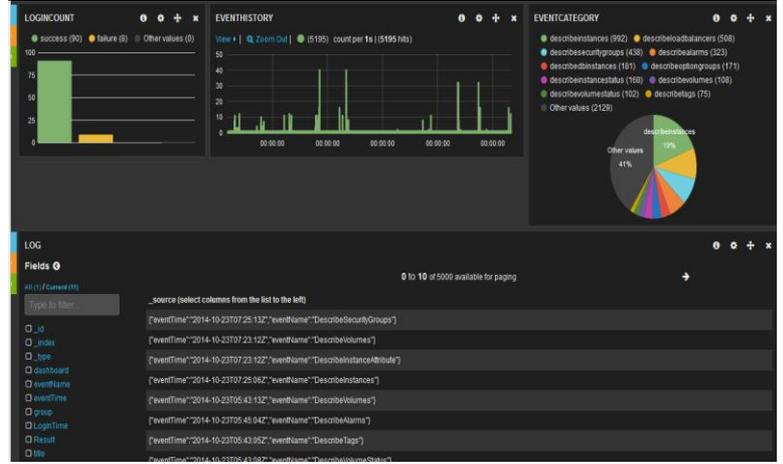
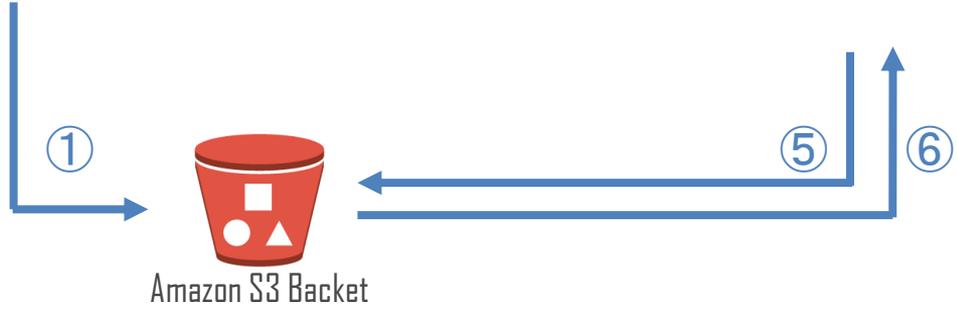
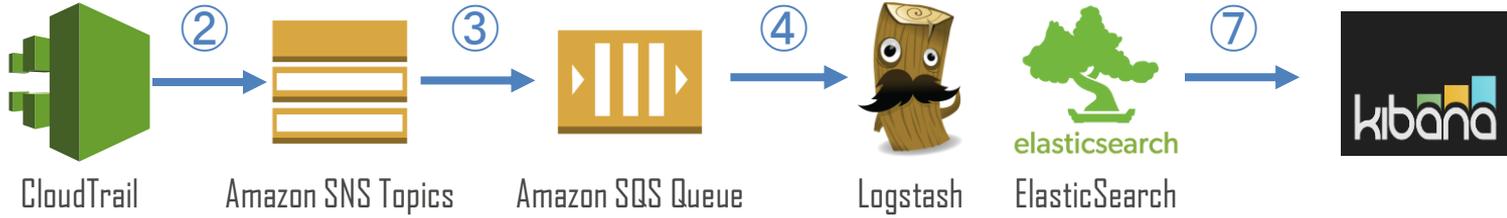
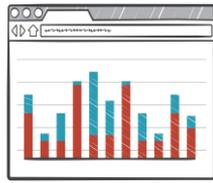
Sort by: Document Score Descending (view raw: JSON or XML) 1 to 10 of 23 Results

1. 325562c8-a8cd-42d8-b0b2-a2194f89686a	
_score	10.123007
user_identity_arn	arn:aws:iam::926983381032:user/root
event_source	sqs.amazonaws.com
event_time	2014-09-22T12:41:00Z
source_ip_address	54.240.197.233
event_id	325562c8-a8cd-42d8-b0b2-a2194f89686a
aws_region	eu-west-1
user_identity_user_name	root
raw	{ "eventVersion": "1.01", "eventID": "325562c8-a8cd-42d8-b0b2-a2194f89686a", "eventTime": "... more..."
user_agent	signin.amazonaws.com
user_identity_account_id	926983381032
user_identity_type	IAMUser
event_name	SetQueueAttributes
2. b3836873-731d-4a1e-bc8e-47ba690ab7c4	
_score	10.123007

Filter Search Results

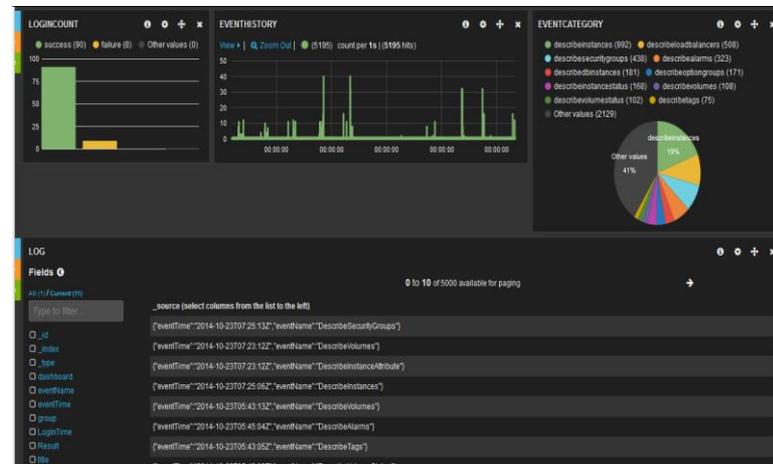
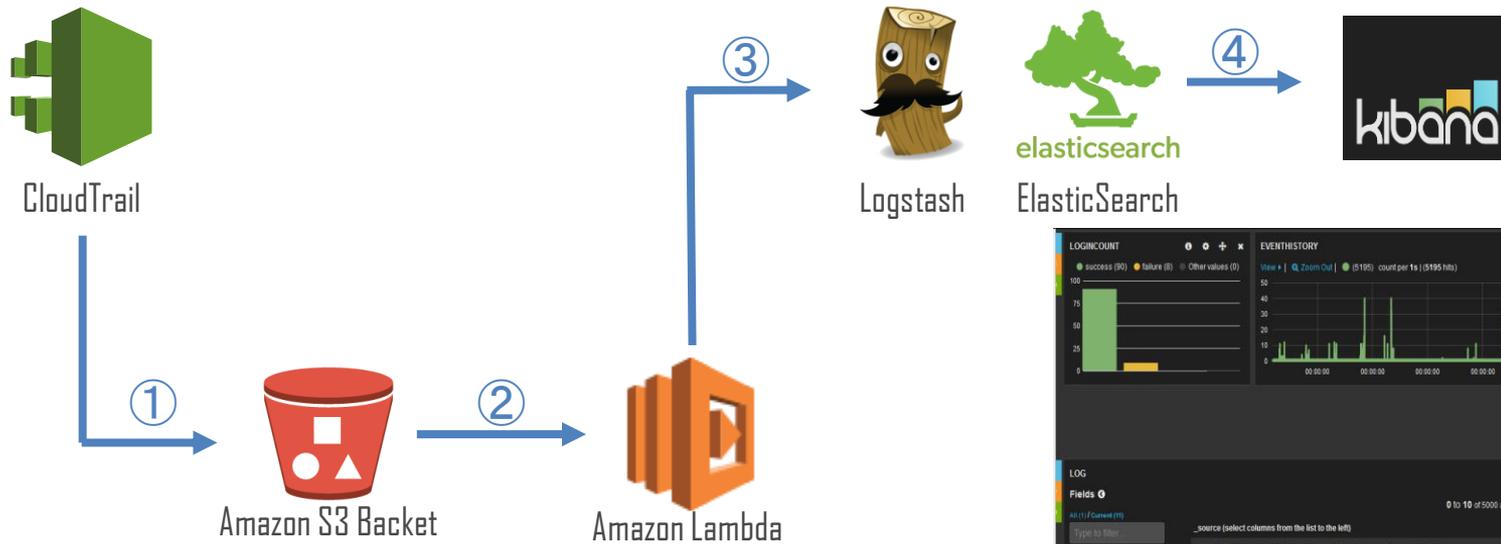
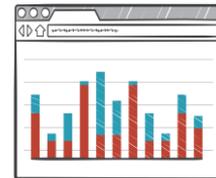
- aws\_region
  - eu-west-1 (23)
- error\_code
- event\_name
  - SetQueueAttributes (13)
  - CreateQueue (7)
  - DeleteQueue (3)
- source\_ip\_address
  - 54.240.197.233 (6)
  - 80.12.59.193 (5)
  - 54.240.197.234 (4)

# ElasticSearch, Kibana



[https://blogs.amazon.com/aws\\_solutions/archive/2014/10/processing-cloudtrail-logs-into-logstashelasticsearchkibana.html](https://blogs.amazon.com/aws_solutions/archive/2014/10/processing-cloudtrail-logs-into-logstashelasticsearchkibana.html)

# ElasticSearch, Kibana, Amazon Lambda



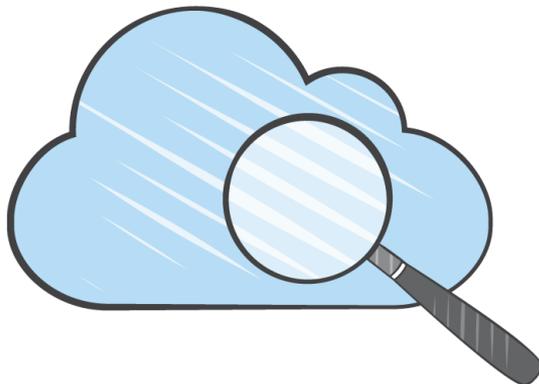
[https://blogs.amazon.com/aws\\_solutions/archive/2014/10/processing-cloudtrail-logs-into-logstashelasticsearchkibana.html](https://blogs.amazon.com/aws_solutions/archive/2014/10/processing-cloudtrail-logs-into-logstashelasticsearchkibana.html)

# 用途に応じた使い分けが必要

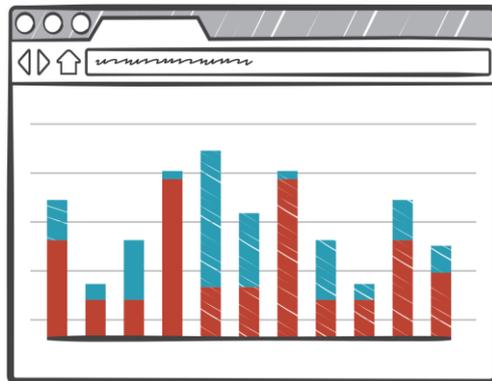
アラート



文字列検索



可視化





**AWS Config**

# AWS Config

- *AWS Config*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ことができるフルマネージドサービスです。
- *AWS Config*は、*Amazon EC2*インスタンスのタグの値、セキュリティグループのルール、*NACL*、*VPC*といった*AWS*リソースの構成属性変更を記録します。



# AWS Config

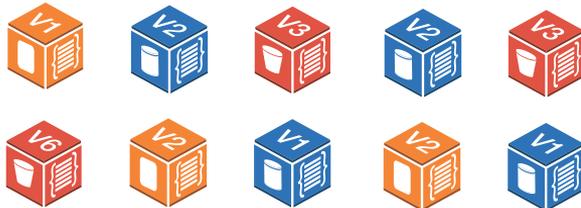
## Configuration Stream

- 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

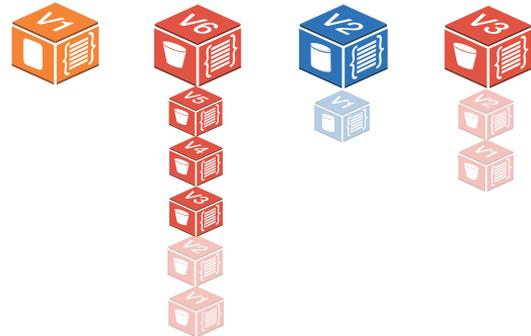
- あるポイントでのコンフィグレーションアイテムの集合
- 自動で定期的あるいは変更トリガで作成され、Amazon S3にエクスポートされる



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

## Configuration Snapshot

- 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

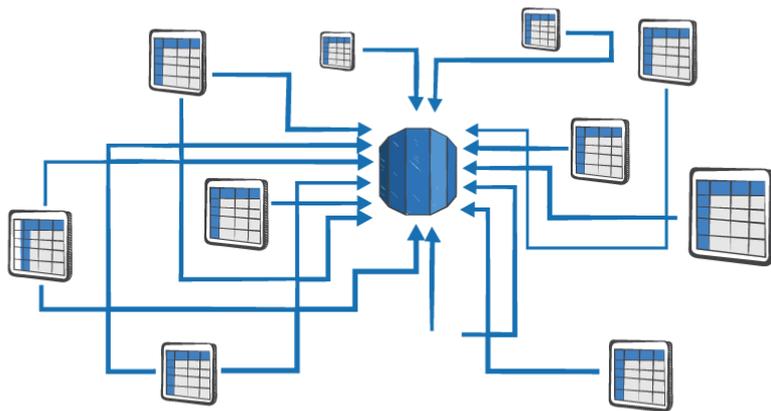


# リレーションシップ

- 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



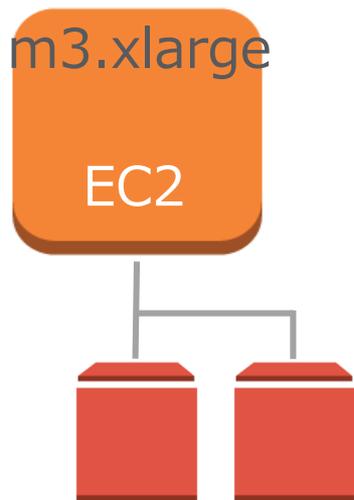
# コンフィグレーション アイテム

コンポーネント	説明	情報
メタデータ	構成アイテムの情報	バージョンID 構成アイテムID 構成アイテムがキャプチャされた時間 設定項目の順序を示す状態ID MD5Hashなど
属性	リソース属性	リソースID タグ リソースタイプ アマゾン リソース名 (ARN) アベイラビリティゾーンなど
リレーションシップ	アカウントに関連付けられたリソースの関係	EBS "vol-1234567 "が EC2インスタンス "i-a1b2c3d4"にアタッチ
現在の構成	リソースの記述またはリストAPIの呼び出しの返り値	DeleteOnTerminationフラグの状態 ボリュームタイプ(gp2, io1)
関連イベント	現在の構成に関連するAWS CloudTrail イベント	AWS CloudTrail イベントID

# リソース構成変更例

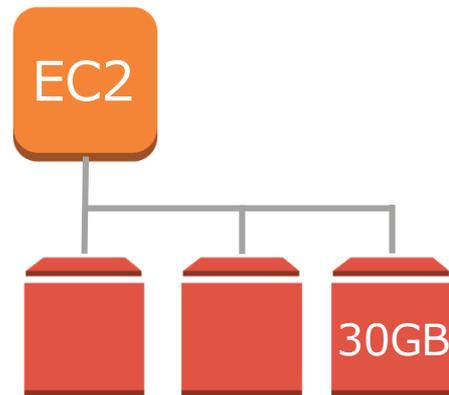
- インスタンスタイプの変更(m3.xlarge → m3.medium)
- EBSボリュームの追加

変更前



変更後

m3.medium



# リソース情報 (変更)

▼ Changes (8)

Configuration Changes (7)

変更前

変更後

Field	From	To
Configuration.LaunchTime	"2014-11-26T10:11:03.000Z"	"2014-11-26T11:25:36.000Z"
Configuration.State.Name	"stopped"	"running"
Configuration.BlockDeviceMappings.0	null	Object
Configuration.StateReason	Object	null
Configuration.StateTransitionReason	"User initiated (2014-11-26 11:19:36 GMT)"	""
Configuration.State.Code	80	16
Configuration.InstanceType	"m3.xlarge"	"m3.medium"

インスタンスタイプの変更

Relationship Changes (1)

ボリュームの追加

Field	From	To
AWS::EC2::Volume	null	"vol-caf71781"

# リソース情報 (リレーション)

変更前

▼ Relationships

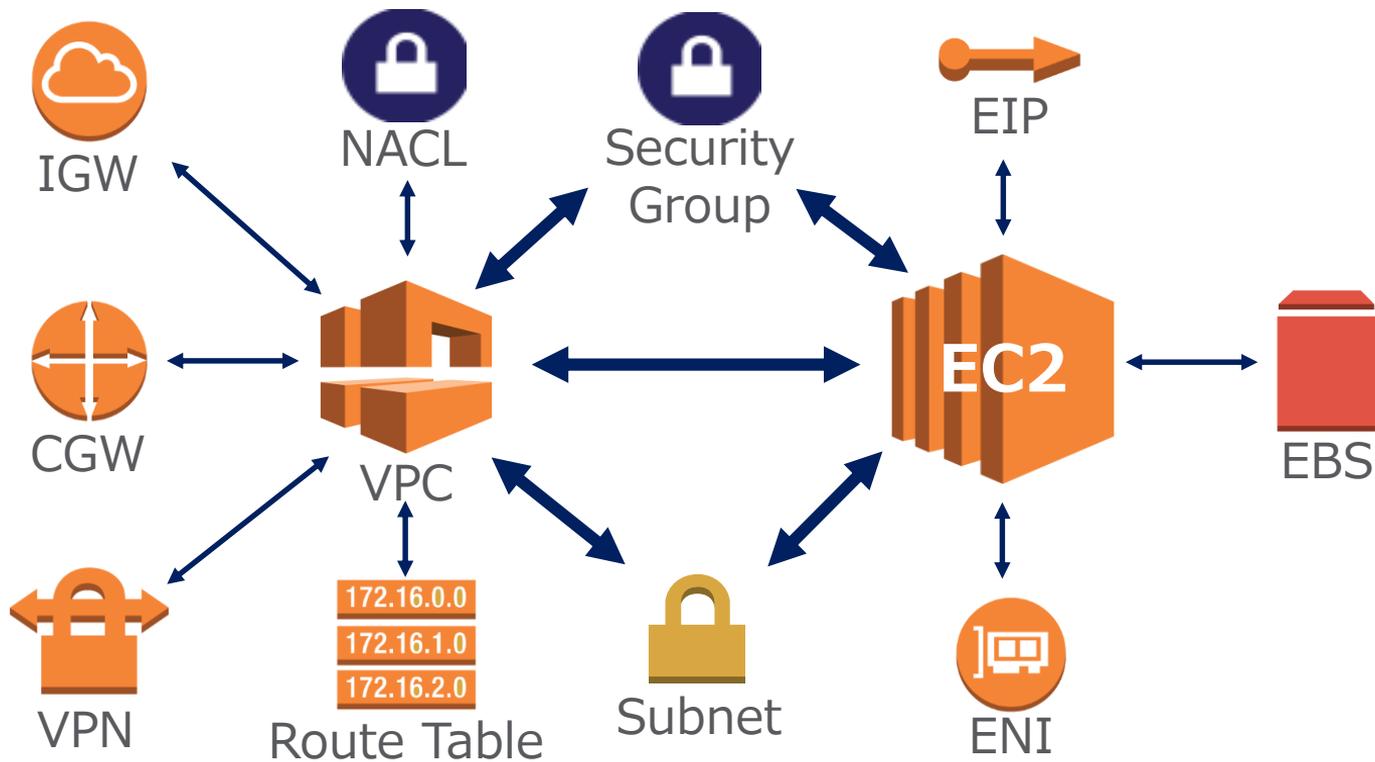
EC2 EIP	EC2 NetworkInterface	EC2 SecurityGroup	EC2 Subnet	EC2 Volume
eipalloc-e6dc7283	eni-827041f4	sg-53f98236	subnet-a1db1cd6	vol-633b3a2b
				vol-bf160af7

変更後

▼ Relationships

EC2 EIP	EC2 NetworkInterface	EC2 SecurityGroup	EC2 Subnet	EC2 Volume
eipalloc-e6dc7283	eni-827041f4	sg-53f98236	subnet-a1db1cd6	vol-633b3a2b
				vol-bf160af7
				vol-caf71781

# AWS Config リレーションシップ



# サポートされるAWSリソース

- AWSリソースは、AWS Management Console、コマンドラインインターフェース（CLI）、AWS SDK、またはAWSパートナーのツールを使いユーザーが作成できるエンティティ



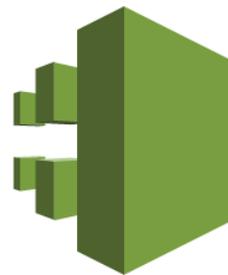
Amazon EC2  
Instance, ENI...



Amazon VPC  
VPC, Subnet...



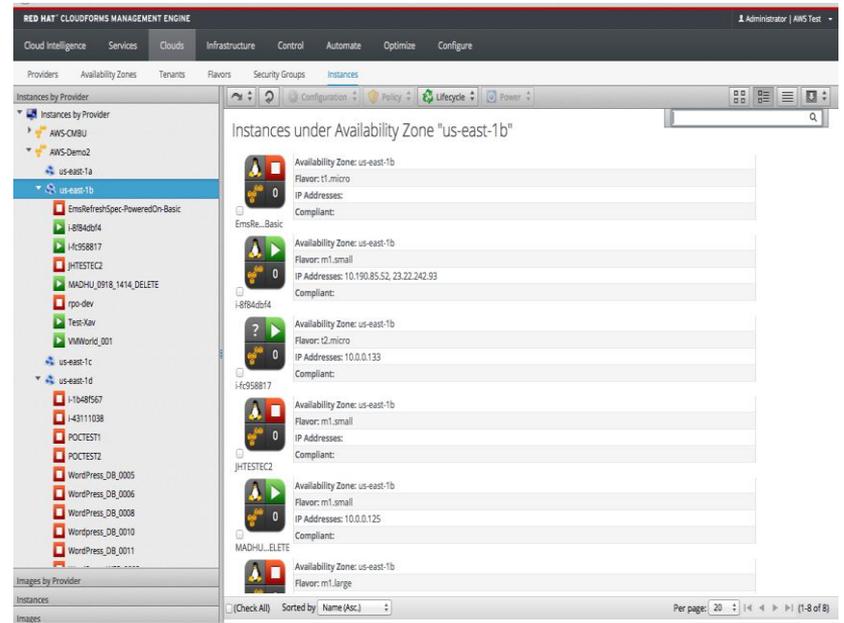
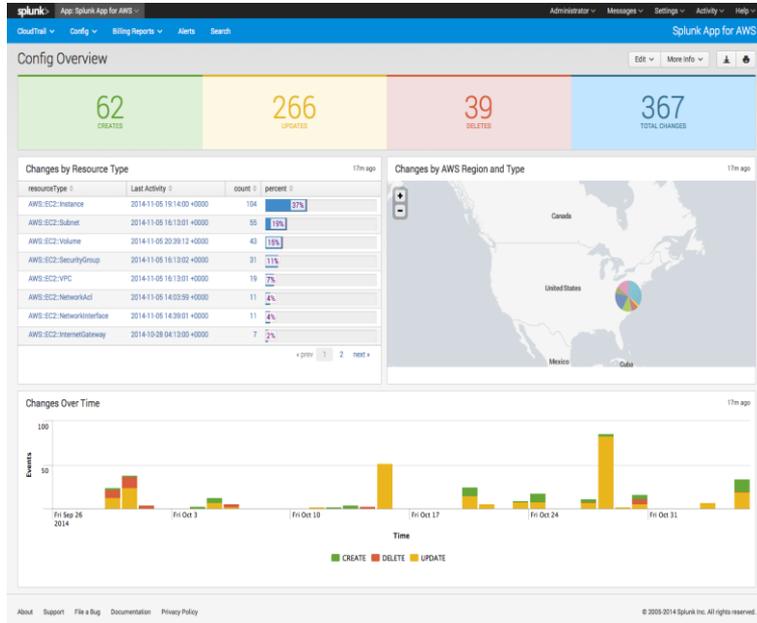
Amazon EBS  
Volumes



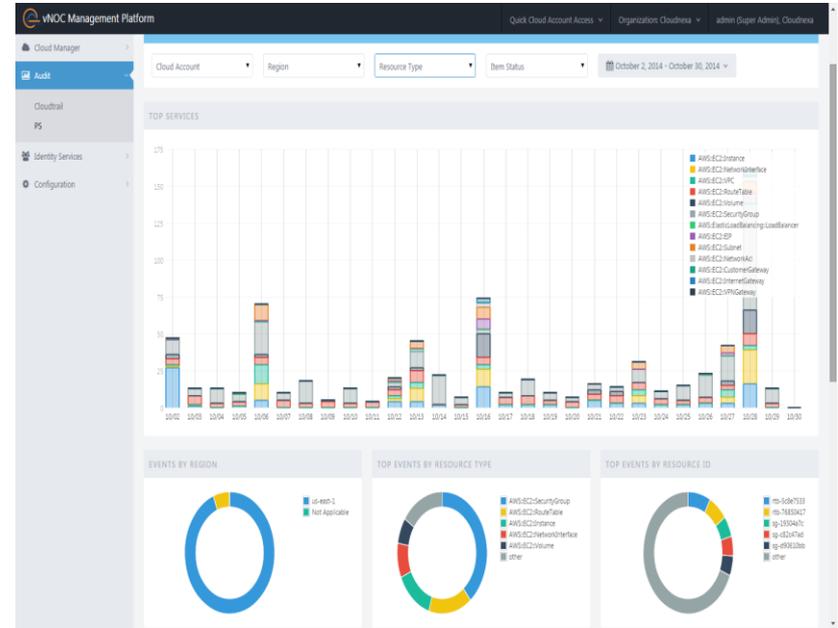
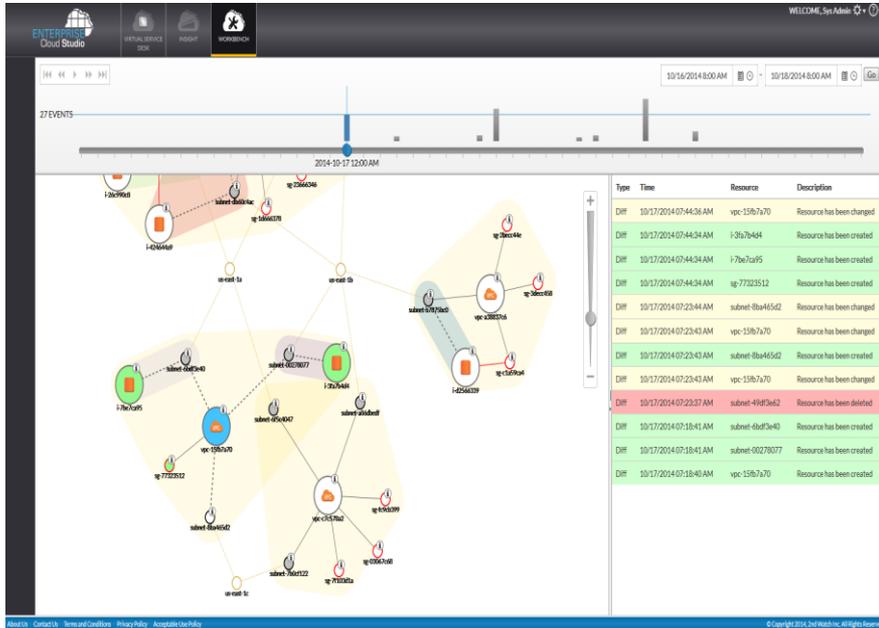
AWS CloudTrail

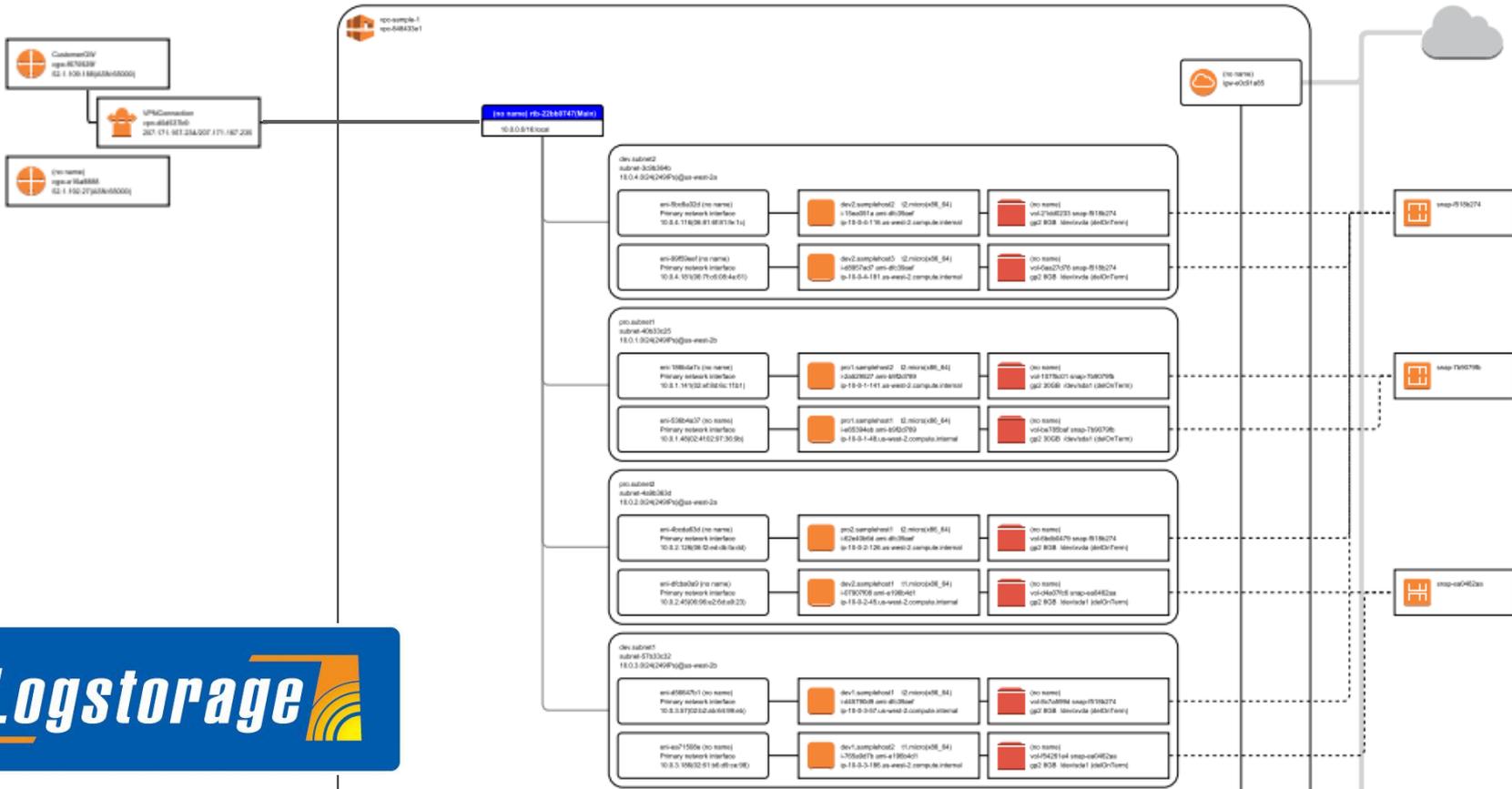
# AWS Config パートナー

splunk >



# AWS Config パートナー





# CloudTrailについて AWSサポートから伝えたい たったひとつのこと



## Turn on CloudTrail

[Learn more](#)

Create a new S3 bucket?  Yes  No

[Documentation](#)

[Forums](#)

[FAQs](#)

# とりあえずON

S3 bucket\*

[Advanced](#)

Required field

Cancel

Turn On

# Q. CloudTrailの料金はその程度かかりますか？

- CloudTrail に追加料金はかかりません
  - S3 と SNS の標準の使用料金

API call の発生状況



S3

API call の発生状況  
SNS設定の有無



SNS

# Q. CloudTrailを有効化していないとどうなりますか？

インスタンス起動失敗したけどエラーメッセージ見逃した！



いつの間にかセキュリティグループが変更されてた・・・



このRedshiftクラスタって誰が起動したんだっけ？



Q. 今はCloudTrailを使う予定がないのですが、とりあえず有効化してみます。後からどう活用できますか？

- **トラブルの個別調査**

- トラブルが発生した場合、記録されたCloudTrailのログをさかのぼって調査することが可能

- **傾向分析**

- 蓄積されたCloudTrailのログをEMR等のデータソースに投入して分析することが可能

# CloudTrailによる 簡単トラブルシューティング

# CloudTrailのログの探し方

- CloudTrail look up
- CloudTrailログファイル(S3)
- その他
  - CloudSearchと連携
  - サードパーティツールと連携

# CloudTrail look up

- Time rangeから探す
- Attributeから探す
  - EventId
  - EventName
  - Username
  - ResourceType
  - ResourceName

# CloudTrail look up – マネジメントコンソール



AWS

Services

Edit

Noritaka Sekiyama

Tokyo

Support

## API Activity History

Configuration

## API Activity History

Look up API activity captured for your AWS account in the last 7 days. Filter using one of the attributes to troubleshoot operational issues or security inci...



Filter:

Event name

Enter event name

Time range:

Select time range



- User name
- Event name**
- Resource type
- Resource name

- A
- AcceptVpcPeeringConnection
- ActivateGateway
- ActivatePipeline
- ActivateUser
- AddCache
- AddClientIDToOpenIDConnectPr...
- AddInstanceGroups
- AddJobFlowSteps
- AddRoleToInstanceProfile
- AddSourceIdentifierToSubscription
- AddTags

Event name	Resource type	Resource name
RevokeSecurityGroupIngress	SecurityGroup	sg-18aa457d

**Event source** ec2.amazonaws.com

**Event time** 2015-03-28, 08:23:05 PM

**Request ID** aaf5a806-026b-4043-9245-3d517164fef9

**Source IP address** 27.0.3.145

**User name** root

### Resources Referenced (0)

[sg-18aa457d](#)  
SecurityGroup

View event

▶ 2015-03-28, 08:17:04...	root	RunInstances	Ami	ami-cbf90ecb
▶ 2015-03-28, 08:16:51	root	RunInstances	Ami	ami-cbf90ecb

# CloudTrail look up – AWS CLI

```
$ aws cloudtrail lookup-events --lookup-attributes  
AttributeKey=<Attribute Key>,AttributeValue=<Attribute Value>  
--start-time <Start Time> --end-time <End Time>
```

```
[  
  {  
    "EventId": "c048e8a4-42d7-4c3c-84e6-87560b3b9eaa",  
    "Username": "root",  
    "EventTime": 1427525552,  
    "CloudTrailEvent": "{\"eventVersion\":\"1.02\", \"userIdentity\": {\"type\": \"Root\", \"principalId\": \"\"},  
    \"eventName\": \"RunInstances\",  
    \"resources\": [{\"resourceType\": \"AWS::EC2::Ami\", \"resourceName\": \"ami-a15666a0\"}, {\"Reso  
  }  
]
```

# CloudTrail ログファイル(S3)

- ログファイルから探す

- bucket\_name>/prefix\_name/AWSLogs/Account ID/CloudTrail/region/YYYY/MM/DD/file\_name.json.gz

```
All Buckets
```

```
  Bucket_Name
```

```
    AWSLogs
```

```
      123456789012
```

```
        CloudTrail
```

```
          ap-northeast-1
```

```
            2015
```

```
              03
```

```
                29
```

```
123456789012_CloudTrail_ap-northeast-1_20150329T1255ZHdkvFTXOA3Vnhbc.json.gz
```

# ケーススタディ

- A. 対象のAPIリクエストにて発生したエラーの原因は何か
- B. 対象のAPIリクエストがいつ発行されたか
- C. 対象のリソースが誰によって変更されたか

# A. 対象のAPIリクエストにて発生したエラーの原因は何か

- 問題設定

- Run Instances API実行時にエラーが発生したが原因が不明
- APIの発行日は 2015/03/29

- 目的の情報

- ErrorCode: エラーコード
- ErrorMessage: エラーメッセージ

# A. 対象のAPIリクエストにて発生したエラーの原因は何か

- トラブルシューティング

- CloudTrail look upによる例

```
$ aws cloudtrail lookup-events --lookup-attributes  
AttributeKey=EventName,AttributeValue=RunInstances  
--start-time 2015-03-29 --end-time 2015-03-29
```

```
"errorCode": "Client.InvalidParameterCombination",  
"errorMessage": "Non-Windows instances with a virtualization type of  
u0027hvmu0027 are currently not supported for this instance type.",
```

## B. 対象のAPIリクエストがいつ発行されたか

- 問題設定
  - セキュリティグループのルールが削除された
  - 操作日時は不明
- 目的の情報
  - EventTime: 発行日時

## B. 対象のAPIリクエストがいつ発行されたか

- トラブルシューティング
  - CloudTrail look upによる例

```
$ aws cloudtrail lookup-events --lookup-attributes  
AttributeKey=EventName,AttributeValue=RevokeSecurityGroupIngress
```

```
"EventTime": 1427541785.0,  
"EventName": "RevokeSecurityGroupIngress",
```

# C. 対象のリソースが誰によって変更されたか

- 問題設定

- 特定のインスタンスに何らかのAPIが発行された可能性がある
- Instance IDは把握しているが、発行元が不明

- 目的の情報

- UserIdentity: 発行ユーザ

## C. 対象のリソースが誰によって変更されたか

- トラブルシューティング
  - CloudTrail look upによる例

```
$ aws cloudtrail lookup-events --lookup-attributes  
AttributeKey=ResourceName,AttributeValue=i-da8dfd29
```

```
"type": "Root",  
"arn": "arn:aws:iam:: 123456789012 ",  
"accountId": "123456789012",  
"accessKeyId": "ASIA*****"
```

# CloudTrail x AWSサポート

# トラブルシューティング時の流れ

## • ユーザー

### – 事象の検知

- ログの確認
- 一次切りわけ
- 問題範囲の限定



## • AWSサポート

### 事象の確認

- AWS 基盤側の調査
- 二次切りわけ
- 再現試験 …etc.

### – ご対応



- 対応策の実施
- 切りわけ再実施



# お問い合わせ時に頂きたい情報

- アカウントID
- 実行IAMユーザ、ロール
- 呼び出し元 (オンプレ環境、インスタンスID等)
- 操作対象のリージョン、リソース
- 発生した事象 (例外の内容)

# お問い合わせ時に頂きたい情報

**赤字：CloudTrailに含まれる情報**

- アカウントID
- 実行IAMユーザ、ロール
- 呼び出し元 (オンプレ環境、インスタンスID等)
- 操作対象のリージョン、リソース
- 発生した事象 (例外の内容)

# CloudTrail よくある質問

# Q. 全てのAPI callが記録されますか？

- 対応サービス、対応APIのcallを記録する
  - サービスの対応状況は [Supported Services - AWS CloudTrail User Guide](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/what-is-cloud-trail-supported-services.html) を参照  
<http://docs.aws.amazon.com/awscloudtrail/latest/userguide/what-is-cloud-trail-supported-services.html>
- EndPointに到達しなかったAPI callは記録されない
  - AWS CLIやSDKのクライアントサイドのエラー調査にはログが必要

# Q. 全てのAPI callが記録されますか？

- 非対応サービスの例：S3
  - API callを記録する方法は現時点で存在しない
  - S3アクセスログがロギングの唯一の手段

# Q. 全てのAPI callが記録されますか？

- 非対応APIをもつサービスの例：CloudWatch

記録されるAPI	記録されないAPI
PutMetricAlarm	GetMetricStatistics
DescribeAlarms	ListMetrics
DescribeAlarmHistory	PutMetricData
DescribeAlarmsForMetric	
DisableAlarmActions	
EnableAlarmActions	
SetAlarmState	
DeleteAlarms	

# Q. リクエスト・レスポンスの中身は記録されますか？

- リクエスト
  - requestParametersに記録される
- レスポンス
  - responseElementsに記録される
  - ※**変更系のAPIのみ記録される**（参照系のAPIではnullになる）

## Q. sourceIPAddressにDNS名が入った見覚えのないログは何ですか？

- AWSサービスサイドから発行されるログ
  - 例:

```
"eventSource": "rds.amazonaws.com",  
"eventName": "CreateDBInstance",  
"awsRegion": "ap-northeast-1",  
"sourceIPAddress": "cloudformation.amazonaws.com",  
"userAgent": "cloudformation.amazonaws.com",  
"requestParameters": {  
  "allocatedStorage": 5,  
  "port": 3306,  
  "masterUserPassword": "*****",
```

Q. API callからCloudTrailに記録されるまでどれくらいかかりますか？

- S3へのログの記録：API callから**15分**以内

ご清聴ありがとうございました。