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

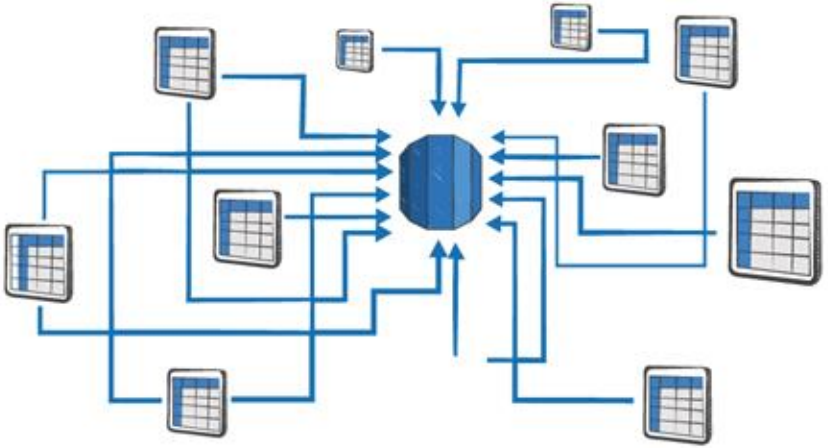
クラウドサポート エンジニア

- 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

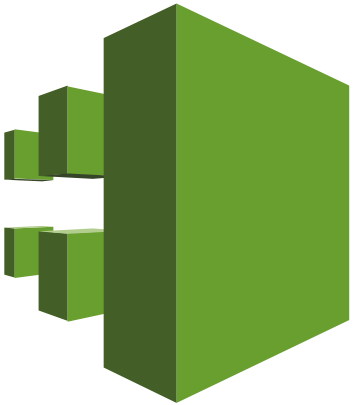
API管理

リソース管理



クラウドならではの運用管理

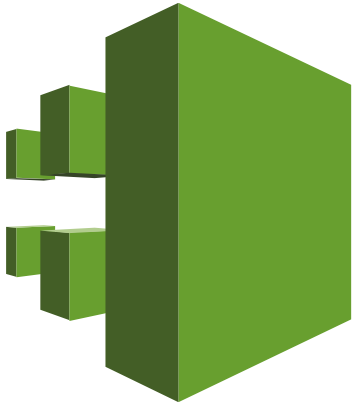
API管理



AWS CloudTrail

リソース管理

AWS Config



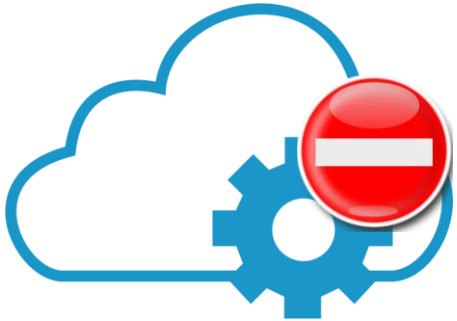
AWS CloudTrail

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



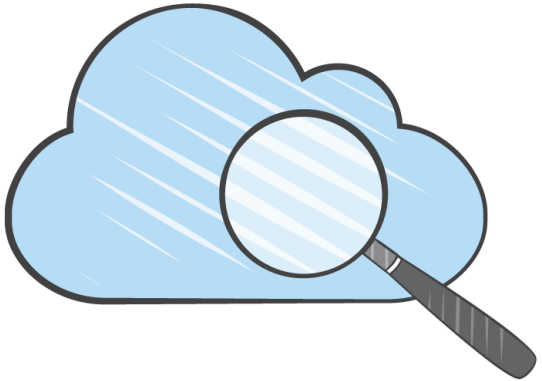
- ユーザのサインイン アクティビティ
  - AWS マネジメント コンソール
  - AWS ディスカッション フォーラム


149022,
"type": "Organization",
"login": "atomicobject",
"starred_url": "https://api.github.com/
"gravatar_id": "bd869a731379aa8c867b1
"received_events_url": "https://api.github.com/
JSON形式での出力

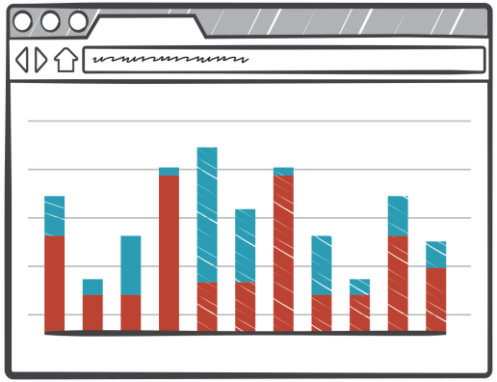
蓄積したJSONファイルをどう扱うか???

アラート

文字列検索

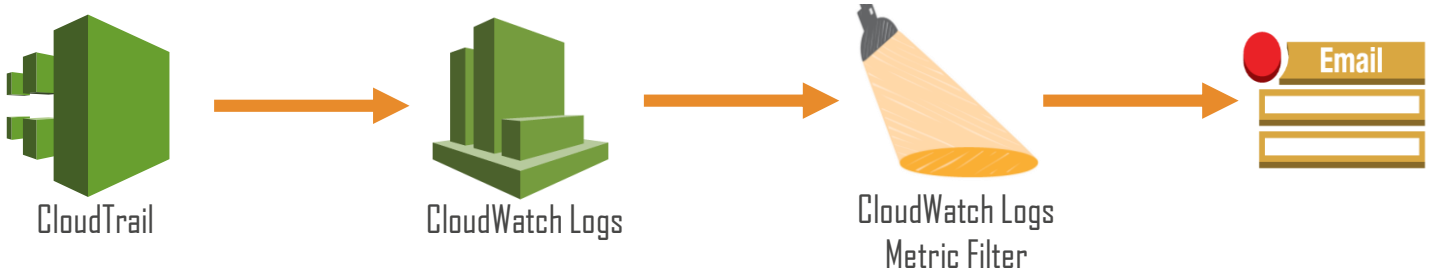


可視化



CloudWatch Logs Metric Filter の利用

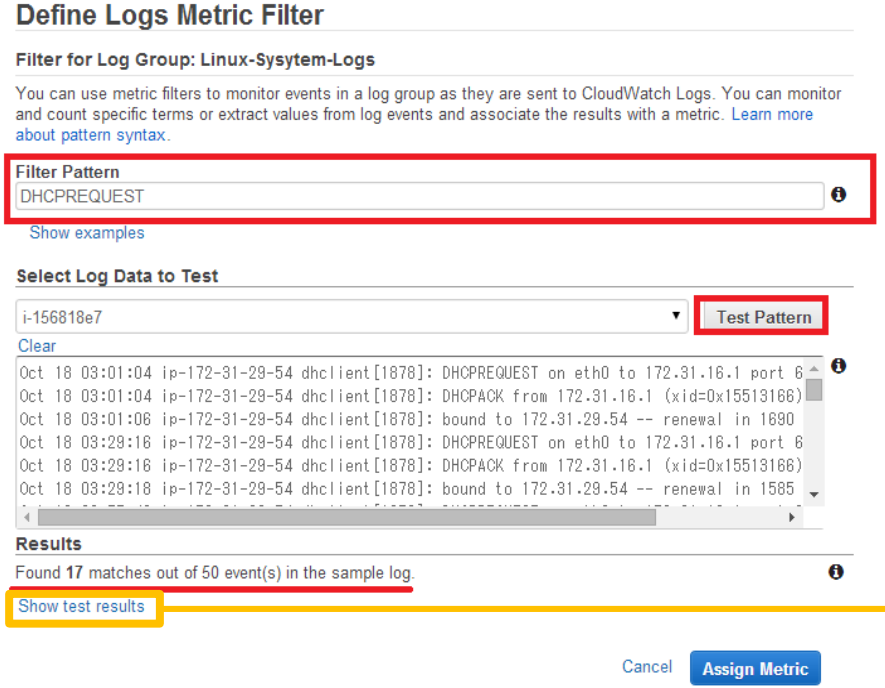
- CloudTrail と CloudWatch Logs の連携
  - アカウント内でコールされた特定のAPIを監視し、呼ばれたときに電子メール通知を受けることが可能

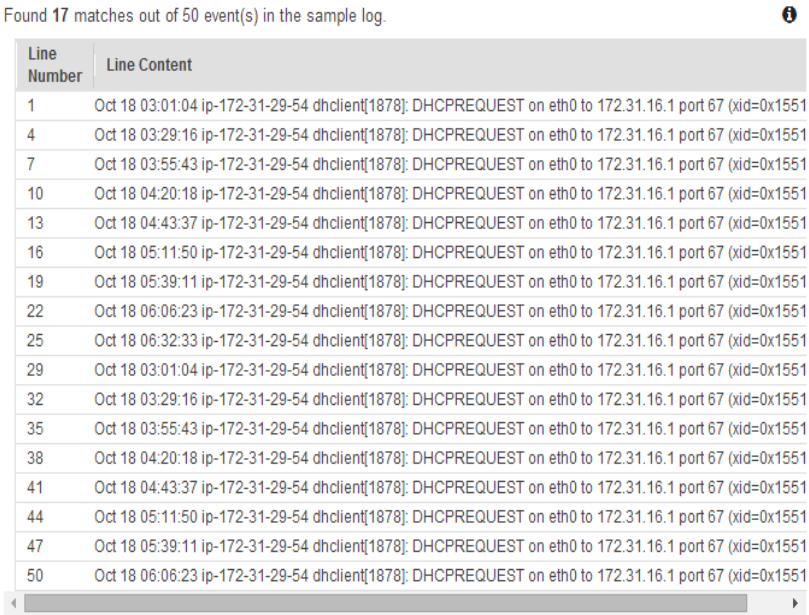


http://aws.typepad.com/aws_japan/2015/03/cloudtrail-integration-with-cloudwatch-in-four-more-regions.html

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

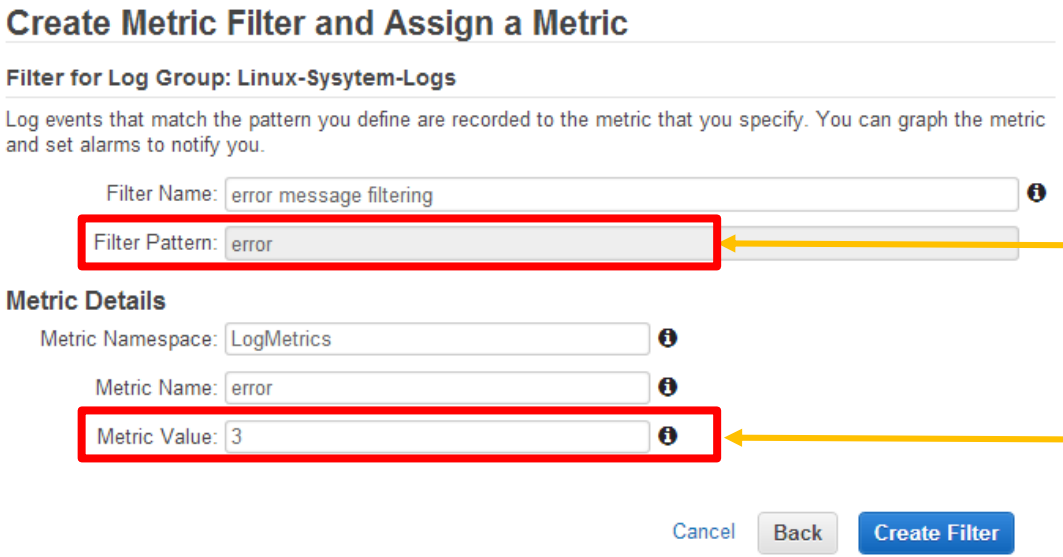




CloudWatch Logs Metric Filter（2/3）

- 特定文字列のエントリ頻度によりアラーム作成が可能

→ **“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**

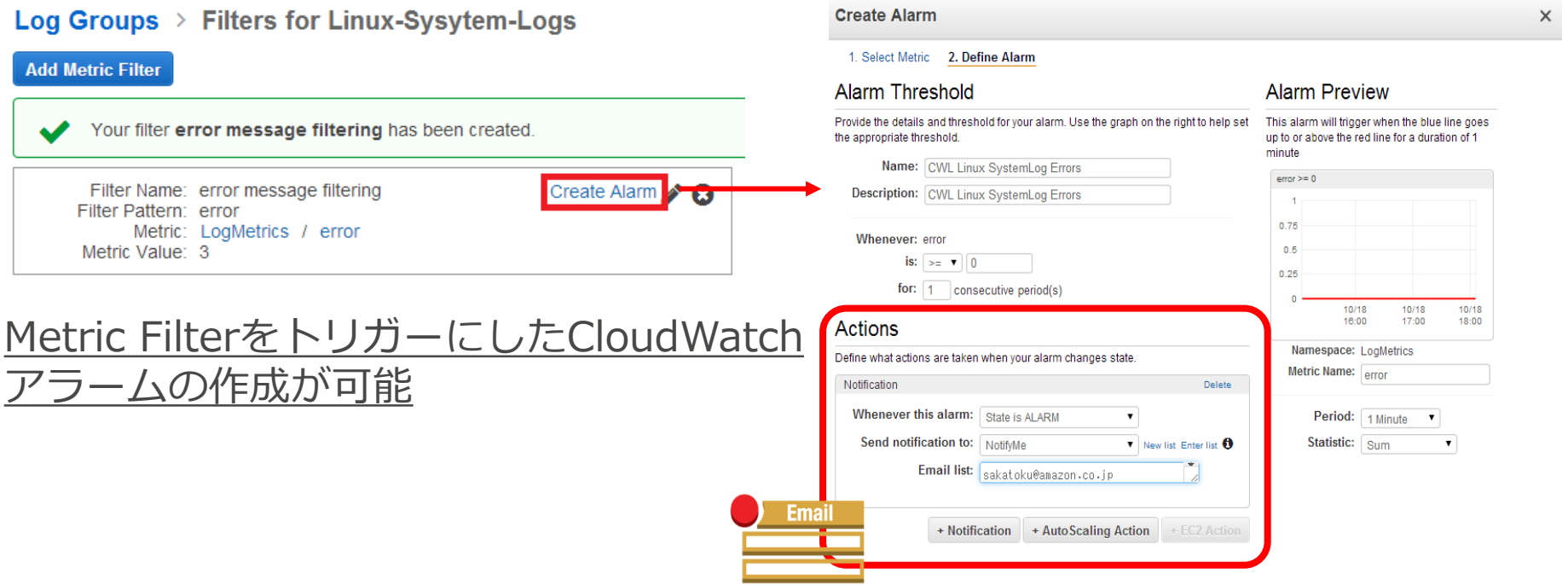


“error”という文字列を監視

“error”という文字列のエントリー回数

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

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

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

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

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

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

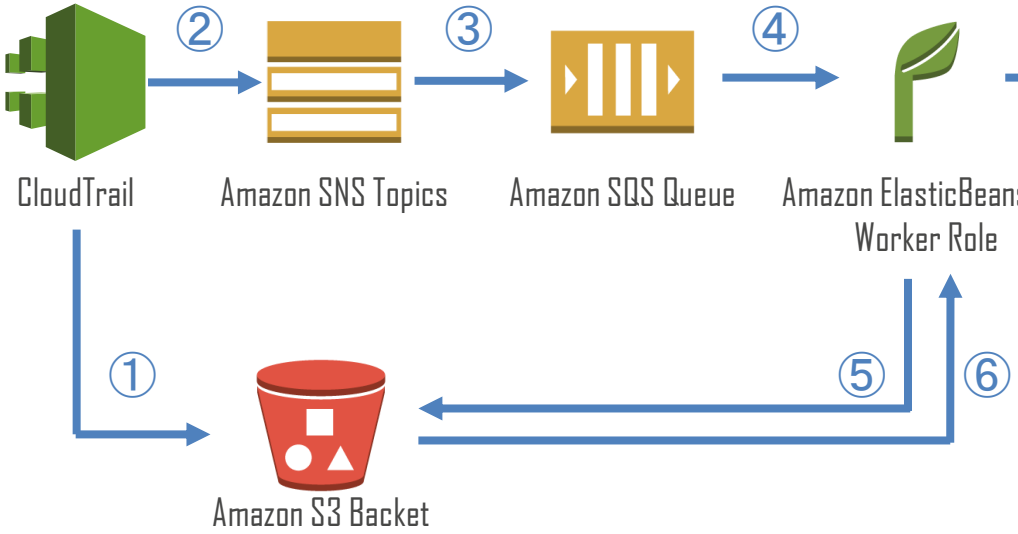
Filter Name: CloudWatchAlarm-CloudTrail-APIActivity-EC2LargeInstanceChangesMetricFilter-V2DOYX90SA20 — Create Alarm
Filter Pattern: { (($.eventName = RunInstances) || ($.eventName = RebootInstances) || ($.eventName = StartInstances) || ($.eventName = StopInstances) || ($.eventName = TerminateInstances))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

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

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.

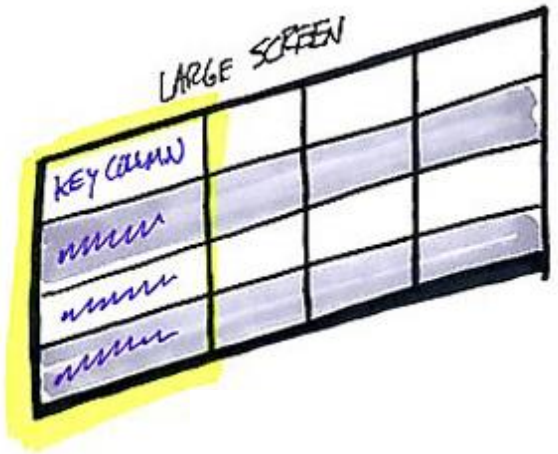
https://medium.com/aws-activate-startup-blog/searching-cloudtrail-logs-easily-with-amazon-cloudsearch-2d716e23efee

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



CloudTrail JSON “userIdentity”


```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "creationDate": "  20131102T010628Z  ",
        "mfaAuthenticated": "false"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIDPPEZS35WEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
        "accountId": "123456789012",
        "userName": "RoleToBeAssumed"
      }
    }
}
```


CloudTrail JSON

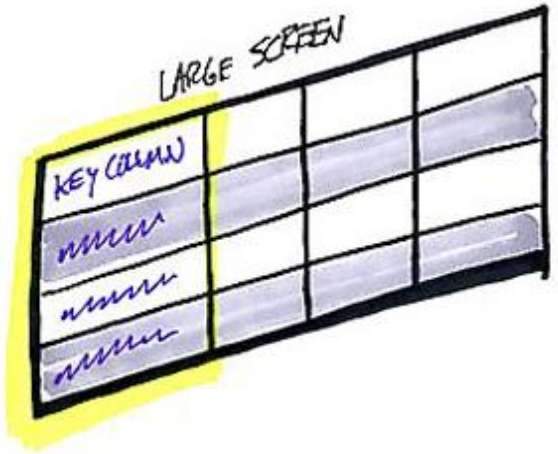
- Type
- arn
- accountID
- accessKeyId
- accountId
- userName

CloudTrail JSON to CloudSearch Table

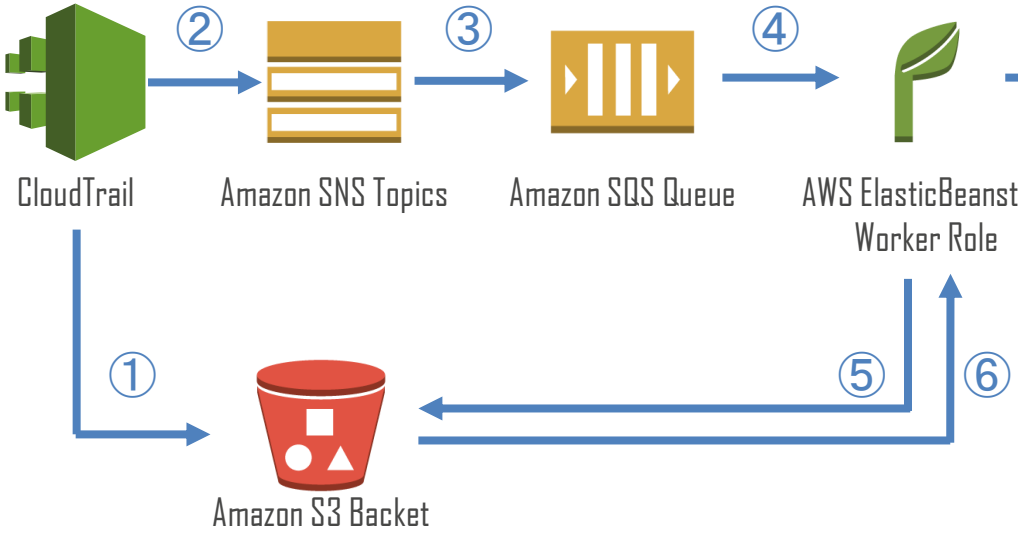
CloudTrail JSON

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

CloudSearch



Amazon CloudSearch, Amazon Elastic Beanstalk



Searching CloudTrail Logs Easily with Amazon CloudSearch

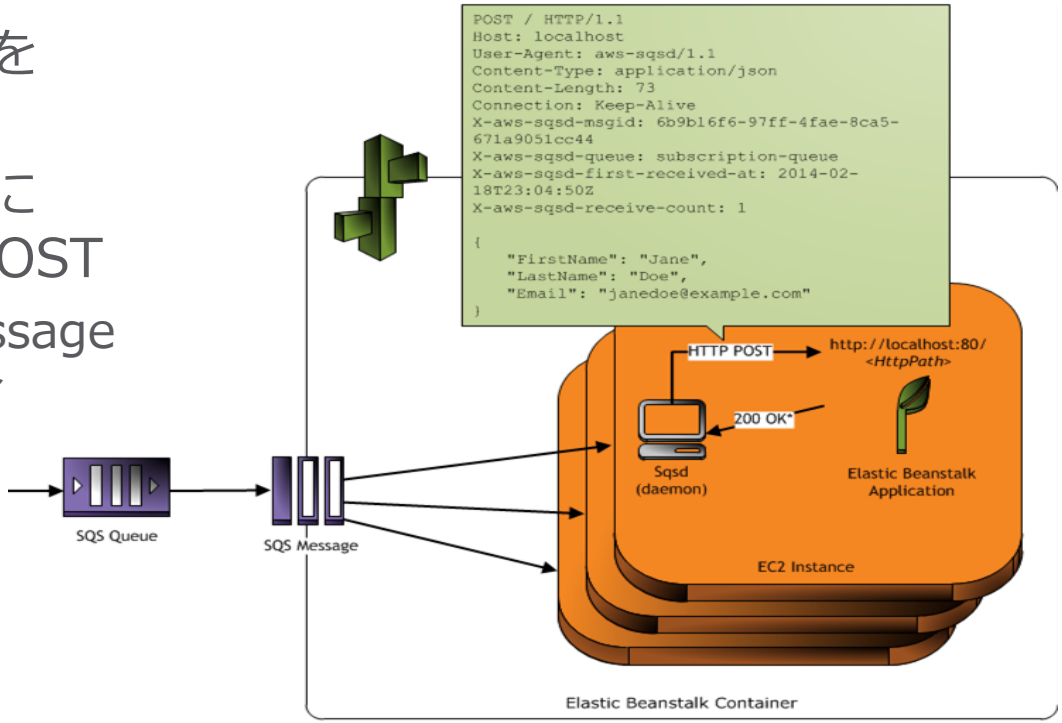
In addition to the flexibility AWS provides startups in creating and deleting application infrastructure, AWS CloudTrail provides a key security service with its detailed security audit logs. It records the API calls made in your AWS account and publishes the resulting log files to an Amazon S3 bucket 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

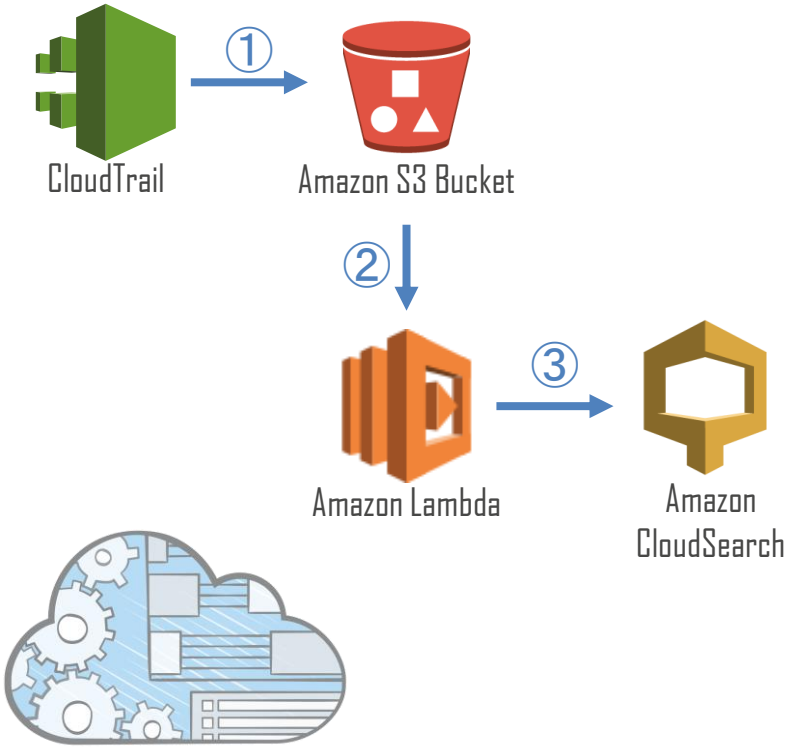
AWS Elastic Beanstalk Worker Tier

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

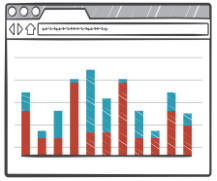
aws_region
- eu-west-1 (23)

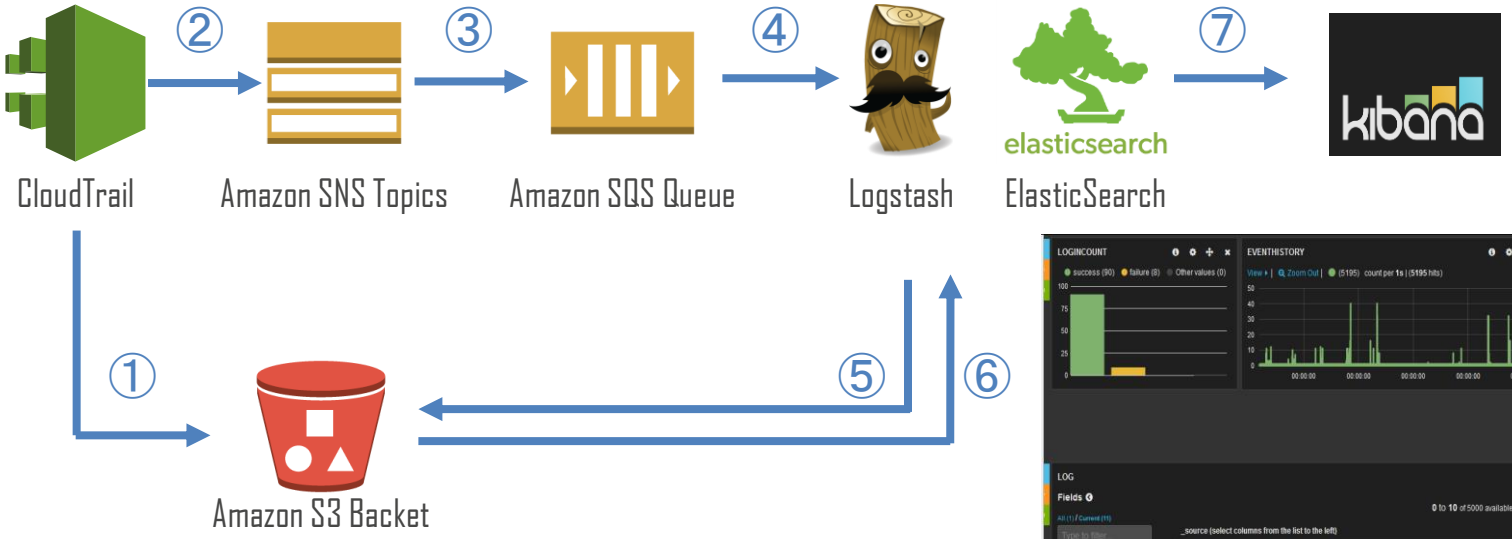
error_code

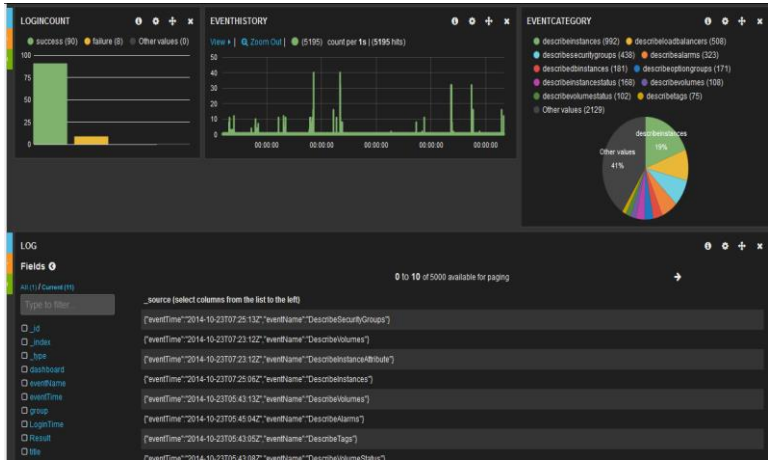
event_name
- SetQueueAttributes (13)
- CreateQueue (7)
- DeleteQueue (3)

source_ip_address
- 54.240.197.233 (6)
- 80.12.59.193 (5)
- 54.240.197.234 (4)

ElasticSearch, Kibana

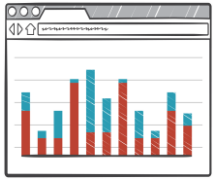


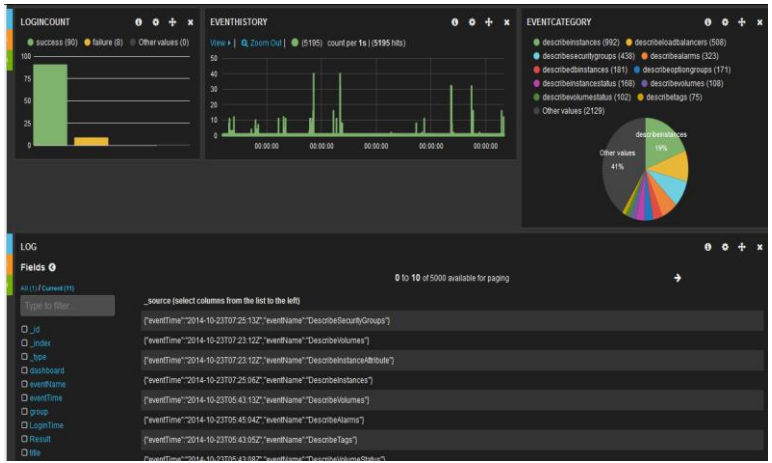




https://blogs.amazon.com/aws_solutions/archive/2014/10/processing-cloudtrail-logs-into-logstashelasticsearchkibana.html

ElasticSearch, Kibana, Amazon Lambda



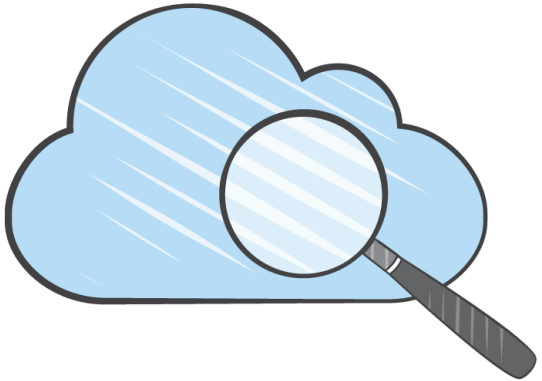


https://blogs.amazon.com/aws_solutions/archive/2014/10/processing-cloudtrail-logs-into-logstashelasticsearchkibana.html

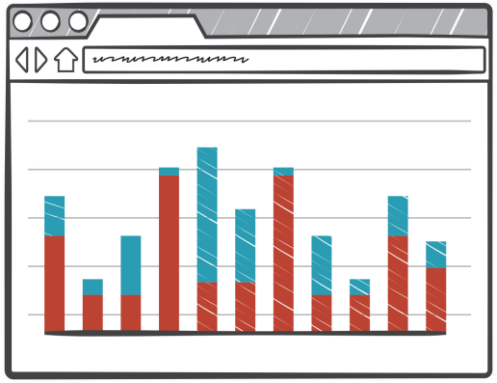
用途に応じた使い分けが必要

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。

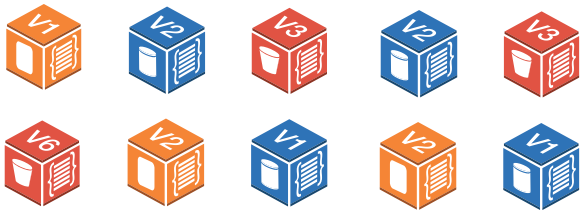
AWS Config

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

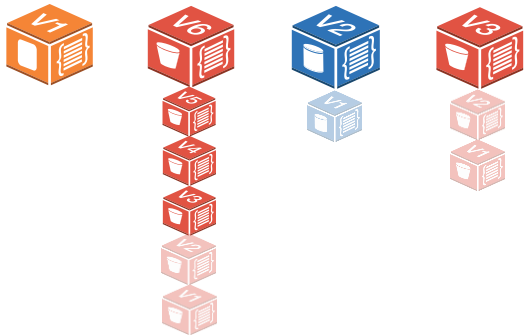
- あるポイントでのコンフィグレーション アイテムの集合
- 自動で定期的あるいは変更トリガで作成され、Amazon S3にエクスポートされる



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

Configuration Snapshot

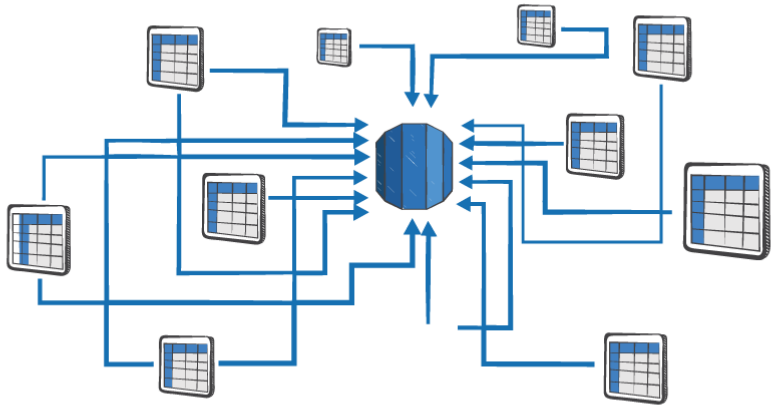
- 設定履歴は、任意の期間における各リソースタイプの構成要素の集合
- リソースの設定履歴を、指定したS3バケットに保存



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

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

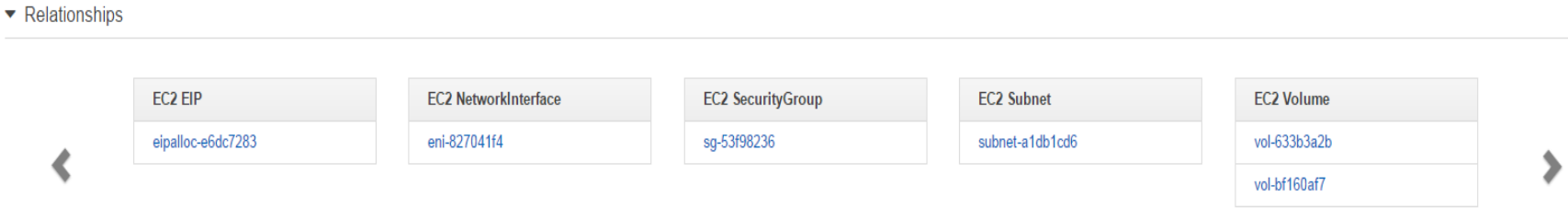
Relationship Changes (1)

ボリュームの追加

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

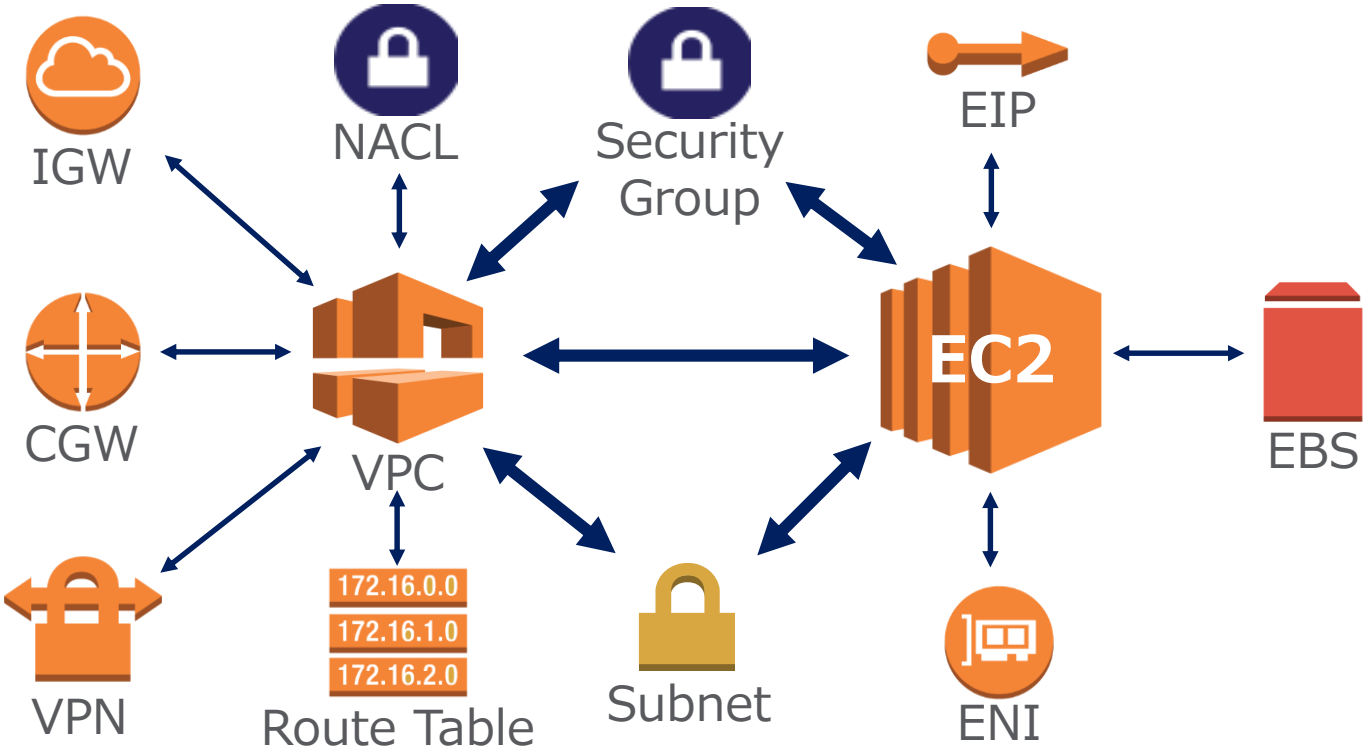
リソース情報（リレーション）

変更前



変更後

AWS Config リレーションシップ



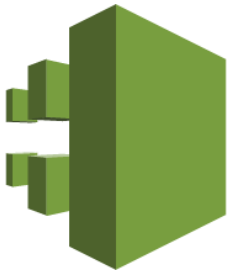
サポートされるAWSリソース

- 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...

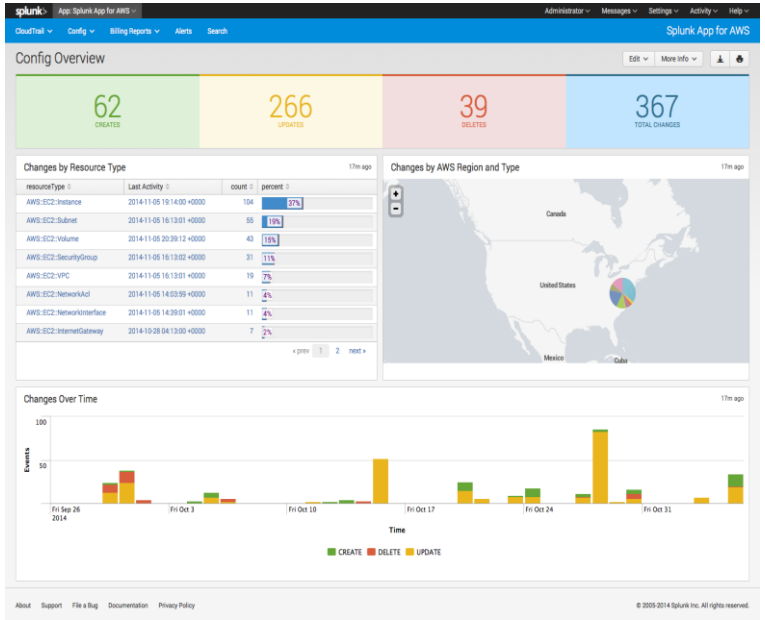
Amazon EBS
Volumes

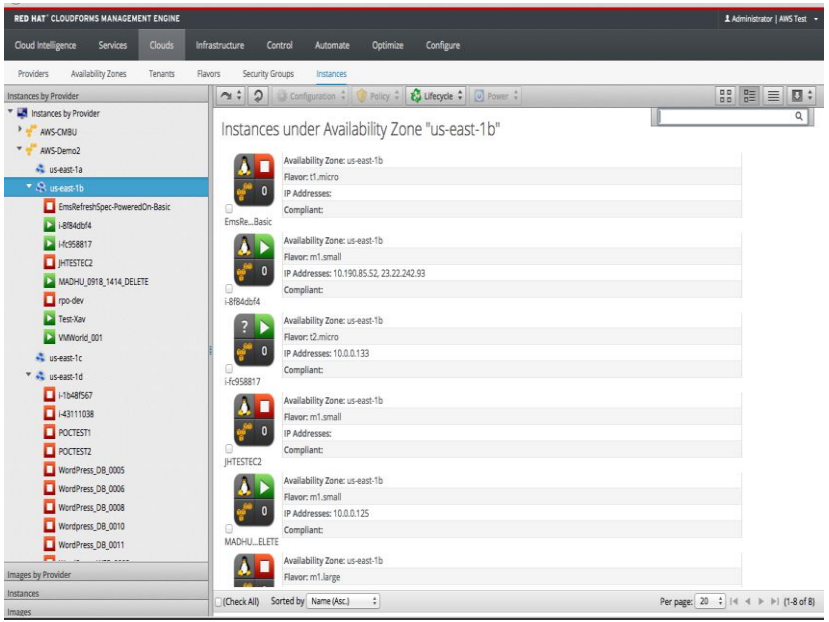


AWS CloudTrail

AWS Config パートナー

splunk>

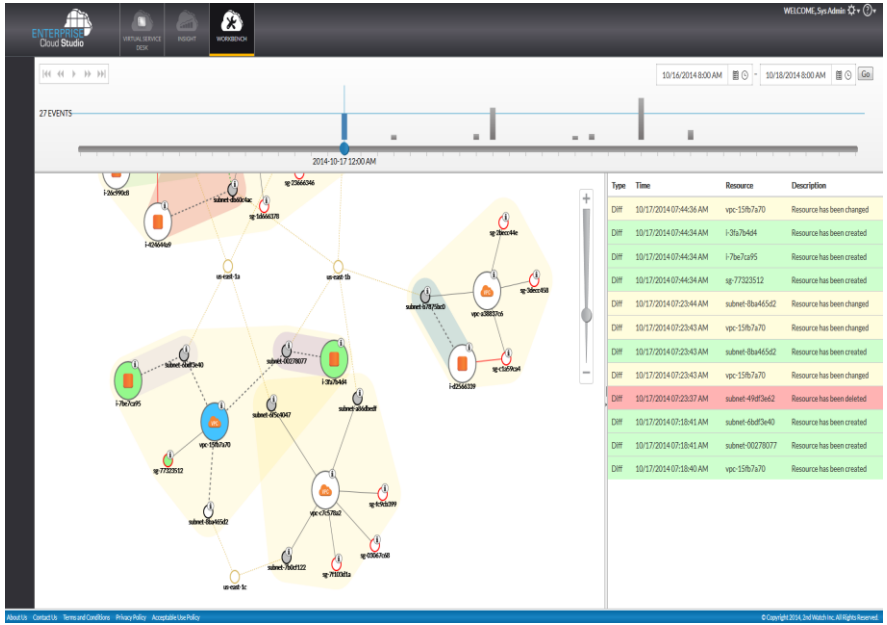


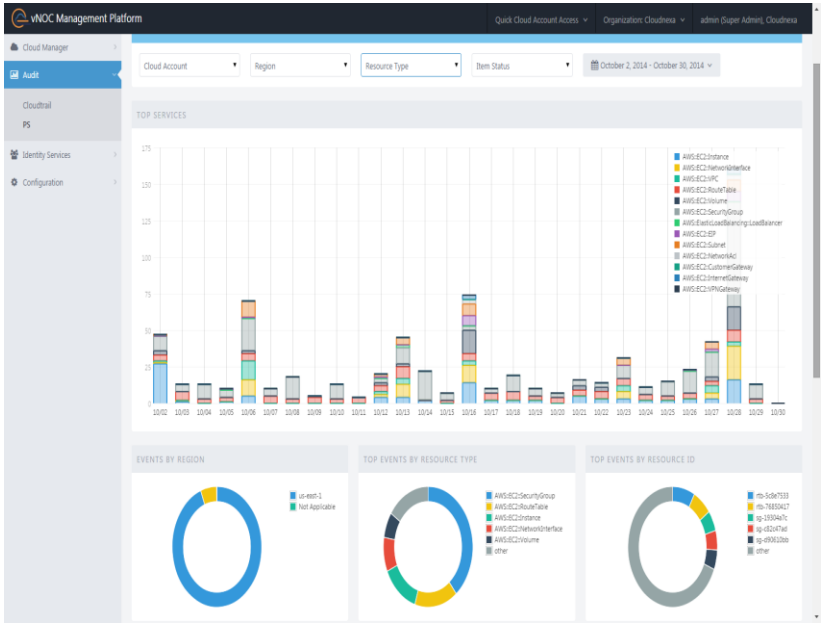


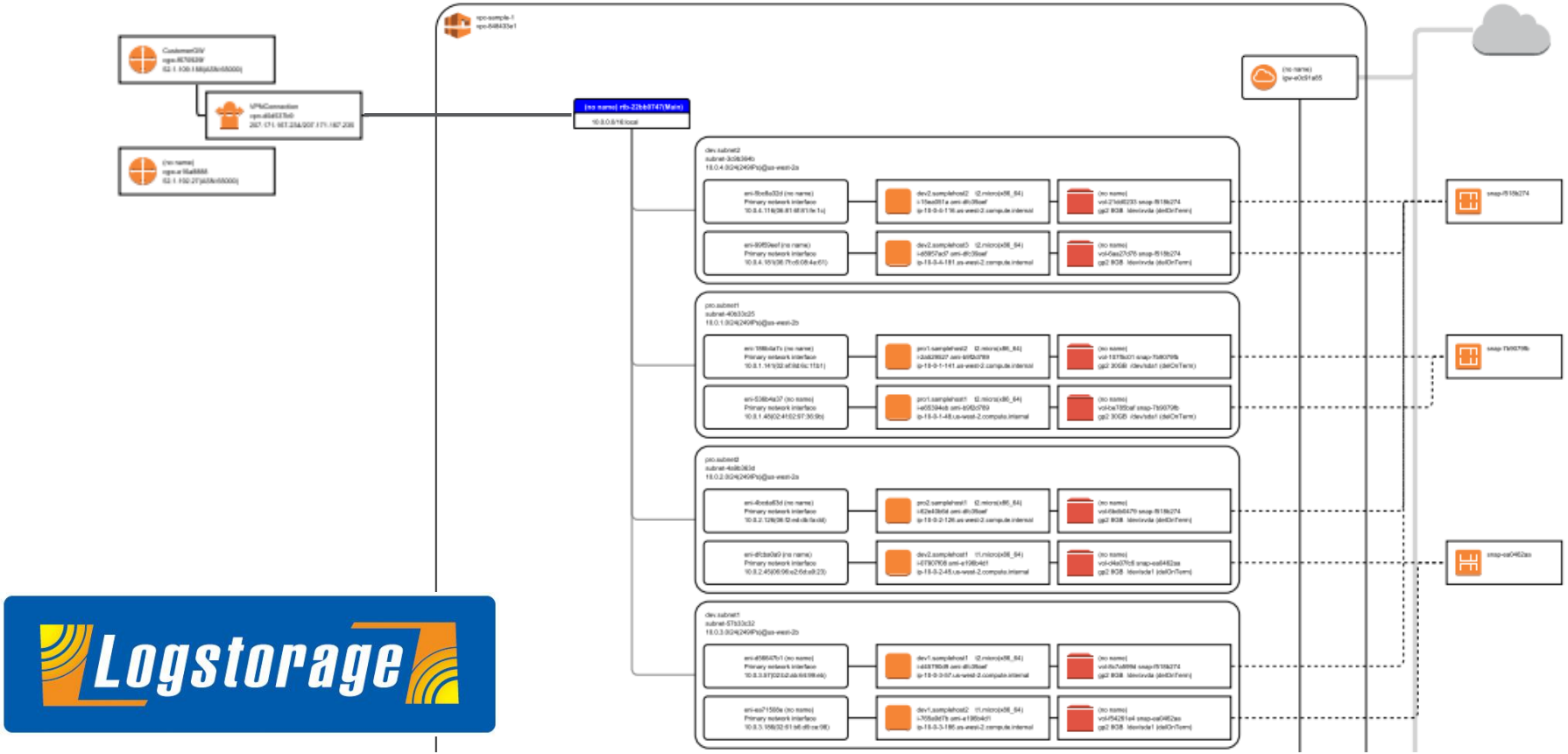
AWS Config パートナー

2ND WATCH

CLOUDNEXA







Logstorage

amazon web services

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


AWS
Services
Edit
Noritaka Sekiyama
N. California
Turn on CloudTrail
Learn more
Documentation
Forums
FAQs
Create a new S3 bucket?
Yes
No
S3 bucket*
Advanced
Required field
Cancel
Turn On
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
とりあえずON

Q. CloudTrailの料金はど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

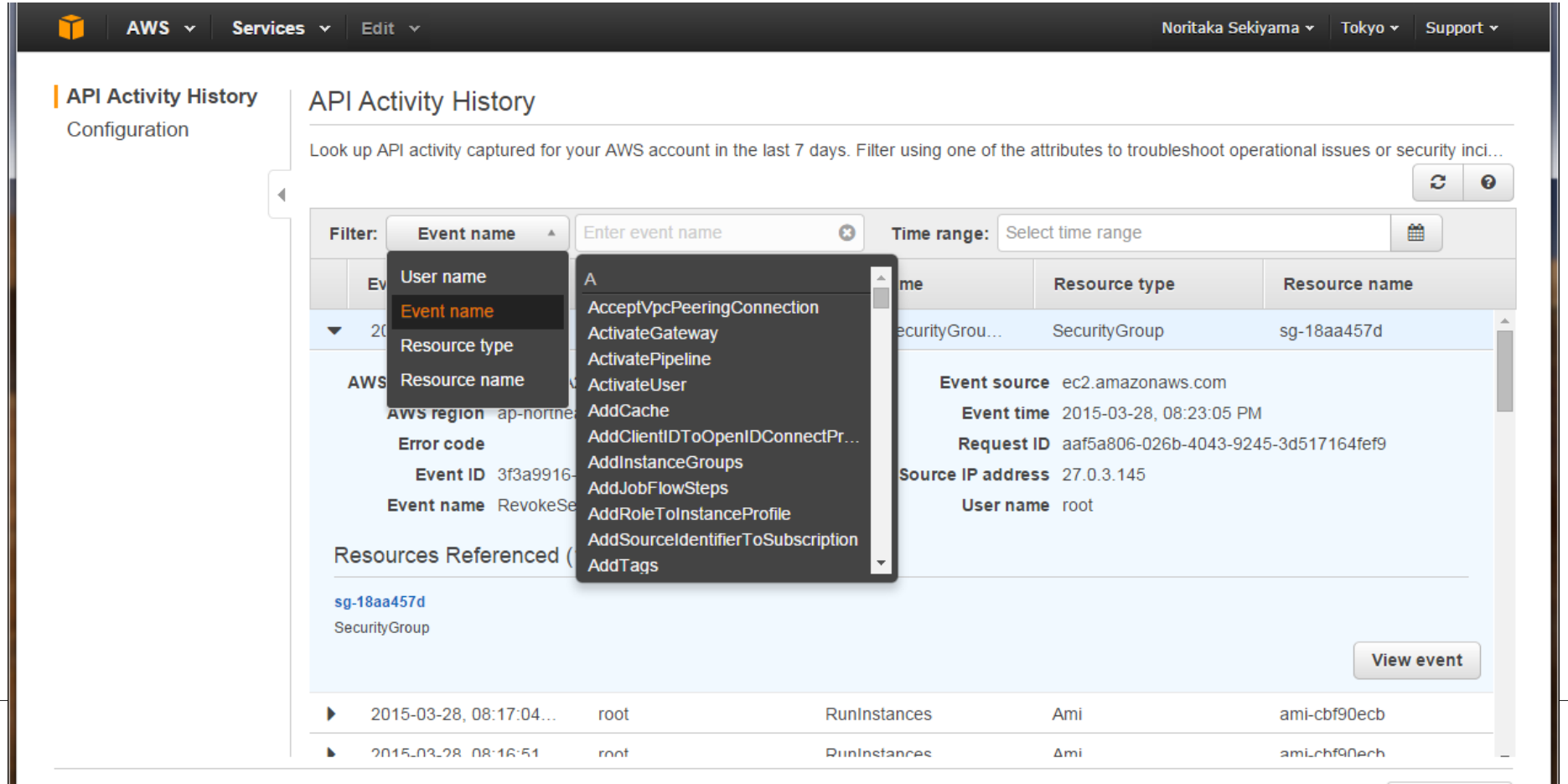
CloudTrailのログの探し方

- 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



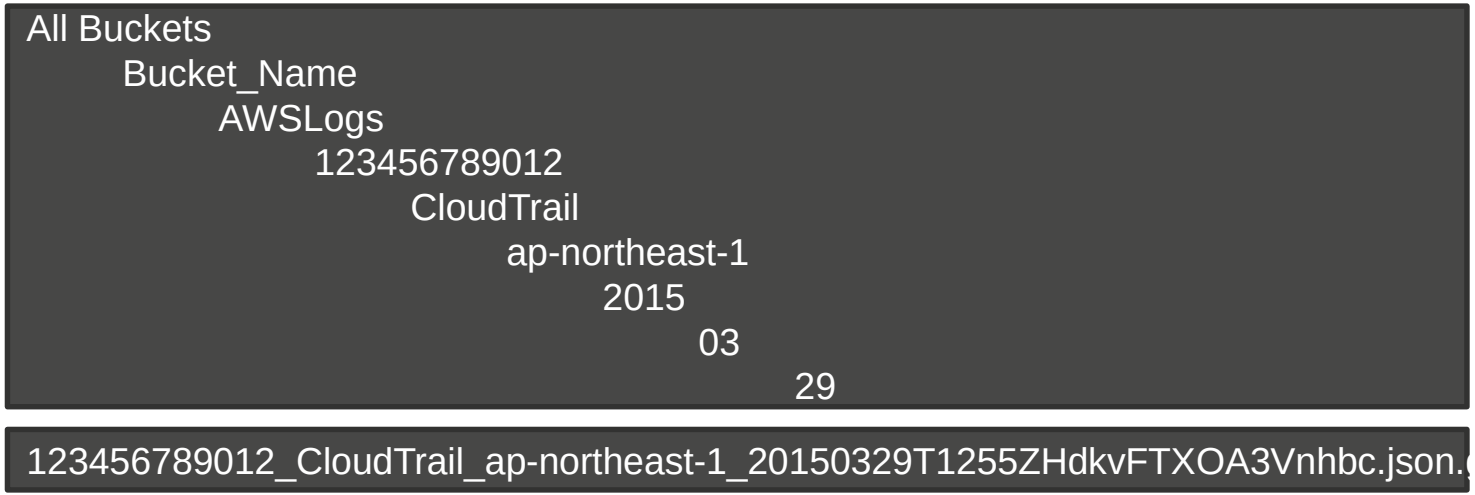
CloudTrail look up – AWS CLI

```
$ 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



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

トラブルシュート時の流れ

- 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
  - ご対応
    - 対応策の実施
    - 切りわけ再実施
- 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.

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 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。