

Deep Dive : résoudre les problèmes opérationnels et de sécurité avec AWS CloudTrail

Julien Simon

Principal Technical Evangelist, AWS

julsimon@amazon.fr

@julsimon

Agenda

Présentation de CloudTrail

Mise en route

Rechercher des événements



Recevoir des notifications lors de l'appel d'une API

Solutions partenaires

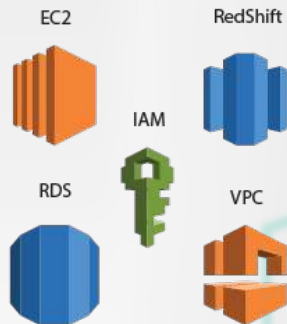
Questions et réponses

Présentation de CloudTrail

CloudTrail



Les clients effectuent des appels d'API...



Sur un ensemble de services de plus en plus vaste dans le monde entier...



CloudTrail enregistre continuellement nos appels d'API...

Utilisateur	Action	Horaires
Tim	Date de création	13 h 30
Sue	Supprimé	14 h 40
Kat	Date de création	15 h 30

Et transmet les fichiers journaux aux clients

CloudTrail prend en charge la plus grande partie des services AWS.

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-supported-services.html>

Cas d'utilisation de CloudTrail

- Analyse de **sécurité**
 - Utilisez les fichiers journaux dans vos solutions d'analyse et de gestion afin de procéder à l'analyse du comportement des utilisateurs.
- Suivi des **modifications** apportées aux ressources AWS
 - Suivez la création, la modification et la suppression de ressources AWS telles que les instances Amazon EC2, les groupes de sécurité Amazon VPC et les volumes Amazon EBS
- Résolution des **problèmes** opérationnels
 - Identifiez rapidement les dernières modifications apportées aux ressources présentes dans votre environnement
- Aide à la **conformité**
 - Il est plus simple de prouver la conformité lorsque l'on dispose de toutes les informations
 - CloudTrail est certifié PCI DSS, ISO 9001 / 27001 / 27017 / 27018, SOC 1 / 2 / 3

Que contient un événement CloudTrail ?

Qui a effectué l'appel de l'API ?

Quand l'appel de l'API a-t-il été effectué ?

Quelle était la nature de l'appel d'API ?

Quelles ressources ont été utilisées dans le cadre de l'appel d'API ?

A partir d'où l'appel d'API a-t-il été effectué et vers quelle destination ?

En règle générale, les fichiers journaux contenant des événements sont transmis à S3 **en moins de 10 minutes**.

Ces fichiers peuvent être **chiffrés** à l'aide de clés gérées par KMS.

Disponibilité et tarification

- Disponible dans **toutes** les régions AWS, y compris GovCloud et les régions chinoises
- CloudTrail est très économique
 - *Management Events*: **\$2.00 / 100,000 appels**
 - *Data Events (S3)* : **\$0.10 / 100,000 appels**
 - Stockage : tarif S3 habituel.

Mise en route

Activer CloudTrail dans toutes les régions

Nous vous recommandons de le faire **dès que possible**.

L'historique d'appels est une ressource **très précieuse** !

CloudTrail est la boîte noire de votre plate-forme :
utilisez-la sans attendre.

Activer CloudTrail dans toutes les régions

L'opération peut se faire très simplement dans la [console CloudTrail](#).

Voici également un script pour le faire [programmatiquement](#) :

```
CLOUDTRAIL_S3_BUCKET="yourbucket"
PROFILE="yourprofile"
REGION_FOR_GLOBAL_EVENTS="us-east-1"
regionlist=$(aws ec2 describe-regions --query Regions[*].RegionName --output text))
for region in ${regionlist[@]}
do
  if
    [ $region = $REGION_FOR_GLOBAL_EVENTS ]
  then
    aws --profile $PROFILE --region $region cloudtrail create-trail --name $region --s3-bucket-name
    $CLOUDTRAIL_S3_BUCKET --include-global-service-events --output table
    aws --profile $PROFILE --region $region cloudtrail start-logging --name $region --output table
  else
    aws --profile $PROFILE --region $region cloudtrail create-trail --name $region --s3-bucket-name
    $CLOUDTRAIL_S3_BUCKET --no-include-global-service-events --output table
```



Démonstration : créer un nouveau *trail* avec la console CloudTrail

Recherche dans CloudTrail



Recherche d'événements CloudTrail dans la console

- Diagnostiquez les problèmes opérationnels et de sécurité liés à votre compte AWS
- Recherchez les événements
 - Création, suppression et modification des ressources AWS
 - 7 derniers jours
- Filtrez les événements
 - Plage de temps
 - Nom utilisateur
 - Nom de la ressource
 - Type de ressource
 - Nom de l'événement
 - ID d'événement



Démonstration :



rechercher des événements avec la console CloudTrail



Recherche d'événements CloudTrail dans la console

API activity history

The following list includes the last 7 days of API activity for [supported services](#). The list only includes API activity for **create**, **modify**, and **delete** API calls. For read-only API activity, go to your Amazon S3 bucket or CloudWatch Logs.

You can filter the list using the available attributes, and you can choose an event to see more detail about the event. [Learn more](#).



Filter: Resource type Bucket  Time range: Select time range 					
	Event time	User name	Event name	Resource type	Resource name
▶	2016-12-14, 04:53:14 PM	julien	PutBucketLifecycle	S3 Bucket	cloudtrail-jsimon-allregions
▶	2016-12-14, 04:52:13 PM	julien	PutBucketVersioning	S3 Bucket	cloudtrail-jsimon-allregions
▶	2016-12-14, 04:51:33 PM	julien	DeleteBucket	S3 Bucket	elasticbeanstalk-eu-west-1-613904...
▶	2016-12-12, 11:06:18 AM	julien	CreateTrail	S3 Bucket and 1 more	cloudtrail-jsimon-allregions and 2 m...
▶	2016-12-12, 11:06:17 AM	julien	PutBucketPolicy	S3 Bucket	cloudtrail-jsimon-allregions
▶	2016-12-12, 11:06:16 AM	julien	CreateBucket	S3 Bucket	cloudtrail-jsimon-allregions
No more events					

Rechercher des événements avec la ligne de commande

- Tous les événements des 7 derniers jours

```
aws cloudtrail lookup-events
```

- Tous les événements pour lesquels le nom d'utilisateur est 'root'

```
aws cloudtrail lookup-events --lookup-attributes  
AttributeKey=Username,AttributeValue=root
```

- Tous les événements portant sur une instance EC2

```
aws cloudtrail lookup-events --lookup-attributes  
AttributeKey=ResourceType,AttributeValue=AWS::EC2::Instance
```


Recevoir des notifications
lors de l'appel
d'une API spécifique

Recevoir des notifications

Pourquoi ?

- Surveiller les tendances éventuelles dans les événements CloudTrail
- Agir immédiatement lorsqu'un événement spécifique a lieu

Que devez-vous faire ?

- Configurer les événements CloudTrail de façon à ce qu'ils soient consignés dans **CloudWatch Logs**
 - Coût de CloudWatch Logs : \$0.50 / Go ingéré + stockage S3
- Configurer des **alarmes CloudWatch**
- Note : il est également possible d'intégrer CloudTrail avec CloudWatch Events, pour réagir à des appels d'API (par exemple avec Lambda)

Quels événements dois-je surveiller ?

Les événements liés à la **sécurité** et au **réseau**, par exemple :

1. Création, suppression et modification des **groupes de sécurité** et des **VPC**
2. Modifications apportées aux **stratégies IAM**
3. **Echecs de connexion** à la console
4. Appels d'API ayant entraîné des **échecs d'autorisation**

Les événements liés à des **ressources spécifiques**, par exemple :

5. Lancement / arrêt d'instances EC2, RDS, EMR, etc.
6. Création des instances EC2 les plus coûteuses : 4xlarge, 8xlarge, etc.

Configuration d'alarmes CloudWatch pour CloudTrail

- Pour commencer, utilisez le modèle **CloudFormation** qui comporte **10 alarmes prédéfinies**, notamment les exemples mentionnés précédemment.
- Créez ces 10 alarmes CloudWatch **en moins de 5 minutes** !
- Recevez des **notifications par e-mail** lorsque ces événements ont lieu dans votre compte AWS



Ajouter une alarme CloudWatch pour CloudTrail

1. Configurez l'export des événements CloudTrail vers CloudWatch Logs.
2. Créez un nouveau filtre de métrique, en utilisant la syntaxe de CloudWatch.
3. Créez une nouvelle alarme CloudWatch basée sur la nouvelle métrique.
4. Définissez une notification associée à l'alarme.

Démonstration :



ajouter une notification

Exporter les événements CloudTrail vers CloudWatch Logs

Console CloudTrail

▼ CloudWatch Logs (Optional)



Log group CloudTrail-all-
regions/DefaultLogGroup

✔ **Last log file delivered** 12-14-2016, 6:15 pm

IAM role CloudTrail_CloudWatchLo
gs_Role

Create CloudWatch Alarms for Security and Network related API activity using CloudFormation template.

Créer un filtre de métrique dans CloudWatch Logs

Console CloudWatch Logs

Log Groups > Filters for CloudTrail-all-regions/Defa...

Add Metric Filter

Filter Name: eventName-DeleteBucket
Filter Pattern: { \$.eventName = "DeleteBucket" }
Metric: [LogMetrics](#) / [metric-DeleteBucket](#)
Metric Value: 1

Create Alarm



Alarm: [Delete-Bucket-Alarm](#)



Créer une alarme basée sur la métrique

Console CloudWatch

Alarm Threshold

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

Name: Delete-Bucket-Alarm

Description: send email when an S3 Bucket is deleted

Whenever: metric-DeleteBucket

is: \geq 0

for: 1 consecutive period(s)

Actions

Define what actions are taken when your alarm changes state.

Notification

Delete

Whenever this alarm: State is ALARM

Send notification to: julien-AWS [New list](#) [Enter list](#) ⓘ

Email list: julsimon@amazon.fr

+ 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

Delete-Bucket-Alarm

metric-DeleteBucket \geq 0



Namespace: LogMetrics

Metric Name: metric-DeleteBucket

Period: 1 Minute

Statistic: ☒ Standard ☐ Custom

Sum

Effectuer l'action qui déclenche l'alarme

```
➔ ~ aws s3 mb s3://jsimon-cloudtrail-testbucket  
make_bucket: jsimon-cloudtrail-testbucket  
➔ ~ aws s3 rb s3://jsimon-cloudtrail-testbucket  
remove_bucket: jsimon-cloudtrail-testbucket
```

Visualiser l'action dans CloudTrail

Filter: <input type="button" value="Select attribute"/> <input type="text" value="Enter lookup value"/>					
Time range: <input type="text" value="Select time range"/>					
	Event time	User name	Event name	Resource type	Resource name
▶	2016-12-14, 06:02:19 PM	julien	DeleteBucket	S3 Bucket	jsimon-cloudtrail-testbu...
▶	2016-12-14, 06:02:09 PM	julien	CreateBucket	S3 Bucket	jsimon-cloudtrail-testbu...

Déclenchement de l'alarme dans CloudWatch

[Create Alarm](#) [Modify](#) [Copy](#) [Delete](#)

Filter: **State is ALARM** 1 to 1 of 1 alarms

State	Name	Threshold	Config Status
<input checked="" type="checkbox"/> ALARM	Delete-Bucket-Alarm	metric-DeleteBucket > 0 for 1 minute	

1 Alarm selected

Alarm: Delete-Bucket-Alarm

[Details](#) [History](#)

State Details: State changed to ALARM at 2016/12/14. Reason: Threshold Crossed: 1 datapoint (1.0) was greater than or equal to the threshold (0.0).

Description: send email when an S3 Bucket is deleted

Threshold: metric-DeleteBucket > 0 for 1 minute

Actions: In ALARM: • Send message to topic "julien-AWS" (julsimon@amazon.fr)

Namespace: LogMetrics

Metric Name: metric-DeleteBucket

Dimensions:

Statistic: Sum

Period: 1 minute

Delete-Bucket-Alarm
metric-DeleteBucket >= 0


Time	Value
12/14 18:00	1.0

Réception de l'email de notification

ALARM: "Delete-Bucket-Alarm" in EU - Ireland

☐ AWS Notifications

Sent: mercredi 14 décembre 2016 18:08

To:  Simon, Julien

You are receiving this email because your Amazon CloudWatch Alarm "Delete-Bucket-Alarm" in the EU - Ireland region has entered the ALARM state, because "Threshold Crossed: 1 datapoint (1.0) was greater than or equal to the threshold (0.0)." at "Wednesday 14 December, 2016 17:08:21 UTC".

View this alarm in the AWS Management Console:

<https://console.aws.amazon.com/cloudwatch/home?region=eu-west-1#s=Alarms&alarm=Delete-Bucket-Alarm>

Alarm Details:

- Name:	Delete-Bucket-Alarm
- Description:	send email when an S3 Bucket is deleted
- State Change:	INSUFFICIENT_DATA -> ALARM
- Reason for State Change:	Threshold Crossed: 1 datapoint (1.0) was greater than or equal to the threshold (0.0).
- Timestamp:	Wednesday 14 December, 2016 17:08:21 UTC
- AWS Account:	[REDACTED]

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 0.0 for 60 seconds.

Monitored Metric:

- MetricNamespace:	LogMetrics
- MetricName:	metric-DeleteBucket
- Dimensions:	
- Period:	60 seconds
- Statistic:	Sum
- Unit:	not specified

State Change Actions:

- OK:
- ALARM: [arn:aws:sns:eu-west-1:[REDACTED]:julien-AWS]
- INSUFFICIENT_DATA:

Créer une notification depuis CloudWatch Events

Console CloudWatch Events

Étape 1 : Créer une règle

Créez des règles pour automatiser les actions dans votre environnement AWS.

Sélecteur d'événements

Créez un modèle pour sélectionner les événements qui seront traités par vos cibles.

Appel d'API AWS

Nom du service

S3

Operation Type

Bucket Level Operations

☐ Toute opération

☒ Opération(s) spécifique(s)

x DeleteBucket

► Afficher les options avancées

* Obligatoire

Cibles

Sélectionnez les cibles qui recevront les événements correspondant à la règle que vous avez définie.

Rubrique SNS

Rubrique*

julien-SMS

► Configurer l'entrée

+ Ajouter une cible*

Annuler

Configurer les détails

Solutions partenaires

Partenaires technologiques intégrés à CloudTrail

Gestion et analyse de logs



GRAYLOG2

logentries

loggly

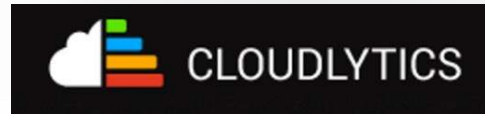
splunk>

sumologic

Partenaires consulting



Cognizant



Ressources complémentaires

Livres blancs AWS

<https://aws.amazon.com/whitepapers/auditing-security-checklist-for-use-of-aws/>

<https://aws.amazon.com/blogs/security/new-whitepaper-security-at-scale-logging-in-aws/>

<https://aws.amazon.com/whitepapers/overview-of-risk-and-compliance/>

AWS re:Invent 2016: Automated Governance of Your AWS Resources (DEV302)

<https://www.youtube.com/watch?v=2P2I7HlrFtA>

AWS re:Invent 2016: Scaling Security Operations and Automating Governance (SAC315)

https://www.youtube.com/watch?v=_yfeCvqHdNg

Slides et vidéos des webinaires : <http://bit.ly/2hKPihB>

Merci !

Julien Simon

Principal Technical Evangelist, AWS

julsimon@amazon.fr

@julsimon

Lundi

- Bonnes pratiques d'authentification avec AWS IAM
- Chiffrez vos données avec AWS

Mardi

- Fireside chat avec Matthieu Bouthors et Julien Simon
- Re:Invent update 1

Mercredi

- Deep dive : Amazon Virtual Private Cloud
- Bonnes pratiques anti-DDoS

Jeudi

- Re:Invent update 2
- Gérez les incidents de sécurité avec AWS CloudTrail

Vendredi

- Automatisez vos audits de sécurité avec Amazon Inspector
- Bonnes pratiques de sécurité sur AWS