COLOMBIA POTENCIA DE LA VIDA

TIC

LECCIÓN 2: CÓMO SE CAPTURAN Y RECOPILAN LOS REGISTROS

TALENTO TECH | AZ PROYECTOS EDUCATIVOS | UTP Universidad Tecnológica de Pereira

AWS CLOUDTRAIL

- Lo ayuda a habilitar la gobernanza y el cumplimiento, así como la auditoría operativa y de riesgos de su cuenta de AWS.

- Registra las acciones realizadas por un usuario, rol o servicio de AWS como eventos.

- Brinda visibilidad de los eventos en la consola de CloudTrail.

- Se puede utilizar para ver, buscar, descargar, archivar, analizar y responder a la actividad de la cuenta en toda su infraestructura de AWS.

AWS CloudTrail es un servicio de AWS que le permite habilitar la gobernanza, el cumplimiento y la auditoría operativa y de riesgo en su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail. Los eventos incluyen acciones realizadas en la consola de administración de AWS, la Command Line Interface de AWS (AWS CLI) y los kits de desarrollo de software (SDK) y las API de AWS. Puede ver, buscar, descargar, archivar, analizar y responder a estos eventos registrados en la consola de CloudTrail.

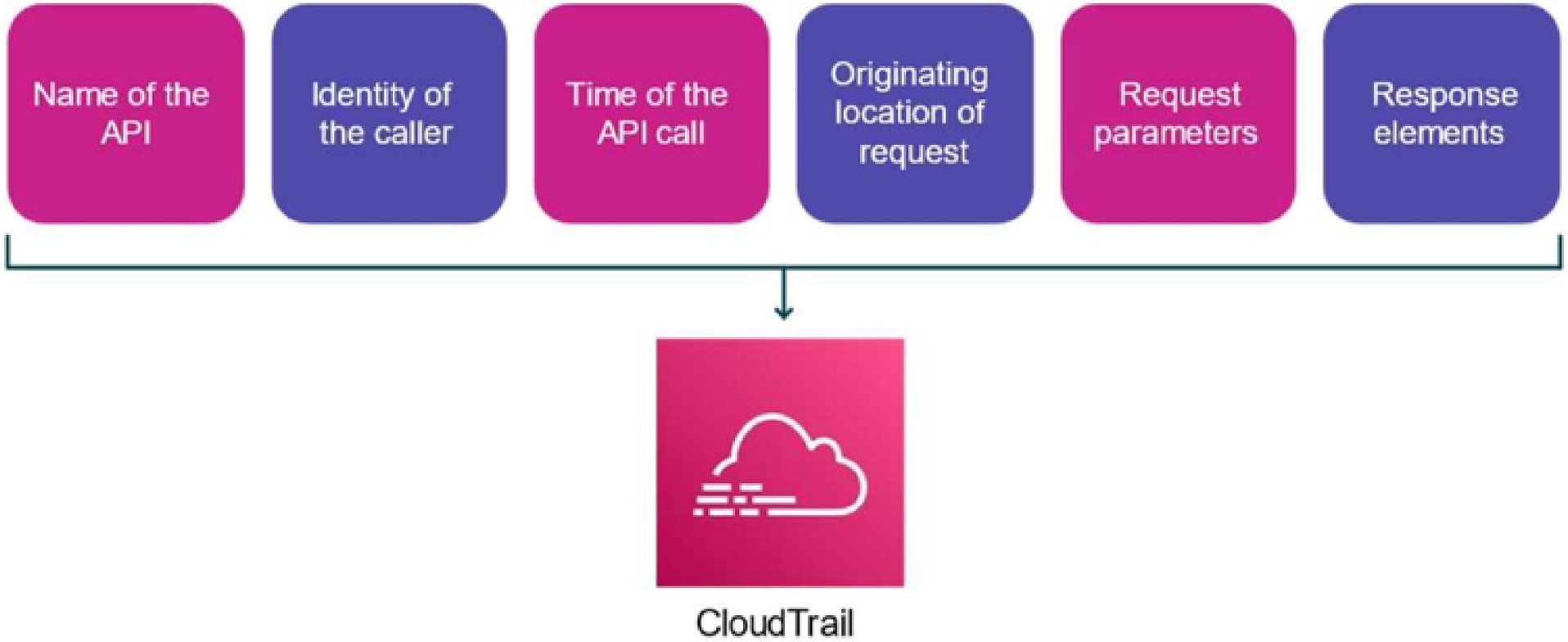
Puede integrar CloudTrail en las aplicaciones mediante la API, automatizar la creación de pistas para su organización, verificar el estado de las pistas que crea y controlar cómo ven los usuarios los eventos de CloudTrail.

Para más información, consulte AWS CloudTrail en https://aws.amazon.com/cloudtrail

INFORMACIÓN PERTINENTE PARA LA SEGURIDAD DE LA API

AWS CloudTrail es un servicio de AWS que le permite habilitar la gobernanza, el cumplimiento y la auditoría operativa y de riesgo en su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail. Los eventos incluyen acciones realizadas en la consola de administración de AWS, la Command Line Interface de AWS (AWS CLI) y los kits de desarrollo de software (SDK) y las API de AWS. Puede ver, buscar, descargar, archivar, analizar y responder a estos eventos registrados en la consola de CloudTrail.

Puede utilizar el historial de llamadas API de AWS que produce CloudTrail para realizar un seguimiento de los cambios en los recursos de AWS. Entre dichos cambios, se incluyen la creación, modificación y eliminación de recursos de AWS, como las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y los grupos de seguridad de Amazon VPC. En el ejemplo del archivo de registro de las siguientes diapositivas, se muestran acciones de una usuaria de AWS Identity and Access Management (IAM) llamada Jane. Jane usó el comando ec2-stop-instances en la AWS CLI para llamar a la acción StopInstances de Amazon EC2.


Name of the API
Identity of the caller
Time of the API call
Originating location of request
Request parameters
Response elements
CloudTrail

COLOMBIA POTENCIA DE LA VIDA

TIC

ACTIVIDAD DIRIGIDA POR EL EJECUTOR, LEERÁ UN ARCHIVO DE REGISTRO DE CLOUDTRAIL.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

LECTURA DE UN REGISTRO: IDENTIDAD DEL INTERMEDIARIO


```
{
  "Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::111122223333:user/Jane",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "Jane"
    },
```

COLOMBIA POTENCIA DE LA VIDA

TIC

Este archivo de registro se generó cuando alguien o algo realizaron algún tipo de acción.

Dedique un momento a revisar este fragmento de archivo de registro y luego responda las siguientes preguntas individualmente o en grupo:

1) ¿Sobre qué tipo de cuenta recopiló información el registro?

2) ¿Qué puede determinar a partir del elemento arn?

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

EN LA SIGUIENTE IMAGEN , PODRÁ VER CUÁNDO SE REALIZÓ ESTA LLAMADA.

Lectura de un registro: hora y origen de la solicitud


```
"eventTime": "2021-07-06T21:01:59Z",
"eventSource": "ec2.amazonaws.com",
"eventName": "StopInstances",
"awsRegion": "us-east-2",
"sourceIPAddress": "203.0.113.176",
"userAgent": "ec2-api-tools 1.6.12.2",
```

COLOMBIA POTENCIA DE LA VIDA

TIC

DEDIQUE UN MOMENTO A REVISAR ESTE FRAGMENTO DE ARCHIVO DE REGISTRO Y LUEGO RESPONDA LAS SIGUIENTES PREGUNTAS INDIVIDUALMENTE O EN GRUPO:

1) ¿Sobre qué le da información el campo eventSource?

2) En el campo eventName, ¿qué indica el valor StopInstances?

3) ¿Qué método se utilizó para realizar esta acción? (Consola, AWS CLI u otro) Ahora veamos qué estaba involucrado en esta solicitud.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

LECTURA DE UN REGISTRO: PARÁMETROS DE SOLICITUD Y ELEMENTOS DE RESPUESTA


```
"requestParameters": {
  "instancesSet": {
    "items": [{
      "instanceId": "i-ebeaf9e2" } ] },
  "force": false },
"responseElements": {
  "instancesSet": {
    "items": [{
      "instanceId": "i-ebeaf9e2",
      "currentState": {
        "code": 64,
        "name": "stopping" },
      "previousState": {
        "code": 16,
        "name": "running" } } ] },
```

COLOMBIA POTENCIA DE LA VIDA

TIC

DEDIQUE UN MOMENTO A REVISAR ESTE FRAGMENTO DE ARCHIVO DE REGISTRO Y LUEGO RESPONDA LAS SIGUIENTES PREGUNTAS INDIVIDUALMENTE O EN GRUPO:

1) En el campo instanceId ¿qué indica el valor i-ebeaf9e2?

2)¿Qué acción se realizó?

Si necesita realizar un seguimiento de los cambios en dichos recursos, responder preguntas sobre la actividad de los usuarios, demostrar el cumplimiento, solucionar problemas o realizar análisis de seguridad, puede usar CloudTrail para detectar amenazas y brindar seguridad.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

ESTOS SON ALGUNOS APRENDIZAJES CLAVE DE ESTA LECCIÓN DE ESTA UNIDAD

- **CloudTrail lo ayuda a habilitar la gobernanza, el cumplimiento y la auditoría de su cuenta de AWS.**
- **Las acciones realizadas por un usuario, rol o servicio de AWS se registran como eventos.**
- **CloudTrail registra información importante sobre cada llamada API, incluida la identidad del intermediario, la hora de la llamada API en UTC y el origen de la llamada.**