Module 31
CloudTrail

Overview

You used CloudWatch mainly to log Lambda activities (in a way like a log file). And the type of logging you did is for debugging and tracing that your code logic is progressing and behaving as you expect it to. If your cloud application has many resources in it (dozens of Lambdas, S3 buckets, queues, EventBridge buses and rules, etc.) it becomes difficult to assemble all activities. And some operations cannot be logged in CloudWatch. For example, assume a developer changed the role used with some Lambda function and this caused the application to fail (the developer could have used the AWS CLI or simply signed in to the AWS console and manually changed the role). How can we capture that such an operation took place, and by who?

Also many industries have regulations that require that applications have an audit trail. This simply means that the application needs to record who did what and what was changed. For example, here is a fictitious audit trail for a banking application (a banker with employee ID 667788 signed in to the banking application and changed the mailing preference of customer John Smith from standard mail to electronic mail).

User	Datetime	Event	Detail
667788	6/14/2022 7:58 AM	Login	
667788	6/14/2022 8:01 AM	OpenAccount	Opened account of customer 2134-9987645 (John Smith)
667788	6/14/2022 8:03 AM	AccountChange	Mail preference changed from standard to electronic

The above audit trail is useful because it allows us to know who did what and when. For example, we now know that the mailing preference of customer John Smith was changed by employee with ID 667788 on June 14 at 8:03 AM.

Your Cloud Application may need to have such audit trail capability, either to comply with some regulation, or for operational monitoring. And activities need to be captured irrespective of how they were done (via APIs, CLIs, or UIs). CloudTrail allows you to do that and consolidate activities into one place.

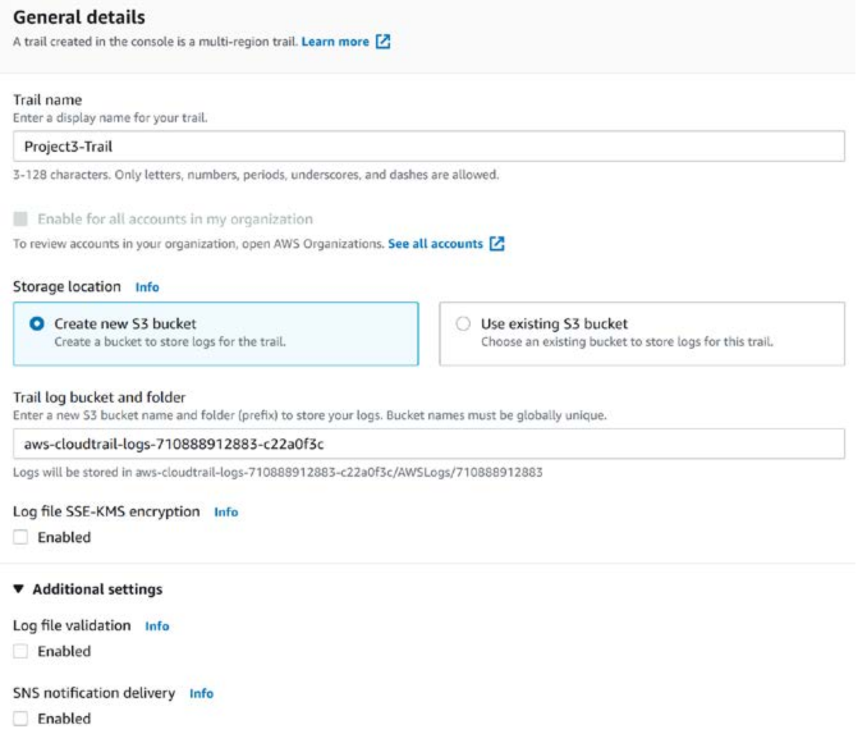
In this module, you will create a CloudTrail trail and use Project3 to test it

Create a Trail

1. Sign in to Canvas and to the AWS Console. Then go to the **CloudTrail** service.

2. From the left navigation bar, click the **Trails** link (you most likely don’t have any trail yet).

3. Click the **Create trail** button, and complete the screen as sown below:



General details

A trail created in the console is a multi-region trail. Learn more

Trail name

Enter a display name for your trail.

Project3-Trail

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

□ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. See all accounts

Storage location Info

● Create new S3 bucket
Create a bucket to store logs for the trail.

○ Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

aws-cloudtrail-logs-710888912883-c22a0f3c

Logs will be stored in aws-cloudtrail-logs-710888912883-c22a0f3c/AWSLogs/710888912883

Log file SSE-KMS encryption Info

□ Enabled

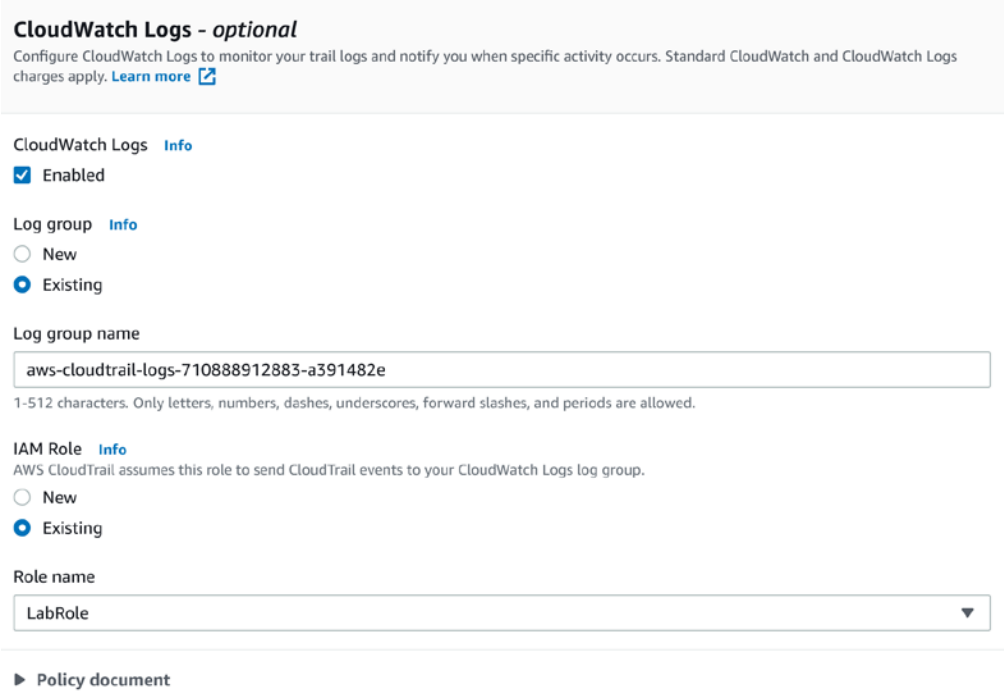
▼ Additional settings

Log file validation Info

□ Enabled

SNS notification delivery Info

□ Enabled



CloudWatch Logs - *optional*

Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. Learn more

CloudWatch Logs Info

☑ Enabled

Log group Info

○ New

● Existing

Log group name

aws-cloudtrail-logs-710888912883-a391482e

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

IAM Role Info

AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

○ New

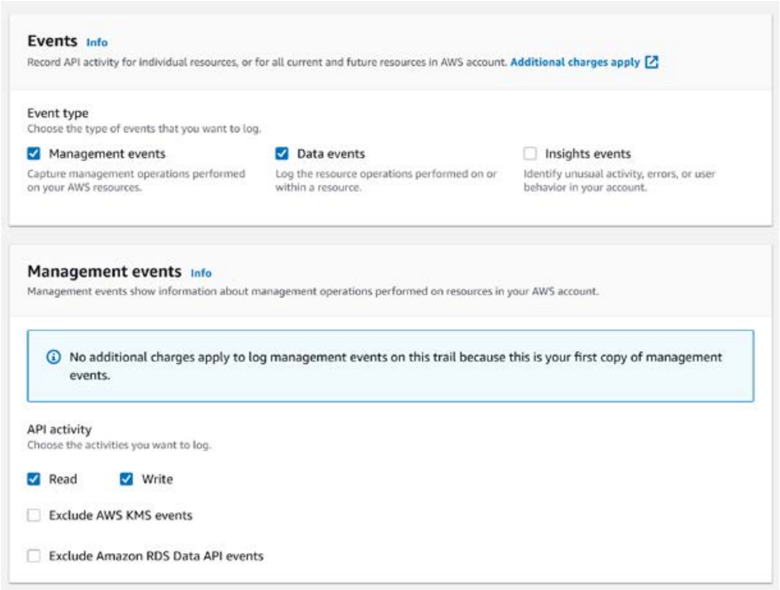
● Existing

Role name

LabRole ▼

▶ Policy document

4. Click the **Next** button. Then complete the Choose log events screen as shown below:



Events Info

Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply

Event type

Choose the type of events that you want to log.

☑ Management events

Capture management operations performed on your AWS resources.

☑ Data events

Log the resource operations performed on or within a resource.

□ Insights events

Identify unusual activity, errors, or user behavior in your account.

Management events Info

Management events show information about management operations performed on resources in your AWS account.

ⓘ No additional charges apply to log management events on this trail because this is your first copy of management events.

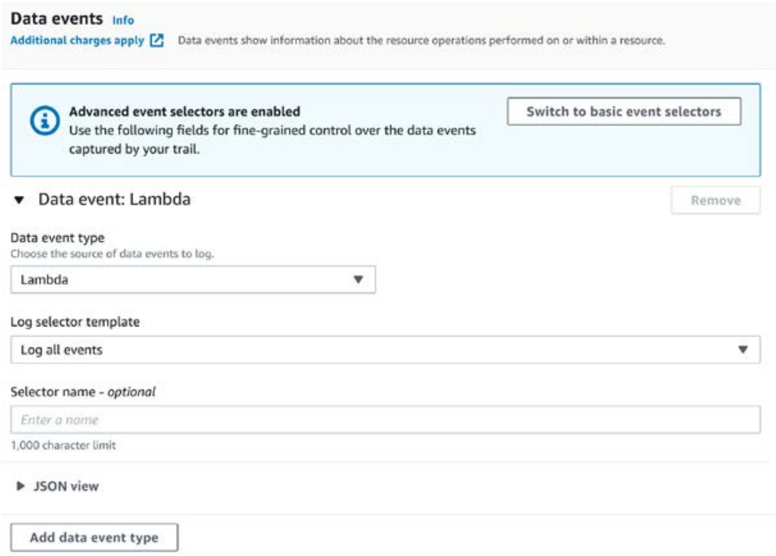
API activity

Choose the activities you want to log.

☑ Read ☑ Write

□ Exclude AWS KMS events

□ Exclude Amazon RDS Data API events



Data events Info

Additional charges apply

Data events show information about the resource operations performed on or within a resource.

Advanced event selectors are enabled
Use the following fields for fine-grained control over the data events captured by your trail.

Switch to basic event selectors

▼ Data event: Lambda

Remove

Data event type
Choose the source of data events to log.
Lambda ▼

Log selector template
Log all events ▼

Selector name - *optional*
Enter a name
1,000 character limit

▶ JSON view

Add data event type

Click the **Add data event type** button. Choose **S3** for the Data event type and **Log all events**.

Click the **Next** button.

5. Click the **Create trail** button.

6. Go to the **S3** service and notice that a new bucket got created for you. It has many subfolders (they are likely empty now).

7. Use your Project3 by uploading a few license plates. Go to the AWS console, change some Lambda property value (e.g., change the timeout to a higher value), go to S3 and manually delete some plate file.

8. Go to the CloudTrail bucket that was created and drill down the folders until you see *.gz files.

9. Unzip a *.gz file, open the resulting JSON in VSCode, and right-click the document in VSCode editor and choose menu **Format Document** to format the JSON. Look at the various events that CloudTrail captured.

   NOTE: You might need to wait a few minutes before you see things in CloudTrail (there is a bit of delay).

What to Submit

Nothing to submit for this module