AWS - CloudTrail

By

Keshav Kummari

Prerequisites

- AWS Account with Console Access
- Root or Admin privileges(AWS Account)
- SSH Client to use AWS CLI
- Email Account

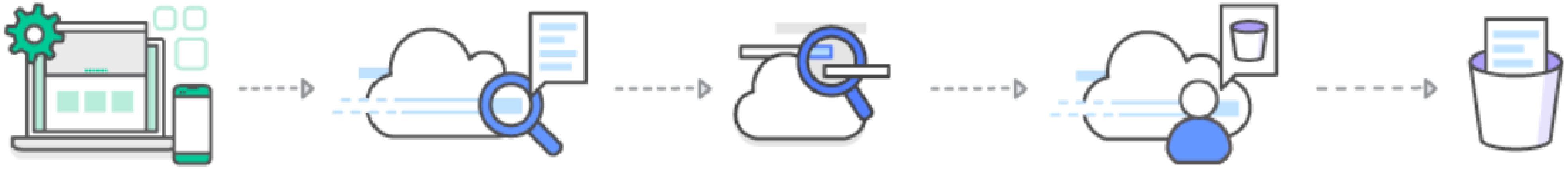
Overview

- AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.

- With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

- This event history simplifies security analysis, resource change tracking, and troubleshooting.

How It Works



Account activity occurs

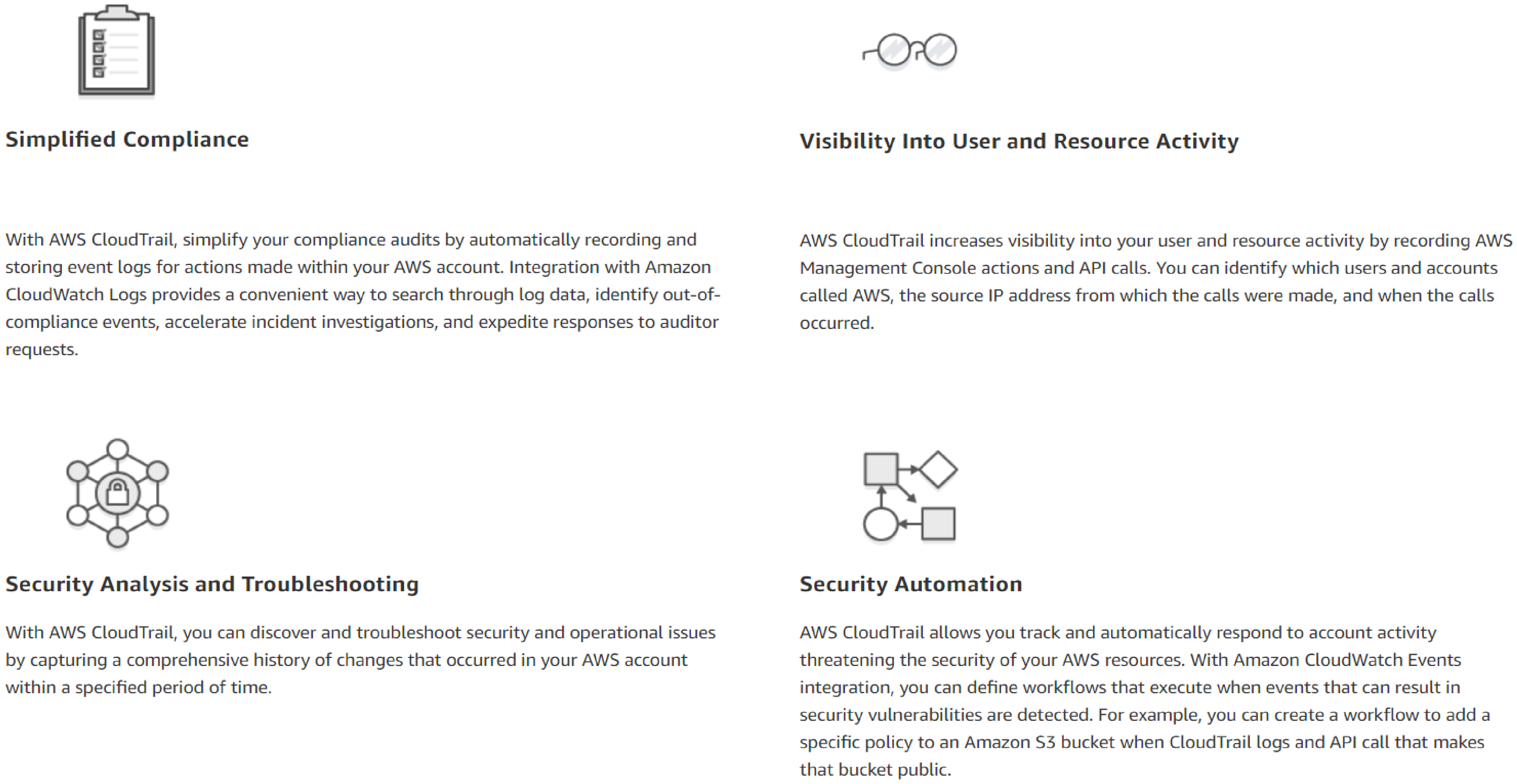
CloudTrail captures and records the activity as a CloudTrail Event

You can view and download your activity in the CloudTrail Event History

You can set up CloudTrail and define an Amazon S3 bucket for storage

A log of CloudTrail events is delivered to S3 bucket and optionally delivered to CloudWatch Logs and CloudWatch Events

Benefits



Simplified Compliance

With AWS CloudTrail, simplify your compliance audits by automatically recording and storing event logs for actions made within your AWS account. Integration with Amazon CloudWatch Logs provides a convenient way to search through log data, identify out-of-compliance events, accelerate incident investigations, and expedite responses to auditor requests.

Visibility Into User and Resource Activity

AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

Security Analysis and Troubleshooting

With AWS CloudTrail, you can discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in your AWS account within a specified period of time.

Security Automation

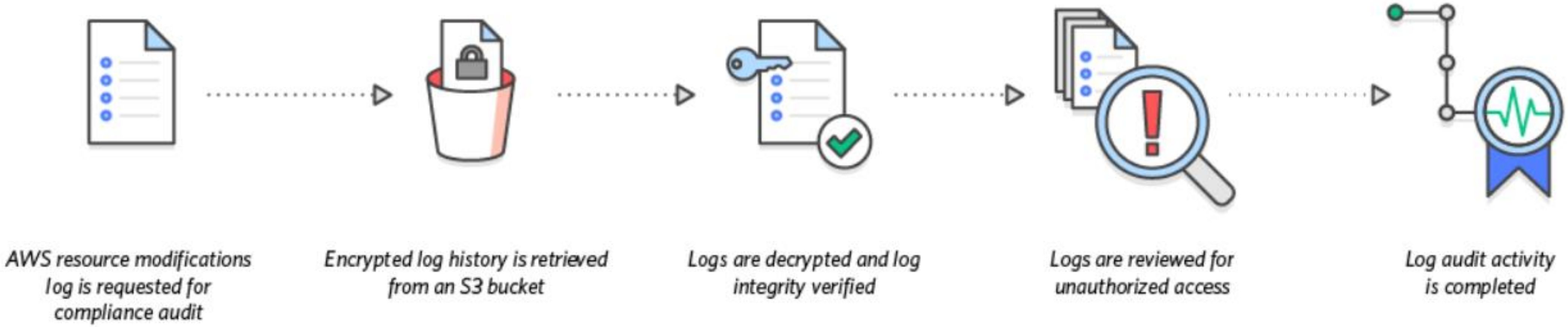
AWS CloudTrail allows you track and automatically respond to account activity threatening the security of your AWS resources. With Amazon CloudWatch Events integration, you can define workflows that execute when events that can result in security vulnerabilities are detected. For example, you can create a workflow to add a specific policy to an Amazon S3 bucket when CloudTrail logs and API call that makes that bucket public.

Compliance Aid

- AWS CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards by providing a history of activity in your AWS account.

- For more information, download the AWS compliance whitepaper, "Security at Scale: Logging in AWS."

Compliance Aid



AWS resource modifications log is requested for compliance audit

Encrypted log history is retrieved from an S3 bucket

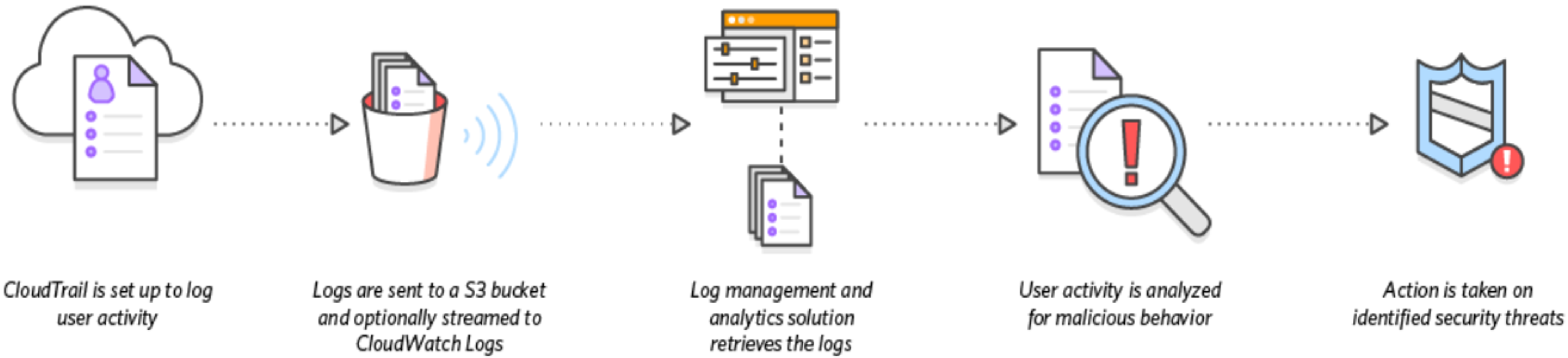
Logs are decrypted and log integrity verified

Logs are reviewed for unauthorized access

Log audit activity is completed

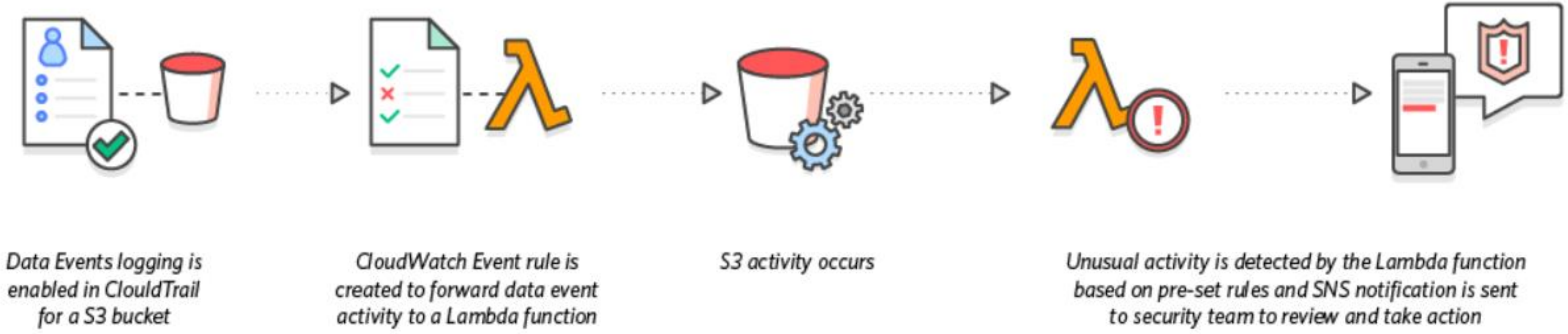
Security Analysis

- You can perform security analysis and detect user behavior patterns by ingesting AWS CloudTrail events into your log management and analytics solutions.


CloudTrail is set up to log user activity
Logs are sent to a S3 bucket and optionally streamed to CloudWatch Logs
Log management and analytics solution retrieves the logs
User activity is analyzed for malicious behavior
Action is taken on identified security threats

Data Exfiltration

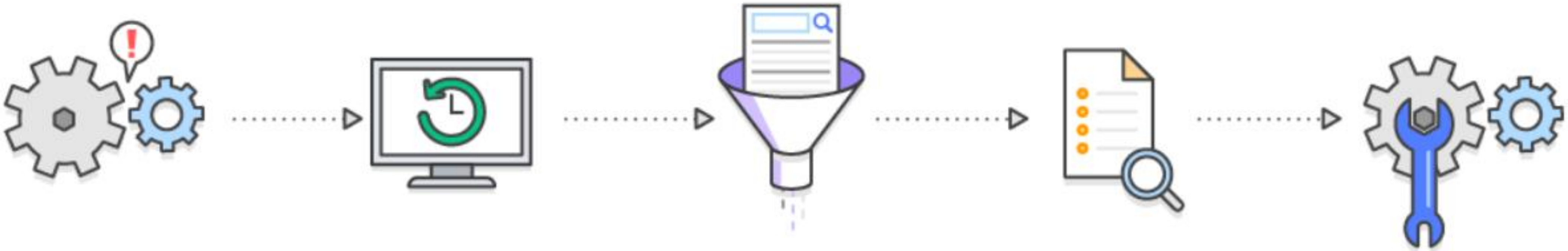
- You can detect data exfiltration by collecting activity data on S3 objects through object-level API events recorded in CloudTrail.
- After the activity data is collected, you can use other AWS services, such as Amazon CloudWatch Events and AWS Lambda, to trigger response procedures.


Data Events logging is enabled in ClouldTrail for a S3 bucket
CloudWatch Event rule is created to forward data event activity to a Lambda function
S3 activity occurs
Unusual activity is detected by the Lambda function based on pre-set rules and SNS notification is sent to security team to review and take action

Operational Issue Troubleshooting

- You can troubleshoot operational issues by leveraging the AWS API call history produced by AWS CloudTrail.
- For example, you can quickly identify the most recent changes made to resources in your environment, including creation, modification, and deletion of AWS resources (e.g., Amazon EC2 instances, Amazon VPC security groups, and Amazon EBS volumes).

Operational Issue Troubleshooting



An AWS resource change causes an operation issue

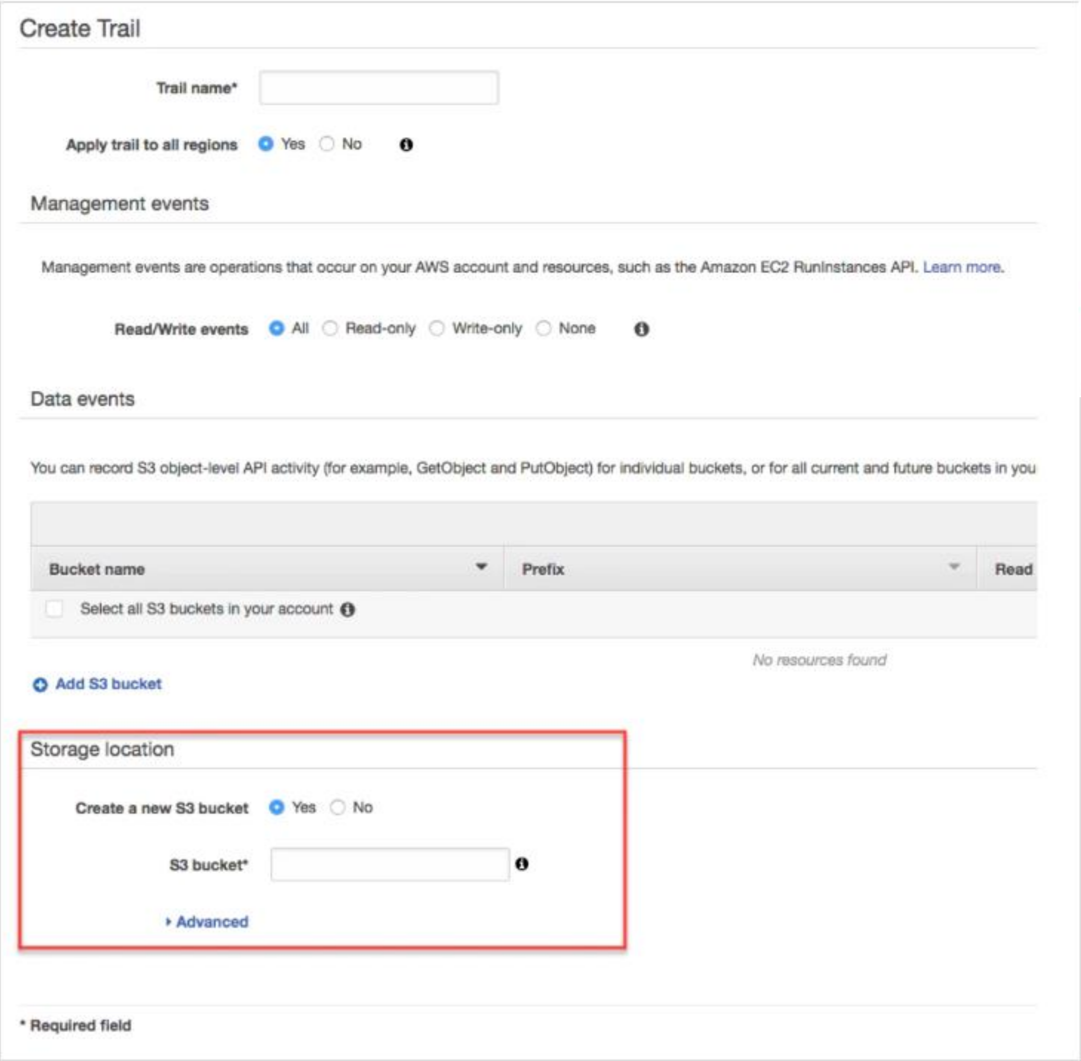
API Activity History is reviewed from the CloudTrail console

Search results are filtered by impacted resource name

Captured details, including what change was made and by whom, are reviewed

Corrective action is taken to resolve the issue

Enable Cloudtrail Logging



Create Trail

Trail name*

Apply trail to all regions ● Yes ○ No

Management events

Management events are operations that occur on your AWS account and resources, such as the Amazon EC2 RunInstances API. Learn more.

Read/Write events ● All ○ Read-only ○ Write-only ○ None

Data events

You can record S3 object-level API activity (for example, GetObject and PutObject) for individual buckets, or for all current and future buckets in you

Bucket name	Prefix	Read
□ Select all S3 buckets in your account		

No resources found

Add S3 bucket

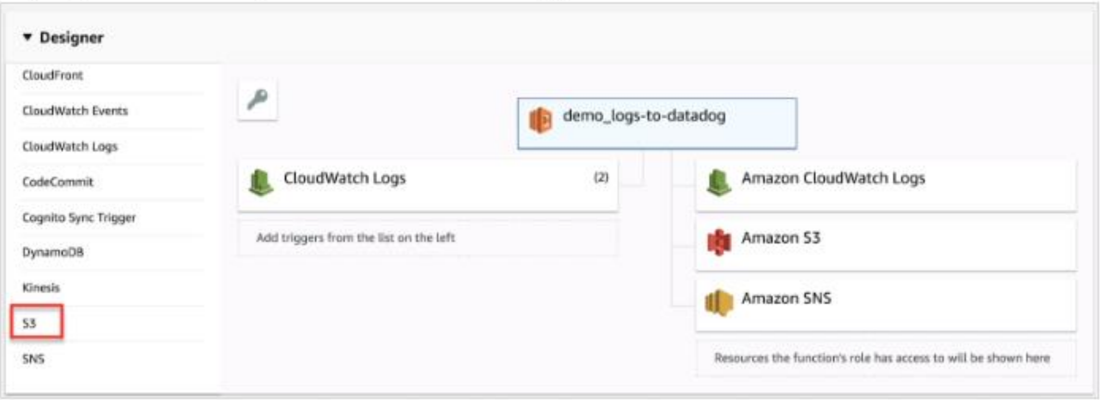
Storage location

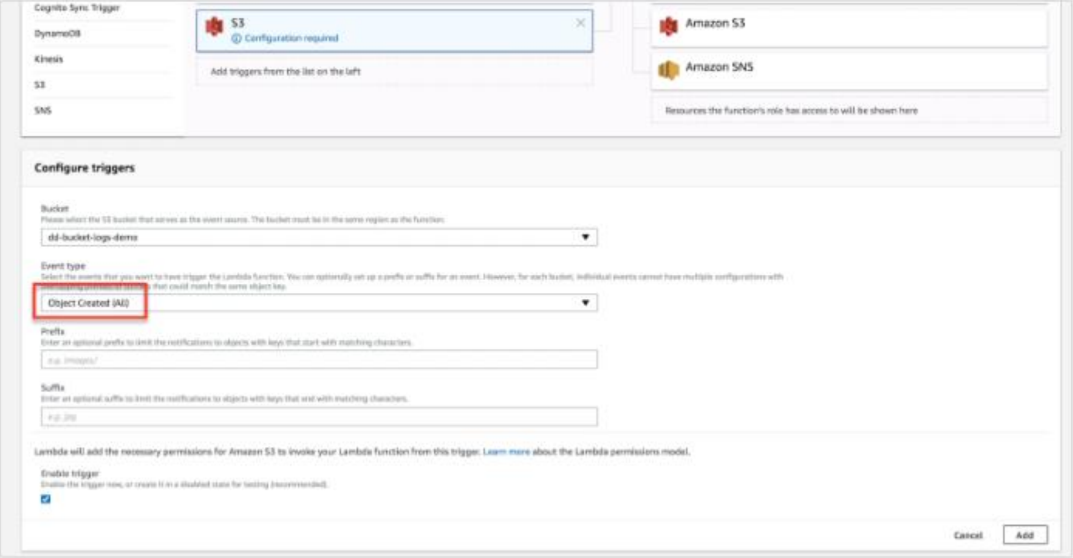
Create a new S3 bucket ● Yes ○ No

S3 bucket*

Advanced

* Required field





Cognito Sync Trigger
DynamoDB
Kinesis
S3
SNS
S3
Configuration required
Add triggers from the list on the left
Amazon S3
Amazon SNS
Resources the function's role has access to will be shown here

Configure triggers

Bucket
Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.
dd-bucket-logs-demo

Event type
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.
Object Created (All)

Prefix
Enter an optional prefix to limit the notifications to objects with keys that start with matching characters.
e.g. images/

Suffix
Enter an optional suffix to limit the notifications to objects with keys that end with matching characters.
e.g. .jpg

Lambda will add the necessary permissions for Amazon S3 to invoke your Lambda function from this trigger. Learn more about the Lambda permissions model.

Enable trigger
Enable the trigger now, or create it in a disabled state for testing (recommended).
☑

Cancel Add