



Configuring Amazon S3 security settings and access controls

Getting started at an AWS hosted workshop

▼ S3 Security Best Practices

▼ Prepare Your Lab

- Attach IAM Role to EC2 Instance
- Connect to the EC2 Instance
- Bucket Name

▼ Lab 1 - S3 Security Exercises

- Require HTTPS
- Require SSE-KMS Encryption
- Restrict Access to an S3 VPC Endpoint
- Use AWS Config Rules to Detect a Public Bucket
- Use Amazon Access Analyzer for S3

▼ Lab 2 - S3 Access Grants

- S3 Access Grants Lab - Initial Setup
- Configure S3 Access Grants for IAM user

▼ Lab 3 - Enabling Malware Protection for S3 by using GuardDuty

- Enabling Malware Protection for S3 for your bucket
- Testing GuardDuty Malware with an object.

▼ Lab 4 - S3 Access Control Lists

- Block Public ACLs
- Configure S3 Block Public Access
- Disable S3 ACLs

▼ Finding S3 access control lists with S3 Inventory

- Enabling Amazon S3 Inventory
- Setting up Amazon Athena
- Use Amazon Athena to query Amazon S3 Inventory and identify objects with ACL elements

▼ Use Amazon Athena to query CloudTrail logs and identify S3 requests that depend on ACLs

[Enabling Cloudtrail data events](#)

Setting up Amazon Athena

Lab Summary

[Configuring Amazon S3 security settings and access controls](#) > ... > [Use Amazon Athena to query CloudTrail logs and](#)

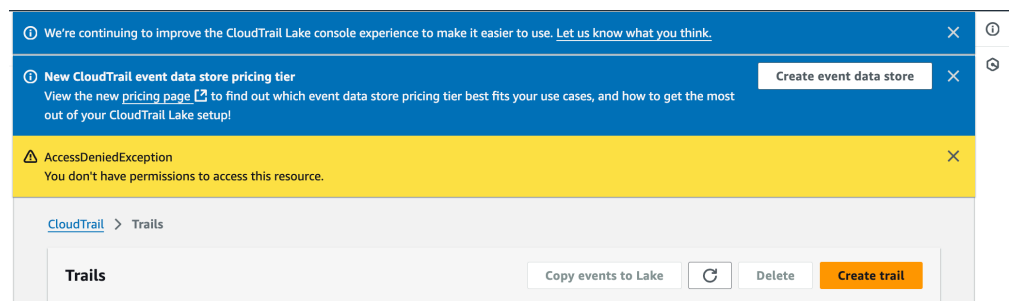
Enabling Cloudtrail data events

In this exercise, we will walk through how to enable data events for S3 in CloudTrail. *Note* that we will not be using the CloudTrail data from this account, rather the same S3 bucket, `sid-security-xxxxxxx` is pre-populated with synthetic CloudTrail logs under the `cloudtrail` prefix.

From the AWS console in the top search bar, search and select S3.

- Click the bucket name starting with `sid-security-xxxxxxx`.
- Click on the **Properties** tab.
- Scroll down to **AWS CloudTrail data events**
- Click **Configure** in CloudTrail
- You might see a yellow error box at the top, that is ok to ignore for now.

Your screen should look like the following:



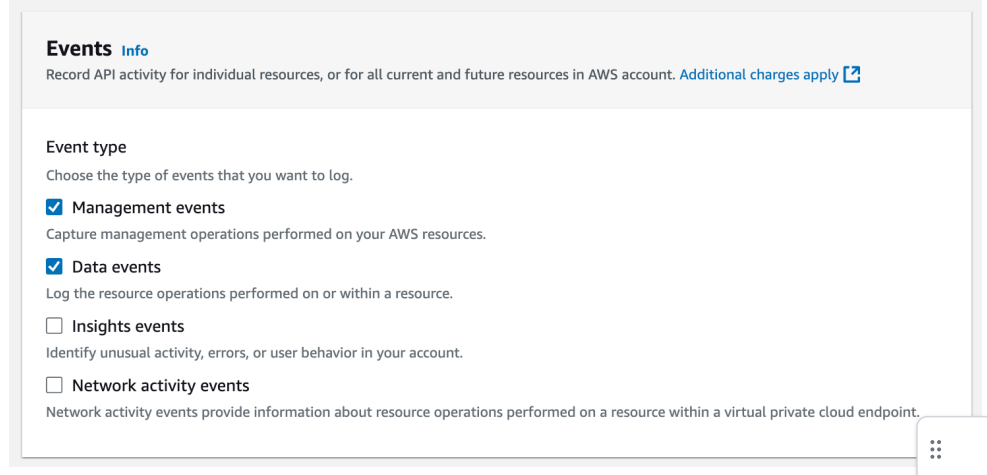
Click **Create trail**

- Configure Trail name as `cloudtrailacl`
- Under **Log file SSE-KMS encryption** un-check the "Enabled" box
- Keep everything else as default settings and click **Next**

Under **Choose log events**

- Under **Events**, select **Data events**

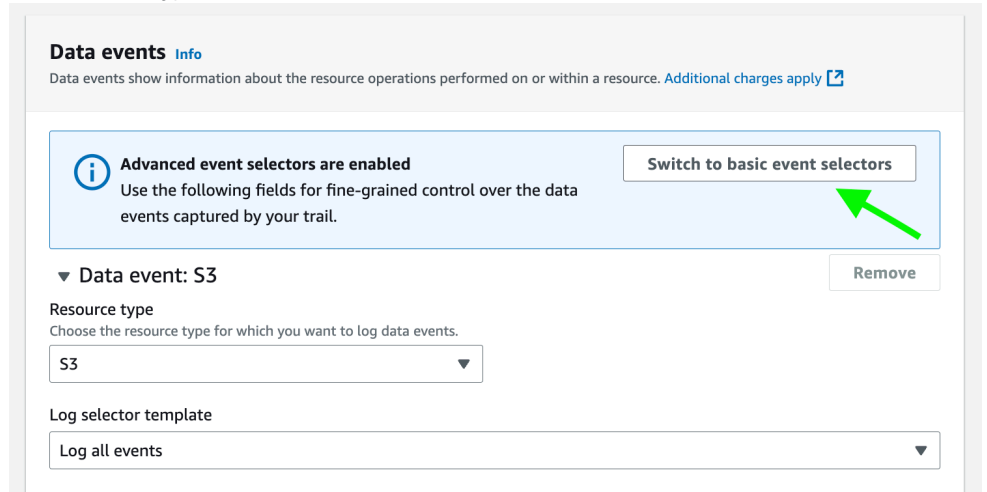
Choose log events



Under **Data Events**



- For Resource type select S3 from the drop down menu



Data events [Info](#)

Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

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: S3** [Remove](#)

Resource type

Choose the resource type for which you want to log data events.

S3 ▼

Log selector template

Log all events ▼

i Keep in mind that if you enable data events in your own account, you will incur additional cost.

Using the above screenshot as context, notice that you can include or exclude specific events in the Management events section. In the Data events section the current selection is S3 but there are other services that can be changed or added to the Cloudtrail by using the Add data event type at the bottom. If you only want to enable data events for a specific bucket you can click on Switch to basic event selectors as referenced by the green arrow and further customize.

Since this is more informational, we will click Next and Create trail on the last page.

[Previous](#)[Next](#)