Basic CloudTrail Set Up

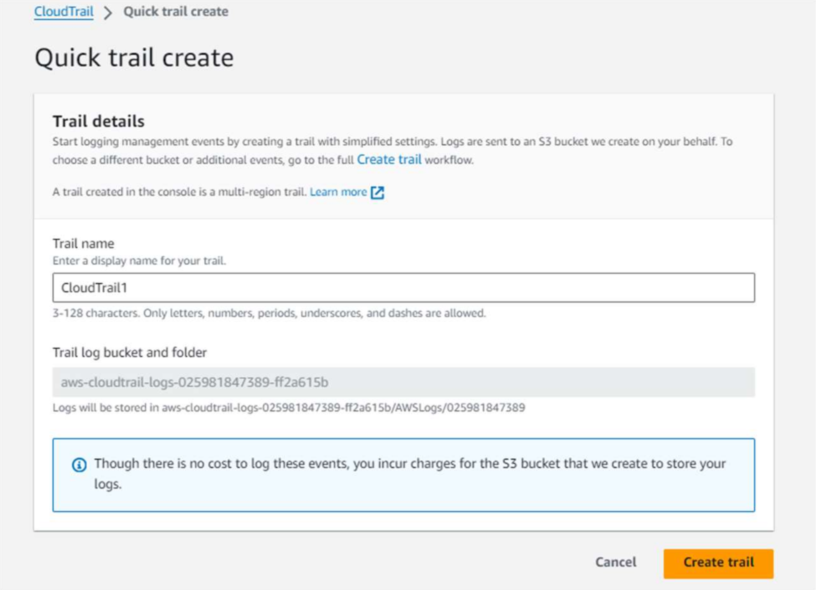
Setting up AWS CloudTrail for basic operations involves enabling the service, creating trails to record your AWS API activity, and configuring additional security measures like log file encryption. Here are detailed instructions to get you started:

Step 1: Enable AWS CloudTrail

1. **Log in to the AWS Management Console.**
2. **Open the CloudTrail Service:**
   - Navigate to the CloudTrail console.

Step 2: Create a New Trail

1. **Create Trail:**
   - In the CloudTrail console, click on “Trails” in the sidebar.
   - **Name the Trail:** Give your trail a descriptive name.
   - Click on “Create trail.”
     1. CloutTrail Will make a new S3 Bucket to store the logs, or you can choose an existing one.



Quick trail create

Trail details

Start logging management events by creating a trail with simplified settings. Logs are sent to an S3 bucket we create on your behalf. To choose a different bucket or additional events, go to the full Create trail workflow.

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

Trail name

Enter a display name for your trail.

CloudTrail1

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

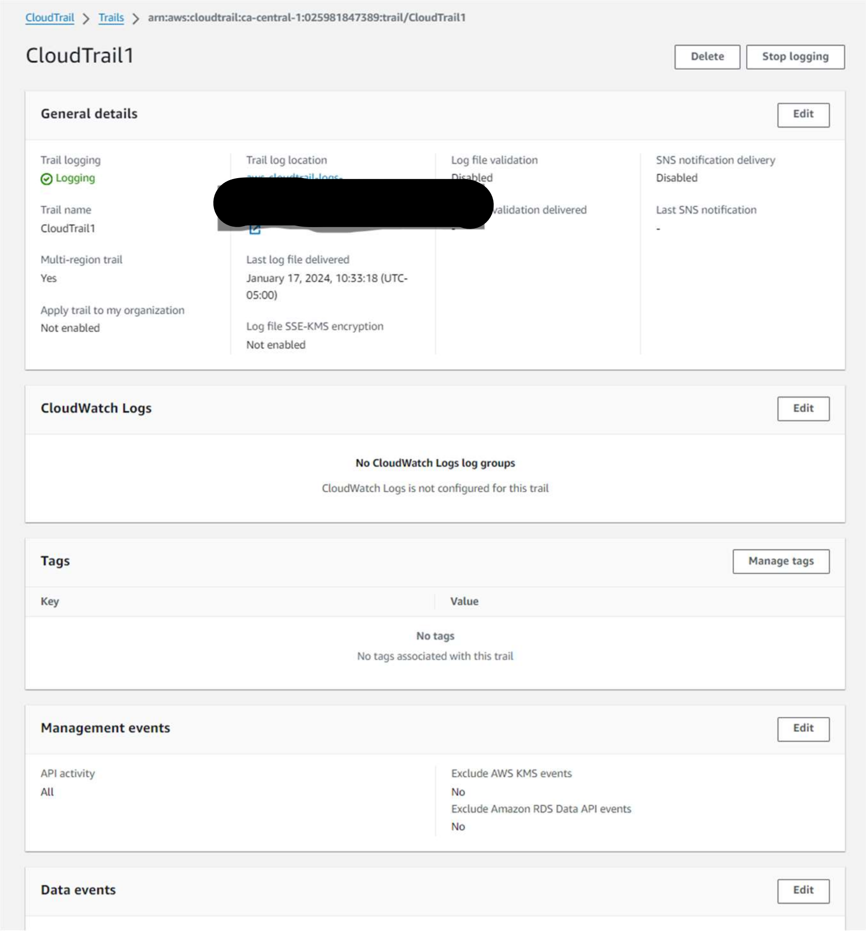
Trail log bucket and folder

aws-cloudtrail-logs-025981847389-ff2a615b

Logs will be stored in aws-cloudtrail-logs-025981847389-ff2a615b/AWSLogs/025981847389

Though there is no cost to log these events, you incur charges for the S3 bucket that we create to store your logs.

2. **Trail Settings:** Click on the Trail After its created then click edit on the desired section you wish to change.
   - **Apply Trail to a Region**
   - **Management Events:** Choose to log Read/Write events or All events.


CloudTrail > Trails > arn:aws:cloudtrail:ca-central-1:025981847389:trail/CloudTrail1

CloudTrail1

General details

Trail logging
Logging

Trail name
CloudTrail1

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Trail log location
[redacted]

Last log file delivered
January 17, 2024, 10:33:18 (UTC-05:00)

Log file SSE-KMS encryption
Not enabled

Log file validation
Disabled

validation delivered
-

SNS notification delivery
Disabled

Last SNS notification
-

CloudWatch Logs

No CloudWatch Logs log groups
CloudWatch Logs is not configured for this trail

Tags

Key	Value
No tags No tags associated with this trail	

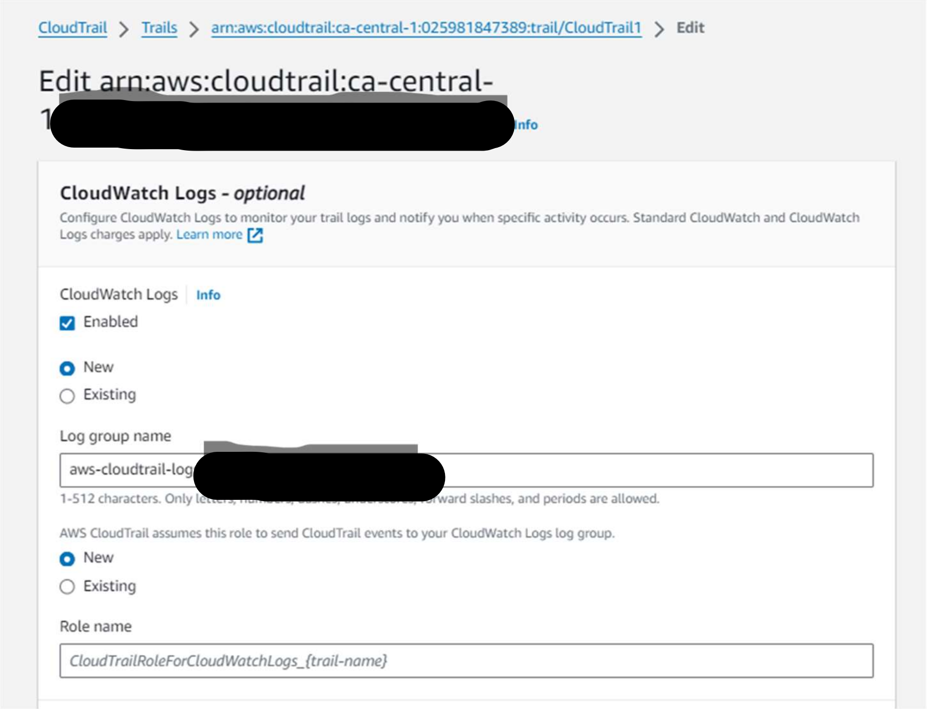
Management events

API activity
All

Exclude AWS KMS events
No
Exclude Amazon RDS Data API events
No

Data events

3. **Choose Log File Destination:**
    - **Create a new S3 bucket** or select an existing one to store your CloudTrail logs. Ensure this bucket is secured and access is limited.
    - Optionally, enable S3 bucket log file validation to verify the integrity of the logs.
4. **Configure Additional Settings (Optional):**
    - **Log File Encryption:** Enable log file encryption using AWS Key Management Service (KMS) for added security. You can choose an existing KMS key or create a new one.
    - **CloudWatch Logs Integration:** Optionally, you can configure CloudTrail to send logs to CloudWatch Logs for real-time monitoring and alerting.
        1. Enter a name for the IAM Role and CloudTrail will make a new custom Role for this Action (Convenient!)
    - **SNS Notification:** Set up an Amazon SNS topic to receive notifications when new log files are delivered.



CloudTrail > Trails > arn:aws:cloudtrail:ca-central-1:025981847389:trail/CloudTrail1 > Edit

Edit arn:aws:cloudtrail:ca-central-1[redacted] Info

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

● New

○ Existing

Log group name

aws-cloudtrail-log[redacted]

1-512 characters. Only le ward slashes, and periods are allowed.

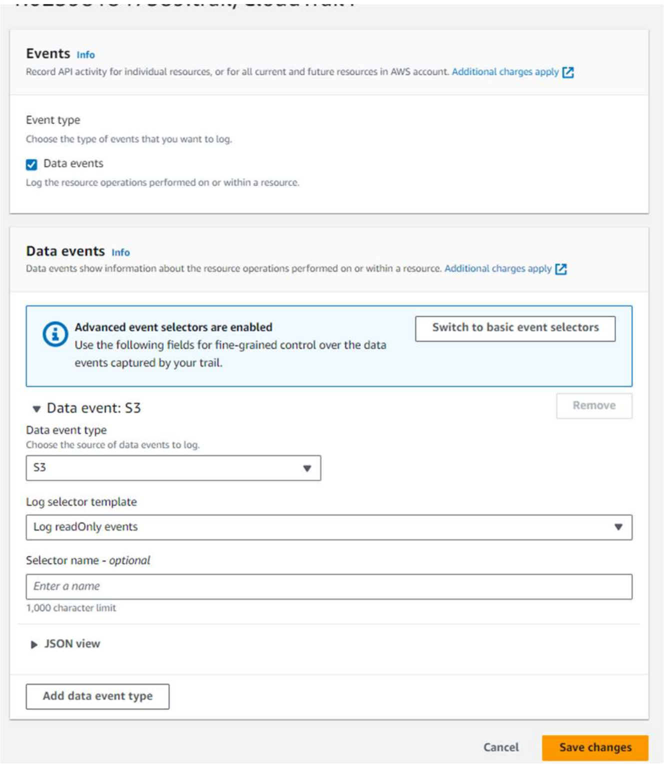
AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

● New

○ Existing

Role name

CloudTrailRoleForCloudWatchLogs_{trail-name}



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.

☑ Data events

Log the resource operations performed on or within a resource.

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.

▼ Data event: S3

Data event type

Choose the source of data events to log.

S3

Log selector template

Log readOnly events

Selector name - *optional*

Enter a name

1,000 character limit

- Data Events: Optionally, you can log data events for resources like S3 buckets or Lambda functions, but note that logging data events can increase the volume of your CloudTrail logs. This is useful if you want to track things like get requests for documents stored in S3

Step 3: Continuous Monitoring and Analysis

1. **Regular Log Review:**
    - Periodically check your CloudTrail logs for unusual or unexpected activity. This can include spikes in API activity, unexpected API calls, or unauthorized resource modifications.
    - Utilize log analysis tools or services for more efficient log analysis.
2. **Integrate with CloudWatch for Alerts:**
    - If integrated with CloudWatch Logs, create metric filters and alarms for specific events or patterns in your logs.
    - For instance, set up an alarm for multiple failed login attempts or API calls to sensitive resources.

Step 4: Audit Changes to AWS Resources

- Regularly audit your CloudTrail logs to understand the sequence of events leading to changes in your AWS environment.
- Use CloudTrail to backtrack and investigate security incidents or compliance issues.

Additional Tips:

- **Review Access Policies:** Regularly review the access policies of your S3 bucket where logs are stored to ensure they are not overly permissive.
- **Regular Updates:** Keep track of and adapt to any new features or changes in CloudTrail and related AWS services.