

[illegible]

Name	AWS CloudTrail : Creating Trail
URL	https://attackdefense.com/challengedetails?cid=2485
Type	AWS Cloud Security : Defense

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

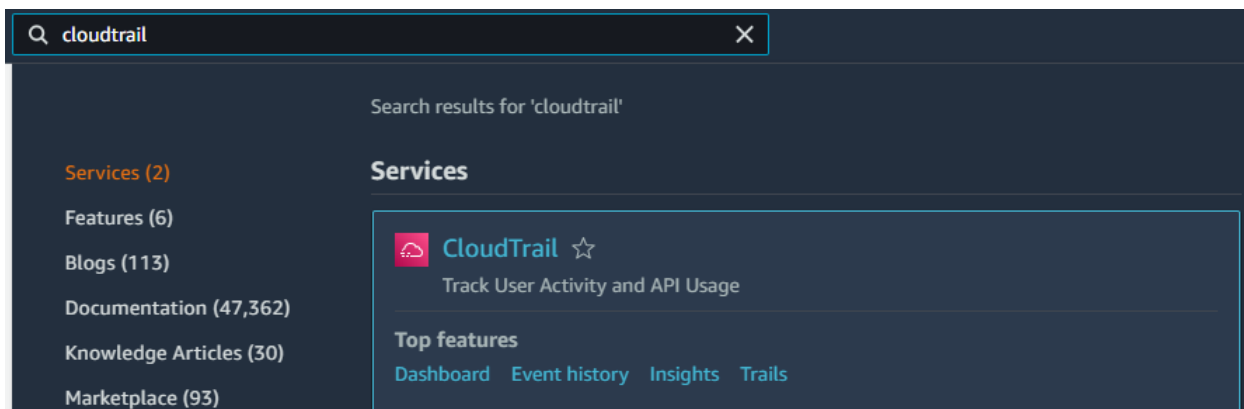
Solution:

Step 1: Click the lab link button to get access credentials.

Access Credentials to your AWS lab Account

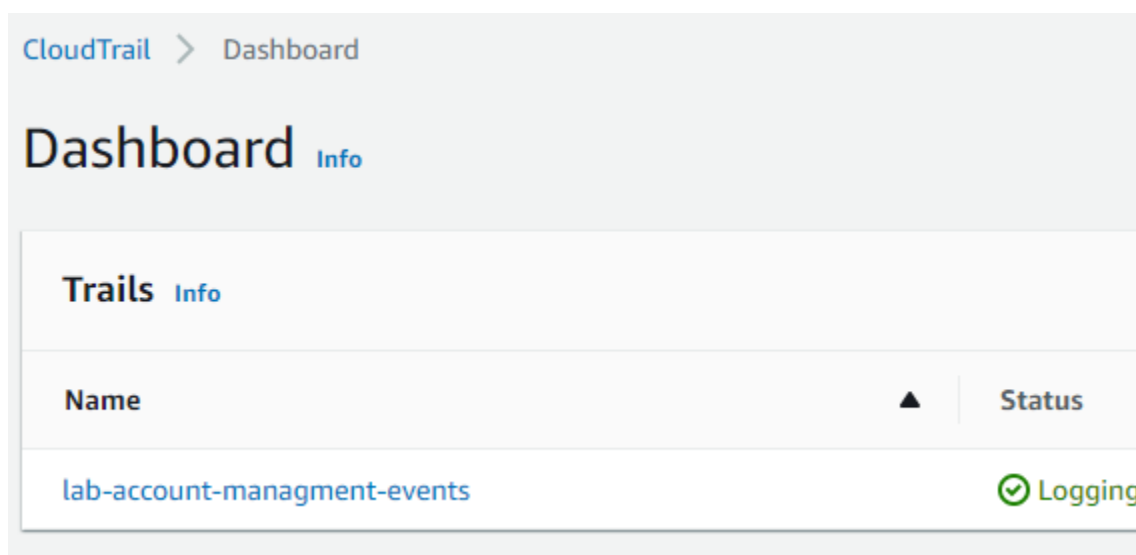
Login URL	https://270463904202.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad9xPRt2ExqU5ACc
Access Key ID	AKIAT56HHVHFOWJACDGJ
Secret Access Key	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

Step 2: Search for CloudTrail in the search bar and navigate to the CloudTrail dashboard.



Dashboard will list all the available trails.

“lab-account-managment-events” trail was created by the management account for the organization and hence cannot edit or delete this trail through this account.



Step 3: Click on “Event history”.

Dashboard

Event history

Insights

Lake

Trails

Event history will list all the event names which are already created. It helps to look up events related to creation, modification, or deletion of resources (such as IAM users or Amazon EC2 instances) in your AWS account on a per-region basis.

Event history (50+) Info				
Event history shows you the last 90 days of management events.				
Read-only ▼ Q false				
<input type="checkbox"/>	Event name	Event time	User name	Event source
<input type="checkbox"/>	AssumeRole	September 04, 2022, 21:33:31 (...)	-	sts.amazonaws.com
<input type="checkbox"/>	AssumeRole	September 04, 2022, 21:33:31 (...)	-	sts.amazonaws.com
<input type="checkbox"/>	AssumeRole	September 04, 2022, 21:32:30 (...)	-	sts.amazonaws.com
<input type="checkbox"/>	AssumeRole	September 04, 2022, 21:32:30 (...)	-	sts.amazonaws.com
<input type="checkbox"/>	CreateUser	September 04, 2022, 21:31:52 (...)	student	iam.amazonaws.com
<input type="checkbox"/>	CreateDefaultVpc	September 03, 2022, 09:51:50 (...)	AdminSessionRole	ec2.amazonaws.com
<input type="checkbox"/>	AttachAccessPolicy	September 03, 2022, 09:51:49 (...)	AdminSessionRole	iam.amazonaws.com

Step 4: Click on “Trails”.

Dashboard

Event history

Insights

Lake

Trails

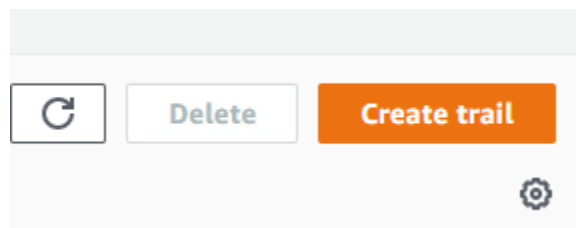
A trail is a configuration that enables delivery of CloudTrail events to an Amazon S3 bucket, CloudWatch Logs, and CloudWatch Events. This page will list all the available trails in detail.

CloudTrail > Trails

Trails

	Name ▲	Home region ▼	Multi-region trail ▼	Insights ▼	Organization trail ▼	S3 bucket ▼
<input type="radio"/>	lab-account-managment-events	US East (N. Virginia)	Yes	Disabled	Yes	lab-account-managment-events

Step 5: Click on “Create trail”.



Step 6: Set trail name as “student-management-events” and choose “Create new S3 bucket” option and append “management-events” in between S3 bucket name.

Trail name

Enter a display name for your trail.

student-management-events

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 the 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-management-events-logs-270463904202-ebba162b

Logs will be stored in aws-cloudtrail-management-events-logs-270463904202-ebba162b/AWSLogs/270463904202

Step 7: Disable Log file SSE-KMS encryption and Log file validation.

Log file SSE-KMS encryption [Info](#)

☐ Enabled

▼ Additional settings

Log file validation [Info](#)

☐ Enabled

SNS notification delivery [Info](#)

☐ Enabled

Click on “Next” button.

Cancel

Next

Step 8: In Events choose “Management events” and “Insights events”.

For differentiating between events, we will use two different trails and two different buckets for management events and data events. Insights events will only work with management events.

Management events provide visibility into management operations that are performed on resources in your AWS account. These are also known as control plane operations. Management events can also include non-API events that occur in your account. For example, when a user logs into your account, CloudTrail logs the ConsoleLogin event.

Insights events are logged when CloudTrail detects unusual write management API activity in your account. If you have CloudTrail Insights enabled and CloudTrail detects unusual activity, Insights events are delivered to the destination S3 bucket for your trail.

Note: After you enable CloudTrail Insights for the first time on a trail, it can take up to 36 hours for CloudTrail to deliver the first Insights event.

Choose log events

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.

Step 9: Enable Read and Write API activities log in management events .

Management events [Info](#)

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

 Charges apply to log management events on this trail because you are logging at least one other copy of management events in your account.


API activity

Choose the activities you want to log.

- ☒ Read ☒ Write
- ☐ Exclude AWS KMS events
- ☐ Exclude Amazon RDS Data API events

Step 10: Enable API call rate and API error rate in “Insights types”.

Insights events [Info](#)

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

Choose Insights types

Insights measure unusual activity against a seven-day baseline.

- ☒ **API call rate**
A measurement of write-only management API calls that occur per minute against a baseline API call volume.
- ☒ **API error rate**
A measurement of management API calls that result in error codes. The error is shown if the API call is unsuccessful.

[Cancel](#)

[Previous](#)

[Next](#)

Review the details.

Review and create

Step 1: Choose trail attributes

General details

Trail name student-management-events	Trail log location aws-cloudtrail-management-events-logs-270463904202-ebba162b/AWSLogs/270463904202	Log file validation Disabled
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled	SNS notification delivery Disabled
Apply trail to my organization Not enabled		

Click on “Create trail” button.

Previous

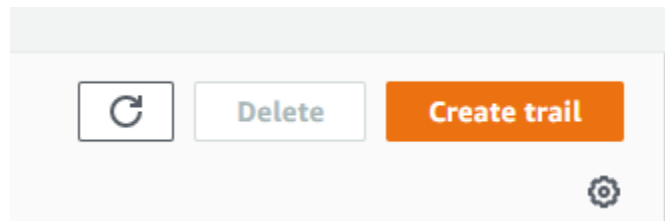
Create trail

Successfully created trail for management events.

Trails

	Name ▲	Home region ▼	Multi-region trail ▼	Insights ▼	Organization trail ▼
<input type="radio"/>	lab-account-managment-events	US East (N. Virginia)	Yes	Disabled	Yes
<input type="radio"/>	student-management-events	US East (N. Virginia)	Yes	Enabled	No

Step 11: Create trail for data events. Click on the “Create trail” button.



Step 12: Set trail name as “student-data-events” and choose “Create new S3 bucket” option and append “data-events” in between S3 bucket name.

Trail name

Enter a display name for your trail.

student-data-events

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 stor

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-data-events-logs-270463904202-10df1aad

Logs will be stored in aws-cloudtrail-data-events-logs-270463904202-10df1aad/AWSLogs/270463904202

Step 13: Disable Log file SSE-KMS encryption and Log file validation.

Log file SSE-KMS encryption [Info](#)

☐ Enabled

▼ Additional settings

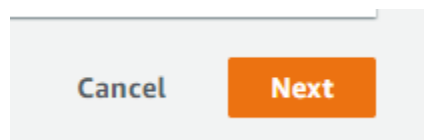
Log file validation [Info](#)

☐ Enabled

SNS notification delivery [Info](#)

☐ Enabled

Click on the “Next” button.



Step 14: In Events choose “Data events”.

Data events provide visibility into the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities.

For example Amazon DynamoDB object-level API activity on tables (PutItem, DeleteItem, and UpdateItem API operations).

What you want to log.

☒ Data events

Operations performed

Log the resource operations performed on or within a resource.

Step 15: Select data event type as “DynamoDB” and Log selector template as “Log all events”. Set any name as the selector name and click on the “Next” button.

Using the information collected by CloudTrail, you can determine the request that was made to DynamoDB, the IP address from which the request was made, who made the request, when it was made, and additional details.

The screenshot shows the 'Data events' configuration page in the AWS CloudTrail console. At the top, there's a header 'Data events' with an 'Info' link. Below it, a note states 'Additional charges apply' with a link icon, followed by the text 'Data events show information about the resource operations performed on or within a resource.' A blue box contains an information icon and the text 'Advanced event selectors are enabled' with a sub-note: 'Use the following fields for fine-grained control over the data events captured by your trail.' A button 'Switch to basic event selectors' is located to the right of this box. Below this, a section titled 'Data event: DynamoDB' has a 'Remove' button. Under 'Data event type', it says 'Choose the source of data events to log.' and shows a dropdown menu with 'DynamoDB' selected. The 'Log selector template' dropdown also has 'Log all events' selected. There is a text input field for 'Selector name - optional' containing 'DynamoDB', with a '1,000 character limit' note below it. A 'JSON view' link is present. At the bottom of the configuration area is an 'Add data event type' button. At the very bottom of the console window are 'Cancel', 'Previous', and 'Next' buttons.

Data events [Info](#)
Additional charges apply [\[link\]](#) 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: DynamoDB** [Remove](#)

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

Log selector template
Log all events ▼

Selector name - optional
DynamoDB
1,000 character limit

► [JSON view](#)

[Add data event type](#)

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

Review the details.

Review and create

Step 1: Choose trail attributes

General details

Trail name student-data-events	Trail log location aws-cloudtrail-data-events-logs-270463904202-10df1aad/AWSLogs/270463904202	Log file validation Disabled
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled	SNS notification delivery Disabled
Apply trail to my organization Not enabled		

Click on the “Create trail” button.

Cancel

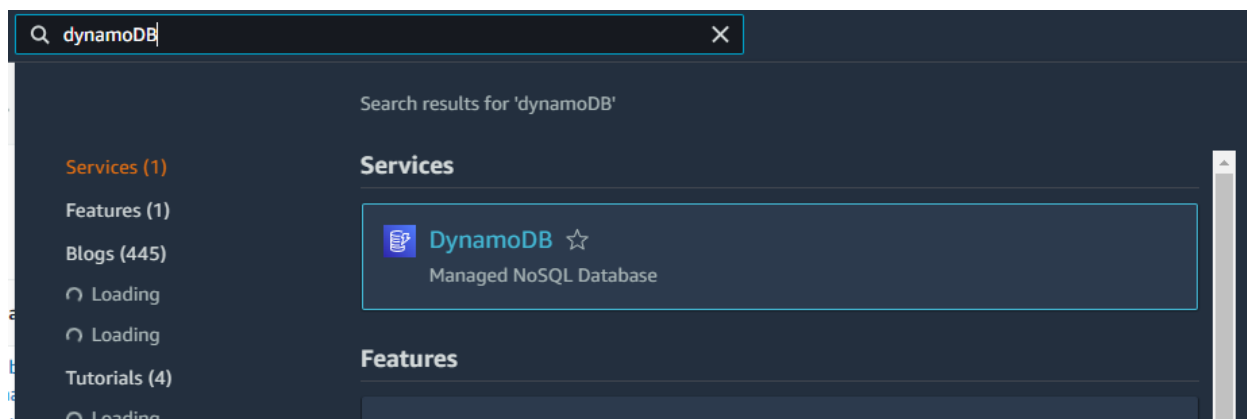
Previous

Create trail

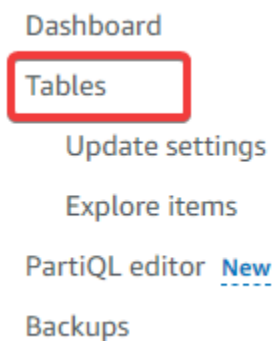
Step 16: Successfully created data events trail.

	Name ▲	Home region ▼	Multi-region trail ▼	Insights ▼	Organization trail ▼
<input type="radio"/>	lab-account-managment-events	US East (N. Virginia)	Yes	Disabled	Yes
<input type="radio"/>	student-data-events	US East (N. Virginia)	Yes	Disabled	No
<input type="radio"/>	student-management-events	US East (N. Virginia)	Yes	Enabled	No

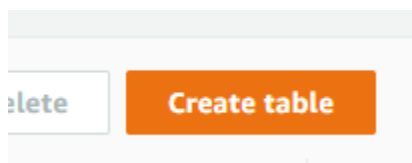
Step 17: Search for DynamoDB in the search bar and navigate to the DynamoDB dashboard.



Step 18: Click on “Tables” from the navigation pane.



Step 19: Click on the “Create table” button.



Step 20: Set Table name as “Users” and partition key as “id” with data type “Number”.

Create table

Table details [Info](#)

DynamoDB is a schemaless database that requires only a table name and a primary key when you create the table.

Table name

This will be used to identify your table.

Between 3 and 255 characters, containing only letters, numbers, underscores (_), hyphens (-), and periods (.).

Partition key

The partition key is part of the table's primary key. It is a hash value that is used to retrieve items from your table hosts for scalability and availability.



1 to 255 characters and case sensitive.

Sort key - *optional*

You can use a sort key as the second part of a table's primary key. The sort key allows you to sort or search among items with the same partition key.



1 to 255 characters and case sensitive.

Step 21: Choose "Default settings" in table settings.

Table settings



Default settings

The fastest way to create your table. You can modify these settings now or after your table has been created.

Step 22: Click on “Create table”.

Cancel

Create table

Wait until the “Creating” state changes to “Active” state.

DynamoDB > Tables

Tables (1) [Info](#)

<input type="checkbox"/>	Name	Status	Partition key	Sort key	Indexes	Read capacity mode
<input type="checkbox"/>	Users	Creating	id (N)	-	0	Provisioned (5)

Step 23: Click on “Explore items”.

Tables

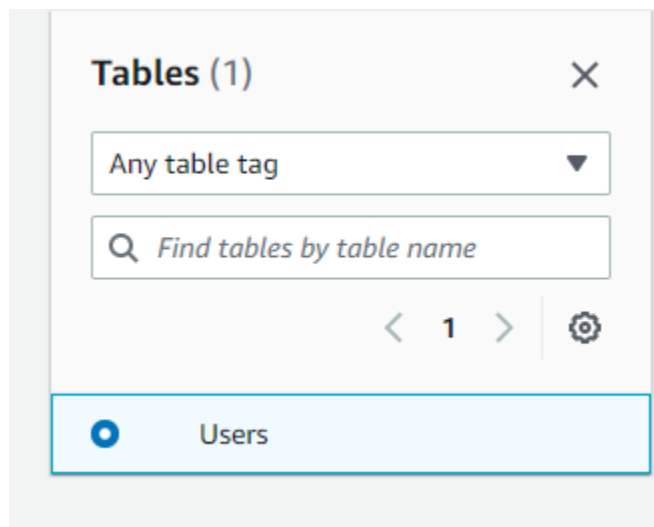
Update settings

Explore items

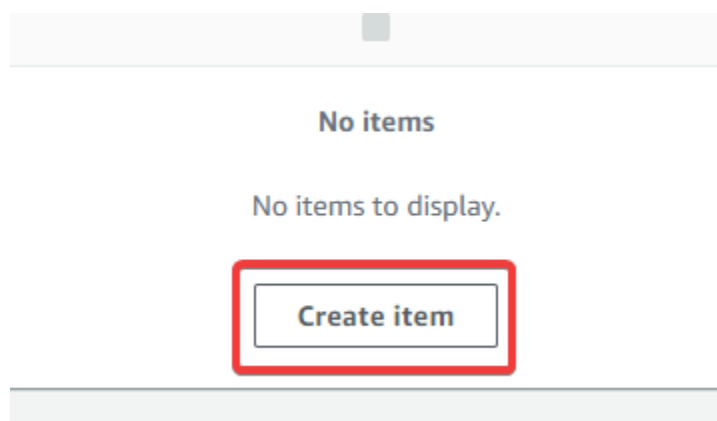
PartiQL editor [New](#)

Backups

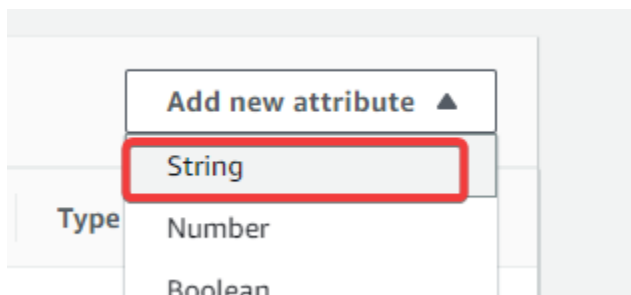
Step 24: Click on “Users”.



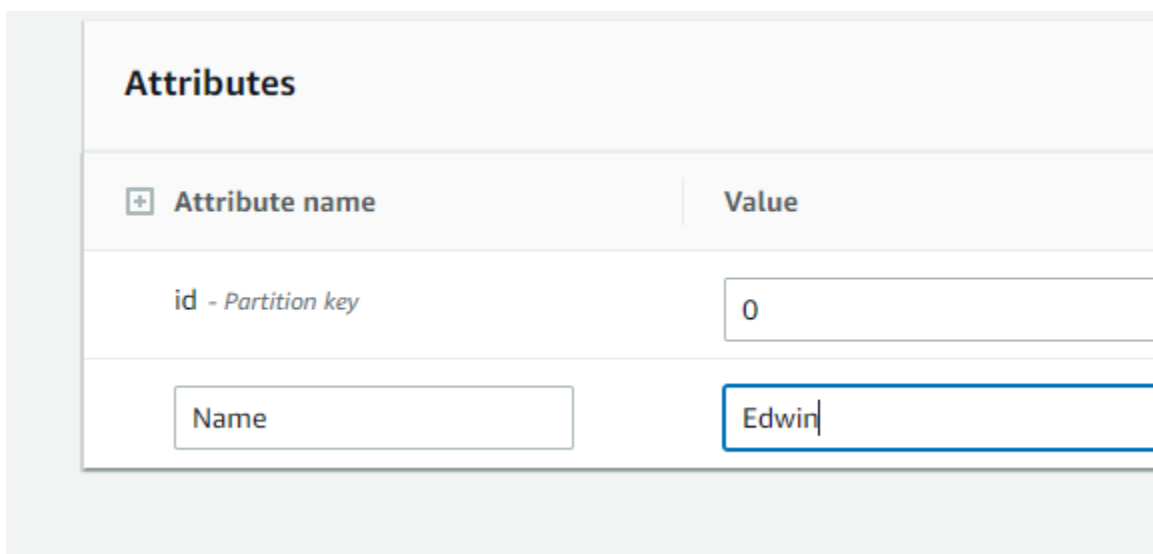
Step 25: There is no item available in the table. Click on the “Create item” button to add items into the table.



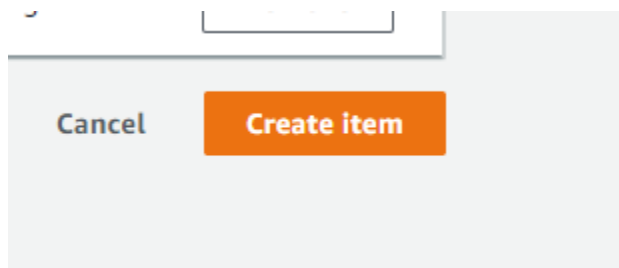
Step 26: Click on “String” under “Add new attribute” to set data type for new attribute.



Step 27: Enter “Name” as Attribute name and any value.

A screenshot of a web interface titled 'Attributes'. It contains a table with two columns: 'Attribute name' and 'Value'. The first row has 'id - Partition key' in the 'Attribute name' column and '0' in the 'Value' column. The second row has 'Name' in the 'Attribute name' column and 'Edwin' in the 'Value' column. The 'Name' and 'Edwin' cells are highlighted with blue borders, indicating they are the current focus of the user's input.

Step 28: Click on the “Create item” button.



Successfully created an item inside the users table.

<input type="checkbox"/>	id	Name
<input type="checkbox"/>	0	Edwin

Navigate back to the CloudTrail dashboard and click on “Trails”.

- Dashboard
- Event history
- Insights
- Lake
- Trails**

Step 29: Click on “student-management-events”.

<input type="radio"/>	student-management-events	US East (N. Virginia)	Yes	Enabled
-----------------------	---	-----------------------	-----	---------

Step 30: Check the logs from the management events bucket. Click on “Trail log location”.

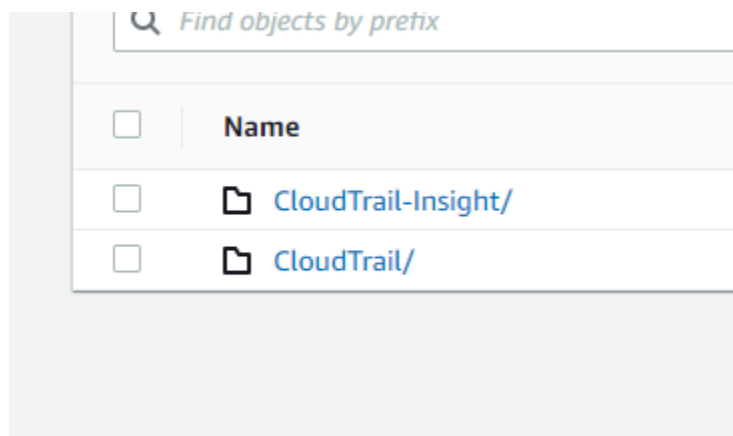
CloudTrail publishes log files to your S3 bucket in a gzip archive. In the S3 bucket, the log file has a formatted name.

The following syntax shows the log file location.


Path: bucket_name/prefix_name/AWSLogs/Account_ID


















Trail log location
aws-cloudtrail-management-
events-logs-270463904202-
ebba162b/AWSLogs/27046390420
2

Step 31: Click on “CloudTrail” directory.



Step 32: Click on the “us-east-1” directory.



<input type="checkbox"/>	Name	▲	Type
<input type="checkbox"/>	 ap-northeast-1/		Folder
<input type="checkbox"/>	 ap-northeast-2/		Folder
<input type="checkbox"/>	 ap-northeast-3/		Folder
<input type="checkbox"/>	 ap-south-1/		Folder
<input type="checkbox"/>	 ap-southeast-1/		Folder
<input type="checkbox"/>	 ap-southeast-2/		Folder
<input type="checkbox"/>	 ca-central-1/		Folder
<input type="checkbox"/>	 eu-central-1/		Folder
<input type="checkbox"/>	 eu-north-1/		Folder
<input type="checkbox"/>	 eu-west-1/		Folder
<input type="checkbox"/>	 eu-west-2/		Folder
<input type="checkbox"/>	 eu-west-3/		Folder
<input type="checkbox"/>	 sa-east-1/		Folder
<input type="checkbox"/>	 us-east-1/		Folder
<input type="checkbox"/>	 us-east-2/		Folder
<input type="checkbox"/>	 us-west-1/		Folder
<input type="checkbox"/>	 us-west-2/		Folder

Click on the folder having the current year as name followed by month and date.

Now the current path will be the following.

Path: bucket_name/prefix_name/AWSLogs/Account ID/CloudTrail/region/YYYY/MM/DD/





Step 33: Check the log using the JSON files available.

Objects (4)

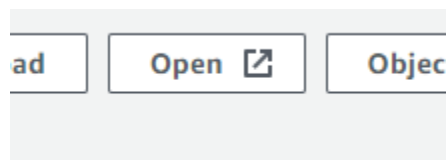
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket.

  Copy S3 URI  Copy URL  Download  Open  Delete

 Find objects by prefix

<input type="checkbox"/>	Name
<input type="checkbox"/>	 270463904202_CloudTrail_us-east-1_20220904T1620Z_atMxszimNPUBlIwb.json.gz
<input type="checkbox"/>	 270463904202_CloudTrail_us-east-1_20220904T1620Z_HrpY2xnvIQH9HPnw.json.gz
<input type="checkbox"/>	 270463904202_CloudTrail_us-east-1_20220904T1620Z_Pq06RU6eykuSKFXj.json.gz
<input type="checkbox"/>	 270463904202_CloudTrail_us-east-1_20220904T1625Z_d9M8msub7Xjl9yLr.json.gz

Step 34: Click on the “Open” button. It will open the JSON file in the browser.



This log is recorded while updating the DynamoDB table so the event name will be “UpdateTable”. This operation is done in order to perform Modifications in the provisioned throughput settings, global secondary indexes, or DynamoDB Streams settings for a given table.


```

    "invokedBy": "application-autoscaling.amazonaws.com"
  },
  "eventTime": "2022-09-04T16:16:28Z",
  "eventSource": "dynamodb.amazonaws.com",
  "eventName": "UpdateTable",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "errorCode": "ValidationException",
  "errorMessage": "2 validation errors detected: Value '-1' at 'provisionedThroughput.readCapacityUnits' fails to satisfy constraint: Member must have value greater than or equal to 1",
  "requestParameters": {
    "tableName": "Users",
    "provisionedThroughput": {
      "readCapacityUnits": -1,

```

This log is recorded while listing the DynamoDB table so the event name will be “ListTables”. This operation will return the list of table names available.

```

  "eventTime": "2022-09-04T16:16:29Z",
  "eventSource": "dynamodb.amazonaws.com",
  "eventName": "ListTables",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "968NMAA31ARGVG4IPS04A97UM3VV4KQNS05AEMVJF66Q9ASUAAJG",
  "eventID": "c4df7658-9314-4339-99cf-91c966381cc1",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "arn": "arn:aws:dynamodb:us-east-1:123456789012:table/Users"

```

This log is recorded while creating the DynamoDB table so the event name will be “CreateTable”. The CreateTable operation adds a new table to your account.

```

    }
  },
  "eventTime": "2022-09-04T16:16:28Z",
  "eventSource": "dynamodb.amazonaws.com",
  "eventName": "CreateTable",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "attributeDefinitions": [
      {
        "attributeName": "id",

```

These are some of the logs available in the management events buckets.

Step 35: Click on “student-data-events”.



	events	virginia)
<input type="radio"/>	student-data-events	US East (N. Virginia)

Step 36: Click on “Trail log location”.

The trail location of data events is similar to the management events.

Trail log location
[aws-cloudtrail-data-events-logs-270463904202-10df1aad/AWSLogs/270463904202](#)

Step 37: Check the log using the JSON files available.

<input type="text" value="Find objects by prefix"/>	
<input type="checkbox"/>	Name
<input type="checkbox"/>	 270463904202_CloudTrail_us-east-1_20220904T1625Z_eOiUJcBV2g85mfY9.json.gz
<input type="checkbox"/>	 270463904202_CloudTrail_us-east-1_20220904T1625Z_okNmaeuObPmmy01L.json.gz

This log is recorded while adding items to the DynamoDB table so the event name will be "PutItem". This operation creates a new item, or replaces an old item with a new item.

```

"eventTime": "2022-09-04T16:20:44Z",
"eventSource": "dynamodb.amazonaws.com",
"eventName": "PutItem",
"awsRegion": "us-east-1",
"sourceIPAddress": "AWS Internal",
"userAgent": "AWS Internal",
▼ "requestParameters": {
  "tableName": "Users",
  ▼ "key": {
    "id": "0"
  },
  ▼ "items": [
    "id",
    "Name"
  ],
  "conditionExpression": "#pk <> :pkValue",
  ▼ "expressionAttributeNames": {
    "#pk": "id"
  }
}

```

This log is recorded while listing a single item in the DynamoDB table so the event name will be "GetItem". This operation returns a set of attributes for the item with the given primary key.


```

},
"eventTime": "2022-09-04T16:20:44Z",
"eventSource": "dynamodb.amazonaws.com",
"eventName": "GetItem",
"awsRegion": "us-east-1",
"sourceIPAddress": "AWS Internal",
"userAgent": "AWS Internal",
▼ "requestParameters": {
  "tableName": "Users",
  ▼ "key": {
    "id": "0"
  },
  "consistentRead": true
},
"responseElements": null,
"requestID": "85ARRFC13GOAQU0C51PR7VLED7VV4KQNS05AEMVJF66Q9ASUAAJG",
"eventID": "8c20ee77-5398-46b1-9c4d-773ad0081a26",
"readOnly": true,
▼ "resources": [
  - ,

```

Step 38: Navigate back to CloudTrail Event history and check out the available events. It will list all the events and also can view the events according to the selected filter such as resource name , resource type etc.

<input type="checkbox"/>	DescribeTable	September 05, 2022, 15:41:19 (...)	student	dynamodb.amazonaws.com
<input type="checkbox"/>	DescribeTable	September 05, 2022, 15:41:19 (...)	student	dynamodb.amazonaws.com
<input type="checkbox"/>	DescribeTable	September 05, 2022, 15:41:06 (...)	student	dynamodb.amazonaws.com
<input type="checkbox"/>	DescribeTable	September 05, 2022, 15:40:58 (...)	student	dynamodb.amazonaws.com
<input type="checkbox"/>	DescribeTable	September 05, 2022, 15:40:58 (...)	student	dynamodb.amazonaws.com
<input type="checkbox"/>	CreateTable	September 05, 2022, 15:40:57 (...)	student	dynamodb.amazonaws.com
<input type="checkbox"/>	DescribeTable	September 05, 2022, 15:40:57 (...)	student	dynamodb.amazonaws.com
<input type="checkbox"/>	UpdateTable	September 05, 2022, 15:40:57 (...)	student	dynamodb.amazonaws.com
<input type="checkbox"/>	DescribeTable	September 05, 2022, 15:40:56 (...)	student	dynamodb.amazonaws.com



Successfully created trails for logging operations that are performed on resources of the AWS account.

References:

1. AWS CloudTrail
(<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>)