

CLOUD TRAIL

AWS CloudTrail is an application programming interface (API) call-recording and log-monitoring service offered by Amazon Web Services (AWS). AWS CloudTrail enables AWS customers to record API calls, sending log files to Amazon Simple Storage Service (Amazon S3) buckets for storage. The service provides the following API activity data:

- The identity of an API caller.
- The time of an API call.
- The source of the IP address of an API caller.
- The request parameters.
- The response elements returned by the AWS service.

CloudTrail publishes a notification for each log file delivered, enabling users to take action upon log file delivery -- a process that takes about five minutes, according to AWS. It can also be configured to aggregate log files across multiple accounts so that log files are delivered to a single S3 bucket.

CloudTrail can facilitate regulatory compliance reporting for organizations that use AWS and need to track the API calls for one or more AWS accounts. The service can also be configured to support security information and event management platforms and resource management.

CloudTrail integrates with AWS services such as CloudWatch, Elasticsearch, Lambda, Simple Notification Service and Simple Queue Service, as well as third-party monitoring platforms.

There are some AWS API tools that CloudTrail does not work with, however, including Sumerian, WorkSpaces Application Manager, Deep Learning Amazon Machine Image, DeepComposer, DeepLens, DeepRacer and Snowmobile.

Key Features of AWS CloudTrail

❖ **Event Logging:**

CloudTrail records AWS API calls for your account and delivers log files to an Amazon S3 bucket that you specify. This includes API calls made via the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

❖ **Management Events:**

CloudTrail captures management events which provide information about management operations performed on resources in your AWS account. Examples include creating, modifying, and deleting EC2 instances, IAM roles, and S3 buckets.

❖ **Data Events:**

Data events provide visibility into the resource operations performed on or in your resource. These are often high-volume activities. Examples include Amazon S3 object-level API activity (GetObject, PutObject, etc.) and AWS Lambda function invocations.

❖ **Insights:**

CloudTrail Insights can detect unusual activity in your AWS account. It helps identify and respond to operational issues more quickly by recognizing patterns of unusual activity.

❖ **Compliance:**

CloudTrail helps you comply with internal policies and regulatory standards by ensuring all account activity is logged and auditable.

❖ **Integration with AWS Services:**

CloudTrail integrates with other AWS services like Amazon CloudWatch, AWS Lambda, and Amazon Athena, allowing you to set up automated responses to specific activities or analyze logs with SQL queries.

Use Cases for AWS CloudTrail

❖ **Security Analysis:**

Identify who made changes to your resources and when, enabling you to detect unauthorized access or activities.

❖ **Operational Troubleshooting:**

Track changes to your AWS resources and investigate operational issues by examining changes and actions taken over time.

❖ **Compliance and Auditing:**

Maintain a comprehensive log of activities to meet regulatory and compliance requirements, ensuring that you have a traceable history of activity.

❖ Resource Management and Change Tracking:

Monitor and record user activities and API calls to manage your resources efficiently and track changes over time.

How CloudTrail Works

Create a Trail:

A trail is a configuration that enables delivery of events to an S3 bucket. You can configure a trail to apply to all regions or a single region.

Event Log Files:

CloudTrail delivers log files to your specified S3 bucket. You can specify how often the log files are delivered (e.g., every 5 minutes).

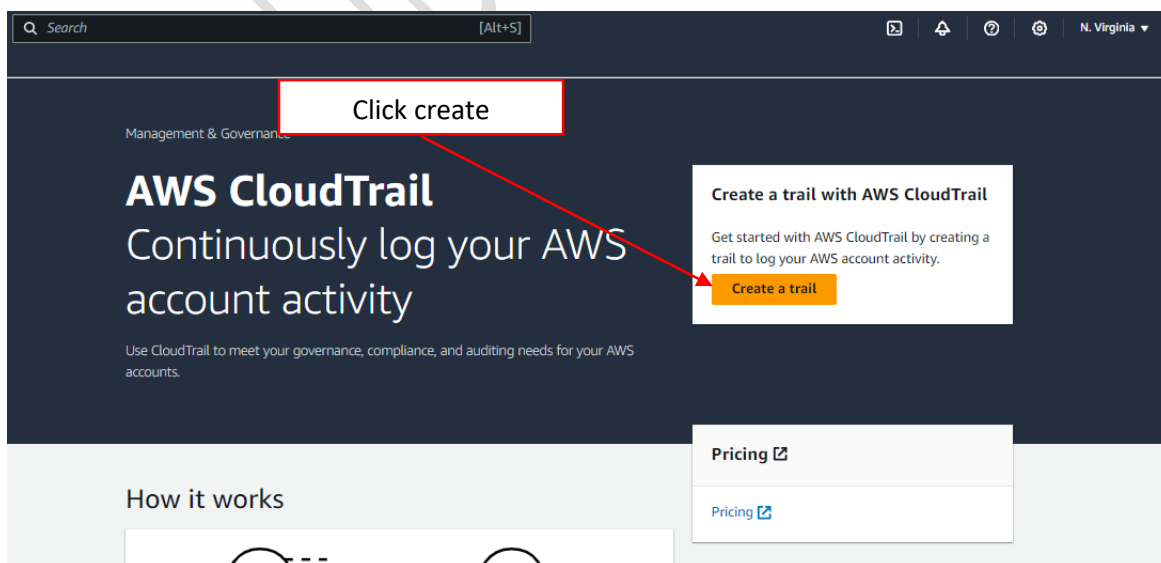
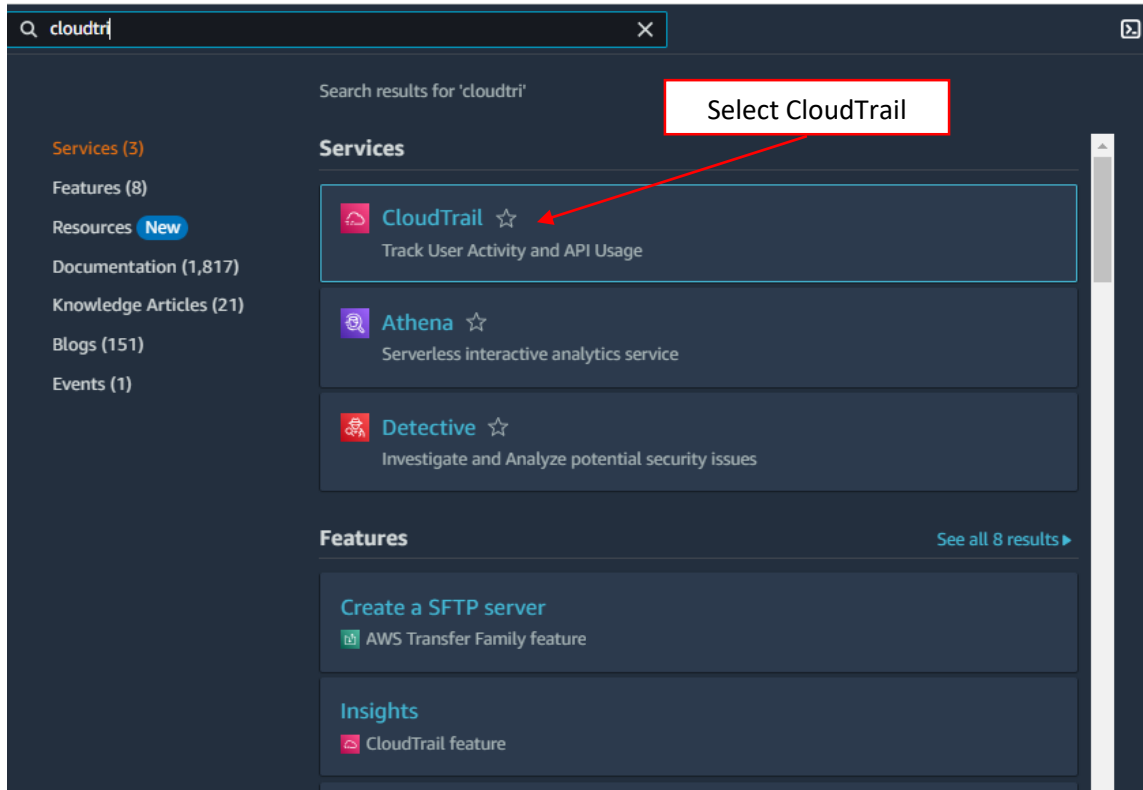
Viewing and Querying Logs:

Use the CloudTrail console to view recent events. For deeper analysis, integrate with CloudWatch Logs or use Athena to query the logs stored in S3.

By providing a history of AWS API calls for your account, AWS CloudTrail helps you manage risk, secure your AWS environment, and comply with best practices and regulatory standards.

CREATE A CLOUD TRAIL, GENERATING AND VIEWING EVENTS THROUGH EC2 INSTANCE

Step 1 : Add a new CloudTrail



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](#)

Mention a name

Trail name

Enter a display name for your trail.

cloudinstitution-trial_x


3-128 characters. Only letters, numbers, periods, underscores,

Automatically creates a bucket

Trail log bucket and folder

aws-cloudtrail-logs-473869189128-fdbae129

Logs will be stored in aws-cloudtrail-logs-473869189128-fdbae129/AWSLogs/473869189128

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

Click create

Cancel

Create trail

The S3 bucket is the designated destination for storing log files. All events related to API calls are captured and recorded in logs, which are then delivered to the S3 bucket.

Trail created successfully

CloudTrail > Trails

Trails


Copy events to Lake



Delete

Create trail



Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
cloudinstitution-trial_x	US East (N. Virginia)	Yes	Disabled	No	aws-cloudtrail-logs-473869189128-fdbae129	-	-	 Logging

Click on the Trail

CloudTrail ×

CloudTrail > Trails > arn:aws:cloudtrail:us-east-1:473869189128:trail/cloudinstitution-trial_x

cloudinstitution-trial_x Delete Stop logging

General details Edit





Trail logging ✔ Logging	Trail log location aws-cloudtrail-logs-473869189128-fdbae129/AWSLogs/473869189128 🔗	Log file validation Disabled	SNS notification delivery Disabled
Trail name cloudinstitution-trial_x		Last file validation delivered -	Last SNS notification -
Multi-region trail Yes	Last log file delivered May 31, 2024, 18:20:53 (UTC+05:30)		
Apply trail to my organization Not enabled	Log file SSE-KMS encryption Not enabled		

Step 2 : Go to S3 bucket

Q s3 ×

Search results for 's3'

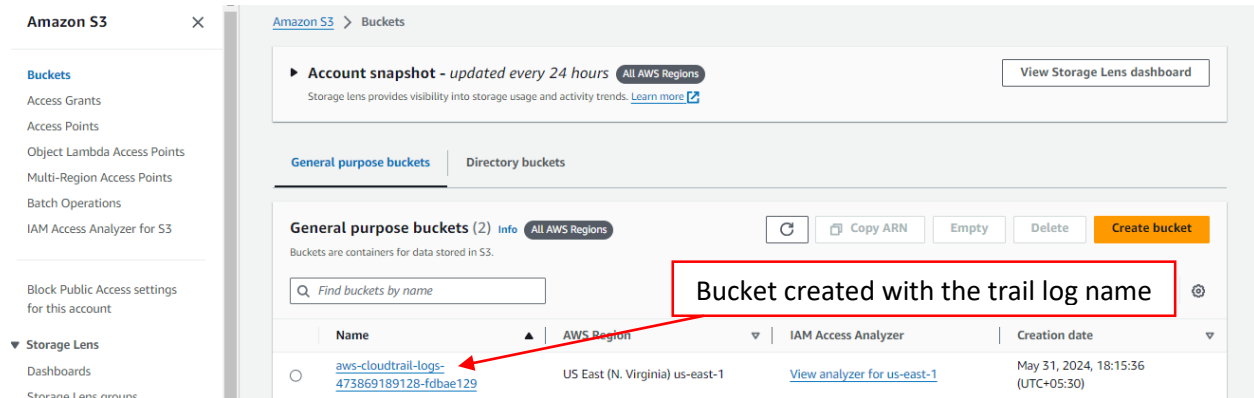
Services See all 8 results ▶

-  **S3** ☆
Scalable Storage in the Cloud
-  **S3 Glacier** ☆
Archive Storage in the Cloud
-  **AWS Snow Family** ☆
Large Scale Data Transport
-  **Storage Gateway** ☆
Hybrid Storage Integration

Features See all 39 results ▶

Now go to S3 bucket

In the bucket table, click the name of your bucket



Amazon S3

Buckets

Account snapshot - updated every 24 hours (All AWS Regions)

View Storage Lens dashboard

General purpose buckets | Directory buckets

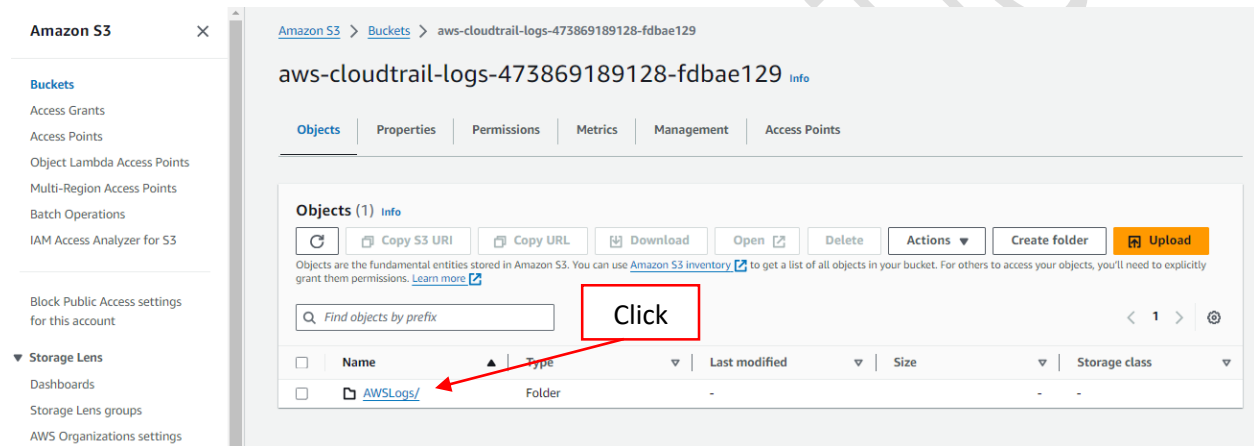
General purpose buckets (2) Info (All AWS Regions)

Buckets are containers for data stored in S3.

Find buckets by name

Bucket created with the trail log name

Name	AWS Region	IAM Access Analyzer	Creation date
aws-cloudtrail-logs-473869189128-fdbae129	US East (N. Virginia) us-east-1	View analyzer for us-east-1	May 31, 2024, 18:15:36 (UTC+05:30)



Amazon S3

Buckets

aws-cloudtrail-logs-473869189128-fdbae129 Info

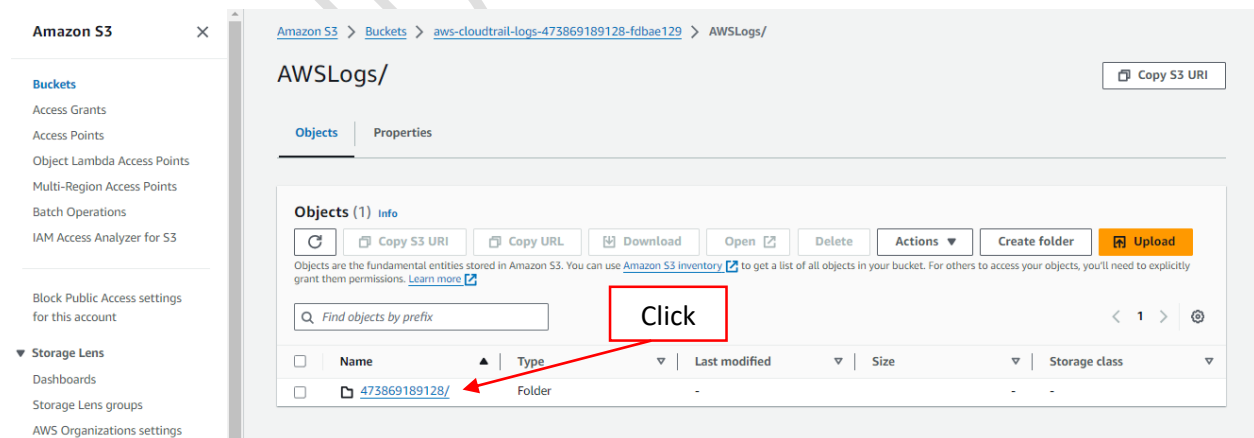
Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (1) Info

Find objects by prefix

Click

Name	Type	Last modified	Size	Storage class
AWSLogs/	Folder	-	-	-



Amazon S3

Buckets

aws-cloudtrail-logs-473869189128-fdbae129 > AWSLogs/

Copy S3 URI

Objects | Properties

Objects (1) Info

Find objects by prefix

Click

Name	Type	Last modified	Size	Storage class
473869189128/	Folder	-	-	-

Amazon S3

Buckets

- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Amazon S3 > Buckets > aws-cloudtrail-logs-473869189128-fdbae129 > AWSLogs/ > 473869189128/

473869189128/ Copy S3 URI

Objects Properties

Objects (1) Info

Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

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. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

Click

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	CloudTrail/	Folder	-	-	-

Amazon S3

Buckets

- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Amazon S3 > Buckets > aws-cloudtrail-logs-473869189128-fdbae129 > AWSLogs/ > 473869189128/ > CloudTrail/

CloudTrail/ Copy S3 URI

Objects Properties

Objects (1) Info

Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

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. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

Click

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	us-east-1/	Folder	-	-	-

Amazon S3

Buckets

- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Amazon S3 > Buckets > aws-cloudtrail-logs-473869189128-fdbae129 > AWSLogs/ > 473869189128/ > CloudTrail/ > us-east-1/

us-east-1/ Copy S3 URI

Objects Properties

Objects (1) Info

Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

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. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

Click

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	2024/	Folder	-	-	-

Amazon S3

- Buckets
- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3
- Block Public Access settings for this account
- Storage Lens
 - Dashboards
 - Storage Lens groups
 - AWS Organizations settings

Amazon S3 > Buckets > aws-cloudtrail-logs-473869189128-fdbae129 > AWSLogs/ > 473869189128/ > CloudTrail/ > us-east-1/ > 2024/

2024/

Copy S3 URI

Objects Properties

Objects (1) Info

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

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. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

Click

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	05/	Folder	-	-	-

Amazon S3

- Buckets
- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3
- Block Public Access settings for this account
- Storage Lens
 - Dashboards
 - Storage Lens groups
 - AWS Organizations settings

Amazon S3 > Buckets > aws-cloudtrail-logs-473869189128-fdbae129 > AWSLogs/ > 473869189128/ > CloudTrail/ > us-east-1/ > 2024/ > 05/

05/

Copy S3 URI

Objects Properties

Objects (1) Info

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

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. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

Click

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	31/	Folder	-	-	-

Here we have a log file created

Amazon S3

- Buckets
- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3
- Block Public Access settings for this account
- Storage Lens
 - Dashboards
 - Storage Lens groups
 - AWS Organizations settings
- Feature spotlight

Amazon S3 > Buckets > aws-cloudtrail-logs-473869189128-fdbae129 > AWSLogs/ > 473869189128/ > CloudTrail/ > us-east-1/ > 2024/ > 05/ > 31/

31/

Copy S3 URI

Objects Properties

Objects (5) Info

Copy S3 URI

Copy URL

Download

Open

Delete

Actions


Create folder

Upload

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. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

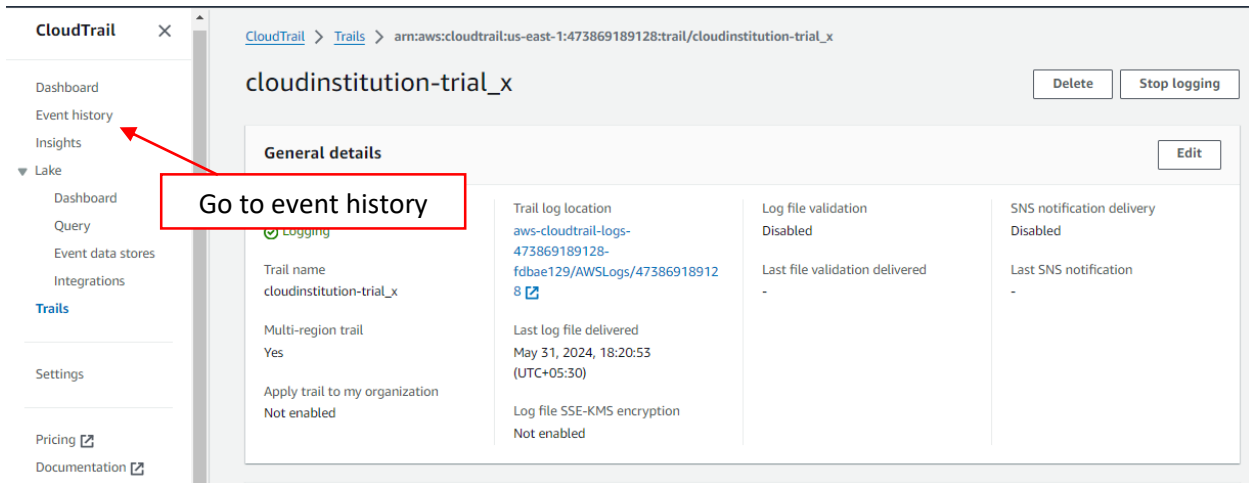
Find objects by prefix

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	473869189128_CloudTrail_us-east-1_20240531T1250Z_AVIYXj7ciGK1SAIN.json.gz	gz	May 31, 2024, 18:20:43 (UTC+05:30)	1.8 KB	Standard


Cloud Institution

No 15,20th Main , 100 ft ring Road, BTM Layout 2nd stage , Bangalore – 560076 <https://cloudinstitution.com/>

Step 3 : On the Cloud Trail Dashboard



CloudTrail

cloudinstitution-trial_x

General details

Trail log location: [aws-cloudtrail-logs-473869189128-fdbae129/AWSLogs/473869189128](#)

Trail name: cloudinstitution-trial_x

Multi-region trail: Yes

Apply trail to my organization: Not enabled

Log file validation: Disabled

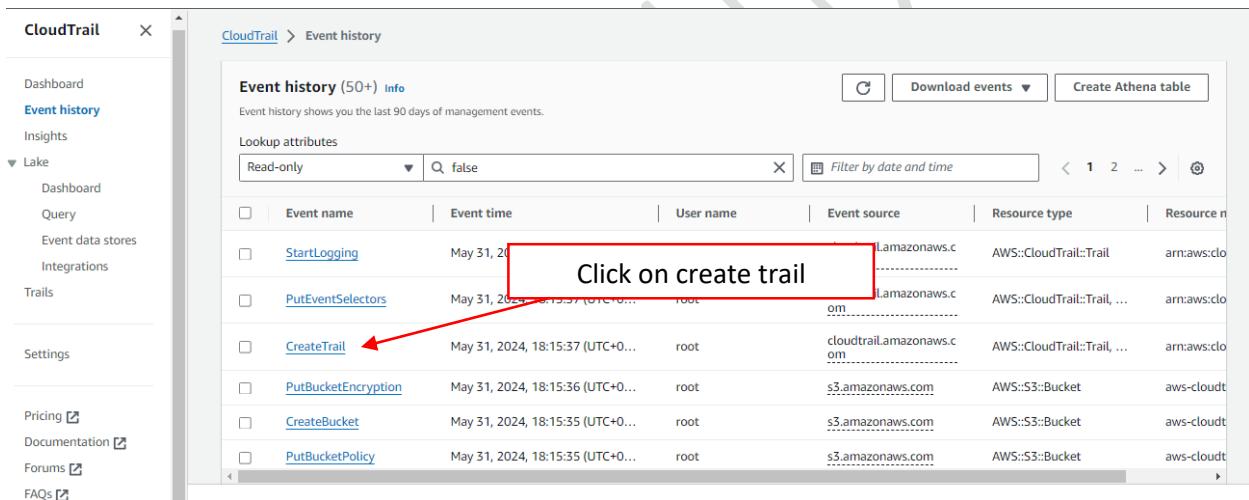
Last file validation delivered: -

Log file SSE-KMS encryption: Not enabled

SNS notification delivery: Disabled

Last SNS notification: -

Go to event history



CloudTrail

Event history (50+) Info

Event history shows you the last 90 days of management events.

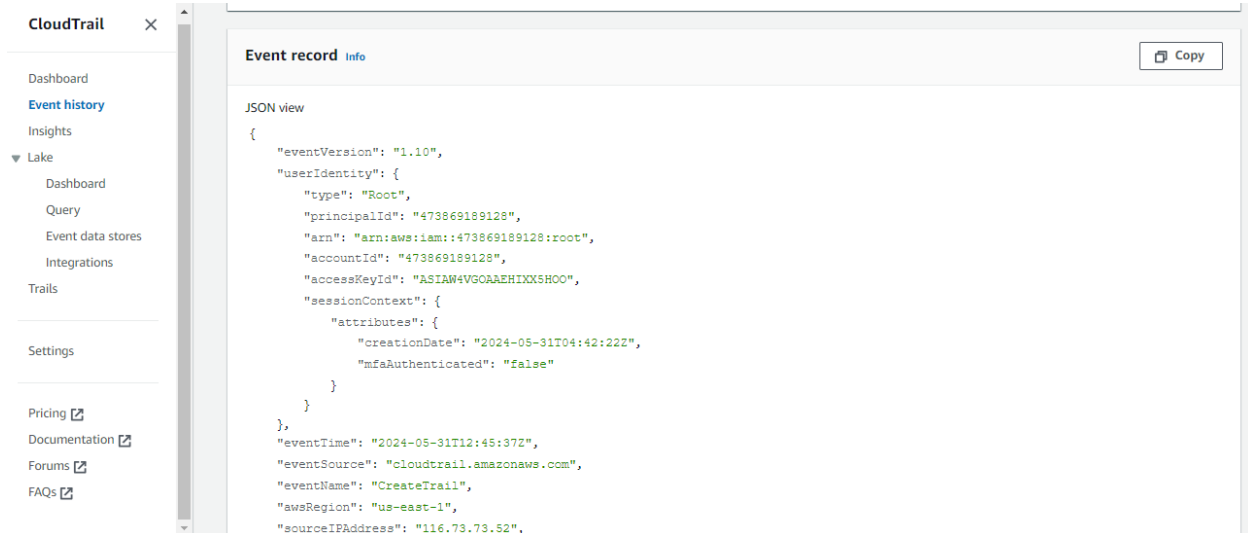
Lookup attributes: Read-only, Q false

Filter by date and time: < 1 2 ... >

Event name	Event time	User name	Event source	Resource type	Resource name
StartLogging	May 31, 2024, 18:15:35 (UTC+05:30)	root	amazonaws.com	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-1:473869189128:trail/cloudinstitution-trial_x
PutEventSelectors	May 31, 2024, 18:15:37 (UTC+05:30)	root	amazonaws.com	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-1:473869189128:trail/cloudinstitution-trial_x
CreateTrail	May 31, 2024, 18:15:37 (UTC+05:30)	root	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-1:473869189128:trail/cloudinstitution-trial_x
PutBucketEncryption	May 31, 2024, 18:15:36 (UTC+05:30)	root	s3.amazonaws.com	AWS::S3::Bucket	aws-cloudtrail-logs-473869189128-fdbae129
CreateBucket	May 31, 2024, 18:15:35 (UTC+05:30)	root	s3.amazonaws.com	AWS::S3::Bucket	aws-cloudtrail-logs-473869189128-fdbae129
PutBucketPolicy	May 31, 2024, 18:15:35 (UTC+05:30)	root	s3.amazonaws.com	AWS::S3::Bucket	aws-cloudtrail-logs-473869189128-fdbae129

Click on create trail

In the event record, scroll down and search for the created trail



The screenshot shows the AWS CloudTrail console. On the left is a navigation menu with options like Dashboard, Event history, Insights, Lake, Trails, and Settings. The main area displays an 'Event record' for the 'CreateTrail' event. The JSON view shows the following details:

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Root",
    "principalId": "473869189128",
    "arn": "arn:aws:iam:473869189128:root",
    "accountId": "473869189128",
    "accessKeyId": "ASIAW4VG0AAEHIXXSHOO",
    "sessionContext": {
      "attributes": {
        "creationDate": "2024-05-31T04:42:22Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-05-31T12:45:37Z",
  "eventSource": "cloudtrail.amazonaws.com",
  "eventName": "CreateTrail",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "116.73.73.52",
```

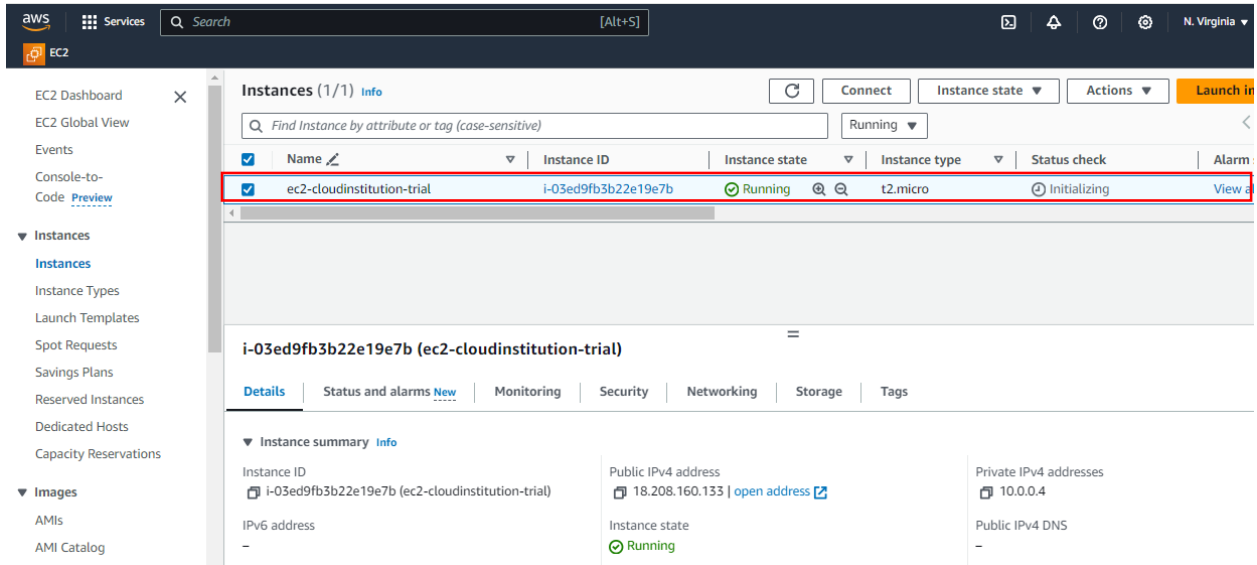


This screenshot shows the 'requestParameters' section of the 'CreateTrail' event record. The parameters are as follows:

```
{
  "name": "cloudinstitution-trial_x",
  "s3BucketName": "aws-cloudtrail-logs-473869189128-fdbae129",
  "includeGlobalServiceEvents": true,
  "isMultiRegionTrail": true,
  "enableLogFileValidation": false,
  "isOrganizationTrail": false
},
"responseElements": {
  "name": "cloudinstitution-trial_x",
  "s3BucketName": "aws-cloudtrail-logs-473869189128-fdbae129",
  "includeGlobalServiceEvents": true,
  "isMultiRegionTrail": true,
  "trailARN": "arn:aws:cloudtrail:us-east-1:473869189128:trail/cloudinstitution-trial_x",
  "logFileValidationEnabled": false,
  "isOrganizationTrail": false
}
```

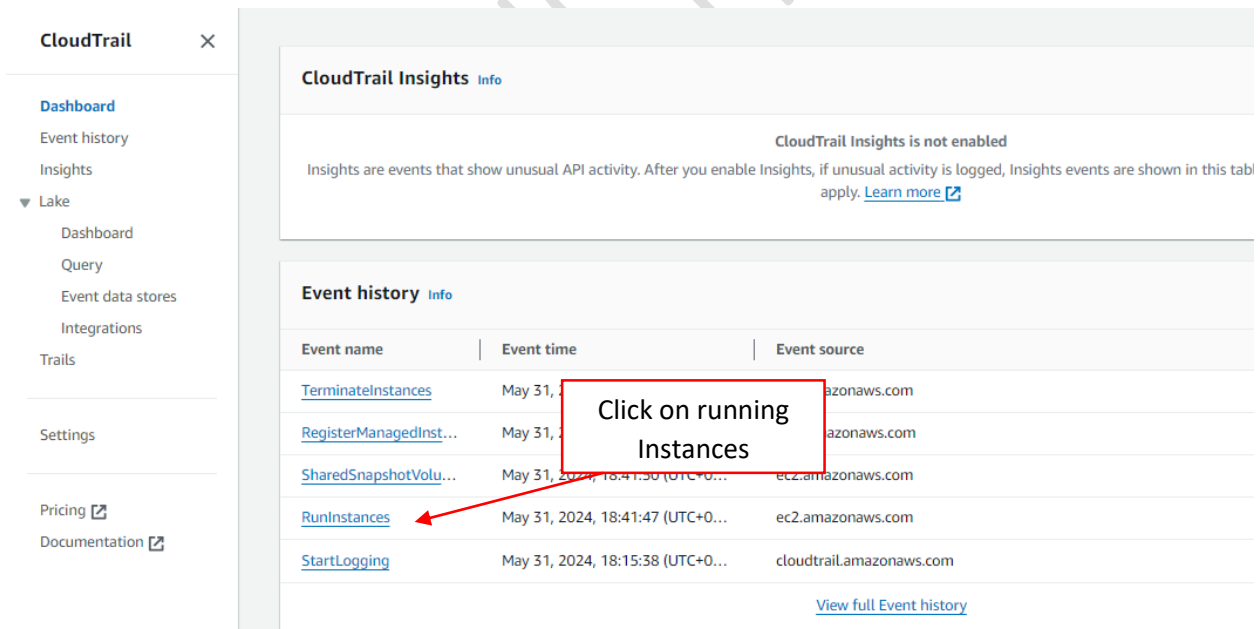
Here we can see the name of the trail, bucket name and region etc

Step 4 : Create a EC2 instance



The screenshot shows the AWS Management Console interface for EC2 instances. The left sidebar contains navigation links for EC2 Dashboard, EC2 Global View, Events, Console-to-Code, and various instance management options. The main content area displays a list of instances under the heading 'Instances (1/1) Info'. A single instance, 'ec2-cloudinstitution-trial' (ID: i-03ed9fb3b22e19e7b), is listed and highlighted with a red border. Its state is 'Running' and its status check is 'Initializing'. Below the list, the details for this specific instance are shown, including its ID, public IPv4 address (18.208.160.133), private IPv4 address (10.0.0.4), and instance type (t2.micro).

Step 5: Now go back to cloud trail



The screenshot shows the AWS CloudTrail console. The left sidebar contains navigation links for CloudTrail, Dashboard, Event history, Insights, Lake, Trails, Settings, Pricing, and Documentation. The main content area displays the 'CloudTrail Insights' section, which is currently disabled. Below this, the 'Event history' table is shown. A red box highlights the 'RunInstances' event in the table, and a red arrow points to it. A text box with the text 'Click on running Instances' is overlaid on the table. The table lists several events, including 'TerminateInstances', 'RegisterManagedInst...', 'SharedSnapshotVolu...', 'RunInstances', and 'StartLogging'.

Event has been captured by cloud trail

CloudTrail

Dashboard

Event history

Insights

▼ Lake

Dashboard

Query

Event data stores

Integrations

Trails

Settings

Pricing

Documentation

```
groupSet: {},
"instancesSet": {
  "items": [
    {
      "instanceId": "i-03ed9fb3b22e19e7b",
      "imageId": "ami-00beae93a2d981137",
      "bootMode": "uefi-preferred",
      "currentInstanceBootMode": "legacy-bios",
      "instanceState": {
        "code": 0,
        "name": "pending"
      },
      "privateDnsName": "ip-10-0-0-4.ec2.internal",
      "keyName": "may-21-laptop",
      "amiLaunchIndex": 0,
      "productCodes": {},
      "instanceType": "t2.micro",
      "launchTime": 1717161107000,
      "placement": {
        "availabilityZone": "us-east-1a",
        "tenancy": "default"
      },
    },
  ],
}
```