Amazon CloudTrail

A Management Service

Case Study



**Introduction**

AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

CloudTrail is enabled on your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view recent events in the CloudTrail console by going to Event history. For an ongoing record of activity and events in your AWS account, [create a trail](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.html). For more information about CloudTrail pricing, see [AWS CloudTrail Pricing](http://aws.amazon.com/cloudtrail/pricing/).

Visibility into your AWS account activity is a key aspect of security and operational best practices. You can use CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account. Optionally, you can enable AWS CloudTrail Insights on a trail to help you identify and respond to unusual activity.

You can integrate CloudTrail into applications using the API, automate trail creation for your organization, check the status of trails you create, and control how users view CloudTrail events.

If you're new to AWS CloudTrail, this tutorial helps you learn how to use its features. In this tutorial, you review your recent AWS account activity in the CloudTrail console and examine an event. You then create a trail, which is an ongoing record of management event activity that is stored in an Amazon S3 bucket. Unlike **Event history**, this ongoing record is not limited to 90 days, logs events in all AWS Regions, and can help you meet your security and auditing needs over time.

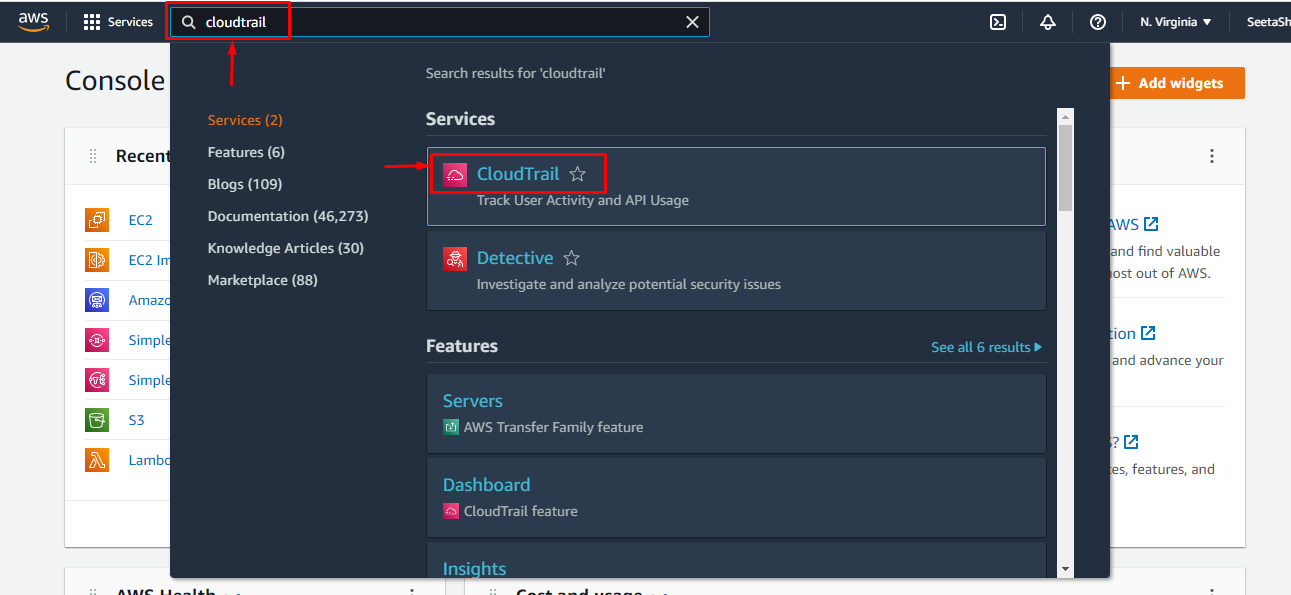
**Topics**

* Prerequisites
* Step 1: Review AWS account activity in event history
* Step 2: Create your first trail
* Step 3: View your log files
* Step 4: Plan for next steps

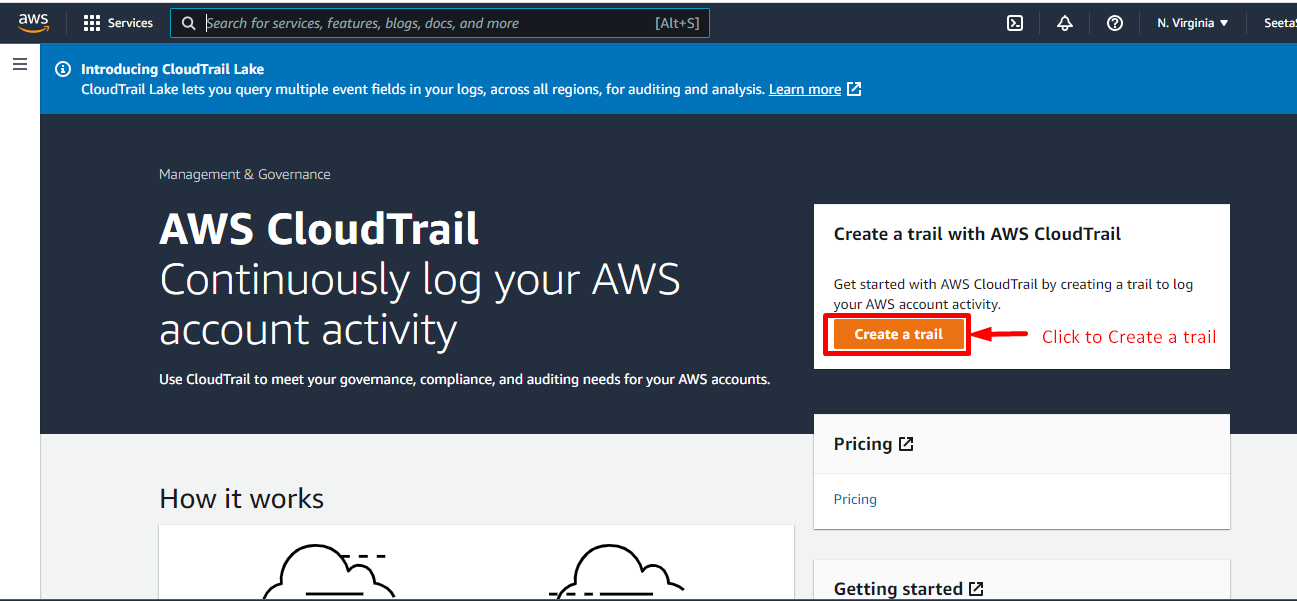
**Step 1: Review AWS account activity in event history**

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in any AWS service that supports CloudTrail, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. In other words, you can view, search, and download recent events in your AWS account before creating a trail, though creating a trail is important for long-term records and auditing of your AWS account activity. Unlike a trail, **Event history** only shows events that have occurred over the last 90 days.

1. Sign in to the AWS Management Console using the IAM user you configured for CloudTrail administration. Open the CloudTrail console



Click to create a cloud trail



Enter trail name

And click on Create cloud trail.

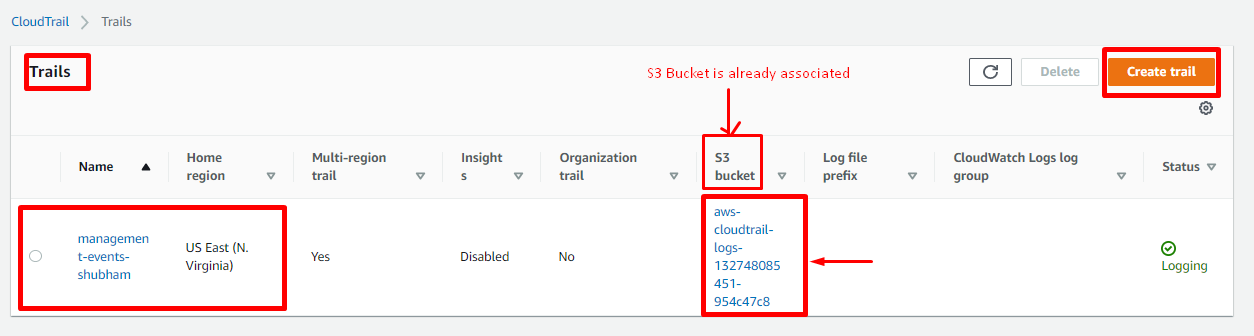
Leave default settings for AWS Organizations organization trails. This option won't be available to change unless you have accounts configured in Organizations.

Graphical user interface, text, application, Teams

Description automatically generated

Your trail is created and associated with S3 bucket.

If any activity you will do in S3 service it will reflect in cloud trail logs.

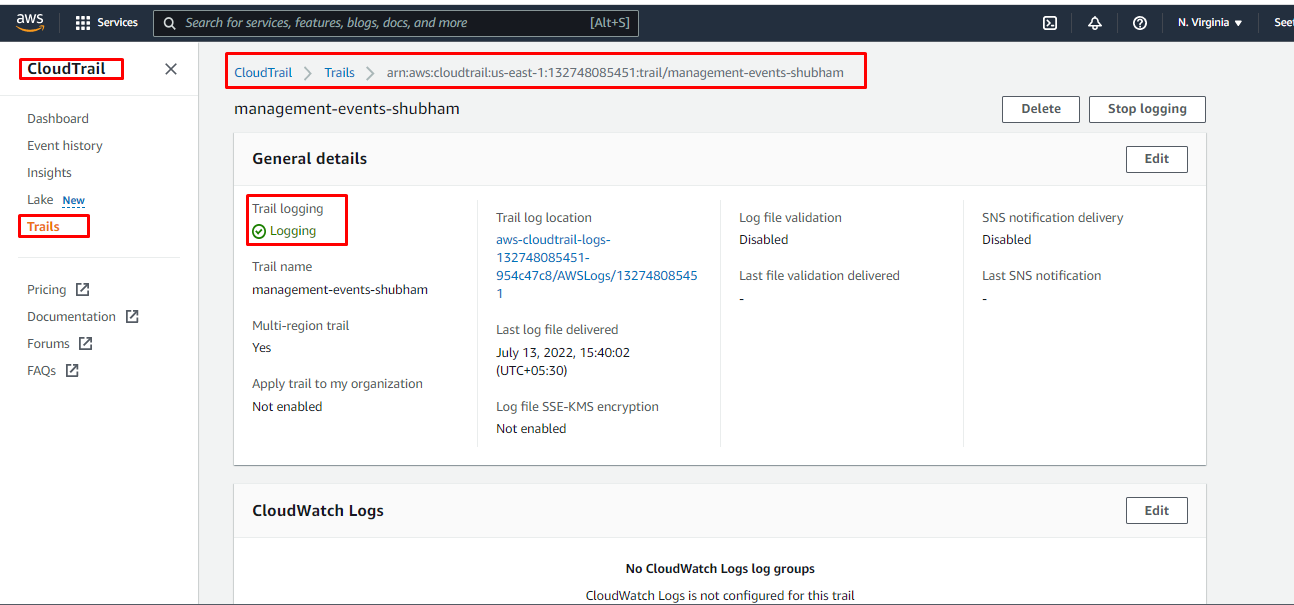


To make it easier to find your logs, create a new folder (also known as a prefix) in an existing bucket to store your CloudTrail logs.

**Step 2: View your log files**

Within an average of about 15 minutes of creating your first trail, CloudTrail delivers the first set of log files to the Amazon S3 bucket for your trail. You can look at these files and learn about the information they contain.

1.In the navigation pane, choose **Trails**. On the **Trails** page, find the name of the trail you just created.



Now go to S3 and create one Bucket, folder and upload any items in it.

You can see in Cloud Watch >> Event History >> its showing just logined in S3 bucket

Recently done activities.

Graphical user interface, application

Description automatically generated

Log Bucket is Automatically get created in S3. Will all log details.

Graphical user interface, application, Word

Description automatically generated

If I select one S3 Bucket then we have to check box and open it.

Graphical user interface, text, application, email

Description automatically generated

Now just simply upload one object in that Bucket

Graphical user interface, text, application, email

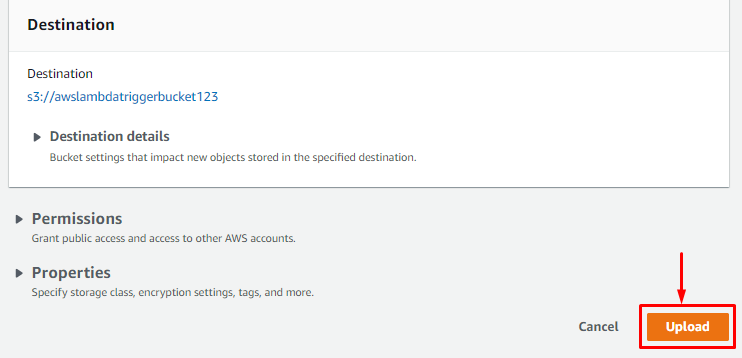
Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated



Now I have uploaded one csv file in S3 Bucket.

Graphical user interface, text, application

Description automatically generated

It will take some time for updating logs in dashboard.

Graphical user interface, application, email

Description automatically generated