CloudTrail

- ❑ AWS Cloud Trail is a web service that records AWS API calls for your account and delivers log files to you.
- ❑ The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.
- ❑ We can view Event history only last 90 days , if we want more than we need to create a trail

1) **View event history for your AWS account**

You can view and search the last 90 days of events recorded by Cloud Trail in the Cloud Trail console or by using the AWS CLI.

2) **Download events**

You can download a CSV or JSON file containing up to the past 90 days of Cloud Trail events for your AWS account.

3) **Create a trail**

A trail enables Cloud Trail to deliver log files to your Amazon S3 bucket.

By default, when you create a trail in the console, the trail applies to all regions.

The trail logs events from all regions in the AWS partition and delivers the log files to the S3 bucket that you specify

1) **Create and subscribe to an Amazon SNS topic**

Subscribe to a topic to receive notifications about log file delivery to your bucket. Amazon SNS can notify you in multiple ways, including programmatically with Amazon Simple Queue Service. Note: If you want to receive SNS notifications about log file deliveries from all regions, specify only one SNS topic for your trail.

2) **View your log files**

Use Amazon S3 to retrieve log files

3) **Manage user permissions**

Use AWS Identity and Access Management (IAM) to manage which users have permissions to create, configure, or delete trails; start and stop logging; and access buckets that have log files.

Questions?