CloudTrail

- 1 Intro
  - 1 AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account
  - 2 Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.
  - 3 Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.
- 2 How Cloud Trail Works
  - 1 CloudTrail is enabled on your AWS account when you create it.
  - 2 When activity occurs in your AWS account, that activity is recorded in a CloudTrail event.
    - The recorded information includes the identity of the user, the start time of the AWS API call, the source IP address, the request parameters, and the response elements returned by the service.
  - 3 You can easily view recent events in the CloudTrail console by going to Event history
    - Event history allows you to view, search, and download the past 90 days of activity in your AWS account.
  - 4 For an ongoing record of activity and events in your AWS account, create a trail.
- 3 What is Trail
  - 1 A trail is a configuration that enables delivery of events to an Amazon S3 bucket that you specify.
  - 2 For an ongoing record of activity and events in your AWS account, create a trail.
  - 3 You can also deliver and analyze events in a trail with Amazon CloudWatch Logs and Amazon CloudWatch Events.
  - 4 CloudTrail typically delivers logs within an average of about 15 minutes of an API call
- 4 Logs Encryption
  - 1 By default, the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3).
  - 2 To provide a security layer that is directly manageable, you can instead use server-side encryption with AWS KMS–managed keys (SSE-KMS) for your CloudTrail log files.
- 5 CloudTrail Log File Integrity
  - 1 To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use CloudTrail log file integrity validation.
  - 2 This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing.
  - 3 This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
- 6 Changes to Global Service Event logs can be done via AWS CLI not AWS console