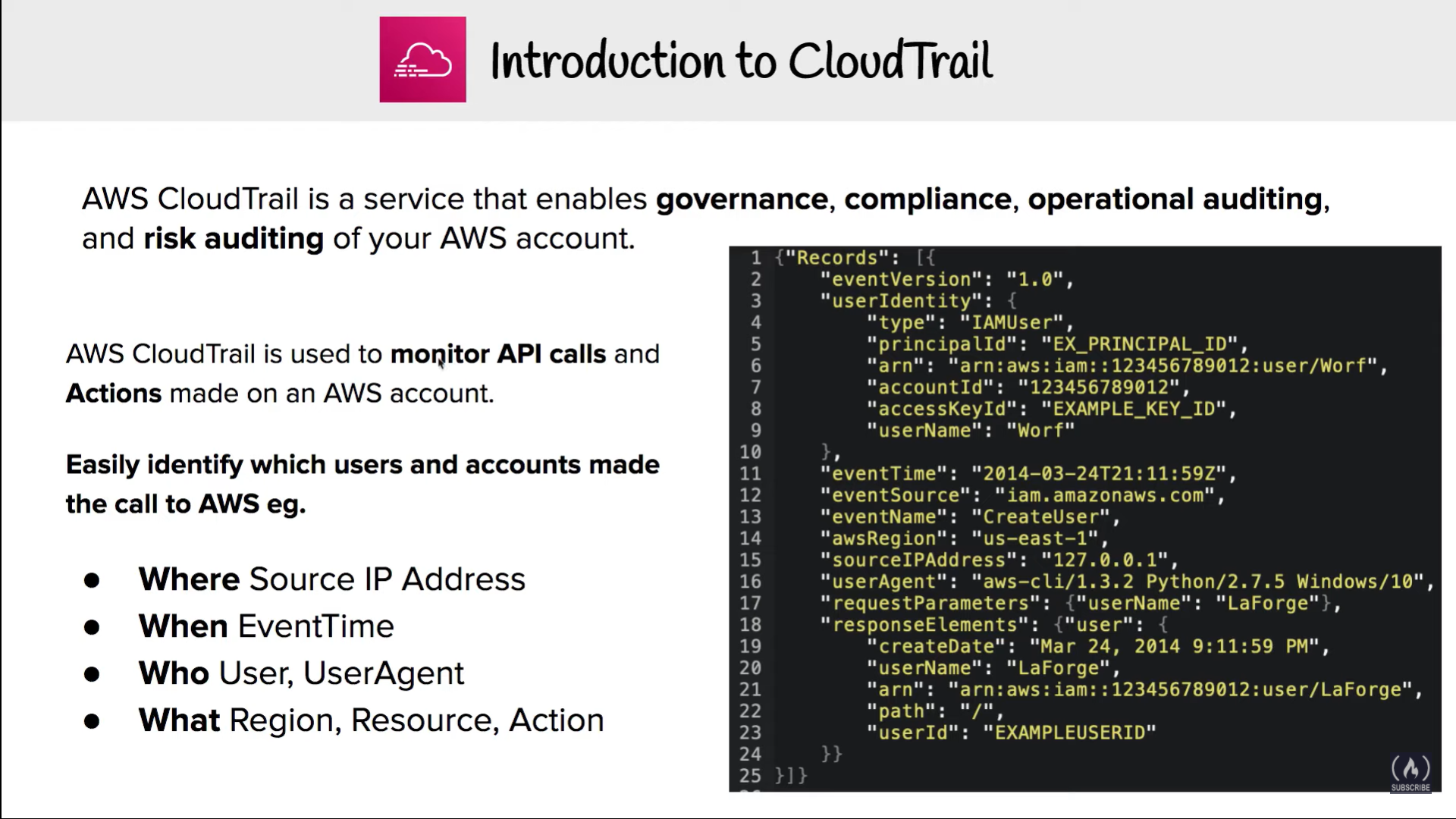
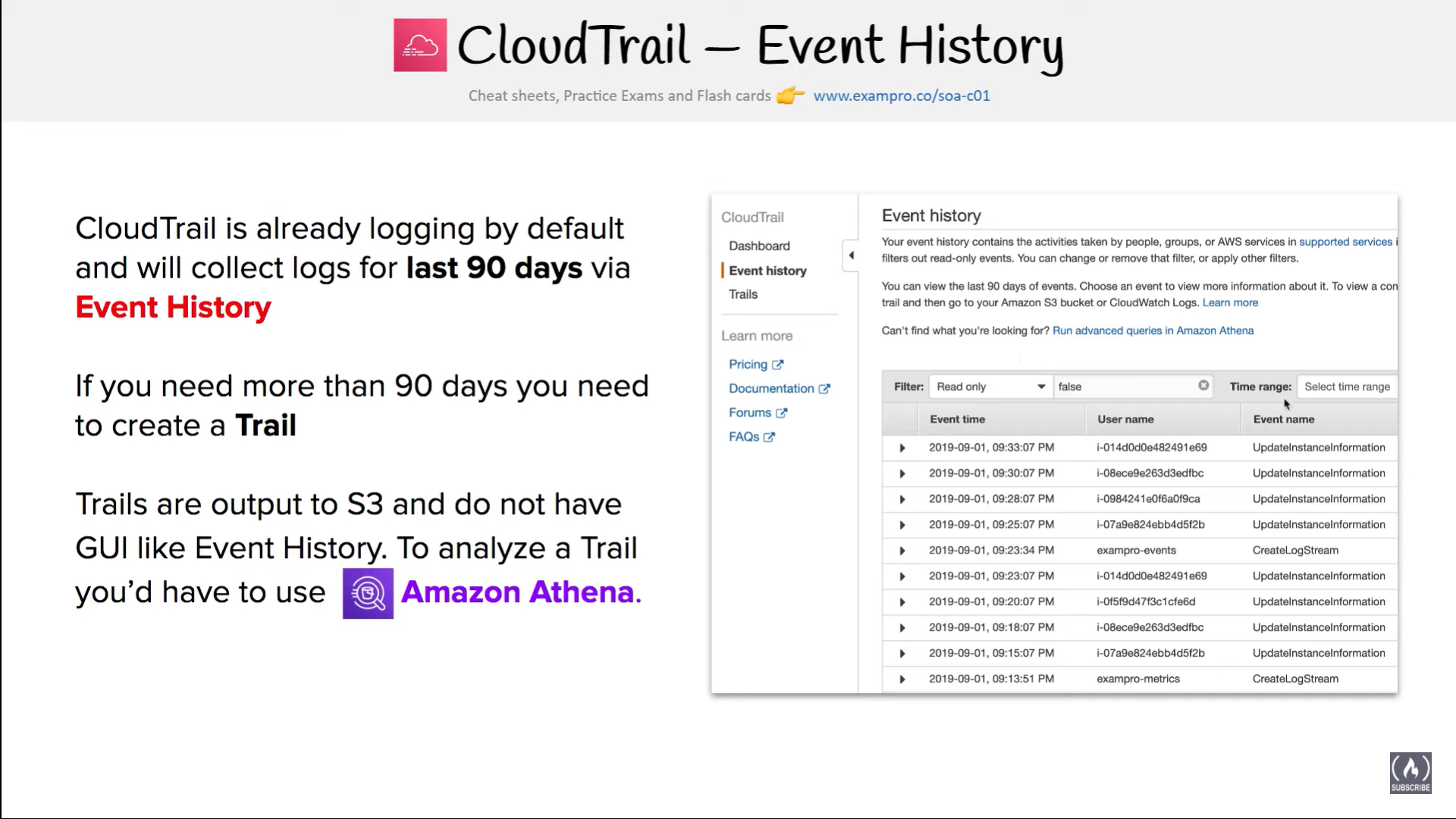
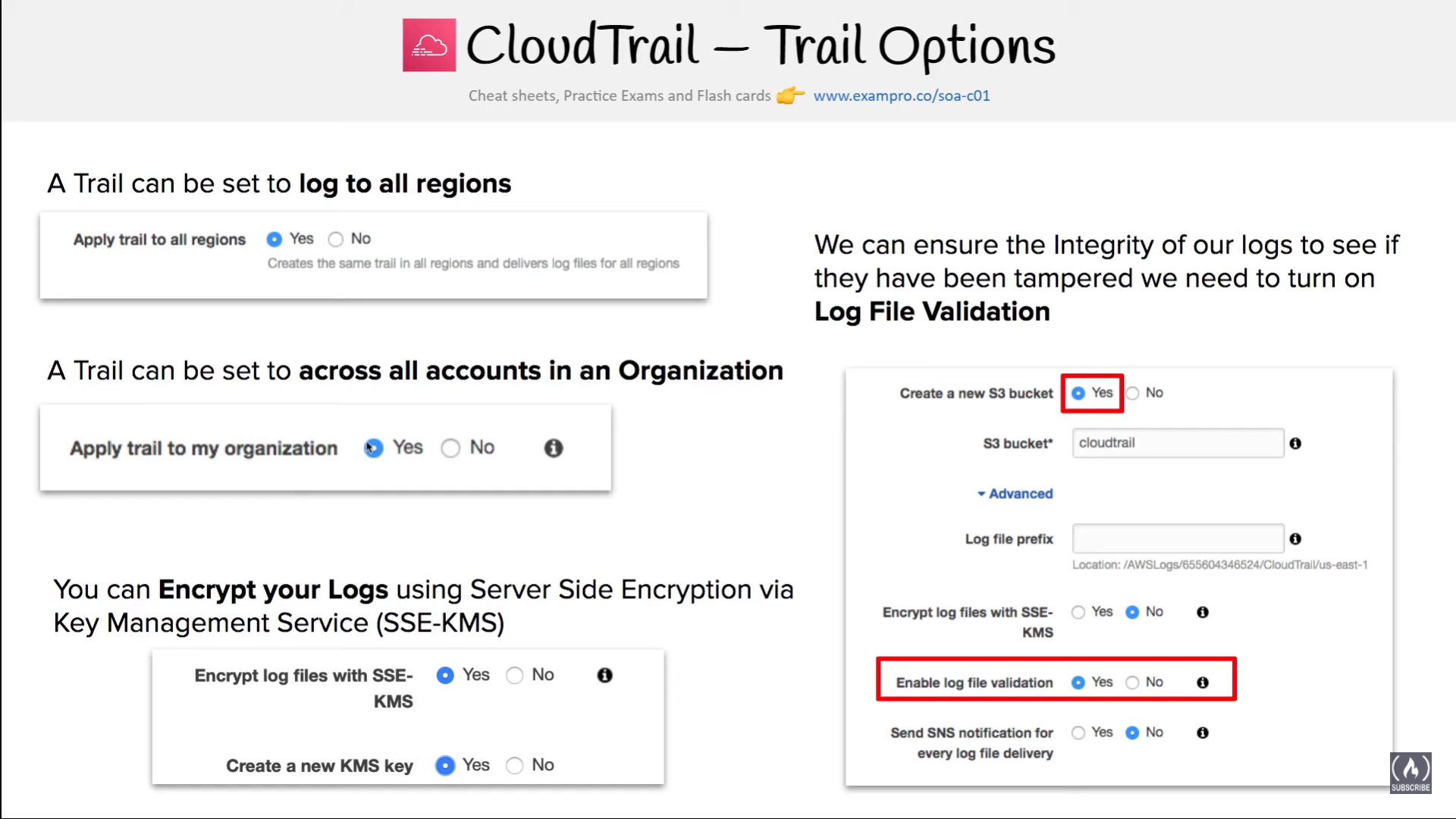
AWS CloudTrail

# AWS CloudTrail Overview

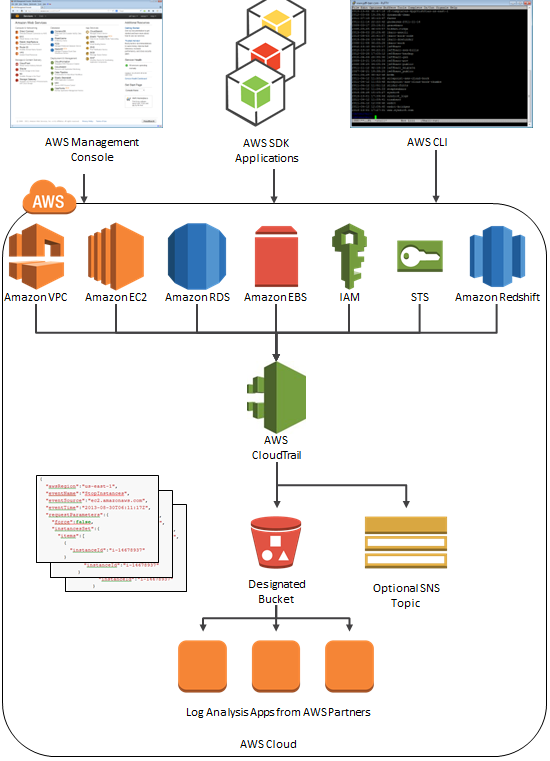




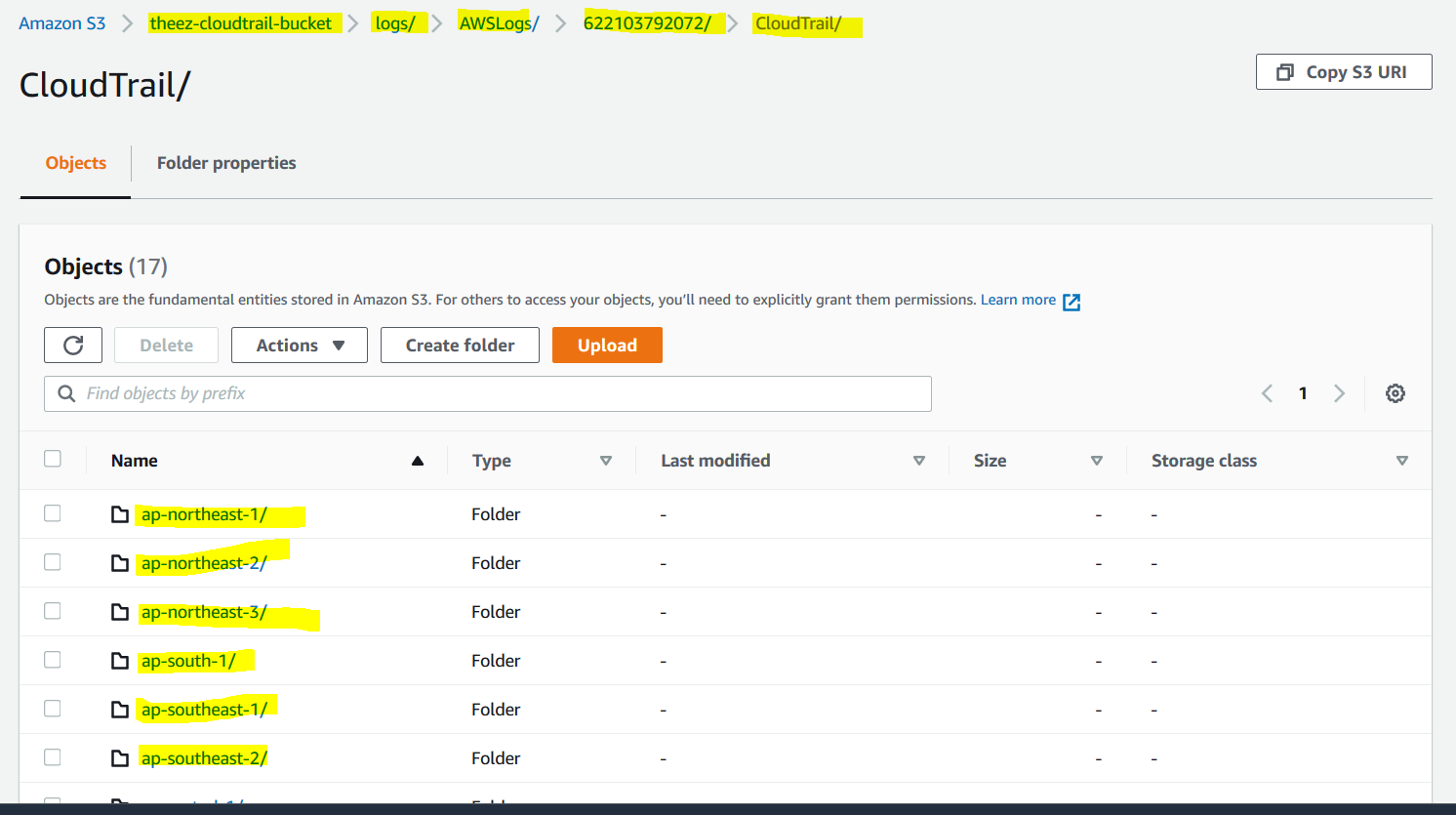
* AWS CloudTrail helps to get a history of AWS API calls and related events for the AWS account.
* CloudTrail tracking includes calls made by using the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation)
* CloudTrail helps to identify which users and accounts called AWS for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred.
* **CloudTrail is per AWS account and enabled per region for all the services supporting it**
* AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing



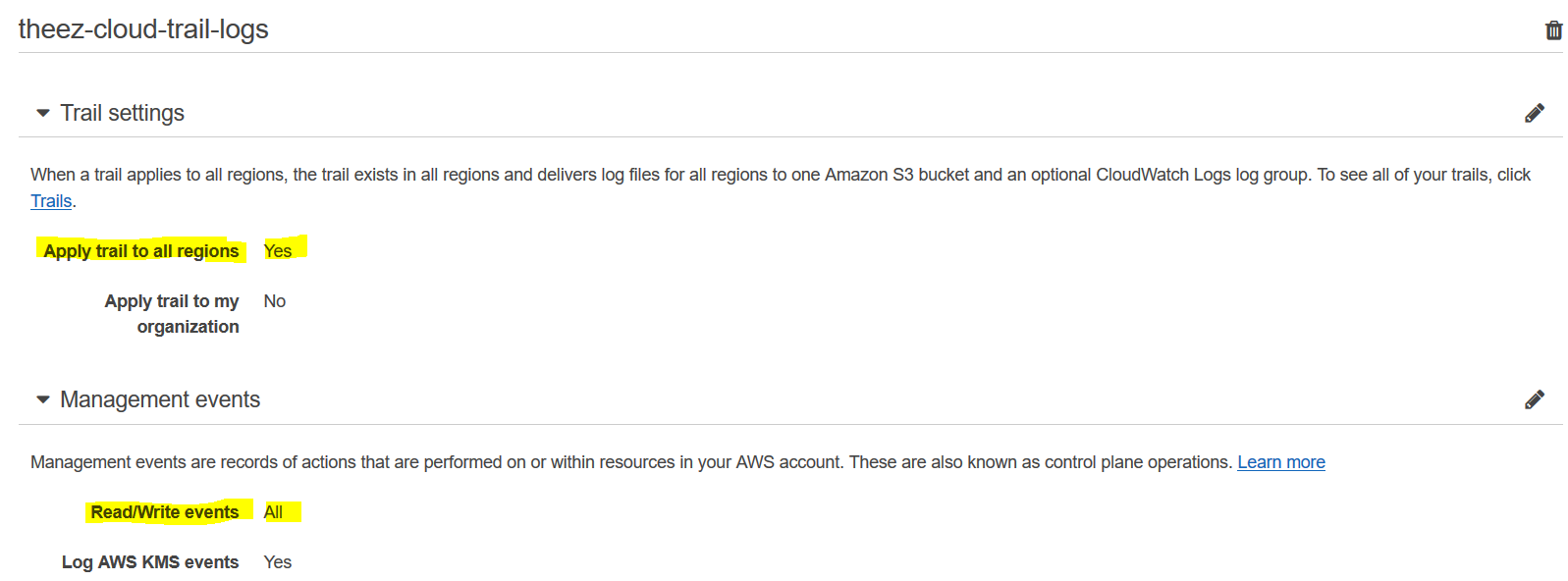
## CloudTrail Works

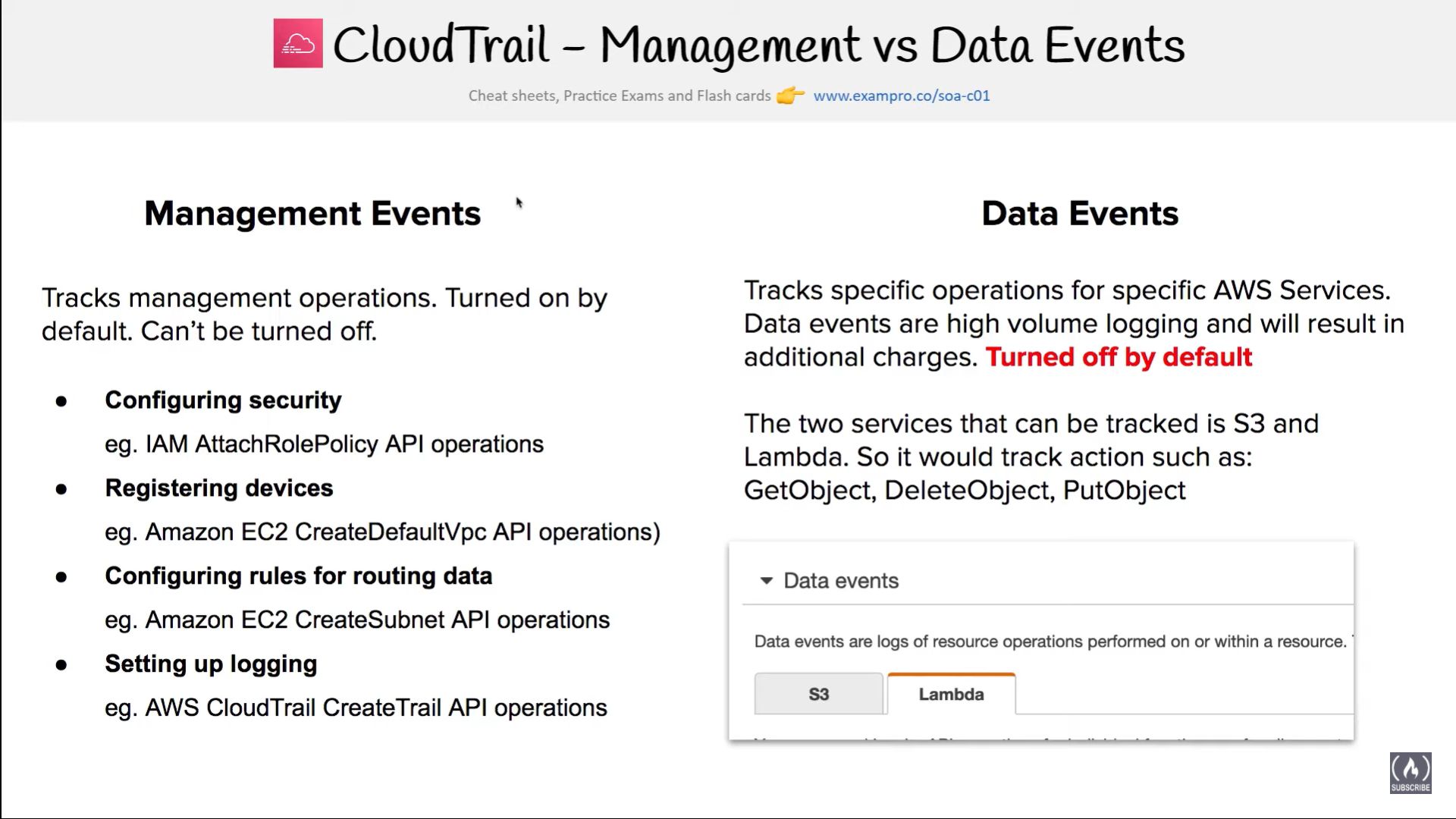


* AWS CloudTrail captures AWS API calls and related events made by or on behalf of an AWS account and delivers log files to an specified S3 bucket.
* **Log files contain API calls from all of the**[**account’s CloudTrail supported services**](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-supported-services.html)
* **Log files from all the regions can be delivered to a single S3 bucket and are encrypted, by default, using S3 server-side encryption (SSE)**
* CloudTrail typically delivers log files within 15 minutes of an API call and publishes new log files multiple times an hour, usually about every 5 mins.
* CloudTrail can be configured, optionally, to deliver events to a log group to be monitored by CloudWatch Logs.
* Amazon SNS notifications can be configured to be sent each time a log file is delivered to your bucket.
* **A trail, which is a configuration, needs to be created that enables logging of the AWS API activity and related events in your account.**
* Trail can be created with CloudTrail console, AWS CLI, or CloudTrail API.
* **A trail can be applied to all regions or a single region**
  + A trail that applies to all regions
    - When a trail is created that applies to all regions, CloudTrail creates the same trail in each region, records the log files in each region, and delivers the log files to the specified single S3 bucket (and optionally to the CloudWatch Logs log group)



* + - Default setting when a trail is created using the CloudTrail console
    - A single SNS topic for notifications and CloudWatch Logs log group for events would suffice for all regions
    - Advantages
      * configuration settings for the trail apply consistently across all regions
      * manage trail configuration for all regions from one location.
      * immediately receive events from a new region
      * receive log files from all regions in a single S3 bucket and optionally in a CloudWatch Logs log group.
      * create trails in regions not used often to monitor for unusual activity





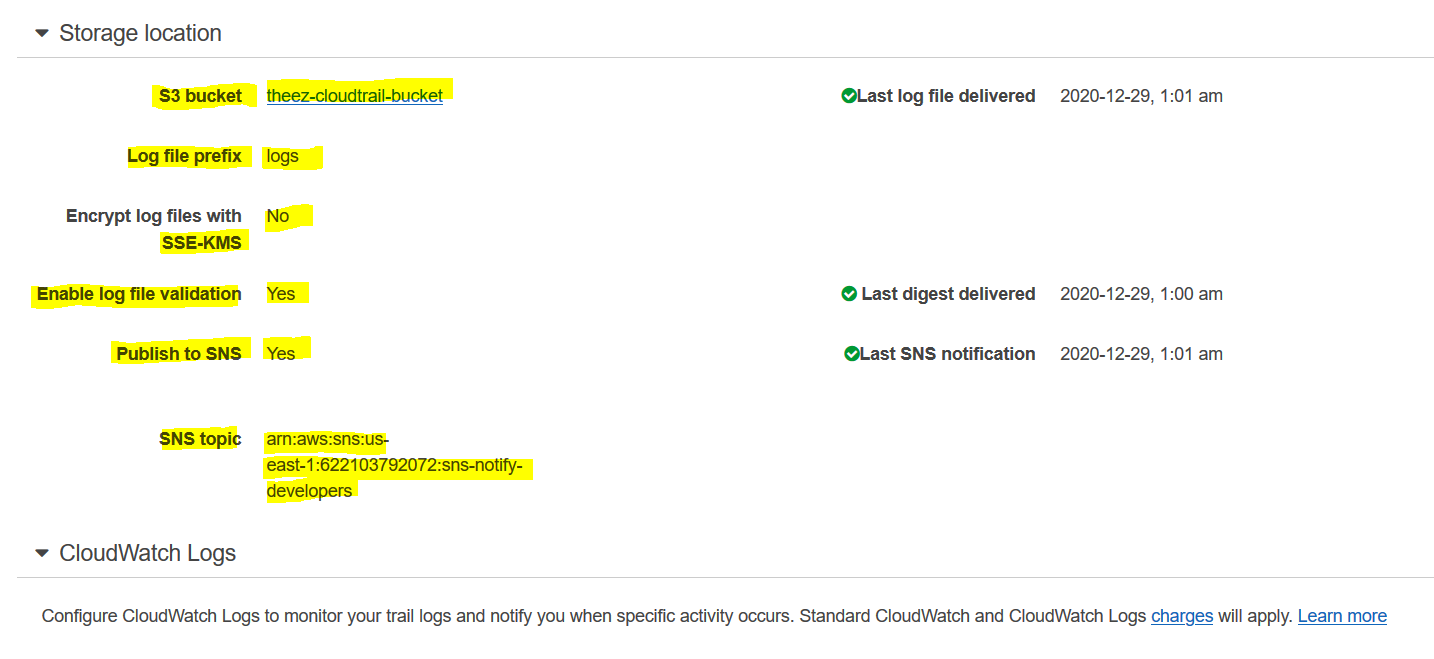
* + A trail that applies to one region
    - A S3 bucket can be specified that receives events only from that region and it can be in any region that you specify.
    - Additional individual trails created that apply to specific regions, those trails can deliver event logs to a single S3 bucket.
* ‘Turning on a trail’ means that create a trail and start logging
* **CloudTrail supports five trails per region**. **A trail that applies to all regions counts as one trail in every region**
* As a best practice, a trail can be created that applies to all regions in the AWS partition for e.g. aws for all standard aws regions or aws-cn for china
* IAM can be used to control which AWS users can create, configure, or delete trails, start and stop logging, and access the buckets that contain log information.
* Log file integrity validation can be enabled to verify that log files have remained unchanged since CloudTrail delivered them.

## Global Services Option

* For most services, events are sent to the region where the action happened.
* **For global services such as IAM, AWS STS, and Amazon CloudFront, events are delivered to any trail that has the Include global services option enabled.**
* **AWS OpsWorks and Amazon Route 53 actions are logged in the US East (N. Virginia) region**.
* To avoid receiving duplicate global service events, remember
  + Global service events are always delivered to trails that have the Apply trail to all regions option enabled.
  + Events are delivered from a single region to the bucket for the trail. This setting cannot be changed.
  + **If you have a single region trail, you should enable the Include global services option.**
  + If you have multiple single region trails, you should enable the Include global services option in only one of the trails.
* About global service events
  + have a trail with the Apply trail to all regions option enabled.
  + have multiple single region trails.
  + do not need to enable the Include global services option for the single region trails. Global service events are delivered for the first trail.

## Validating CloudTrail Log File Integrity

* Validated log files are invaluable in security and forensic investigations
* CloudTrail log file integrity validation can be used to check whether a log file was modified, deleted, or unchanged after CloudTrail delivered it
* Validation feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing which makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection
* When log file integrity validation is enabled:-
  + **CloudTrail creates a hash for every log file that it delivers.**
  + **Every hour, CloudTrail also creates and delivers a digest file that references the log files for the last hour and contains a hash of each.**
  + **CloudTrail signs each digest file using the private key of a public and private key pair.**
  + **After delivery, the public key can be used to validate the digest file.**
  + **CloudTrail uses different key pairs for each AWS region.**
  + **Digest files are delivered to the same Amazon S3 bucket, but a separate folder, associated with the trail for the log files**
  + Separation of digest files and log files enables enforcement of granular security policies and permits existing log processing solutions to continue to operate without modification.
  + Each digest file also contains the digital signature of the previous digest file if one exists.
  + Signature for the current digest file is in the metadata properties of the digest file Amazon S3 object.
  + Log files and digest files can be stored in Amazon S3 or Amazon Glacier securely, durably and inexpensively for an indefinite period of time.
  + To enhance the security of the digest files stored in Amazon S3, Amazon S3 MFA Delete can be enabled.





## CloudTrail Enabled Use Cases

* Track changes to AWS resources
  + Can be used to track creation, modification or deletion of AWS resources
* Compliance Aid
  + easier to demonstrate compliance with internal policy and regulatory standards



* Troubleshooting Operational Issues
  + identify the recent changes or actions to troubleshoot any issues
* Security Analysis
  + use log files as inputs to log analysis tools to perform security analysis and to detect user behavior patterns

## CloudTrail Processing Library (CPL)

* CloudTrail Processing Library (CPL) helps build applications to take immediate action on events in CloudTrail log files
* CPL helps to
  + read messages delivered to SNS or SQS
  + downloads and reads the log files from S3 continuously
  + serializes the events into a POJO
  + allows custom logic implementation for processing
  + fault tolerant and supports multi-threading

## AWS Config vs CloudTrail

* AWS Config reports on **WHAT** has changed, whereas CloudTrail reports on **WHO** made the change, **WHEN**, and from **WHICH** location.
* AWS Config focuses on the configuration of the AWS resources and reports with detailed snapshots on **HOW** the resources have changed, whereas CloudTrail focuses on the events, or API calls, that drive those changes. It focuses on the user, application, and activity performed on the system.

## 

## AWS Certification Exam Practice Questions

1. You currently operate a web application in the AWS US-East region. The application runs on an auto-scaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your EC2, IAM and RDS resources. The solution must ensure the integrity and confidentiality of your log data. Which of these solutions would you recommend?
   1. **Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles, S3 bucket policies and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs. (**Single New bucket with global services option for IAM and MFA delete for confidentiality**)**
   2. Create a new CloudTrail with one new S3 bucket to store the logs. Configure SNS to send log file delivery notifications to your management system. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs. (Missing Global Services for IAM)
   3. Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected Use S3 ACLs and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs. (Existing bucket prevents confidentiality)
   4. Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tools. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs (3 buckets not needed, Missing Global services options)
2. Which of the following are true regarding AWS CloudTrail? Choose 3 answers
   1. **CloudTrail is enabled globally** (it can be enabled for all regions and also per region basis)
   2. CloudTrail is enabled by default (**was not enabled by default, however, it is enabled by default as per the latest**[**AWS enhancements**](https://aws.amazon.com/blogs/aws/new-amazon-web-services-extends-cloudtrail-to-all-aws-customers/))
   3. **CloudTrail is enabled on a per-region basis** (it can be enabled for all regions and also per region basis)
   4. CloudTrail is enabled on a per-service basis (once enabled it is applicable for all the supported services, service can’t be selected)
   5. **Logs can be delivered to a single Amazon S3 bucket for aggregation**
   6. CloudTrail is enabled for all available services within a region. (is enabled only for CloudTrail supported services)
   7. Logs can only be processed and delivered to the region in which they are generated. (can be logged to bucket in any region)
3. An organization has configured the custom metric upload with CloudWatch. The organization has given permission to its employees to upload data using CLI as well SDK. How can the user track the calls made to CloudWatch?
   1. The user can enable logging with CloudWatch which logs all the activities
   2. **Use CloudTrail to monitor the API calls**
   3. Create an IAM user and allow each user to log the data using the S3 bucket
   4. Enable detailed monitoring with CloudWatch
4. A user is trying to understand the CloudWatch metrics for the AWS services. It is required that the user should first understand the namespace for the AWS services. Which of the below mentioned is not a valid namespace for the AWS services?
   1. AWS/StorageGateway
   2. **AWS/CloudTrail (**[CloudWatch supported namespaces](http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/aws-namespaces.html)**)**
   3. AWS/ElastiCache
   4. AWS/SWF
5. Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?
   1. **Use CloudTrail Log File Integrity Validation**. (Refer [link](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html))
   2. Use AWS Config SNS Subscriptions and process events in real time.
   3. Use CloudTrail backed up to AWS S3 and Glacier.
   4. Use AWS Config Timeline forensics.
6. Your CTO has asked you to make sure that you know what all users of your AWS account are doing to change resources at all times. She wants a report of who is doing what over time, reported to her once per week, for as broad a resource type group as possible. How should you do this?
   1. **Create a global AWS CloudTrail Trail. Configure a script to aggregate the log data delivered to S3 once per week and deliver this to the CTO.**
   2. Use CloudWatch Events Rules with an SNS topic subscribed to all AWS API calls. Subscribe the CTO to an email type delivery on this SNS Topic.
   3. Use AWS IAM credential reports to deliver a CSV of all uses of IAM User Tokens over time to the CTO.
   4. Use AWS Config with an SNS subscription on a Lambda, and insert these changes over time into a DynamoDB table. Generate reports based on the contents of this table.