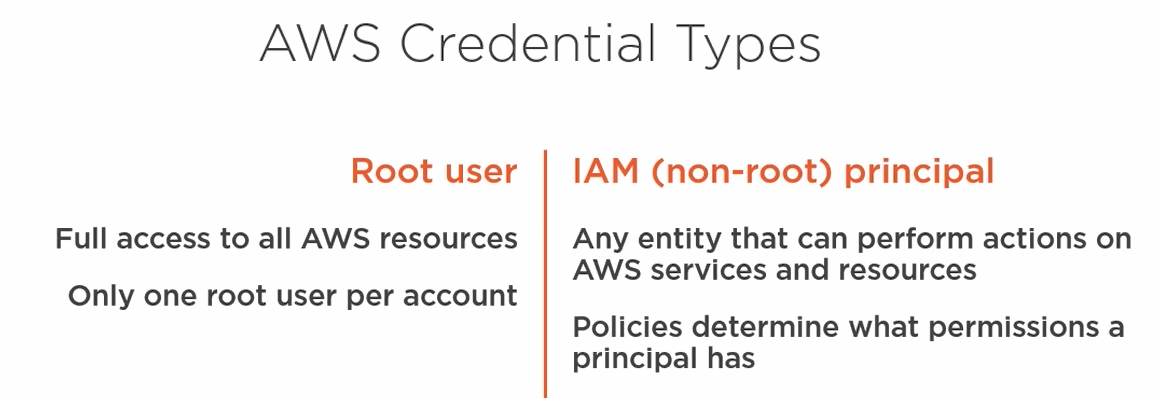
**Architecting for Security on AWS**

The CIA triad : Confidentiality, Integrity, Availability

* Confidentiality : Only authorized parties can access data. eg: ACLs and encryption
* Integrity: Data has not been improperly modified, includes knowing if the data has been modified
* Availability : Authorized parties have access to data when they need it, includes protecting systems that store process and deliver data

**Protecting AWS Credentials**

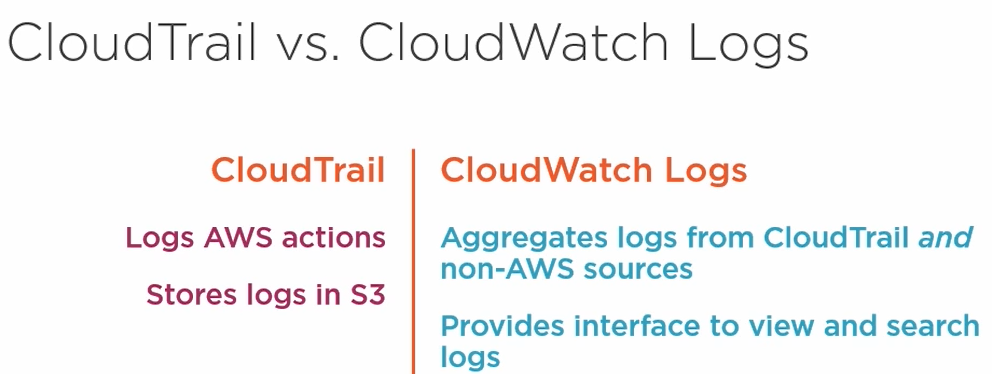
****

**Cloud Trail :**

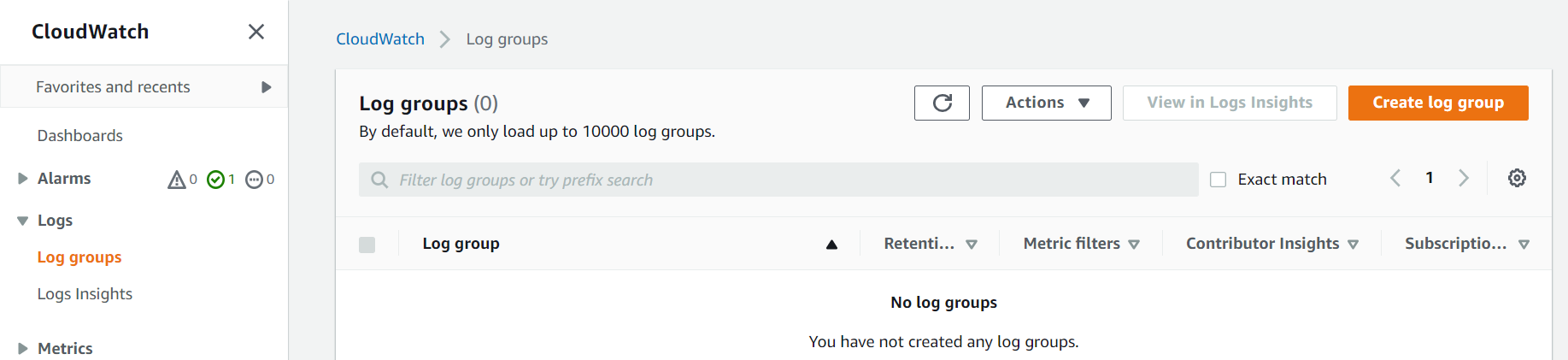
**Event Types**

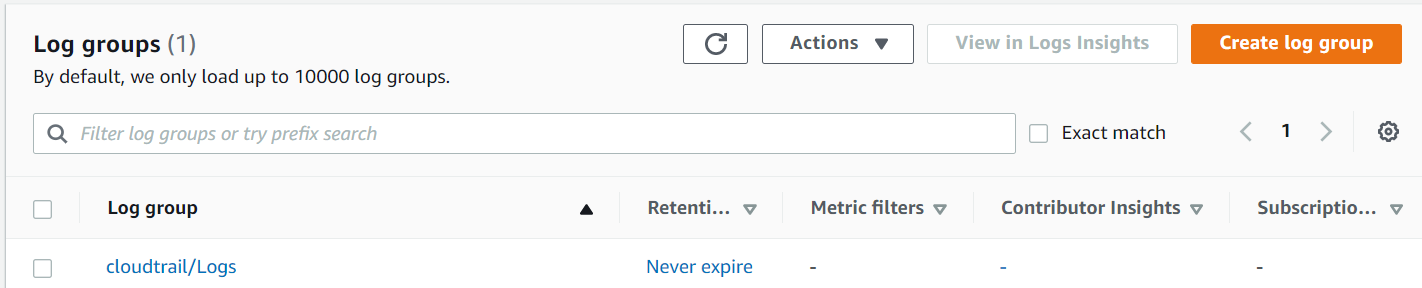
* Management : configuration changes to aws services, reading resources, logging into the management console, Assuming a role
* Data: Access to S3 objects , Lambda function execution

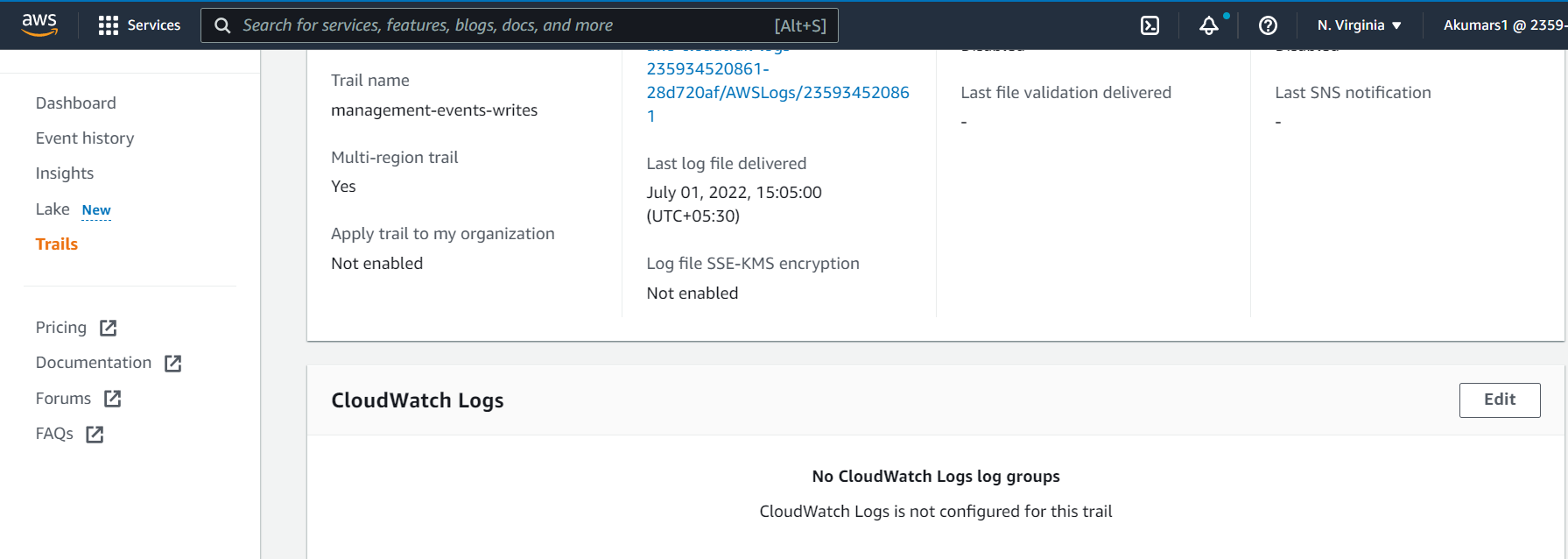
Cloud trail logs are stored in S3. Limit what you log to control costs

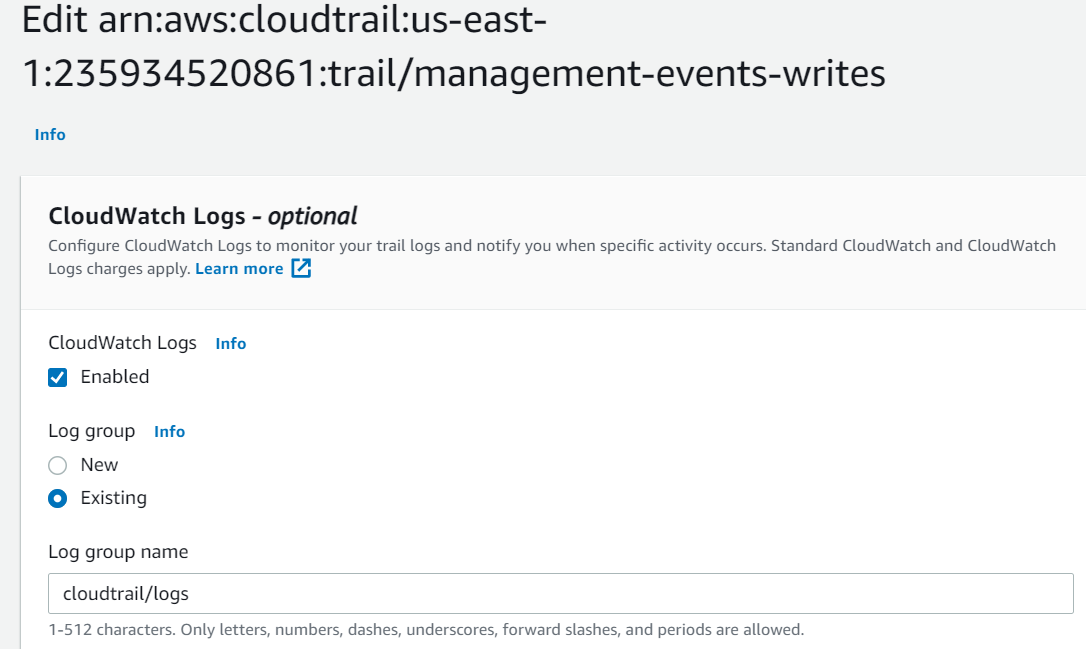


**Configure CloudWatch logs**









**Why Athena :** you don’t want to use cloudwatch logs. You want to search the contents of S3 objects  
  
Cloud trail stores its logs in S3 in JSON format.

Athena uses SQL, you must provide the schema, AWS provides the schema for the cloudtrail logs