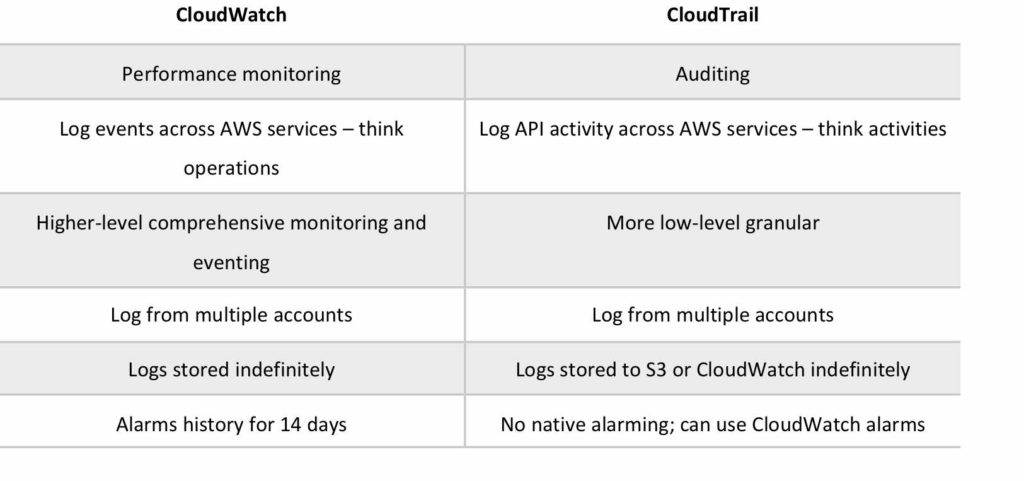
**CloudTrail**

* CT is a web service that records activity made on your account
* CT trail can be created which delivers log ifles to an S3 bucket
* 
* CT is all about logging and saves a history of API calls for your AWS account
* Provides visibility into user activity by recording actions taken on your account
* API history enables securiyt analysis, resource change tracking and compliance auditing
* Logs API calls made via:
  + AWS Management Console
  + AWS SDKs
  + CLI tools
  + Higher-level AWS services(such as CF)
* CT records account activity and service events from most AWS services and logs the following records
  + Identity of API caller
  + Time of API call
  + Source IP address of the API caller
  + Request parameters
  + Response elements returned by the AWS service
* CT is per AWS account
  + Trails can be enabled per region or a trail can be applied to all regions
  + Trails can be configured to log data events and management events:
    - **Data events:** These events provide insight into the resource operations performed on or within a resource. These are also known as data plane operations
    - **Management events:** Management events provide insight into managemtn operations that are performed on resources in your AWS account. Trhese are also known as control plane operations. Management events can also include non-API events that occur in your account
  + CloudTrail log files are encrypted using S3 Server Side Encryption(SSE)
  + You can also enable encryption using SSE KMS for additional security
  + A single KMS key can be used to encrypt log files for trails pplied to all regions
  + You can consolidate logs from multiple accounts using an S3 bucket:
    - Turn on CT in the paying account
    - Create a bucket policy that allow scross-account access
    - Turn on CT in the other accounts and use the bucket in the paying account
  + You can integrate with CT and CW Logs to deliver data events captured by CT to a CW Logs log stream
  + CT log file integrity validation feature allows you to determine wheter a CT log file was unchanged, deleted or modified since CT delivered it to the S3 bucket