**AWS CloudTrail**

* Track events, API calls, changes made to your AWS resources:
  + Who made the request?
  + What action was performed?
  + What are the parameters used?
  + What was the end result?
* (USE CASE) Compliance with regulatory standards
* (USE CASE) Troubleshooting. Locate a missing resource
* Delivers log files to S3 and/or Amazon cloud watch logs log group ( S3 is default )
* You can setup SNS notifications for log file delivery

**AWS Cloud Trail Types**

* Multi Region Trail
  + One trail of all AWS regions
  + Events from all regions can be sent to one CloudWatch logs log group
* Single Region Trail
  + Only events from one region
  + Destination S3 bucket can be in any region

**AWS Cloud Trail - Good to know**

* Log files are automatically encrypted with Amazon S3 SSE
* You can configure S3 Lifecycle rules to archive or delete log files
* Supports log file integrity
  + You can prove that a log file has not been altered

**AWS Config**

* Auditing
  + Create a complete inventory of your AWS resources
* Resource history and change tracking
  + Find how a resource was configured at any point in time
  + Configuration of deleted resources would be maintained Delivers history file to S3 bucket every 6 hours
  + Take configuration snapshots when needed
* Governance
  + Customize Config Rules for specific resources or for entire AWS account
  + Continuously evaluate compliance against desired configuration
  + Get a SNS notification for every configuration change
* Consistent rules and compliance across AWS accounts:
  + Group Config Rules and Remediation Actions into Conformance Packs

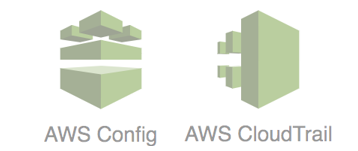
**Predefined Config Rule Examples (80+)**

* **alb-http-to-https-redirection-check** - Checks whether HTTP to HTTPS redirection is configured on all HTTP listeners of Application Load Balancers
* **ebs-optimized-instance** - Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized
* **ec2-instance-no-public-ip** - Do EC2 instances have public IPs?
* **encrypted-volumes** - Are all EC2 instance attached EBS volumes encrypted?
* **eip-attached** - Are all Elastic IP addresses used?
* **restricted-ssh** - Checks whether security groups that are in use disallow unrestricted incoming SSH traffic

**AWS Config Rules**

* (Feature) Create Lambda functions with your custom rules
* (Feature) You can setup auto remediation for each rule
  + Take immediate action on a non compliant resource
  + (Example) Stop EC2 instances without a specific tag!
* Enable AWS Config to use the rules
  + No Free Tier
  + More rules to check => More $$$$

**AWS Config + AWS CloudTrail**



* AWS Config
  + What did my AWS resource look like?
* AWS CloudTrail
  + Who made an API call to modify this resource?

**Monitoring with Amazon CloudWatch**

* Monitoring and observability service
* Collects monitoring and operational data in the form of logs, metrics, and events
* Set alarms, visualize logs, take automated actions and troubleshoot issues
* Integrates with more than 70 AWS services:
  + Amazon EC2
  + Amazon DynamoDB
  + Amazon S3
  + Amazon ECS
  + AWS Lambda and ....

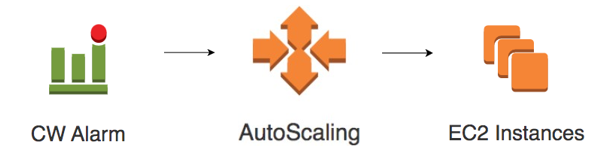
**Amazon CloudWatch Logs**

* Monitor and troubleshoot using system, application and custom log files
* Real time application and system monitoring
  + Monitor for patterns in your logs and trigger alerts based on them
  + Example : Errors in a specific interval exceed a certain threshold
* Long term log retention
  + Store logs in CloudWatch Logs for as long as you want (configurable - default:forever)
  + Or archive logs to S3 bucket (Typically involves a delay of 12 hours)
  + Or stream real time to Amazon Elasticsearch Service (Amazon ES) cluster using CloudWatch Logs subscription

**Amazon CloudWatch Logs**

* CloudWatch Logs Agent
  + Installed on ec2 instances to move logs from servers to CloudWatch logs
* CloudWatch Logs Insights
  + Write queries and get actionable insights from your logs
* CloudWatch Container Insights
  + Monitor, troubleshoot, and set alarms for your containerized applications running in EKS, ECS and Fargate

**Amazon CloudWatch Alarms**



* Create alarms based on:
  + Amazon EC2 instance CPU utilization
  + Amazon SQS queue length
  + Amazon DynamoDB table throughput or
  + Your own custom metrics
* Take immediate action:
  + Send a SNS event notification
    - Send an email using SNS
  + Execute an Auto Scaling policy

**Amazon CloudWatch Alarm - Example**

* You set a CPU Utilization alarm on EC2 instance with a threshold of 80% over 3 periods of 10 minutes. If CPU utilization is 90% for 20 minutes, does the alarm get triggered?
  + No

**Amazon CloudWatch Dashboards**

* Create auto refreshed graphs around all CloudWatch metrics
* Automatic Dashboards are available for most AWS services and resources
* Each Dashboard can have graphs from multiple regions

**Amazon CloudWatch Events**

* Enable you to take immediate action based on events on AWS resources
  + Call a AWS Lambda function when an EC2 instance starts
  + Send event to an Amazon Kinesis stream when an Amazon EBS volume is created
  + Notify an Amazon SNS topic when an Auto Scaling event happens
* Schedule events - Use Unix cron syntax
  + Schedule a call to Lambda function every hour
  + Send a notification to Amazon SNS topic every 3 hours