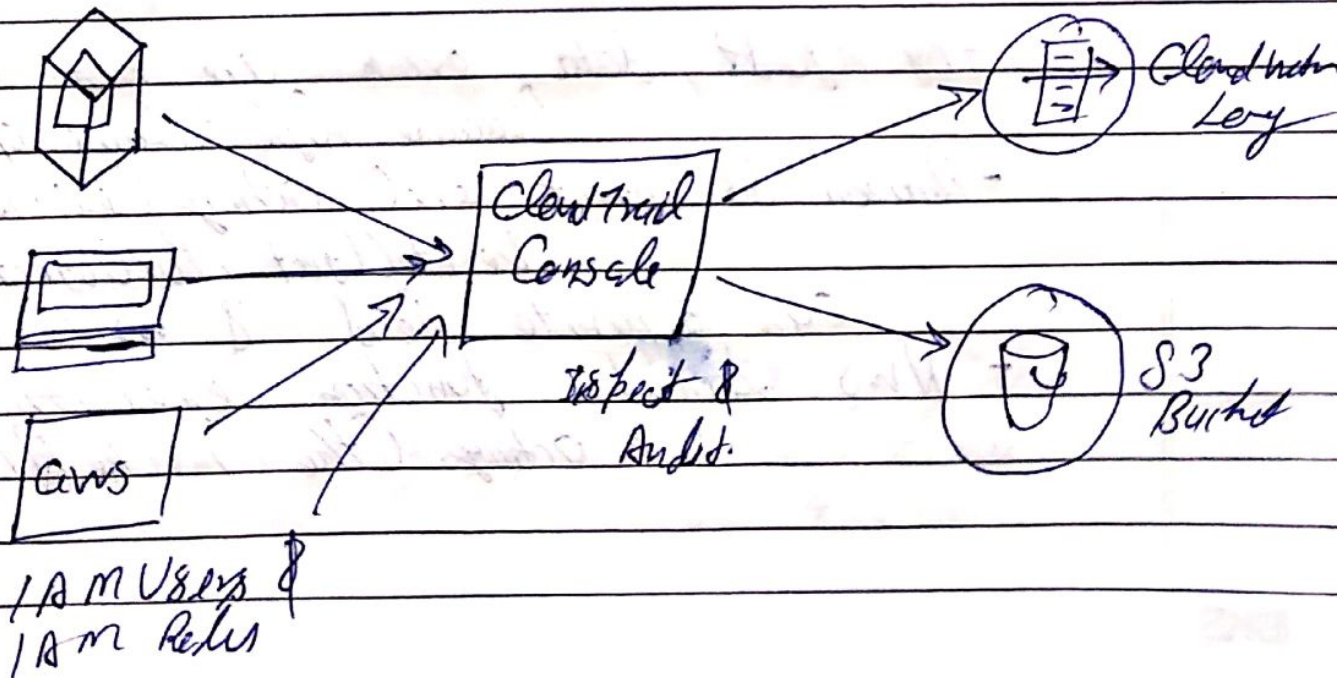


Day 22/100

AWS CloudTrail →

- Provides governance, Compliance and audit for your AWS account
- CloudTrail is enabled by default?
- Get on history of events / API calls made within your AWS Account by:-
 - Console
 - SDK
 - CLI
 - AWS Services
- Can put logs from CloudTrail into CloudWatch Logs or S3.
- A trail can be applied to All Regions (Default) or a single Region
- If a resource is deleted in AWS, investigate CloudTrail first!

⇒ CloudTrail Diagram →



#CloudTrail Events →

• Management Events:

- operations that are performed on resources in your AWS account.
- Example:
 - Configuring Security [IAM AttachRolePolicy]
 - Configuring rules for routing data (Amazon EC2 CreateSubnet)
 - Setting up logging AWS CloudTrail (CreateTrail)
- By default, trails are configured to log management events.
- Can separate Read Events (that don't modify resources) from Write Events (that may modify resources)

• Data Events:

- By default, data events are not logged (because high volume operations).
- Amazon S3 object-level activity (ex: GetObject, DeleteObject, PutObject)
can separate Read & Write Events.
- AWS Lambda function execution activity (the invoke API).

• CloudTrail Insights Events

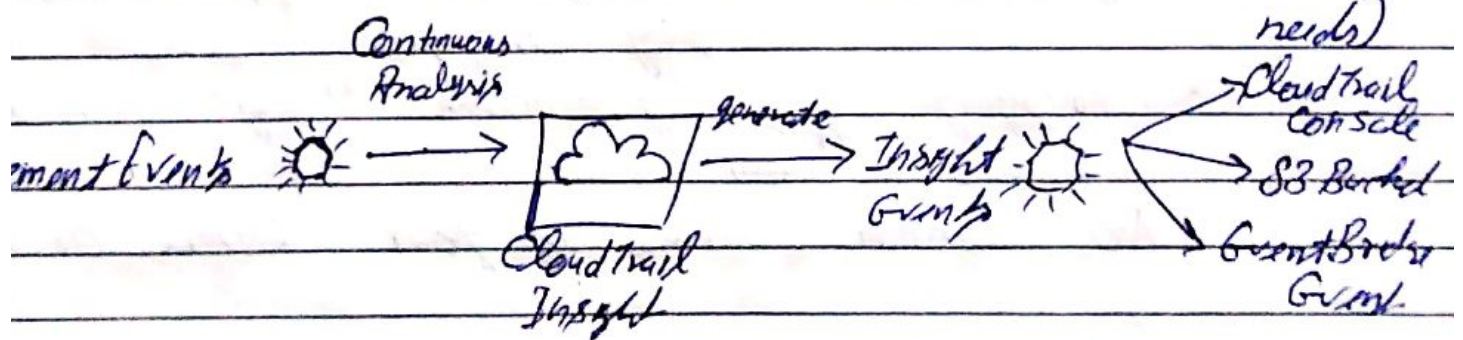
→ Enable CloudTrail Insight to detect unusual activity in your account:

- Inaccurate resource provisioning.
- Hitting service limits.
- Bursts of AWS IAM actions.
- Gaps in periodic maintenance activity.

→ CloudTrail Insight analyzes normal management events to create a baseline.

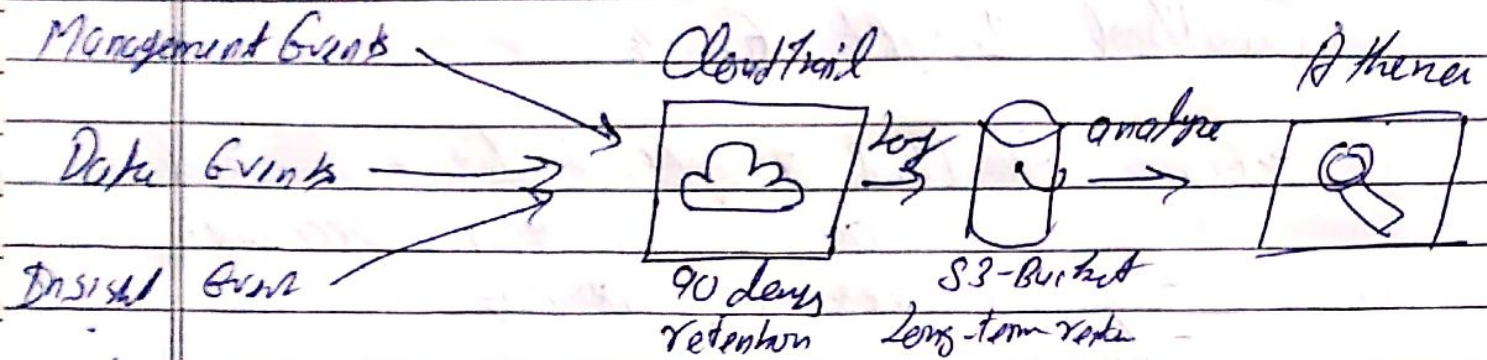
→ And then continuously analyzes writes events to detect unusual patterns.

- Anomalies appear in the CloudTrail Console.
- Event is sent to Amazon S3.
- An EventBridge event is generated (for automation needs).



CloudTrail Events Retention -

- Events are stored for 90 days in CloudTrail.
- To keep events beyond this period, log them to S3 and use Athena.



AWS X-Ray

- Debugging in Production, the good old way!
 - Test locally
 - Add log statements everywhere
 - Re-deploy in production

- Log formats differ across applications & log analysis is hard

- Debugging: One big monolithic "easy" distributed service "hard"

- No common view of your entire architecture

- Enter - AWS X-Ray!

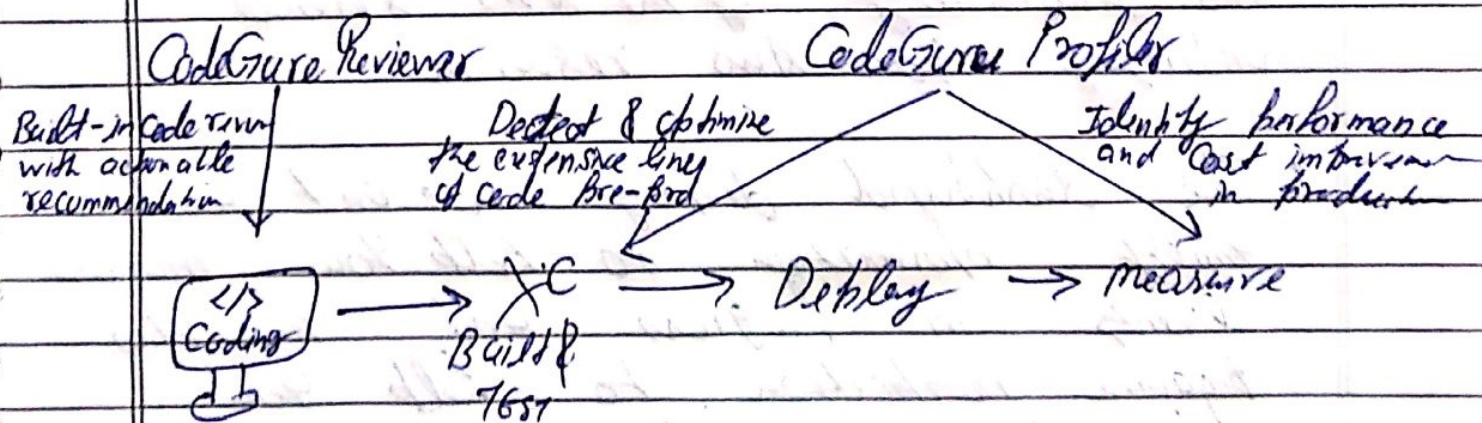
⇒ X-Ray Advantages

- Troubleshooting performance (bottlenecks)
- Understand dependencies in a microservices architecture

- Understand dependencies in a microservice arch.
- Pinpoint service issues
- Review request behaviour
- Find errors & exceptions
- Are we meeting time SLO?
- where I am throttled
- Identify users that are impacted

Amazon CodeGuru:

- An ML-powered service for automated code review and application performance recommendations.
- Provides two functionalities
 - CodeGuru Reviewer: automated code review for static code analysis (development)
 - CodeGuru Profiler: visibility/recommendations about application performance during runtime (production)



AWS Status - Services Health Dashboard

- Show all regions, all service health
- Show Historical information for each day
- Has an RSS feed you can subscribe to

<https://status.aws.amazon.com>

AWS Personal Health Dashboard [AWS PHD]

- AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you.
- While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.
- The dashboard displays relevant and timely information to help you manage events in progress and provides proactive notification to help you plan for scheduled activities.

- Global services <https://phd.aws.amazon.com>
- Show how AWS Outposts directly impact you & your AWS resource
- Alert, remediation, proactive, scheduled activities