**1. What is AWS CloudTrail?**

**Answer:** AWS CloudTrail is a service that records **API calls and user activity** across AWS services.

* Provides event history for security, compliance, and troubleshooting.

**2. What does CloudTrail log?**

**Answer:**

* API calls (AWS Management Console, CLI, SDKs, services)
* IAM user actions
* Changes to AWS resources
* Source IP, request parameters, response elements

**3. What is the difference between CloudTrail and CloudWatch?**

**Answer:**

* **CloudTrail:** Logs **who did what and when** (API activity).
* **CloudWatch:** Monitors **performance metrics, logs, and events**.

**4. What is a CloudTrail Trail?**

**Answer:** A configuration that **delivers CloudTrail events** to a storage location (e.g., S3 bucket) for logging.

**5. Where does CloudTrail store logs by default?**

**Answer:** By default, CloudTrail stores logs in an **S3 bucket** specified during trail creation.

**6. What are Management Events in CloudTrail?**

**Answer:** Events that record **control plane operations** (e.g., creating/deleting resources, IAM changes).

**7. What are Data Events in CloudTrail?**

**Answer:** Events that record **resource-level operations** (e.g., S3 object-level access, Lambda function invocation).

* These are **disabled by default**.

**8. How long are CloudTrail events stored?**

**Answer:**

* Event history: **90 days** (in CloudTrail console)
* S3 logs: As long as you keep them in the bucket.

**9. Does CloudTrail log all AWS regions by default?**

**Answer:** No. You must enable the **trail as a multi-region trail** to log activity in all regions.

**10. Is CloudTrail enabled by default in AWS accounts?**

**Answer:** Yes, **event history** for the past 90 days is always available by default.

* To persist logs, you must **create a trail**.

**11. What are the main components of CloudTrail?**

**Answer:**

* **Trails** – Configuration for logging.
* **Events** – Logged activity.
* **Event History** – 90-day API activity logs.
* **S3 Bucket** – Log storage.
* **CloudWatch Logs Integration** – For real-time monitoring.

**12. What is the difference between Single-Region and Multi-Region Trails?**

**Answer:**

* **Single-Region Trail:** Logs activity in one region.
* **Multi-Region Trail:** Logs activity across all AWS regions.

**13. What is an Organization Trail?**

**Answer:** A trail applied at the AWS Organizations level to **log activity across multiple accounts**.

**14. How do you secure CloudTrail logs?**

**Answer:**

* Enable **log file integrity validation**
* Use **SSE-KMS encryption**
* Apply strict **bucket policies** to prevent tampering

**15. What is Log File Integrity Validation?**

**Answer:** Ensures logs are **not modified or deleted** by generating a hash for every log file.

**16. Can CloudTrail send notifications?**

**Answer:** Yes. By integrating with **CloudWatch Logs** and **SNS**, you can send real-time alerts.

**17. How do you analyze CloudTrail logs?**

**Answer:**

* Use **Athena** to query logs in S3.
* Use **CloudWatch Insights** for log analysis.

**18. What’s the difference between CloudTrail Insights Events and Normal Events?**

**Answer:**

* **Normal Events:** Record API activity as usual.
* **Insights Events:** Detect **unusual activity patterns** (e.g., spikes in API calls).

**19. How do you monitor S3 object-level access?**

**Answer:** Enable **S3 Data Events** in CloudTrail for object-level logging.

**20. What services does CloudTrail integrate with?**

**Answer:**

* **CloudWatch** (for alarms)
* **AWS Config** (for compliance)
* **Athena** (for queries)
* **GuardDuty** (for threat detection)

**21. Scenario: You need to detect unauthorized API calls.**

**Answer:**

* Enable **CloudTrail logging**.
* Send logs to **CloudWatch Logs**.
* Create alarms for AccessDenied events.

**22. Scenario: You want to prevent CloudTrail logs from being deleted.**

**Answer:**

* Use **S3 bucket policy** with Deny on s3:DeleteObject.
* Enable **MFA Delete**.

**23. Scenario: You suspect log tampering. How to verify?**

**Answer:**

* Enable **Log File Integrity Validation**.
* Use the validate-logs AWS CLI command.

**24. Scenario: Need to monitor activity across multiple AWS accounts centrally.**

**Answer:**

* Use **Organization Trail** in AWS Organizations.
* Centralize logs to a single S3 bucket.

**25. Scenario: Detect when IAM Root user is used.**

**Answer:**

* Create a CloudWatch metric filter on CloudTrail logs:

$.userIdentity.type = "Root"

* Trigger an alarm.

**26. What is the difference between CloudTrail and GuardDuty?**

**Answer:**

* **CloudTrail:** Logs API activity.
* **GuardDuty:** Uses CloudTrail (and other sources) to detect threats.

**27. Scenario: Audit who deleted an EC2 instance.**

**Answer:**

* Search CloudTrail logs for TerminateInstances API call.
* Check the userIdentity field.

**28. Scenario: You want to reduce CloudTrail costs.**

**Answer:**

* Log only **necessary events** (disable data events if not needed).
* Optimize retention policies.
* Archive old logs to Glacier.

**29. Scenario: Detect suspicious S3 access from unusual IPs.**

**Answer:**

* Enable CloudTrail S3 data events.
* Use **Athena queries** to analyze source IPs.

**30. Scenario: You need to trigger a Lambda function when someone changes a Security Group.**

**Answer:**

* Use CloudTrail event for AuthorizeSecurityGroupIngress.
* Route via **CloudWatch Event Rule** → Lambda.

**31. What’s the maximum number of trails per region?**

**Answer:** You can have **up to 5 trails** per AWS region (soft limit).

**32. Scenario: Ensure compliance by archiving logs for 7 years.**

**Answer:**

* Store logs in **S3 Glacier Deep Archive**.
* Set S3 lifecycle policy for retention.

**33. Scenario: Identify unused IAM users.**

**Answer:** Analyze CloudTrail logs for **last API activity** of each IAM user.

**34. Can CloudTrail capture read-only API calls?**

**Answer:** Yes, it logs **all API calls**, including read-only (e.g., DescribeInstances).

**35. Scenario: You have duplicate log entries. Why?**

**Answer:** Duplicate logs may occur when **multiple trails** are logging to the same S3 bucket.

**36. What’s the default CloudTrail log file format?**

**Answer:** JSON (compressed in .gz format).

**37. Scenario: Need real-time detection of failed login attempts.**

**Answer:**

* Create metric filter for ConsoleLogin with Failure.
* Set CloudWatch alarm to notify via SNS.

**38. Scenario: Want to track API calls made by AWS services (not users).**

**Answer:** Check CloudTrail logs for userIdentity.type = AWSService.

**39. Scenario: Detect when someone disables CloudTrail logging.**

**Answer:**

* Monitor StopLogging API call.
* Create an alarm when detected.

**40. How to query CloudTrail logs without exporting them?**

**Answer:** Use **AWS Athena** to run SQL queries directly on S3 logs.