You're required to maintain compliance logs for 1 year. How would you configure CloudTrail to support this?

Answer:

Here's what I'd do:

1. **Create a new CloudTrail trail** (or edit existing)
2. **Enable multi-region logging** for full coverage
3. **Send logs to an S3 bucket**
4. In the S3 bucket:
    - Enable **Object Lock (Governance mode)** if immutability is required
    - Set **S3 lifecycle policy** to **retain logs for 1 year**
5. (Optional) Send logs to **CloudWatch Logs** for real-time monitoring and alerts

Tip: For compliance, also enable log file validation to ensure logs are tamper-proof.

Real-world note:

In my last role, our security team required us to retain CloudTrail logs for **13 months** to meet ISO 27001 and SOC2 audit standards. We automated the lifecycle config using Terraform.

What is Object Lock?

Object Lock is an Amazon S3 feature that allows you to **store objects using a write-once-read-many (WORM) model**. This means once data is written, it **cannot be modified or deleted** for a defined retention period.

What is Governance Mode?

There are two Object Lock modes:

- **Governance mode** – Even though the data is locked, **certain users with special permissions** (like s3:BypassGovernanceRetention) can override or delete the object.
- **Compliance mode** – Nobody, not even the root user, can delete or change the object during the retention period.

What is the key difference between **Object Lock Governance mode** and **Compliance mode**?

A. Governance mode allows some privileged users to override retention; Compliance mode blocks all modifications, even from root

B. Governance mode stores logs longer; Compliance mode deletes logs after 1 year

C. Governance mode applies only to CloudTrail; Compliance mode applies only to S3

D. Governance mode supports real-time monitoring; Compliance mode does not

✅ **Correct Answer: A**

Your company’s auditor requires logs to be immutable for 1 year. Which S3 feature should you enable?

A. Versioning
B. Object Lock
C. Lifecycle Policies
D. Server-Side Encryption
✅ **Correct Answer: B**

Why is it recommended to enable **multi-region logging** for CloudTrail?

A. It reduces the cost of storing logs
B. It ensures you capture events from all AWS regions for compliance
C. It allows logs to be compressed before storage
D. It automatically enforces Object Lock
✅ **Correct Answer: B**