AWS Lab 39

Cloud Trail

Overview of the lab

In this lab you will learn how to create a multi-region organization level trail with aws cloud trail

AWS Trail

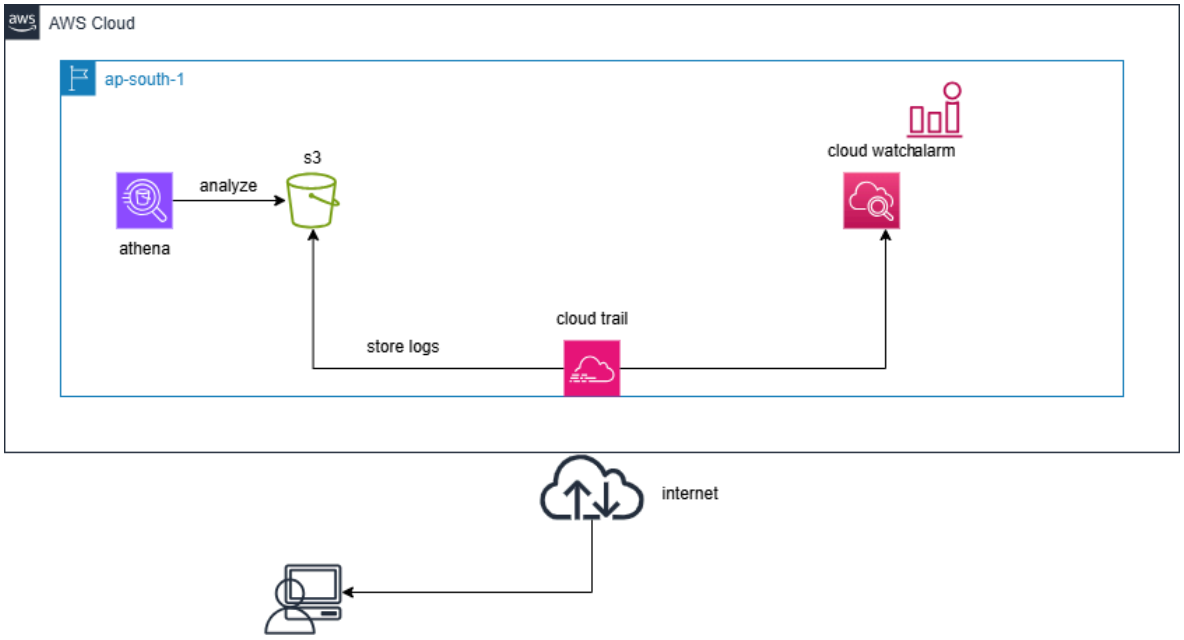
It is used to enable auditing, governance and compliance for aws account, actions taken via management console, aws cli, sdk are recorded in cloud trail

(by default in a newly created aws account 90 days logs will be stored)

Event type

- Management events - capture operations performed on aws resources
- Data events - captures operations performed within the resource
- Insights events - captures unusual activity, errors and user behavior

Architecture



Step by Step Lab

Create Trail

1. In CloudTrail click on (3 dashes) in the left and Click on Dashboard
2. Click on Create trail
    a. Trail name - demo-trail
    b. Enable for all accounts in my organization(can be enabled only if aws organization is enabled)
    c. Create new s3 bucket
    d. Trail log bucket and folder - awsclass-cloudtrail-logs
    e. Uncheck Log file SSE-KMS encrption

3. Click on Next
4. Events
    a. Check - Management events
5. Click on Next
6. Click on Create trail
7. Once trail is created click on the bucket name (bucketname/CloudTrail/) - this folder will have all the logs

Clean Up Step

1. Select the trail - Click on Delete