**AWS Project: EC2 Launch Monitoring & Alerting System**

# Objective

Build an automated system on AWS to monitor EC2 instance launches by IAM users and send real-time email alerts with details of who launched the instance, when it was launched, and the instance ID. This project integrates IAM, CloudTrail, EventBridge, Lambda, and SNS.

# Architecture Overview

1. IAM User launches an EC2 instance.  
2. CloudTrail records the RunInstances API call.  
3. EventBridge Rule detects the event pattern.  
4. Lambda Function is triggered with event details.  
5. SNS Topic publishes the alert to subscribed email(s).

# Step 1: Setup IAM

1. Create an IAM Group (e.g., EC2-Launchers) and attach policy AmazonEC2FullAccess.  
2. Create an IAM User and add it to this group.  
3. Provide AWS Management Console access and set a password.  
4. Test login with the IAM user.

# Step 2: Enable CloudTrail

1. Go to CloudTrail Console → Trails → Create trail.  
2. Trail name: ec2-audit-trail.  
3. Storage: Create a new S3 bucket (e.g., ec2-audit-logs-demo).  
4. Enable management events (default).  
5. Create trail.

# Step 3: Create EventBridge Rule

1. Go to EventBridge → Rules → Create rule.  
2. Rule name: ec2-launch-detect.  
3. Event pattern: Service = EC2, Event type = AWS API Call via CloudTrail, API call = RunInstances.  
4. Target: Lambda function (to be created).

# Step 4: Create Lambda Function

1. Go to Lambda → Create function.  
 - Name: ec2-launch-audit  
 - Runtime: Python 3.12 (or latest)  
 - Execution role: Create new role with basic Lambda permissions  
2. Add additional IAM permissions: sns:Publish to the SNS topic.

# Lambda Function Code :

import json  
import boto3  
  
sns\_client = boto3.client('sns')  
  
*# Replace with SNS Topic ARN*  
SNS\_TOPIC\_ARN = " SNS Topic ARN"  
  
def lambda\_handler(event, context):  
 try:  
 print("Event: ", json.dumps(event))  
  
 user = event['detail']['userIdentity']['userName']  
 event\_time = event['detail']['eventTime']  
 instance\_id = event['detail']['responseElements']['instancesSet']['items'][0]['instanceId']  
  
 message = (  
 f"EC2 Instance Launched!\n\n"  
 f"User: {user}\n"  
 f"Time: {event\_time}\n"  
 f"Instance ID: {instance\_id}"  
 )  
  
 sns\_client.publish(  
 TopicArn=SNS\_TOPIC\_ARN,  
 Message=message,  
 Subject="EC2 Launch Alert"  
 )  
  
 return {"statusCode": 200, "body": json.dumps("Alert sent successfully!")}  
  
 except Exception as e:  
 print("Error: ", str(e))  
 return {"statusCode": 500, "body": json.dumps("Error: " + str(e))}

# Step 5: Setup SNS Topic

1. Go to SNS → Topics → Create topic.  
 - Name: EC2LaunchAlerts  
2. Copy the Topic ARN and update in the Lambda code.  
3. Create a Subscription:  
 - Protocol: Email  
 - Endpoint: your email address  
4. Confirm subscription from your inbox.

# Step 6: Test the System

1. Log in with your IAM user.  
2. Launch an EC2 instance.  
3. Event flow: CloudTrail logs event → EventBridge triggers → Lambda executes → SNS sends email.  
4. Check your inbox for an EC2 Launch Alert.

# Future Enchancements

Depending on user’s requirements this application can be modified for not only EC2 but all other AWS services and can help in keeping track of the activities for long term.

# Outcome

You now have an automated AWS monitoring system. Every time an EC2 is launched, you'll know who did it, when, and the instance ID directly in your email inbox.

