Cloud and DevOps Lab Experiments (7-10)

7) Enable AWS CloudTrail and CloudWatch, Simulate Event and View Logs

Step 1: Enable CloudTrail

- Go to AWS Console > CloudTrail > Create trail

- Choose "Apply to all regions" and an S3 bucket to store logs

Step 2: Enable CloudWatch

- Create a log group in CloudWatch Logs

Step 3: Configure CloudTrail to send logs to CloudWatch

- Under CloudTrail > Trails > Edit > Enable log delivery to CloudWatch

Step 4: Generate Simulated Event

- Log out and log back into AWS account

- Or delete a test DynamoDB table or EC2 instance

Step 5: View Logs

- Go to CloudTrail > Event history > Filter by event type (e.g., ConsoleLogin)

- Or go to CloudWatch > Log groups > View logs

8) Modify EC2 Security Group to Restrict HTTP (Port 80) to Specific IPs and Allow HTTPS (443) for A

Step 1: Go to EC2 > Instances > Select your instance

Step 2: Click on Security > Security Groups > Inbound Rules > Edit

Step 3: Modify HTTP rule

- Protocol: HTTP, Port: 80

- Source: Custom (e.g., 192.168.1.0/24) - restrict to internal IPs

Step 4: Add HTTPS rule

- Protocol: HTTPS, Port: 443

- Source: Anywhere (0.0.0.0/0)

Click Save rules

9) Create IAM Policy to Allow Access to Specific S3 Buckets Only

Step 1: Go to IAM > Policies > Create policy

Step 2: Choose JSON and paste:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::example-bucket",
        "arn:aws:s3:::example-bucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Step 3: Review and create policy with a name like "S3LimitedAccess"

10) Create IAM User 'john_doe' with Specific Access

Step 1: Go to IAM > Users > Add user

Step 2: Set username to "john_doe", enable both programmatic and console access

Step 3: Attach existing policies directly:

- AmazonS3ReadOnlyAccess
- AmazonEC2FullAccess

Step 4: Review and create the user

Step 5: Sign in as john_doe using the AWS account ID login URL

Step 6: Verify Access

- Go to EC2 Dashboard > Should be able to create/terminate instances
- Go to S3 > Buckets > View files allowed, but no write/delete permission