Day 4 – IAM, Monitoring & Automation

---

1. IAM (Identity and Access Management)

🔹 What is IAM?

IAM is a service in AWS that helps you securely control access to AWS services and resources. You can create users, groups, roles, and apply fine-grained permissions using policies.

🔹 Key Concepts:

Term	Description
User	An individual identity with credentials
Group	A collection of IAM users
Role	A set of permissions you can assign to AWS services
Policy	A JSON document that defines permissions

✅ Practical: Create an IAM User with Limited Access

1. **Go to IAM Console:**
   https://console.aws.amazon.com/iam/

2. **Create User:**

   - Click **"Users" > "Add users"**
   - Username: `student-demo-user`
   - Select: **"Access key – Programmatic access"** and **"Password – AWS Management Console access"**
   - Set custom password

3. **Set Permissions:**

- Choose **"Attach existing policies directly"**
- Select `AmazonS3ReadOnlyAccess`

4. **Complete Creation**
   Download access credentials.

5. **Test Login:**
   Open AWS Console login link (provided during creation) and try accessing S3.

✅ Practical: Create a Custom IAM Policy and Group

1. **Go to "Policies" > "Create policy"**

2. Choose **JSON**, paste:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:Describe*",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    }
  ]
}
```

3. Name the policy: `DescribeEC2ListS3Policy`

4. Go to **"Groups" > "Create group"**

5. Attach the policy to group

6. Add user to group

---

2. CloudWatch (Monitoring AWS Resources)

🔹 What is CloudWatch?

Amazon CloudWatch monitors AWS cloud resources like EC2, S3, RDS. You can set **metrics**, view **logs**, and configure **alarms**.

✅ Practical: Monitor EC2 with CloudWatch

A. Enable Detailed Monitoring

1. Launch EC2 with "Enable CloudWatch detailed monitoring" checked (or enable it from EC2 > Actions).

B. Create Alarm on CPU Usage

1. Go to **CloudWatch Console:** https://console.aws.amazon.com/cloudwatch/
2. Click **“Alarms” > “Create Alarm”**
3. Select **EC2 > Per-Instance Metrics**
4. Choose `CPUUtilization` of your instance
5. Set threshold:
   Example: “Whenever CPU > 80% for 5 mins”
6. Notification:
   Create an SNS topic to get email alerts.

✅ Practical: View Logs

1. **Install CloudWatch Agent (Optional):**
   - Use for sending memory, disk metrics, or custom logs from EC2.
   - Requires SSM agent or manual install.
2. **Basic Steps:**
   - Connect to EC2 instance via SSH

- Install CloudWatch Agent using script
- Configure logs using a JSON config file
- Start agent

---

3. CloudTrail (Logging Account Activity)

🔹 What is CloudTrail?

CloudTrail tracks all **API calls** made in your AWS account, like creating an EC2 or deleting a bucket. Useful for **security auditing** and **troubleshooting**.

✅ Practical: Enable CloudTrail

1. Go to **CloudTrail Console:** https://console.aws.amazon.com/cloudtrail/
2. Click **“Create Trail”**
3. Name: `MyTrail`
4. Apply to all regions
5. Create new S3 bucket for log storage
6. Click **"Create trail"**

Now every action in AWS (like user login, EC2 launch, etc.) will be logged.

---

4. AWS CLI (Command Line Interface)

🔹 What is AWS CLI?

A command line tool to manage AWS services directly from terminal instead of using the Console.

✅ Practical: Setup AWS CLI on Windows

A. Install AWS CLI

- Download & install from: https://aws.amazon.com/cli/

B. Configure CLI

1. Open CMD or PowerShell
2. Run:

```
aws configure
```

3. Provide:
    - Access key
    - Secret key
    - Region: `ap-south-1`
    - Output format: `json`

✅ Sample Commands to Try

```
aws s3 ls
aws ec2 describe-instances
aws iam list-users
```

Final Lab: Combine IAM + CloudWatch

🔹 Goal: Create IAM Role and monitor EC2 instance with it

1. **Create IAM Role:**
    - Go to **IAM > Roles > Create Role**
    - Choose **EC2** as trusted service
    - Attach policy: `CloudWatchAgentServerPolicy`
    - Name: `EC2CloudWatchRole`
2. **Launch EC2 with IAM Role:**
    - While launching EC2, under “IAM Role” choose `EC2CloudWatchRole`
3. **Install CloudWatch Agent on EC2**
    - SSH into EC2
    - Run:

```
sudo yum install amazon-cloudwatch-agent
sudo
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-
wizard
```

- Follow wizard to select metrics to send

4. **View in CloudWatch:**
    - Go to CloudWatch > Metrics > EC2
    - Confirm custom metrics are visible
