CLOUD TRAIN
ACCELERATE YOUR GROWTH

ASSIGNMENT - MODULE 7

IAM & MONITORING

AWS Workshop

Contact us

TO ACCELERATE YOUR CAREER GROWTH

For questions and more details:

please call @ +91 98712 72900, or

visit https://www.thecloudtrain.com/, or

email at support@thecloudtrain.com, or

WhatsApp us @ +91 98712 72900

Exercise 1: AWS IAM Users, Groups and Roles

IAM User

a) Create an IAM user named **devuser** with AWS Management Console access and grant him AmazonEC2FullAccess to login to AWS console and manage EC2 resources.
b) Use the new user's credentials and try to login from separate browser instance and confirm the user has only EC2 access.

IAM Group

a) Create an IAM Group named **devgroup** and user **devuser** inside this group.
b) Assign this group only AmazonEC2FullAccess permission using policy.

IAM Role

a) Create an IAM Role named **devrole** for Another AWS Account **devuser** and mention the Account ID of **devuser**. (Refer hands-on doc for solution)
b) Assign AmazonEC2FullAccess permission to it and review the created role in IAM Console.

Exercise 2: Instance Role

a) Need to enable Full S3 access for an EC2 instance through an Instance role or IAM role.
b) Create an IAM Role named **InstanceS3Access** for **AWS Service** – **EC2**. (Refer hands-on doc for solution)
c) Assign AmazonS3FullAccess permission to it and review the created role in IAM Console.
d) Launch an EC2 instance by attaching this newly created role in IAM role key of configure instance.
e) Login to instance and try to test S3 access from it using below command. This command should list all S3 buckets in your account:

```
aws s3 ls
```

Exercise 3: IAM Policies

a) Create a JSON policy document to block S3 access to the Instance Role created in Exercise 2.
b) Create a custom policy from IAM console with name **BlockS3Access** using below policy document:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

c) Attach this custom policy to the Instance role **InstanceS3Access** created in Exercise 2 by opening it and clicking on Attach Policy inside.
d) Test your S3 access again from same EC2 instance where this role is attached. Your S3 access should be blocked now due to the effect of this new custom policy.

NOTE: DELETE ALL THE RESOURCES CREATED TO AVOID UNNECESSARY COSTS IN YOUR AWS ACCOUNT