AWS Module 3 Task

Sr. No.	Tasks
1.	Create an IAM user named "unnati". Attach the "AmazonS3ReadOnlyAccess" policy to this user. Generate an access key for the user and verify the user has read-only access to S3 buckets.
2.	"Create two IAM users: one named 'developer' with the 'AmazonEC2ReadOnlyAccess' policy attached to verify read-only access to EC2 instances, and another named 'admin' with the 'AdministratorAccess' policy attached to ensure full admin access. Generate access keys for both users."
3.	Launch a spot instance named "my-spot" with the AMI "Amazon Linux 2 AMI (HVM) (architecture x86_64), SSD Volume Type" in the us-east-1 region, with the key pair "myapp-key". Take an SSH session of the instance and create a file named greeting.txt which contains the text "Greetings from MyApp". Use the t2.micro instance type.
4.	Create an S3 bucket in the "us-east-1" region, key = class and value = kucl2.1, upload an Text file named "unnati.txt" to the bucket, and verify the upload by checking the file in the S3 console. Also, could you confirm if the content of "unnati.txt" should be "Hello from unnati" (Make Public “file” unnati.txt)
5.	Launch an instance named "WebServer" using the "Amazon Linux 2 AMI (HVM) - Kernel 5.10" image in the "us-east-1" region. Use "t2.micro" as the instance type and key pair "WebServer-Key". SSH into the instance and install HTTPD web server. Create an index.html file in the default web directory that contains the text "Welcome to WebServer".
6.	Create a S3 bucket in us-east-1 region with a tag, key = class and value = kucl2.0. Upload a index.html file into the bucket, content of index.html should be "hello from unnati". Configure to use this bucket to host a static website, IndexDocument should be index.html

7.	Launch instance using CLI (detials add myself) Launch an EC2 instance using CLI, use the following parameters: Name - "AWS CLI", region - "us-east-1", AMI - "Ubuntu Server 22.04 LTS (HVM) ((64-bit (x86)), SSD Volume Type", instance_type - "t2.micro", key pair - "Unnati-KuCL2.0". Take SSH/Putty session and create a file named mydata which contains "Hello AWS CLI".
8.	Create the following Policy, user group and users and assign specific policies to those groups: 1. Policy name: EC2-Admin, Group name: ec2-admin, users: user1, user2. ec2-admin group should have user1 and user2 in it. ec2-admin group should have permission to view, create and stop the ec2-instances. 2. Policy name: EC2-support, Group name: ec2-support, users: user3, user4. ec2-support group should have user3, user4 in it. ec2-support group should have read only permission for ec2-instances. 3. Policy name: S3-support, Group name: s3-support, users: user5, user6. s3-support group should have user5, user6 in it. ec2-support group should have read only permission for s3 storage
9.	Create a S3 bucket in us-east-1 region with a tag, key = course and value = aws and upload a object log.txt in the bucket. Use IAM to assign the following permission.(Create a policy) 1) For myuser1, give the permission as a list and read for a bucket 2) For myuser2, list, read and write for a specific object of the bucket 3) For myuser3, all permissions for a bucket
10	Lauch two instance name nfs-server and nfs-client in region us-east-1, AMI should be "Amazon Linux 2023 AMI", instance type should be t2.micro. Use key pair "Unnati-KuCL2.0". On nfs-server instance create a directory nfsshare at / location, configure NFS server to export this directory. On nfs-client instance create a directory nfstest in home directory of logged in user, configure this nfstest directory as NFS client. Then create a directory in nfstest called Kucl2.0 which contains a text file called mynotes.txt.

11.	Create a S3 bucket through AWS CLI in us-east-1 region with tag, key=cloud and value=AWS. Perform the following actions: - create 10 files named report1.pdf, report2.pdf ... report10.pdf and upload the 10 file to the bucket. - rename the report10.pdf to myreport.pdf from the bucket - remove the report2.pdf from the bucket