# Second Practical Assignment on Clouds

## Introduction Reminder

AWS Management Console is a web interface (via browser) that allows you to work with all AWS services. This is where you will create users, groups, and policies without using the command line or programmatic tools.

## Task 1: Creating the First IAM User

Objective: To become familiar with the basic element of the AWS access system — the IAM user.

### Steps:

1. Sign in to the AWS Management Console with the root account (this is the account you receive by default after registering in AWS).  
2. In the service search bar, find and open the IAM service.  
3. In the left menu, select Users → click Add users.  
4. Enter a username, for example: student1.  
5. Choose Password — AWS Management Console access (to create a password for console login).  
6. Enable Require password reset (so the user changes the password at first login).  
7. Complete the user creation process without adding groups or policies (the user will have minimal rights).  
8. Log in to the console under this user (using another browser or an incognito window).

### Result to be submitted:

- Screenshot of the user list in IAM showing student1.  
- Screenshot of successful login under student1 in the AWS Management Console.

## Task 2: Creating a Group and Assigning a Policy

Objective: To learn how to manage user access through groups and policies in the AWS console.

### Steps:

1. Sign in to the AWS Management Console with the root account.  
2. In IAM, open User groups → click Create group.  
3. Enter the group name: ReadOnlyGroup.  
4. In the list of policies, find and add IAMReadOnlyAccess.  
5. Complete the group creation.  
6. In the Users section, select student1 → Groups tab → click Add user to groups → add the user to ReadOnlyGroup.  
7. Sign out of the root account and sign in to the console under student1.  
8. Verify that the user can view information in IAM but cannot modify or delete resources.

### Result to be submitted:

- Screenshot of the ReadOnlyGroup with the attached policy.  
- Screenshot of the student1 user belonging to the group.  
- Screenshot of the console under student1 showing restricted actions.

## Task 3: Managing Users and Groups in IAM

Objective: To learn how to create multiple users, organize them into groups with different access rights, and apply policies.

### Steps:

1. Sign in to the AWS Management Console with the root account.  
2. In IAM, open Users → click Add users.  
3. Create four new users (e.g., admin1, user1, user2, user3).  
 Enable AWS Management Console access (with password).  
 For simplicity, use the Require password reset option.  
4. In the left menu, open User groups → click Create group.  
5. Create a group named Admins and attach the AdministratorAccess policy.  
6. Create a second group named ReadOnlyUsers and attach the IAMReadOnlyAccess policy.  
7. Add admin1 to the Admins group.  
8. Add user1, user2, user3 to the ReadOnlyUsers group.  
9. Verify that the users appear in their groups.

### Result to be submitted:

- Screenshot of the list of created users (admin1, user1, user2, user3).  
- Screenshot of the Admins group with the attached AdministratorAccess policy.  
- Screenshot of the ReadOnlyUsers group with the attached IAMReadOnlyAccess policy.  
- Screenshot of the users in their groups (1 in Admins, 3 in ReadOnly).

## Task 4: Configuring MFA for the Root Account

Objective: To provide an additional level of protection for the root account by enabling multi-factor authentication (MFA).

### Steps:

1. Sign in to the AWS Management Console with the root account.  
2. In the top menu, select your name (or root email address) → click Security credentials.  
3. In the Multi-factor authentication (MFA) section, click Assign MFA device.  
4. Select the Authenticator app option.  
5. Install the Google Authenticator app on your phone (if not already installed).  
6. Scan the QR code in Google Authenticator.  
7. Enter two consecutive codes from the app into the console.  
8. Confirm MFA activation.

### Result to be submitted:

- Screenshot in the AWS Management Console showing that MFA is enabled for the root account.