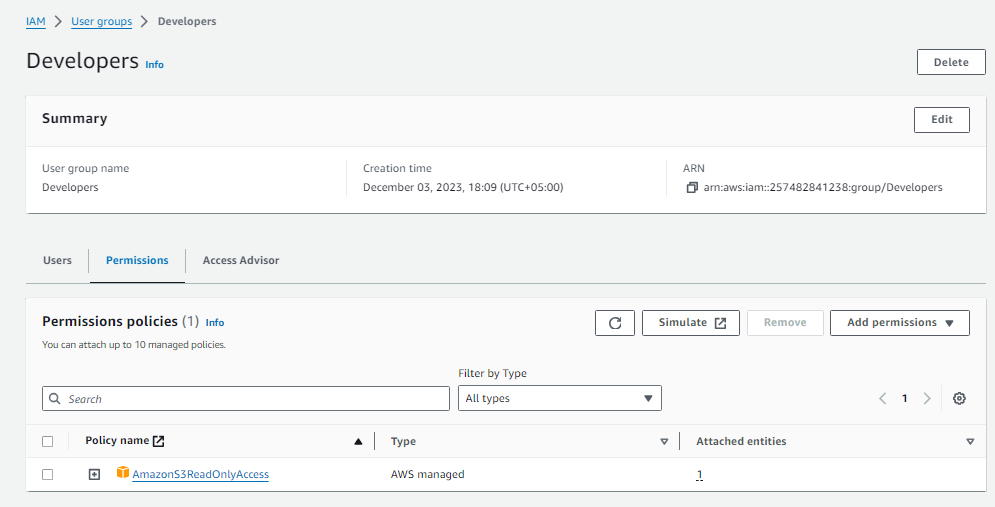
**Name Rimsha Azmat**

**Course DevOps**

**Submitted to Sir Sajjad**

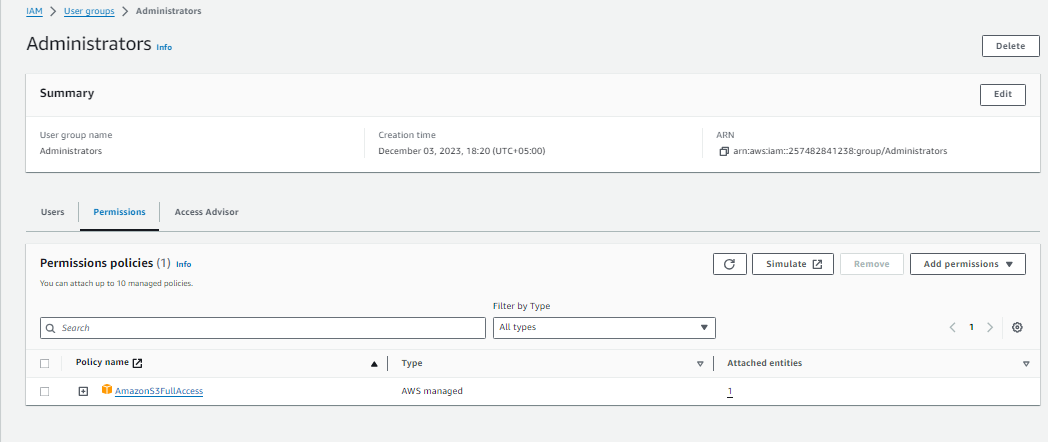
**AWS IAM Role and Policy Assignment**

1. **Create IAM Groups:**
   * Log in to the AWS Management Console.
   * Go to the IAM service.
   * Click on "Groups" in the left navigation pane.
   * Click "Create New Group" and name it "Developers."
   * Repeat the previous step to create a group called "Administrators."
2. **Create IAM Policies:**
   * Click on "Policies" in the left navigation pane.
   * For the "Developers" policy attach the following policy to the role:
     + AmazonS3ReadOnlyAccess
   * For the "Administrators" policy attach the following policy to the role:
     + AmazonS3FullAccess
3. **Attach Policies to Groups:**
   * Go to the "Groups" page again.
   * Click on the "Developers" group.
   * In the "Permissions" tab, click "Attach Policy."
   * Select the "Developers" policy and click "Attach Policy."
   * Repeat the previous steps for the "Administrators" group, attaching the "Administrators" policy.



Developer user group with AmazonS3 Read Only Access

Users with this policy can view, download, and list the contents of S3 buckets, but they can't make changes like uploading new files or deleting existing ones.

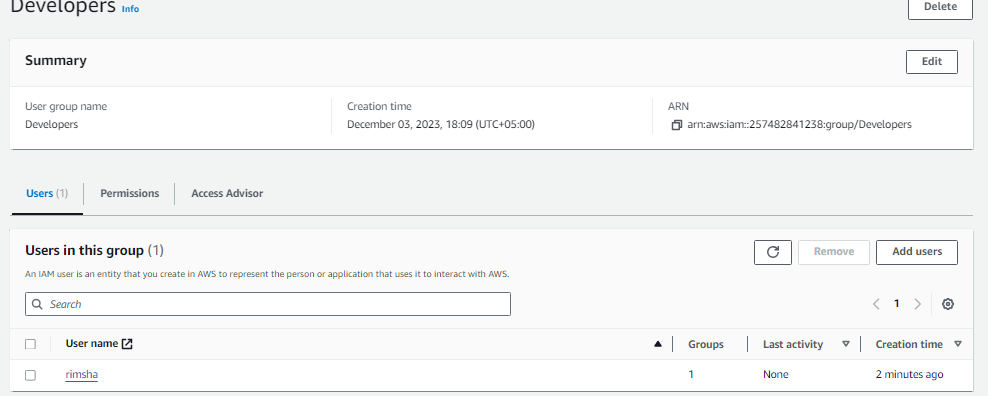


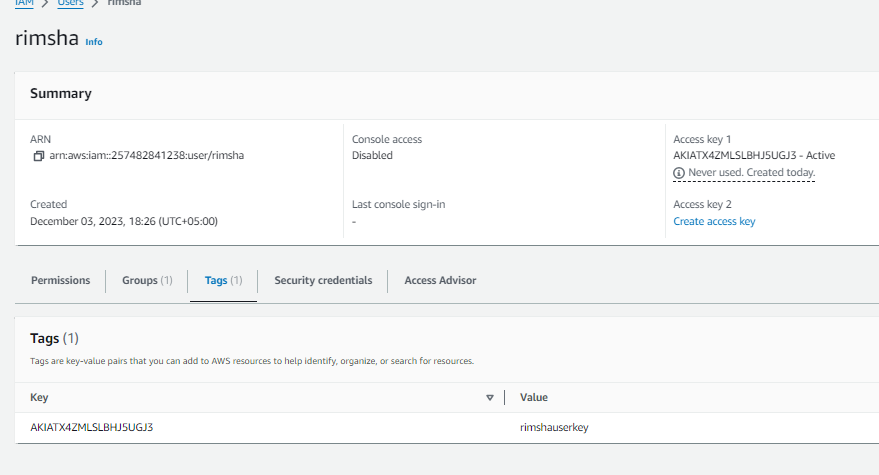
Administrators user group with AmazonS3 Full Access

Users or entities with this policy have full control over S3 resources. They can perform a wide range of actions, including creating, modifying, and deleting buckets, as well as uploading, downloading, and deleting any files.

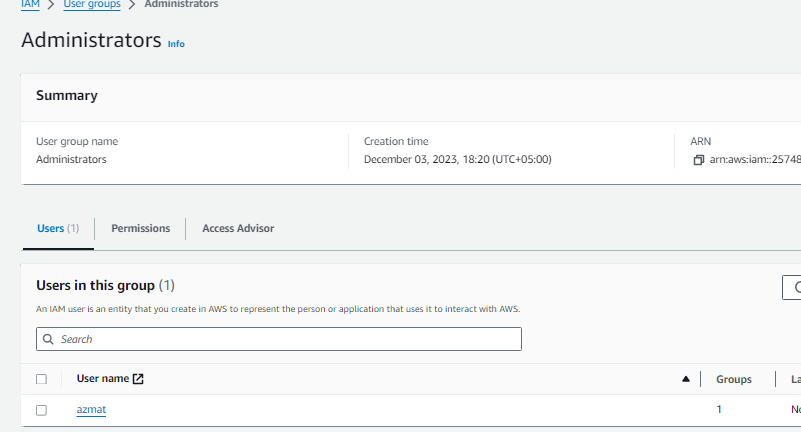
1. **Create IAM Users for each group:**
   * Go to the IAM service.
   * Click on "Users" in the left navigation pane.
   * Click "Add users"
   * Set the user name
   * Add user to group
   * For each user under "Security credentials"
     + Create access key
     + Command Line Interface (CLI)

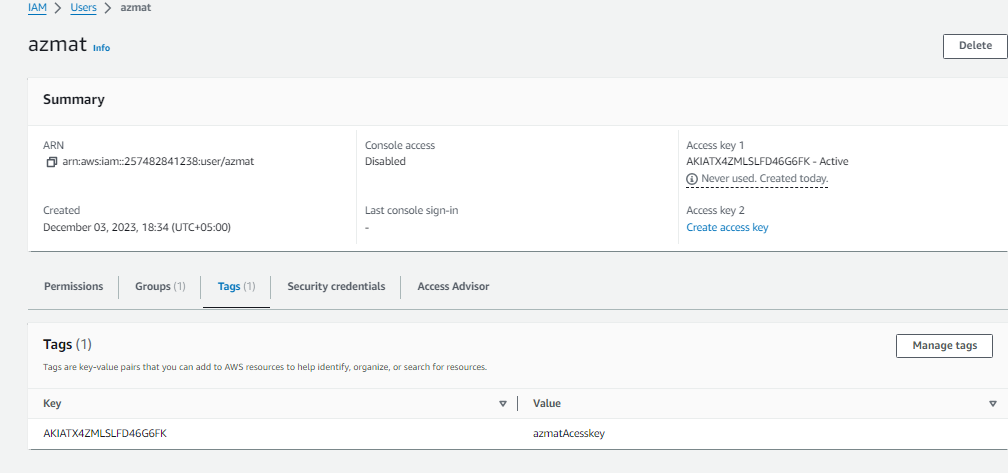
**For Developers**





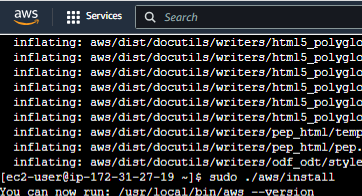
**For Administrators**



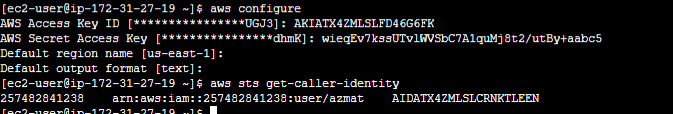


**Test the IAM Configurations:**

* Upload a file to the S3 bucket
  + FileName.EXT
* Launch an EC2 instance
* Login under ec2-user user
  + Install AWS CLI
    - curl "https://awscli.amazonaws.com/awscli-exe-linux-x86\_64.zip" -o "awscliv2.zip"  
      unzip awscliv2.zip  
      sudo ./aws/install



* aws configure
  + Enter User key
  + Enter Secret key
* Verify the user
  + aws sts get-caller-identity

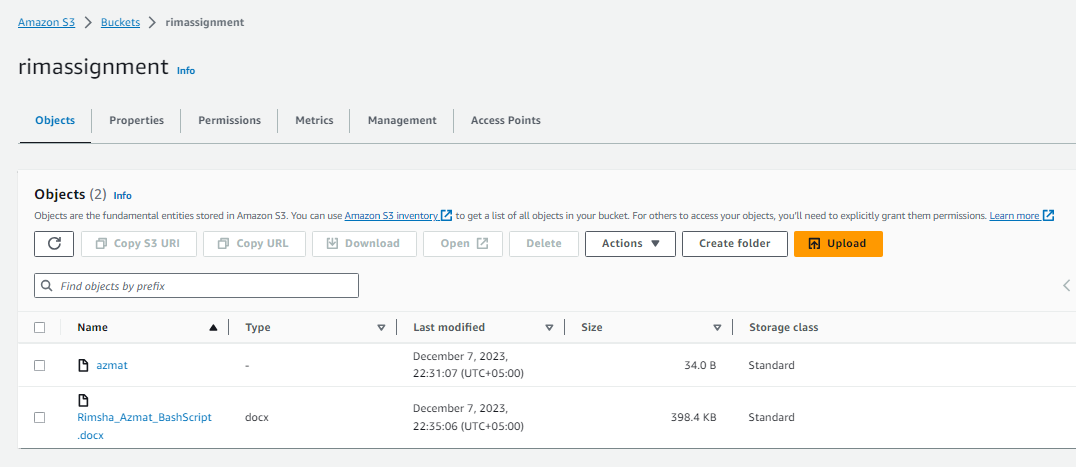


* **Download the file from S3**
  + - * aws s3 cp s3://devops-eit-202306XXXX/FileName.EXT .



* **Upload a file**
  + - aws s3 cp FileName.EXT s3://devops-eit-202306XXXX

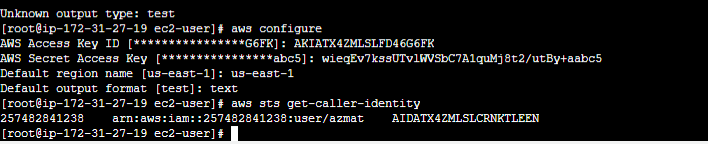




Login under root user

* Install AWS CLI
  + cd /home/ec2-user/
  + ./aws/install
  + aws configure
    - Enter User key
    - Enter Secret key







**For rimsha with ready only access permission**

