Create Cognito Identity Pool

Cognito Identity Pools provide secure, temporary AWS credentials to your users, whether they are authenticated (logged in) or unauthenticated (guests). For our project, we'll leverage unauthenticated identities to allow direct uploads from your frontend.

1. Set Up a Cognito Identity Pool

1. Open the Cognito Console: Search for "Cognito" in the AWS console and go to the service. Make sure you are in the correct AWS region.
2. Choose "Federated Identities" (Classic): On the left navigation pane, you'll see "User Pools" and "Federated Identities". Select "Federated Identities" (sometimes labeled "Manage Identity Pools" or "Identity Pools (new console experience)" with a link to "Go to old console"). We're looking for the *classic* experience here, which is often found under "Federated Identities".
3. Create a New Identity Pool:
    - Click the "Create new identity pool" button.
    - "Identity pool name": Give it a descriptive name, like S3UploadFrontend
    - Under "Unauthenticated identities", make sure to check the box next to "Enable access to unauthenticated identities". This is essential for guest users to upload.
    - Click "Next".
4. Attach IAM Roles: AWS will now prompt you to attach IAM roles. By default, it will offer to create two new roles for you: one for authenticated users and one for unauthenticated users.
    - Simply click "Allow" or "Create Role" to let Cognito create these default roles. We'll modify the unauthenticated role in the next step.
5. Finish the Setup: Follow any remaining prompts to complete the creation of the identity pool.

6. Copy the Identity Pool ID: Once created, you'll be redirected to a dashboard for your new identity pool. You'll see an Identity Pool ID in the format REGION:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (e.g., ap-south-1:1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p). Copy this ID down, as you'll need it for your frontend application to interact with Cognito.

2. Modify IAM Role for Unauthenticated Users

The default unauthenticated role created by Cognito only has very basic permissions. We need to explicitly allow it to upload files to your S3 input bucket.

1. Go to the IAM Console: Open the IAM service in your AWS console.
2. Find the IAM Role:
    - In the left navigation pane, click on "Roles".
    - Search for the role that Cognito just created for unauthenticated users. It will typically have a name like: Cognito_S3UploadFrontendUnauth_Role_ap-south-1_... (the suffix will be a random string, and the region might differ).
3. Attach This Inline Policy:
    - Click on the found role to view its details.
    - Go to the "Permissions" tab.
    - Click "Add permissions" and then "Create inline policy".
    - Select the "JSON" tab and paste the following policy document. Remember to replace image-processing-input-internship with your actual input bucket name, image-processing-input!

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3Upload",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
```

```
            ],
            "Resource": "arn:aws:s3:::image-processing-input/*"
        }
    ]
}
```

Explanation of the policy:

- "Sid": "AllowS3Upload": A unique identifier for this policy statement.
- "Effect": "Allow": Grants permission.
- "Action": ["s3:PutObject"]: Specifically allows the PutObject action, which is used for uploading files to S3.
- "Resource": "arn:aws:s3:::image-processing-input/*": **Crucially**, this restricts the upload permission to *only* objects within your image-processing-input bucket. The /* means all objects *within* that bucket.

Click **"Review policy"**.

Give the policy a name, such as S3UploadAccess.

Click **"Create policy"**.