Create an IAM Role for Lambda (with S3 Permissions)

This IAM role is specifically designed to allow your Lambda function to:

- **Read from the input bucket: So, it can access the original images uploaded by users.**
- **Write to the output bucket: To save the processed images after transformation.**
- **Log to CloudWatch: Essential for debugging, monitoring, and viewing any output from your Lambda function.**

Let's get this set up:

1. **Navigate to the IAM Console: In your AWS console, search for "IAM" and click on the service.**
2. **Start Creating a New Role:**
   - **In the left-hand navigation pane, click on "Roles".**
   - **Then, click the "Create role" button.**
3. **Select Trusted Entity and Use Case:**
   - **For "Trusted entity type", choose "AWS service".**
   - **For "Use case", select "Lambda" from the list.**
   - **Click "Next".**
4. **Attach Permissions Policies: Now, we'll grant the specific permissions our Lambda function needs. In the "Add permissions" section:**
   - **In the search bar, type and select the following policies:**
     - **AmazonS3FullAccess (For simplicity during setup, we're granting full S3 access. In a production environment, you would want to restrict this to only the necessary read/write actions on your specific buckets.)**

- **CloudWatchLogsFullAccess (This allows your Lambda function to write logs to CloudWatch, which is incredibly useful for troubleshooting.)**

- **Click "Next".**

5. **Name and Create the Role:**
   - **For "Role name", enter: lambda-image-processing-role**
   - **(Optional: You can add a description to explain the role's purpose.)**
   - **Review the selected policies and settings.**
   - **Finally, click "Create role".**