**Documentation: Create and Test an EC2 Instance Profile Role for S3 Access**

Set up an IAM role for an EC2 instance to access Amazon S3 and test if the permissions are working as expected.

**Step 1: Create the IAM Role with S3 Access Permissions**

1. **Sign in to the AWS Management Console**.
   * Go to **IAM Dashboard**.
2. **Create a New Role**:
   * In the **IAM** dashboard, select **Roles** from the left-hand menu.
   * Click **Create role**.
   * Under **Select trusted entity**, choose **AWS service**.
   * Select **EC2** as the use case for the role. This defines that the role is meant to be used by EC2 instances.
   * Click **Next**.
3. **Attach S3 Access Policy**:
   * In the **Permissions** step, attach the necessary S3 access policy:
     + **AmazonS3ReadOnlyAccess** if the EC2 instance only needs read access to S3.
     + **AmazonS3FullAccess** if the EC2 instance requires full access to S3.
   * Alternatively, create a custom policy for more granular control.
4. **Name the Role and Create It**:
   * Name the role, for example, EC2S3AccessRole.
   * Click **Create role** to finalize.

**Step 2: Launch an EC2 Instance with the IAM Role Attached**

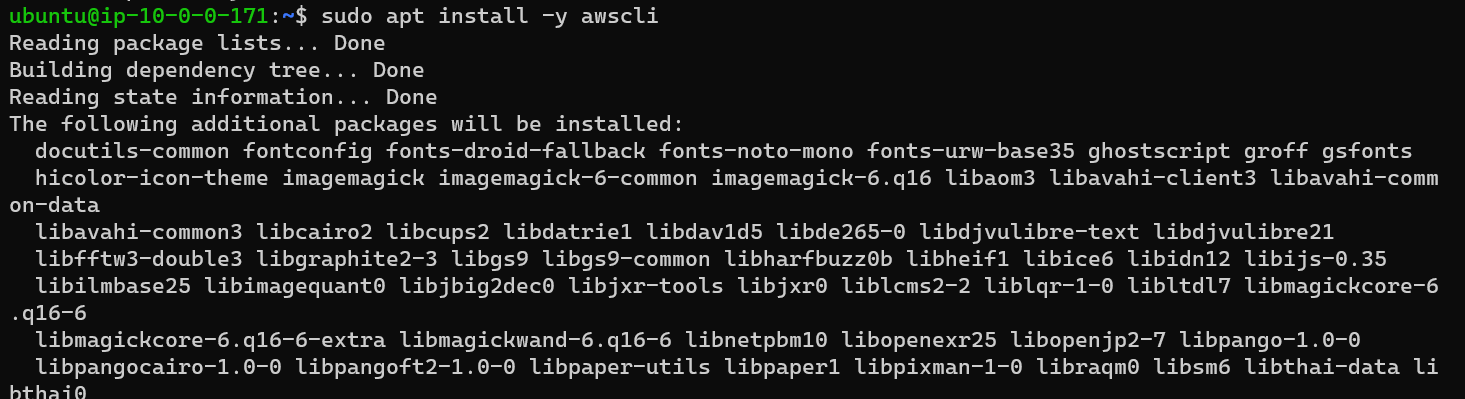
1. **Navigate to EC2 and Launch an Instance**:
   * Go to the **EC2 Dashboard** and click **Launch Instance**.
2. **Configure the Instance and Attach the IAM Role**:
   * Under **IAM role**, select the EC2S3AccessRole that you created.
   * Choose other configuration options as required (e.g., AMI, instance type, key pair, network settings).
3. **Launch the Instance**:
   * Click **Launch** to start the instance with the attached role.

**Step 3: Connect to the EC2 Instance**

1. **Connect to the EC2 Instance Using SSH**:
   * Use the key pair you selected when launching the instance.
   * Run the following command to connect:

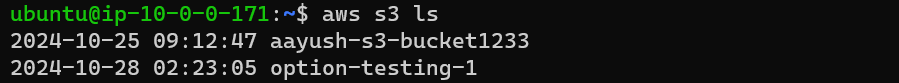
**ssh -i "path/to/your-key.pem" ec2-user@<public-ip-address>**

1. **Ensure AWS CLI is Available**:
   * Amazon Linux AMIs typically come with the AWS CLI pre-installed. If not, install it by running:

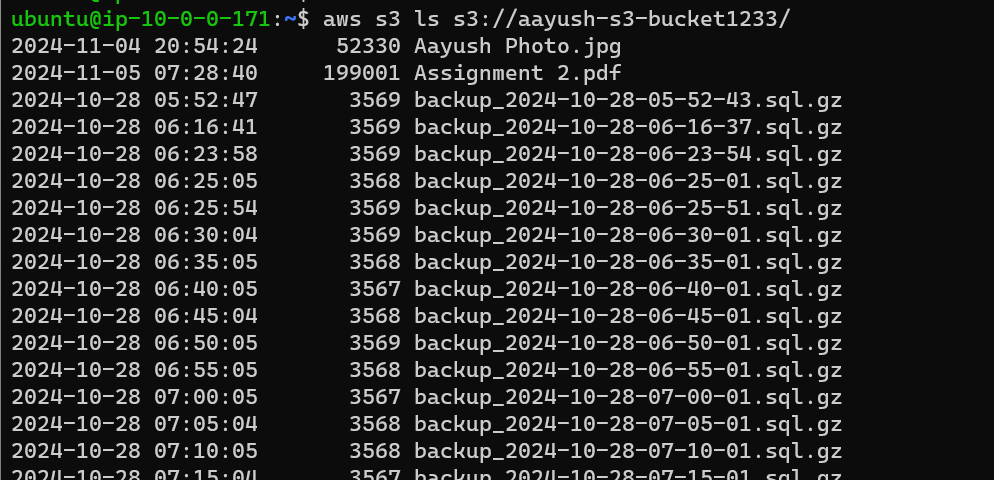
**sudo apt install -y awscli  
  
**

**Step 4: Test S3 Access from the EC2 Instance**

1. **Verify Permissions by Listing S3 Buckets**:
   * Run this command to check if you have access to S3:

**aws s3 ls  
**

* + If the IAM role is configured correctly, this command will list all accessible S3 buckets.
  + To see all the content of specific bucket

aws s3 ls s3://aayush-s3-bucket1233/  


1. **Test Additional S3 Actions (Based on Role Permissions)**:
   * **Read Access**: Test downloading a file (requires s3:GetObject permission).

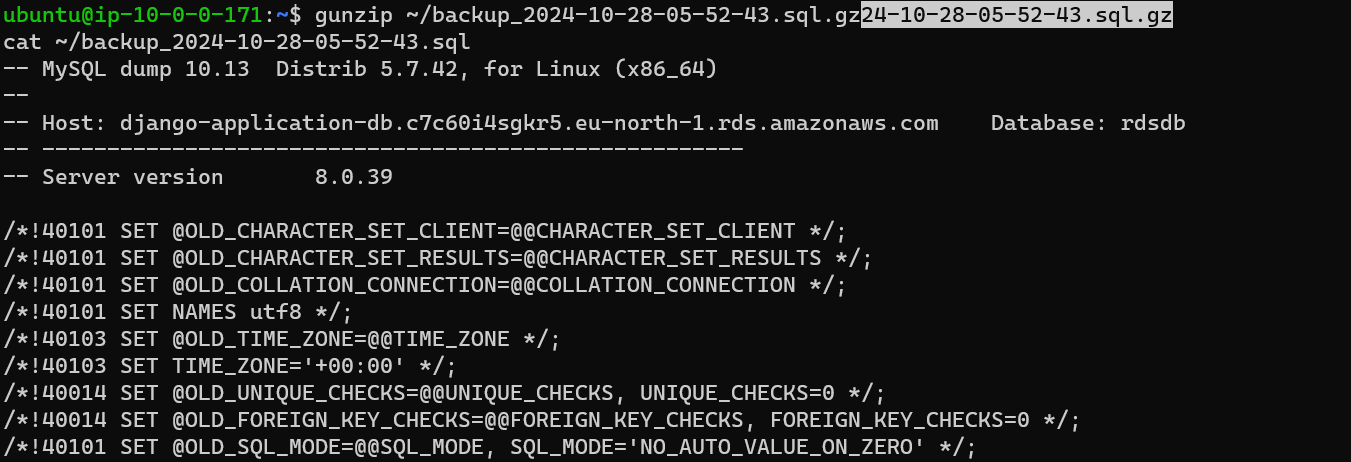
**aws s3 cp s3://aayush-s3-bucket1233/backup\_2024-10-28-05-52-43.sql.gz ~/**

* + **Write Access**: Test uploading a file (requires s3:PutObject permission).

**echo "Testing S3 access from EC2 instance" > testfile.txt**

**aws s3 cp testfile.txt s3://aayush-s3-bucket1233/**

* + To read the file you need to first unzip it.



1. **Troubleshooting**:
   * If you receive an AccessDenied error, ensure:
     + The EC2 instance is using the correct IAM role.
     + The IAM role has the correct S3 permissions.
     + Any bucket policy attached to the S3 bucket allows the necessary actions.

**Summary**

**By following these steps, we should be able to verify that the EC2 instance can access S3 resources as specified by the IAM role's permissions. Testing the permissions confirms that the instance profile role is set up correctly.**