

POSTMAN: AWS IAM Policy (`src/Utils/multer/s3.config.ts`)

- في الملف ده، إحنا بنستخدم الـ `Access Key` والـ `Secret Key` والـ `Bucket Name` اللي متخزين في ملف الـ `.env`.
- لو الـ `IAM Policy` في AWS مش مديّة صلاحيات لليوزر (اللي إنتي غالباً مسمياه `s3permission`) إنه يوصل للـ `Bucket` ده، الـ `S3 Client` في الكود كان هيطلع لك `error` (غالباً `Access Denied`).

2. لوحة تحكم AWS (حيث توضع الـ Policy):

المكان الحقيقي للـ `Policy` مش في فايل في الكود، هو جوه `AWS Console` تحت خدمة الـ `IAM` (Identity and Access Management).

- هناك إنتي بتختاري الـ `User` اللي الكود بيستخدم الـ `Keys` بتاعته.
- وبتضيفي له `Inline Policy` أو `Attached Policy` اللي فيها الـ `JSON` اللي بيسمح بـ `s3:PutObject` و `s3:PutObjectAcl`.

```
}
message": "User: arn:aws:iam::600696639571:user/s3permission is not authorized to"
perform: s3:PutObject on resource:
\"arn:aws:s3:::nodes3c/SOCIAL_MEDIA_APP/users/undefined/5e167fe0-7a8d-45d7-8d39-1
c1abcd109a0-toleen1.jpeg\" because no identity-based policy allows the s3:PutObject
\"action
{
```

1. تحليل المشكلة (AWS IAM Policy)

اليوزر اللي إنتي مستخدمة الـ `Access Key` بتاعه (اللي اسمه `s3permission`) معندوش صلاحية إنه يرفع ملفات `(s3:PutObject)` على الـ `Bucket` اللي اسمه `nodes3c`.

2. الحل من داخل حساب AWS (خطوات سريعة):

1. افتحي `AWS Console` وروحي لخدمة الـ `IAM`.
2. اختاري `Users` من القائمة اللي على الشمال، ودوسي على اليوزر اللي اسمه `s3permission`.
3. دوسي على زر `Add permissions` ثم `Create inline policy`.

4. اختاري تبويب **JSON** وامسحي اللي فيه وحطي الكود ده:

4. اختاري تبويب **JSON** وامسحي اللي فيه وحطي الكود ده:

```
JSON

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::nodes3c/*"
    }
  ]
}
```

5. دوسي **Review policy** وسميها أي اسم (مثلاً **S3UploadPolicy**) ودوسي **Create**.

و انا اعرف اكتب الكود ده منين لما اعوز اعمل الحركة دي

```
6. }
7. "Version": "2012-10-17"
8. ]:"Statement"
9. }
10. "Effect": "Allow"
11. ]:"Action"
12. "s3:PutObject"
13. "s3:PutObjectAcl"
14. "s3:GetObject"
15. ,[
16. "*/Resource": "arn:aws:s3:::nodes3c"
17. {
18. [
19. {
20.
```

سؤال ممتاز! الكود ده اسمه **IAM Policy**، وهو لغة التواصل مع **AWS** عشان تحدد مين مسموح له يعمل إيه. إنتي مش محتاجة تحفظيه خالص، فيه **3 طرق** تخليكي توصلي له بسهولة:

1. الـ Visual Editor (أسهل طريقة للمبتدئين)

جوة AWS وأنت بتضيفي Permission لليوزر، هتلاقي اختياريين: **JSON** و **Visual**.

- لو اخترتي **Visual**، الـ AWS هيطلع لك واجهة فيها مربعات اختيار (Dropdowns).
- بتختاري الخدمة: **S3**.
- بتختاري الأكشن: **PutObject**.
- بتختاري الـ **Bucket Name**.
- وفي الآخر AWS هو اللي بيحول اختياراتك دي لكود الـ JSON اللي شوفتيه.

2. الـ AWS Policy Generator (الأداة الرسمية)

فيه موقع رسمي من أمازون اسمه [AWS Policy Generator](#).

- بتحدد نوع الـ Policy (IAM Policy).
- بتكتبي الأكشنز اللي محتاجها (زي **PutObject**).
- بتدوسي **Generate**، وهو بيكتبك الكود جاهز تاخديه كوبي بيست.

3. فهم الـ Structure (عشان تبقي "برنسياسة" في الـ IAM)

الكود ده عبارة عن 4 قطع أساسية لو فهمتيهم هتعرفي تكتبيه بنفسك:

1. **Effect**: دي دايماً يا إما **Allow** (سماح) أو **Deny** (منع).
2. **Action**: دي "الفعل" اللي الكود هيعمله. لو رفع ملفات يبقى **PutObject**. لو قراءة ملفات يبقى **GetObject**.
3. **Resource**: دي "المكان" اللي الفعل ده هيجصل فيه. وبستخدم فيها الـ **ARN** (عنوان الـ Bucket بناعك).
4. **Version**: دي ثابتة دايماً بتاريخ **2012-10-17** (ده تاريخ إصدار اللغة دي في AWS).

💡 نصيحة للمستقبل:

أي خدمة تانية هتعوزي تربطها (زي SES للإيميلات أو DynamoDB للبيانات)، كل اللي عليك عمليه هو سيرش بسيط في جوجل على: **"AWS IAM policy for S3 upload example"**، وهتلاقي أمازون حاطة الكود ده كـ Template ثابت.