Your CloudFront distribution serves content from S3. Suddenly, users report 403 Forbidden errors. What could cause this? How would you debug and fix it?

CloudFront is serving content from an **S3 bucket**. Suddenly users see:
403 Forbidden → means *CloudFront tried to fetch the file, but S3 refused access.*

Common Causes

1. **S3 Bucket is Private** (default setting in S3 is *block public access*).
   - If CloudFront doesn't have permission, S3 rejects with 403.
2. **Wrong Bucket Policy**
   - Maybe policy was misconfigured or removed.
3. **Origin Access Control (OAC) or Origin Access Identity (OAI)**
   - If using OAC/OAI, the S3 bucket must allow access **only to CloudFront**.
   - If not set properly, you get 403.

Debugging Steps

Step 1: Check if file exists

- Try opening the S3 file directly (e.g., https://bucket.s3.amazonaws.com/index.html).
- If that also gives 403 → file missing or bucket access problem.

Step 2: Check if CloudFront is allowed

- Go to your CloudFront origin settings:
  - Are you using **OAI** (older method) or **OAC** (new recommended method)?
- Then check the **S3 bucket policy** or **resource policy**.

✅ Fixing It

🔷 **Case 1: Using Origin Access Control (OAC) (recommended)**

1. In CloudFront → Attach OAC to your S3 origin.
2. In S3 → Set **bucket policy to allow access from that OAC**.
   Example policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::my-bucket/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn":
"arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE"
        }
      }
    }
  ]
}
```

Your CloudFront distribution serves content from an S3 bucket. Suddenly users get **403 Forbidden** errors. What is the most likely cause?
A. S3 bucket is private and CloudFront doesn’t have permission.
B. CloudFront can’t cache JavaScript files.
C. Route53 DNS record is incorrect.
D. The object TTL expired in CloudFront.

A. S3 bucket is private and CloudFront doesn’t have permission. ✅

You are using CloudFront with **Origin Access Control (OAC)**, but still getting **403 Forbidden**. What should you check first?
A. Whether the S3 bucket policy allows the OAC to access the bucket.
B. Whether CloudFront supports S3 origins.
C. Whether CloudFront distribution is in the same region as S3.
D. Whether invalidation was created.

A. Whether the S3 bucket policy allows the OAC to access the bucket. ✅

While debugging a **403 from CloudFront**, you try opening the S3 file directly (https://bucket.s3.amazonaws.com/index.html) and it also gives 403. What does this mean?

A. File doesn’t exist or bucket access is blocked.
B. CloudFront cache is corrupted.
C. CloudFront distribution is disabled.
D. Route53 health checks failed.

A. File doesn’t exist or bucket access is blocked. ✅