🔵 PART 1 — Prerequisites

✓ You already have:

- Application Load Balancer (ALB)
- Region: **us-east-1**
- AWS Account ID: **526018540742**

🔵 PART 2 — Create S3 bucket

1. Go to **S3 → Create bucket**
2. Bucket name:

```
alb-logs-ags01
```

3. Region: **same as ALB (us-east-1)**
4. Leave defaults → Create

🔵 PART 3 — Bucket Policy (MOST IMPORTANT)

For **us-east-1**, ALB uses this AWS account to write logs:

```
127311923021
```

Go to:

S3 → alb-logs-ags01 → Permissions → Bucket policy

DELETE everything and paste:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSALBLogDeliveryWrite",
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::127311923021:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::alb-logs-ags01/AWSLogs/526018540742/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": "AWSALBLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::127311923021:root"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::alb-logs-ags01"
    }
  ]
}
```

Save.

⬤ PART 4 — Do NOT touch ACLs

Go to:

S3 → alb-logs-ags01 → Permissions → ACL

✓ Leave as default

✗ Do NOT add:

- S3 log delivery group
- Everyone
- Authenticated users

ALB uses bucket policy, not ACL.

🔵 PART 5 — Enable logs on ALB

Go to:

EC2 → Load Balancers → AGS-01 → Attributes

Enable:

✓ Access logs

Bucket:

`s3://alb-logs-ags01`

Save.

🔵 PART 6 — Generate traffic

Open in browser:

http://AGS-01-619536953.us-east-1.elb.amazonaws.com

Refresh 4–5 times.

🔵 PART 7 — Verify logs

Go to:

S3 → alb-logs-ags01

You should see:

```
AWSLogs/
  526018540742/
    elasticloadbalancing/
      us-east-1/
        2026/01/...
```

Files = success 🎉

🌐 TROUBLESHOOTING (VERY IMPORTANT)

❌ Error: "Access Denied for bucket"

Causes & fixes:

1️⃣ Wrong principal

❌ elasticloadbalancing.amazonaws.com

✅ `arn:aws:iam::127311923021:root`

2️⃣ Missing GetBucketAcl

Must allow:

`s3:GetBucketAcl`

3️⃣ Wrong Resource path

Must be:

`arn:aws:s3:::alb-logs-ags01/AWSLogs/526018540742/*`

Not:

```
arn:aws:s3:::alb-logs-ags01/*
```

4 Bucket in wrong region

ALB region = S3 bucket region

Both must be **us-east-1**

5 Tried to fix with ACLs

❌ Wrong

✓ Fix bucket policy only

🎯 EXAM ONE-LINERS

"ALB access logs are stored in S3 by enabling access logs in ALB attributes and granting the regional ELB log delivery account permission to write to the bucket."

"ALB logging uses a special AWS account, not elasticloadbalancing.amazonaws.com, to write logs."

🧠 MEMORY HOOK (so you don't forget)

ALB logs need:

```
S3 bucket
+ Correct region
+ Correct log delivery account
+ PutObject
+ GetBucketAcl
```