# PART 1 — TAG YOUR TWO DATA SERVER INSTANCES

### On the 2 data servers only, add a tag:

EC2 → Select instance → **Tags** → Add tag

```
Key: Access
Value: Restricted
```

👉 Meaning in simple words:

**“This server is marked as restricted.”**

# PART 2 — CREATE THE DENY POLICY

IAM → Policies → Create policy → JSON tab → paste this:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Access": "Restricted"
        }
      }
    }
  ]
}
```

Name it:

```
Deny-Restricted-EC2
```

## PART 3 — CREATE A GROUP AND ATTACH POLICY

IAM → Groups → Create group

Name:

```
Restricted-Users
```

Attach policy:

```
Deny-Restricted-EC2
```

## PART 4 — ADD THE TWO USERS TO THIS GROUP

IAM → Users → select user1 & user2 → Add to group

Choose:

```
Restricted-Users
```

DONE ✅

## 🧠 WHAT JUST HAPPENED (SIMPLE)

- 2 servers have tag → `Access=Restricted`

- Group policy says → ❌ “Deny EC2 access to anything with this tag”
- 2 users are in that group
- Result:

✓ They can access 3 normal servers

❌ They cannot access 2 data servers

## 🗒 SIMPLE ONE-LINERS (TERMS)

**Tag:**

👉 A label on AWS resources (like a sticker on a machine)

**IAM Policy:**

👉 A rule that says what you can or cannot do

**Group:**

👉 A collection of users with same permissions

**Explicit Deny:**

👉 A hard NO that overrides any YES

*ec2: :**

👉 All EC2 actions (start, stop, terminate, etc.)

**Condition:**

👉 Apply rule only when something matches (here: tag)

**ResourceTag:**

👉 Read the tag on the instance

# 🎯 INTERVIEW ONE-LINER

“Tag restricted instances and attach an explicit deny policy to a group for selected users; deny overrides allow.”