1. **Can an IAM User be Added to Role?**

We can't directly attach a user to a role. Instead, a user can *assume* a role when needed, which gives them temporary permissions. This is used to give extra or special access for a limited time without permanently attaching it to the user.

Ex: Think of a doctor in a hospital — normally they have access to patient records, but if they need to enter the operation theatre, they wear a special access badge (role). Once they leave, they give the badge back. Similarly, in AWS a user assumes a role temporarily to get extra permissions and then returns to their normal access.

2. **If One IAM User have AdministratorAccess but still not able to Use EC2 & S3?**

Even if a user has AdministratorAccess, they might not be able to use EC2 or S3 if there are **Service Control Policies (SCPs), Permission Boundaries, or explicit Deny policies applied**. In AWS, Deny always overrides Allow, so higher-level restrictions can block access even with admin rights.

There are **4 main ways** an IAM user with AdministratorAccess might still be blocked:

- **Service Control Policies (SCPs)** – In AWS Organizations, SCPs can restrict what even admins can do.
- **Permission Boundaries** – These act like a "maximum limit" on what the user can do, no matter what their policy says.
- **Explicit Deny in Policies** – If any policy (IAM, S3 bucket policy, etc.) has an explicit Deny, it overrides Allow.
- **Resource-based Policies** – Services like S3, KMS, or SQS have their own policies. If those deny access, the user can't use them.

Ex: **It's like having Pluralsight Cloud+ access — you get almost everything. But sometimes certain courses, regions, or features are restricted by the company**.