# The AWS Certified Solutions Architect Professional Exam

IAM

* Ec2 Instances Roles: uses EC2 metadata service- 1 role at a time per instance
* Service Roles: API Gateway, Code Deploy, etc.,
* Cross Account Roles: helpful to access another account to perform some action in that account

Policies: Defined what a role or individual can do, and they are of 3 types

* AWS Managed – Maintained by AWS
* Customer Managed – maintained by us and we can version them
* Inline policies – Policies assigned to one specific user or a role.

Resource Based Policies (S3 bucket, SQS policies, etc.,)

* Explicit Deny has precedence over Allow
* Best practice use least privilege for maximum security

**IAM AWS Managed Policies:**

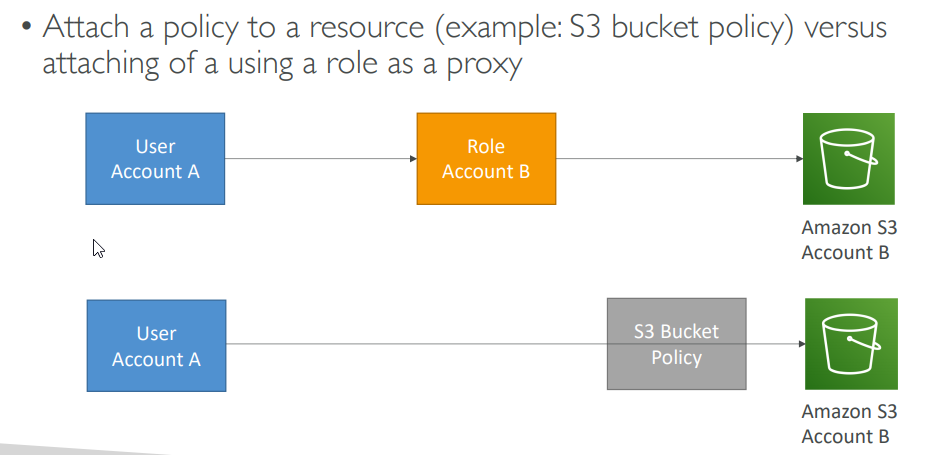
* **AdministratorAccess**- Provide access to all the resources
* **PowerUserAccess** –
  + Does not allow to modify IAM, organizations, accounts
  + Allow some few IAM actions like (iam:CreateServiceLinkedRole, DeleteServiceLinkedRole, ListRoles, DescribeOrganization, ListRegions)

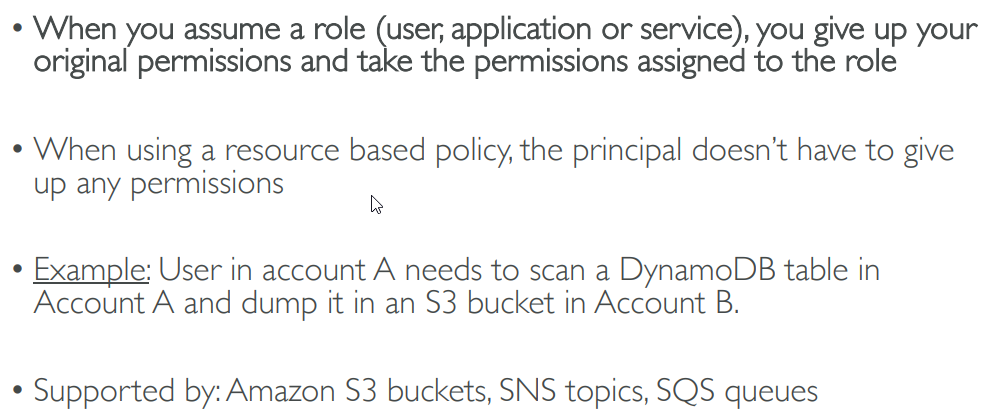
Note: If in case if you do not want to deny all the actions with in a resource then you have to use Allow followed by NotAction by using deny it will explicitly deny all the Allow actions if we allow few actions with in the same resource.



* IAM Policies Conditions: 6 of them
  + String
  + Boolean
  + Numeric
  + Date
  + IP Address
  + Null
* IAM Policies Variables and Tags: 3 of them
  + AWS Specific
  + Service Specific
  + Tag Based

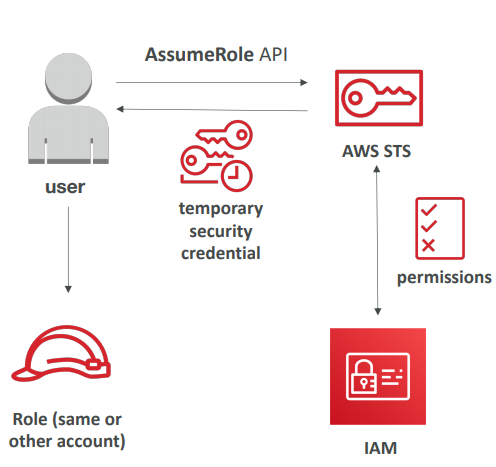
**\*\*\*\*IAM Roles vs Resource Base Policies\*\*\*\***

****

****

**\*\*\*\*Using STS to Assume a Role \*\*\*\*\*\***

* **STS – Security Token Service**
* **Temporary credentials are valid for 15 mins- 1hr**

****