# 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:**

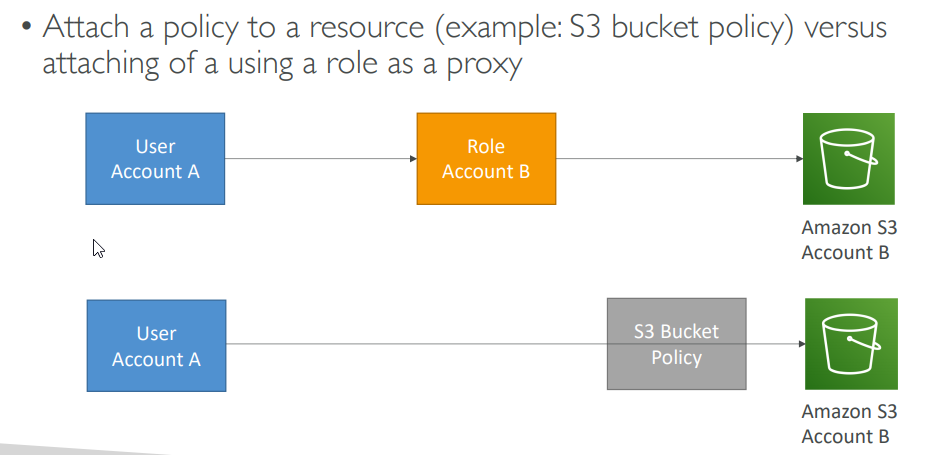
* **AdministratorAccess**- Provide access to all the resources
* **PowerUserAccess** –
  + Does not allow to modify IAM, organizations, accounts
  + Allow some few IAM actions like (iam:CreateServiceLinkedRole, DeleteServiceLinkedRole, ListRoles, DescribeOrganization, ListRegions)

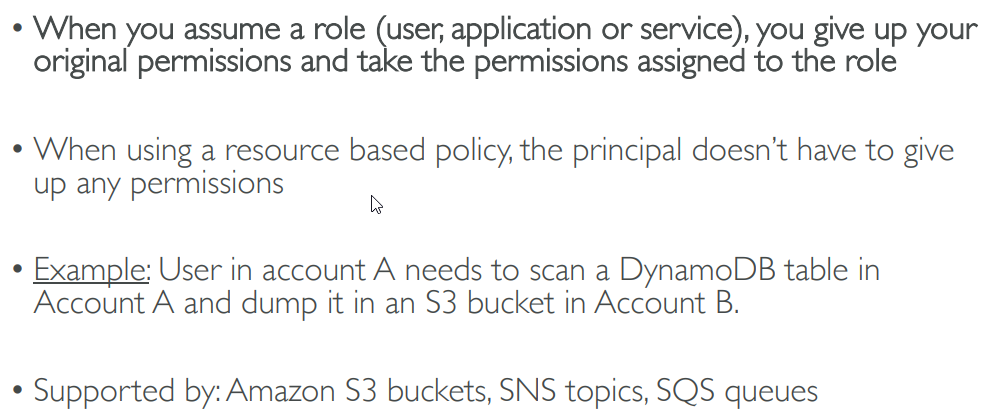
Note: If in case if you do not want to deny all the actions with in a resource then you have to use Allow followed by NotAction by using deny it will explicitly deny all the Allow actions if we allow few actions with in the same resource.



* 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

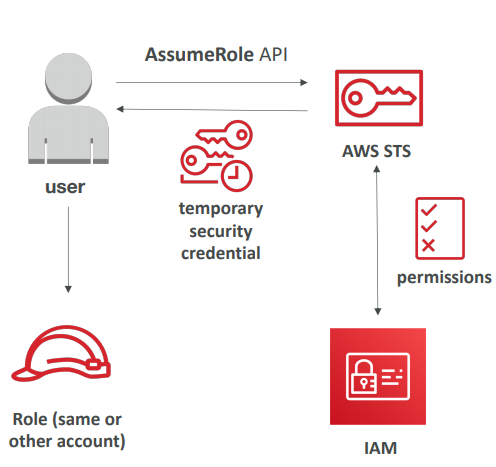
**\*\*\*\*IAM Roles vs Resource Base Policies\*\*\*\***

****

****

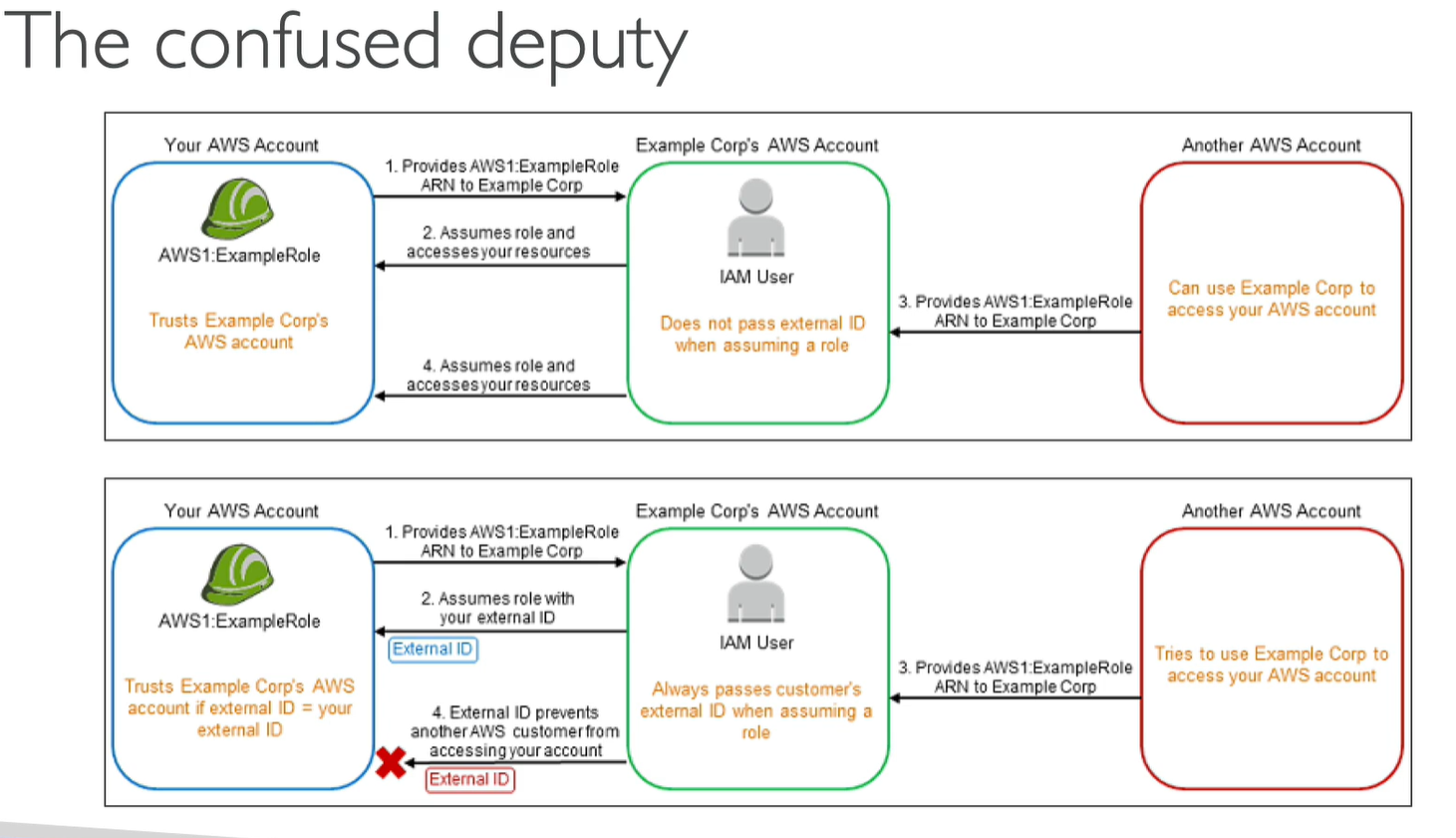
**\*\*\*\*Using STS to Assume a Role \*\*\*\*\*\***

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

****

**Providing Access to Third Parties**

* Zone of Trust- Accounts with in Organization
* Outside Zone of Trust – 3 Parties
* IAM Analyzers are used to identify the resources that are exposed.
  + External ID – Secret between you and 3 Party



**Identity Federation in AWS**

* Federations allows users that are outside the AWS account allow to access the resources by providing them access roles
* Federations can have of Multiple flavors
  + SAML 2.0
  + Custom Identity Broker
  + Web Identity Federation with Amazon Cognito
  + Web Identity Federation without Amazon Cognito
  + Single Sign on
  + Non-SAML with AWS Microsoft AD
* Using Federation you don’t need to create a IAM users

**SAML 2.0 –**

* To integrate AD/ADFS with AWS
* Provides Access to AWS Console or CLI
* No need to re create an IAM user for each of our employee.

**Custom Identity Broker:**

* In this case its custom identity broker that communicates with STS service to get temporary credentials to access AWS console or Resources
* Note: This must be used only if you don’t have backend that is compatible with SAML 2.0

**Web Identity Federation:**

* Not recommended way by AWS

**Cognito benefits:**

* Support for anonymous users
* Support for MFA
* Data synchronization

Note: In exam if any question related to web Identity Federation is asked solution will be with Cognito. Cognito replaces TVM which is an old way.

**3 types of AD Services**

* **AWS Managed Microsoft AD**
* **AD Connector –** Proxy to redirect to on prem AD, no caching capability, doesn’t work with SQL server, manages users solely on prem
* **Simple AD –** inexpensive**,** low scale**,** basic AD or LDAP compatible,doesn’t support **(MFA, RDS SQL Server, AWS SSO),** can’t be joined with on prem AD

**AWS Managed Microsoft AD DC (Direct Connect):**

On prem AD and AWS managed AD can be either connected using Direct Connect (DX)or VPN Connection

* One-way Trust – AWS to On prem
* One-way Trust – On prem to AWS
* Two-way forest trust – On prem to AWS and Vice versa
  + Forest trust is different than synchronization and replication is not supported.

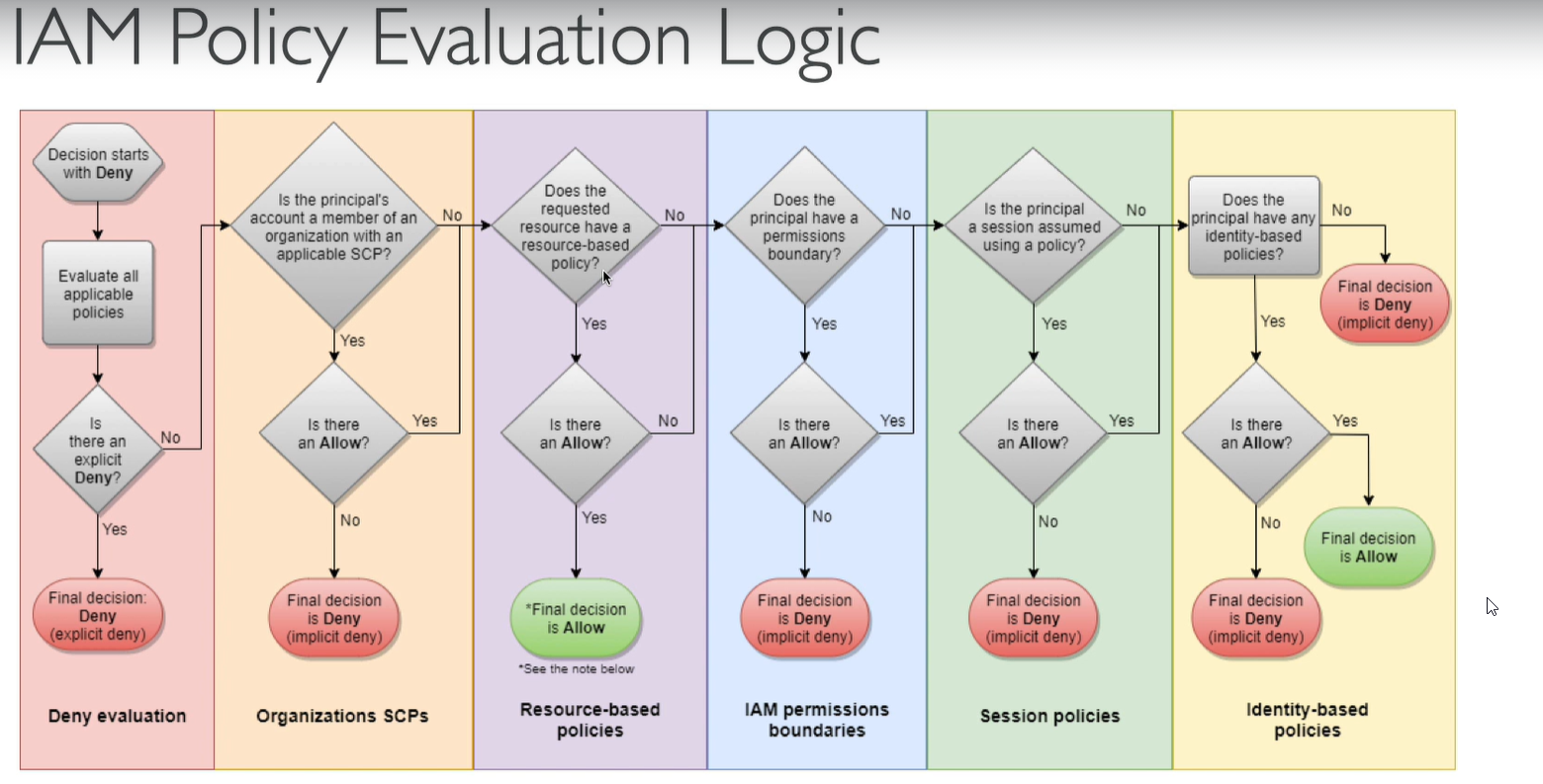
**AWS Organizations:**

2 types of features Consolidated Billing Feature, All Features (Default)

* SCP- Service Control Policy
* Can’t switch to Consolidated Billing Feature once you choose All Features.

Service Control Policies: (SCP)

* Whitelist or blacklist IAM actions
* SCP must have an explicit Allow (does not allow anything by default)
* Use cases:
  + Restrict access to certain service.
  + Enforce Payment card industry(PCI) compliance by explicitly disabling services.



Note: How do you share VPC’s across multiple accounts? – Using RAM (Resource Access Manage)

**AWS Single Sign-On (SSO):**

* Centrally manage single Sign-on to access multiple accounts and 3rd party business applications.
* Integrated with AWS organizations, On-prem AD
* Centralized Auditing with Cloud Trail.
* Centralized Permission Management.