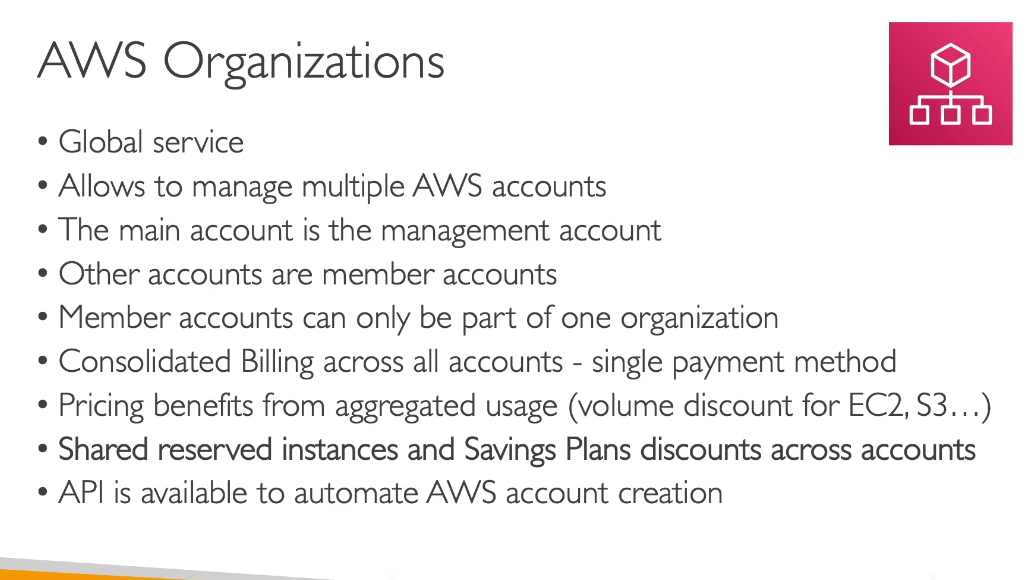
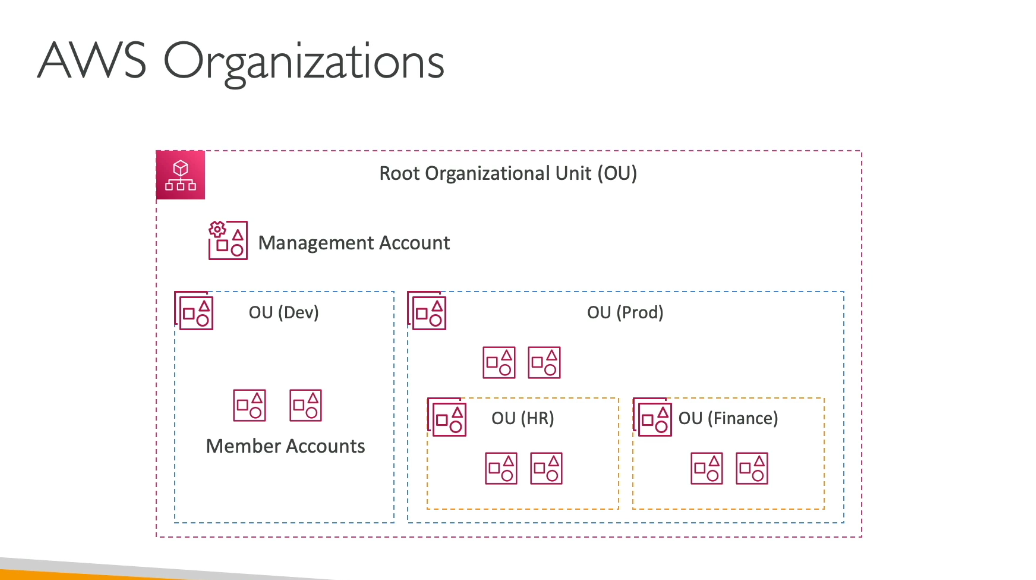
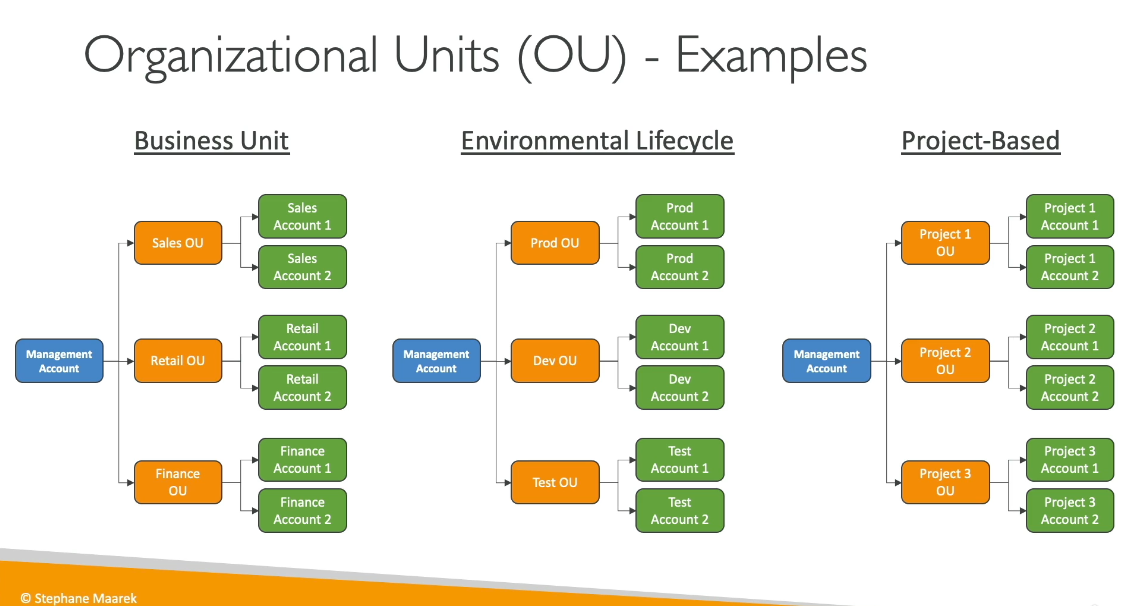
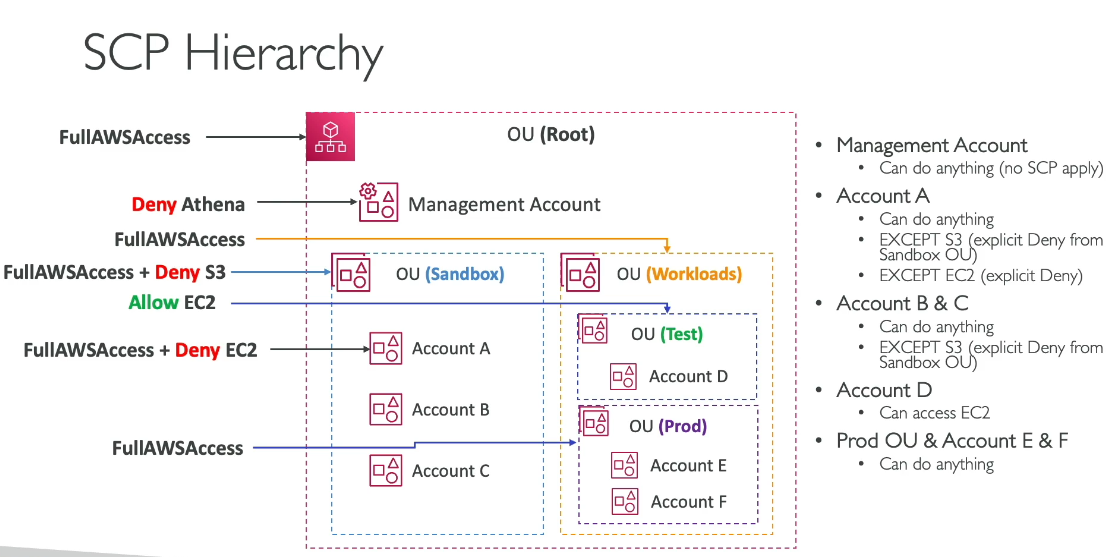
AWS Organizations:



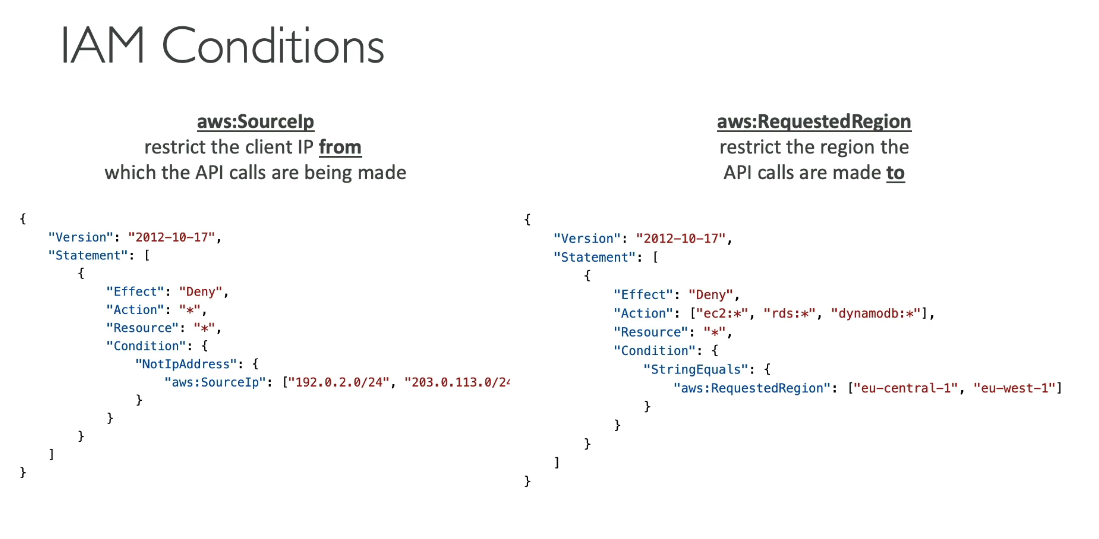






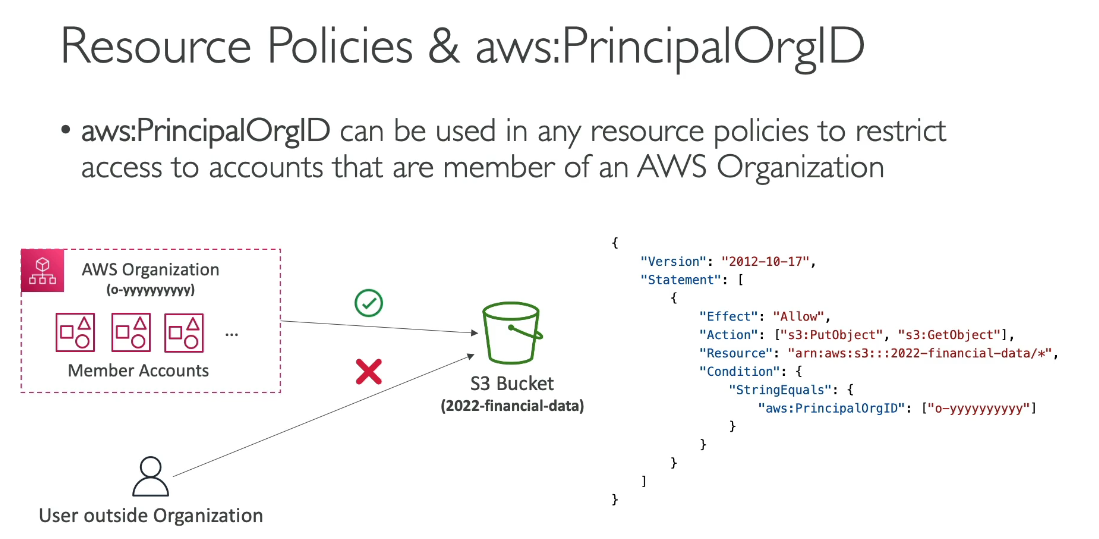


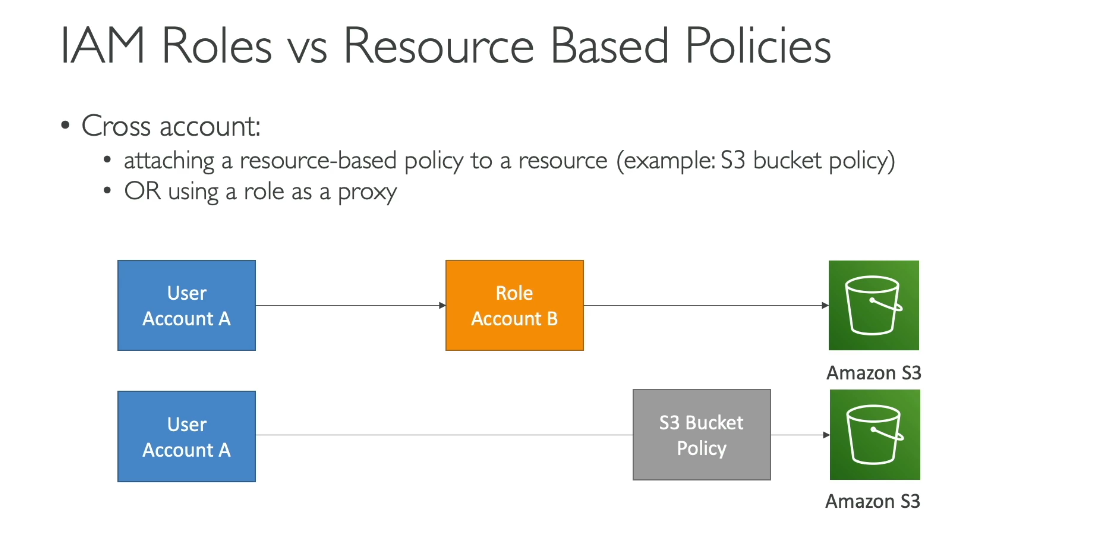


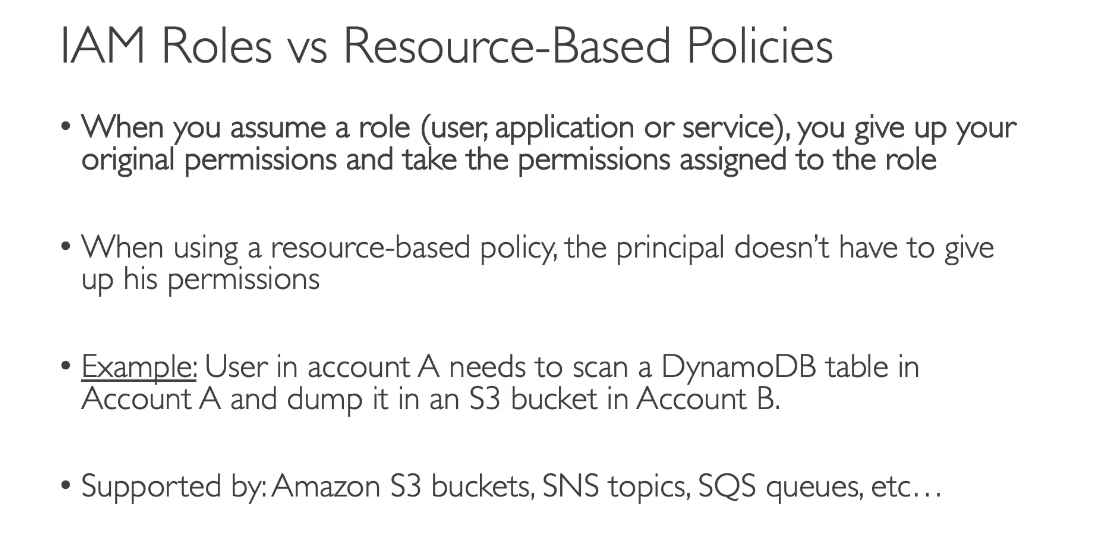


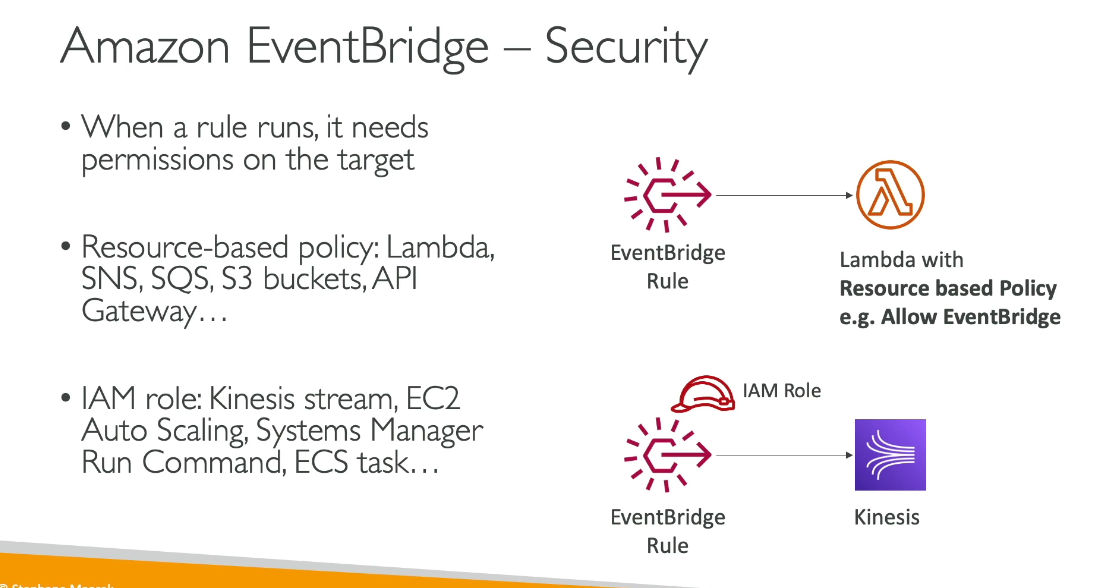












IAM roles and resource-based policies are two different approaches to granting access to AWS resources, each serving distinct purposes.

IAM Role:

* A principal (user, service, or application) assumes a role to temporarily obtain permissions
* The role's permissions apply to whoever assumes it
* Used when you need to delegate access across accounts or to AWS services
* The principal "becomes" the role and uses its permissions

Resource-Based Policy:

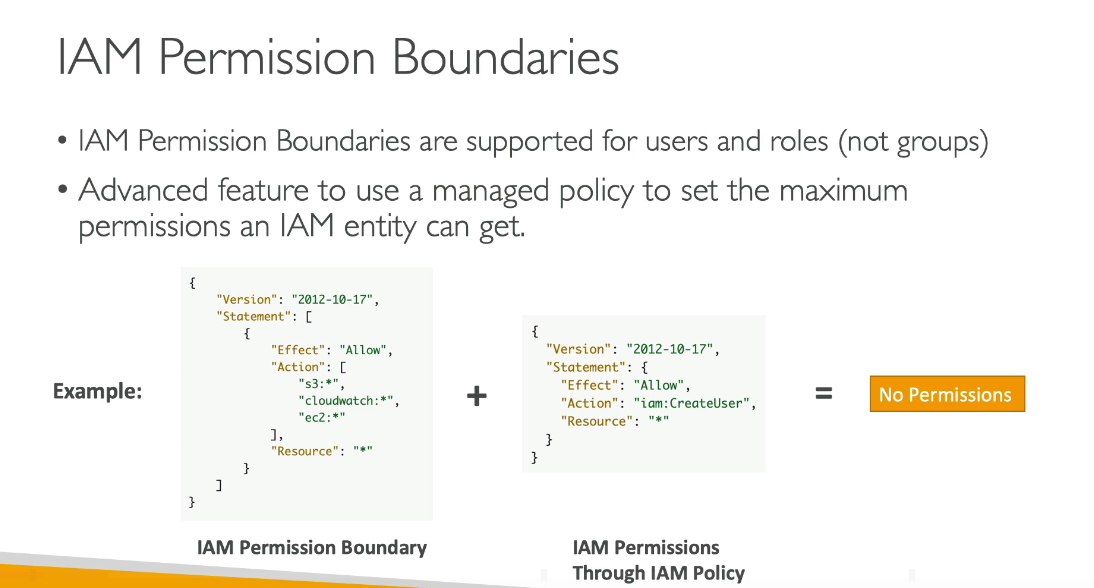
* Attached directly to a resource (like S3 buckets, SQS queues, or KMS keys)
* Specifies which principals can access the resource and what actions they can perform
* The principal retains their original permissions while accessing the resource
* Only supported by certain AWS services

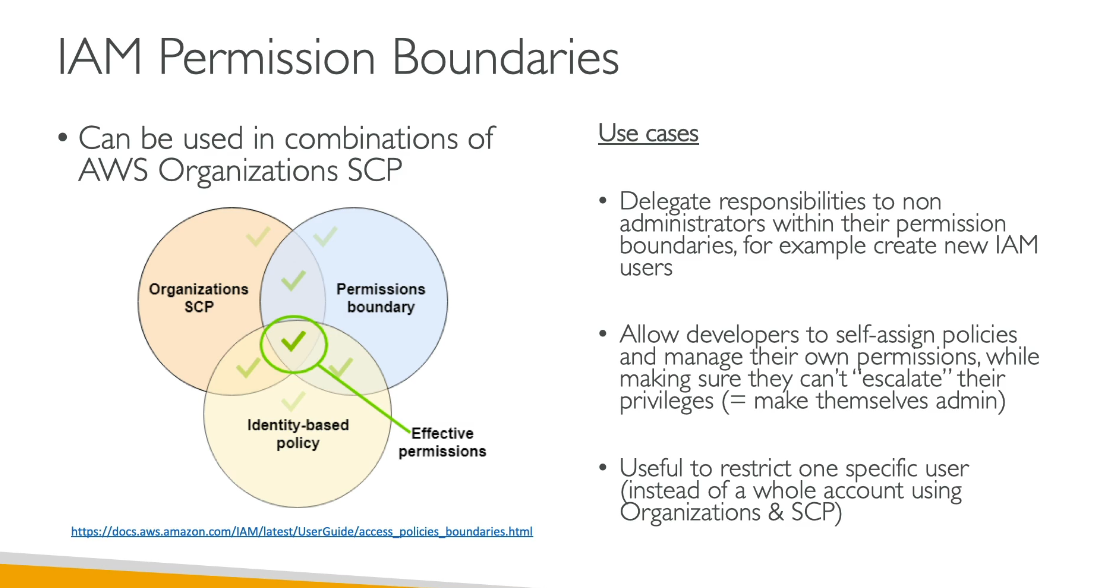
Key Difference: With IAM roles, you don't specify the principal in the policy (it's implicit). With resource-based policies, you explicitly specify which principals can access the resource.

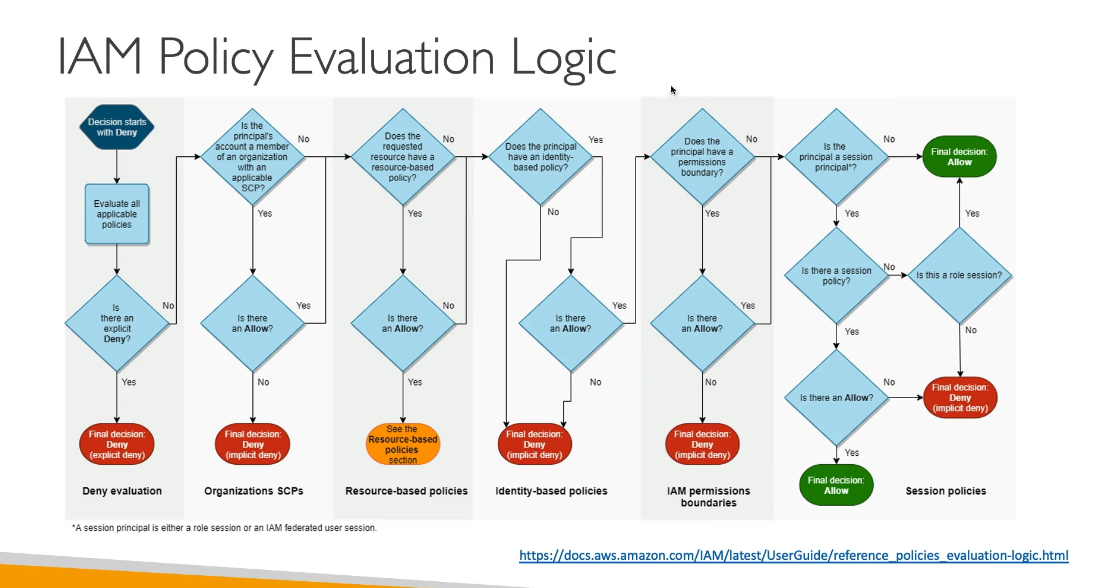
Common Use Cases:

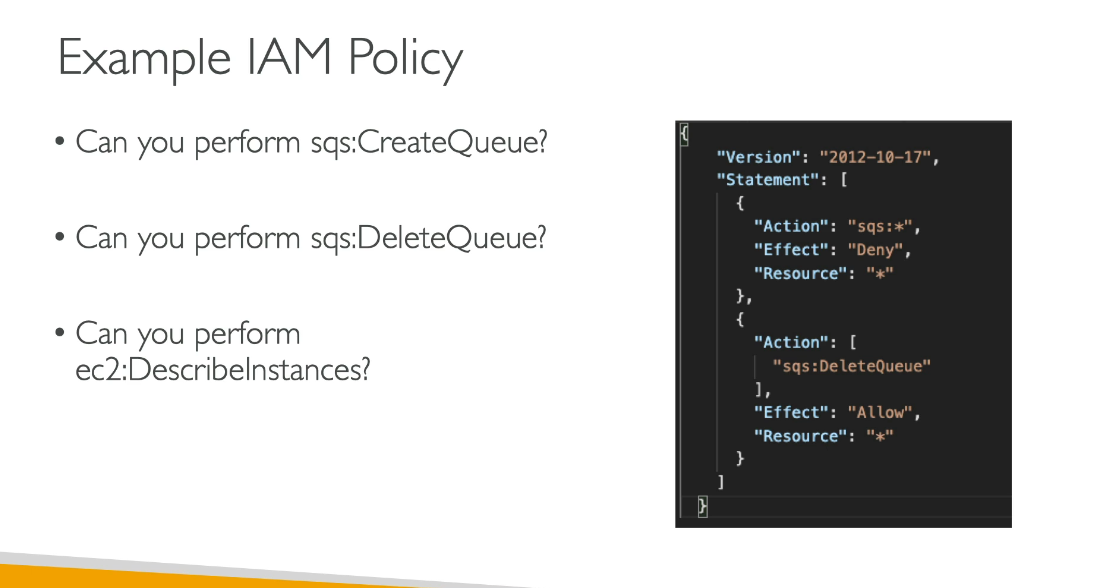
* IAM Roles - Cross-account access, granting EC2 instances permissions to access AWS services, temporary credentials for applications
* Resource-Based Policies - Granting cross-account access to S3 buckets, allowing Lambda functions to be invoked by other accounts, sharing KMS keys across accounts

Note: IAM roles are unique as they function as both a principal and a resource, requiring trust policies (a type of resource-based policy) even within the same account.





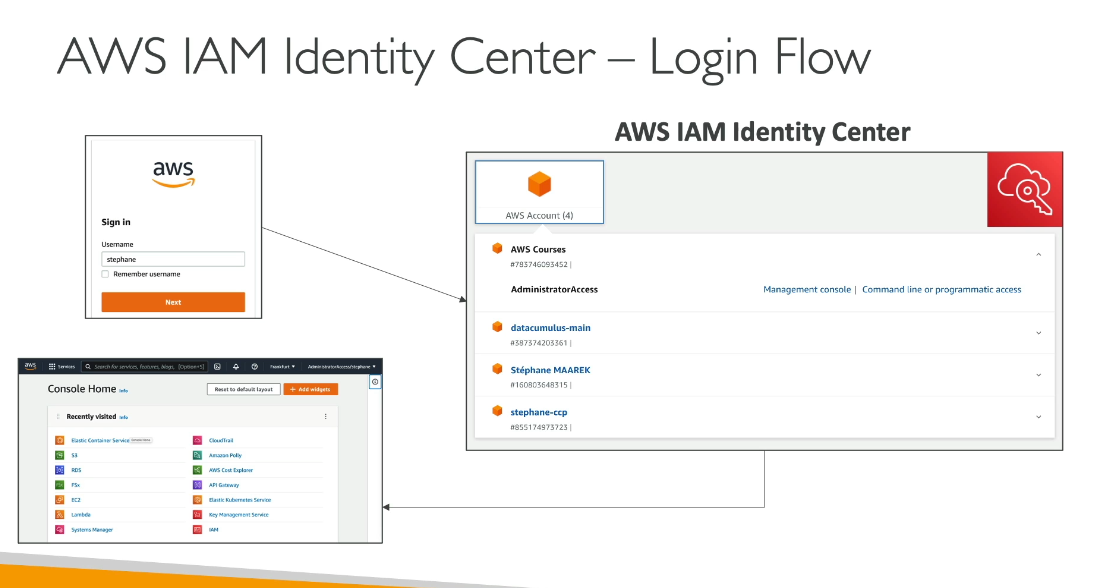


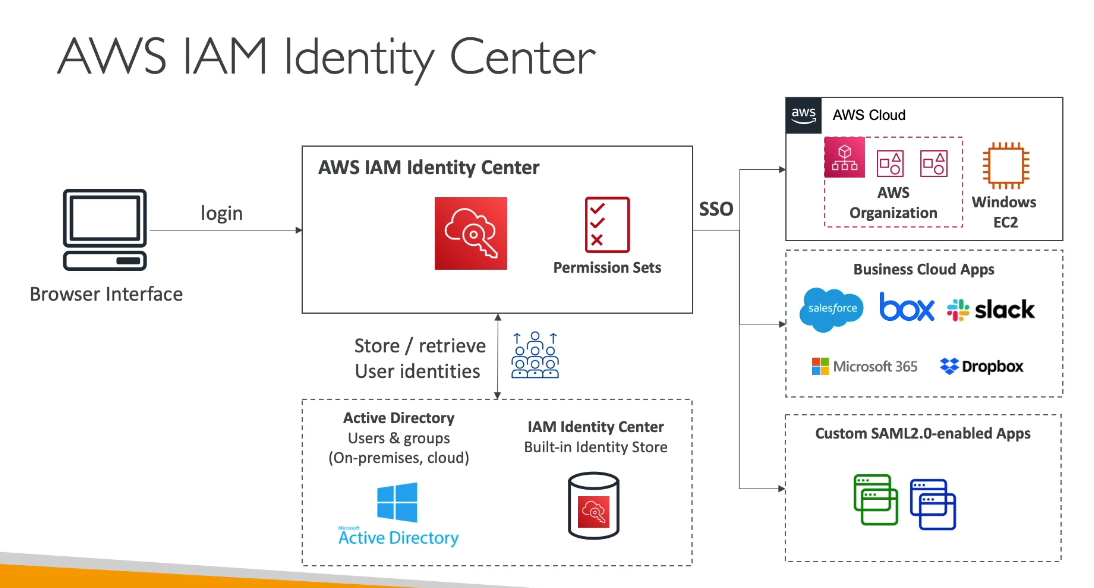


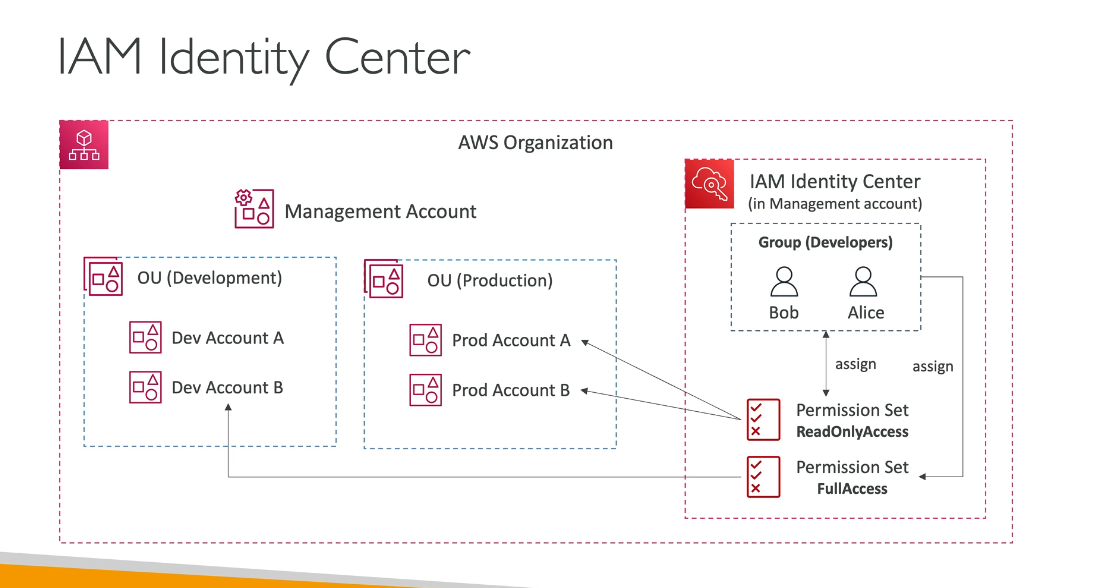
For all questions the answer is False

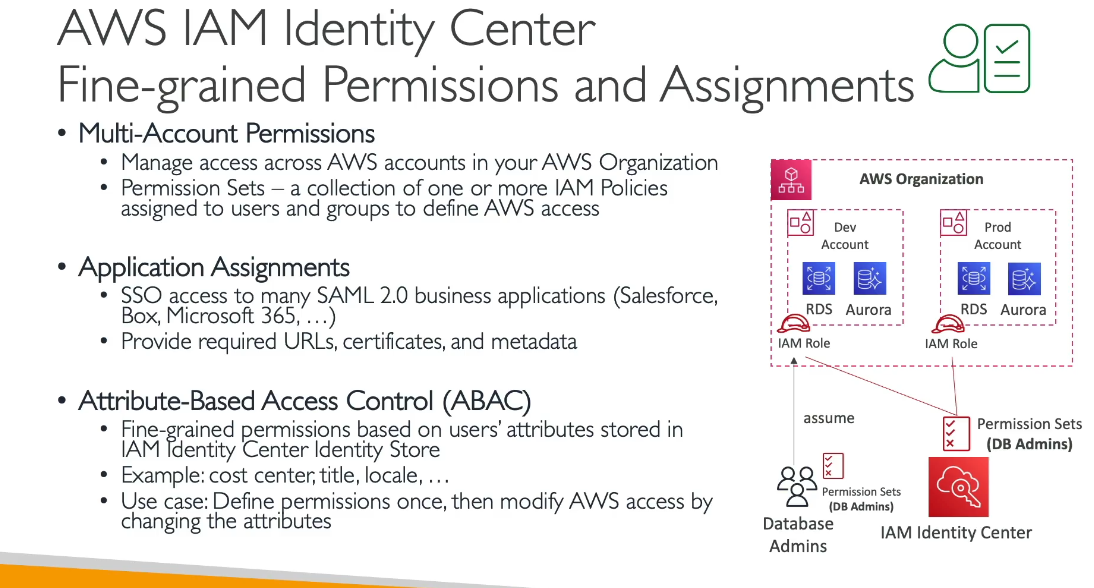
Identity Center











Active Directory:

