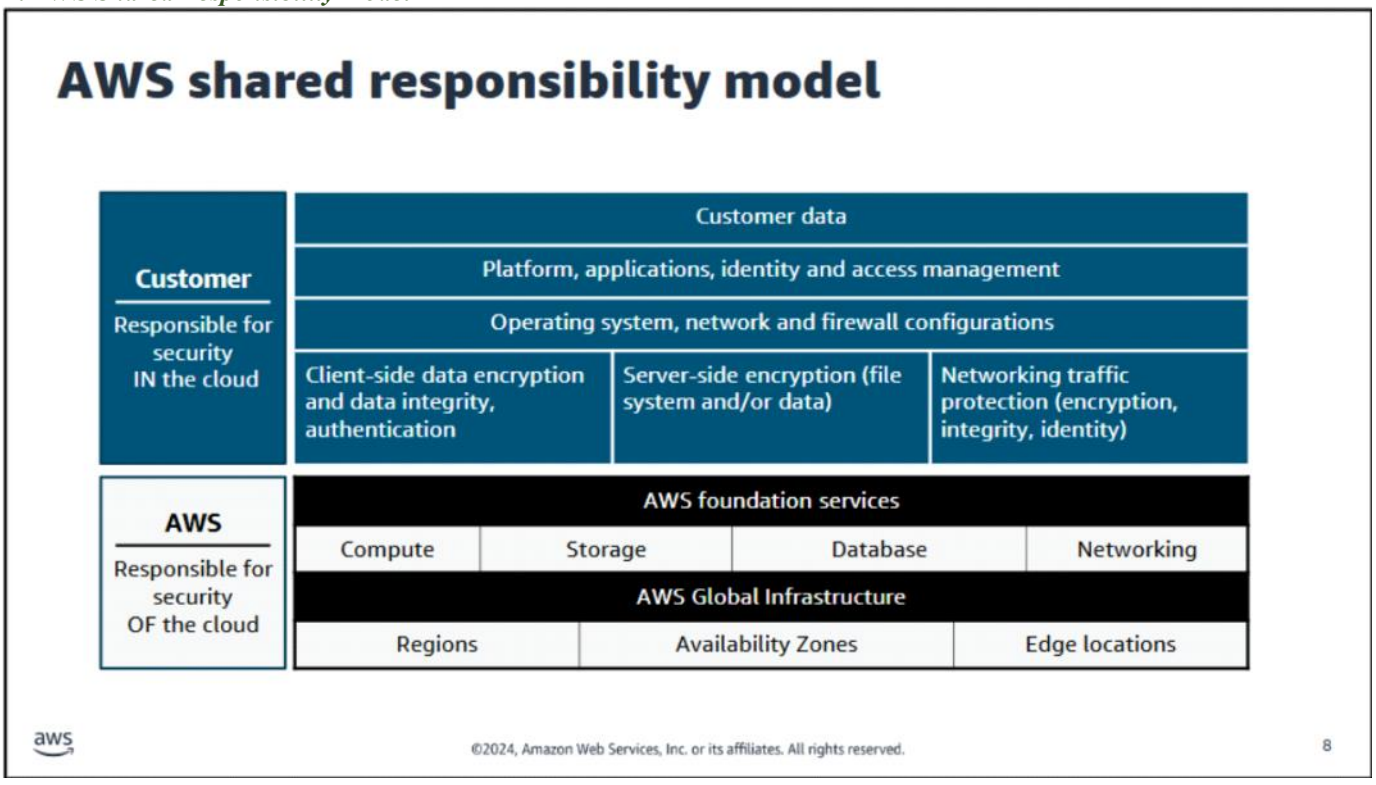
Module 3: Security Access

Monday, September 29, 2025 8:12 PM

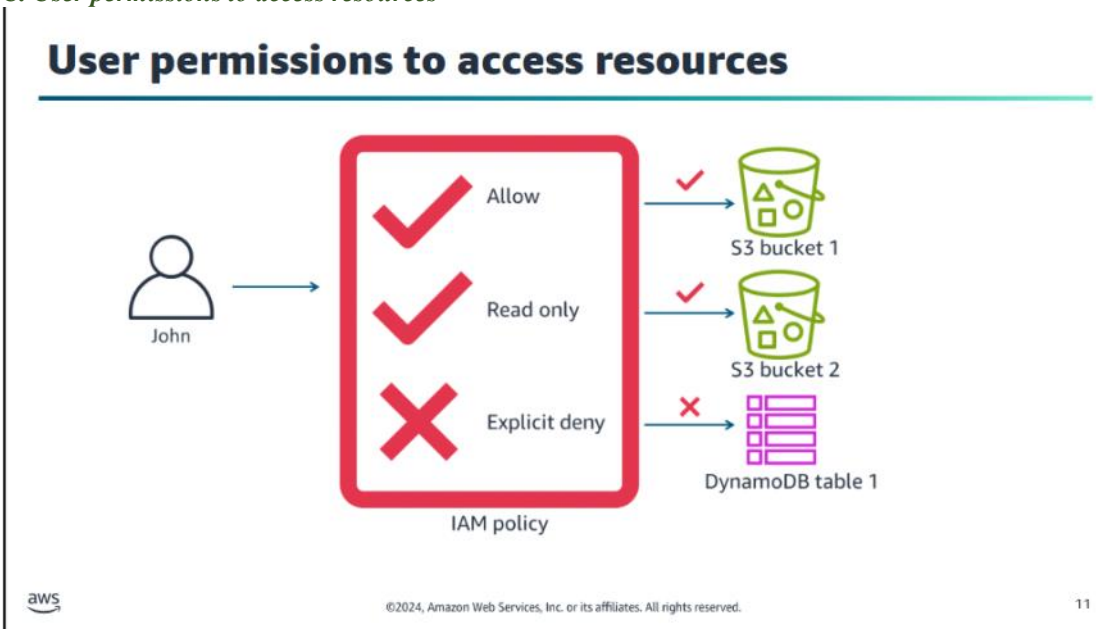
A. AWS Shared Responsibility Model



B. Design principles for the Security Pillar

- Implement a strong identity foundation
- Protect data in transit and at rest
- Apply security at all layers
- Keep people away from data
- Maintain traceability
- Prepare for security events
- Auomate security best practces

C. User permissions to access resources



The scenario demonstrates a **strong identity foundation** by applying the **principle of least privilege** to user John. This means:

1. **Granting only necessary permissions:** John is given full control (read, write, delete) only for the specific resource where he needs it (**S3 bucket 1**).
2. **Restricting permissions:** His access is intentionally limited to read-only for another resource (**S3 bucket 2**).
3. **Explicitly denying access:** He is completely blocked from a resource he should not touch (**DynamoDB table**).

In essence, John's access is tailored and compartmentalized based strictly on the tasks he needs to perform, thereby minimizing the potential blast radius of any error or malicious action.

D. AWS Identiy and Access Management (IAM)

- Controls individual and group access to user AWS resources.
- Integretes with other AWS services
- Provides federated indentiy management
- Supports multi-factor authentication (MFA)
- Allows granular permissions

Term	Definition
IAM resource	User, group, role, policy, and identity-provider objects stored in IAM
IAM entity	IAM resources objects that are used by AWS for authentication (users and roles)
IAM identity	IAM reosurce objects that can be authorized in policies to perform actions and acess resources (user, group, or role
Principal	Person or application that can sign in and make requests to AWS

E. Using IAM to control access to AWS resource

- IAM User: A person or applcation that can authenticate with an AWS account.
- IAM group: A collection of IAM users who are granted identical authorization
- IAM role: An identify that is used to grant a temporary set of permissions to make AWS service requests
- IAM policy: The document that defines which resources can be accessed and the level of access to each resource

F. IAM credentials for authentication

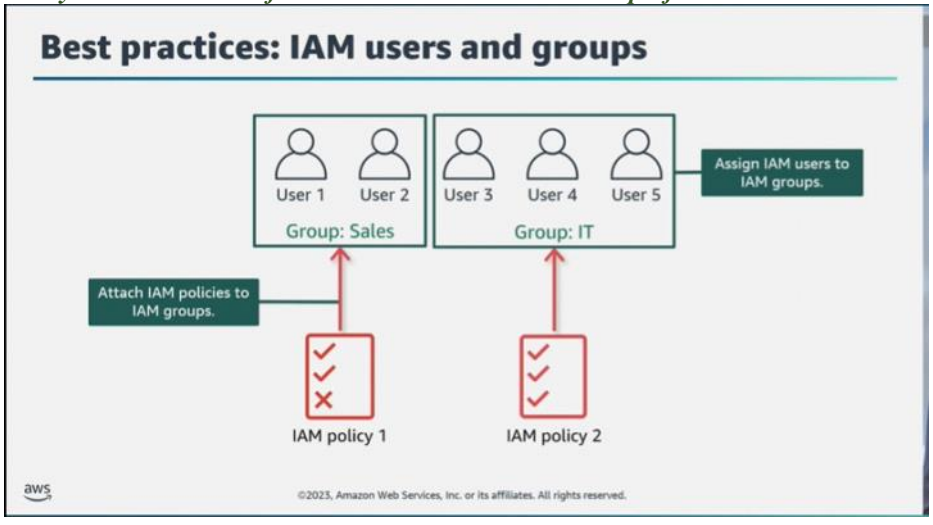
Action	*Credentials needed*
Sign in to AWS Management Console	Username and Password
Run commands from the AWS Command Line Interface (AWS CLI)	AWS access key
Make programmic calls to AWS	AWS access key

G. Best practices to secure access

- Follow the principle of least privilege
- Enable Multifactor authentication (MFA)
- Require human users to access AWS by using temporary credentials
- Rotate access keys for use cases that require long-term credentials
- Use strong, complex passwords
- Secure local credentials
- Use AWS Organization
- Enable AWS CloudTrail
- Protect the root user

H. Protecting the root user

- For daily tasks, create an administrative user in AWS IAM Identity Center (successor to AWS Single Sign-On)
- Only use the root user for tasks that other users cannot perform



I. IAM roles

- Characteristics:

+ Provides temporary security credentials

+ Isn't uniquely associated with one person
+ Can be assumed by a person, application, or service
+ Is often used to delegate access

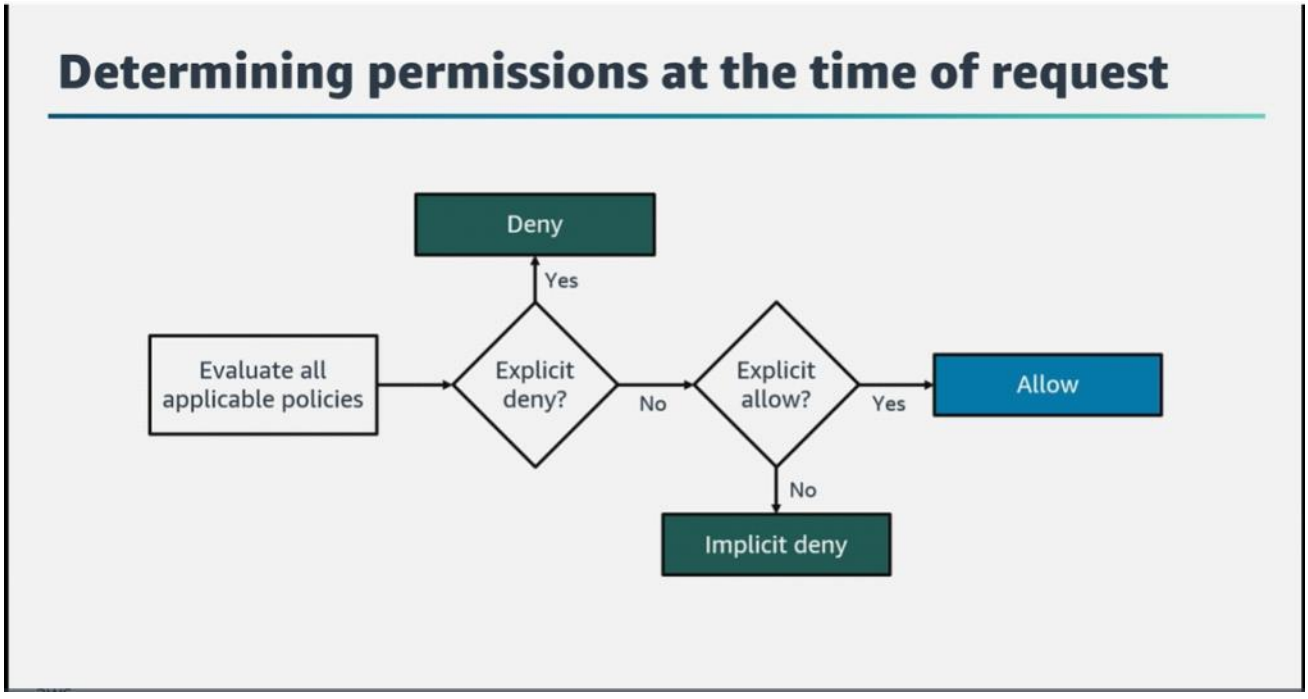
- Common use cases:

+ Application that runs on Amazon Elastic Compute Clous (Amazon EC2)
+ Cross-account access for an IAM user
+ Mobile applications

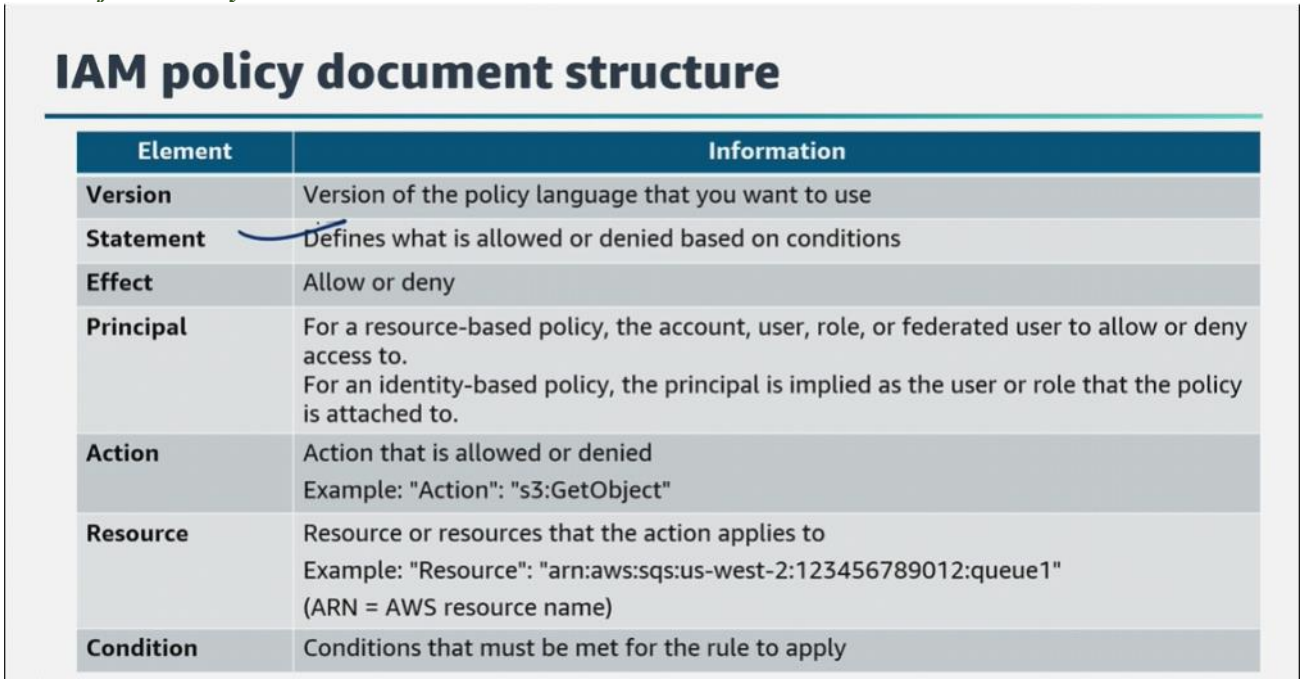
I. Autjprizing Users

- IAM policies and permissions

Use policies to fine-tune the permissions that are granted to principals	**Define permissions in IAM policy documents**
Identity-based: Attach to an IAM user, group, or role Resource-based: Attach to an AWS resource	The document is formatted in JSON The policy defines which resources and operation are allowed or denied Folloe the principle of leasr privilege



J Parts of IAM Policy



IAM policy document structure

Element	Information
Version	Version of the policy language that you want to use
Statement	Defines what is allowed or denied based on conditions
Effect	Allow or deny
Principal	For a resource-based policy, the account, user, role, or federated user to allow or deny access to. For an identity-based policy, the principal is implied as the user or role that the policy is attached to.
Action	Action that is allowed or denied Example: "Action": "s3:GetObject"
Resource	Resource or resources that the action applies to Example: "Resource": "arn:aws:sqs:us-west-2:123456789012:queue1" (ARN = AWS resource name)
Condition	Conditions that must be met for the rule to apply

- IAM policies are stored as JSON documents. Each statement includes information about a single permission

- Key elements of an IAM policy statement include the effect, action, and resources. Toghether, these elements determine policy permissions.