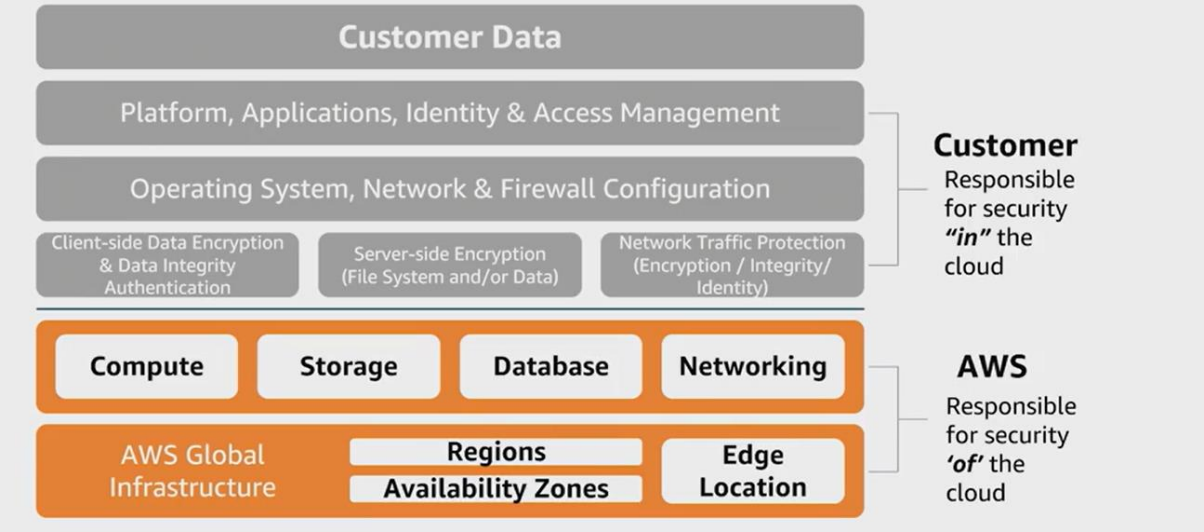
Domain 2:

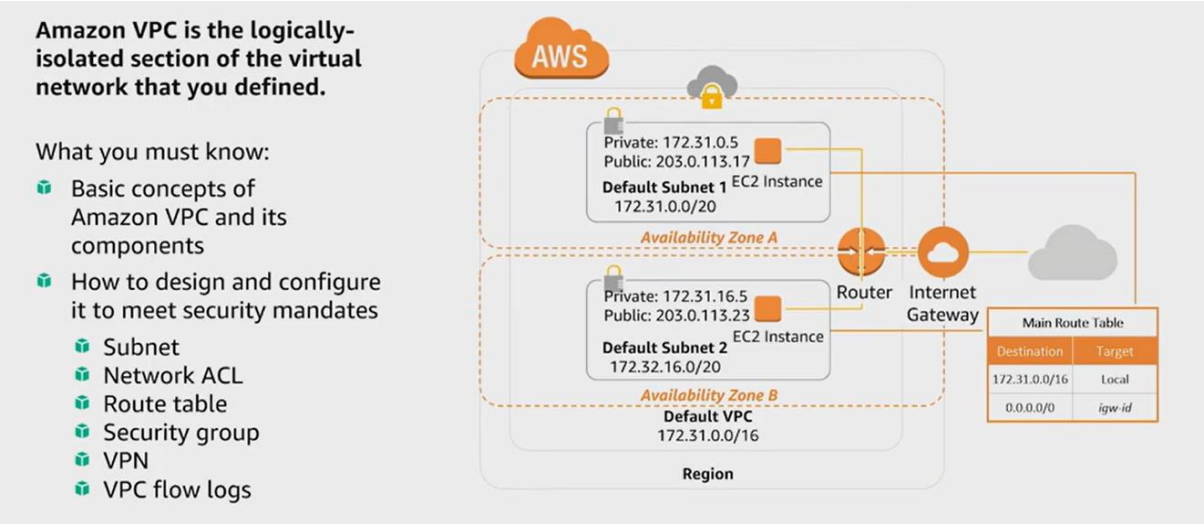
Security:

Shared Responsibility Model:



Data and Application Security:

Amazon Virtual Private Cloud:



Security – data and application:

1. AWS key management service
2. AWS certificate manager

Know how to protect data in transit and at rest.

- SSL/TLS endpoint, data encryption
- AWS Certificate Manager (ACM), in Transit Provision trusted SSL/TLS certificates provided by AWS for use with AWS resources:
  - Load Balancing
  - Amazon CloudFront distributions

Understand data encryption. Know available encryption options.

- Client-side encryption
  - You encrypt your data ***before*** data submitted to service.
  - You supply encryption keys **or** use keys in your AWS account.
- Server-side encryption
  AWS encrypts data on your behalf ***after*** data is received by service.
- Key Management Service
- CloudHSM

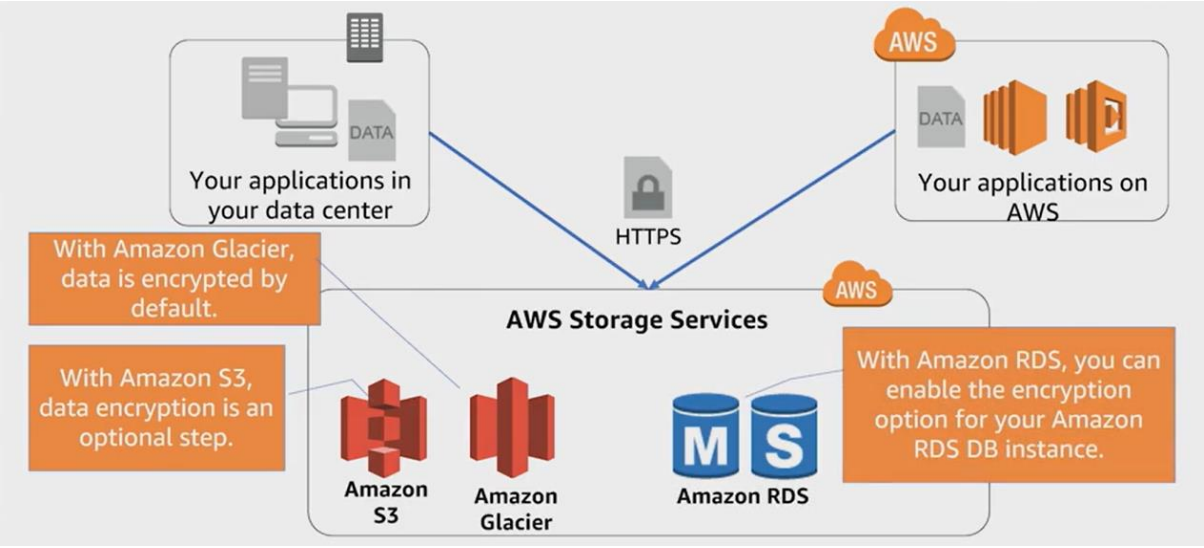
Security – Protecting data at rest on Amazon S3:

Amazon S3 provides server-side encryption (AES-256) using AWS-maintained keys or customer-provided keys.

Customers may also encrypt data before storage in Amazon S3 (client-side encryption).

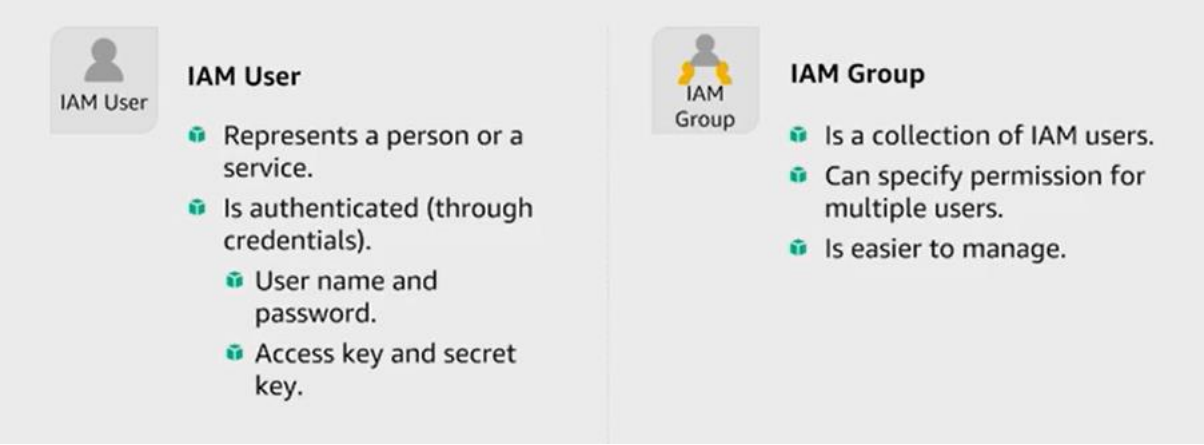
- Amazon S3-Managed Keys (SSE-S3)
- KMS-Managed Keys (SSE-KMS)
- Customer-Provided Keys (SSE-C)

AWS server-side encryption:

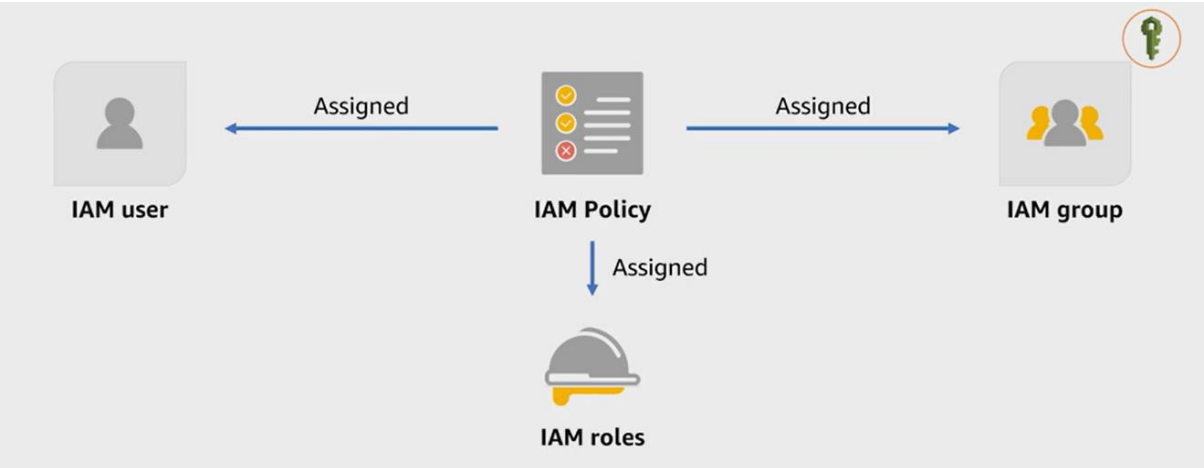


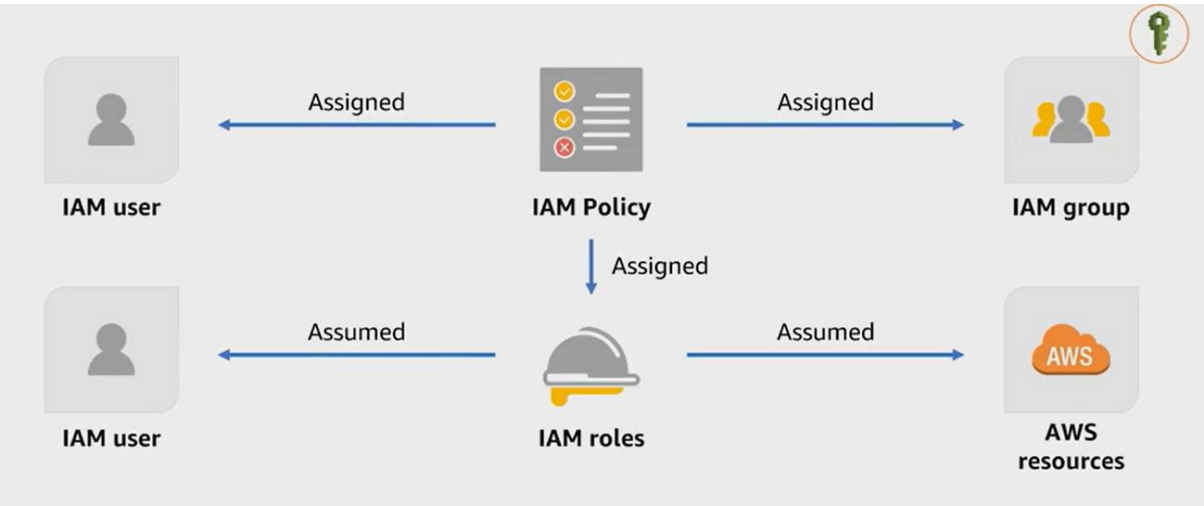
IAM, STS and identity federation:

AWS identity and access management (IAM):



IAM Policy management:





Identity Federation:

Authenticate using **external identities** (federated users)

- Grant access to AWS resources without having to create IAM users.

May include:

- Web identity federation
  - Amazon Cognito, Log in with Amazon, Facebook, Google, OpenID Connect (OIDC)
- SAML 2.0 (Security Assertion Markup Language 2.0)-based federation
  - Microsoft Active Directory, LDAPS, Open LDAP