AWS Solution Architect Associate

Version : C03

Domain 1

Task 3

Determine appropriate data security controls

AWS - Data access and governance

- Data access in AWS involves the mechanisms for retrieving, viewing and interacting with data across its different services
- It is about securely managing and controlling how data is accessed and used across
- Key features/services
  - Identity and Access Management
  - S3 Access Controls
  - Security Measures
  - Organizational Controls
  - Programmatic & Temporary Access
  - Monitoring and Compliance
- Data governance is the process of defining and implementing policies, standards, and procedures for managing data throughout its lifecycle.
- It aims to ensure that data is accurate, consistent, secure and compliant with regulations and business requirements.
- Types of data governance
  - Centralized data governance
  - Federated data governance
  - Self-serve or decentralized data governance

AWS Tech - Compliance Requirements

- Security and Compliance is a shared responsibility between AWS and the customer.
- The IT infrastructure that AWS provides to its customers is designed and managed in alignment with best security practices and a variety of IT security standards.
- AWS services related to compliance are
  - AWS IAM
  - Amazon GuardDuty
  - AWS Config
  - Amazon CloudTrail
  - Amazon Macie
  - Amazon Inspector
  - Amazon KMS
  - AWS Security Hub
  - AWS Firewall Manager

AWS - Encryption

- Encryption works by using an algorithm with a key to convert data into an unreadable data (ciphertext) that can only become readable again with the right key.
- AWS offers several encryption options
  - SSL/TLS
  - IPSec
  - S3 Encryption
  - KMS Encryption
- Data can be encrypted at 2 stages
  - Data Encryption at rest
  - Data Encryption in transit
- There are 2 levels of encryption
  - Server Side Encryption
  - Client Side Encryption

Data Encryption at Rest

- Data at rest represents any data that persists in non-volatile storage for any duration
- Protecting data at rest have different options
  - **Server Side Encryption** - S3 managed keys(SSE-S3) is the default encryption. Different encryption can be specified explicitly. AWS services -
    - **AWS KMS** : Key Management Service
    - **AWS SSE-KMS** : Server Side Encryption with KMS
    - **AWS SSE-S3** : Server Side Encryption with S3 managed keys
    - **AWS DSSE-KMS** : Dual layer server side encryption with KMS
    - **SSE-C** : Server Side Encryption with customer provided keys
  - **Client Side Encryption** - Data is encrypted at the client side and uploaded. Encryption process, keys and related tools are managed by client/user.

Data Encryption in Transit

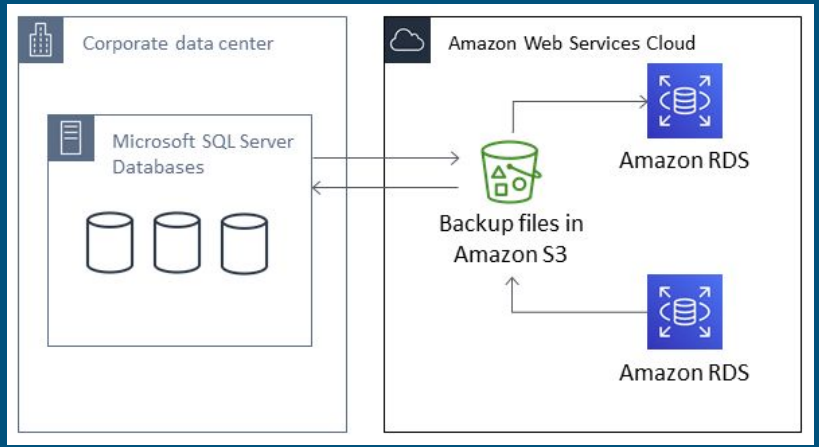
- Data in transit can be protected by using Secure Socket Layer / Transport Layer Security (SSL/TLS) or client side encryption
- TLS is a set of industry-standard cryptographic protocols used for encrypting information that is exchanged over the network.
- AES-256 is a 256-bit encryption cipher used for data transmission in TLS. AWS Services -
  - **AWS Certificate Manager** - It allows to provision, manage and deploy SSL/TLS certificates for use with AWS services and internal resources. It also ensures that data transmitted between the resources and external clients is encrypted using industry-standard encryption protocols, such as SSL/TLS.

Data Backups and Replications

- Fully managed backup service that makes it easy to centralize and automate the backup of data across AWS on premises using the AWS Storage Gateway.
- Backup policies can be centrally configured and monitored for AWS resources
- It automates and consolidates backup tasks previously performed service-by-service, removing the need to create custom scripts and manual processes.
- It provides a fully managed, policy-based backup solution, simplifying the backup management, which enables to meet the business and regulatory backup compliance requirements

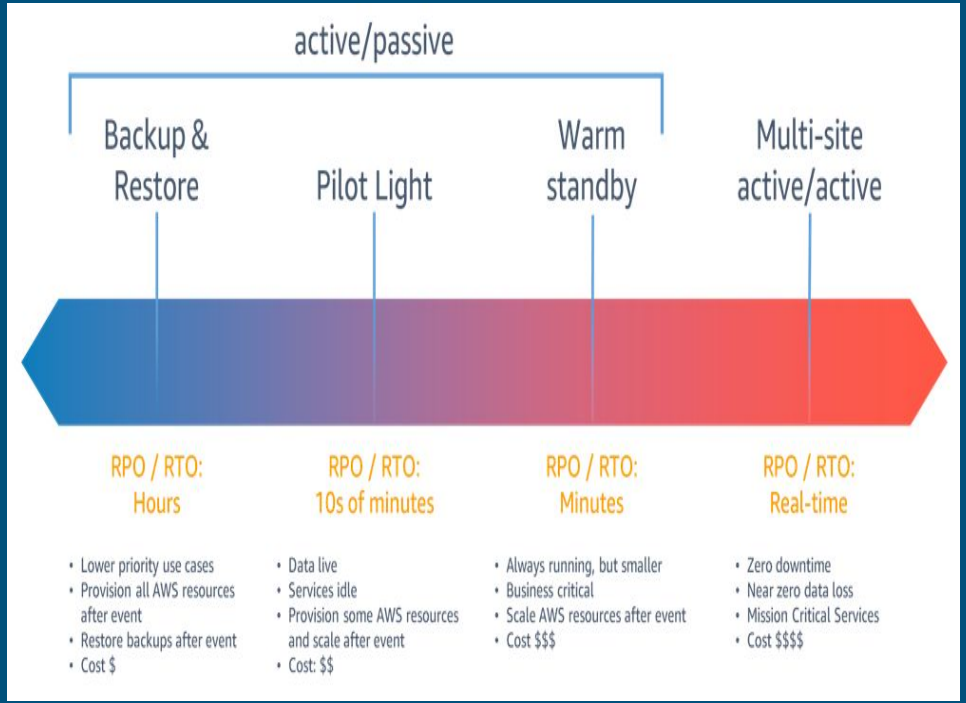
How does data backup work ?

- Data backup process starts with identifying and prioritizing the criticality of an organization's data and systems
- Regular backup with backup software can be scheduled to ensure critical data copies are up to date
- Data backup methods
  - **Full backup**
  - **Incremental backup**
  - **Differential backup**
  - **Mirror backup**
- Considerations in selecting data backup solution
  - Cost
  - Time to copy and recover
  - Storage persistence and scalability
  - Location and energy efficiency
  - Data security and compliance



AWS - Data recovery / Failover

- Different data recovery strategies
  - Backup and Restore
  - Pilot Light
  - Warm Standby
  - Multi site active\active
- Amazon S3 is an ideal destination for quick access to the backup
- A lifecycle policy can be used to move old backups to progressively more cost efficient storage classes over time



AWS - Data recovery

- **Backup and Restore**
  - RPO/RTO : Hours
  - Lower priority use cases
  - Provision all AWS resources after event
  - Restore backups after event
  - Cost ($)
- **Pilot Light**
  - RPO/RTO : 10s of minutes
  - Data Live
  - Services Idle
  - Provision some AWS resources and scale after event
  - Cost($$)
- **Warm Standby**
  - RPO/RTO : Minutes
  - Always running but smaller
  - Business Critical
  - Scale AWS resources after event
  - Cost($$$)
- **Multi site active\active**
  - RPO/RTO : Real-time
  - Zero Downtime
  - Near zero data loss
  - Mission Critical Services
  - Cost($$$$)

AWS - Data retention and classification

- **Data retention** is the storage of data in an organisation , guided by a clear policy
- AWS services for data retention management
  - Amazon S3 Lifecycle Policies
  - Amazon S3 Intelligent-Tiering
  - Amazon EBS Snapshots
  - Amazon Data Lifecycle Manager
  - AWS Glue Crawlers
- **Data classification** involves categorizing data stored within its services by sensitivity, importance and usage
- AWS offers tools for classification
  - S3
  - Glacier
  - Macie
  - Resource Tagging
  - IAM
  - AWS Organizations
  - Amazon SageMaker
  - AWS Glue DataBrew

Data Access , Life Cycle and protection policies

- Refers to the stages that data goes through when it is stored in AWS.
- These stages include creation, storage, retrieval and deletion.
- AWS provides various protection policies like encryption, access control and audit trails to ensure that data is secure during these stages
- Lifecycle configuration is a set of rules that define actions that applies to a group of objects.
- There are two types of actions -
  - Transition actions - Defines when objects transition to another storage class
  - Expiration actions - Defines when object expires
- Data protection policies offered by AWS
  - SLA's
  - Security Services
  - Compliance Certifications

Rotating Encryption Keys and Renewing Certificates

- ➔ Rotating encryption keys and renewing certificates regularly helps in mitigating the risks associated with compromised keys or certificates.
- ➔ It also helps in preventing unauthorized access to encrypted data by invalidating previous keys and generating new ones.
- ➔ Renewing certificates ensures continued trust and authentication in SSL/TLS communications by updating expired certificates with fresh ones.
- ➔ Implementing automated key rotation and certificate renewal processes reduces manual overhead and ensures timely updates without service disruptions.
- ➔ Regularly monitoring key rotation and certificate renewal activities helps detect anomalies or issues and ensures adherence to security policies.
- ➔ **AWS Key Management Service (KMS)** can be used to streamline key rotation processes and provides centralized control over key lifecycles.
- ➔ **AWS Certificate Manager (ACM)** can be used to simplify the certificate renewal tasks

AWS Solution Architect Associate

Version : C03

Domain 1

Task 3

The END