AWS Cloud Practitioner Exam (2/4)

Domain 2: Security and Compliance

Topics

2.1 Define the AWS shared responsibility

- Recognize the elements of the Shared Responsibility Model
- Describe the customer's responsibly on AWS
    - Describe how the customer's responsibilities may shift depending on the service used (e.g. with RDS, Lambda, or EC2

2.2 Define AWS Cloud security and compliance concepts

- Identify where to find AWS compliance concepts
    - Locations of lists of recognized available compliance controls (e.g. HIPAA, SOCs)
    - Recognize that compliance requirements vary among AWS services
- At a high level, describe how customers achieve compliance on AWS
    - Identify different encryption options on AWS (e.g. In transit, At rest)
- Describe who enables encryption on AWS for a given service
- Recognize there are services that will aid in auditing and reporting
    - Recognize that logs exist for auditing and monitoring
    - Define Amazon CloudWatch, AWS Config and AWS CloudTrail
- Explain the concept of least privileged access

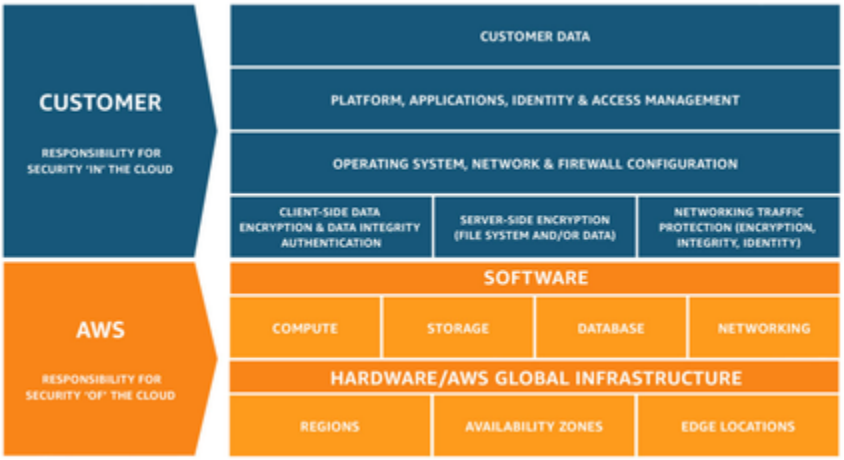
2.3 Identify AWS access management capabilities

- Understand the purpose of User and Identity Management
    - Access keys and password policies (rotation, complexity)
    - Multi-Factor Authentication (MFA)
    - AWS Identity and Access Management (IAM)
        - Groups/users
        - Roles
        - Policies, managed policies compared to custom policies
    - Tasks that require use of root accounts | Protection of root accounts

2.4 Identify resources for security support

- Recognize that there are different network security capabilities
    - Native AWS Services (e.g. security groups, Network ACLs, AWS WAF)
    - 3rd party security products from the AWS Marketplace
- Recognize there is documentation and where to find it (e.g. best practices, white papers, official documents)
    - AWS Knowledge Center, Security Center, security forum, and security blogs
    - Partner Systems Integrators
- Know that security checks are a component of AWS Trusted Advisor

READ: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html



AWS Shared Responsibility Model

- Security and compliance is a shared responsibility between AWS and user
    - AWS: "Security of the cloud"
        - protection of infrastructure (hardware, software, networking and facilities)
    - User: "Security in the cloud"

- user can determine the amount of configuration work that must be performed as part of their security responsibilities
- e.g. EC2 (which is a IaaS), requires the customer to perform all of the necessary security configuration and management tasks
- e.g. S3 or DynamoDB, AWS manages the operating system, platform & customers access the endpoints to store and retrieve data; customers are responsible for managing their data, classifying their assets and using IAM tools to apply the appropriate permissions

AWS Cloud and Security Concepts

Link to find AWS compliance concepts: https://aws.amazon.com/compliance/programs/

- AWS helps users and businesses improve their ability to meet core security and compliance requirements (e.g. data locality, protection and confidentiality) with AWS' comprehensive services and features by automating manual security tasks.
- AWS offers the ability to encrypt data at rest and in transit
  - Key Management System - centralised control over cryptographic keys used to protect data
  - CloudHSM (hardware security module) - generate own encryption keys
  - ACM - service that allows easy provision, management and deployment of public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates
- AWS Key Management System (KMS) integrates with the majority of services to let customers control the lifecycle of permissions and keys used to encrypt data on the customer's behalf
  - server-side encryption - control when data is decrypted, by whom and under which conditions; customers can isolate control over access to the data, from access to hte keys
  - client-side encryption - users can encrypt data within their own application environment using AWS KMS, taking AWS services out of their trust boundary
- To protect data in transit, AWS encourages customers to leverage a multi-level approach
  - Network traffic between AWS centers, within a CPV and between peered VPCs across regions are transparently encrypted at the network later when using supported EC2 instance types
  - At the application layer, customers can customise the use of encryption using a protocol like Transport Layer Security (TLS) that is supported by all AWS service endpoints

Logs

Logs exist in AWS to allow for auditing and monitoring, provided through these services:

AWS CloudWatch	• Monitoring service for AWS services (EC2 instances, Dynamo, etc.) • collect and track metrics, log files and set alarms • Provides stream events to provide visibility of application performance
AWS Config	• Provides AWS resource inventory, configuration history and config change notifications to enable security and governance
AWS CloudTrail	• log continuously and monitor AWS account activity (management console, people/applications resource access) • Simplifies security management

Least Privilege Access - Standard security practice of granting only the permissions required to perform a task. This is done by determining what users (and roles) need to do and then craft policies that allow them to perform *only* those tasks

AWS Access Management Capabilities

Access Keys and Password Policies

- Access keys are long-term credentials for an IAM user used to sign programmatic requests to the AWS CLI or AWS API
- consists of an access key ID and a secret access key
- Ability to create, modify, view or rotate access keys (max of 2 access keys)
- Secret access key is available only at the time of creation; losing the secret access key requires one to delete the access key and create a new one
- IAM password policy does not apply to the AWS account root user password or IAM user access keys. If a password expires, the IAM user can't sign in to the AWS Management Console but can continue to use their access keys
- Setting customised password policies by
  - defining minimum length and character type
  - set password expiration period
  - CANNOT set a "lockout policy"

Multi-Factor Authentication

- extra security measure that requires users to provide a unique authentication from AWS supported mechanism in addition to their regular sign-in credentials
  - Virtual MFA devices - software app emulating physical device; six-digit numeric code
  - U2F security key - device that plugs into computer
  - Hardware MFA device - hardware device; similar six-digit numeric code
  - SMS text-message based - SMS through phone number; six-digit numeric code

IAM

- AWS IAM enables management of access to AWS services and resources securely by creating AWS users and groups, and using permissions to allow and deny their access to AWS resources
- Best common practices
    - Using root user only to create first IAM user account and lock away root user credentials only to be used for account and service management tasks
- Users and Roles can be defined to manage access to AWS services and resources
- Possible to organize IAM users into IAM groups and attach a policy into a group
    - Multiple policies can be attached to users or groups to grant different permissions
    - AWS managed policies - created and managed by AWS
    - Customer managed policies - created and managed by users in their AWS account

Root Users

- Root user (account owner or IAM user) is allowed full access to all resources in the account; IAM policies cannot be used to explicitly deny the root user access
- Tasks only possible for the root user
    - Closing of the account
    - Change account settings
    - Restore IAM user permissions
    - Activate IAM access to the Billing and Cost Management
    - Change AWS support plan
    - Configure an AWS S3 bucket to enable MFA Delete

Security Support

There are Native AWS services available as well as 3rd party security products on Marketplace for network security:

- security groups, Network ACLs, AWS WAF

Security Groups	• Acts as a virtual firewall for services to control incoming/outgoing traffic
Network ACLs	• Network Access Control List • Optional layer of security for VPCs that acts as a firewall
AWS WAF	• Web Application Firewall • protects web applications or APIs against common web exploits and bots that affect availability, compromise security, or consume excessive resources

AWS Trusted Advisor

- Online resource to reduce cost, improve security and improve performance
- provides real-time guidance for provision of resources and recommends best-practices for:
    - Cost Optimization
    - Performance
    - Security
    - Fault-tolerance
    - Service limits
- Security checks are a component of the AWS Trusted Advisor