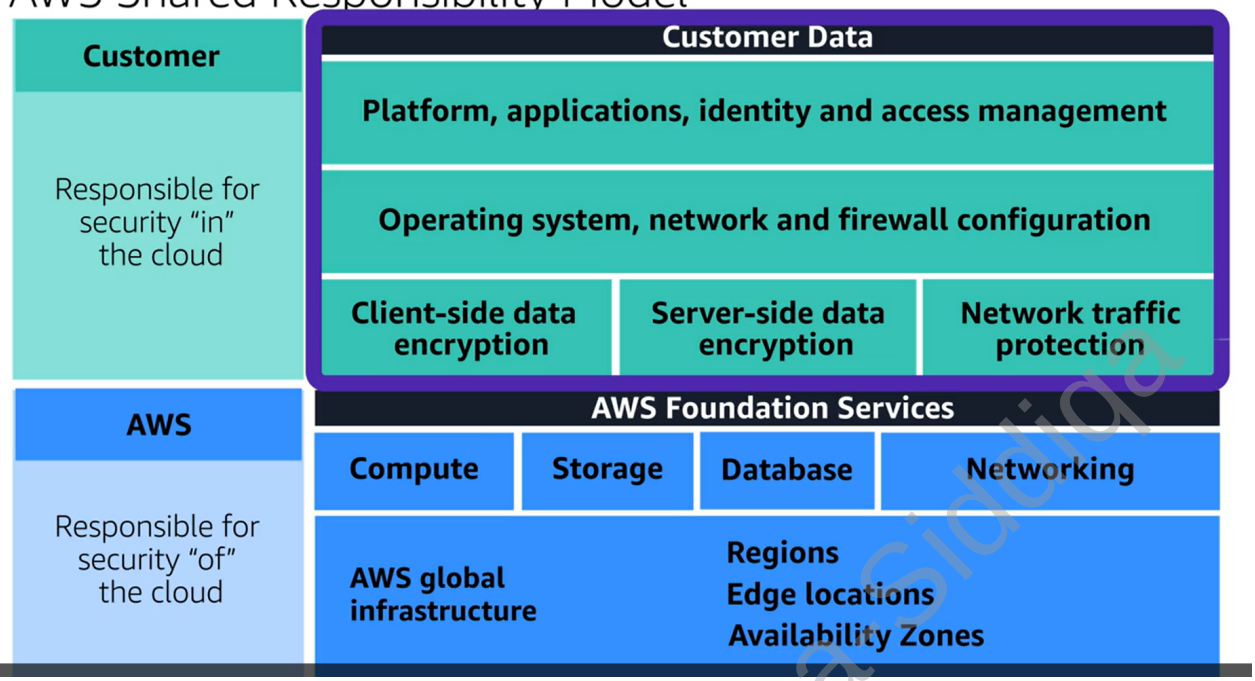
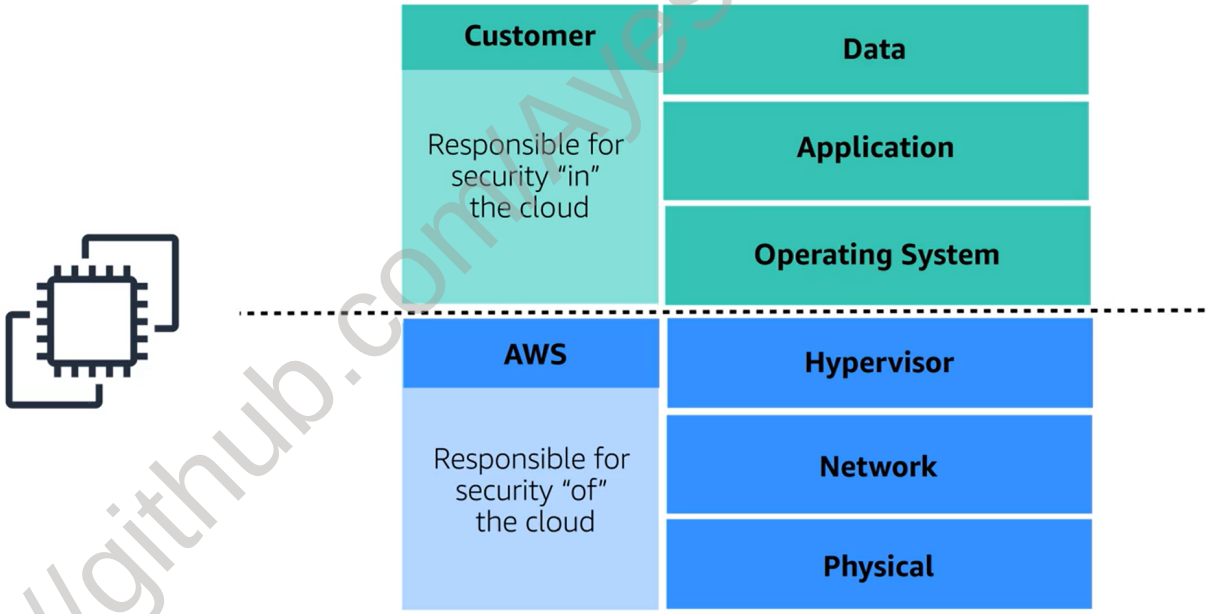
AWS Module 6 - Security

What is the shared responsibility model in AWS, and what are the respective responsibilities of customers and AWS in terms of security?

- **Shared Responsibility Model:**
  - In AWS, security is managed under a shared responsibility model, which divides responsibilities into two categories: customer responsibilities (security in the cloud) and AWS responsibilities (security of the cloud).
- **Customer Responsibilities (Security in the Cloud):**
  - Customers are responsible for the security of everything they create and put in the AWS Cloud.
  - Customers have control over their content, including what they store in AWS, which AWS services they use, and who has access to their content.
  - Customers are responsible for managing access rights, configurations, and security requirements, based on their specific operational and security needs.
  - Responsibilities include selecting, configuring, and patching operating systems on Amazon EC2 instances, configuring security groups, and managing user accounts.
- **AWS Responsibilities (Security of the Cloud):**
  - AWS takes on the responsibility for the security of the cloud itself.
  - AWS operates, manages, and controls infrastructure layers, including the host operating system, virtualization, and physical data center security.
  - AWS ensures the security of the global infrastructure supporting all services in the AWS Cloud, including Regions, Availability Zones, and edge locations.
  - Responsibilities encompass physical security of data centers, hardware and software infrastructure, network infrastructure, and virtualization infrastructure.
  - AWS provides third-party audited reports verifying compliance with various computer security standards and regulations to assure customers of the security of the cloud infrastructure.

AWS Shared Responsibility Model





Which tasks are the responsibilities of customers? (Select TWO.)

- ☒ Maintaining network infrastructure
- ☑ Patching software on Amazon EC2 instances
- ☒ Implementing physical security controls at data centers
- ☑ Setting permissions for Amazon S3 objects
- ☒ Maintaining servers that run Amazon EC2 instances

AWS Identity and Access Management (IAM)

- enables you to manage access to AWS services and resources securely.
- IAM gives you the flexibility to configure access based on your company's specific operational and security needs.

AWS account root user

- When you first create an AWS account, you begin with an identity known as the root user.
- The root user is accessed by signing in with the email address and password that you used to create your AWS account.
- It has complete access to all the AWS services and resources in the account.

IAM users

- An **IAM user** is an identity that you create in AWS. It represents the person or application that interacts with AWS services and resources. It consists of a name and credentials.
- By default, when you create a new IAM user in AWS, it has no permissions associated with it. To allow the IAM user to perform specific actions in AWS, such as launching an Amazon EC2 instance or creating an Amazon S3 bucket, you must grant the IAM user the necessary permissions.

IAM policies

- An **IAM policy** is a document that allows or denies permissions to AWS services and resources.

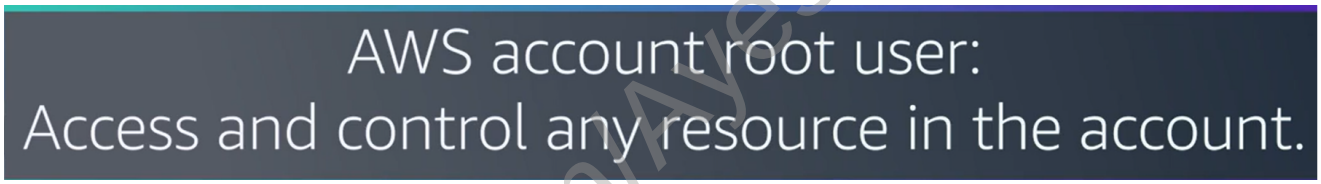
- IAM policies enable you to customize users' levels of access to resources. For example, you can allow users to access all of the Amazon S3 buckets within your AWS account, or only a specific bucket.
- Follow the security principle of **least privilege** when granting permissions.

IAM groups

- An IAM group is a collection of IAM users. When you assign an IAM policy to a group, all users in the group are granted permissions specified by the policy.

IAM roles

- When the employee needs to switch to a different task, they give up their access to one workstation and gain access to the next workstation. The employee can easily switch between workstations, but at any given point in time, they can have access to only a single workstation. This same concept exists in AWS with IAM roles.
  - An IAM role is an identity that you can assume to gain temporary access to permissions.
  - IAM roles are ideal for situations in which access to services or resources needs to be granted temporarily, instead of long-term.



AWS Organizations

- Suppose that your company has multiple AWS accounts. You can use **AWS Organizations** to consolidate and manage multiple AWS accounts within a central location.
- When you create an organization, AWS Organizations automatically creates a **root**, which is the parent container for all the accounts in your organization.
- In AWS Organizations, you can centrally control permissions for the accounts in your organization by using **Services Control Policies**. SCPs enable you to place restrictions on the AWS services, resources, and individual API actions that users and roles in each account can access.

Organizational units

- In AWS Organizations, you can group accounts into organizational units (OUs) to make it easier to manage accounts with similar business or security requirements.
- When you apply a policy to an OU, all the accounts in the OU automatically inherit the permissions specified in the policy.
- By organizing separate accounts into OUs, you can more easily isolate workloads or applications that have specific security requirements. For instance, if your company has accounts that can access only the AWS services that meet certain regulatory requirements, you can put these accounts into one OU. Then, you can attach a policy to the OU that blocks access to all other AWS services that do not meet the regulatory requirements.

AWS Organizations:
A central location to manage multiple AWS accounts

You are configuring service control policies (SCPs) in AWS Organizations. Which identities and resources can SCPs be applied to? (Select TWO.)

- [x] IAM users
- [x] IAM groups
- [✓] An individual member account
- [x] IAM roles
- [✓] An organizational unit (OU)

Correct

The correct two response options are:

- **An individual member account**
- **An organizational unit (OU)**

In AWS Organizations, you can apply service control policies (SCPs) to the organization root, an individual member account, or an OU. An SCP affects all IAM users, groups, and roles within an account, including the AWS account root user.

You can apply IAM policies to IAM users, groups, or roles. You cannot apply an IAM policy to the AWS account root user.

AWS Artifact

- It is a service that provides on-demand access to AWS security and compliance reports and select online agreements.
- AWS Artifact consists of two main sections: AWS Artifact Agreements and AWS Artifact Reports.
- In AWS Artifact Agreements, you can review, accept, and manage agreements for an individual account and for all your accounts in AWS Organizations. Different types of agreements are offered to address the needs of customers who are subject to specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA).
- AWS Artifact Reports provide compliance reports from third-party auditors. These auditors have tested and verified that AWS is compliant with a variety of global, regional, and industry-specific security standards and regulations.

Which tasks can you complete in AWS Artifact? (Select TWO.)

- [x] Access AWS compliance reports on-demand.
- [ ] Consolidate and manage multiple AWS accounts within a central location.
- [ ] Create users to enable people and applications to interact with AWS services and resources.
- [ ] Set permissions for accounts by configuring service control policies (SCPs).
- [x] Review, accept, and manage agreements with AWS.

What is **Denial-of-service** and which AWS service helps to protect against DoS ?

- A **denial-of-service (DoS) attack** is a deliberate attempt to make a website or application unavailable to users.
- For example, an attacker might flood a website or application with excessive network traffic until the targeted website or application becomes overloaded and is no longer able to respond. If the website or application becomes unavailable, this denies service to users who are trying to make legitimate requests.
- AWS Shield is a service that protects applications against DDoS attacks. AWS Shield provides two levels of protection: Standard and Advanced.
  - **AWS Shield Standard** automatically protects all AWS customers at no cost. It protects your AWS resources from the most common, frequently occurring types of DDoS attacks.
    - As network traffic comes into your applications, AWS Shield Standard uses a variety of analysis techniques to detect malicious traffic in real time and automatically mitigates it.
    - **AWS Shield Advanced** is a paid service that provides detailed attack diagnostics and the ability to detect and mitigate sophisticated DDoS attacks.
    - It also integrates with other services such as Amazon CloudFront, Amazon Route 53, and Elastic Load Balancing. Additionally, you can integrate AWS Shield with AWS WAF by writing custom rules to mitigate complex DDoS attacks.

What is **AWS Key Management Service (AWS KMS)**?

- It enables you to perform encryption operations through the use of **cryptographic keys**. A cryptographic key is a random string of digits used for locking (encrypting) and unlocking (decrypting) data. You can use AWS KMS to create, manage, and use cryptographic keys. You can also control the use of keys across a wide range of services and in your applications.
- With AWS KMS, you can choose the specific levels of access control that you need for your keys. For example, you can specify which IAM users and roles are able to manage keys. Alternatively, you can temporarily disable keys so that they are no longer in use by anyone. Your keys never leave AWS KMS, and you are always in control of them.

What is WAF?

- It is a web application firewall that lets you monitor network requests that come into your web applications.
- AWS WAF works together with Amazon CloudFront and an Application Load Balancer.
- AWS WAF works to block or allow traffic. However, it does this by using a web access control lists to protect your AWS resources.
- Suppose that your application has been receiving malicious network requests from several IP addresses. You want to prevent these requests from continuing to access your application, but you also want to ensure that legitimate users can still access it. You configure the web ACL to allow all requests except those from the IP addresses that you have specified.
- When a request comes into AWS WAF, it checks against the list of rules that you have configured in the web ACL. If a request does not come from one of the blocked IP addresses, it allows access to the application. However, if a request comes from one of the blocked IP addresses that you have specified in the web ACL, AWS WAF denies access.

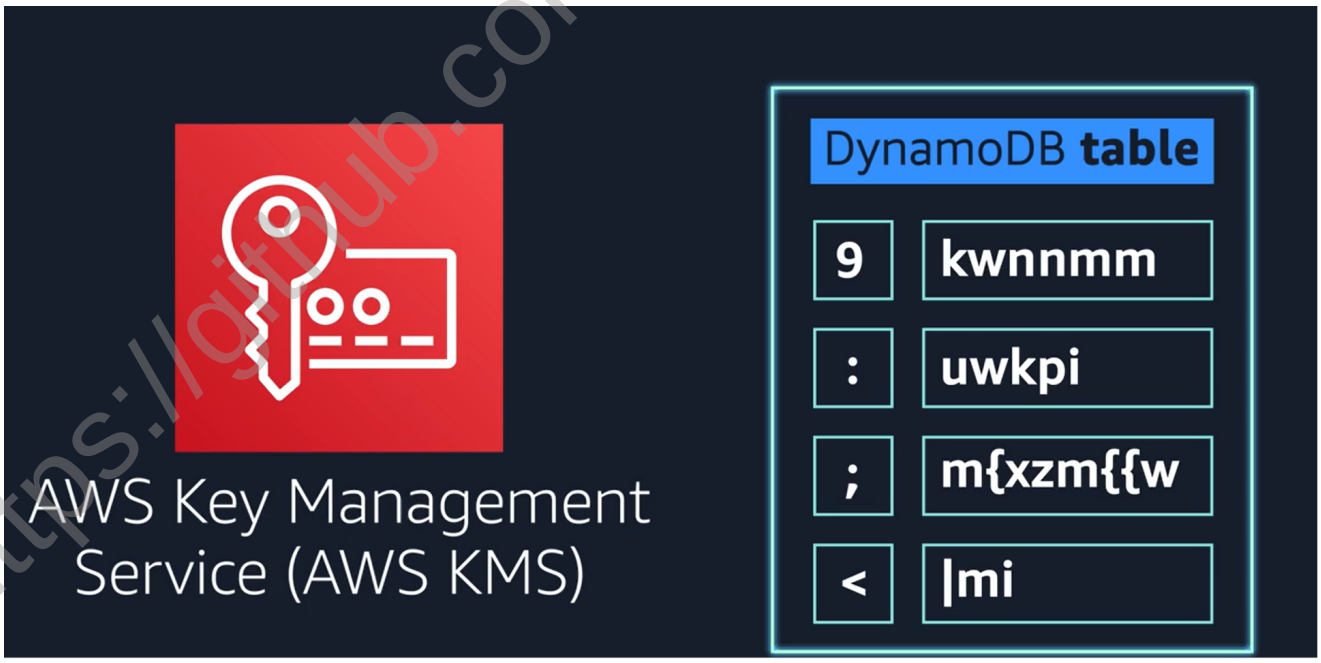
Amazon Inspector

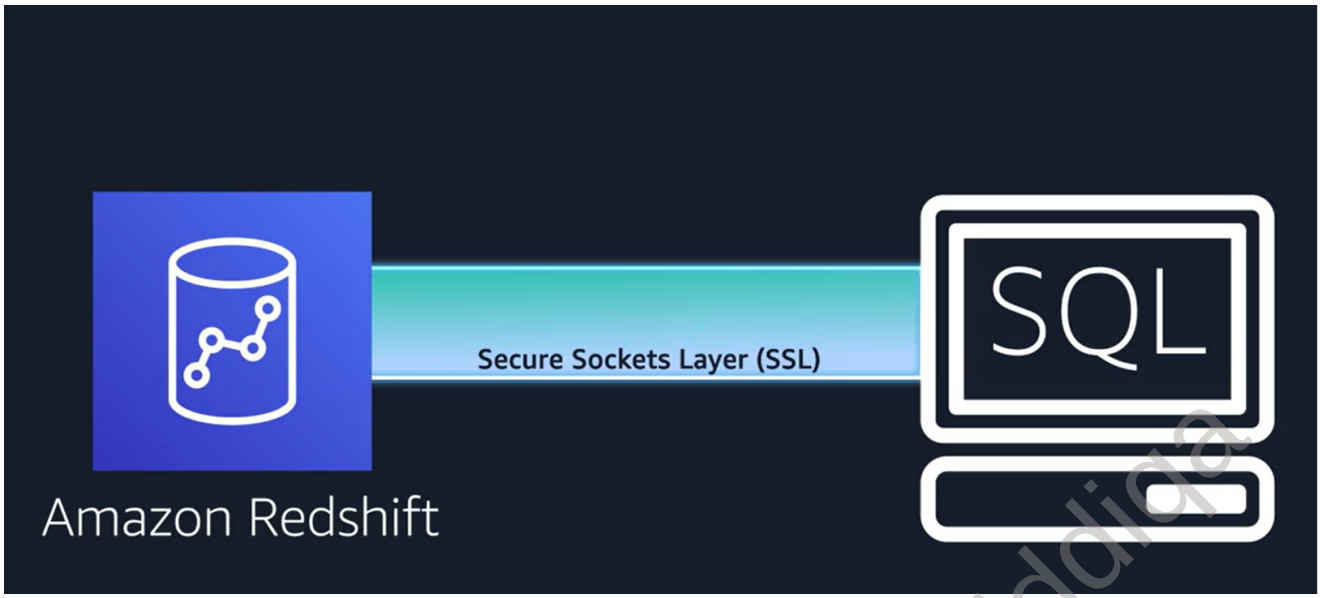
- Amazon Inspector helps to improve the security and compliance of applications by running automated security assessments. It checks applications for security vulnerabilities and deviations from security best practices, such as open access to Amazon EC2 instances and installations of vulnerable software versions.
- Eg: Suppose that the developers at the coffee shop are developing and testing a new ordering application. They want to make sure that they are designing the application in accordance with security best practices. However, they have several other applications to develop, so they cannot spend much time conducting manual assessments. To perform automated security assessments, they decide to use Amazon Inspector.
- After Amazon Inspector has performed an assessment, it provides you with a list of security findings. The list prioritizes by severity level, including a detailed description of each security issue and a recommendation for how to fix it. However, AWS does not guarantee that following the provided recommendations resolves every potential security issue. Under the shared responsibility model, customers are responsible for the security of their applications, processes, and tools that run on AWS services.

Amazon GuardDuty

- It is a service that provides intelligent threat detection for your AWS infrastructure and resources.

- It identifies threats by continuously monitoring the network activity and account behavior within your AWS environment.
- The 4 important steps are:
  - Enable
  - Analyze
  - Intelligently detect
  - review new findings to take action
- After you have enabled GuardDuty for your AWS account, GuardDuty begins monitoring your network and account activity. You do not have to deploy or manage any additional security software.
- GuardDuty then continuously analyzes data from multiple AWS sources, including VPC Flow Logs and DNS logs.
- If GuardDuty detects any threats, you can review detailed findings about them from the AWS Management Console.
- Findings include recommended steps for remediation. You can also configure AWS Lambda functions to take remediation steps automatically in response to GuardDuty's security findings.





Amazon Inspector

- Network configuration reachability piece
- Amazon agent
- Security assessment service

Which statement best describes an IAM policy?

- ✗ An authentication process that provides an extra layer of protection for your AWS account
- ✓ A document that grants or denies permissions to AWS services and resources
- ✗ An identity that you can assume to gain temporary access to permissions
- ✗ The identity that is established when you first create an AWS account

An employee requires temporary access to create several Amazon S3 buckets.

Which option would be the best choice for this task?

- ✗ AWS account root user
- ✗ IAM group
- ✓ IAM role
- ✗ Service control policy (SCP)

Which statement best describes the principle of least privilege?

- ✗ Adding an IAM user into at least one IAM group
- ✗ Checking a packet's permissions against an access control list
- ✓ Granting only the permissions that are needed to perform specific tasks
- ✗ Performing a denial of service attack that originates from at least one device

Which service helps protect your applications against distributed denial-of-service (DDoS) attacks?

- ✗ Amazon GuardDuty
- ✗ Amazon Inspector
- ✗ AWS Artifact
- ✓ AWS Shield

Which task can AWS Key Management Service (AWS KMS) perform?

- ✗ Configure multi-factor authentication (MFA).
- ✗ Update the AWS account root user password.
- ✓ Create cryptographic keys.
- ✗ Assign permissions to users and groups.

Some other Security Services

AWS Single Sign-On

- AWS Single Sign-On (SSO) is a cloud SSO service that makes it easy to centrally manage SSO access to multiple AWS accounts and business applications.

AWS Security Hub

- AWS Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts.

AWS Secrets Manager

- helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

AWS Resource Access Manager

- helps you securely share your resources across AWS accounts, within your organization or organizational units (OUs) in AWS Organizations, and with IAM roles and IAM users for supported resource types.

AWS Network Firewall

- It is a managed service that makes it easy to deploy essential network protections for all of your Amazon Virtual Private Clouds (VPCs).

AWS Firewall Manager

- It is a security management service that makes it easier to centrally configure and manage AWS WAF rules across your accounts and applications.

AWS Directory Service

- Also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.

AWS CloudHSM

- It is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

AWS Certificate Manager

- It is a service that lets you easily provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal 68Overview of Amazon Web Services AWS Whitepaper AWS CloudHSM connected resources.

AWS Audit Manager

- It helps you continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards.

Amazon Macie

- It is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

Amazon Detective

- Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations.

Amazon Cloud Directory

- With Cloud Directory, you can create directories for a variety of use cases, such as organizational charts, course catalogs, and device registries.

Amazon Cognito

- It lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.