module 6: security

learning objectives -

- explain the benefits of the shared responsibility model.
- describe multi-factor authentication (mfa).
- differentiate between the AWS Identity and Access Management (IAM) security levels.
- explain the main benefits of AWS Organizations.
- describe security policies at a basic level.
- summarize the benefits of compliance with AWS.
- explain additional AWS security services at a basic level.

▼ ***What is the shared responsibility model?***

It's a security mechanism

▼ ***How does AWS interact with the customers in the shared responsibility model?***

AWS controls security of the cloud and customers control security within in the cloud.

AWS controls the data centers, security of the services, and all layers in this section.

The workloads AWS customers run in the cloud are their responsibility.

▼ ***Imagine that the shared responsibility model is like securing a house. Explain this analogy:***

The builder constructs the house with four walls and a door. The builder's responsibility is to make sure the walls and door are strong. But as a homeowner, you need to close and lock the doors.

▼ ***What is AWS in the house model?***

AWS is the physical perimeter. We have the network and hypervisor.

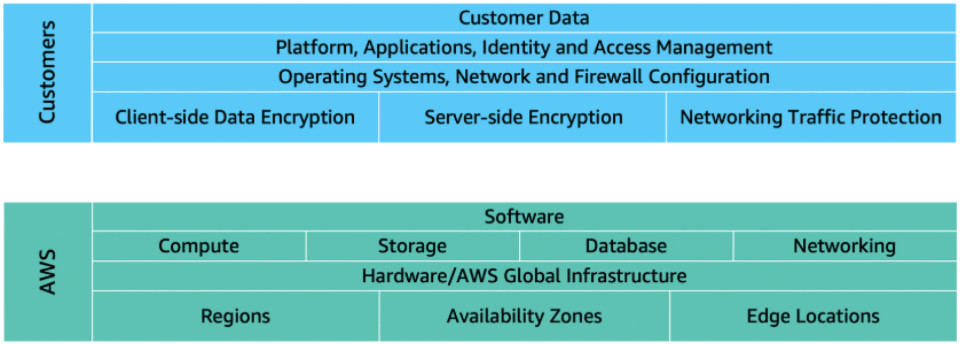
▼ ***How do you know that AWS is providing security?***

There are numerous third party auditors who go through code and infra to provide the right documentation you need for security.

▼ *What are you 100% in charge of?*

The Operating System - AWS can’t access ur system. You and you alone have the encryption key to log into the root of the OS.

And data.



Customers

Customer Data

Platform, Applications, Identity and Access Management

Operating Systems, Network and Firewall Configuration

Client-side Data Encryption | Server-side Encryption | Networking Traffic Protection

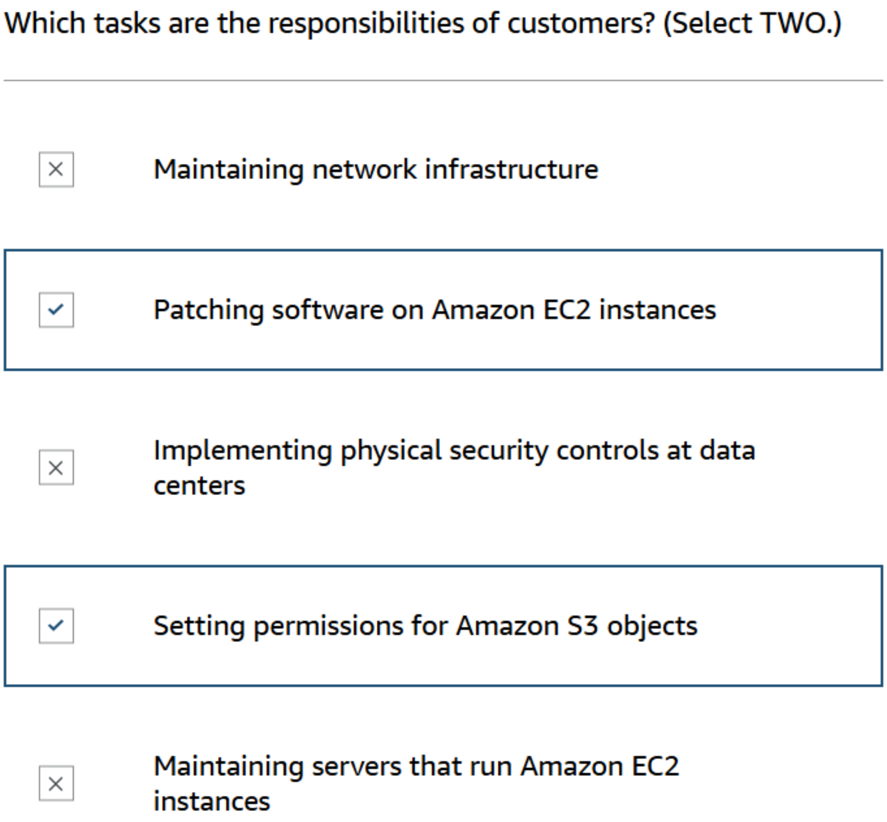
AWS

Software

Compute | Storage | Database | Networking

Hardware/AWS Global Infrastructure

Regions | Availability Zones | Edge Locations



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

▼ ***Who is the root user?***

The owner of the AWS account. They cannot be restricted. They can access and control any resource.

▼ ***How do you control access?***

Granularly, by using IAMs

▼ ***After creating a user, what’s the default?***

They don’t have any permissions

▼ ***What is the least privilege principle?***

The idea that you give people access only to what they need and nothing else.

▼ ***What is an IAM policy?***

It’s a JSON document that describes what API calls a user can or cannot make.

▼ ***What are groups?***

Literally groups of people where you can attach a policy to a group and all of the users in that group.

▼ ***What are roles?***

You can create identities in AWS that are called roles. So roles have associated permissions that allow or deny specific actions. These roles can be temporary and they have no username and password.

▼ ***What happens when an identity assumes a role?***

It abandons all of the previous permissions that it has and it assumes the permissions of that role.

▼ ***What does it mean by federating users into your account?***

It means that they could use their regular corporate credentials to log into AWS by mapping their corporate identities to IAM roles.

▼ ***What is an IAM user?***

An identity that you create in AWS. It represents the person or application that interacts with AWS services and resources.

▼ ***What is the best practice for IAM users?***

Create individual IAM users for each person who needs to access AWS.

▼ ***Before an IAM user, app, or service can assume an IAM role…***

They must be granted permissions to switch to the role.

▼ ***What are AWS organizations?***

A way to install order and to enforce who is allowed to perform certain functions in what account

▼ ***What is one way to explain Organizations?***

A central location that manages multiple AWS accounts.

▼ ***What are the features of AWS Organizations?***

Centralized Management

Consolidated Billing

Hierarchical Groupings of your accounts to meet needs

▼ ***What are SCPs?***

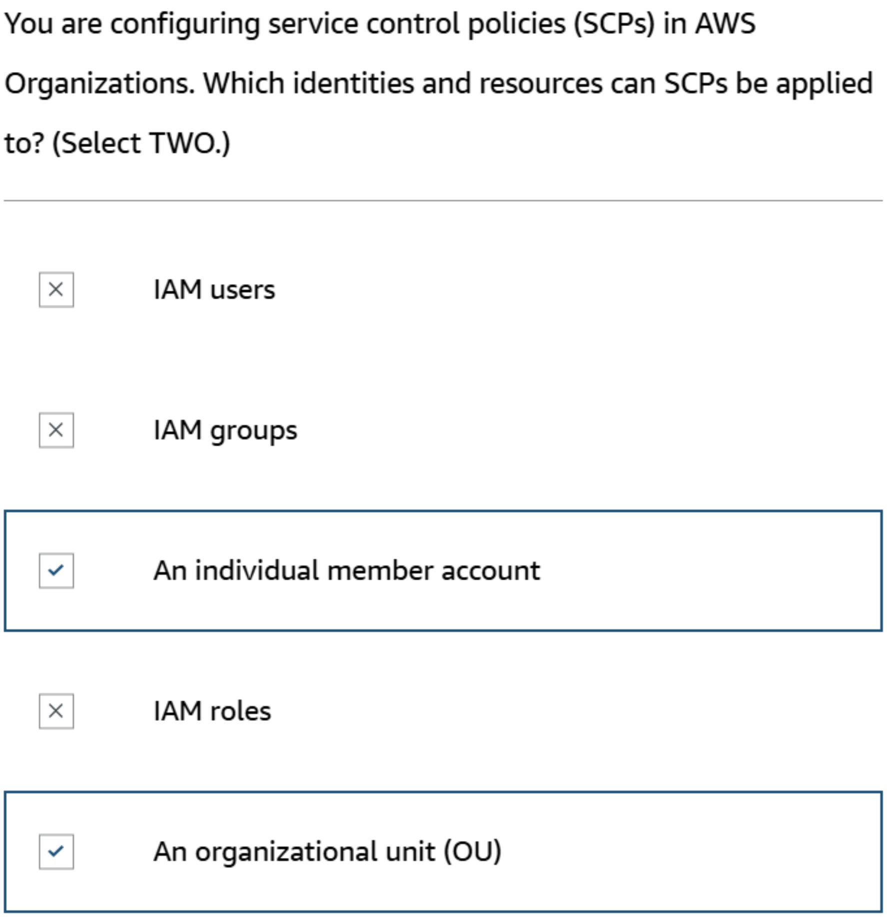
Security Control Policies

▼ ***What are Organization Roots?***

A parent container for all the accounts in the organization

▼ ***When you apply a policy to an OU…***

All the accounts in the OU automatically inherit the permissions specified in the policy.



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

☒ IAM users

☒ IAM groups

☑ An individual member account

☒ IAM roles

☑ An organizational unit (OU)

▼ ***How does the Region relate to the compliance regulations?***

It might help you meet compliance regulations

▼ ***How can you access these documents?***

AWS Artifact. With AWS Artifact, you can gain access to compliance reports by third parties.

▼ ***What are AWS Artifact Agreements?***

Ways to review, accept, and manage agreements for an individual account and for all your accounts in AWS Organizations.

▼ ***What are AWS Artifact Reports?***

Provide compliance reports from third-party auditors.

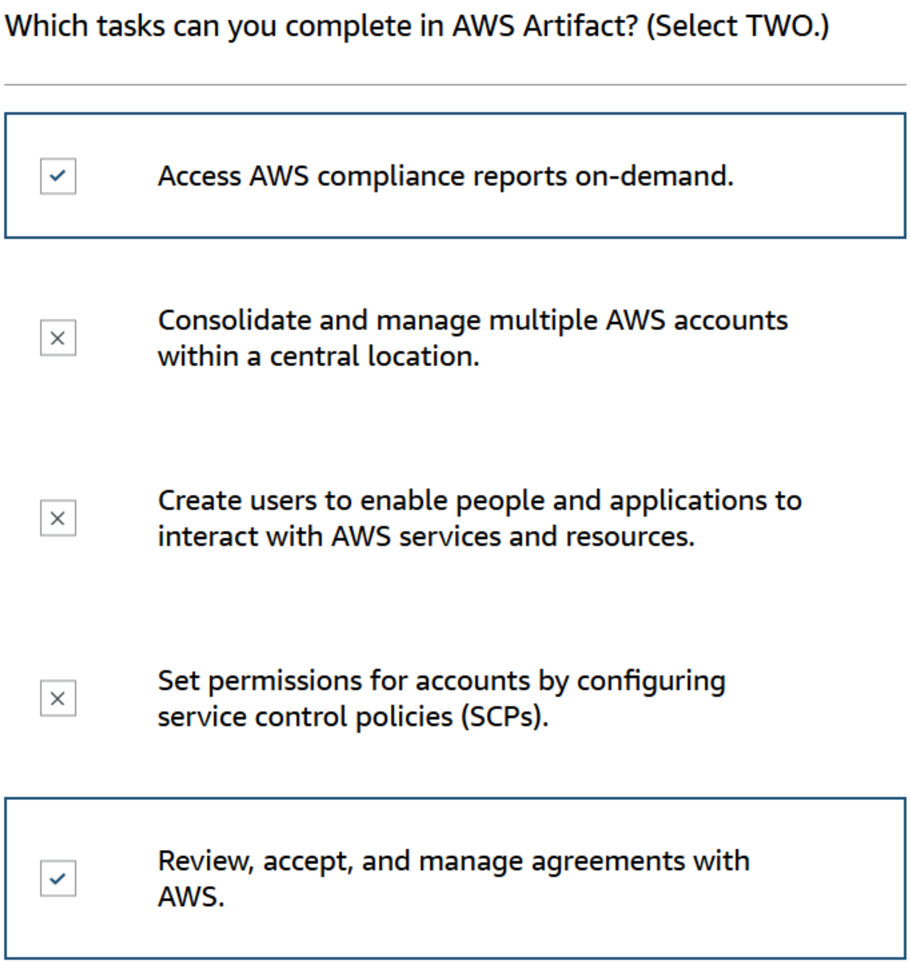
Global
CSA cloud security alliance
ISO 9001
ISO 27001
ISO 27017
ISO 27018
PCI
AICPA SOC
AICPA SOC
AICPA SOC
USA
FR
FedRAMP
FFIEC
FIPS
FISMA
HIPAA
HITRUST CSF Certified
ITAR
Europe
C5
CYBER ESSENTIALS PLUS
ens
Asia Pacific
irap
iDA
SINGAPORE
TÜV AUSTRIA
TISAX

▼ ***What is the Customer Compliance Center?***

Contains resources to help you learn more about AWS compliance.

▼ ***What are some topics that the whitepapers cover?***

- AWS answers to key compliance questions
- An overview of AWS risk and compliance
- An auditing security checklist



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

☑ 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).

☑ Review, accept, and manage agreements with AWS.

- ▼ ***What does DDoS stand for?***

  Distributed Denial of Service

- ▼ ***What does DDoS do?***

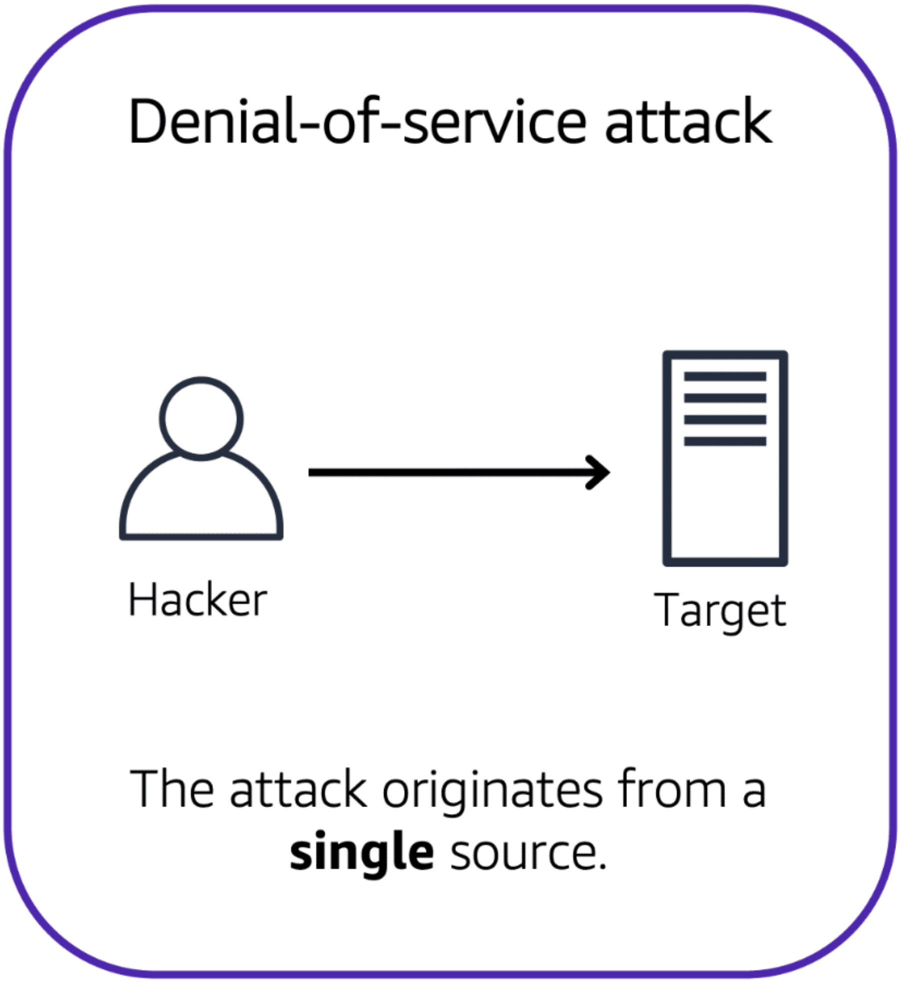
  It should shut down your application’s ability to function by overwhelming the system to the point it can no longer operate. It tries to overwhelm the capacity of your application, basically to deny anyone your services. It creates an army of zombie bots, brainlessly assaulting your enterprise.

- ▼ ***What service is overwhelmed?***

  ELB - but ELB is scalable. And in order to overwhelm ELB, we need to overwhelm the entire region.

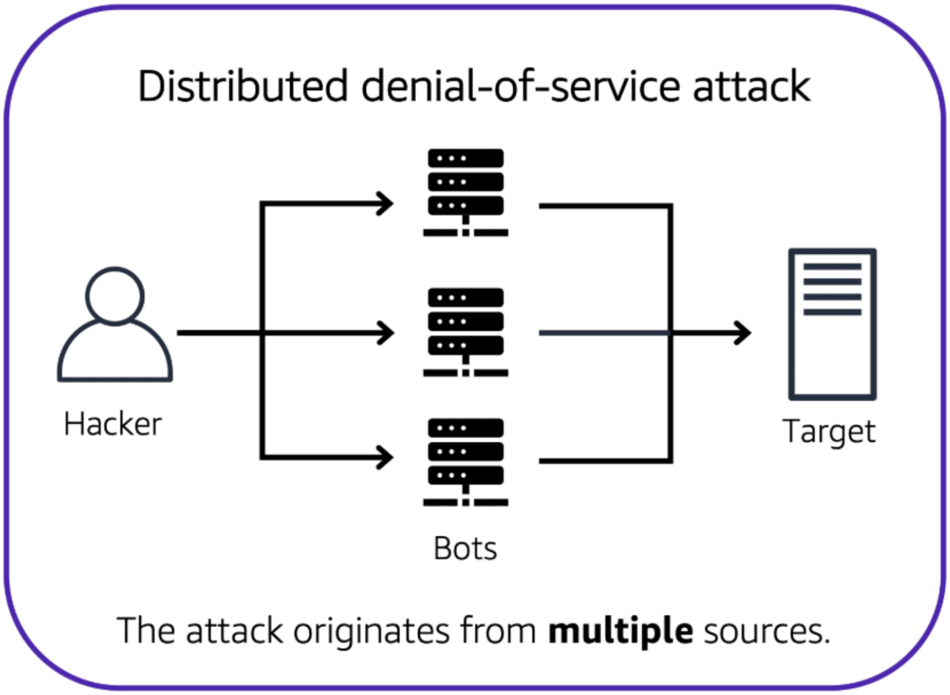
▼ ***What is AWS WAF?***

Web Application Firewall to filter incoming traffic for the signatures of bad actors.



Denial-of-service attack

The attack originates from a **single** source.


Distributed denial-of-service attack
Hacker
Bots
Target
The attack originates from **multiple** sources.

▼ ***What's the difference between AWS Shield Standard and Advanced?***

Standard is free, Advanced is a paid service.

▼ ***What is AWS KMS?***

Enables you to perform encryption operations through the use of cryptographic keys.

▼ ***What is encryption at rest?***

In storage

▼ ***What is encryption in transit?***

Data while it is being transmitted.

▼ ***What can you do with the keys?***

You can specify which IAM users and roles are able to manage keys.

You can also temporarily disable keys so that they are no longer in use by anyone.

▼ ***Can keys leave AWS KMS?***

No, and you are always in control of them

- ▼ ***What is AWS WAF?***

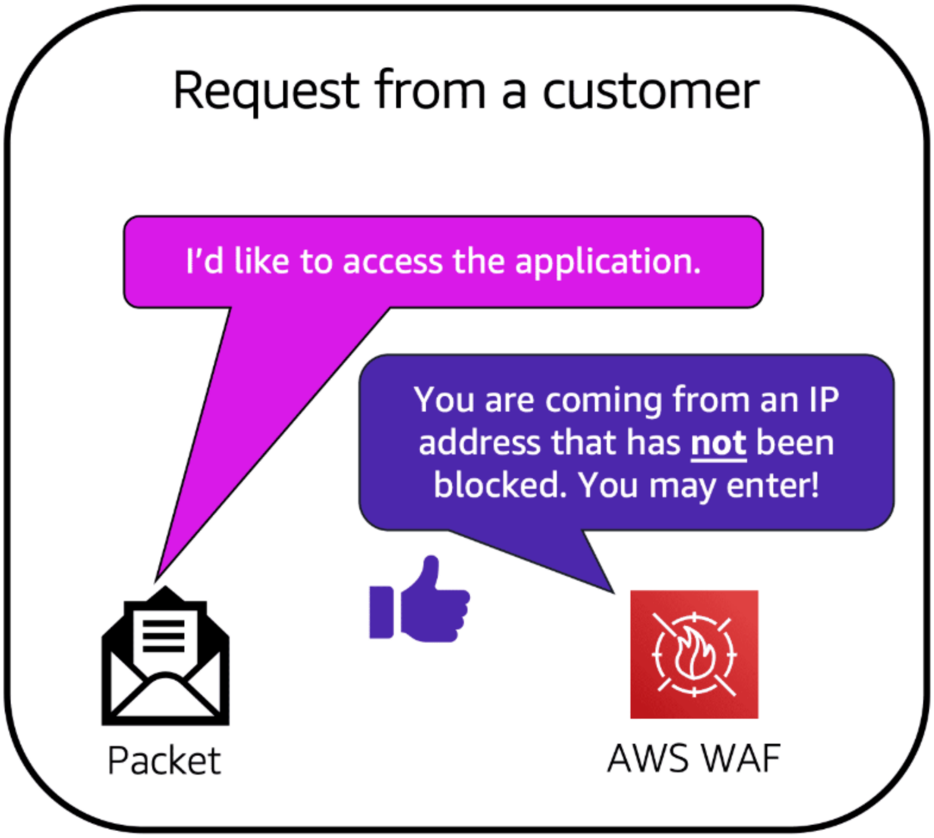
  A web application firewall that lets you monitor network requests that come into your web apps

- ▼ ***What does AWS WAF work together with?***

  Amazon CloudFront and Application Load Balancer.

- ▼ ***To what thing does AWS WAF work similar to?***

  NACLs. But it uses ACLs to protect AWS resources.

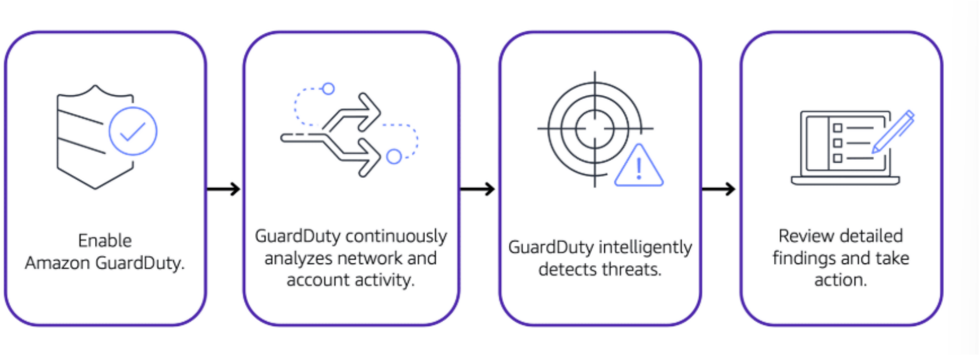

Request from a customer
I'd like to access the application.
You are coming from an IP address that has not been blocked. You may enter!
Packet
AWS WAF

- ▼ ***What is Amazon Inspector?***

  Performs automated security assessments. This will help improve the security and compliance of applications by running automated security assessments.

- ▼ ***What is Amazon Guard Duty?***

  Intelligent threat detection



Enable Amazon GuardDuty.

GuardDuty continuously analyzes network and account activity.

GuardDuty intelligently detects threats.

Review detailed findings and take action.

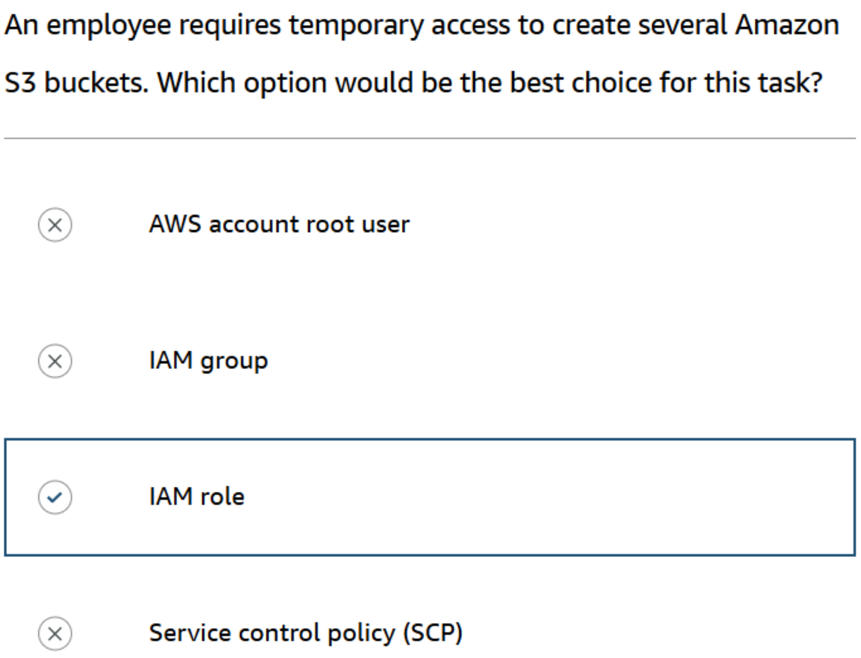
Which statement best describes an IAM policy?

✗ 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

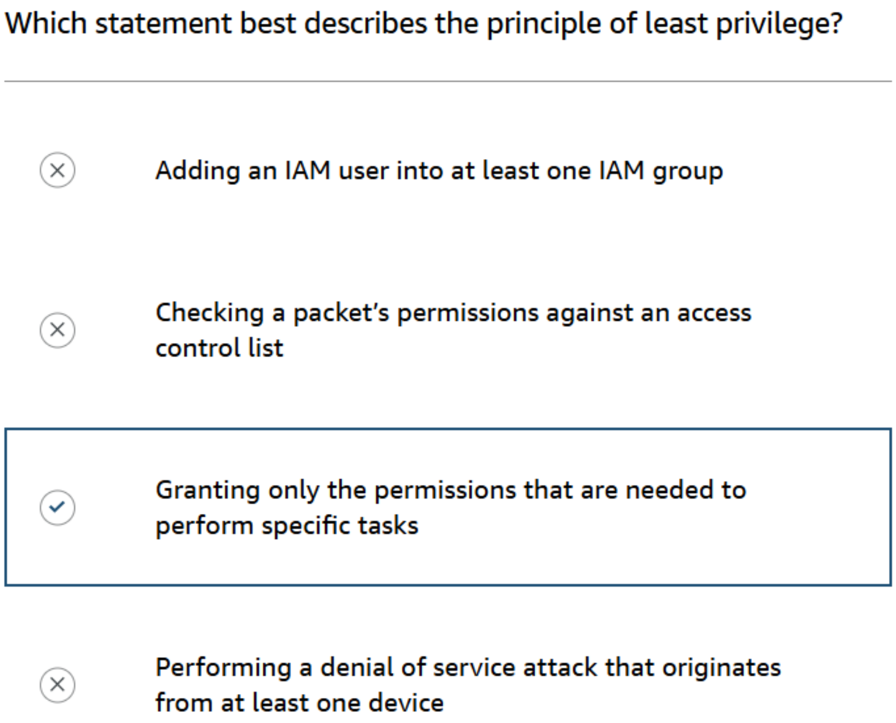
✗ An identity that you can assume to gain temporary access to permissions

✗ The identity that is established when you first create an AWS account



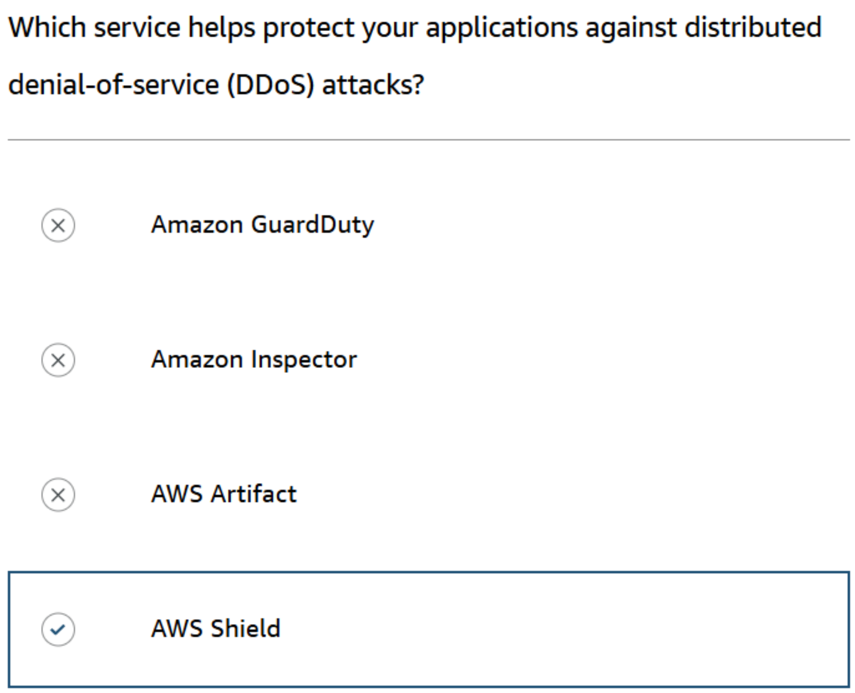
An employee requires temporary access to create several Amazon S3 buckets. Which option would be the best choice for this task?

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



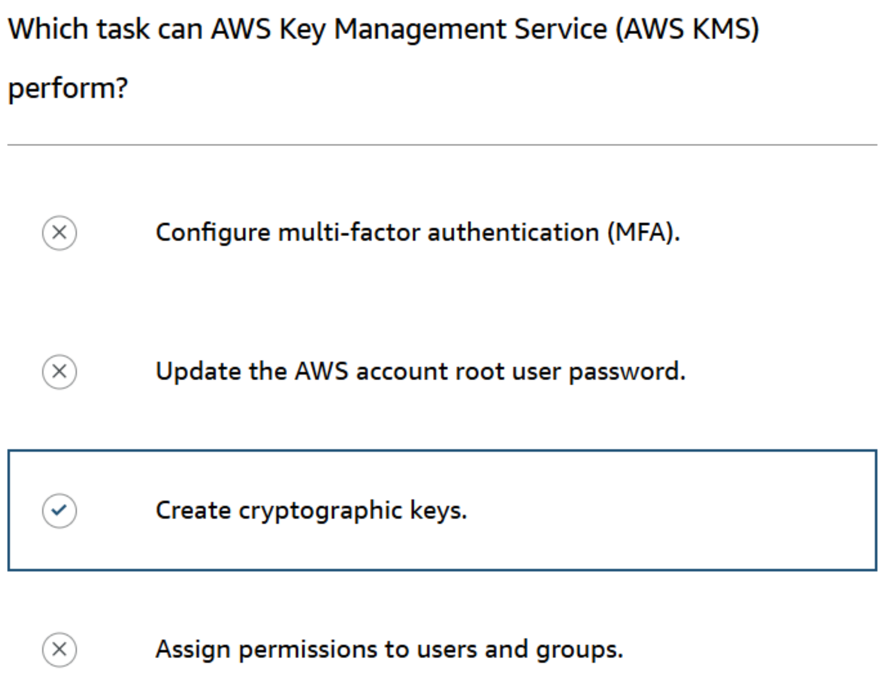
Which statement best describes the principle of least privilege?

- ⊗ 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.