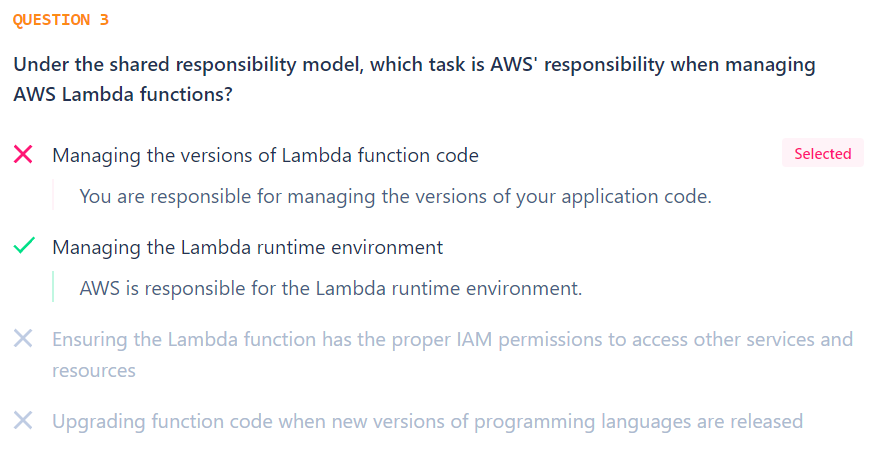
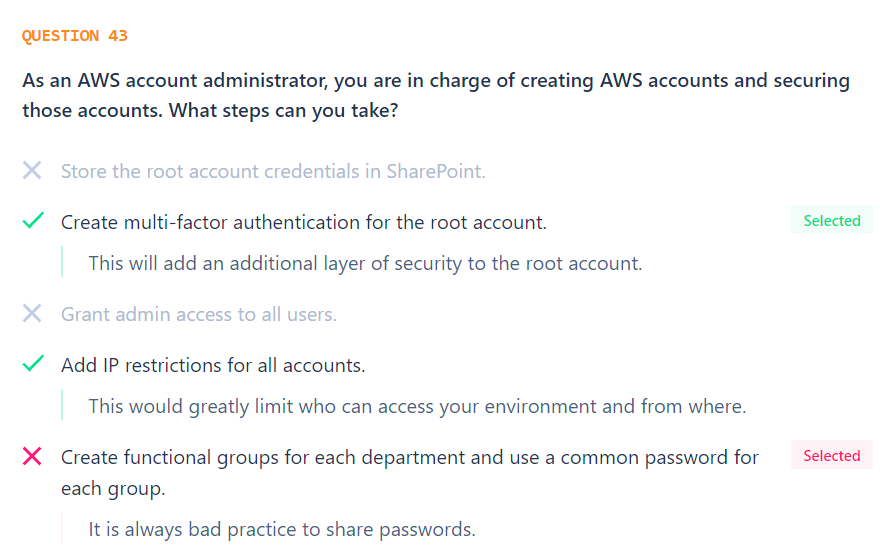
ACCP Questions

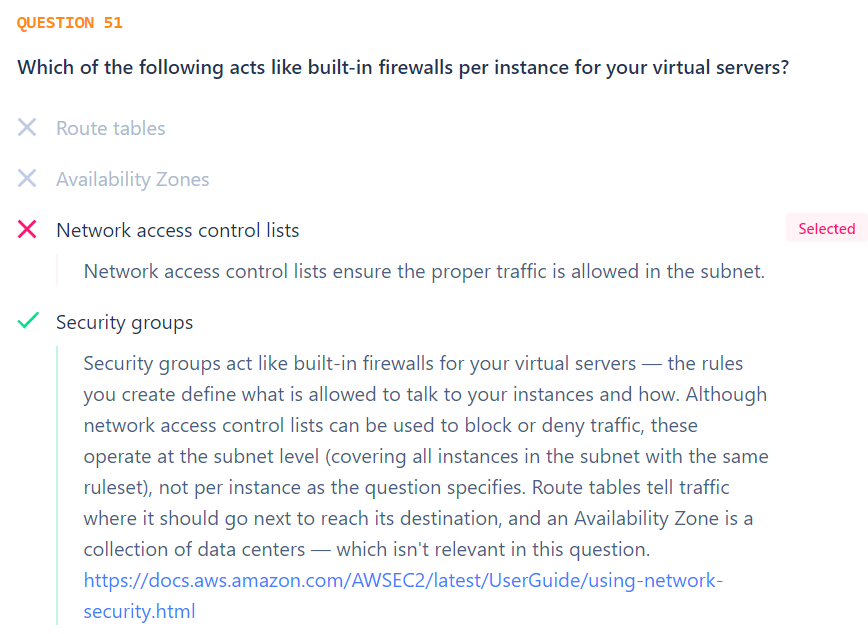
* Security and Compliance

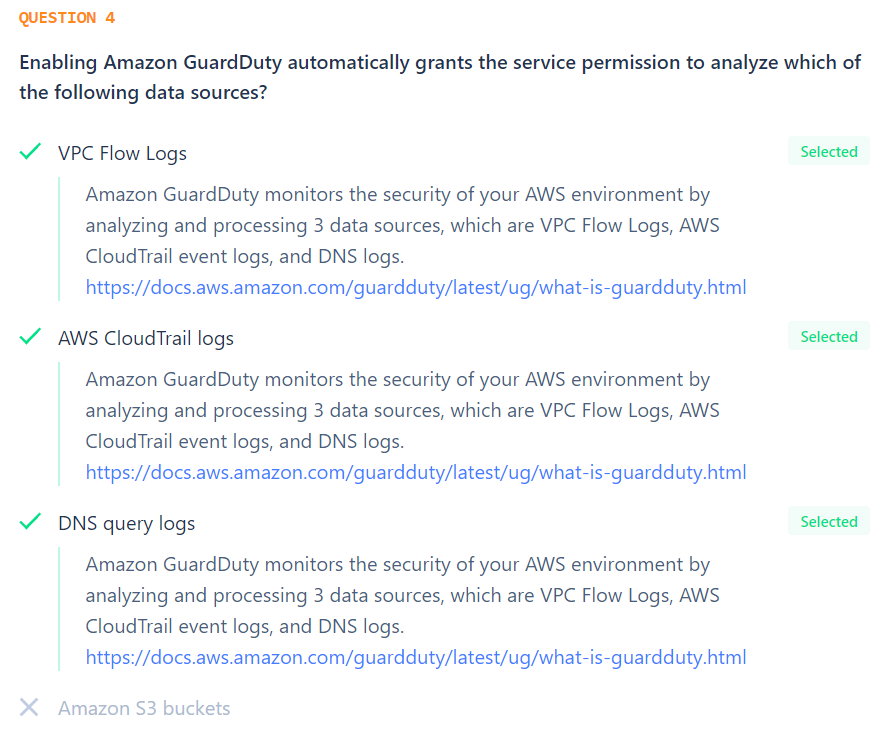
Points to be remembered

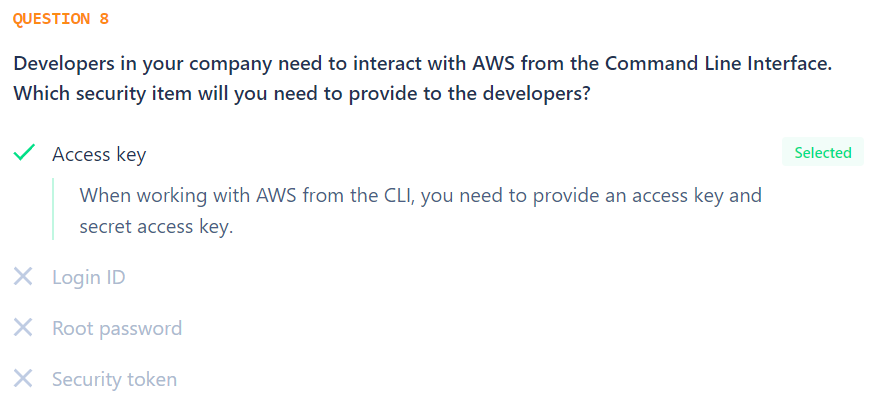
* AWS is responsible for managing lambda runtime environment.
* You are responsible for version of lambda function code.
* Security groups act like built-in firewalls per instance for your virtual servers. Although network access control lists can be used to block or deny traffic, these operate at the subnet level, not per instance as the question specifies.
* Amazon GuardDuty monitors the security of your AWS environment by analyzing and processing 3 data sources, which are VPC Flow Logs, AWS CloudTrail event logs, and DNS logs. GuardDuty continuously monitor CloudTrail logs, VPC Flow Logs, DNS Logs to uncover unauthorized behavior.
* Don’t delete root user password. Delete root access keys.
* IAM controls authentication and authorization within an AWS account.
* IAM allows you to create and manage access keys for IAM user for CLI.
* AWS is responsible for ensuring malicious traffic does not impair network hardware.
* You are responsible for ensuring malicious traffic does not reach your EC2 instance.
* Data in transit is the data that moves from one location to another.
* Entities are users and roles that are created and used for authentication. Identity is an IAM resource object that is used to identify and group. We can attach a policy to IAM identity. There include users, groups and roles.
* Customer Service Policy for Penetration Testing- providing information on performing penetration testing on EC2 instance.
* Customer is responsible for VPC, Security Group and Subnet.
* AWS Trusted Advisor helps you to access fault tolerance of AWS environment.
* Customer is responsible for updating database software.
* Customer is responsible for updating guest OS.
* Customer is responsible for managing access to database.
* The IAM policy simulator allows you to test and troubleshoot identity-based policies, IAM permissions boundaries, service control policies (SCPs), and resource-based policies.
* A principal is a person or application that uses the AWS account root user, an IAM user, or an IAM role to sign in and make requests to AWS.
* Federated access is when you use external directory such as corporate directory to grant users in that directory access to AWS resources.
* Service Control Policies allow you to create permissions that apply to all accounts within an organization.
* Authentication: who can access
* Authorization: what can they access
* By default, new security group allow all outbound traffic and deny all inbound traffic
* Group-> pre-defined set of permissions based on role
* IAM Password Policy-> for strong passwords
* Free of vulnerable- Inspector
* Web attacks- WAF

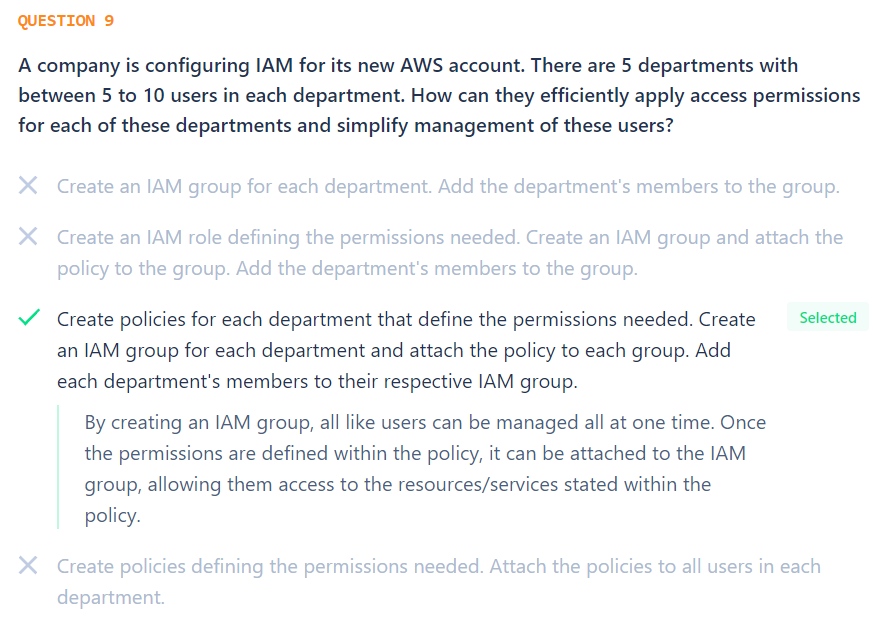


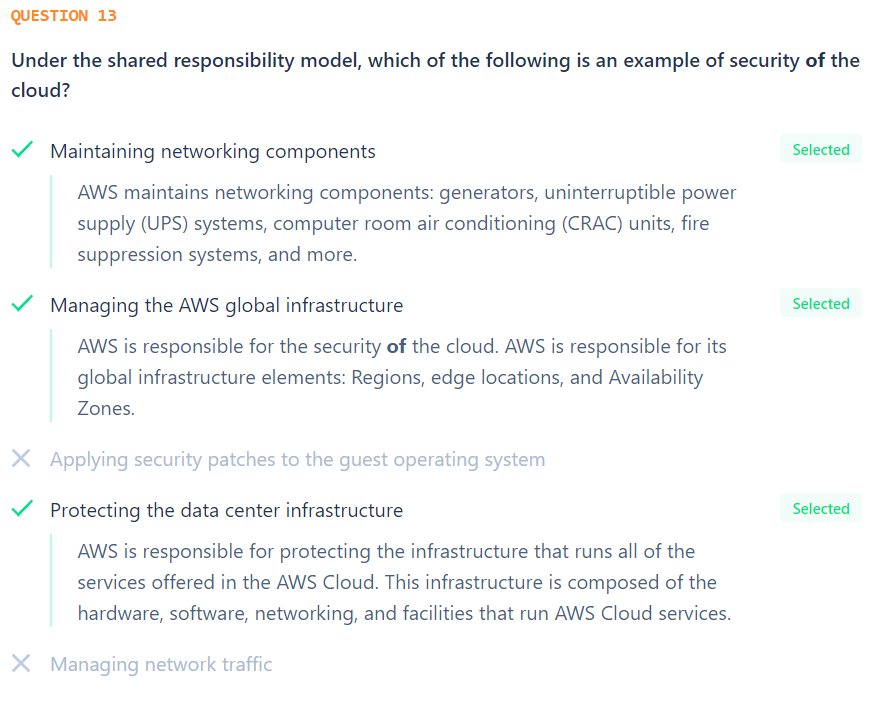


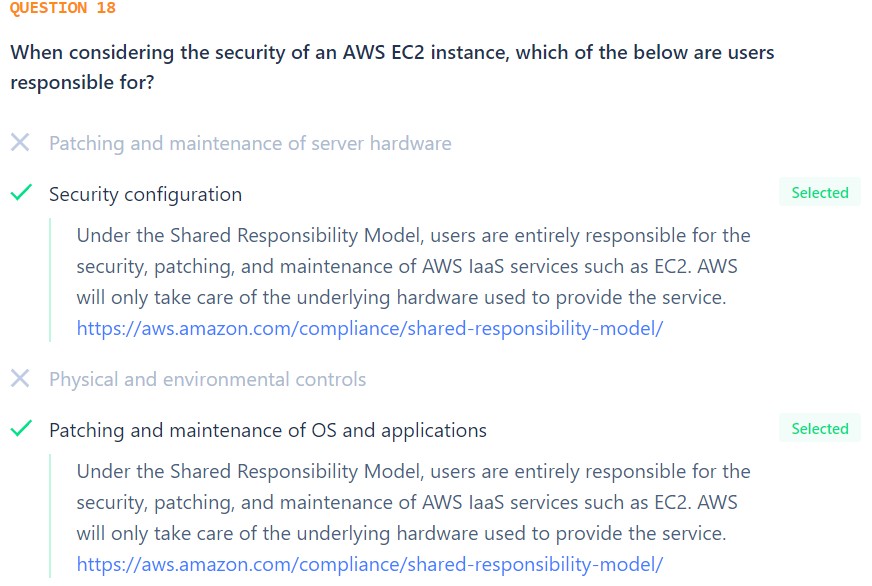


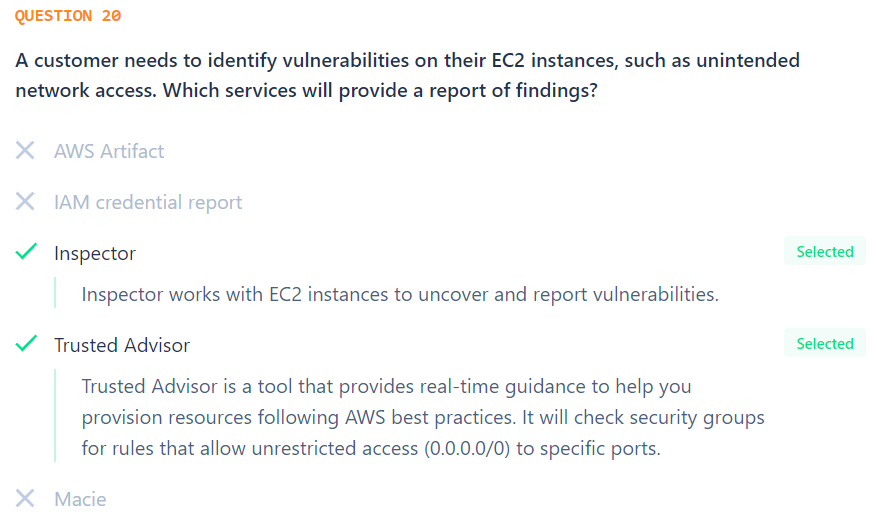




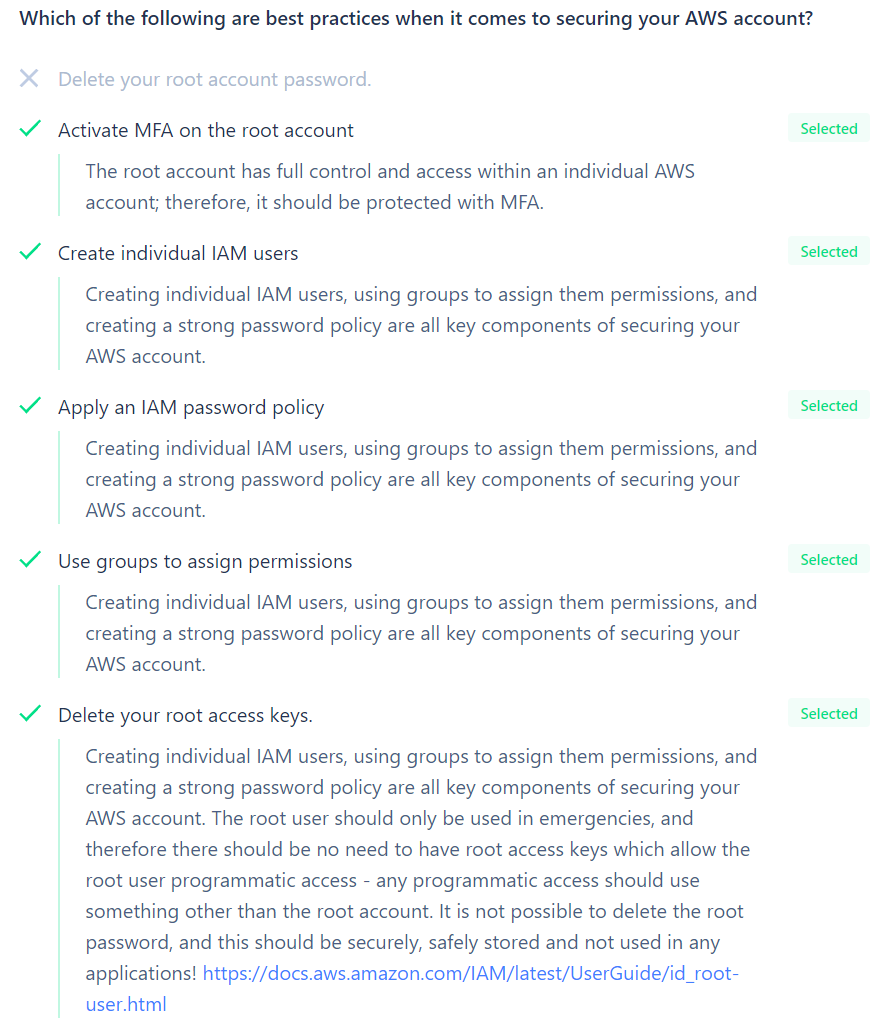






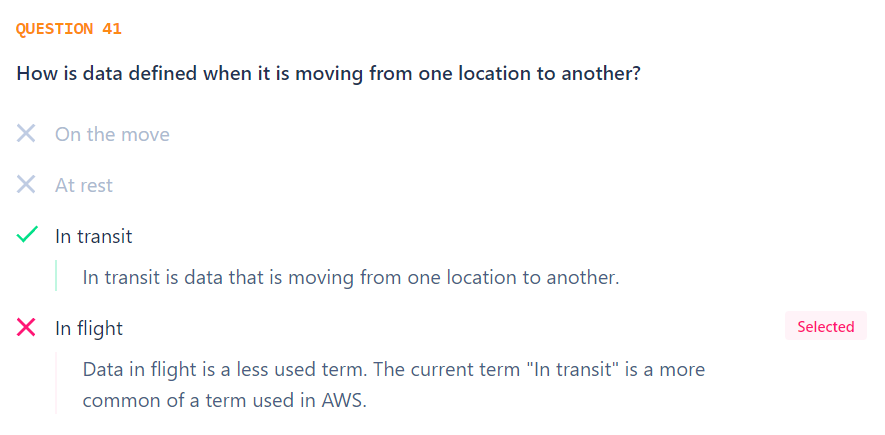


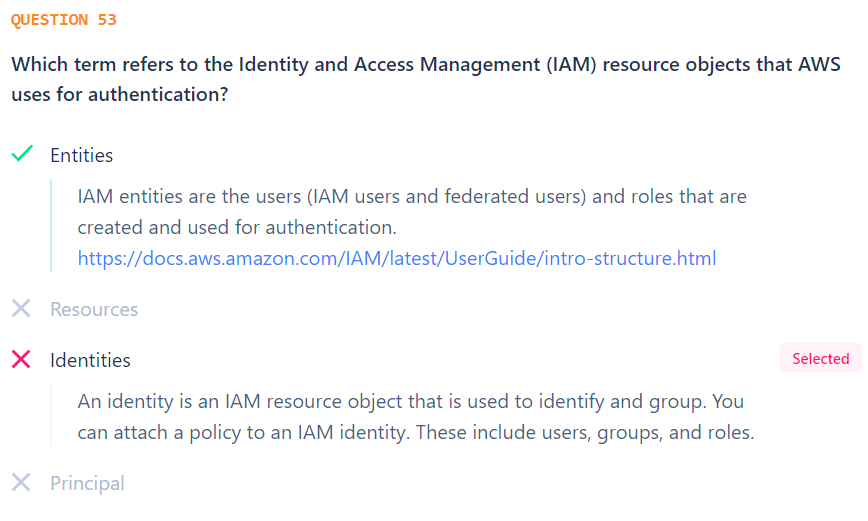


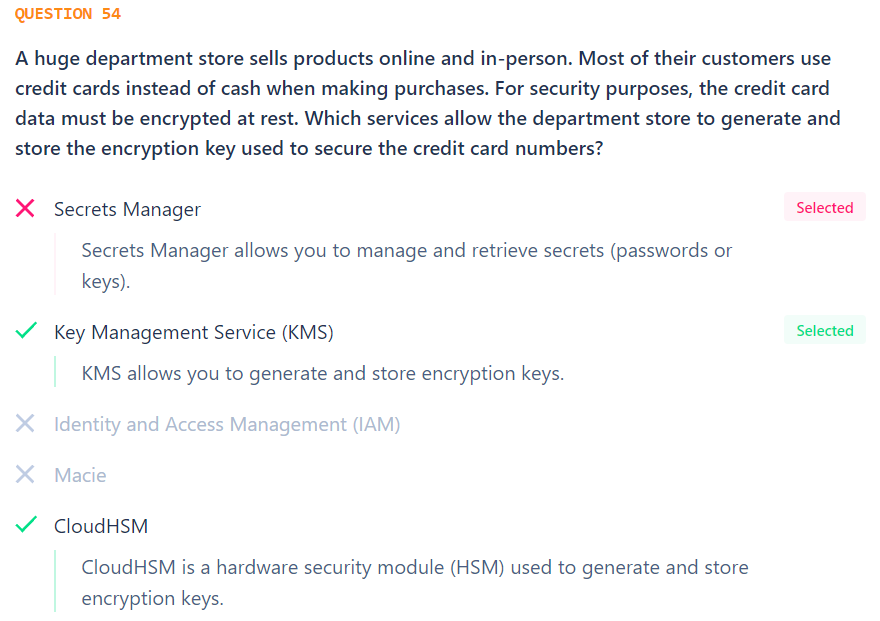


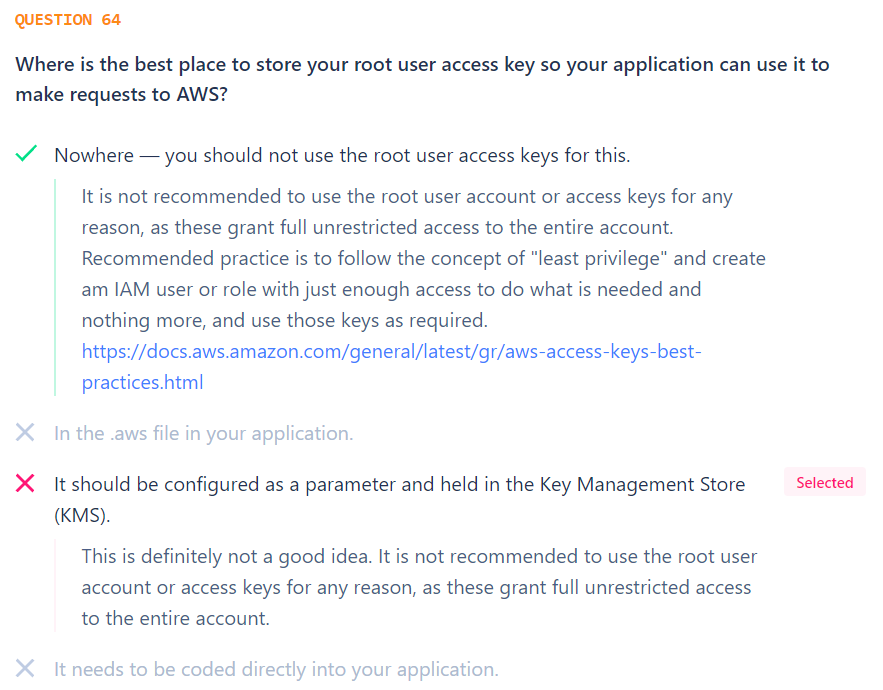


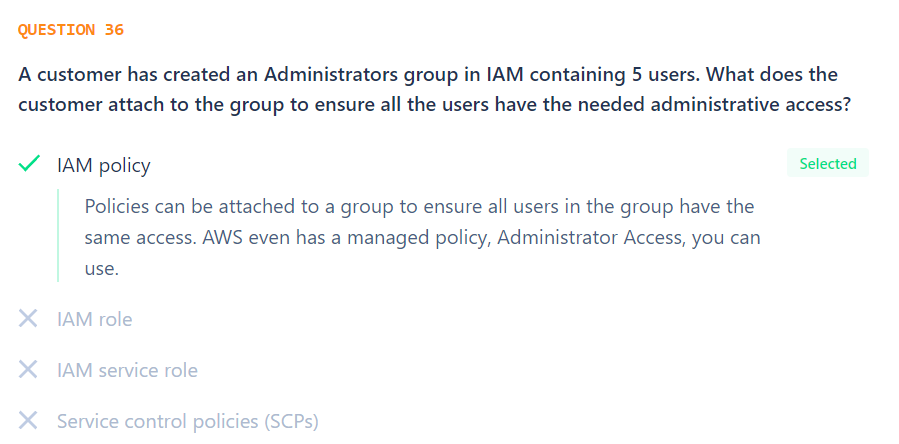


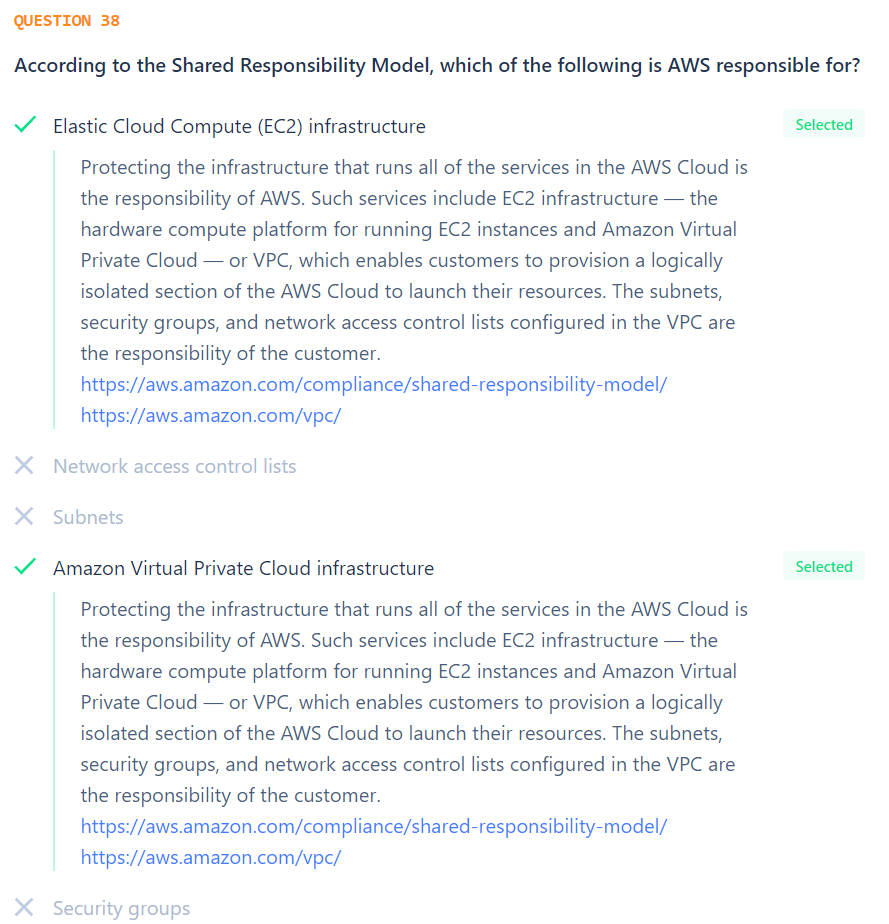


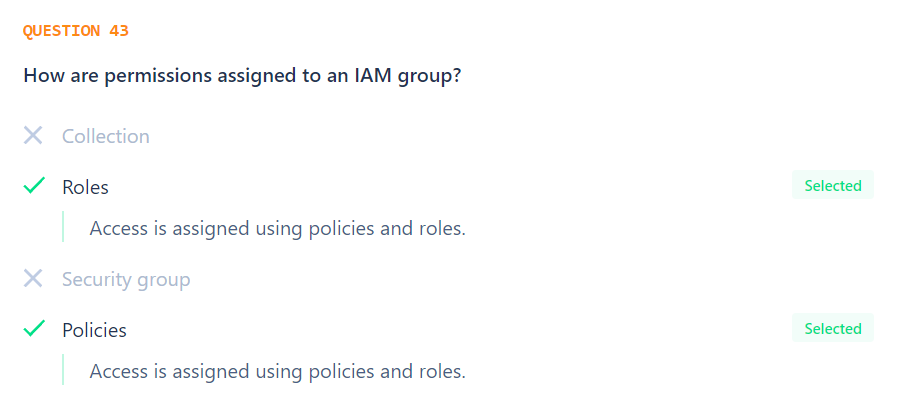


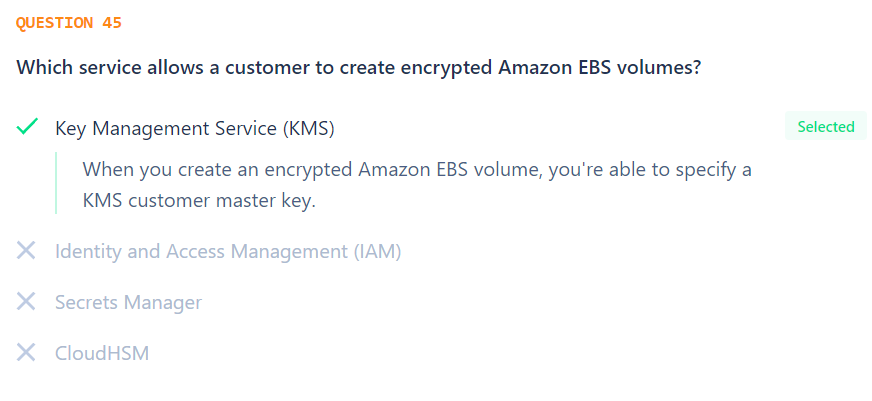




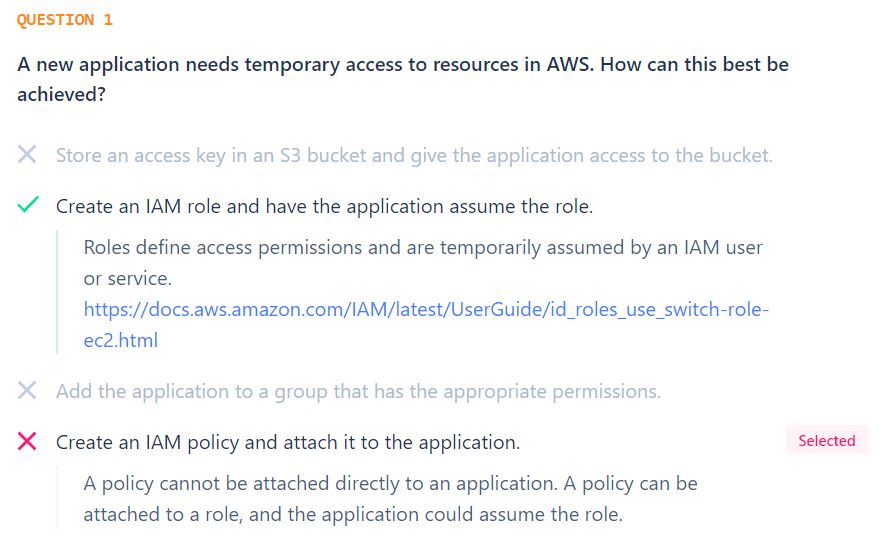






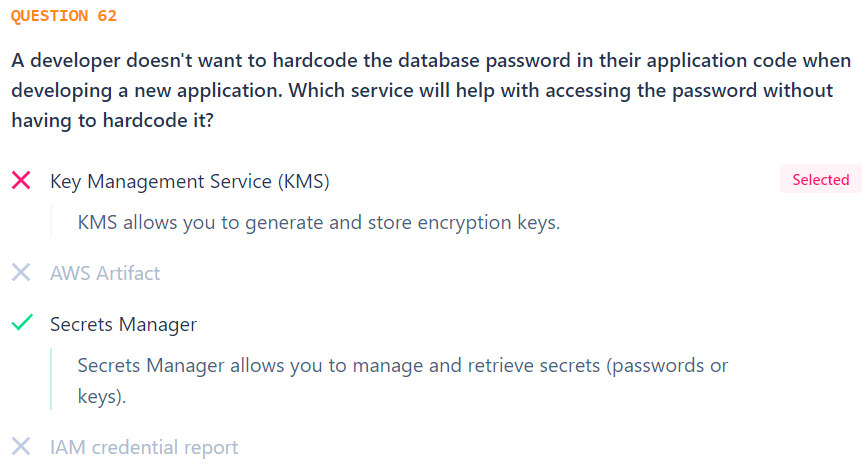


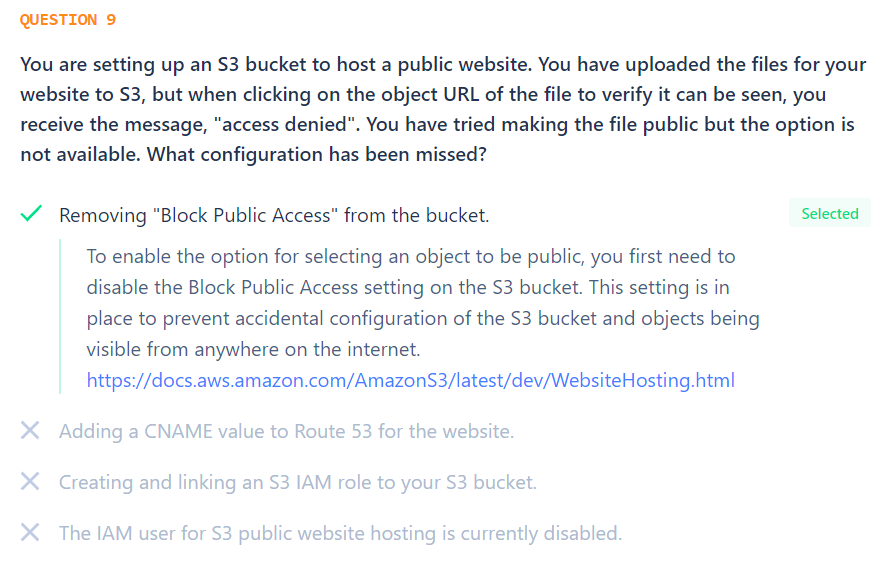
Marked



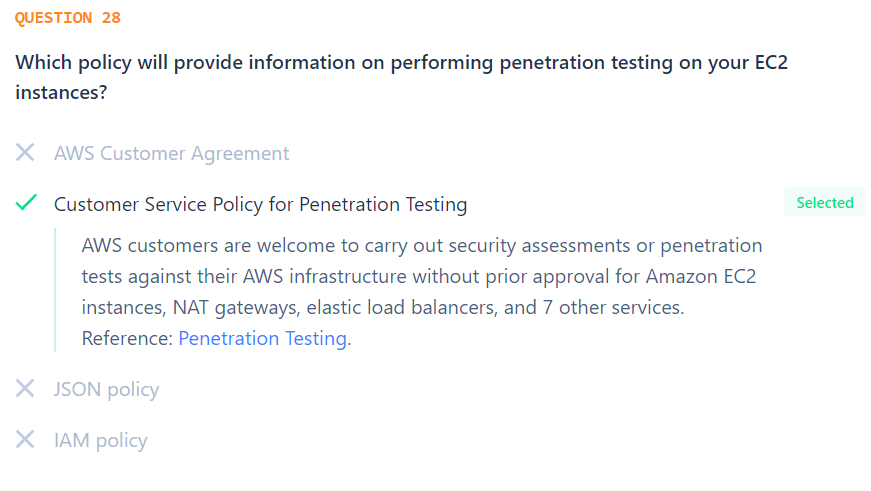
Temporary access- Role

Marked





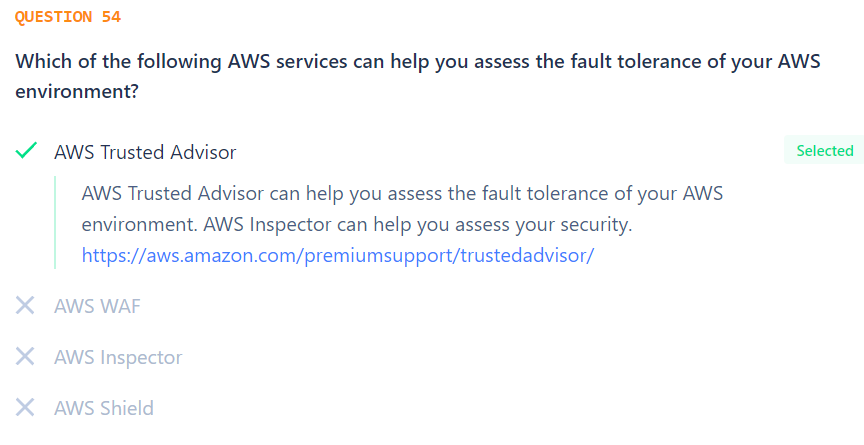




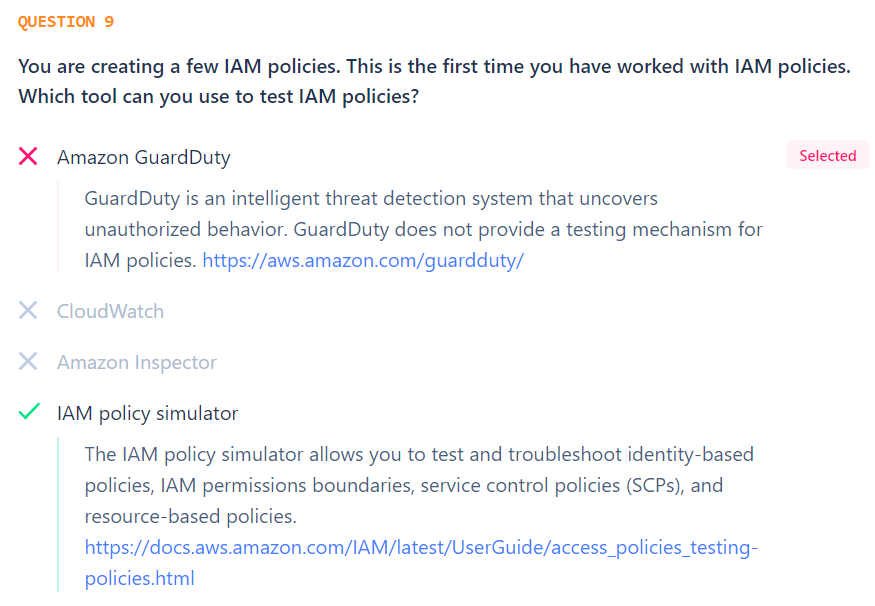


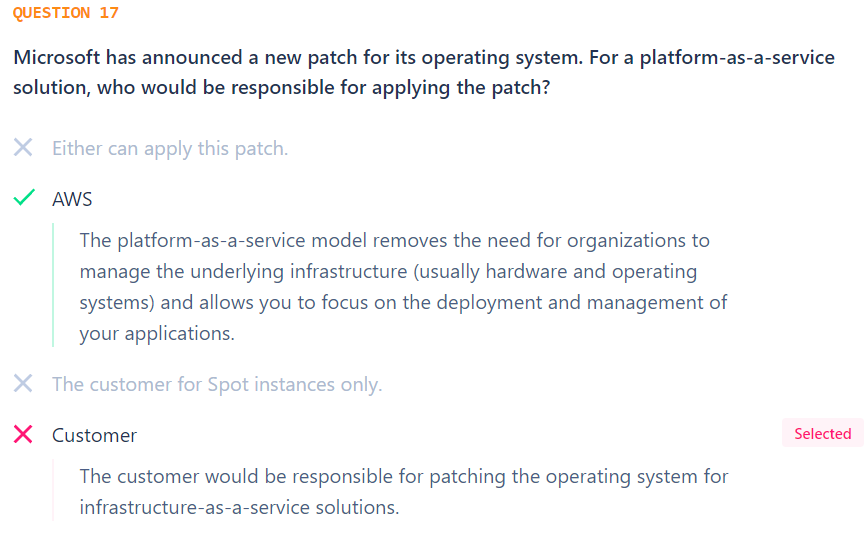


Marked

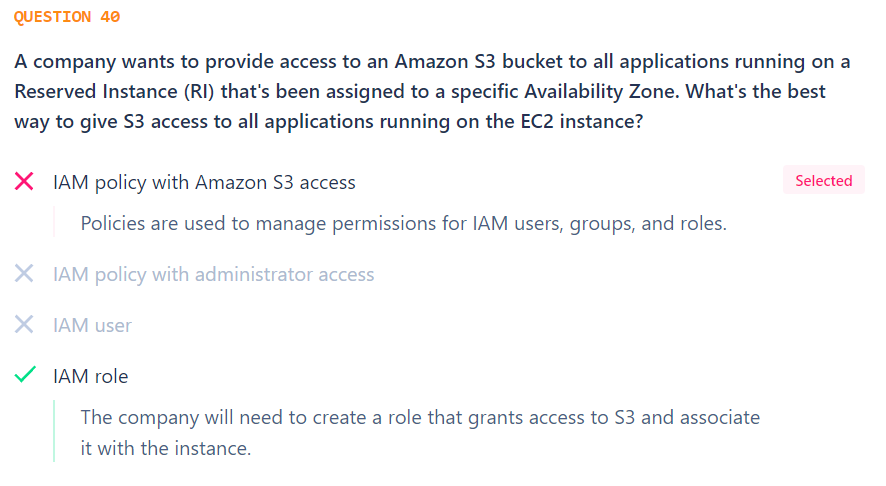








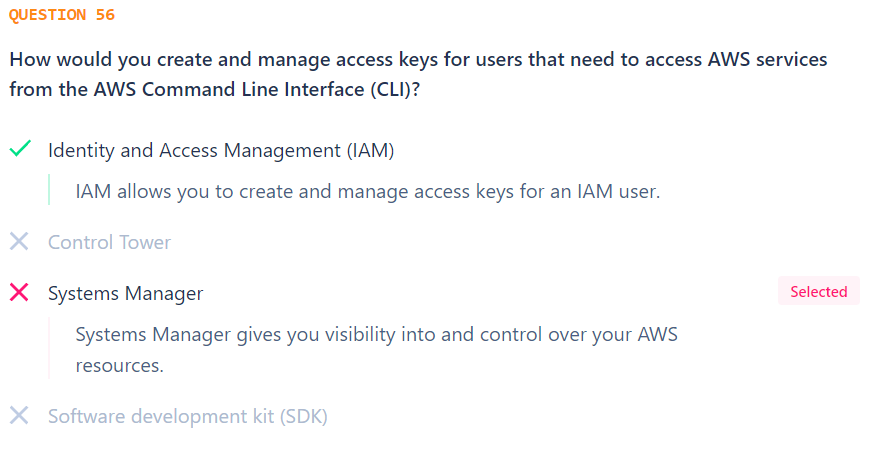
Marked

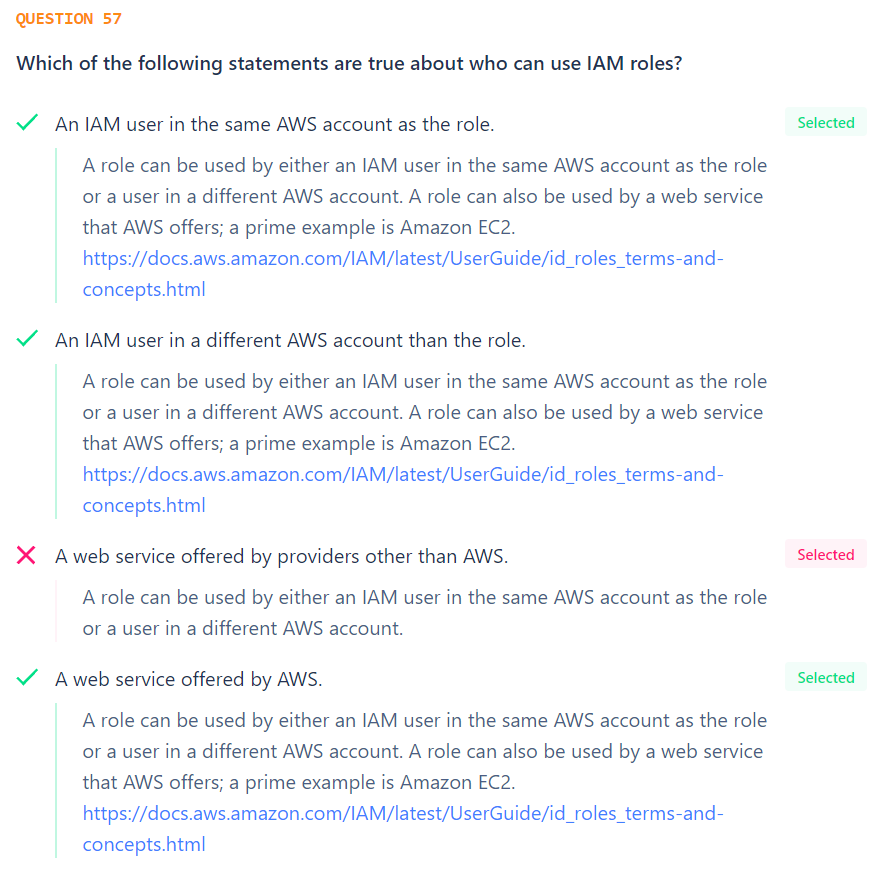


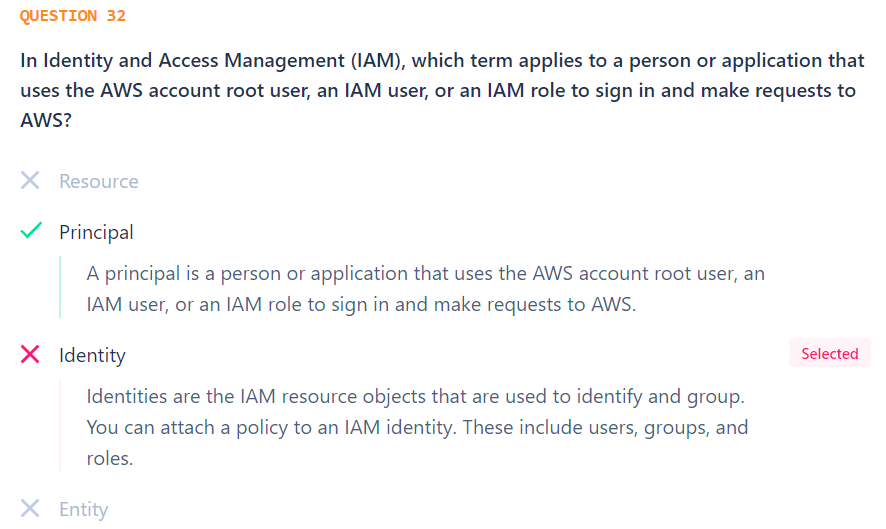
Instance level access- role

User, group, role permission- policy

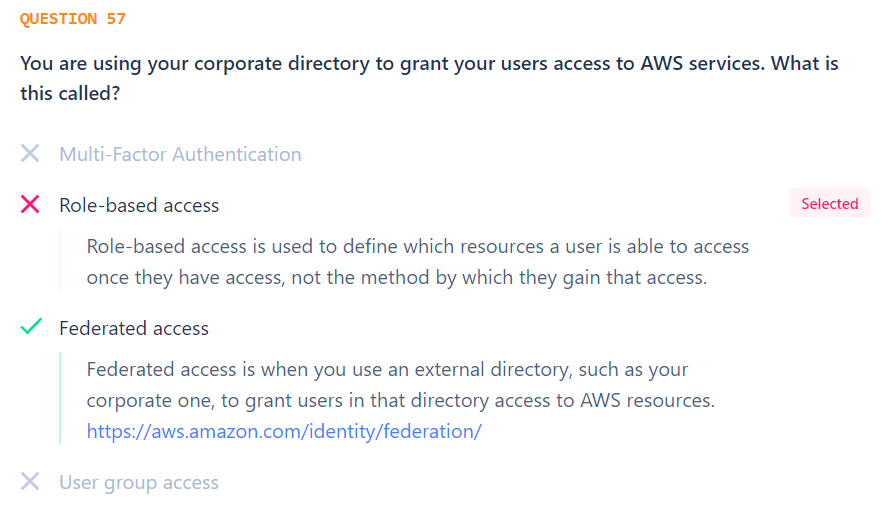
Marked

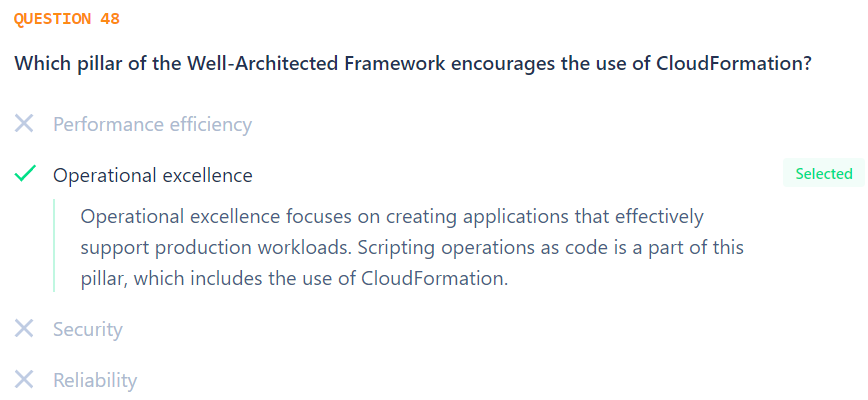




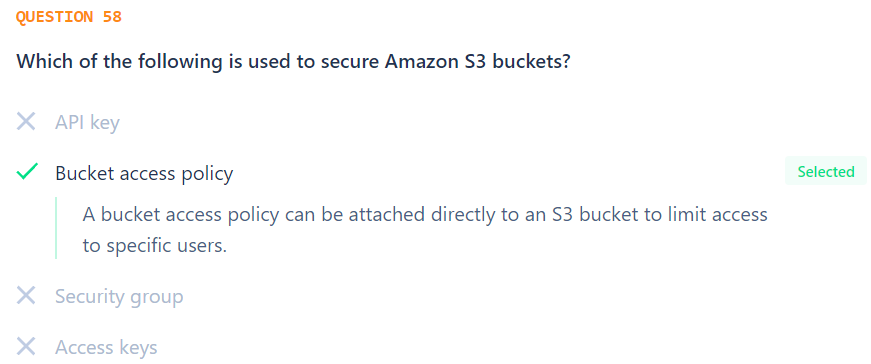


Marked

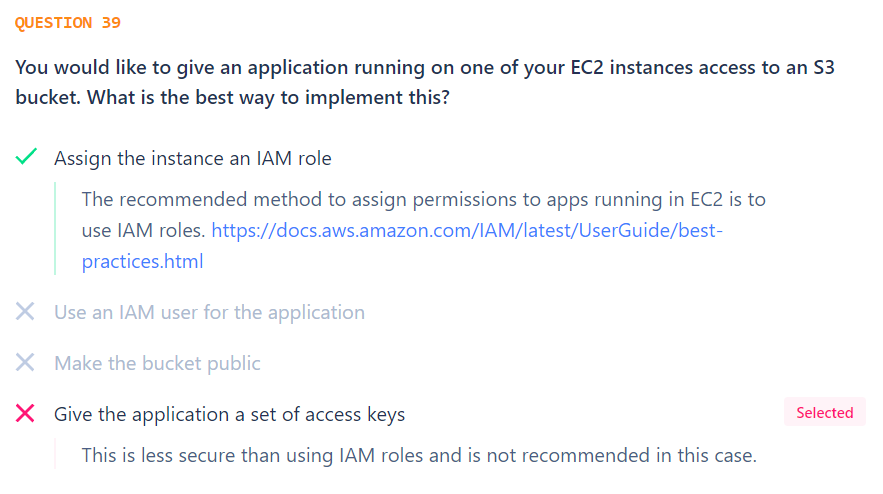




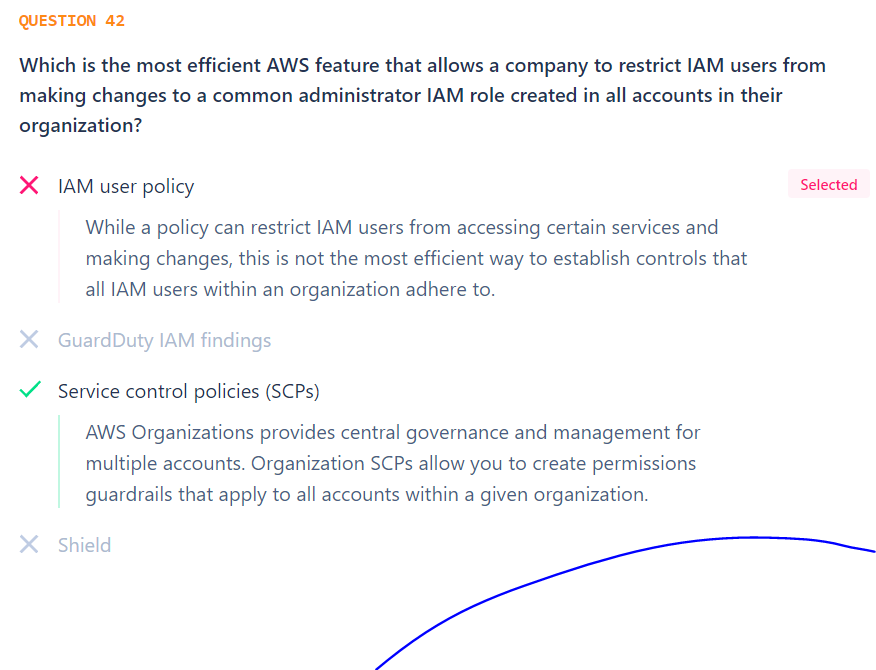
Marked

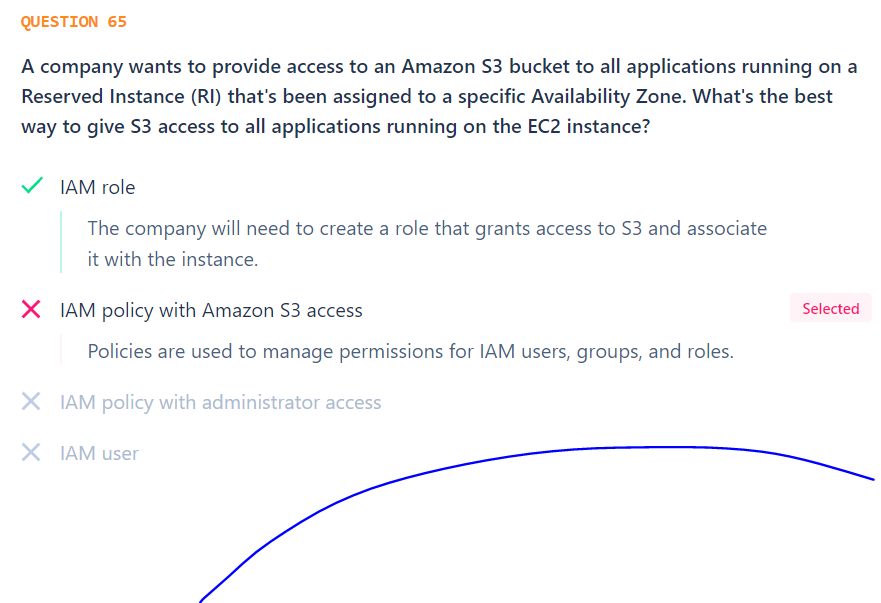


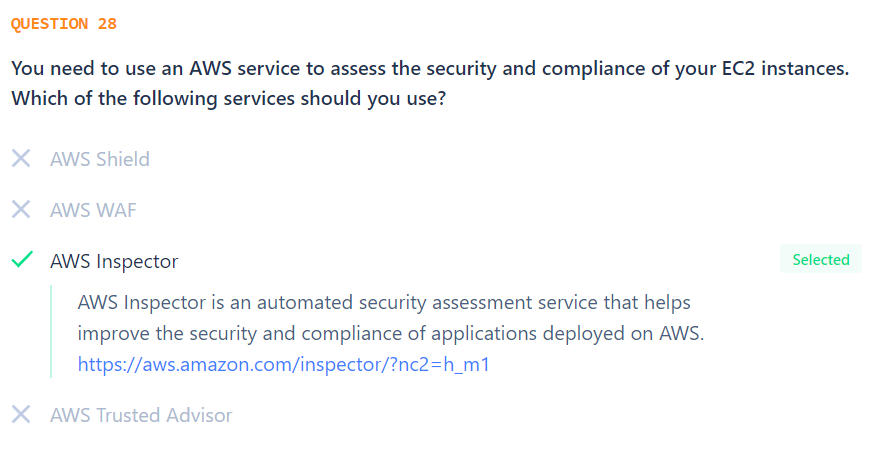
Marked



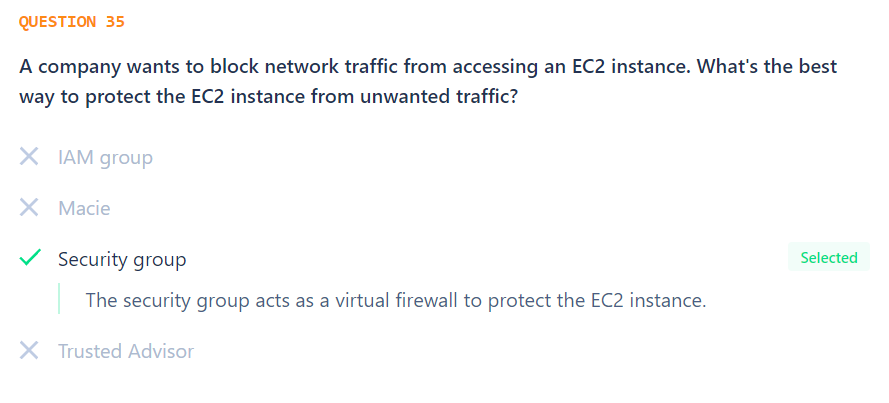
Marked

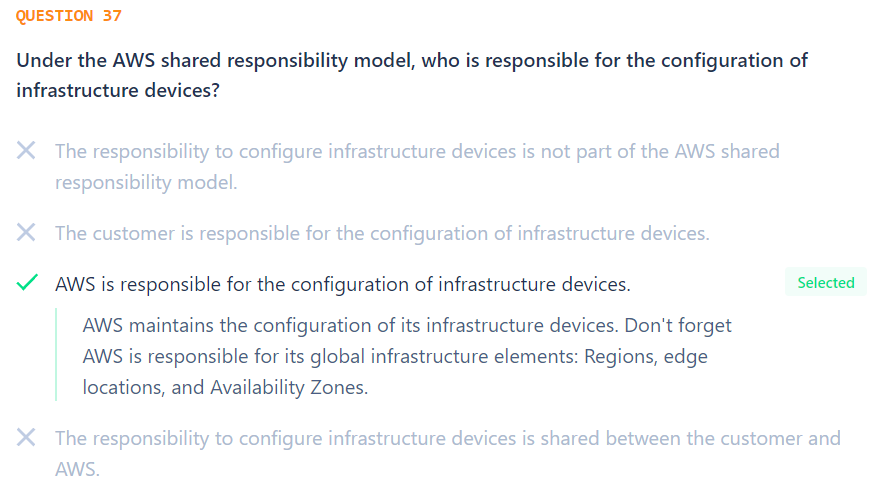






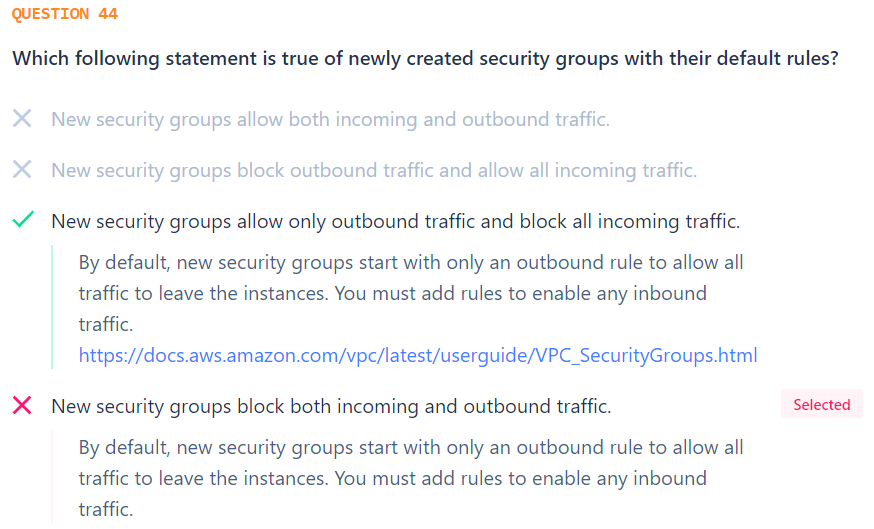
Marked



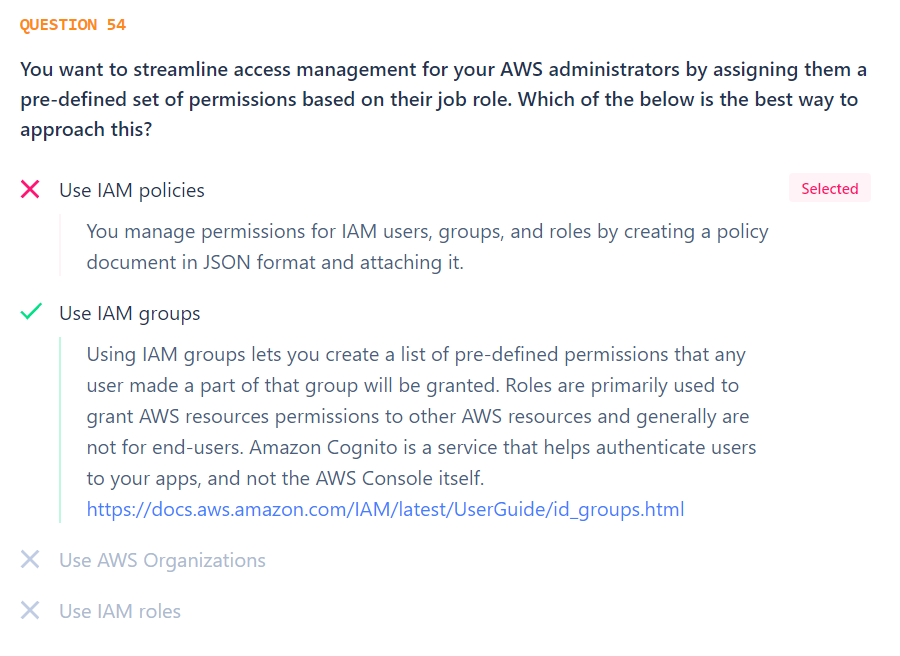


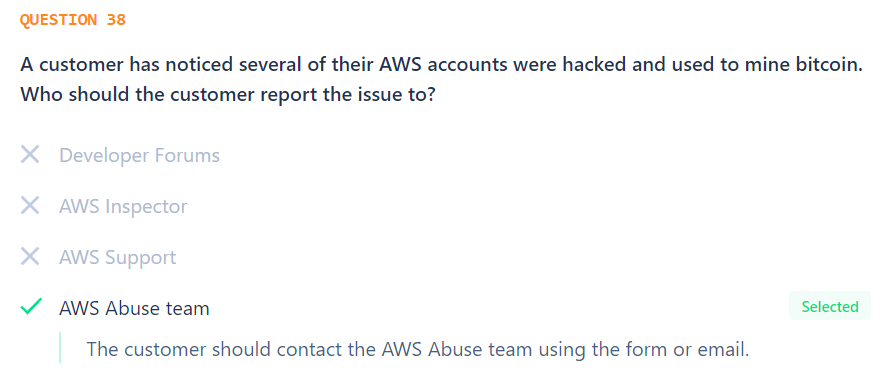
Marked

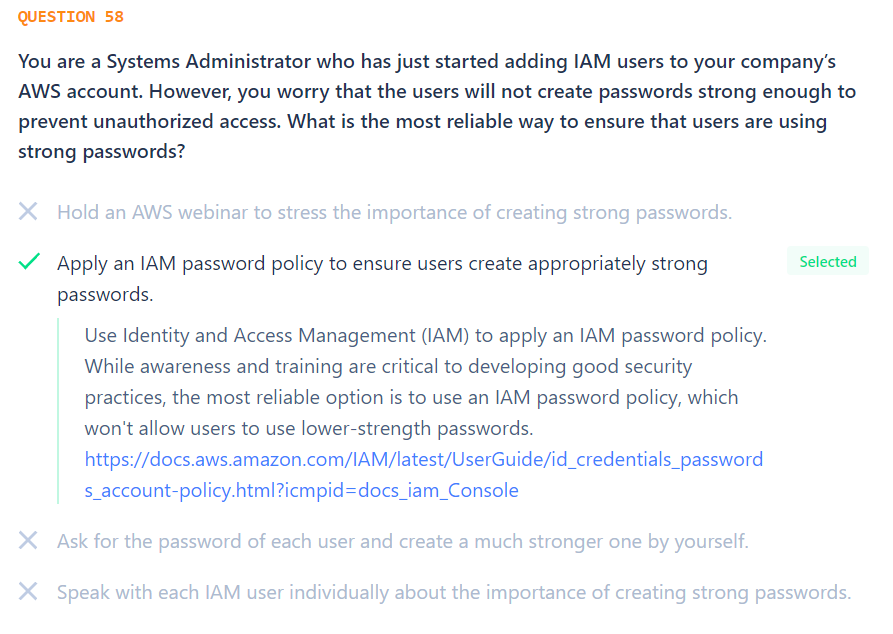




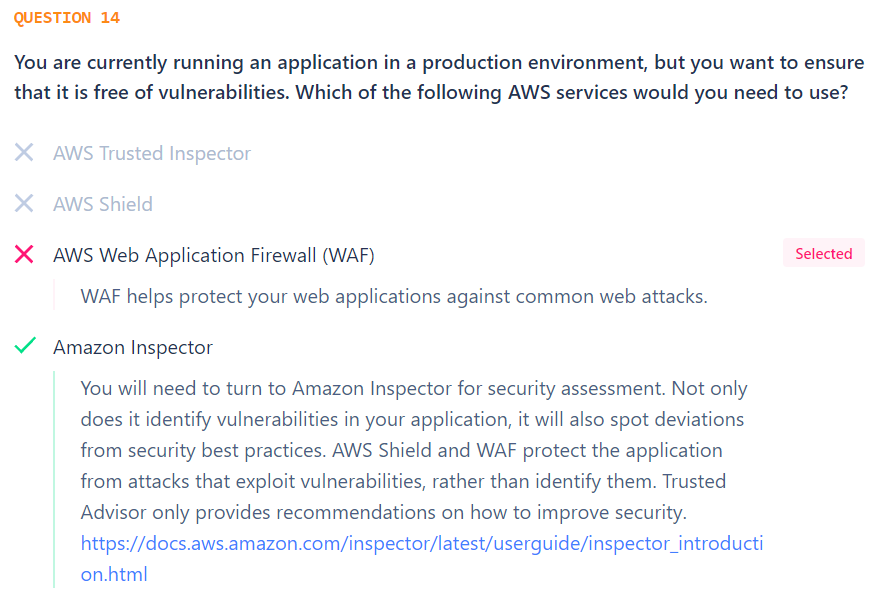
Marked



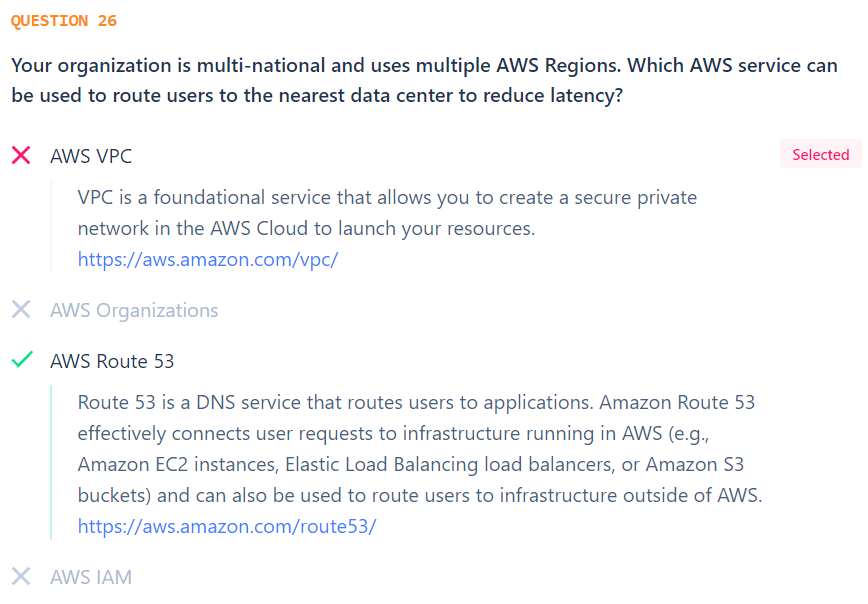


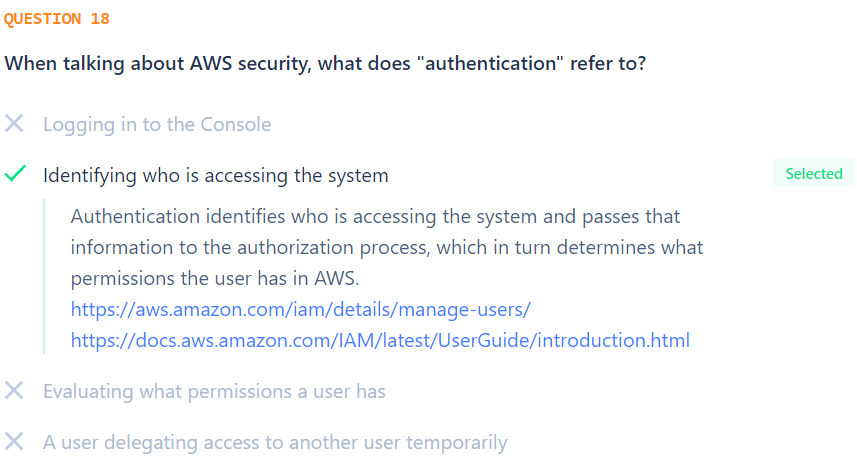


Marked



Marked





Marked

