Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

AWS-CSS Dumps
AWS-CSS Braindumps
AWS-CSS Real Questions
AWS-CSS Practice Test
AWS-CSS Actual Questions

PASS

Amazon

AWS-CSS

AWS Certified Security - Specialty ((SCS-C01)

QUESTION 58
A company has deployed a custom DNS server in AWS. The Security Engineer wants to ensure that Amazon EC2 instances cannot use the Amazon-provided DNS.

How can the Security Engineer block access to the Amazon-provided DNS in the VPC?

A. Deny access to the Amazon DNS IP within all security groups.
B. Add a rule to all network access control lists that deny access to the Amazon DNS IP.
C. Add a route to all route tables that black holes traffic to the Amazon DNS IP.
D. Disable DNS resolution within the VPC configuration.

Answer: D

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html

QUESTION 59
An employee accidentally exposed an AWS access key and secret access key during a public presentation. The company Security Engineer immediately disabled the key. How

can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

A. Analyze AWS CloudTrail for activity.
B. Analyze Amazon CloudWatch Logs for activity.
C. Download and analyze the IAM Use report from AWS Trusted Advisor.
D. Analyze the resource inventory in AWS Config for IAM user activity.
E. Download and analyze a credential report from IAM.

Answer: AE

QUESTION 60 Which of the following minimizes the potential attack surface
for applications?

A. Use security groups to provide stateful firewalls for Amazon EC2 instances at the hypervisor level.
B. Use network ACLs to provide stateful firewalls at the VPC level to prevent access to any specific AWS resource.
C. Use AWS Direct Connect for secure trusted connections between EC2 instances within private subnets.
D. Design network security in a single layer within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet) to facilitate quicker responses to threats.

Answer: B

QUESTION 61
A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.

What would be the BEST way to reduce the potential impact of these attacks in the future?

A. Use custom route tables to prevent malicious traffic from routing to the instances.

B. Update security groups to deny traffic from the originating source IP addresses.
C. Use network ACLs.
D. Install intrusion prevention software (IPS) on each instance.

Answer: C

QUESTION 62
A company plans to move most of its IT infrastructure to AWS. They want to leverage their existing on-premises Active Directory as an identity provider for AWS. Which

combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with AWS? (Choose two.)

A. Create IAM roles with permissions corresponding to each Active Directory group.
B. Create IAM groups with permissions corresponding to each Active Directory group.
C. Configure Amazon Cloud Directory to support a SAML provider.
D. Configure Active Directory to add relying party trust between Active Directory and AWS.
E. Configure Amazon Cognito to add relying party trust between Active Directory and AWS.

Answer: AC

QUESTION 63
A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.

What should the Security Engineer use to isolate and research this event? (Choose three.)

A. AWS CloudTrail
B. Amazon Athena
C. AWS Key Management Service (AWS KMS)
D. VPC Flow Logs
E. AWS Firewall Manager
F. Security groups

Answer: ADF

QUESTION 64
A financial institution has the following security requirements:
▪ Cloud-based users must be contained in a separate authentication domain. ▪ Cloud-
based users cannot access on-premises systems.
As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.

How would the organization manage its resources in the MOST secure manner? (Choose two.)

A. Configure an AWS Managed Microsoft AD to manage the cloud resources.

B. Configure an additional on-premises Active Directory service to manage the cloud resources.
C. Establish a one-way trust relationship from the existing Active Directory to the new Active Directory service.
D. Establish a one-way trust relationship from the new Active Directory to the existing Active Directory service.
E. Establish a two-way trust between the new and existing Active Directory services.

Answer: BC

QUESTION 65
An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the AWS Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.

How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

A. Use a filter in AWS CloudTrail to exclude the IP addresses of the Security team's EC2 instances.
B. Add the Elastic IP addresses of the Security team's EC2 instances to a trusted IP list in Amazon GuardDuty.
C. Install the Amazon Inspector agent on the EC2 instances that the Security team uses.
D. Grant the Security team's EC2 instances a role with permissions to call Amazon GuardDuty API operations.

Answer: C

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit https://killexams.com/vendors-exam-list
Kill your exam at First Attempt....Guaranteed!