Amazon

SCS-C01 Exam

Amazon AWS Certified Security - Specialty Exam

Thank you for Downloading SCS-C01 exam PDF Demo

You can Buy Latest SCS-C01 Full Version Download

https://www.certkillers.net/Exam/SCS-C01

Version: 21.0

Question: 1

A global company that deals with International finance is investing heavily in cryptocurrencies and wants to experiment with mining technologies using AWS. The company's security team has enabled Amazon GuardDuty and is concerned by the number of findings being generated by the accounts. The security team wants to minimize the possibility of GuardDuty finding false negatives for compromised instances that are performing mining
How can the security team continue using GuardDuty while meeting these requirements?

A. In the GuardDuty console, select the CryptoCurrency:EC2/BitcoinTool B'DNS finding and use the suppress findings option
B. Create a custom AWS Lambda function to process newly detected GuardDuty alerts Process the CryptoCurrency EC2/BitcoinTool BIDNS alert and filter out
the high-severity finding types only.
C. When creating a new Amazon EC2 Instance, provide the instance with a specific tag that indicates it is performing mining operations Create a custom AWS Lambda function to process newly detected GuardDuty alerts and filter for the presence of this tag
D. When GuardDuty produces a cryptocurrency finding, process the finding with a custom AWS Lambda function to extract the instance ID from the finding Then use the AWS Systems Manager Run Command to check for a running process performing mining operations

Answer: A

Question: 2

A security engineer must develop an encryption tool for a company. The company requires a cryptographic solution that supports the ability to perform cryptographic erasure on all resources protected by the key material in 15 minutes or less
Which AWS Key Management Service (AWS KMS) key solution will allow the security engineer to meet these requirements?

A. Use Imported key material with CMK
B. Use an AWS KMS CMK
C. Use an AWS managed CMK.
D. Use an AWS KMS customer managed CMK

Answer: C

Question: 3

A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running In Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns
Which solution would have the MOST scalability and LOWEST latency?

A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers
D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers

Answer: A

Question: 4

A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in AWS Systems Manager Parameter Store When the application tries to access the secure string key value, it fails
Which factors could be the cause of this failure? (Select TWO.)

A. The EC2 instance role does not have decrypt permissions on the AWS Key Management Sen/ice (AWS KMS) key used to encrypt the secret
B. The EC2 instance role does not have read permissions to read the parameters In Parameter Store
C. Parameter Store does not have permission to use AWS Key Management Service (AWS KMS) to decrypt the parameter
D. The EC2 instance role does not have encrypt permissions on the AWS Key Management Service (AWS KMS) key associated with the secret
E. The EC2 instance does not have any tags associated.

Answer: C, E

Question: 5

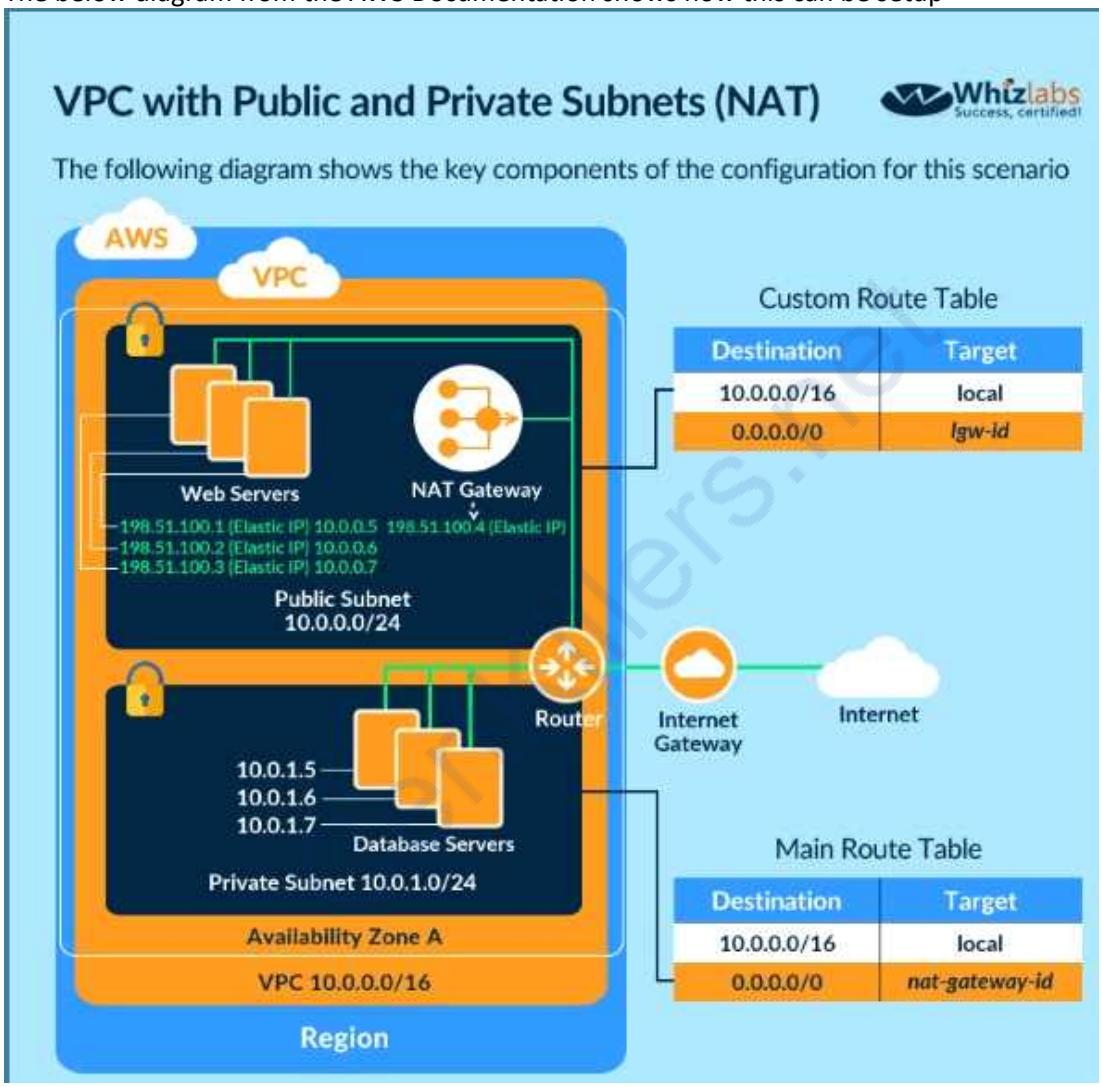
Your current setup in AWS consists of the following architecture. 2 public subnets, one subnet which has the web servers accessed by users across the internet and the other subnet for the database server. Which of the following changes to the architecture would add a better security boundary to the resources hosted in your setup
Please select:

A. Consider moving the web server to a private subnet
B. Consider moving the database server to a private subnet
C. Consider moving both the web and database server to a private subnet

D. Consider creating a private subnet and adding a NAT instance to that subnet

Answer: B

Explanation:
The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet.
The below diagram from the AWS Documentation shows how this can be setup



Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users Option D is invalid because NAT instances should be present in the public subnet
For more information on public and private subnets in AWS, please visit the following url .com/AmazonVPC/latest/UserGuide/VPC Scenario2.
The correct answer is: Consider moving the database server to a private subnet Submit your Feedback/Queries to our Experts

Question: 6

A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.
Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data
Which solution will meet these requirements?

A. Use AWS Secrets Manager and an AWS SDK to create a unique secret for the customer-specific data
B. Use AWS Key Management Service (AWS KMS) and the AWS Encryption SDK to generate and store a data encryption key for each customer.
C. Use AWS Key Management Service (AWS KMS) with service-managed keys to generate and store customer-specific data encryption keys
D. Use AWS Key Management Service (AWS KMS) and create an AWS CloudHSM custom key store Use CloudHSM to generate and store a new CMK for each customer.

Answer: A

Question: 7

A security engineer has created an Amazon Cognito user pool. The engineer needs to manually verify the ID and access token sent by the application for troubleshooting purposes
What is the MOST secure way to accomplish this?

A. Extract the subject (sub), audience (aud), and cognito:username from the ID token payload Manually check the subject and audience for the user name In the user pool
B. Search for the public key with a key ID that matches the key ID In the header of the token. Then use a JSON Web Token (JWT) library to validate the signature of the token and extract values, such as the expiry date
C. Verify that the token is not expired. Then use the token_use claim function In Amazon Cognito to validate the key IDs
D. Copy the JSON Web Token (JWT) as a JSON document Obtain the public JSON Web Key (JWK) and convert It to a pem file. Then use the file to validate the original JWT.

Answer: A

Question: 8

A security engineer must use AWS Key Management Service (AWS KMS) to design a key

management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive dat
a. The solution needs to ensure that the key material automatically expires in 90 days.
Which solution meets these criteria?
A. A customer managed CMK that uses customer provided key material
B. A customer managed CMK that uses AWS provided key material
C. An AWS managed CMK
D. Operating system-native encryption that uses GnuPG

Answer: B

Question: 9

A Security Engineer discovered a vulnerability in an application running on Amazon ECS. The vulnerability allowed attackers to install malicious code. Analysis of the code shows it exfiltrates data on port 5353 in batches at random time intervals.
While the code of the containers is being patched, how can Engineers quickly identify all compromised hosts and stop the egress of data on port 5353?

A. Enable AWS Shield Advanced and AWS WAF. Configure an AWS WAF custom filter for egress traffic on port 5353
B. Enable Amazon Inspector on Amazon ECS and configure a custom assessment to evaluate containers that have port 5353 open. Update the NACLs to block port 5353 outbound.
C. Create an Amazon CloudWatch custom metric on the VPC Flow Logs identifying egress traffic on port 5353. Update the NACLs to block port 5353 outbound.
D. Use Amazon Athena to query AWS CloudTrail logs in Amazon S3 and look for any traffic on port 5353. Update the security groups to block port 5353 outbound.

Answer: C

Question: 10

A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application A Security Engineer Has been asked to review the security controls for authentication and authorization of the application
Which combination of actions would provide the MOST secure solution? (Select TWO)

A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway Attach the policy to the role used by the legacy EC2 instances
B. Enable AWS WAF for API Gateway Configure rules to explicitly allow connections from the legacy EC2 instances
C. Create a VPC endpoint for API Gateway Attach an IAM resource policy that allows the role of the legacy EC2 instances to call specific APIs
D. Create a usage plan Generate a set of API keys for each application that needs to call the API.

E. Configure cross-origin resource sharing (CORS) in each API Share the CORS information with the applications that call the API.

Answer: A, E

Thank You for trying SCS-C01 PDF Demo

To Buy Latest SCS-C01 Full Version Download visit link below

https://www.certkillers.net/Exam/SCS-C01

Start Your SCS-C01 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your SCS-C01 preparation with actual exam questions.