SCS-C01 Q&As

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/aws-certified-security-specialty.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company hosts business-critical applications on Amazon EC2 instances in a VPC. The VPC uses default DHCP options sets. A security engineer needs to log all DNS queries that internal resources make in the VPC. The security engineer also must create a list of the most common DNS queries over time.

Which solution will meet these requirements?

A. Install the Amazon CloudWatch agent on each EC2 instance in the VPC. Use the CloudWatch agent to stream the DNS query logs to an Amazon CloudWatch Logs log group. Use CloudWatch metric filters to automatically generate metrics that list the most common DNS queries.

B. Install a BIND DNS server in the VPC. Create a bash script to list the DNS request number of common DNS queries from the BIND logs.

C. Create VPC flow logs for all subnets in the VPC. Stream the flow logs to an Amazon CloudWatch Logs log group. Use CloudWatch Logs Insights to list the most common DNS queries for the log group in a custom dashboard.

D. Configure Amazon Route 53 Resolver query logging. Add an Amazon CloudWatch Logs log group as the destination. Use Amazon CloudWatch Contributor Insights to analyze the data and create time series that display the most common DNS queries.

Correct Answer: D

QUESTION 2

A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.

What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

A. Store the scripts in the AMI and encrypt the sensitive data using AWS KMS Use the instance role profile to control access to the KMS keys needed to decrypt the data.

B. Store the sensitive data in AWS Systems Manager Parameter Store using the encrypted string parameter and assign the GetParameters permission to the EC2 instance role.

C. Externalize the bootstrap scripts in Amazon S3 and encrypt them using AWS KMS.Remove the scripts from the instance and clear the logs after the instance is configured.

D. Block user access of the EC2 instance\\'s metadata service using IAM policies. Remove all scripts and clear the logs after execution.

Correct Answer: B

QUESTION 3

Two Amazon EC2 instances in different subnets should be able to connect to each other but cannot. It has been confirmed that other hosts in the same subnets are able to communicate successfully, and that security groups have

valid ALLOW rules in place to permit this traffic.

Which of the following troubleshooting steps should be performed?

A. Check inbound and outbound security groups, looking for DENY rules.

B. Check inbound and outbound Network ACL rules, looking for DENY rules.

C. Review the rejected packet reason codes in the VPC Flow Logs.

D. Use AWS X-Ray to trace the end-to-end application flow

Correct Answer: C

QUESTION 4

A Security Engineer must design a system that can detect whether a file on an Amazon EC2 host has been modified. The system must then alert the Security Engineer of the modification. What is the MOST efficient way to meet these requirements?

A. Install antivirus software and ensure that signatures are up-to-date. Configure Amazon CloudWatch alarms to send alerts for security events.

B. Install host-based IDS software to check for file integrity. Export the logs to Amazon CloudWatch Logs for monitoring and alerting.

C. Export system log files to Amazon S3. Parse the log files using an AWS Lambda function that will send alerts of any unauthorized system login attempts through Amazon SNS.

D. Use Amazon CloudWatch Logs to detect file system changes. If a change is detected, automatically terminate and recreate the instance from the most recent AMI. Use Amazon SNS to send notification of the event.

Correct Answer: B

QUESTION 5

A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.

Which solution will meet these requirements with the LEAST operational overhead?

A. Configure the S3 Block Public Access feature for the AWS account.

B. Configure the S3 Block Public Access feature for all objects that are in the bucket.

C. Deactivate ACLs for objects that are in the bucket.

D. Use AWS PrivateLink for Amazon S3 to access the bucket.

Correct Answer: D

SCS-C01 Practice Test SCS-C01 Study Guide SCS-C01 Braindumps