Download Free Amazon SCS-C03 Exam PDF | PrepBolt

Don't miss out! Download the latest free Amazon AWS Certified Security - Specialty exam PDF questions. Access real SCS-C03 dumps with verified answers and boost your chances to pass your certification on the first try with PrepBolt SCS-C03 exam pdf questions and answers.

Thank you for Downloading SCS-C03 exam PDF Demo

https://prepbolt.com/SCS-C03.html

QUESTIONS & ANSWERS

DEMO VERSION

(LIMITED CONTENT)

Question 1

Question Type: MultipleChoice

A company runs an internet-accessible application on several Amazon EC2 instances that run Windows Server. The company used an instance profile to configure the EC2 instances. A security team currently accesses the VPC that hosts the EC2 instances by using an AWS Site-to-Site VPN tunnel from an on-premises office. The security team issues a policy that requires all external access to the VPC to be blocked in the event of a security incident. However, during an incident, the security team must be able to access the EC2 instances to obtain forensic information on the instances.

Which solution will meet these requirements?

Options:

A- Install EC2 Instance Connect on the EC2 instances. Update the IAM policy for the IAM role to grant the required permissions. Use the AWS CLI to open a tunnel to connect to the instances.

B- Install EC2 Instance Connect on the EC2 instances. Configure the instances to permit access to the ec2-instance-connect command user. Use the AWS Management Console to connect to the EC2 instances.

C- Create an EC2 Instance Connect endpoint in the VPC. Configure an appropriate security group to allow access between the EC2 instances and the endpoint. Use the AWS CLI to open a tunnel to connect to the instances.

D- Create an EC2 Instance Connect endpoint in the VPC. Configure an appropriate security group to allow access between the EC2 instances and the endpoint. Use the AWS Management Console to connect to the EC2 instances.

Answer:

D

Explanation:

During an incident, the company wants to block ''external access to the VPC'' (for example, shutting down VPN ingress or internet-exposed paths) yet still allow the security team to access instances for forensics. AnEC2 Instance Connect Endpoint (EIC Endpoint)provides a managed, private connectivity path that lets authorized users connect to instances in a VPCwithout requiring inbound access from the internet or from on-premises. The endpoint lives inside the VPC, and access is controlled by IAM permissions plus security group rules between the endpoint and the instances. This supports incident containment (no external network entry) while preserving controlled administrative access for investigation.

Options A and B require installing Instance Connect on the instances and typically rely on network reachability patterns that may be blocked when external access is cut off; they also do not provide the same VPC-resident endpoint model. With an EIC endpoint, the security team can use theAWS Management Consoleto initiate connections (Option D) even while the VPC is isolated from on-prem and the public internet, because the connectivity is mediated through AWS control plane and the endpoint inside the VPC.

Option C mentions using the CLI to open a tunnel, but the most straightforward and commonly used operational method for responders is console-based access via the EIC endpoint. Therefore, creating an Instance Connect Endpoint and using the console meets the requirement.

Question 2

Question Type: MultipleChoice

A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally. A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data. All logs must be kept for a minimum of 1 year for auditing purposes.

What should the security engineer recommend?

Options:

A- Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is created. When the instance is terminated, the EBS volume can be reattached to another instance for log review.
B- Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation. Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.
C- Add an Amazon CloudWatch agent into the AMI used in the Auto Scaling group. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.
D- Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer:

C

Explanation:

In an Auto Scaling group, instances are ephemeral---local disks and instance-level log files can disappear during scale-in or replacement. The most durable, operationally simple pattern is tostream logs off-host continuouslyto a managed log service. Installing and configuring theCloudWatch agent(or unified agent) to ship application logs toAmazon CloudWatch Logsensures logs are centralized and remain available regardless of instance lifecycle events. This directly solves the ''logs lost after scale-in'' problem and provides high availability for audit and investigation.

CloudWatch Logs also supports retention controls. The security engineer can set the log group retention toat least 1 year(or longer), meeting the audit requirement without building custom storage workflows. Access can be controlled with IAM to restrict who can view or export logs, and CloudWatch logs can be further integrated with Athena/OpenSearch/SIEM tools if needed.

Option A adds complexity and still ties durability to managing volumes across instance churn, with operational risk and scaling challenges. Option B requires daily copy jobs and can still lose logs between copy intervals; it also adds shared filesystem management overhead. Option D is manual and does not ensure durability, and it introduces operational friction during scale-in. Therefore, centralized log shipping to CloudWatch Logs is the best recommendation.

Question 3

Question Type: MultipleChoice

A company needs a solution to protect critical data from being permanently deleted. The data is stored in Amazon S3 buckets. The company needs to replicate the S3 objects from the company's primary AWS Region to a secondary Region to meet disaster recovery requirements. The company must also ensure that users who have administrator access cannot permanently delete the data in the secondary Region.

Which solution will meet these requirements?

Options:

A- Configure AWS Backup to perform cross-Region S3 backups. Select a backup vault in the secondary Region. Enable AWS Backup Vault Lock in governance mode for the backups in the secondary Region.
B- Implement S3 Object Lock in compliance mode in the primary Region. Configure S3 replication to replicate the objects to an S3 bucket in the secondary Region.
C- Configure S3 replication to replicate the objects to an S3 bucket in the secondary Region. Create an S3 bucket policy to deny the s3:ReplicateDelete action on the S3 bucket in the secondary Region.
D- Configure S3 replication to replicate the objects to an S3 bucket in the secondary Region. Configure S3 object versioning on the S3 bucket in the secondary Region.

Answer:

B

Explanation:

The requirement is twofold:cross-Region replicationfor disaster recovery andimmutabilityso that even administrators cannot permanently delete data in the secondary Region. The S3-native feature designed to prevent deletion (including version deletion) for a defined retention period isS3 Object Lock. When Object Lock is configured incompliance mode,no user, including the root user and administrators, can remove Object Lock protections or permanently delete protected object versions before retention expires. This meets the ''admins cannot permanently delete'' requirement far better than policy-based controls.

To replicate the data for DR, the company can configureS3 replicationfrom the primary Region bucket to a bucket in the secondary Region. With Object Lock in place (and the destination bucket appropriately configured to support Object Lock and versioning), replicated objects can be retained immutably, providing a strongly protected copy for recovery.

Option D (versioning alone) prevents accidental overwrites but does not stop an admin from deleting all versions. Option C only blocks replication deletes; it does not prevent an admin from deleting objects directly in the secondary bucket. Option A uses AWS Backup vault lock ingovernancemode, which still allows privileged users with special permissions to override retention; it also creates backups rather than true object-level replication. Therefore, Object Lock in compliance mode combined with replication is the best match.

Question 4

Question Type: MultipleChoice

A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon Route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon RDS cluster. A recent report suggests this software platform is vulnerable to SQL injection attacks, with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The security engineer's solution must involve the least amount of effort and maintain normal operations during implementation.

What should the security engineer do to meet these requirements?

Options:

A- Create an Application Load Balancer with the existing EC2 instances as a target group. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the ALB. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to

the ALB. Update security groups on the EC2 instances to prevent direct access from the internet.
B- Create an Amazon CloudFront distribution specifying one EC2 instance as an origin. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the distribution. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to CloudFront.
C- Obtain the latest source code for the platform and make the necessary updates. Test the updated code to ensure that the vulnerability has been mitigated, then deploy the patched version of the platform to the EC2 instances.
D- Update the security group that is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the EC2 instances. Test to ensure the vulnerability has been mitigated, then restore the security group to the original setting.

Answer:

A

Explanation:

The fastest, least-effort way to mitigate SQL injection at the edge---without modifying legacy application code---is to place the application behind a component that supportsAWS WAFand applymanaged SQL injection protections. AnApplication Load Balancerintegrates directly with AWS WAF, allowing the security engineer to deploy a web ACL (including AWS Managed Rules for SQL injection and custom patterns based on the provided samples) and immediately start blocking malicious payloads before they reach the EC2 instances and the database.

Option A also preserves normal operations during rollout: you can create the ALB, register the existing EC2 instances as targets, validate health checks and traffic behavior, apply WAF protections, and then shift Route 53 weighted records to the ALB with minimal downtime. Finally, tightening the EC2 security groups to prevent direct internet access ensures all inbound web traffic is forced through the ALB + WAF inspection point, reducing exposure quickly.

Option B is risky because it uses only one EC2 origin (reducing availability) and adds CloudFront origin configuration complexity under a 24-hour deadline. Option C requires code changes on unsupported software and is unlikely to be safely delivered in time. Option D is invalid because AWS WAF cannot be attached directly to EC2 instances, and changing DB-port exposure doesn't address SQL injection on the web layer.

Question 5

Question Type: MultipleChoice

A development team is creating an open source toolset to manage a company's software as a service (SaaS) application. The company stores the code in a public repository so that anyone can view and download the toolset's code. The company discovers that the code contains an IAM access key and secret key that provide access to internal resources in the company's AWS environment. A security engineer must implement a solution to identify whether unauthorized usage of the exposed credentials has occurred. The solution also must prevent any additional usage of the exposed credentials.

Which combination of steps will meet these requirements? (Select TWO.)

Options:

A- Use AWS Identity and Access Management Access Analyzer to determine which resources the exposed credentials accessed and who used them.
B- Deactivate the exposed IAM access key from the user's IAM account.
C- Create a rule in Amazon GuardDuty to block the access key in the source code from being used.
D- Create a new IAM access key and secret key for the user whose credentials were exposed.
E- Generate an IAM credential report. Check the report to determine when the user that owns the access key last logged in.

Answer:

B, E

Explanation:

The immediate containment step for exposed access keys is todisable (deactivate) the compromised IAM access key(Option B). This prevents any further use of the leaked credentials, which is essential once secrets are publicly exposed. Creating a new key (Option D) may be part of recovery later, but it does not stop abuse of the already exposed key unless the exposed key is first deactivated.

To determine whether the credentials were used, you need evidence of access activity. Among the provided options, the best fit is generating and reviewing theIAM credential report(Option E). The report includes metadata such as access key status and ''last used'' style details that help triage whether the user's credentials have been exercised recently. While deeper investigation would typically rely on CloudTrail ''AccessKeyId'' searches, the credential report is a quick AWS-native step aligned to the answer choices.

Option A is not correct: IAM Access Analyzer helps identify external access paths to resources and validate policies; it does not provide a definitive history of what a specific access key did. Option C is not a GuardDuty capability---GuardDuty generates findings; it does not ''block'' a specific access key. Therefore, deactivating the key and using credential reporting to assess recent usage best matches the requirements.

Question 6

Question Type: MultipleChoice

A corporate cloud security policy states that communications between the company's VPC and KMS must travel entirely within the AWS network and not use public service endpoints.

Which combination of the following actions MOST satisfies this requirement? (Select TWO.)

Options:

A- Add theaws:sourceVpcecondition to the AWS KMS key policy referencing the company's VPC endpoint ID.

B- Remove the VPC internet gateway from the VPC and add a virtual private gateway to the VPC to prevent direct, public internet connectivity.

C- Create a VPC endpoint for AWS KMS withprivate DNS enabled.

D- Use the KMS Import Key feature to securely transfer the AWS KMS key over a VPN.

E- Add the following condition to the AWS KMS key policy:'aws:SourceIp': '10.0.0.0/16'.

Answer:

A, C

Explanation:

To ensure traffic from a VPC to AWS KMS stays on the AWS network and does not use public endpoints, you should use aninterface VPC endpoint (AWS PrivateLink) for KMS. Creating aVPC endpoint for KMS with private DNS enabled(Option C) causes standard KMS DNS names (for example, kms.<region>.amazonaws.com) to resolve to theprivateendpoint IPs inside the VPC, routing requests over the AWS private network rather than through the internet. This is the core networking control that satisfies ''no public service endpoints.''

To enforce that only calls that come through the intended VPC endpoint can use the key, add an authorization guardrail in theKMS key policyusing the aws:sourceVpce condition (Option A). This ensures that even if a principal has credentials, KMS will deny usage unless the request is made via the specified VPC endpoint, preventing accidental or malicious use over public paths.

Option B is neither necessary nor sufficient: removing an internet gateway does not prevent all public endpoint use (NAT, other egress paths, or other VPCs could still be involved) and can break workloads. Option D is unrelated to runtime KMS API traffic. Option E is weaker because SourceIp checks can be bypassed via other AWS network paths and does not guarantee PrivateLink usage the way sourceVpce does.

Question 7

Question Type: MultipleChoice

A company is running its application on AWS. The company has a multi-environment setup, and each environment is isolated in a separate AWS account. The company has an organization in AWS Organizations to manage the accounts. There is a single dedicated security account for the organization. The company must create an inventory of all sensitive data that is stored in Amazon S3 buckets across the organization's accounts. The findings must be visible from a single location.

Which solution will meet these requirements?

Options:

A- Set the security account as the delegated administrator for Amazon Macie and AWS Security Hub. Enable and configure Macie to publish sensitive data findings to Security Hub.
B- Set the security account as the delegated administrator for AWS Security Hub. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive data. Publish sensitive data findings to Security Hub.
C- In each account, configure Amazon Inspector to scan the S3 buckets for sensitive data. Enable Amazon Inspector integration with AWS Trusted Advisor. Publish sensitive data findings to Trusted Advisor.
D- In each account, enable and configure Amazon Macie to detect sensitive data. Enable Macie integration with AWS Trusted Advisor. Publish sensitive data findings to Trusted Advisor.

Answer:

A

Explanation:

AmazonMacieis the AWS service purpose-built todiscover and classify sensitive data in S3(PII, financial data, credentials, etc.) and produce findings that can be aggregated centrally. In a multi-account organization, the recommended centralized model is to designate adelegated administrator accountfor Macie so the security team can manage discovery across member accounts from one place.

To make the findings visible from a single location and integrate them with broader security visibility,AWS Security Hubprovides centralized aggregation of security findings across accounts and services. By also configuring the security account as thedelegated administrator for Security Hub, the company can aggregate findings across the organization. Macie integrates with Security Hub so that sensitive data discovery findings flow into Security Hub's centralized view, giving the security team a single console and API surface to build an ''inventory'' of sensitive data locations and severity.

Inspector (options B and C) is focused on vulnerability management (EC2, ECR, and related scanning use cases), not sensitive data classification in S3. Trusted Advisor is not the primary destination for sensitive data discovery findings at organizational scale. Therefore, Macie + Security Hub with delegated administration in the security account is the correct solution.