Free Questions for SCS-C02 by certsinside

Shared by Carter on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company runs workloads in the us-east-1 Region. The company has never deployed resources to other AWS Regions and does not have any multi-Region resources.

The company needs to replicate its workloads and infrastructure to the us-west-1 Region.

A security engineer must implement a solution that uses AWS Secrets Manager to store secrets in both Regions. The solution must use AWS Key Management Service (AWS KMS) to encrypt the secrets. The solution must minimize latency and must be able to work if only one Region is available.

The security engineer uses Secrets Manager to create the secrets in us-east-1.

What should the security engineer do next to meet the requirements?

Options:

A- Encrypt the secrets in us-east-1 by using an AWS managed KMS key. Replicate the secrets to us-west-1. Encrypt the secrets in us-west-1 by using a new AWS managed KMS key in us-west-1.

B- Encrypt the secrets in us-east-1 by using an AWS managed KMS key. Configure resources in us-west-1 to call the Secrets Manager endpoint in us-east-1.

C- Encrypt the secrets in us-east-1 by using a customer managed KMS key. Configure resources in us-west-1 to call the Secrets

Manager endpoint in us-east-1.

D- Encrypt the secrets in us-east-1 by using a customer managed KMS key. Replicate the secrets to us-west-1. Encrypt the secrets in us-west-1 by using the customer managed KMS key from us-east-1.

Answer:

D

Explanation:

To ensure minimal latency and regional availability of secrets, encrypting secrets in us-east-1 with a customer-managed KMS key and then replicating them to us-west-1 for encryption with the same key is the optimal approach. This method leverages customer-managed KMS keys for enhanced control and ensures that secrets are available in both regions, adhering to disaster recovery principles and minimizing latency by using regional endpoints.

Question 2

Question Type: **MultipleChoice**

A company uses HTTP Live Streaming (HL'S) to stream live video content to paying subscribers by using Amazon CloudFront. HLS splits the video content into chunks so that the user can request the right chunk based on different conditions. Because the video events

last for several hours, the total video is made up of thousands of chunks.

The origin URL is not disclosed, and every user is forced to access the CloudFront URL. The company has a web application that authenticates the paying users against an internal repository and a CloudFront key pair that is already issued.

What is the simplest and MOST effective way to protect the content?

Options:

A- Develop the application to use the CloudFront key pair to create signed URLs that users will use to access the content.

B- Develop the application to use the CloudFront key pair to set the signed cookies that users will use to access the content.

C- Develop the application to issue a security token that Lambda@Edge will receive to authenticate and authorize access to the content

D- Keep the CloudFront URL encrypted inside the application, and use AWS KMS to resolve the URL on-the-fly after the user is authenticated.

Answer:

B

Explanation:

Utilizing CloudFront signed cookies is the simplest and most effective way to protect HLS video content for paying subscribers. Signed cookies provide access control for multiple files, such as video chunks in HLS streaming, without the need to generate a signed URL for each video chunk. This method simplifies the process for long video events with thousands of chunks, enhancing user experience while

ensuring content protection.

Question 3

Question Type: MultipleChoice

A company is storing data in Amazon S3 Glacier. A security engineer implemented a new vault lock policy for 10 TB of data and called the initiate-vault-lock operation 12 hours ago. The audit team identified a typo in the policy that is allowing unintended access to the vault.

What is the MOST cost-effective way to correct this error?

Options:

A- Call the abort-vault-lock operation. Update the policy. Call the initiate-vault-lock operation again.

B- Copy the vault data to a new S3 bucket. Delete the vault. Create a new vault with the data.

C- Update the policy to keep the vault lock in place

D- Update the policy. Call the initiate-vault-lock operation again to apply the new policy.

Answer:

A

Explanation:

The most cost-effective way to correct a typo in a vault lock policy during the 24-hour initiation period is to call the abort-vault-lock operation. This action stops the vault lock process, allowing the security engineer to correct the policy and re-initiate the vault lock with the corrected policy. This approach avoids the need for data transfer or creating a new vault, thus minimizing costs and operational overhead.

Question 4

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:

Implementing S3 Object Lock in compliance mode on the primary Region and configuring S3 replication to a secondary Region ensures the immutability of S3 objects, preventing them from being deleted or altered. This setup meets the requirement of protecting critical data from permanent deletion, even by users with administrative access. The replicated objects in the secondary Region inherit the Object Lock from the primary, ensuring consistent protection across Regions and aligning with disaster recovery requirements.

Question 5

Question Type: MultipleChoice

A company used AWS Organizations to set up an environment with multiple AWS accounts. The company's organization currently has two AWS accounts, and the company expects to add more than 50 AWS accounts during the next 12 months The company will require all existing and future AWS accounts to use Amazon GuardDuty. Each existing AWS account has GuardDuty active. The company reviews GuardDuty findings by logging into each AWS account individually.

The company wants a centralized view of the GuardDuty findings for the existing AWS accounts and any future AWS accounts. The company also must ensure that any new AWS account has GuardDuty automatically turned on.

Which solution will meet these requirements?

Options:

A- Enable AWS Security Hub in the organization's management account. Configure GuardDuty within the management account to send all GuardDuty findings to Security Hub.

B- Create a new AWS account in the organization. Enable GuardDuty in the new account. Designate the new account as the delegated administrator account for GuardDuty. Configure GuardDuty to add existing accounts as member accounts. Select the option to automatically add new AWS accounts to the organization

C- Create a new AWS account in the organization. Enable GuardDuty in the new account. Enable AWS Security Hub in each account. Select the option to automatically add new AWS accounts to the organization.

D- Enable AWS Security Hub in the organization's management account. Designate the management account as the delegated administrator account for Security Hub. Add existing accounts as member accounts. Select the option to automatically add new AWS accounts to the organization. Send all Security Hub findings to the organization's GuardDuty account.

Answer:

B

Explanation:

For a company using AWS Organizations that requires centralized management and automatic activation of Amazon GuardDuty across all current and future AWS accounts, setting up a delegated administrator account for GuardDuty is the optimal solution. By enabling GuardDuty in a new account and designating it as the delegated administrator, the company can centrally manage GuardDuty findings and automatically enroll new AWS accounts into GuardDuty as they are created within the organization. This approach ensures consistent threat detection and continuous monitoring across all accounts, aligning with best security practices.

Question 6

Question Type: MultipleChoice

A company has a web-based application that runs behind an Application Load Balancer (ALB). The application is experiencing a credential stuffing attack that is producing many failed login attempts. The attack is coming from many IP addresses. The login attempts are using a user agent string of a known mobile device emulator.

A security engineer needs to implement a solution to mitigate the credential stuffing attack. The solution must still allow legitimate logins to the application.

Which solution will meet these requirements?

Options:

A- Create an Amazon CloudWatch alarm that reacts to login attempts that contain the specified user agent string. Add an Amazon Simple Notification Service (Amazon SNS) topic to the alarm.

B- Modify the inbound security group on the ALB to deny traffic from the IP addresses that are involved in the attack.

C- Create an AWS WAF web ACL for the ALB. Create a custom rule that blocks requests that contain the user agent string of the device emulator.

D- Create an AWS WAF web ACL for the ALB Create a custom rule that allows requests from legitimate user agent strings

Answer:

C

Explanation:

To mitigate a credential stuffing attack against a web-based application behind an Application Load Balancer (ALB), creating an AWS WAF web ACL with a custom rule to block requests containing the known malicious user agent string is an effective solution. This approach allows for precise targeting of the attack vector (the user agent string of the device emulator) without impacting legitimate users. AWS WAF provides the capability to inspect HTTP(S) requests and block those that match defined criteria, such as specific strings in the user agent header, thereby preventing malicious requests from reaching the application.

Question 7

Question Type: MultipleChoice

A company needs to implement DNS Security Extensions (DNSSEC) for a specific subdomain. The subdomain is already registered with Amazon Route 53. A security engineer has enabled DNSSEC signing and has created a key-signing key (KSK). When the security engineer tries to test the configuration, the security engineer receives an error for a broken trust chain.

What should the security engineer do to resolve this error?

Options:

A- Replace the KSK with a zone-signing key (ZSK).

B- Deactivate and then activate the KSK.

C- Create a Delegation Signer (DS) record in the parent hosted zone.

D- Create a Delegation Signer (DS) record in the subdomain.

Answer:

C

Question 8

Question Type: MultipleChoice

A company has AWS accounts in an organization in AWS Organizations. The company needs to install a corporate software package on all Amazon EC2 instances for all the accounts in the organization.

A central account provides base AMIs for the EC2 instances. The company uses AWS Systems Manager for software inventory and patching operations.

A security engineer must implement a solution that detects EC2 instances ttjat do not have the required software. The solution also must automatically install the software if the software is not present.

Which solution will meet these requirements?

Options:

A- Provide new AMIs that have the required software pre-installed. Apply a tag to the AMIs to indicate that the AMIs have the required software. Configure an SCP that allows new EC2 instances to be launched only if the instances have the tagged AMIs. Tag all existing EC2 instances.

B- Configure a custom patch baseline in Systems Manager Patch Manager. Add the package name for the required software to the approved packages list. Associate the new patch baseline with all EC2 instances. Set up a maintenance window for software deployment.

C- Centrally enable AWS Config. Set up the ec2-managedinstance-applications-required AWS Config rule for all accounts Create an Amazon EventBridge rule that reacts to AWS Config events. Configure the EventBridge rule to invoke an AWS Lambda function that uses Systems Manager Run Command to install the required software.

D- Create a new Systems Manager Distributor package for the required software. Specify the download location. Select all EC2 instances in the different accounts. Install the software by using Systems Manager Run Command.

Answer:

C

Explanation:

Utilizing AWS Config with a custom AWS Config rule (ec2-managedinstance-applications-required) enables detection of EC2 instances lacking the required software across all accounts in an organization. By creating an Amazon EventBridge rule that triggers on AWS Config events, and configuring it to invoke an AWS Lambda function, automated actions can be taken to ensure compliance. The Lambda function can leverage AWS Systems Manager Run Command to install the necessary software on non-compliant instances.

This approach ensures continuous compliance and automated remediation, aligning with best practices for cloud security and management.

Question 9

Question Type: MultipleChoice

A company needs to create a centralized solution to analyze log files. The company uses an organization in AWS Organizations to manage its AWS accounts.

The solution must aggregate and normalize events from the following sources:

* The entire organization in Organizations

* All AWS Marketplace offerings that run in the company's AWS accounts

* The company's on-premises systems

Which solution will meet these requirements?

Options:

A- Configure a centralized Amazon S3 bucket for the logs Enable VPC Flow Logs, AWS CloudTrail, and Amazon Route 53 logs in all accounts. Configure all accounts to use the centralized S3 bucket. Configure AWS Glue crawlers to parse the log files Use Amazon Athena to query the log data.

B- Configure log streams in Amazon CloudWatch Logs for the sources that need monitoring. Create log subscription filters for each log stream. Forward the messages to Amazon OpenSearch Service for analysis.

C- Set up a delegated Amazon Security Lake administrator account in Organizations. Enable and configure Security Lake for the organization. Add the accounts that need monitoring. Use Amazon Athena to query the log data.

D- Apply an SCP to configure all member accounts and services to deliver log files to a centralized Amazon S3 bucket. Use Amazon OpenSearch Service to query the centralized S3 bucket for log entries.

Answer:

C

Explanation:

Amazon Security Lake, when configured with a delegated administrator account in AWS Organizations, provides a centralized solution for aggregating, organizing, and prioritizing security data from multiple sources including AWS services, AWS Marketplace solutions, and on-premises systems. By enabling Security Lake for the organization and adding the necessary AWS accounts, the solution centralizes the collection and analysis of log data. This setup leverages the organization's structure to streamline log aggregation and normalization, making it an efficient solution for the specified requirements. The use of Amazon Athena for querying the log data further enhances the ability to analyze and respond to security findings across the organization.

Question 10

Question Type: MultipleChoice

A security engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.

Which solution meets these requirements?

Options:

A- Use AWS KMS with AWS managed keys and the ScheduleKeyDeletion API with a PendingWindowInDays set to 0 to remove the keys if necessary.

B- Use KMS with AWS imported key material and then use the DeleteImportedKeyMaterial API to remove the key material if necessary.

C- Use AWS CloudHSM to store the keys and then use the CloudHSM API or the PKCS11 library to delete the keys if necessary.

D- Use the Systems Manager Parameter Store to store the keys and then use the service API operations to delete the keys if necessary.

Answer:

A

To Get Premium Files for SCS-C02 Visit

https://www.p2pexams.com/products/scs-c02

For More Free Questions Visit

https://www.p2pexams.com/amazon/pdf/scs-c02