SCS-C02Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

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

https://www.pass2lead.com/scs-c02.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 is hosting a static website on Amazon S3 The company has configured an Amazon CloudFront distribution to serve the website contents The company has associated an IAM WAF web ACL with the CloudFront distribution. The web ACL ensures that requests originate from the United States to address compliance restrictions.

THE company is worried that the S3 URL might still be accessible directly and that requests can bypass the CloudFront distribution

Which combination of steps should the company take to remove direct access to the S3 URL? (Select TWO.) A. Select "Restrict Bucket Access" in the origin settings of the CloudFront distribution

B. Create an origin access identity (OAI) for the S3 origin

C. Update the S3 bucket policy to allow s3 GetObject with a condition that the IAM Referer key matches the secret value Deny all other requests

D. Configure the S3 bucket poky so that only the origin access identity (OAI) has read permission for objects in the bucket

E. Add an origin custom header that has the name Referer to the CloudFront distribution Give the header a secret value.

Correct Answer: AD

QUESTION 2

An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket. The key is used to access 2 TB of sensitive data that is stored in the S3 bucket.

A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.

What is the FASTEST way to prevent the sensitive data from being exposed?

A. Download the data from the existing S3 bucket to a new EC2 instance. Then delete the data from the S3 bucket. Re-encrypt the data with a client-based key. Upload the data to a new S3 bucket.

B. Block access to the public range of S3 endpoint IP addresses by using a host-based firewall. Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.

C. Revoke the IAM role\\'s active session permissions. Update the S3 bucket policy to deny access to the IAM role. Remove the IAM role from the EC2 instance profile.

D. Disable the current key. Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new key. Schedule the compromised key for deletion.

Correct Answer: D

QUESTION 3

A company uses Amazon RDS for MySQL as a database engine for its applications. A recent security audit revealed an RDS instance that is not compliant with company policy for encrypting data at rest. A security engineer at the company needs to ensure that all existing RDS databases are encrypted using server-side encryption and that any future deviations from the policy are detected.

Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

A. Create an IAM Config rule to detect the creation of unencrypted RDS databases. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger on the IAM Config rules compliance state change and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.

B. Use IAM System Manager State Manager to detect RDS database encryption configuration drift. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to track state changes and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.

C. Create a read replica for the existing unencrypted RDS database and enable replica encryption in the process. Once the replica becomes active, promote it into a standalone database instance and terminate the unencrypted database instance.

D. Take a snapshot of the unencrypted RDS database. Copy the snapshot and enable snapshot encryption in the process. Restore the database instance from the newly created encrypted snapshot. Terminate the unencrypted database instance.

E. Enable encryption for the identified unencrypted RDS instance by changing the configurations of the existing database

Correct Answer: AD

QUESTION 4

A developer signed in to a new account within an IAM Organization organizational unit (OU) containing multiple accounts. Access to the Amazon $3 service is restricted with the following SCP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

How can the security engineer provide the developer with Amazon $3 access without affecting other account?

A. Move the SCP to the root OU of organization to remove the restriction to access Amazon $3.

B. Add an IAM policy for the developer, which grants $3 access.

C. Create a new OU without applying the SCP restricting $3 access. Move the developer account to this new OU.

D. Add an allow list for the developer account for the $3 service.

Correct Answer: C

QUESTION 5

A company is using Amazon Macie, AWS Firewall Manager, Amazon Inspector, and AWS Shield Advanced in its AWS account. The company wants to receive alerts if a DDoS attack occurs against the account.

Which solution will meet this requirement?

A. Use Macie to detect an active DDoS event. Create Amazon CloudWatch alarms that respond to Macie findings.

B. Use Amazon Inspector to review resources and to invoke Amazon CloudWatch alarms for any resources that are vulnerable to DDoS attacks.

C. Create an Amazon CloudWatch alarm that monitors Firewall Manager metrics for an active DDoS event.

D. Create an Amazon CloudWatch alarm that monitors Shield Advanced metrics for an active DDoS event.

Correct Answer: D

This answer is correct because AWS Shield Advanced is a service that provides comprehensive protection against DDoS attacks of any size or duration. It also provides metrics and reports on the DDoS attack vectors, duration, and size. You

can create an Amazon CloudWatch alarm that monitors Shield Advanced metrics such as DDoSAttackBitsPerSecond, DDoSAttackPacketsPerSecond, and DDoSAttackRequestsPerSecond to receive alerts if a DDoS attack occurs against

your account.

For more information, see Monitoring AWS Shield Advanced with Amazon CloudWatch and AWS Shield Advanced metrics and alarms.

QUESTION 6

A company is using AWS to run a long-running analysis process on data that is stored in Amazon S3 buckets. The process runs on a fleet of Amazon EC2 instances that are in an Auto Scaling group. The EC2 instances are deployed in a private subnet Of a VPC that does not have internet access. The EC2 instances and the S3 buckets are in the same AWS account

The EC2 instances access the S3 buckets through an S3 gateway endpoint that has the default access policy. Each EC2 instance is associated With an instance profile role that has a policy that explicitly allows the s3:GetObject action and the s3:PutObject action for only the required S3 buckets.

The company learns that one or more of the EC2 instances are compromised and are exfiltrating data to an S3 bucket that is outside the companys organization in AWS Organizations. A security engtneer must implement a solution to stop this exfiltration of data and to keep the EC2 processing job functional.

Which solution will meet these requirements?

A. Update the policy on the S3 gateway endpoint to allow the S3 actions CY11y if the values of the aws:ResourceOrglD and aws:PrincipalOrglD condition keys match the companys values.

B. Update the policy on the instance profile role to allow the S3 actions only if the value of the aws:ResourceOrglD condition key matches the company\\'s value.

C. Add a network ACL rule to the subnet of the EC2 instances to block outgoing connections on port 443.

D. Apply an SCP on the AWS account to allow the $3 actions only if the values of the aws:ResourceOrglD and aws:PrincipalOrglD condition keys match the company\\'s values.

Correct Answer: D

To stop the data exfiltration from the compromised EC2 instances, the security engineer needs to implement a solution that can deny access to any S3 bucket that is outside the company\\'s organization. The solution should also allow the EC2 instances to access the required S3 buckets within the company\\'s organization for the analysis process. Option A is incorrect because updating the policy on the S3 gateway endpoint will not affect the access to S3 buckets that are outside the company\\'s organization. The S3 gateway endpoint only applies to S3 buckets that are in the same AWS Region as the VPC. The compromised EC2 instances can still access S3 buckets in other Regions or other AWS accounts through the internet gateway or NAT device. Option B is incorrect because updating the policy on the instance profile role will not prevent the compromised EC2 instances from using other credentials or methods to access S3 buckets outside the company\\'s organization. The instance profile role only applies to requests that are made using the credentials of that role. The compromised EC2 instances can still use other IAM users, roles, or access keys to access S3 buckets outside the company\\'s organization. Option C is incorrect because adding a network ACL rule to block outgoing connections on port 443 will also block legitimate connections to S3 buckets within the company\\'s organization. The network ACL rule will prevent the EC2 instances from accessing any S3 bucket through HTTPS, regardless of whether it is inside or outside the company\\'s organization. Option D is correct because applying an SCP on the AWS account will effectively deny access to any S3 bucket that is outside the company\\'s organization. The SCP will apply to all IAM users, roles, and resources in the AWS account, regardless of how they access S3. The SCP will use the aws:ResourceOrgID and aws:PrincipalOrgID condition keys to check whether the S3 bucket and the principal belong to the same organization as the AWS account. If they do not match, the SCP will deny the S3 actions.

References: Using service control policies AWS Organizations service control policy examples

QUESTION 7

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 ONS 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

https://aws.amazon.com/blogs/aws/log-your-vpc-dns-queries-with-route-53-resolver-query-logs/

QUESTION 8

The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.

What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

A. Use AWS Certificate Manager to encrypt all traffic between the client and application servers.

B. Review the application security groups to ensure that only the necessary ports are open.

C. Use Elastic Load Balancing to offload Secure Sockets Layer encryption.

D. Use Amazon Inspector to periodically scan the backend instances.

E. Use AWS Key Management Services to encrypt all the traffic between the client and application servers.

Correct Answer: BD

The steps that the Security Engineer should take to check for known vulnerabilities and limit the attack surface are:

B. Review the application security groups to ensure that only the necessary ports are open. This is a good practice to reduce the exposure of the EC2 instances to potential attacks from the Internet. Application security groups are a feature of Azure that allow you to group virtual machines and define network security policies based on those groups.

D. Use Amazon Inspector to periodically scan the backend instances. This is a service that helps you to identify vulnerabilities and exposures in your EC2 instances and applications. Amazon Inspector can perform automated security assessments based on predefined or custom rules packages2.

QUESTION 9

A company manages three separate IAM accounts for its production, development, and test environments, Each Developer is assigned a unique IAM user under the development account. A new application hosted on an Amazon EC2 instance in the developer account requires read access to the archived documents stored in an Amazon S3 bucket in the production account.

How should access be granted?

A. Create an IAM role in the production account and allow EC2 instances in the development account to assume that role using the trust policy. Provide read access for the required S3 bucket to this role.

B. Use a custom identity broker to allow Developer IAM users to temporarily access the S3 bucket.

C. Create a temporary IAM user for the application to use in the production account.

D. Create a temporary IAM user in the production account and provide read access to Amazon S3. Generate the temporary IAM user\\'s access key and secret key and store these on the EC2 instance used by the application in the development account.

Correct Answer: A

https://IAM.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/

QUESTION 10

A company finds that one of its Amazon EC2 instances suddenly has a high CPU usage. The company does not know whether the EC2 instance is compromised or whether the operating system is performing background cleanup.

Which combination of steps should a security engineer take before investigating the issue? (Select THREE.)

A. Disable termination protection for the EC2 instance if termination protection has not been disabled.

B. Enable termination protection for the EC2 instance if termination protection has not been enabled.

C. Take snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance.

D. Remove all snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance.

E. Capture the EC2 instance metadata, and then tag the EC2 instance as under quarantine.

F. Immediately remove any entries in the EC2 instance metadata that contain sensitive information.

Correct Answer: BCE

https://d1.awsstatic.com/WWPS/pdf/aws_security_incident_response.pdf

QUESTION 11

A company hosts an application on Amazon EC2 that is subject to specific rules for regulatory compliance. One rule states that traffic to and from the workload must be inspected for network-level attacks. This involves inspecting the whole packet.

To comply with this regulatory rule, a security engineer must install intrusion detection software on a c5n.4xlarge EC2 instance. The engineer must then configure the software to monitor traffic to and from the application instances. What should the security engineer do next?

A. Place the network interface in promiscuous mode to capture the traffic.

B. Configure VPC Flow Logs to send traffic to the monitoring EC2 instance using a Network Load Balancer.

C. Configure VPC traffic mirroring to send traffic to the monitoring EC2 instance using a Network Load Balancer.

D. Use Amazon Inspector to detect network-level attacks and trigger an IAM Lambda function to send the suspicious packets to the EC2 instance.

Correct Answer: D

QUESTION 12

A company usesAWS Organizations to run workloads in multiple AWS accounts Currently the individual team members at the company access all Amazon EC2 instances remotely by using SSH or Remote Desktop Protocol (RDP) The company does not have any audit trails and security groups are occasionally open The company must secure access management and implement a centralized togging solution

Which solution will meet these requirements MOST securely?

A. Configure trusted access for AWS System Manager in Organizations Configure a bastion host from the management account Replace SSH and RDP by using Systems Manager Session Manager from the management account Configure Session Manager logging to Amazon CloudWatch Logs

B. Replace SSH and RDP with AWS Systems Manager Session Manager Install Systems Manager Agent (SSM Agent) on the instances Attach the

C. AmazonSSMManagedInstanceCore role to the instances Configure session data streaming to Amazon CloudWatch Logs Create a separate logging account that has appropriate cross-account permissions to audit the log data

D. Install a bastion host in the management account Reconfigure all SSH and RDP to allow access only from the bastion host Install AWS Systems Manager Agent (SSM Agent) on the bastion host Attach the AmazonSSMManagedInstanceCore role to the bastion host Configure session data streaming to Amazon CloudWatch Logs in a separate logging account to audit log data

E. Replace SSH and RDP with AWS Systems Manager State Manager Install Systems Manager Agent (SSM Agent) on the instances Attach the AmazonSSMManagedInstanceCore role to the instances Configure session data streaming to Amazon CloudTrail Use CloudTrail Insights to analyze the trail data

Correct Answer: C

To meet the requirements of securing access management and implementing a centralized logging solution, the most secure solution would be to:

Install a bastion host in the management account. Reconfigure all SSH and RDP to allow access only from the bastion host. Install AWS Systems Manager Agent (SSM Agent) on the bastion host. Attach the

AmazonSSMManagedInstanceCore role to the bastion host. Configure session data streaming to Amazon CloudWatch Logs in a separate logging account to audit log data This solution provides the following security benefits:

It uses AWS Systems Manager Session Manager instead of traditional SSH and RDP protocols, which provides a secure method for accessing EC2 instances without requiring inbound firewall rules or open ports. It provides audit trails by configuring Session Manager logging to Amazon CloudWatch Logs and creating a separate logging account to audit the log data. It uses the AWS Systems Manager Agent to automate common administrative tasks and improve the security posture of the instances. The separate logging account with cross-account permissions provides better data separation and improves security posture.

https://aws.amazon.com/solutions/implementations/centralized-logging/

QUESTION 13

A company is running workloads in a single IAM account on Amazon EC2 instances and Amazon EMR clusters a recent security audit revealed that multiple Amazon Elastic Block Store (Amazon EBS) volumes and snapshots are not encrypted

The company\\'s security engineer is working on a solution that will allow users to deploy EC2 Instances and EMR clusters while ensuring that all new EBS volumes and EBS snapshots are encrypted at rest. The solution must also minimize operational overhead

Which steps should the security engineer take to meet these requirements?

A. Create an Amazon Event Bridge (Amazon Cloud watch Events) event with an EC2 instance as the source and create volume as the event trigger. When the event is triggered invoke an IAM Lambda function to evaluate and notify the security engineer if the EBS volume that was created is not encrypted.

B. Use a customer managed IAM policy that will verify that the encryption ag of the Createvolume context is set to true. Apply this rule to all users.

C. Create an IAM Config rule to evaluate the conguration of each EC2 instance on creation or modication. Have the IAM Cong rule trigger an IAM Lambdafunction to alert the security team and terminate the instance it the EBS volume is not encrypted. 5

D. Use the IAM Management Console or IAM CLi to enable encryption by default for EBS volumes in each IAM Region where the company operates.

Correct Answer: D

To ensure that all new EBS volumes and EBS snapshots are encrypted at rest and minimize operational overhead, the security engineer should do the following:

Use the AWS Management Console or AWS CLI to enable encryption by default for EBS volumes in each AWS Region where the company operates. This allows the security engineer to automatically encrypt any new EBS volumes and

snapshots created from those volumes, without requiring any additional actions from users.

QUESTION 14

A company\\'s security team needs to receive a notification whenever an AWS access key has not been rotated in 90 or more days. A security engineer must develop a solution that provides these notifications automatically.

Which solution will meet these requirements with the LEAST amount of effort?

A. Deploy an AWS Config managed rule to run on a periodic basis of 24 hours. Select the access-keys-rotated managed rule, and set the maxAccessKeyAge parameter to 90 days. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with an event pattern that matches the compliance type of NON_COMPLIANT from AWS Config for the managed rule. Configure EventBridge (CloudWatch Events) to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

B. Create a script to export a .csv file from the AWS Trusted Advisor check for IAM access key rotation. Load the script into an AWS Lambda function that will upload the .csv file to an Amazon S3 bucket. Create an Amazon Athena table query that runs when the .csv file is uploaded to the S3 bucket. Publish the results for any keys older than 90 days by using an invocation of an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

C. Create a script to download the IAM credentials report on a periodic basis. Load the script into an AWS Lambda function that will run on a schedule through Amazon EventBridge (Amazon CloudWatch Events). Configure the Lambda script to load the report into memory and to filter the report for records in which the key was last rotated at least 90 days ago. If any records are detected, send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

D. Create an AWS Lambda function that queries the IAM API to list all the users. Iterate through the users by using the ListAccessKeys operation. Verify that the value in the CreateDate field is not at least 90 days old. Send an Amazon Simple Notification Service (Amazon SNS) notification to the security team if the value is at least 90 days old. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule the Lambda function to run each day.

Correct Answer: A

QUESTION 15

A company is evaluating its security posture. In the past, the company has observed issues with specific hosts and host header combinations that affected

the company\\'s business. The company has configured AWS WAF web ACLs as an initial step to mitigate these issues.

The company must create a log analysis solution for the AWS WAF web ACLs to monitor problematic activity. The company wants to process all the AWS WAF logs in a central location. The company must have the ability to filter out requests based on specific hosts.

A security engineer starts to enable access logging for the AWS WAF web ACLs.

What should the security engineer do next to meet these requirements with the MOST operational efficiency?

A. Specify Amazon Redshift as the destination for the access logs. Deploy the Amazon Athena Redshift connector. Use Athena to query the data from Amazon Redshift and to filter the logs by host.

B. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon CloudWatch Logs Insights to design a query to filter the logs by host.

C. Specify Amazon CloudWatch as the destination for the access logs. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and to filter the logs by host.

D. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon Redshift Spectrum to query the logs and to filter the logs by host.

Correct Answer: C

Specify Amazon CloudWatch as the destination for the access logs. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and to filter the logs by host.

According to the AWS documentation, AWS WAF offers logging for the traffic that your web ACLs analyze. The logs include information such as the time that AWS WAF received the request from your protected AWS resource, detailed information about the request, and the action setting for the rule that the request matched. You can send your logs to an Amazon CloudWatch Logs log group, an Amazon Simple Storage Service (Amazon S3) bucket, or an Amazon Kinesis Data Firehose. To create a log analysis solution for the AWS WAF web ACLs, you can use Amazon Athena, which is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. You can use Athena to query and filter the AWS WAF logs by host or any other criteria. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.

To use Athena with AWS WAF logs, you need to export the CloudWatch logs to an S3 bucket. You can do this by creating a subscription filter that sends your log events to a Kinesis Data Firehose delivery stream, which then delivers the data to an S3 bucket. Alternatively, you can use AWS DMS to migrate your CloudWatch logs to S3. After you have exported your CloudWatch logs to S3, you can create a table in Athena that points to your S3 bucket and use the AWS service log format that matches your log schema. For example, if you are using JSON format for your AWS WAF logs, you can use the AWSJSONSerDe serde. Then you can run SQL queries on your Athena table and filter the results by host or any other field in your log data. Therefore, this solution meets the requirements of creating a log analysis solution for the AWS WAF web ACLs with the most operational efficiency. This solution does not require setting up any additional infrastructure or services, and it leverages the existing capabilities of CloudWatch, S3, and Athena. The other options are incorrect because:

A. Specifying Amazon Redshift as the destination for the access logs is not possible, because AWS WAF does not support sending logs directly to Redshift. You would need to use an intermediate service such as Kinesis Data Firehose or AWS DMS to load the data from CloudWatch or S3 to Redshift. Deploying the Amazon Athena Redshift connector is not necessary, because you can query Redshift data directly from Athena without using a connector. This solution would also incur additional costs and operational overhead of managing a Redshift cluster.

B. Specifying Amazon CloudWatch as the destination for the access logs is possible, but using Amazon CloudWatch Logs Insights to design a query to filter the logs by host is not efficient or scalable. CloudWatch Logs Insights is a feature that enables you to interactively search and analyze your log data in CloudWatch Logs. However, CloudWatch Logs Insights has some limitations, such as a maximum query duration of 20 minutes, a maximum of 20 log groups per query, and a maximum retention period of 24 months. These limitations may affect your ability to perform complex and long-running analysis on your AWS WAF logs. D. Specifying Amazon CloudWatch as the destination for the access logs is possible, but using Amazon Redshift Spectrum to query the logs and filter them by host is not efficient or cost-effective. Redshift Spectrum is a feature of Amazon Redshift that enables you to run queries against exabytes of data in S3 without loading or transforming any data. However, Redshift Spectrum requires a Redshift cluster to process the queries, which adds additional costs and operational overhead. Redshift Spectrum also charges you based on the number of bytes scanned by each query, which can be expensive if you have large volumes of log data.

References:

1: Logging AWS WAF web ACL traffic -Amazon Web Services

2: What Is Amazon Athena? -Amazon Athena

3: Streaming CloudWatch Logs Data to Amazon S3 -Amazon CloudWatch Logs

4: Migrate data from CloudWatch Logs using AWS Database Migration Service -AWS Database Migration Service

5: Querying AWS service logs -Amazon Athena

6: Querying data from Amazon Redshift -Amazon Athena

7: Analyzing log data with CloudWatch Logs Insights -Amazon CloudWatch Logs

8: CloudWatch Logs Insights quotas -Amazon CloudWatch

9: Querying external data using Amazon Redshift Spectrum -Amazon Redshift

10: Amazon Redshift Spectrum pricing -Amazon Redshift