

SCS-C03 Cheap Dumps - SCS-C03 Valid Exam Guide



What's more, part of that FreeDumps SCS-C03 dumps now are free: <https://drive.google.com/open?id=1RQjf0Xpo23BRQHBJ5WondYjYFTWLyW8y>

SCS-C03 exam certification is considered as a standard in measuring your professional skills in your industry. Besides, those possessing the Amazon SCS-C03 certification are more likely to receive higher salaries. So it is very necessary to get SCS-C03 certification. Here, FreeDumps SCS-C03 free pdf download can give you some reference. First, you should have preview about the content of SCS-C03 real test. Amazon SCS-C03 contains the comprehensive contents with explanations where is available. With the assist of SCS-C03 training material, you will get success.

If you are going to purchase SCS-C03 Study Materials online, you may pay attention to your money safety. With applying the international recognition third party for the payment, your money and account safety can be guaranteed if you choose us. And the third party will protect your interests. In addition, SCS-C03 training materials are high-quality, for we have a professional team to research the latest information, and you can use them at ease. Besides if you have little time to prepare for your exam, you can also choose us, you just need to spend 48 to 72 hours on studying, you can pass the exam. Choose us, and you will never regret!

>> SCS-C03 Cheap Dumps <<

Benefits of buying Amazon SCS-C03 exam practice material today

We provide you free demo with you to help you have a deeper understanding about SCS-C03 study materials. Free demo can be found in our website, and we recommend you to have a try before buying. Furthermore, SCS-C03 exam materials of us have the questions and answers, and you can have a convenient check of your answers after you finish practicing. We are pass guarantee and money back guarantee for your failure after purchasing SCS-C03 Study Materials. You just need to give your failure scanned and we will give you full refund. Choose us, and we can help you to pass the exam successfully.

Amazon AWS Certified Security - Specialty Sample Questions (Q90-Q95):

NEW QUESTION # 90

A company wants to establish separate AWS Key Management Service (AWS KMS) keys to use for different AWS services. The company's security engineer created a key policy to allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role. The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key for other services.

Which change to the policy should the security engineer make to resolve these issues?

- A. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change the `kms:ViaService` value to `ec2.us-east-1.amazonaws.com`.
- B. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change `StringEquals` to `StringLike`.
- C. In the policy document, add a new statement block that grants the `kms:Disable*` permission to the security engineer's IAM role.
- D. In the policy document, remove the statement block that contains the Sid "Enable IAM User Permissions". Add key management policies to the KMS policy.

Answer: A

Explanation:

AWS KMS key policies can restrict how and where a key is used by leveraging condition keys such as kms:ViaService. According to the AWS Certified Security - Specialty documentation, kms:ViaService limits key usage to requests that originate from a specific AWS service in a specific Region. If this condition is overly broad or incorrect, other IAM roles and services may unintentionally use the key.

By explicitly setting the kms:ViaService condition value to ec2.us-east-1.amazonaws.com, the key policy ensures that the KMS key can only be used when requests are made through the Amazon EC2 service in that Region, such as for EBS volume encryption. This prevents other services or unintended IAM roles from using the key.

Option A weakens the condition logic and can broaden access. Option B removes essential permissions that allow IAM policies to function with KMS keys and is not recommended. Option D relates to administrative control of the key, not service-level usage restrictions.

AWS best practices recommend using kms:ViaService and precise condition values to enforce service-specific key usage and strong separation of duties.

Referenced AWS Specialty Documents:

AWS Certified Security - Specialty Official Study Guide

AWS KMS Key Policy Condition Keys

AWS KMS Best Practices

NEW QUESTION # 91

A company needs to prevent Amazon S3 objects from being shared with IAM identities outside of the company's organization in AWS Organizations. A security engineer is creating and deploying an SCP to accomplish this goal. The company has enabled the S3 Block Public Access feature on all of its S3 buckets. What should the SCP do to meet these requirements?

- A. Deny the S3:PutAccountPublicAccessBlock action with a Condition element that comprises an operator of StringLike, a key of aws:PrincipalArn, and the values of the external IAM principals.
- B. Allow the S3:* action with a Condition element that comprises an operator of StringNotEquals, a key of aws:PrincipalOrgID, and a value of S {aws:PrincipalOrgID}.
- C. Deny the S3:* action with a Condition element that comprises an operator of StringLike, a key of aws:PrincipalArn, and the values of the external IAM principals
- **D. Deny the S3:* action with a Condition element that comprises an operator of StringNotEquals, a key of aws:ResourceOrgID, and a value of S {aws:PrincipalOrgID}.**

Answer: D

Explanation:

To restrict access to Amazon S3 objects so that they are only accessible by IAM identities within the company's AWS Organization, the SCP should deny access to any S3:* action where the resource's organization ID (aws:ResourceOrgID) does not match the principal's organization ID (aws:PrincipalOrgID). Using StringNotEquals ensures that only IAM identities within the organization can access the S3 objects. If the resource and principal organization IDs are different, access will be denied.

NEW QUESTION # 92

A security engineer has designed a VPC to segment private traffic from public traffic. The VPC includes two Availability Zones. The security engineer has provisioned each Availability Zone with one private subnet and one public subnet. The security engineer has created three route tables for use with the environment. One route table is for the public subnets, and two route tables are for the private subnets (one route table for the private subnet in each Availability Zone).

The security engineer discovers that all four subnets are attempting to route traffic out through the internet gateway that is attached to the VPC.

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

- **A. Modify the route tables that are associated with each of the private subnets. Create a new route for the destination 0.0.0.0/0. Specify the NAT gateway in the public subnet of the same Availability Zone as the target of the route.**
- **B. Verify that a NAT gateway has been provisioned in the public subnet in each Availability Zone.**
- C. Modify the route tables that are associated with each of the private subnets. Create a new route for the destination 0.0.0.0/0. Specify the internet gateway as the target of the route.
- D. Modify the route tables that are associated with each of the public subnets. Create a new route for local destinations to the VPC CIDR range.
- E. Verify that a NAT gateway has been provisioned in the private subnet in each Availability Zone.

Answer: A,B

Explanation:

In a properly segmented VPC architecture, public subnets route internet-bound traffic to an internet gateway, while private subnets route outbound internet traffic through a NAT gateway that resides in a public subnet. According to the AWS Certified Security - Specialty Official Study Guide and Amazon VPC documentation, private subnets must never have a direct route to an internet gateway.

The issue described indicates that private subnets are incorrectly routing traffic directly to the internet gateway. To remediate this, a NAT gateway must be provisioned in each public subnet to ensure high availability across Availability Zones. This satisfies the requirement that private resources can initiate outbound connections without being directly reachable from the internet.

Next, the route tables associated with the private subnets must be updated so that the default route (0.0.0.0/0) points to the NAT gateway in the same Availability Zone. This ensures proper traffic flow and prevents cross-AZ dependencies.

Option B is incorrect because NAT gateways must reside in public subnets. Option C is unnecessary because local routes to the VPC CIDR range are automatically created. Option E is explicitly insecure, as it would reintroduce direct internet gateway access from private subnets.

AWS documentation consistently identifies NAT gateways plus correct private subnet routing as the standard design for secure VPC segmentation.

* AWS Certified Security - Specialty Official Study Guide

* Amazon VPC Route Table Documentation

* AWS Well-Architected Framework - Security Pillar

NEW QUESTION # 93

A company uses Amazon Elastic Kubernetes Service (Amazon EKS) clusters to run its Kubernetes-based applications. The company uses Amazon GuardDuty to protect the applications.

EKS Protection is enabled in GuardDuty. However, the corresponding GuardDuty feature is not monitoring the Kubernetes-based applications.

Which solution will cause GuardDuty to monitor the Kubernetes-based applications?

- A. Ensure that the AmazonGuardDutyFullAccess AWS managed policy is attached to the GuardDuty service role.
- B. Enable VPC flow logs for the VPC that hosts the EKS clusters.
- C. Assign the CloudWatchEventsFullAccess AWS managed policy to the EKS clusters.
- **D. Enable the control plane logs in Amazon EKS. Ensure that the logs are ingested into Amazon CloudWatch.**

Answer: D

Explanation:

Amazon GuardDuty's EKS Protection relies on Amazon EKS control plane logs to monitor Kubernetes activity and detect potential security threats. Enabling control plane logging (e.g., API server logs) in EKS and sending these logs to Amazon CloudWatch allows GuardDuty to analyze the Kubernetes activity, making it possible to detect threats in the EKS clusters.

NEW QUESTION # 94

A company is developing an application that runs across a combination of Amazon EC2 On-Demand Instances and Spot Instances. A security engineer needs to provide a logging solution that makes logs for all instances available from a single location. The solution must allow only a specific set of users to analyze the logs for event patterns. The users must be able to use SQL queries on the logs to perform root cause analysis.

Which solution will meet these requirements?

- **A. Configure the EC2 instances to send application logs to a single Amazon CloudWatch Logs log group. Allow only specific users to access the log group. Use CloudWatch Logs Insights to query the log group.**
- B. Configure each EC2 instance to send its application logs to its own specific Amazon CloudWatch Logs log group. Allow only specific users to access the log groups. Use Amazon Athena to query all the log groups.
- C. Configure the EC2 instances to send application logs to a single Amazon S3 bucket. Allow only specific users to access the S3 bucket. Use Amazon CloudWatch Logs Insights to query the log files in the S3 bucket.
- D. Configure the EC2 instances to send application logs to a single Amazon CloudWatch Logs log group. Grant Amazon Detective access to the log group. Allow only specific users to use Detective to analyze the logs.

Answer: A

Explanation:

Amazon CloudWatch Logs provides a centralized, scalable service for collecting and storing logs from Amazon EC2 instances, regardless of whether the instances are On-Demand or Spot Instances. According to the AWS Certified Security - Specialty Official Study Guide, CloudWatch Logs is the recommended service for centralized log aggregation and near-real-time analysis of application and system logs.

By configuring all EC2 instances to send logs to a single CloudWatch Logs log group, the security engineer ensures that logs from all instances are available in one centralized location. Access to the log group can be restricted by using IAM policies, ensuring that only authorized users can view and analyze the logs.

CloudWatch Logs Insights provides a powerful query language with SQL-like syntax, enabling users to search, filter, aggregate, and analyze log data efficiently. This directly satisfies the requirement for SQL-style queries to identify event patterns and perform root cause analysis without requiring data movement or additional services.

Option B is incorrect because CloudWatch Logs Insights cannot query log files stored in Amazon S3. Option C is inefficient and operationally complex, as Athena cannot directly query CloudWatch Logs log groups.

Option D is invalid because Amazon Detective is designed for security investigations using GuardDuty findings, not for general application log analysis.

AWS documentation explicitly states that CloudWatch Logs combined with CloudWatch Logs Insights is the most efficient and secure approach for centralized log analysis in EC2-based architectures.

* AWS Certified Security - Specialty Official Study Guide

* Amazon CloudWatch Logs Documentation

* CloudWatch Logs Insights Query Guide

NEW QUESTION # 95

.....

At the FreeDumps, we strive to provide our customers with updated and real Amazon SCS-C03 exam questions. We are committed to helping our students reach their goals and advance their careers through comprehensive, convenient, and cost-effective preparation for your AWS Certified Security - Specialty (SCS-C03) exam preparation material.

SCS-C03 Valid Exam Guide: <https://www.freedumps.top/SCS-C03-real-exam.html>

We hypothesize that you fail the exam after using our SCS-C03 learning engine we can switch other versions for you or give back full refund, That means if you fail the exam or the dumps have no use so that you fail, we will fully refund the money of our SCS-C03 exam simulate, Amazon SCS-C03 Cheap Dumps So don't hesitate to buy our {Examcode} study materials, we will give you the high-quality product and professional customer services, On the other hand, in order to cater to the different demands of our customers, we have prepared the free demo of SCS-C03 test braindumps materials in this website for your reference, the contents in the free demo is a little part of our SCS-C03 pass-for-sure materials, we believe that you will find the advantages of our SCS-C03 exam guide materials by yourself after trying, what's more, our company has always kept an affordable price in the international market during the ten years, I believe that you can feel our sincerity of helping more people in the world from that.

The failover mechanism must be aware of the location SCS-C03 and availability of the objects that comprise an application in a cluster, User interface element, We hypothesize that you fail the exam after using our SCS-C03 Learning Engine we can switch other versions for you or give back full refund.

Quiz SCS-C03 - Marvelous AWS Certified Security - Specialty Cheap Dumps

That means if you fail the exam or the dumps have no use so that you fail, we will fully refund the money of our SCS-C03 exam simulate, So don't hesitate to buy our {Examcode} study SCS-C03 Reliable Exam Online materials, we will give you the high-quality product and professional customer services.

On the other hand, in order to cater to the different demands of our customers, we have prepared the free demo of SCS-C03 test braindumps materials in this website for your reference, the contents in the free demo is a little part of our SCS-C03 pass-for-sure materials, we believe that you will find the advantages of our SCS-C03 exam guide materials by yourself after trying, what's more, our company has always kept an affordable price in the international market during the ten years, I believe that you can feel our sincerity of helping more people in the world from that.

We also have online and offline SCS-C03 Valid Exam Guide service stuff, if you have any question, you can consult us.

- SCS-C03 Exam Cram Latest SCS-C03 Exam Bootcamp SCS-C03 Exam Voucher Search for ✨ SCS-C03 ✨ and download it for free on { www.vceengine.com } website Authentic SCS-C03 Exam Questions
- Reliable SCS-C03 Test Question Lab SCS-C03 Questions Reliable SCS-C03 Test Question Immediately

