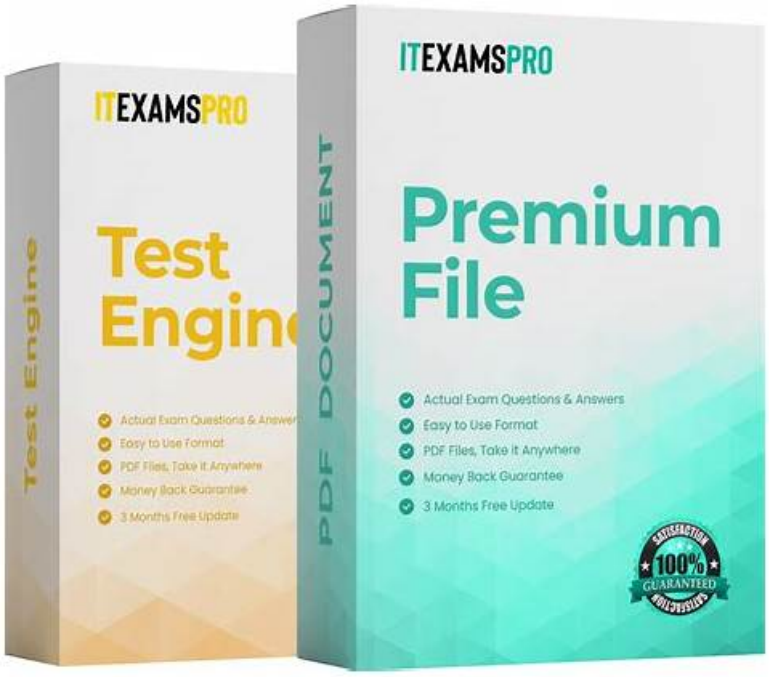
Reliable Amazon SOA-C02 Braindumps Free - New SOA-C02 Test Vce Free



What's more, part of that Pass4sures SOA-C02 dumps now are free: https://drive.google.com/open?id=1oBATNURHzYuvX9GI5xqD1pKBLicx_0XL

The passing rate of our SOA-C02 study materials is 99% and the hit rate is also high. Our study materials are selected strictly based on the real SOA-C02 exam. Our expert team guarantees that each answer and question is useful and valuable. We also update frequently to guarantee that the client can get more learning SOA-C02 resources and follow the trend of the times. So if you use our study materials you will pass the test with high success probability.

The AWS Certified SysOps Administrator - Associate (SOA-C02) certification exam is designed for professionals who are responsible for managing and deploying applications on the AWS platform. SOA-C02 exam is intended to validate the candidate's skills and knowledge in various areas related to AWS, including system operations, deployment, management, security, and troubleshooting.

The SOA-C02 certification exam is a challenging exam that requires individuals to have a solid understanding of AWS services and best practices. SOA-C02 exam consists of 65 multiple-choice and multiple-response questions that must be completed within 130 minutes. To pass the exam, individuals must score 720 out of 1000 points. Individuals who fail the exam can retake it after a waiting period of 14 days.

The Amazon SOA-C02 Exam covers a wide range of topics, including AWS deployment and management, security, networking, storage, and monitoring. Candidates are expected to have a strong understanding of these topics, as well as experience working with AWS in a production environment. AWS recommends that candidates take the AWS Certified SysOps Administrator – Associate training course to prepare for the exam.

>> Reliable Amazon SOA-C02 Braindumps Free <<

SOA-C02 Quiz Braindumps - SOA-C02 Test Guide & SOA-C02 Test Bootcamp

In today's competitive IT industry, passing Amazon certification SOA-C02 exam has a lot of benefits. Gaining Amazon SOA-C02 certification can increase your salary. People who have got Amazon SOA-C02 certification often have much higher salary than counterparts who don't have the certificate. But Amazon Certification SOA-C02 Exam is not very easy, so Pass4sures is a website that can help you grow your salary.

Amazon AWS Certified SysOps Administrator - Associate (SOA-C02) Sample Questions (Q268-Q273):

NEW QUESTION # 268
The company's security team needs to consolidate Security Hub findings to reduce duplicate notifications for the same misconfigurations.
Options:

- A. Set up an AWS Config aggregator instead of Security Hub. Deploy a custom conformance pack by consolidating AWS Config rules.
- B. Turn on consolidated control findings in the Security Hub delegated administrator account.
- C. Launch an Amazon EC2 instance in the organization's management account. Configure a custom script to assume a role in each linked account to extract and consolidate findings from the accounts.
- D. Export the Security Hub findings. Consolidate the findings based on control ID. Visualize the findings in Amazon QuickSight.

Answer: B

Explanation:
Enabling consolidated control findings in Security Hub reduces duplication by merging findings for similar controls across multiple standards. This reduces the operational burden of prioritizing remediation based on multiple copies of the same findings.
Consolidated Control Findings: Merges findings for controls across standards to avoid duplicates, providing a clearer view of misconfigurations without the need for additional infrastructure or manual processing.
Least Operational Overhead: This solution is managed within Security Hub without the need for external tools or manual exports. Using AWS Config aggregators, QuickSight visualization, or custom EC2-based solutions would introduce additional complexity and overhead.

NEW QUESTION # 269
A company hosts a web application on an Amazon EC2 instance. The web server logs are published to Amazon CloudWatch Logs. The log events have the same structure and include the HTTP response codes that are associated with the user requests. The company needs to monitor the number of times that the web server returns an HTTP 404 response.
What is the MOST operationally efficient solution that meets these requirements?

- A. Create a CloudWatch Logs subscription filter that counts the number of times that the web server returns an HTTP 404 response.
- B. Create a CloudWatch Logs metric filter that counts the number of times that the web server returns an HTTP 404 response.
- C. Create an AWS Lambda function that runs a CloudWatch Logs Insights query that counts the number of 404 codes in the log events during the past hour.
- D. Create a script that runs a CloudWatch Logs Insights query that counts the number of 404 codes in the log events during the past hour.

Answer: B

Explanation:
This is the most operationally efficient solution that meets the requirements, as it will allow the company to monitor the number of times that the web server returns an HTTP 404 response in real-time. The other solutions (creating a CloudWatch Logs subscription filter, an AWS Lambda function, or a script) will require additional steps and resources to monitor the number of times that the web server returns an HTTP 404 response.
A metric filter allows you to search for specific terms, phrases, or values in your log events, and then to create a metric based on the number of occurrences of those search terms. This allows you to create a CloudWatch Metric that can be used to create alarms and dashboards, which can be used to monitor the number of HTTP 404 responses returned by the web server.

NEW QUESTION # 270
A company has a security AWS account and a production AWS account. The company stores API keys as a secret in AWS Secrets Manager in the security account. The company uses an AWS Key Management Service (AWS KMS) AWS managed key to encrypt the secret.
An AWS Lambda function in the production account returns an error when the function attempts to access the secret.

Which combination of actions in the security account will allow the Lambda function to access the secret? (Choose two.)

- A. Update the AWS managed KMS key's resource policy. In the policy, allow the Lambda function to perform the kms:Decrypt and kms:DescribeKey actions.
- B. Add a resource policy to the secret. In the policy, allow the Lambda function to perform the secretsmanager:GetSecretValue action.
- C. Create a customer managed KMS key. Add a resource policy that allows the Lambda function to perform the kms:Decrypt and kms:DescribeKey actions. Change the key that encrypts the secret to be the new customer managed KMS key.
- D. Add a resource policy to the secret. In the policy, allow the Lambda function to perform the secretsmanager:DescribeSecret action.
- E. Create a customer managed KMS key. Add a resource policy that allows the Lambda function to perform the kms:CreateGrant and kms:GenerateDataKey actions. Change the key that encrypts the secret to be the new customer managed KMS key.

Answer: B,C

Explanation:
Use a customer managed KMS key so you can grant the Lambda role kms:Decrypt and kms:DescribeKey, then re-encrypt the secret with that key. Also attach a resource policy on the secret that lets the Lambda role call secretsmanager:GetSecretValue. Together, these permissions allow cross-account retrieval and decryption.

NEW QUESTION # 271
A company currently runs its infrastructure within a VPC in a single Availability Zone The VPC is connected to the company's on-premises data center through an AWS Site-to-SIte VPN connection attached to a virtual pnvate gateway. The on-premises route tables route all VPC networks to the VPN connection Communication between the two environments is working correctly. A SysOps administrator created new VPC subnets within a new Availability Zone, and deployed new resources within the subnets. However, communication cannot be established between the new resources and the on-premises environment.
Which steps should the SysOps administrator take to resolve the issue?

- A. Add a route to the route tables of the new subnets that send on-premises traffic to the virtual private gateway.
- B. Establish a new Site-to-Site VPN connection between a virtual private gateway attached to the new Availability Zone and the on-premises data center
- C. Replace the Site-to-Site VPN connection with an AWS Direct Connect connection.
- D. Create a ticket with AWS Support to request adding Availability Zones to the Site-to-Site VPN route configuration.

Answer: A

Explanation:
Adding a Route to the Route Tables:
* When new subnets are created, they need appropriate routing to ensure communication with on-premises networks.
* Steps:
* Go to the AWS Management Console.
* Navigate to VPC.
* Select the route table associated with the new subnets.
* Choose "Edit routes."
* Add a new route with the destination CIDR block of the on-premises network.
* For the target, select the virtual private gateway (VGW).
* This ensures that traffic destined for the on-premises network is routed correctly through the VPN connection.
* AWS VPC Route Tables

NEW QUESTION # 272
A company has its accounts in an organization in AWS Organizations. The company deploys its first service control policy (SCP) to an organizational unit (OU). The SCP denies the iam:CreateUser action. Only the newly created SCP is attached to the OU. After deployment of the SCP, users in the OU who assume a developer IAM role can no longer launch Amazon EC2 instances.
Which action should a SysOps administrator take to resolve this issue?

- A. Update the SCP to include an additional statement that allows the ec2:RunInstances action.
- B. Update the SCP by changing the denied iam:CreateUser action to iam:Create*.

- C. Add a permissions boundary to the developer IAM role to explicitly allow the ec2:RunInstances action.
- D. Update the SCP to include an additional statement that allows all actions on all resources.

Answer: A

Explanation:
Service Control Policies (SCPs) in AWS Organizations act as permission guardrails, defining the maximum available permissions for IAM entities within an organization. An SCP does not grant permissions but instead limits them. When an SCP is attached to an organizational unit (OU), it restricts the permissions of all accounts within that OU.
In this scenario, the SCP explicitly denies the iam:CreateUser action. However, if the SCP does not explicitly allow other necessary actions, such as ec2:RunInstances, those actions are implicitly denied. This is because, by default, all actions are denied unless explicitly allowed in the SCP.
To resolve the issue, the SCP should be updated to include an explicit allow statement for the ec2:
RunInstances action. This will permit users in the OU to launch EC2 instances while still denying the creation of IAM users.
Reference:
AWS Organizations Documentation: Service control policies (SCPs) - AWS Organizations

NEW QUESTION # 273
.....