SOA-C02$^{\text{Q\&As}}$

AWS Certified SysOps Administrator - Associate (SOA-C02)

Pass Amazon SOA-C02 Exam with 100% Guarantee

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

https://www.pass4itsure.com/soa-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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

A company needs to archive all audit logs for 10 years. The company must protect the logs from any future edits. Which solution will meet these requirements?

A. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Configure AWS Key Management Service (AWS KMS) encryption.

B. Store the data in an Amazon S3 Glacier vault. Configure a vault lock policy for write- once, read-many (WORM) access.

C. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Configure server-side encryption.

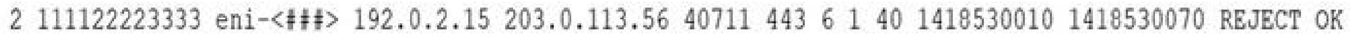
D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Configure multi-factor authentication (MFA).

Correct Answer: B

To meet the requirements of the workload, a company should store the data in an Amazon S3 Glacier vault and configure a vault lock policy for write-once, read-many (WORM) access. This will ensure that the data is stored securely and cannot be edited in the future. The other solutions (storing the data in an Amazon Elastic Block Store (Amazon EBS) volume and configuring AWS Key Management Service (AWS KMS) encryption, storing the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA) and configuring server-side encryption, or storing the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA) and configuring multi-factor authentication (MFA)) will not meet the requirements, as they do not provide a way to protect the audit logs from future edits.
https://docs.aws.amazon.com/zh_tw/AmazonS3/latest/userguide/object-lock.html

QUESTION 2

A company hosts a web application on an Amazon EC2 instance in a production VPC. Client connections to the application are failing. A SysOps administrator inspects the VPC flow logs and finds the following entry:



```
2 111122223333 eni-<###> 192.0.2.15 203.0.113.56 40711 443 6 1 40 1418530010 1418530070 REJECT OK
```

What is a possible cause of these failed connections?

A. A security group deny rule is blocking traffic on port 443.

B. The EC2 instance is shut down.

C. The network ACL is blocking HTTPS traffic.

D. The VPC has no internet gateway attached.

Correct Answer: C

QUESTION 3

A SysOps administrator migrates NAT instances to NAT gateways. After the migration, an application that is hosted on Amazon EC2 instances in a private subnet cannot access the internet. Which of the following are possible reasons for this problem? (Choose two.)

A. The application is using a protocol that the NAT gateway does not support.

B. The NAT gateway is not in a security group.

C. The NAT gateway is in an unsupported Availability Zone.

D. The NAT gateway is not in the Available state.

E. The port forwarding settings do not allow access to internal services from the internet.

Correct Answer: AD

https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-troubleshooting.html#nat-gateway-troubleshooting-no-internet-connection

QUESTION 4

A company\\'s SysOps administrator uses AWS IAM Identity Center (AWS Single Sign-On) to connect to an Active Directory. The SysOps administrator creates a new account that all the company\\'s users need to access.

The SysOps administrator uses the Active Directory Domain Users group for permissions to the new account because all users are already members of the group. When users try to log in, their access is denied.

Which action will resolve this access issue?

A. Create a new group. Add users to the new group to provide access.

B. Correct the time on the Active Directory domain controllers.

C. Remove the account. Re-add the account to the organization that is integrated with IAM Identity Center.

D. Correct the permissions on the Active Directory group so that IAM Identity Center has read access.

Correct Answer: D

QUESTION 5

A company uses AWS Organizations to manage multiple AWS accounts. Corporate policy mandates that only specific AWS Regions can be used to store and process customer data. A SysOps administrator must prevent the provisioning of

Amazon EC2 instances in unauthorized Regions by anyone in the company.

What is the MOST operationally efficient solution that meets these requirements?

A. Configure AWS CloudTrail in all Regions to record all API activity. Create an Amazon EventBridge (Amazon CloudWatch Events) rule in all unauthorized Regions for ec2:RunInstances events. Use AWS Lambda to terminate the launched EC2 instances.

B. In each AWS account, create a managed IAM policy that uses a Region condition to deny the ec2:RunInstances action in all unauthorized Regions. Attach this policy to all IAM groups in each AWS account.

C. In each AWS account, create an IAM permissions boundary policy that uses a Region condition to deny the ec2:RunInstances action in all unauthorized Regions. Attach the permissions boundary policy to all IAM users in each AWS account.

D. Create a service control policy (SCP) in AWS Organizations to deny the ec2:RunInstances action in all unauthorized Regions. Attach this policy to the root level of the organization.

Correct Answer: D

SOA-C02 VCE Dumps SOA-C02 Study Guide SOA-C02 Braindumps