SOA-C01 Q&As

AWS Certified SysOps Administrator - Associate (SOA-C01)

Pass Amazon SOA-C01 Exam with 100% Guarantee

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

https://www.pass4itsure.com/aws-sysops.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 1

A company runs an Amazon RDS MySQL DB instance. Corporate policy requires that a daily backup of the database must be copied to a separate security account.

What is the MOST cost-effective way to meet this requirement?

A. Copy an automated RDS snapshot to the security account using the copy-db-snapshotcommand with the AWS CLI.

B. Create an RDS MySQL Read Replica for the critical database in the security account, then enable automatic backups for the Read Replica.

C. Create an RDS snapshot with the AWS CLI create-db-snapshotcommand, share it with the security account, then create a copy of the shared snapshot in the security account.

D. Use AWS DMS to replicate data from the critical database to another RDS MySQL instance in the security account, then use an automated backup for the RDS instance.

Correct Answer: C

QUESTION 2

A sys admin has enabled logging on ELB. Which of the below mentioned fields will not be a part of the log file name?

A. Load Balancer IP

B. EC2 instance IP

C. S3 bucket name

D. Random string

Correct Answer: B

Explanation: Elastic Load Balancing access logs capture detailed information for all the requests made to the load balancer. Elastic Load Balancing publishes a log file from each load balancer node at the interval that the user has specified. The load balancer can deliver multiple logs for the same period. Elastic Load Balancing creates log file names in the following format: “{Bucket}/{Prefix}/AWSLogs/{AWS AccountID}/elasticloadbalancing/{Region}/{Year}/{Month}/{Day}/{AWS Account ID}_elasticloadbalancing_{Region}_{Load Balancer Name}_{End Time}_{Load Balancer IP}_ {Random String}.log“

QUESTION 3

Your customers are concerned about the security of their sensitive data and their inquiry asks about what happens to old storage devices on AWS. What would be the best answer to this question?

A. AWS uses a 3rd party security organization to destroy data as part of the decommissioning pro-cess.

B. AWS uses the techniques detailed in DoD 5220.22-M to destroy data as part of the decommis-sioning process.

C. AWS reformats the disks and uses them again.

D. AWS uses their own proprietary software to destroy data as part of the decommissioning pro-cess.

Correct Answer: B

Explanation:

When a storage device has reached the end of its useful life, AWS procedures include a decommis

sioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Oper-ating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accord-ance with industry-standard practices. Reference: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

QUESTION 4

A storage admin wants to encrypt all the objects stored in S3 using server side encryption. The user does not want to use the AES 256 encryption key provided by S3. How can the user achieve this?

A. The admin should upload his secret key to the AWS console and let S3 decrypt the objects

B. The admin should use CLI or API to upload the encryption key to the S3 bucket. When making a call to the S3 API mention the encryption key URL in each request

C. S3 does not support client supplied encryption keys for server side encryption

D. The admin should send the keys and encryption algorithm with each API call

Correct Answer: D

Explanation:

AWS S3 supports client side or server side encryption to encrypt all data at rest. The server side

encryption can either have the S3 supplied AES-256 encryption key or the user can send the key along

with each API call to supply his own encryption key. Amazon S3 never stores the user\\'s encryption key.

The user has to supply it for each encryption or decryption call.

QUESTION 5

Which of the following terms is NOT a key CloudWatch concept?

A. Namespaces

B. Units

C. Time Stamps

D. Indexes

Correct Answer: D

Explanation:

The terminology and concepts that are central to one\\'s understanding and use of Amazon Cloud-Watch are as follows: metrics, namespaces, dimensions, timestamps, units, statistics, periods, aggre-gation, alarms, and regions.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html