EXTENDED OFFER | Flat 15% OFF SITEWIDE | Use Coupon - WHIZOFFER15

🏠 > My Courses > AWS Certified Solutions Architect Associate > Objective : Elastic Block Storage >

Report

Search Courses 🔍

Objective : Elastic Block Storage

Attempt

3

Completed on

Tuesday , 01 October 2019 , 08:23 AM

Marks Obtained

5 / 5

Time Taken

00 H 01 M 34 S

Your score is

100%

Result

Pass

Mode

Exam

Domains wise Quiz Performance Report

No	1
Domain	Other
Total Question	5
Correct	5
Incorrect	0
Unattempted	0
Marked for review	0
Total	Total
All Domain	All Domain
Total Question	5
Correct	5
Incorrect	0
Unattempted	0
Marked for review	0

Review the Answers

Sorting by

Question 1   **Correct**

Domain : Other

Topic : EBS Encryption
Your company is planning to migrate to AWS and looking for encryption of sensitive data at rest. You are considering the possible options for protecting data of EBS boot volume, attached to an EC2 instance. As cloud solution architect you are exploring the options, select which one is true regarding EBS boot volume encryption?

    A.   **Do nothing as EBS volumes are encrypted by default.**

    B.   **EBS volume doesn't support boot volume so it cannot be encrypted.**

    C.   **Implement SSL for all services running on the server boot volume.**

✓   **D.**   **EBS encryption supports boot volume while copying an EBS snapshot with the encryption option.**   ✅

Explanation:

Explanation:

Correct Answer is D

Each EBS backed AMI contains references to one or more snapshots of EBS volumes. The first reference is to an image of the boot volume. The others (if present) are to snapshots of data volumes. When you launch the AMI, an EBS volume is created from each snapshot. Because EBS already supports encryption of data volumes (and by implication the snapshots associated with the volumes), you can create a single AMI with a fully-encrypted set of boot and data volumes.

Find more details here LINK:

    https://aws.amazon.com/blogs/aws/new-encrypted-ebs-boot-volumes/

Ask our Experts

Rate this Question? 🙂 🙁

Question 2   Correct

                                                                            Domain : Other

Topic : EBS Encryption
Your customer want to use Customer Master Key (CMK) for Elastic Block Stored (EBS) volume
encryption. What are true options to use Customer Master Key for EBS encryption (Choose 2 Answers).

   ✓   A.   **You cannot change the CMK that is associated with an existing snapshot or encrypted volume.**   ✓

       B.   **It is possible to change CMK for existing encrypted volume.**

       C.   **You need to always use same CMK while encrypting a copy of an unencrypted snapshot.**

   ✓   D.   **You can associate a different CMK during a snapshot copy operation so that the resulting copied**   ✓
             snapshot uses the new CMK.

Explanation:

Correct Answers are A and D

You cannot change the CMK that is associated with an existing snapshot or encrypted volume.

However, you can associate a different CMK during a snapshot copy operation (including encrypting a
copy of an unencrypted snapshot) and the resulting copied snapshot use the new CMK.

 Find more details here LINK:

     http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#EBSEncryption_key_mg

                              Ask our Experts
            Rate this Question?   ☺   ☹

Question 3   Correct

                                                                            Domain : Other

Topic : EBS Encryption
When you create an encrypted EBS volume and attach it to a supported instance type, the following
types of data are encrypted (Choose 3):

   ✓   A.   **Data at rest inside the volume.**   ✓

✓   **B.   All data moving between the volume and the instance.**   ✓

    C.   All data moving between the volume and S3.

✓   **D.   All snapshots created from the volume.**   ✓

Explanation:

Explanation :

Correct Answers are A , B and D

Amazon EBS encryption offers you a simple encryption solution for your EBS volumes without the need for you to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:

    Data at rest inside the volume

    All data moving between the volume and the instance

    All snapshots created from the volume

Find more details here LINK:

    http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#EBSEncryption_key_mg

Ask our Experts

Rate this Question?   ☺   ☹

Question 4   Correct

Domain : Other

Topic : EBS Encryption
Your customer worried about data security of launching new EC2 instance using auto scaling .
You as a AWS solution architect suggested to create encrypted AMI. Which options are true regarding encrypted volume (Choose 2 Answers).

✓   **A.   Snapshots of data volume can be encrypted and attached to an AMI.**   ✓

✓ B.   **Snapshots of root volume can be encrypted and attached to an AMI.** ✓

C.   EC2 instances with encrypted volumes can not be launched from AMIs.

D.   **Root volume can not be encrypted within AMI.**

Explanation:

Explanation :

Correct Answers are A and B

AMIs that are backed by Amazon EBS snapshots can take advantage of Amazon EBS encryption. Snapshots of both data and root volumes can be encrypted and attached to an AMI.EC2 instances with encrypted volumes are launched from AMIs in the same way as other instances.

Find more details here LINK:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIEncryption.html

---

Ask our Experts

Rate this Question? ☺ ☹

Question 5   **Correct**

Domain : Other

Topic : EBS Encryption
Your customer want to encrypt data stored in existing EBS volume. Which is true regarding EBS encrypted volume .

A.   **You can use one click option to enable existing EBS volume.**

B.   **All EBS volumes are encrypted by default so don't need to do anything.**

✓ C.   **You cannot enable encryption for an existing EBS volume.** ✓

D.   **Enable SSL and use CMK to encrypt existing EBS volume.**

Explanation:

Explanation :

Correct Answer is C

you cannot enable encryption for an existing EBS volume. Instead, you must create a new,

encrypted volume and copy the data from the old one to the new one using the file manipulation tool of your choice.

Find more details here LINK:

https://aws.amazon.com/blogs/aws/protect-your-data-with-new-ebs-encryption/

Ask our Experts

Rate this Question?   ☺ ☹

Finish Review

Certification

Cloud Certification

Java Certification

PM Certification

Big Data Certification

Company

Support

Discussions

Blog

Follow us