Quiz: Disaster Recovery, CloudFront, Storage Gateway

Chandra Lingam,

1. Your company has a single on-premises data center. For disaster recovery and for long term storage, data is regularly backed up in tapes and physically moved to a third-party offsite location.

   How can AWS Cloud help in this situation?

   A. Use Snowball Appliance for backup
   B. Use Storage Gateway as Virtual Tape Backup device
   C. Physically ship tapes to AWS for long term storage
   D. Use Storage Gateway as a Volume Gateway to seamlessly store backup in S3

2. Your customer is a small business that manages media content (videos and pictures) and data needs to be backed up in a secure offsite location.

   New content is accessed often but after few days, they are rarely accessed.

   All content needs be accessible when required

   What option would meet this need?

   A. Use AWS Storage Gateway deployed as a Volume Gateway
   B. Use AWS Storage Gateway deployed as a Tape Gateway
   C. Use AWS Storage Gateway deployed as a File Gateway
   D. Any of the above would work

3. You want to use AWS Cloud for securely backing up on-premises application data. All backed up data needs to be accessible and available even if internet connection is intermittently down.

   What solution would meet this requirement?
   A. Volume Gateway Configured as Stored Mode
   B. Volume Gateway Configured as Cached Mode
   C. File Gateway
   D. Store directly in S3

4. Your business is transitioning from on-premise systems to Cloud based systems. Your existing data is over 100 TB. You need a cost-effective mechanism to transfer all this data in to AWS Cloud. What options do you have for this initial transfer?
   A. Glacier

B. S3
C. Tape Gateway
D. Snowball Appliance

5. You are using AWS Snowball device for transferring data from your data warehouse system and prepare it for storing in Redshift database. Data is critical and you are concerned with security of your data during transfer. How is data protected?
   A. Snowball is a tamper resistant data transport solution and data is encrypted using customer specified KMS Keys
   B. Snowball is not ideal for this scenario as un-encrypted data can accessed by AWS Support Staff when importing data into AWS
   C. Snowball integrates only with S3. You cannot use Snowball for Redshift

6. You are evaluating the current Disaster Recovery procedures for an organization. Based on process and procedures, you notice that it may take up to 5 hours to restore services under a disaster scenario. What industry term is used in disaster planning to capture this information?
   A. Recovery Time Objective (RTO)
   B. Recovery Point Objective (RPO)

7. Under a disaster scenario to your primary on-site data center, Recovery Point Objective is set to 2 hours. What does this mean?
   A. It will take at least 2 hours to restore your system after a disaster strikes
   B. It will take a maximum of 2 hours to restore your system after a disaster strikes
   C. It indicates acceptable amount of data loss measured in time

8. To distribute content with CloudFront, you need application generating original content on:
   A. S3
   B. Web Servers running on AWS
   C. External web servers
   D. Any of the above

9. With CloudFront, you can distribute only static content (and not dynamically generated content)
   A. True
   B. False

10. CloudFront service can be used for:
   A. Public content
   B. Private content
   C. Public and Private content

11. You want to distribute content in a S3 bucket using CloudFront edge locations. You also want to restrict access to only the users who are authorized by your application. How can you accomplish this?
    A. Configure content to be accessible only using signed URLs or Signed cookies in CloudFront
    B. Create a CloudFront user known as Origin Access Identity (OAI) and Grant read access to S3 bucket for OAI identity
    C. Remove permissions for anyone else to access your S3 bucket
    D. All the above

Answers:

1. B - The Tape Gateway presents itself to your existing backup application as an industry-standard iSCSI-based virtual tape library (VTL), consisting of a virtual media changer and virtual tape drives. You can continue to use your existing backup applications and workflows while writing to a nearly limitless collection of virtual tapes. Each virtual tape is stored in Amazon S3. Snowball is used for transferring multi-peta byte data to Cloud (usually during Cloud migration). AWS does not support physical storage of tapes. Volume Gateway is not the right gateway for this requirement. Ref: https://aws.amazon.com/storagegateway/features/
2. C – Storage Gateway configured as a File Gateway would meet this requirement. The file gateway allows you to cost-effectively and durably store large files and media assets on AWS. Local applications also benefit from a low-latency local cache of frequently used content. The result is tiered, hybrid cloud content storage, which can be accessed easily by on-premises applications via NFS or SMB. Tape Gateway is for large backup. Volume gateway is suitable when you need a block storage device. In this case, we need to store and access individual files. https://aws.amazon.com/storagegateway/file/
3. A – Volume Gateway offers two modes: Cached and Stored Mode. In cached mode, primary data store is S3 and frequently accessed data is cached locally. With this mode, you can achieve substantial cost savings on primary storage, minimizing the need to scale your storage on-premises, while retaining low-latency access to your frequently accessed data. However, in this mode, your data is not accessible if internet access is down. In stored mode, you store your entire data set locally, while making an asynchronous copy of your volume in Amazon S3 and point-in-time EBS snapshots. This mode provides durable and inexpensive offsite backups that you can recover locally, to another site or in Amazon EC2. File Gateway caches only frequently accessed data and primary storage is S3.
4. D - Snowball offers convenient way to transfer large amount of data by physically shipping the data using secure snowball appliance. Snowball is a petabyte-scale data transport solution that uses devices designed to be secure to transfer large amounts of data into and out of the AWS Cloud. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. Ref: https://aws.amazon.com/snowball/
5. A - Snowball offers convenient way to transfer large amount of data by physically shipping the data using secure snowball appliance. Data is imported to S3 and from there you can load it to Redshift or any other system. Only customer can access unencrypted data as data is encrypted using customer specified master keys.
6. A - Recovery Time Objective captures time it takes to restore business process after a disaster

7. C - Recovery Point Objective indicates acceptable amount of data loss measured in time. If disaster strikes at time T, if RPO is 2 hours, then you have process and procedures in place to restore the systems as it appeared at T-2.
8. D – CloudFront Origin Server can be S3 or AWS hosted Webservers or even external web servers.
9. B - CloudFront can be used to distribute both static and dynamically generated content
10. C - Amazon CloudFront has an optional private content feature. When this option is enabled, Amazon CloudFront will only deliver files when you say it is okay to do so by securely signing your requests.
11. D – You would need to perform all the steps to prevent unauthorized content access