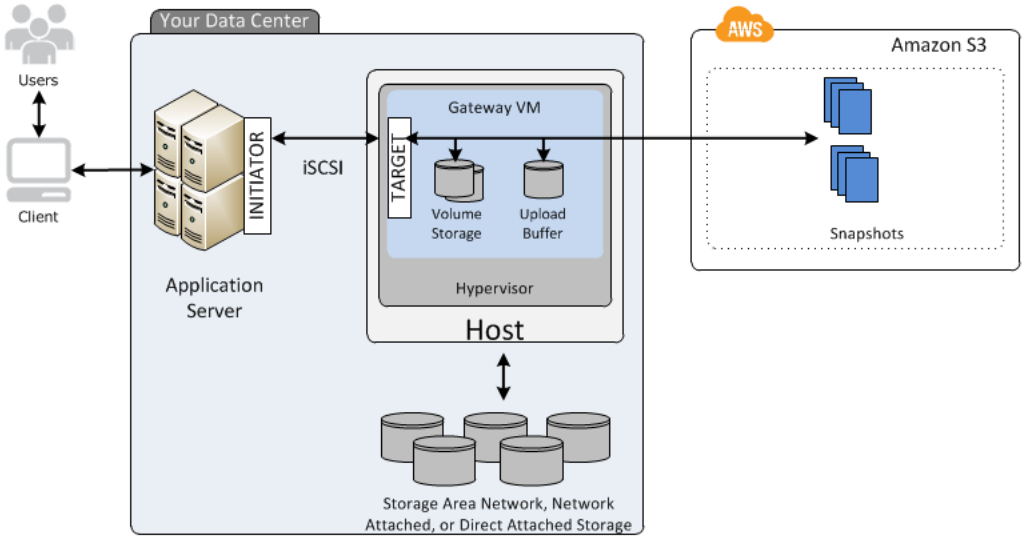
AWS - Storage Gateway

- AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure.
- You can use the service to store data in the AWS Cloud for scalable and cost-effective storage that helps maintain data security.
- **Volume Gateway** Based option uses Internet SCSI protocol **(Internet Small Computer System Interface (iSCSI))**



File Gateway –

- A file gateway supports a file interface into Amazon Simple Storage Service (Amazon S3) and combines a service and a virtual software appliance.
- By using this combination, you can store and retrieve objects in Amazon S3 using industry-standard file protocols such as Network File System (NFS) and Server Message Block (SMB).
- The software appliance, or gateway, is deployed into your on-premises environment as a virtual machine (VM) running on VMware ESXi, Microsoft Hyper-V, or Linux Kernel-based Virtual Machine (KVM) hypervisor. The gateway provides access to objects in S3 as files or file share mount points.
- A file gateway simplifies file storage in Amazon S3, integrates to existing applications through industry-standard file system protocols, and provides a cost-effective alternative to on-premises storage.
- It also provides low-latency access to data through transparent local caching. A file gateway manages data transfer to and from AWS, buffers applications from network congestion, optimizes and streams data in parallel, and manages bandwidth consumption

Volume Gateway –

- A volume gateway provides cloud-backed storage volumes that you can mount as Internet Small Computer System Interface (iSCSI) devices from your on-premises application servers

- The volume gateway is deployed into your on-premises environment as a VM running on VMware ESXi, KVM, or Microsoft Hyper-V hypervisor.
- The gateway supports the following volume configurations:
- **Cached volumes** –
  - You store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally.
  - Cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on-premises.
  - You also retain low-latency access to your frequently accessed data.
- **Stored volumes** –
  - If you need low-latency access to your entire dataset, first configure your on-premises gateway to store all your data locally.
  - Then asynchronously back up point-in-time snapshots of this data to Amazon S3.
  - This configuration provides durable and inexpensive offsite backups that you can recover to your local data center or Amazon Elastic Compute Cloud (Amazon EC2).
  - For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2.

SCENARIO

By using cached volumes, you can use Amazon S3 as your primary data storage, while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to frequently accessed data. You can create storage volumes up to 32 TiB in size and afterwards, attach these volumes as iSCSI devices to your on-premises application servers. When you write to these volumes, your gateway stores the data in Amazon S3. It retains the recently read data in your on-premises storage gateway's cache and uploads buffer storage.

Cached volumes can range from 1 GiB to 32 TiB in size and must be rounded to the nearest GiB. Each gateway configured for cached volumes can support up to 32 volumes for a total maximum storage volume of 1,024 TiB (1 PiB).

In the cached volumes solution, AWS Storage Gateway stores all your on-premises application data in a storage volume in Amazon S3. Hence, the correct answer is ***Cached Volume Gateway***.

References:

https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html#volume-gateway-concepts

https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

Tape Gateway –

- A tape gateway provides cloud-backed virtual tape storage. The tape gateway is deployed into your on-premises environment as a VM running on VMware ESXi, KVM, or Microsoft Hyper-V hypervisor.

- With a tape gateway, you can cost-effectively and durably archive backup data in GLACIER or DEEP_ARCHIVE.
- A tape gateway provides a virtual tape infrastructure that scales seamlessly with your business needs and eliminates the operational burden of provisioning, scaling, and maintaining a physical tape infrastructure.
- You can run AWS Storage Gateway either on-premises as a VM appliance, as a hardware appliance, or in AWS as an Amazon EC2 instance.
- You deploy your gateway on an EC2 instance to provision iSCSI storage volumes in AWS.
- You can use gateways hosted on EC2 instances for disaster recovery, data mirroring, and providing storage for applications hosted on Amazon EC2.
- For an architectural overview, see How AWS Storage Gateway Works (Architecture). To see the wide range of use cases that AWS Storage Gateway helps make possible, see AWS Storage Gateway.

LIMITS - File Gateway

Description	File Gateway
Maximum number of file shares per Amazon S3 bucket. There is a one-to-one mapping between a file share and an S3 bucket	1
Maximum number of file shares per gateway	10
The maximum size of an individual file, which is the maximum size of an individual object in S3	5 TB

LIMITS - Storage VOLUMES

Description	Cached Volumes	Stored Volumes
Maximum size of a volume	32 TiB	16 TiB
Maximum number of volumes per gateway	32	32
Total size of all volumes for a gateway	1,024 TiB	512 TiB

LIMITS - TAPES

Description	Tape Gateway
Minimum size of a virtual tape	100 GiB
Maximum size of a virtual tape	2.5 TiB
Maximum number of virtual tapes for a VTL	1,500
Total size of all tapes in a VTL	1 PiB
Maximum number of virtual tapes in archive	No limit
Total size of all tapes in a archive	No limit

Disaster Recovery - STORAGE GATEWAY

Since this uses a Volume Storage Gateway, you have to generate an EBS Volume to restore the data. Hence, the following option is correct:

1. Deploy the Oracle database and the NGINX app server on an EC2 instance.

2. Restore the Recovery Manager (RMAN) Oracle backups from an Amazon S3 bucket.

3. Generate an EBS volume of static content from the Storage Gateway and attach it to the NGINX EC2 server.

Amazon RDS does not use RMAN for backups, you can use the package to execute RMAN validation commands against the database, control file, SPFILE, tablespaces, or data files.

The volume gateway provides block storage to your applications using the iSCSI protocol. Data on the volumes are stored in Amazon S3. To access your iSCSI volumes in AWS, you can take EBS snapshots which can be used to create EBS volumes.

Reference:

https://aws.amazon.com/storagegateway/faqs/

Check out this AWS Storage Gateway Cheat Sheet:

https://tutorialsdojo.com/aws-cheat-sheet-aws-storage-gateway/

Tutorials Dojo's AWS Certified Solutions Architect Professional Exam Study Guide:

https://tutorialsdojo.com/aws-cheat-sheet-aws-certified-solutions-architect-professional/

Reference:

http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html

Check out this AWS Storage Gateway Cheat Sheet:

https://tutorialsdojo.com/aws-cheat-sheet-aws-storage-gateway/

Tutorials Dojo's AWS Certified Solutions Architect Associate Exam Study Guide:

https://tutorialsdojo.com/aws-cheat-sheet-aws-certified-solutions-architect-associate/