

AWS Storage Gateway FAQs

General

Q: What is the AWS Storage Gateway service?

The AWS Storage Gateway service enables hybrid storage between on-premises environments and the AWS Cloud. It seamlessly integrates on-premises enterprise applications and workflows with Amazon's block and object cloud storage services through industry standard storage protocols. It provides low-latency performance by caching frequently accessed data on premises, while storing data securely and durably in Amazon cloud storage services. It provides an optimized data transfer mechanism and bandwidth management, which tolerates unreliable networks and minimizes the amount of data being transferred. It brings the security, manageability, durability, and scalability of AWS to existing enterprise environments through native integration with AWS encryption, identity management, monitoring, and storage services. Typical use cases include backup and archiving, disaster recovery, moving data to S3 for in-cloud workloads, and tiered storage.

AWS Storage Gateway supports three storage interfaces: file, volume, and tape. Each gateway you have can provide one type of interface.

The *file gateway* enables you to store and retrieve objects in Amazon S3 using file protocols, such as NFS. Objects written through file gateway can be directly accessed in S3.

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

The *tape gateway* provides your backup application with an iSCSI virtual tape library (VTL) interface, consisting of a virtual media changer, virtual tape drives, and virtual tapes. Virtual tape data is stored in Amazon S3 or can be archived to Amazon Glacier.

Q: How do I use the AWS Storage Gateway service?

You can have two touchpoints to use the service: the AWS Management Console and a gateway virtual machine (VM).

You use the AWS Management Console to download the gateway, configure storage, and manage and monitor the service. The gateway connects your applications to AWS storage by providing standard storage interfaces. It

provides transparent caching, efficient data transfer, and integration with AWS monitoring and security services.

To get started, sign up for the AWS Storage Gateway by choosing “Sign Up Now” on the [AWS Storage Gateway detail page](#). To sign-up, you must have an Amazon Web Services account; if you don't already have one, you are prompted to create one when you begin the AWS Storage Gateway sign-up process.

After you sign up, you visit the AWS Storage Gateway Management Console to download a gateway with a file, volume, or tape interface. Once you've downloaded and installed your gateway, you associate it with your AWS Account through our activation process. After activation, you configure the gateway to connect to the appropriate storage type. For file gateway, you configure file shares that are mapped to selected S3 buckets, using IAM roles. For volume gateway, you create and mount volumes as iSCSI devices. For tape gateway, you connect your backup application to create and manage tapes. Once configured, you start using the gateway to write and read data to and from AWS storage. You can monitor the status of your data transfer and your storage interfaces through the AWS Management Console. Additionally, you can use the API or SDK to programmatically manage your application's interaction with the gateway.

Q: What is file gateway?

File gateway provides a virtual file server, which enables you to store and retrieve Amazon S3 objects through standard file storage protocols. File gateway allows your existing file-based applications or devices to use secure and durable cloud storage without needing to be modified. With file gateway, your configured S3 buckets will be available as Network File System (NFS) mount points. Your applications read and write files and directories over NFS, interfacing to the gateway as a file server. In turn, the gateway translates these file operations into object requests on your S3 buckets. Your most recently used data is cached on the gateway for low-latency access, and data transfer between your data center and AWS is fully managed and optimized by the gateway. Once in S3, you can access the objects directly or manage them using features such as S3 Lifecycle Policies, object versioning, and cross-region replication. You can run file gateway on-premises or in EC2.

Q: What is volume gateway?

Volume gateway provides an iSCSI target, which enables you to create volumes and mount them as iSCSI devices from your on-premises or EC2 application servers. The volume gateway runs in either a cached or stored mode.

- In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access.
- In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up

to AWS.

In either mode, you can take point-in-time snapshots of your volumes and store them in Amazon S3, enabling you to make space-efficient versioned copies of your volumes for data protection and various data reuse needs.

Q: What is tape gateway?

Tape gateway presents your backup application with a virtual tape library (VTL) interface, consisting of a media changer and tape drives. You can create virtual tapes in your virtual tape library using the AWS Management Console. Your backup application can read data from or write data to virtual tapes by mounting them to virtual tape drives using the virtual media changer. Virtual tapes are discovered by your backup application using its standard media inventory procedure. Virtual tapes are available for immediate access and are backed by Amazon S3. You can also archive tapes. Archived tapes are stored in Amazon Glacier.

Q: What benefits does AWS Storage Gateway provide?

AWS Storage Gateway provides a set of features that enable you to effectively leverage AWS storage within your existing applications and workflows. It provides a standard set of protocols such as iSCSI and NFS, which allow you to use your existing applications without any changes. Through its local cache, the gateway provides low-latency access to frequently used data. The gateway optimizes data transfer to AWS storage, such as optimization of transfer through intelligent buffering, upload management to address network variations, and bandwidth management. The gateway provides you an effective mechanism to store data in AWS across the range of storage services most suitable for your use cases. The gateway is easy to deploy and leverages your existing virtual infrastructure investments and integrates with native hypervisors. The gateway is stateless, allowing you to easily create and manage new instances of your gateway as your storage needs evolve. Finally, it integrates natively into AWS management services such as Amazon CloudWatch, AWS CloudTrail, AWS KMS, and IAM.

[Back to Top](#)

File Gateway

Q: What is file gateway?

File gateway provides a virtual on-premises file server, which enables you to store and retrieve Amazon S3 objects through standard file storage protocols.

Q: What can I do with file gateway?

The use cases for file gateway include: (a) ingesting file-based data into S3 for object workloads, (b) "cloud-bursting", where you can move data to AWS, run a workload, and access results within your on-premises application, (c) migrating

file to objects in S3, (d) cost-effective storage for backup and archive, (f) disaster recovery, and (g) tiering on-premises file storage to S3.

Q: What are the benefits of using file gateway to store data in S3?

File gateway enables your existing file-based applications, devices, and workflows to use cloud storage without modification. File gateway securely and durably stores both file contents and metadata as objects in your Amazon S3 buckets using standard file protocols.

Q: What protocols are supported? Can I use Microsoft Windows?

File gateway supports clients connecting to the gateway using NFS v3 and v4.1. Microsoft Windows clients that support NFS v3 can connect to file gateway.

Q: How do I create and configure a file share?

You can create a file share using the AWS Management Console or service API, and associate it with a new or existing S3 bucket. You can configure your file share with administrative controls such as limiting access to specific NFS clients or networks, read-only or read-write, or enabling user permission squashing.

Q: How does file gateway access my S3 bucket?

File gateway uses an AWS Identity and Access Management (IAM) role to access your S3 bucket. You can set this up yourself, or have it automatically setup by the AWS Storage Gateway Management Console. For automatic setup, AWS Storage Gateway will create a new IAM role in your account and associate it with an IAM Access Policy to access your S3 bucket. The IAM role and IAM access policy are created in your account and you can fully manage them yourself.

Q: How does my application access my file share?

To use the file share, you mount it from your application using standard UNIX or Windows commands. For convenience, example command lines are shown in the management console

Q: What is the relationship between files and objects?

Files are stored as objects in your S3 buckets and you can configure the initial storage class for objects that file gateway creates. There is a one-to-one relationship between files and objects, and you can configure the initial storage class for objects that file gateway creates.

The object key is derived from the file path within the file system. For example, if you have a gateway with hostname *file.amazon.com* and have mapped *my-bucket*, then file gateway will expose a mount point called *file.amazon.com:/export/my-bucket*. If you then mount this locally on */mnt/my-bucket* and create a file named *file.html* in a directory */mnt/my-bucket/dir* this file will be stored as an object in the bucket *my-bucket* with a key of *dir/file.html*.

Q: What file system operations are supported by file gateway?

Your NFS client can create, read, update, and delete, files and directories. Files are stored as individual objects in S3. Directories are managed as folder objects in S3, using the same syntax as the S3 console.

Symbolic links and hard links are not supported. Attempting to create a link will result in an NFS error. Creating sparse files will result in a non-sparse zero-filled object in S3.

Rename operations will appear atomic to NFS clients, but S3 does not support renaming of objects. When you rename a file or directory the gateway performs copy-put requests to create a copy of the objects in S3 under the new keys and then deletes the originals. This avoids having to re-send large files over the network. Renaming directories containing a large number of files is not instantaneous and will result in 2 copies of your data being stored in S3 until the rename operation completes.

Q: What file system metadata can my NFS client access?

Your NFS client can access file system metadata including ownership, permissions, and timestamps, for files and directories. Ownership, permissions, and timestamps, are durably stored in S3 in the user-metadata of the object associated with the file. You can configure default ownership and permissions for objects which were stored in the S3 bucket directly, not by file gateway.

Q: Can I use multiple NFS clients with a single file gateway?

You can have multiple NFS clients accessing a single file gateway. However, as with any NFS server, concurrent modification from multiple NFS clients can lead to unpredictable behavior. Application level coordination is required to do this in a safe way.

Q: Can I have multiple writers to my S3 bucket?

No. We recommend a single writer to objects in your S3 bucket. If you directly overwrite or update an object previously written by file gateway, it results in undefined behavior when the object is accessed through the file share. Concurrent modification of the same object (e.g. via the S3 API and the file gateway) can lead to unpredictable results and we recommend against this configuration.

Q: Can I have two gateways writing independent data to the same bucket?

We do not recommend configuring multiple writers to a single bucket because it can lead to unpredictable results. You could enforce unique object names or prefixes through your application workflow. File gateway doesn't monitor or report on conflicts in such a setup.

Q: Can I have multiple gateways reading data from the same bucket?

Yes, you can have multiple readers on a bucket managed through a file gateway. You can configure a file share as read-only, and allow multiple gateways to read objects from the same bucket. Additionally, you can refresh

the inventory of objects that your gateway knows about using the [RefreshCache API](#).

Note however that if you do not configure a file share as read-only, file gateway does not monitor or restrict these readers from inadvertently writing to the bucket. It is up to you to maintain a single writer/multi reader configuration from your application.

Q: How do I know when my file is uploaded?

You must poll your objects to make sure they are completely uploaded. Note that just checking the length of the file might not be sufficient because it is likely that you have an intermediate object that has the same length as the final object.

Q: What if my bucket already contains objects?

If your bucket already contains objects when you configure it for use with file gateway, they will appear as files to NFS clients. The files are given default file system metadata. These defaults are configurable.

To reduce latency and S3 requests, file gateway only scans the object headers when you explicitly list the files or directories. Data is downloaded only when the entire object is read.

Q: Can I detect new objects created in my S3 bucket after the file share has been created (e.g. created from an object-based workload)?

You can refresh the inventory of objects that your gateway knows about using the [RefreshCache API](#) and console action.

Q: Can I directly access objects stored in S3 by using file gateway?

Yes. Once objects are stored in S3, you can access them directly in AWS for in-cloud workloads without requiring file gateway. Your objects inherit the properties of the S3 bucket in which they are stored, such as lifecycle management, and cross-region replication.

An object that needs to be accessed by using a file share should only be managed by the gateway. If you directly overwrite or update an object previously written by file gateway, it results in undefined behavior when the object is accessed through the file share.

Q: How many file shares can I create per bucket?

There is a one-to-one mapping between a file share and a bucket. We do not limit the number of file shares per bucket. However, we recommend having a single writer to the bucket, either a file gateway or client accessing S3 directly.

Q: How many file shares can I create per gateway?

You can create up to 10 file shares per gateway.

Q: What is the maximum size of an individual file?

The maximum size of an individual file is 5 TB, which is the maximum size of an individual object in S3. If you write a file larger than 5 TB, you will get a "file too large" error message and only the first 5 TB of the file will be uploaded.

Q: My application checks storage size before copying data. What storage size does the gateway return?

The gateway returns a large number (8 EB) as your total capacity. Amazon S3 does not limit total storage.

Q: Can I use versioning, lifecycle, cross-region replication, and S3 event notification?

Yes. Your bucket policies for versioning, lifecycle management, cross-region replication, and S3 event notification, apply directly to objects stored in your bucket through AWS Storage Gateway.

You can use S3 lifecycle policies to change an object's storage tier or delete old objects or object versions. In the case of objects deleted by lifecycle policy, you will need to call the [RefreshCache API](#) to reflect these changes to your NFS clients.

When using an S3 bucket which is the target for cross-region replication, you may need to use the [RefreshCache API](#) to ensure the gateway cache and S3 bucket are in sync.

If using S3 event notifications you may receive events for partial files created by the gateway to ensure your data is durably stored in S3. Partial files occur for a number of reasons, such as the gateway needing to free up cache space or . These partial files may not be application consistent.

Q: Can I read and write files directly to Amazon Glacier?

Your bucket lifecycle policies will enable you to move files to Amazon Glacier. If you read a file that is in Amazon Glacier, you will receive a generic I/O error.

Q: Can I use file gateway with my backup application?

File gateway supports NFS v3 and v4.1 clients. We are continuing to do on-going testing with common backup apps. Please provide us specific apps you'd like to see compatibility with.

Q: Can I use file gateway to write files to EFS?

No. File gateway allows you to write files as objects in S3.

Q: When should I use file gateway vs. the S3 API?

You can use file gateway when you want to access objects in S3 as files using standard filesystem operations. File gateway additionally provides low-latency local access and efficient data transfer. You can use the S3 API when your application doesn't require file system operations and can manage data transfer directly.

Q: How does file gateway manage the local cache? What data gets stored locally?

Local disk storage on the gateway is used to temporarily hold changed data that needs to be transferred to AWS, and to locally cache data for low-latency read access. File gateway automatically manages the cache maintaining the most recently accessed data based on NFS client read and write operations. Data is evicted from the cache only when space is needed to store more recently used data.

To maximize write performance, the gateway uses a write-back mechanism where data is first persisted to disk and then asynchronously uploaded to S3. The gateway serves data from the local cache to maximize read performance. If not present, data is efficiently synchronously fetched from Amazon S3 using byte-range gets.

The local cache should generally be sized for the working set of data that you need low-latency access to. If the cache is too small then read latencies will increase as data being requested must be fetched from S3, and writes could fail if there is no free cache space to store data locally pending upload to S3.

Q: Does file gateway perform data reduction (deduplication or compression)?

No. Files are mapped to objects one-to-one in your bucket without modification, enabling you to access your data directly in S3 without needing to use the gateway or deploy additional software to rehydrate your data.

File gateway uses multipart uploads and copy put, so only changed data is uploaded to S3 which can reduce data transfer. The gateway does not automatically download full objects or all the data that exists in your bucket; data is only downloaded when explicitly accessed by your NFS client.

Q: Can I use file gateway with Amazon S3 Transfer Acceleration?

If your bucket is configured for S3 Transfer Acceleration, file gateway will not use the accelerated endpoints.

Q: How does file gateway read and write my S3 bucket?

File gateway uses an IAM role to access your S3 bucket. You can create this role yourself, or use the automated mechanism provided in the AWS Management Console. For automatic role creations, file gateway will create a new IAM role in your account and associate this role with an IAM access policy to access your S3 bucket. The IAM role and IAM access policy are created in your account, and you can fully manage them.

Q: What sort of encryption does file gateway use to protect my data?

All data transferred between the gateway and AWS storage is encrypted using SSL. By default, all data stored in S3 is encrypted server-side with Amazon S3-Managed Encryption Keys (SSE-S3). For each file share you can optionally

configure to have your objects encrypted with AWS KMS-Managed Keys using SSE-KMS

[Back to Top](#)

Volume Gateway

Q: What is the relation between the volume gateway and previously available gateway-cached and gateway-stored modes?

The volume gateway represents the family of gateways that support block-based volumes, previously referred to as gateway-cached and gateway-stored modes.

In the cached volume mode, your data is stored in Amazon S3 and a cache of the frequently accessed data is maintained locally by the gateway. With this mode, you can achieve cost savings on primary storage, and minimize the need to scale your storage on-premises, while retaining low-latency access to your most used data.

In the stored volume mode, data is stored on your local storage with volumes backed up asynchronously as Amazon EBS snapshots stored in Amazon S3. This provides durable and inexpensive off-site backups. You can recover these backups locally to your gateway or in-cloud to Amazon EC2, for example, if you need replacement capacity for disaster recovery.

Q: How much volume data can I manage per gateway? What is the maximum size of a volume?

Each *volume gateway* can support up to 32 volumes. In *cached mode*, each volume can be up to 32 TB for a maximum of 1 PB of data per gateway (32 volumes, each 32 TB in size). In *stored mode*, each volume can be up to 16 TB for a maximum of 512 TB of data per gateway (32 volumes, each 16 TB in size).

Volume gateways compress data before that data is transferred to AWS and while stored in AWS. This compression can reduce both data transfer and storage charges. Volume storage is not pre-provisioned; you will be billed for only the amount of data stored on the volume, not the size of the volume you create.

Q: When I look in Amazon S3 why can't I see my volume data?

Your volumes are stored in Amazon S3 and accessible through AWS Storage Gateway. You cannot directly access them by using Amazon S3 API actions. You can take point-in-time snapshots of gateway volumes that are made available in the form of Amazon EBS snapshots. Use the file interface to work with your data natively in S3.

Q: Why would I use snapshots?

You can take point-in-time snapshots of your volume gateway volumes in the form of Amazon EBS snapshots. You can use a snapshot of your volume as the starting point for a new Amazon EBS volume, which you can then attach to an Amazon EC2 instance. Using this approach, you can easily supply data from your on-premises applications to your applications running on Amazon EC2 if you require additional on-demand compute capacity for data processing or replacement capacity for disaster recovery purposes.

For cached volumes, where your volume data is already stored in Amazon S3, you can use snapshots to preserve versions of your data. Using this approach, you can revert to a prior version when required or repurpose a point-in-time version as a new volume. You can initiate snapshots on a scheduled or ad hoc basis. When taking a new snapshot, only the data that has changed since your last snapshot is stored. If you have a volume with 100 GB of data, but only 5 GB of data have changed since your last snapshot, only the 5 additional GB of snapshot data will be stored in Amazon S3. When you delete a snapshot, only the data not needed for any other snapshot is removed.

For stored volumes, where your volume data is stored on-premises, snapshots provide durable, off-site backups in Amazon S3. You can create a new volume from a snapshot if you need to recover a backup. You can also use a snapshot of your volume as the starting point for a new Amazon EBS volume which you can then attach to an Amazon EC2 instance.

Q: What data will my snapshot contain? How do I know when to take a snapshot to ensure my data is backed up?

Snapshots represent a point-in-time copy of the volume at the time the snapshot is requested. They contain all of the information needed to restore your data (from the time the snapshot was taken) to a new volume. Data written to the volume by your application prior to taking the snapshot, but not yet been uploaded to AWS, will be included in the snapshot.

In practical terms, the snapshot will be assigned an ID and visible in the AWS Management Console and AWS Command Line Interface (AWS CLI) immediately, but will initially be in a PENDING status. When all data written to the volume prior to the snapshot request has been uploaded from the gateway and into EBS, the status will change to AVAILABLE. At this point you can use the snapshot as the base for a new gateway or EBS volume.

Q: How do I restore a snapshot to a gateway?

Each snapshot is given a unique identifier that you can view using the AWS Management Console. You can create AWS Storage Gateway or Amazon EBS volumes based on any of your existing snapshots by specifying this unique identifier.

Using the AWS Management Console, you can create a new volume from a snapshot you've stored in Amazon S3. You can then mount this volume as an iSCSI device to your on-premises application server.

Because cached volumes store your primary data in Amazon S3, when creating a new volume from a snapshot, your gateway keeps the snapshot data in Amazon S3 where it becomes the primary data for your new volume.

Because stored volumes store your primary data locally, when creating a new volume from a snapshot, your gateway downloads the data contained within the snapshot to your local hardware. There it becomes the primary data for your new volume.

Q: Do the AWS Storage Gateway's volumes need to be un-mounted in order to take a snapshot? Does the snapshot need to complete before the volume can be used again?

No, taking snapshots does not require you to un-mount your volumes, nor does it impact your application's performance. However, snapshots only capture data that has been written to your AWS Storage Gateway volume, which may exclude any data that has been locally buffered by your application or OS.

Q: Can I schedule snapshots of my AWS Storage Gateway volumes?

Yes, you can create a snapshot schedule for each of your volumes. You can modify both the time the snapshot occurs each day, as well as the frequency (every 1, 2, 4, 8, 12, or 24 hours).

Q: How long does it take to complete a snapshot?

The time it takes to complete a snapshot is largely dependent upon the size of your volume and the speed of your Internet connection to AWS. The AWS Storage Gateway compresses all data prior to upload, reducing the time to take a snapshot.

Q: Will I be able to access my snapshot data using Amazon S3's APIs?

No, snapshots are only accessible from the AWS Storage Gateway and Amazon EBS and cannot be directly accessed using Amazon S3 APIs.

Q: What are the snapshot limits per gateway?

There are no limits to the number of snapshots or the amount of snapshot data a single gateway can produce.

[Back to Top](#)

Tape Gateway

Q: How much data can I store on a virtual tape?

When creating virtual tapes, you select one of the following sizes: 100 GB, 200 GB, 400 GB, 800 GB, 1.5 TB, and 2.5 TB.

Q: How many tapes can the virtual tape library (VTL) hold?

A tape gateway can have up to 1,500 virtual tapes with a maximum aggregate capacity of 1 PB.

Q: How much data can I store in tape archives?

There is no limit to the amount or size of virtual tapes that you can archive.

Q: How do I access my data on virtual tapes?

The virtual tape containing your data must be stored in a virtual tape library before it can be accessed. Access to virtual tapes in your virtual tape library is instantaneous. If the virtual tape containing your data is archived, you can retrieve the virtual tape using the AWS Management Console. First select the virtual tape, then choose the virtual tape library into which you want the virtual tape to be loaded. It takes about 24 hours for the retrieved virtual tape to be available in the selected virtual tape library. Once the virtual tape is available in the virtual tape library, you can use your backup application to make use of the virtual tape to restore data.

Q: What backup applications can I use with tape gateway?

The VTL interface is compatible with backup and archival applications that use the industry-standard iSCSI-based tape library interface. For a full list of the supported backup applications see the requirements section of the AWS Storage Gateway user guide.

Q: Will I be able to access the virtual tapes in my virtual tape library using Amazon S3 or Amazon Glacier APIs?

No. You cannot access virtual tape data using Amazon S3 or Amazon Glacier APIs. However, you can use the tape gateway APIs to manage your virtual tape library and your virtual tape shelf.

[Back to Top](#)

Performance, Monitoring, and Maintenance

Q: What performance can I expect?

Because the AWS Storage Gateway VM sits between your application and Amazon storage, the performance you experience depends upon a number of factors. These include the network bandwidth between your iSCSI initiator or NFS client and gateway, the speed and configuration of your underlying local disks, the configuration of your VM, the amount of local storage allocated to your gateway, and the bandwidth between your gateway and Amazon storage.

Our technical documentation provides guidance on how to optimize your environment setup for best performance.

Q: What are the minimum hardware and software requirements for the AWS Storage Gateway?

For these see the requirements section in the AWS Storage Gateway User Guide.

Q: Can I use the AWS Storage Gateway with AWS Direct Connect?

Yes, you can use AWS Direct Connect to increase throughput and reduce your network costs by establishing a dedicated network connection between your on-premises gateway and AWS. Note that the AWS Storage Gateway efficiently uses your Internet bandwidth to help speed up the upload of your on-premises application data to AWS.

Q: Can I route my AWS Storage Gateway Internet traffic through a local proxy server?

Yes. Volume and tape gateways support configuration of a Socket Secure version 5 (SOCKS5) proxy between your on-premises gateway and AWS. File gateways support configuration of an HyperText Transfer Protocol (HTTP) proxy.

Q: What type of data reduction does AWS Storage Gateway perform?

Volume and tape gateways perform compression of data in-transit and at-rest which can reduce both data transfer and storage charges. The AWS Storage Gateway only uploads data that has changed, minimizing the amount of data sent over the Internet.

Q: Does the AWS Storage Gateway support bandwidth throttling?

Yes, using the AWS Management Console you can restrict the bandwidth between your tape and volume gateway and AWS based on a rate that you provide. You can specify individual rates for inbound and outbound traffic.

Q: How do I monitor my gateway?

You can use [Amazon CloudWatch](#) to monitor the [performance metrics for your gateway](#), giving you insight into storage, bandwidth, throughput, and latency. These metrics are accessible directly from CloudWatch; or by following links in the AWS Storage Gateway Console, which take you directly to the CloudWatch metrics for the resource being viewed. Please refer to the [CloudWatch](#) details and pricing pages for additional information.

Q: How can I measure the cache performance of my gateway?

You can use Amazon CloudWatch metrics including CachePercentDirty, CacheHitPercent, CacheFree, and CachePercentUsed. These can be viewed by following the Monitoring link on the gateway details tab in the AWS Storage Gateway Console.

Q: How can I measure the bandwidth used by my gateway?

You can use Amazon CloudWatch metrics including CloudBytesUploaded and CloudBytesDownloaded.

Q: How does the AWS Storage Gateway manage updates?

AWS Storage Gateway periodically deploys important updates and software patches to your gateway virtual machine (VM). You can configure a weekly maintenance schedule allowing you to control when these updates will be applied to your gateway. Alternatively, you can apply updates manually when they are made available, either through the [AWS Storage Gateway Console](#) or API. Updates should take only a few minutes to complete. For more information, please visit the [Managing Gateway Updates](#) section of our documentation.

[Back to top](#)

Billing

Q: How will I be billed for my use of AWS Storage Gateway?

There are 3 elements to how you will be billed for AWS Storage Gateway: storage, requests, and data transfer. For detailed pricing information, please visit the [AWS Storage Gateway Pricing](#) page.

Q: How will I be charged for file storage when using a file gateway?

File gateways store data directly in Amazon S3. You are billed by Amazon S3 for the objects stored and requests made by your file gateway. For more information, please visit the [Amazon S3 Pricing](#) page.

Q: How will I be charged for volume or virtual tape storage when using a volume or tape gateway?

You are billed for the amount of volume and virtual tape data you store in AWS. This fee is prorated daily and prices vary by region. You are only billed for the portion of volume or virtual tape capacity that you use, not for the provisioned size of the resource. All volume and virtual tape data is compressed before it is transferred to AWS by the gateway, which can reduce your storage charges. For detailed pricing information, please visit the [AWS Storage Gateway Pricing](#) page.

Q: How will I be charged for EBS snapshots taken from my AWS Storage Gateway volumes?

EBS snapshots taken from your Storage Gateway volumes are stored and billed by Amazon EBS. When taking a new snapshot only the data that has changed since your last snapshot is stored to reduce your storage charges. For more information, please visit the [Amazon EBS Pricing](#) page.

Q: How will I be charged for reading and writing data?

When your gateway writes data to AWS you will be charged at a flat rate of \$0.01 per GB of data written to AWS up to a monthly maximum of no more than \$125 per gateway. There is no charge for reading data from AWS. Since the gateway performs caching, bandwidth optimization, and, for volume and tape gateways, compression, the amount of data written to AWS may be less than the amount of data written to the gateway by your application. You can

monitor the amount of data written by your gateway to AWS through the provided [Amazon CloudWatch](#) metrics and you can [configure bandwidth limits](#) on your gateway to manage your costs.

Q: How will I be charged when retrieving data an archived virtual tape?

You are charged when retrieving a virtual tape that has been archived at a flat rate of \$0.01 per GB of data stored on the tape. For example, retrieving 5 tapes that contain 100 GB each would cost $5 \times 100\text{GB} \times \$0.01 = \$5.00$.

Q: How will I be charged for deleting an archived virtual tape that is less than 3 months old?

If a virtual tape is deleted within three months of being archived, you will be charged an early deletion fee. If the virtual tape has been stored for three months or longer there is no charge for deletion.

In the US East (Northern Virginia) Region, you would be charged a prorated early deletion fee of \$0.012 per GB deleted within three months. For example, if you delete 1 virtual tape containing 1 GB of data 1 month after uploading it, you would be charged a \$0.008 early deletion fee. If, instead you delete the same virtual tape after 2 months, you would be charged a \$0.004 early deletion fee.

Q: How will I be charged for network data transfer to and from AWS when using AWS Storage Gateway?

You are billed for Internet data transfer for each GB downloaded from AWS to your gateway. All data transfer for uploading to AWS is free.

Q: How can I tell how much storage I am going to be billed for?

The Billing and Cost Management console shows an estimate of month-to-date usage for each service, including AWS Storage Gateway volumes and virtual tapes. For a breakdown of usage by individual volume or virtual tape Detailed Billing Reports enables you to see usage for each resource on a daily basis.

Q: When using file gateway, will I incur S3 request charges?

You will pay for the S3 requests made by file gateway on your behalf to store and retrieve your files in S3 as objects. The gateway caches data up to the capacity of the local disks you allocate, which can help reduce costs for data retrieval.

Q: When does each monthly billing cycle begin?

The billing system follows Coordinated Universal Time (UTC). The calendar month begins midnight UTC on the first day of every month.

Q: Do your prices include taxes?

Except as otherwise noted, our prices are exclusive of applicable taxes and duties, including VAT and applicable sales tax. For customers with a Japanese

billing address, use of the Asia Pacific (Tokyo) Region is subject to Japanese Consumption Tax.

[Back to Top](#)

Support

Q: Does AWS Premium Support cover the AWS Storage Gateway?

Yes, AWS Premium Support covers issues related to your use of the AWS Storage Gateway. Please see the [AWS Premium Support detail page](#) for further information and pricing.

Q: What other support options are available?

You can tap into the breadth of existing AWS community knowledge through the [AWS Storage Gateway discussion forum](#).

[Back to top](#)
