AWS Storage Gateway FAQs

General

Q: What is AWS Storage Gateway?

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Storage Gateway provides a standard set of storage protocols such as iSCSI, SMB, and NFS, which allow you to use AWS storage without rewriting your existing applications. It provides low-latency performance by caching frequently accessed data on premises, while storing data securely and durably in Amazon cloud storage services. Storage Gateway optimizes data transfer to AWS by sending only changed data and compressing data. Storage Gateway also integrates natively with Amazon S3 and Amazon FSx for Windows File Server cloud storage, which makes your data available for in-cloud processing, AWS Identity and Access Management (AWS IAM) for securing access management to services and resources, AWS

Key Management Service (AWS KMS) for encrypting data at rest in the cloud, Amazon CloudWatch for monitoring, and AWS CloudTrail for logging account activity.

Q: Why should I use AWS Storage Gateway?

Storage Gateway enables you to reduce your on-premises storage footprint and associated costs by leveraging AWS storage services.

Q: What use cases does AWS Storage Gateway support?

Storage Gateway supports four key hybrid cloud use cases – (1) move backups and archives to the cloud, (2) reduce on-premises storage with cloud-backed file shares, (3) provide on-premises applications low-latency access to data stored in AWS, and (4) data lake access for pre and post processing workflows.

Q: How does AWS Storage Gateway provide on-premises applications access to cloud storage?

Depending on your use case, Storage Gateway provides three types of storage interfaces for your on-premises applications: file, volume, and tape.

The Amazon S3 File Gateway enables you to store and retrieve objects in Amazon Simple Storage Service (S3) using file protocols such as Network File System (NFS) and Server Message Block (SMB). Objects written through S3 File Gateway can be directly accessed in S3.

The Amazon FSx File Gateway enables you to store and retrieve files in Amazon FSx for Windows File Server using the SMB protocol. Files written through Amazon FSx File Gateway are directly accessible in Amazon FSx for Windows File Server.

The Volume Gateway provides block storage to your on-premises applications using iSCSI connectivity. Data on the volumes is stored in Amazon S3 and you can take point-in-time copies of volumes that are stored in AWS as Amazon EBS snapshots. You can also take copies of volumes and manage their retention using AWS Backup. You can restore EBS snapshots to a Volume Gateway volume or an EBS volume.

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 tapes are stored in Amazon S3 and can be archived to Amazon S3 Glacier or Amazon S3 Glacier Deep Archive.

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 that is available as a virtual machine (VM) or as a physical hardware appliance.

You use the AWS Management Console to download the virtual appliance gateway or purchase the hardware appliance, 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 an AWS account and visit the AWS Storage Gateway Management Console to download a gateway VM appliance, or purchase the hardware appliance. Once you've 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 Amazon S3 File Gateway, you configure file shares that are mapped to selected S3 buckets or S3 prefixes, using IAM roles. For Amazon FSx File Gateway, you configure file shares by attaching an existing Amazon FSx file system that contains one or more file shares, using a service account. 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: Where can I deploy a Storage Gateway appliance?

On-premises, you can deploy a virtual machine containing the Storage Gateway software on VMware ESXi, Microsoft Hyper-V, or Linux KVM, or you can deploy Storage Gateway as a hardware appliance. You can also deploy the Storage Gateway VM in VMware Cloud on AWS, or as an AMI in Amazon EC2.

Q: What is Amazon S3 File Gateway?

Amazon S3 File Gateway presents a file-based interface to Amazon S3, which appears as a network file share. It 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 S3 File Gateway, your configured S3 buckets will be available as Network File System (NFS) mount points or Server Message Block (SMB) file shares. Your applications read and write files and directories over NFS or SMB, 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 S3 features such as S3 Lifecycle Policies and S3 Cross-Region Replication (CRR). You can run S3 File Gateway on-premises or in EC2.

Q: What is Amazon FSx File Gateway?

Amazon FSx File Gateway optimizes on-premises access to Windows file shares on Amazon FSx, making it easy for users to access FSx for Windows File Server data with low latency and conserving shared bandwidth. Users benefit from a local cache of frequently used data that they can access, enabling faster performance and reduced data transfer traffic. File system operations, such as reading and writing files, are all performed against the local cache, while Amazon FSx File Gateway synchronizes changed data to FSx for Windows File Server in the background. With these capabilities, you can consolidate all of your on-premises file share data in AWS on FSx for Windows File Server and benefit from protected, resilient, fully managed file systems.

Q: What is Tape Gateway?

Tape Gateway is a cloud-based Virtual Tape Library (VTL). It presents your backup application with a 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 S3 Glacier or Amazon S3 Glacier Deep Archive.

Q: What is Volume Gateway?

Volume Gateway provides an iSCSI target, which enables you to create block storage 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, which are stored as Amazon EBS Snapshots in AWS, enabling you to make space-efficient versioned copies of your volumes for data protection, recovery, migration and various other copy data needs.

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, SMB and NFS, which allow you to use your existing applications without any changes. Through its local cache, the gateway provides low-latency access to recently 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 can use your existing virtual infrastructure and hypervisor investments, or can be installed in your data center or remote offices as a hardware appliance. The gateway software running as a VM or on the hardware appliance is stateless, allowing you to easily create and manage new instances of your gateway as your storage needs evolve. Finally, the service integrates natively into AWS management services such as Amazon CloudWatch, AWS CloudTrail, AWS Key Management Service (KMS), and AWS Identity and Access Management (IAM).

Q: What AWS Storage Gateway types can I manage through AWS Backup?

You can manage backup and retention policies for cached and stored volume modes of Volume Gateway through AWS Backup.

Q: What is the maximum supported size of the local cache per gateway?

The maximum supported size of the local cache for a gateway running on a virtual machine is 64 TiB.

Amazon S3 File Gateway

Q: What is Amazon S3 File Gateway?

Amazon S3 File Gateway is a configuration of the AWS Storage Gateway service that provides your applications a file interface to seamlessly store files as objects in Amazon S3, and access them using industry standard file protocols.

Q: What can I do with Amazon S3 File Gateway?

Use cases for Amazon S3 File Gateway include: (a) migrating on-premises file data to Amazon S3, while maintaining fast local access to recently accessed data, (b) backing up on-premises file data as objects in Amazon S3 (including Microsoft SQL Server and Oracle databases and logs), with the ability to use S3 capabilities such as lifecycle management and cross region replication, and, (c) hybrid cloud workflows using data generated by on-premises applications for processing by AWS services such as machine learning, big data analytics or serverless functions.

Q: What are the benefits of using File Gateway to store data in S3?

Amazon S3 File Gateway enables your existing file-based applications, devices, and workflows to use Amazon S3, without modification. Amazon S3 File Gateway securely and durably stores both file contents and metadata as objects, while providing your on-premises applications low-latency access to cached data.

Q: Which Amazon S3 storage classes does S3 File Gateway support?

Amazon S3 File Gateway supports Amazon S3 Standard, S3 Intelligent-Tiering, S3 Standard - Infrequent Access (S3 Standard-IA) and S3 One Zone-IA. For details on storage classes, refer to the Amazon S3 documentation. You configure the initial storage class for objects that the gateway creates, and then you can use bucket lifecycle policies to move files from Amazon S3 to Amazon S3 Glacier. If an application attempts to access a file/object stored through Amazon File Gateway that is now in Amazon S3 Glacier, you will receive a generic I/O error.

Q: What protocols does Amazon S3 File Gateway support?

Amazon S3 File Gateway supports Linux clients connecting to the gateway using Network File System (NFS) versions 3 and 4.1, and supports Windows clients connecting to the gateway using Server Message Block (SMB) versions 2 and 3.

Q: How can I create and use a file share?

You can create an NFS or SMB file share using the AWS Management Console or service API and associate the file share with a new or existing Amazon S3 bucket. To access the file share from your applications, you mount it from your application using standard UNIX or Windows commands. For convenience, example command lines for each environment are shown in the management console.

Q: What options do I have to configure an NFS file share?

You can configure your NFS 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: What options do I have to configure an SMB file share?

You can configure your SMB file share to be accessed by Active Directory (AD) users only or provide authenticated guest access to users in your organization. You can further limit access to the file share as read-only or read-write, or to specific AD users and groups.

Q: Does Amazon S3 File Gateway support access-based enumeration for SMB file shares?

Yes, you can configure access-based enumeration for your SMB file shares to prevent users from seeing folders and files that they would not be able to open based on their access permissions. You can also control whether the file shares on the Amazon S3 File Gateway are browsable by users.

Q: Does Amazon S3 File Gateway support integration with on-premises Microsoft Active Directory (AD)?

Yes, Amazon S3 File Gateway integrates with Microsoft Active Directory on-premises as well as with in-cloud Active Directory solutions such as Managed Microsoft AD.

Q: Can I export an SMB file share without Active Directory?

Yes. You can export an SMB file share using a guest username and password. You will need to change the default password using the Console or service API before setting up your file share for guest access.

Q: Can I export a mix of NFS and SMB file shares on the same gateway?

Yes.

Q: Can I export an NFS and SMB file share on the same bucket?

No. Currently, file metadata, such as ownership, stored as S3 object metadata cannot be mapped across different protocols.

Q: How does Amazon S3 File Gateway access my S3 bucket?

Amazon S3 File Gateway uses an AWS Identity and Access Management (IAM) role to access your S3 bucket. You can set up an IAM role yourself or have it automatically set up 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: How is my file share mapped to my S3 bucket?

The file share can be mapped to the root of the S3 bucket or it can be mapped to an S3 prefix within an S3 bucket. If you specify an S3 prefix when creating a file share you are tying the file share to the S3 prefix. If you do not create an S3 prefix when creating a file share then the file share is tied to the root of the S3 bucket.

Q: Can I give my file share a custom name?

Yes, the file share name does not have to be the same as the S3 bucket or S3 prefix names.

Q: Can I change my file share name?

Yes, you can change your file share name.

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 Amazon S3 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/my-prefix*, then File Gateway will expose a mount point called *file.amazon.com:/export/my-bucket/my-prefix*. If you then mount this locally on */mnt/my-bucket/my-prefix* and create a file named file.html in a directory */mnt/my-bucket/my-prefix/dir* this file will be stored as an object in the bucket my-bucket with a key of *my-prefix/dir/file.html*. Creating sparse files will result in a non-sparse zero-filled object in S3.

Q: What file system operations are supported by Amazon S3 File Gateway?

Your clients can create, read, update, and delete files and directories. Your clients can also change permissions and ownership of files and folders. Files are stored as individual objects in Amazon 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 error. Common file operations change file metadata, which results in the deletion of the current S3 object and the creation of a new S3 object.

Rename operations will appear atomic to your 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 original objects. This avoids having to re-send large files over the network. Renaming directories containing a large number of files is not instantaneous, will result in 2 copies of your data being stored in S3, and operations in the directories will be blocked until the rename operation completes.

Q: What file system metadata can my client access and where is the metadata stored?

Your clients can access POSIX-style metadata including ownership, permissions, and timestamps that are durably stored in S3 in the user metadata of the object associated with the file. When you create a file share on an existing bucket, the stored metadata will be restored and made accessible to your clients.

Q: How do I set the Content-Type for files uploaded to S3?

For each file share, you can enable guessing of MIME types for uploaded objects upon creation or enable the feature later. If enabled, File Gateway will use the filename extension to determine the MIME type for the file and set the S3 objects Content-Type accordingly. This is beneficial if you are using File Gateway to manage objects in S3 that you access directly via URL or distribute through Amazon CloudFront.

Q: Can I directly access objects stored in S3 by using Amazon S3 File Gateway?

Yes. Once objects are stored in S3, you can access them directly in AWS for in-cloud workloads without requiring Amazon S3 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 Amazon S3 File Gateway, it results in undefined behavior when the object is accessed through the file share.

Q: What if my bucket already contains objects?

If your bucket already contains objects when you configure it for use with Amazon S3 File Gateway, object keys will be used to present the objects as files to the NFS and SMB clients. The files are given default file system metadata.

To reduce latency and number of Amazon S3 requests, Amazon S3 File Gateway only scans the headers for file metadata associated with the objects when you explicitly list the files or directories. File metadata is collected as a part of that scan; file contents are downloaded only when the object is read.

Q: How are buckets accessed by the gateway? Are entire bucket or file contents downloaded?

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

Q: What metadata can my NFS client access for objects created outside of the gateway?

For objects uploaded to the S3 bucket directly, i.e. not using File Gateway and an NFS share, you can configure default ownership and permissions.

Q: What metadata can my SMB client access for objects created outside of the gateway?

For objects uploaded to the S3 bucket directly, i.e. without using Amazon S3 File Gateway and an SMB share, metadata such as ownership and permissions will be inherited from the object's parent folder. Permissions at the root of the share are fixed and objects created directly under the root folder will inherit these fixed permissions. Refer to the documentation on metadata settings of objects created outside the gateway.

Q: Can I use multiple NFS clients with a single Amazon S3 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 Amazon S3 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. S3 File Gateway will emit Health Notifications when conflicts occur 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 an Amazon S3 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 Storage Gateway Console, the automated periodic cache refresh process, or the RefreshCache API.

Note however that if you do not configure a file share as read-only, Amazon S3 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: Can I monitor my file share using Amazon CloudWatch?

Yes, you can monitor usage of your file share using Amazon CloudWatch metrics and get notified on completion of file operations through CloudWatch Events. To learn more, visit Monitoring your File Share.

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

When you write files to your file share with Amazon S3 File Gateway, the data is stored locally first and then asynchronously uploaded to your S3 bucket. You can request notifications through AWS CloudWatch Events when the upload of an individual file completes. These notifications can be used to trigger additional workflows, such as invoking an AWS Lambda function or Amazon EC2 Systems Manager Automation, which is dependent upon the data that is now available in S3. To learn more, please refer to the documentation for File Upload Notification.

Q: How is a file upload notification different from an S3 event notification?

The file upload notification provides a notification for each individual file that is uploaded to Amazon S3 through S3 File Gateway. S3 event notifications provide notifications that include partial file uploads so there is no way to tell from the S3 event notification that the file upload has completed.

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

When you write files to your file share with Amazon S3 File Gateway, the data is stored locally first and then asynchronously uploaded to your S3 bucket. You can request notifications through Amazon CloudWatch Events when the upload of a working file set completes. These notifications can be used to trigger additional workflows, such as invoking an AWS Lambda function or Amazon EC2 Systems Manager Automation, which is dependent upon the data that is now available in S3. To learn more, please refer to the documentation for Working File Set Upload Notification.

Q: Can I update my Amazon S3 File Gateway's view of a bucket to see objects created from an object-based workload or another File Gateway?

Yes, you can refresh the inventory of objects that your Amazon S3 File Gateway knows about using the Console, the file system driven cache refresh process, or the RefreshCache API. You will receive notifications through AWS CloudWatch Events when the RefreshCache API operation has

completed. These notifications can be used to send emails using Amazon Simple Notification Service (SNS), or trigger local processing using the updated contents. To learn more, please refer to the documentation.

Q: Can I use the gateway to update data in a bucket that belongs to another AWS account?

Yes, you can use the gateway for cross-account access to buckets. To learn more, please refer to the documentation for Using File Share for Cross-Account access.

Q: Can I use the gateway to access data in Requester Pays S3 buckets?

Yes, when creating your file share you can enable access to Requester Pays S3 buckets. As a requester, you will incur the charges associated with accessing data from Requester Pays buckets.

Q: How do I create multiple shares per bucket in a gateway?

You can create multiple file shares for a single S3 bucket by specifying an S3 prefix during file share creation process.

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

You can create up to 10 shares for an S3 bucket in a single gateway. We do not limit the number of file shares per bucket across multiple gateways but each gateway is limited to 10 shares. However, we recommend having a single writer to the bucket, either an Amazon S3 File Gateway or client accessing S3 directly.

Q: Can I change the name of a file share?

Yes, you can change the name of a file share.

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 Amazon S3 lifecycle, cross-region replication, and S3 event notification with File Gateway?

Yes. Your bucket policies for 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 enable the periodic cache refresh feature or call the RefreshCache API to reflect these changes to your NFS clients.

When using an S3 bucket that is the target for cross-region replication, you may need to enable the periodic cache refresh feature or 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 may occur for a number of reasons, such as the gateway needing to free up cache space, or a high rate of writes to a file. These partial files may not be application consistent.

Q: Can I use Amazon S3 File Gateway with my backup application?

Amazon S3 File Gateway supports SMB versions 2 and 3 as well as NFS versions 3, 4.0, and 4.1. We are continuing to do ongoing testing with common backup apps. Please let us know via AWS Support or through your AWS account team of any specific apps with which you'd like to see compatibility tested.

Q: Can I use Amazon S3 File Gateway to write files to EFS?

No. Amazon S3 File Gateway allows you to store files as objects in S3.

Q: When should I use Amazon S3 File Gateway vs. the S3 API?

You can use Amazon S3 File Gateway when you want to access objects in S3 as files using standard filesystem operations. Amazon S3 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 Amazon S3 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 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: What guidance should I use to provision the size of the gateway's cache disk? What happens if I provision a smaller cache disk?

You should provision your cache based on:
1/ The size of your working dataset to which you need low-latency access, so you can reduce read latencies by decreasing the frequency with which data is requested from S3, and
2/ The size of files written to the gateway by your applications.

Smaller cache disks can result in poor performance and failures during writes if there is no free cache space to store data locally when pending upload to S3. To learn more about monitoring your cache usage, refer to Monitoring Your File Share in the documentation.

Q: When does data in the cache get evicted?

Data written to the cache from your applications or through retrieval from Amazon S3 is evicted from the cache only when space is needed to store more recently accessed data.

Q: Does Amazon S3 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.

Amazon S3 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 Amazon S3 File Gateway with Amazon S3 Transfer Acceleration?

File Gateway will not use the accelerated endpoints even if your bucket is configured for S3 Transfer Acceleration.

Q: What sort of encryption does Amazon S3 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. To learn more, please see "Encrypting Your Data Using AWS Key Management System," in the Storage Gateway User Guide, which includes critical details about usage of the feature.

Amazon FSx File Gateway

Q: What is Amazon FSx File Gateway?

Amazon FSx File Gateway optimizes on-premises access to Windows file shares on Amazon FSx, making it easy for users to access FSx for Windows File Server data with low latency and conserving shared bandwidth. Users benefit from a local cache of frequently used data that they can access, enabling faster performance and reduced data transfer traffic. File system operations, such as reading and writing files, are all performed against the local cache, while Amazon FSx File Gateway synchronizes changed data to FSx for Windows File Server in the background. With these capabilities, you can consolidate all of your on-premises file share data in AWS on FSx for Windows File Server and benefit from protected, resilient, fully managed file systems.

Q: Why should I use Amazon FSx File Gateway?

Many on-premises desktop applications are latency-sensitive, which may cause delays to your end users and slow performance when they are directly accessing files in AWS from remote locations. Additionally, allowing large numbers of users to directly access data in the cloud can cause congestion on your shared bandwidth resources such as AWS Direct Connect links. Amazon FSx File Gateway allows you to use Amazon FSx for Windows File Server for these workloads, and help replace your on-premises storage with fully managed, scalable, and highly reliable file storage in AWS without impacting your applications or network.

Q: How does Amazon FSx File Gateway solve these problems for on-premises applications?

Amazon FSx File Gateway provides an SMB file protocol server for clients to connect to, and an on-premises cache of the frequently used data that they can access with the same low latency as they would experience inside AWS. File system operations, such as reading and writing files, are

all performed against the local cache, while Amazon FSx File Gateway synchronizes changed data to Amazon FSx for Windows File Server in the background. Amazon FSx File Gateway also helps minimize the amount of data transfer, while optimizing the usage of network bandwidth to AWS.

Q: How do I use Amazon FSx File Gateway?

To use Amazon FSx File Gateway, you need to have at least one running Amazon FSx file system, and ensure that you have on-premises access to Amazon FSx for Windows File Server either through a VPN or through an AWS Direct Connect connection. To get started with FSx for Windows File Server, view the documentation instructions here. You then begin either by downloading and deploying an Amazon FSx File Gateway VMware virtual appliance, or an AWS Storage Gateway hardware appliance into your on-premises environment. Once your Amazon FSx File Gateway is installed and you can access FSx for Windows File Server, you can use the AWS Management Console to attach an FSx for Windows File Server file system. The AWS Management Console will then walk you through all the steps needed to make file shares accessible on premises.

After the file shares are configured, client systems can then browse and connect to the file shares on Amazon FSx File Gateway that correspond to the selected Amazon FSx file systems. When the file shares are connected, users can read and write their files locally, while benefiting from all the features available on FSx for Windows File Server.

Q: What regions is Amazon FSx File Gateway available in?

Amazon FSx File Gateway can be used to access Windows file systems in all AWS regions where FSx for Windows File Server is offered.

Q: How much does Amazon FSx File Gateway cost?

You are billed hourly for Amazon FSx File Gateway. For pricing information, please visit the AWS Storage Gateway pricing page.

Q: What protocols does Amazon FSx File Gateway support?

Amazon FSx File Gateway supports versions 2.x and 3.x of the Server Message Block (SMB) protocol. SMB is supported by Microsoft Windows, MacOS, and the Linux OS.

Q: What is the relationship between files I see in Amazon FSx File Gateway and files I see in Amazon FSx for Windows File Server?

Amazon FSx File Gateway maps local file shares and their contents to file shares stored remotely in Amazon FSx for Windows File Server. There is a 1:1 correspondence between the remote and

locally visible files and their shares.

Q: Does Amazon FSx File Gateway allow me to access the same file shares in AWS?

Yes. You may access your file shares from both Amazon FSx File Gateway as well as directly from Amazon FSx in AWS; however, you should ensure that files can only be written from a single location at a time. In this release, Amazon FSx File Gateway will not prevent writes from multiple locations to overlap in a way that creates conflicts.

Q: How does Amazon FSx File Gateway allow me to manage my Amazon FSx for Windows File Server?

You can manage Amazon FSx for Windows File Server via a remote management interface using all of the tools provided by FSx for Windows File Server.

Q: Can Amazon FSx File Gateway be connected to more than one Amazon FSx for Windows file system?

Yes. You are allowed to attach a gateway to shares on up to 5 file systems as long as they are all members of the same Active Directory domain. Amazon FSx File Gateway will only join a single Active Directory Domain.

Q: What deployment options are supported?

You can deploy a virtual machine containing the Amazon FSx File Gateway software on VMware ESXi, Microsoft Hyper-V, or Linux KVM, or you can deploy Storage Gateway as a hardware appliance.

Q: How do I use my Active Directory to provide credentials?

Amazon FSx File Gateway becomes a member of the Active Directory domain whether the AD infrastructure is hosted in AWS Directory Service, or if it is managed on-premises. Once Amazon FSx File Gateway is a member of the domain, it has access to all users and policies that are set in that domain for the purposes of enforcing security. Amazon FSx File Gateway then will behave identically to any Windows Server and enforce all applicable file access policies based on what is configured in Active Directory.

Q: Is Amazon FSx File Gateway compatible with my existing Windows Access Controls and Active Directory credentials?

Amazon FSx File Gateway uses native Windows Access Controls and is compatible with any existing static access lists that work with Microsoft Windows. The maximum size of an ACL is 64KB or approximately 1820 Access Control Entries. This is identical to Windows Server hosts.

Access controls are set and stored on FSx Windows File Server, so you only need to create them once and they will be reflected in all attached File Gateways.

Q: Is data encrypted in transit?

Yes. Amazon FSx File Gateway supports SMB encryption up to the latest SMB v3.1.1 specification, including AES 128 CCM and AES 128 GCM. Compatible clients will connect using encryption automatically. Additionally, Amazon FSx File Gateway uses SMB encryption when it communicates with FSx for Windows File Server in AWS. You must either configure a VPN or a Direct Connect link to AWS, and set appropriate policies to allow SMB traffic and management traffic to pass through to AWS.

Q: How does Amazon FSx File Gateway provide high availability?

Just like Amazon S3 File Gateway, Amazon FSx File Gateway achieves high availability on VMware by running a series of continuous health checks against the operation of the gateway that connect to the VMware monitoring service. During a hardware, software, or network failure, VMware will trigger a gateway restart on a new host or on its existing host if the host is still operational. At a maximum, users and applications will experience up to 60 seconds of downtime during a restart. After a restart, connections to the gateway are automatically re-established, never needing manual intervention. On re-initialization the gateway will send metrics back to the cloud to give customers a full view of the availability event.

Q: What types of failures are covered by Amazon FSx File Gateway with high availability?

Amazon FSx File Gateway, with VMware HA enabled and application monitoring configured, will detect and recover from hardware failures, hypervisor failures, network failures, as well as software issues that lead to connection timeouts or file-share unavailability.

Q: How many sessions and file shares does Amazon FSx File Gateway support?

Amazon FSx File Gateway supports up to 50 shares and 500 active client sessions connected to Amazon FSx File Gateway instances in a single instance configuration.

Tape Gateway

Q: How do I get started with AWS Snowball to migrate my tape data?

To get started, in the AWS Snow Family console, order a Snowball Edge Storage Optimized device with Tape Gateway. When you receive the device from AWS, unlock it, and connect to your local network. Then start Tape Gateway, which looks like a physical tape library. Connect to

AWS and copy data from physical tapes to virtual tapes on Tape Gateway using your existing backup application. After you complete your data copy, ship the Snowball Edge device back to AWS. Your data will be stored in either S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive. You can view your virtual tapes stored on AWS through the AWS Storage Gateway console and access data on them through a Tape Gateway that runs on premises as a virtual machine or hardware appliance or on an Amazon Elastic Compute Cloud (Amazon EC2) instance on AWS.

Q: How much storage is available on a Snowball Edge Storage Optimized device that I can use with Tape Gateway?

The Snowball Edge Storage Optimized device provides 80 terabytes of usable block storage or object storage and can migrate that amount of tape data to S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive.

Q: When do I use Tape Gateway with a Snowball Edge Storage Optimized device and when do I use Tape Gateway with a virtual or a hardware appliance?

You use a Snowball Edge Storage Optimized device with Tape Gateway in constrained network bandwidth environments to migrate data stored in your tape archives to AWS. After you complete your data copy to the device, you send it back to AWS. With Tape Gateway on Snowball, your data is migrated to AWS offline. You use Tape Gateway on a virtual or a hardware appliance when you want to copy new backups and archives to AWS and don't have network constraints. With Tape Gateway on a virtual or hardware appliance, your data is transferred to AWS using the network and you keep the virtual or hardware appliance permanently in your data center.

Q: Can I use Snowball with Tape Gateway as an on-premises virtual tape library (VTL) instead of using it for offline data migration?

No, a Snowball Edge Storage Optimized device with Tape Gateway is not designed and built for meeting your on-premises VTL needs—only for meeting your offline data migration needs. After your backup application exports virtual tapes, your virtual tapes on Snowball with Tape Gateway can't be accessed until they are imported into AWS. For on-premises VTL needs, use a Tape Gateway that runs on a virtual machine, on a hardware appliance, or on an Amazon EC2 instance.

Q: What are the benefits of storing virtual tapes in AWS compared to warehousing tapes offsite?

You get 11 9s of data durability, fixity checks by AWS on a regular basis, data encryption, right data when you restore, and cost savings, when storing virtual tapes in AWS using Tape Gateway with S3 Glacier Deep Archive compared to warehousing physical tapes offsite. First, all virtual

tapes stored in S3 Glacier Deep Archive are replicated and stored across at least three geographically-dispersed Availability Zones, protected by 11 9s of durability. Second, AWS performs fixity checks on a regular basis to confirm your data can be read and no errors have been introduced. Third, all tapes stored in S3 Glacier Deep Archive are protected by S3 Server Side Encryption using default keys or your KMS keys. In addition, you also avoid physical security risk associated with tape portability. Fourth, compared to the experience of warehousing tapes offsite where you may receive an incorrect or broken tape during restore, with Tape Gateway, you always get correct data. Finally, you can save in monthly storage costs when storing your data in S3 Glacier Deep Archive compared to warehousing tapes offsite.

Q: What Amazon S3 storage classes does Tape Gateway support?

Tape Gateway supports S3 Standard, S3 Glacier, and S3 Glacier Deep Archive storage classes. Data on your virtual tapes is stored in a virtual tape library in Amazon S3 when the backup application is writing data to tapes. After you eject tapes from the backup application, your tapes are archived to S3 Glacier or S3 Glacier Deep Archive.

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

The minimum size and maximum size of a virtual tape you can create on a Tape Gateway is 100 GiB and 5 TiB respectively. Please note, you only pay for the amount of data stored on each tape, and not for the size of the tape.

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

A single Tape Gateway can have up to 1,500 virtual tapes in the VTL with a maximum aggregate capacity of 1 PB; however there is no limit to the amount of data or number of virtual tapes you can archive. You can also deploy additional Tape Gateways to scale storage for virtual tapes that are not archived. For more information, please see our documentation on Storage Gateway limits.

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: Which S3 storage classes can I retrieve my archived virtual tape to?

You can retrieve a virtual tape archived in S3 Glacier or S3 Glacier Deep Archive to S3. A tape archived in S3 Glacier is retrieved to S3 using standard retrieval method typically within 3-5 hours. A tape archived in S3 Glacier Deep Archive is retrieved to S3 using standard retrieval method typically within 12 hours.

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 or API. First select the virtual tape, then choose the virtual tape library into which you want the virtual tape to be loaded. You can retrieve a tape archived in S3 Glacier and S3 Glacier Deep Archive to S3, typically within 3-5 hours and 12 hours, respectively. 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: Will I be able to access the virtual tapes in my virtual tape library using Amazon S3 or Amazon S3 Glacier APIs?

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

Q: How do I use Tape Gateway with S3 Glacier Deep Archive storage class?

When creating new tapes through the Storage Gateway console or API, you can set the archival storage target to S3 Glacier Deep Archive. When your backup software ejects the tapes, they will be archived to S3 Glacier Deep Archive. You can retrieve a virtual tape archived in S3 Glacier Deep Archive to S3 using standard retrieval method typically within 12 hours.

Q: Can I move my existing virtual tapes in S3 Glacier to S3 Glacier Deep Archive?

Yes. Tape Gateway supports moving your tapes in S3 Glacier to S3 Glacier Deep Archive. You can assign the tape placed in Glacier Pool to Deep Archive Pool using AWS Storage Gateway Console or API. Tape Gateway will then move the virtual tape to Deep Archive Pool associated with the S3 Glacier Deep Archive storage class. You will incur a tape move charge for moving a tape from S3 Glacier to S3 Glacier Deep Archive and if applicable, an early deletion fee for S3 Glacier, if you move a tape from S3 Glacier to S3 Glacier Deep Archive prior to 90 days.

Q: Can I move a tape in S3 Glacier Deep Archive to S3 Glacier?

No, you cannot move a tape from S3 Glacier Deep Archive to S3 Glacier. You can retrieve a tape from S3 Glacier Deep Archive to S3 or delete a tape from S3 Glacier Deep Archive.

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 Storage Gateway overview page.

Q: What sort of encryption does Tape Gateway use to protect my data?

All data transferred between the gateway and AWS storage is encrypted using SSL. By default, all data stored by Tape Gateway in S3 is encrypted server-side with Amazon S3-Managed Encryption Keys (SSE-S3).

You can optionally configure encryption on tapes using AWS KMS-Managed Keys via the Storage Gateway API. You will be able to specify one of the managed Customer Master Keys (CMKs) as the KMS key. The configured CMK used to encrypt tape data cannot be changed after creation. To learn more, please see "Encrypting Your Data Using AWS Key Management System," in the Storage Gateway User Guide, which includes critical details about usage of the feature.

Volume Gateway

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). For more information, please refer to our documentation on Storage Gateway limits.

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 an Amazon S3 bucket maintained by the AWS Storage Gateway service. Your volumes are accessible for I/O operations through AWS Storage Gateway. You cannot directly access them 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, which can be turned into either Storage Gateway Volumes or EBS Volumes. Use the File Gateway to work with your data natively in S3.

Q: What sort of encryption does Volume Gateway use to protect my data?

All data transferred between the gateway and AWS storage is encrypted using SSL. By default, all data stored by Volume Gateway in S3 is encrypted server-side with Amazon S3-Managed Encryption Keys (SSE-S3).

You can optionally configure encryption for data stored in AWS on volumes using AWS KMS managed keys via the Storage Gateway API. You will be able to specify one of the managed Customer Master Keys (CMKs) as the KMS key. The configured CMK used to encrypt a volume cannot be changed after creation. To learn more, please see "Encrypting Your Data Using AWS Key Management System," in the Storage Gateway User Guide, which includes critical details about usage of the feature.

Q: Can I create an EBS Snapshot from a KMS-encrypted volume?

Yes. You can create an EBS snapshot from an AWS KMS-encrypted volume using the API. The EBS snapshot will be encrypted using the same key as the one used for volume encryption.

Q: Can I create a volume from a KMS-encrypted EBS snapshot?

Yes. You can create an encrypted volume from a KMS-encrypted EBS snapshot using the API. The encrypted volume can use the same key that was used to encrypt the EBS snapshot, or you can specify a different encryption key for encrypting the volume.

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 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.

Q: What are the benefits of using AWS Backup to protect my Volume Gateway volumes?

Using AWS Backup to back up Volume Gateway volumes simplifies and centralizes backup management, thus reducing operational burden and making it easier to meet compliance requirements across all your AWS resources. AWS Backup allows you to set customizable scheduled backup policies that meet your backup requirements. Using AWS Backup, you can set backup retention and expiration rules so you no longer need to develop custom scripts or manually manage the point-in-time backups of your Volume Gateway volumes. Finally, you can manage and monitor backups across multiple Volume Gateways, and other AWS resources such as EBS volumes and RDS databases, from a central view.

Q: How do I protect volumes on Volume Gateway using AWS Backup?

You can use AWS Backup to either take a one-time backup or define a backup schedule for Volume Gateway volumes. The volume backups are stored in Amazon S3 as Amazon EBS snapshots and visible in the AWS Backup console or Amazon EBS console. The volume backups created by AWS Backup can manually or automatically be deleted from the AWS Backup console.

Q: How do I use AWS Backup to manage backup and retention of my Volume Gateway volumes?

You can start from either the Storage Gateway console or the AWS Backup console to manage your backups. If you start from the Storage Gateway console, you have the ability to navigate to

the AWS Backup console to complete your backup plan configuration or initiate an on-demand backup. Alternatively, you can start from the AWS Backup console to configure your backup plan or initiate an on-demand backup of Volume Gateway volumes.

Q: Does anything change with how I have been using Volume Gateway volumes today?

No. All existing Volume Gateway snapshot functionality and your existing Amazon EBS Snapshots remain available and unchanged. You can continue to use the Storage Gateway console to create volumes from your EBS Snapshots and use the Amazon EBS console to view or delete your snapshots.

Q: If I use AWS Backup, can I also continue to use Volume Gateway snapshot schedules and existing snapshots?

Yes. You can continue to use Volume Gateway's existing snapshot capabilities to create Amazon EBS snapshots and use your previously created snapshots for restore purposes. AWS Backup's backup schedule operates independently from the Volume Gateway scheduled snapshots, and provides you an additional way to centrally manage all your backup and retention policies.

Q: If I have a KMS-encrypted volume on Volume Gateway, will AWS Backup be able to back up that volume?

Yes. AWS Backup will back up KMS-encrypted volumes on Volume Gateway with the same key as the one used for volume encryption.

Q: Can I use AWS Backup to create a backup of my Volume Gateway volume in a different region (e.g. cross region)?

AWS Backup supports backup of Volume Gateway volumes within the same region in which AWS Backup operates.

Hardware Appliance

Q: What is the Storage Gateway Hardware Appliance?

AWS Storage Gateway is available as a hardware appliance, which has Storage Gateway software pre-installed on a validated server configuration. You manage the appliance from the AWS Console or API.

Q: What gateway types and storage interfaces are supported on the hardware appliance?

The hardware appliance supports Amazon S3 File Gateway with NFS and SMB interfaces, Amazon FSx File Gateway with SMB, Volume Gateway cached volumes with iSCSI, and Tape Gateway with iSCSI-VTL.

Q: Why might I need a hardware appliance?

The hardware appliance further simplifies procurement, deployment, and management of AWS Storage Gateway on-premises for IT environments such as remote offices and departments that lack existing virtual server infrastructure, adequate disk and memory resources, or staff with hypervisor management skills. It avoids having to procure additional infrastructure necessary for a virtual environment in order to operate the local Storage Gateway VM appliance.

Q: How many models of hardware appliances are available?

There are two models available that offer 5 TB or 12 TB of local SSD cache.

Q: What are the specifications of the hardware appliance?

The hardware appliance is based on validated server configurations. Please refer to the Storage Gateway Hardware Appliance product page for specifications.

Q: Where is the hardware appliance available? With which AWS Regions does it work?

The hardware appliance is available for shipping to all international destinations allowed for exporting by the US government. It is supported in 16 AWS Regions including US East (Northern Virginia, Ohio), US West (Northern California, Oregon), Canada (Central), South America (São Paulo), Europe (Ireland, Frankfurt, London, Paris, Stockholm), and Asia Pacific (Mumbai, Seoul, Singapore, Sydney, Tokyo).

Q: Where do I buy the hardware appliance?

The AWS Storage Gateway Hardware Appliance is available exclusively through resellers. Please contact your preferred reseller for purchasing information and to request a quote. Customers in the United States and Canada can also purchase the appliance directly from CDW.

Q: Who owns the hardware appliance?

After purchase, you own the hardware appliance.

Q: How do I use the hardware appliance?

Once you receive the hardware appliance, you configure your IP address through the local hardware console, and use this IP address in the AWS Storage Gateway console to activate your

appliance. This associates your hardware appliance with your AWS account. Once the hardware appliance is activated, you select your desired gateway type from the console, either file, volume (cached), or tape. The selected type of gateway is then enabled on the appliance. Once activated, you manage and use your new Storage Gateway Hardware Appliance with the AWS Console, CLI, or SDK, similar to how you would with the virtual appliance today. For more information, please see the hardware appliance documentation.

Q: Can I run multiple gateways on a single hardware appliance?

No. Currently, the hardware appliance supports running only one gateway at a time.

Q: Can I change the type of gateway once it is installed on a hardware appliance?

Yes. To change the gateway type after it is installed on a hardware appliance, you choose *Remove Gateway* from the Storage Gateway console, which deletes the gateway and all associated resources. At that point, you are free to launch a new gateway on the hardware appliance.

Q: How can I purchase and use additional storage on the Storage Gateway Hardware Appliance?

If you ordered the 5 TB hardware appliance model, you can increase the usable local cache to 12 TB by purchasing a 5-pack SSD upgrade kit. You can purchase the SSD upgrade kit by following the same process for ordering the hardware appliance. To expand your storage, simply insert the SSDs into the pre-configured appliance. The SSDs are hot pluggable, and the appliance will automatically recognize the extra storage upon adding SSDs to the appliance. View the documentation for instructions.

Q: Can I add more storage to a Storage Gateway Hardware Appliance after it has been activated?

If you have already activated the appliance and associated it with your AWS account, you will need to factory reset it before adding more storage.

Q: Can I add any SSD or hard drive to increase storage capacity for my Storage Gateway Hardware Appliance?

No. Only add the SSDs that are available from the manufacturer of the appliance. These SSDs are qualified by AWS for use in the Storage Gateway Hardware Appliance.

Q: Does the Storage Gateway Hardware Appliance support RAID?

Yes. The hardware appliance uses software-based ZFS RAID and provides protection against storage drive failure. The base appliance offering 5 TB of usable storage tolerates failure of 1 SSD and the 12 TB usable storage configuration tolerates failure of 2 SSDs.

High Availability on VMware

Q: How does Storage Gateway provide high availability?

Storage Gateway achieves high availability by running a series of continuous health-checks against the operation of the gateway that connect to the VMware monitoring service. During a hardware, software, or network failure, VMware will trigger a gateway restart on a new host or on its existing host if the host is still operational. At a maximum, users and applications will experience up to 60 seconds of downtime during a restart. After a restart, connections to the gateway are automatically re-established, never needing manual intervention. On re-initialization the gateway will send metrics back to the cloud to give customers a full view of the availability event.

Q: What environments are enabled for Storage Gateway high availability?

Storage Gateway high availability can currently be enabled in clustered VMware vSphere environments that have VMware HA enabled and have shared volume storage available.

Q: What does Storage Gateway with high availability cost?

There is no additional cost for running Storage Gateway with the high availability integration enabled.

Q: What types of failures are covered by Storage Gateway with high availability?

Storage Gateway with VMware HA enabled and application monitoring configured will detect and recover from hardware failures, hypervisor failures, network failures, as well as software issues that lead to connection timeouts or file-share, volume, or virtual tape library unavailability.

Q: Will NFS and SMB sessions be maintained during a gateway restart?

Yes.

Q: Will gateway reads or writes fail during a gateway restart?

NFS clients connecting to File Gateways may hang for up to 60 seconds on a read or write operation while the gateway restarts and then will retry, given customers use the recommended

mount settings. SMB clients may reject a file read or write during a restart depending on client settings. All iSCSI reads and writes for Volume Gateway and Tape Gateway will hang during a gateway restart and then automatically retry.

Q: Will Storage Gateway HA still have the ability to restart if its connection to AWS is broken?

Yes, gateways will be reinitialized using the same underlying shared storage, preserving local cache and upload queues.

Q: Will I lose data during a gateway restart?

No, gateways will be reinitialized using the same underlying shared storage, preserving local cache and upload queues.

Q: Do I need to make any changes to my VMware environment to take advantage of the HA feature?

If the gateway is deployed to VMware with VMware HA enabled you will be able to configure the restart sensitivity of the Storage Gateway VM in the VMware vSphere control center. The Storage Gateway VM heartbeat will be available giving you the ability to automatically restart the gateway on a specific timeout.

Q: What does Storage Gateway HA give me that I don't already have if I operate VMware HA?

VMware HA monitors underlying infrastructure, such as storage and networking. Storage Gateway provides a range of health checks such as file system availability, SMB endpoint availability, and NFS endpoint availability that monitor all of the critical operations of the gateway, ensuring the whole service and not just the underlying infrastructure is continuously available to your users and applications.

Q: Will this be available for VMware Cloud on AWS?

Yes. Storage Gateway High Availability can be used on VMware Cloud with no additional requirements. VMware Cloud on AWS has VMware HA enabled by default and shared volumes are available.

Q: How will I know if a gateway is capable of high availability and operating in HA-mode?

When setting up a new gateway for VMware, you will be given the option of testing HA. You may also test whether a deployed gateway is HA-capable by choosing the “Test VMware HA” action in the console.

Q: What operational visibility will I have during a gateway restart?

The AWS Storage Gateway console will show availability events in log tables and interruptions in performance graphs during a gateway restart.

Q: Will I see an availability event in CloudWatch when a gateway restart occurs?

Yes, if you have configured the integration with CloudWatch, availability events triggered from the gateway will be available through CloudWatch.

Q: How will I know when a gateway returns to operation?

If you have configured the integration with CloudWatch, a CloudWatch event will be triggered on re-initialization. Additionally, performance graphs will show the gateway's operational metrics including number of active sessions.

Q: Will I be able to set a service timeout that triggers a gateway restart?

Yes, administrators will be able to set a timeout in the vSphere console that will restart the service if the gateway is unreachable for the specified number of seconds.

Security and Compliance

Q: What encryption does AWS Storage Gateway use to protect my data?

All data transferred between any type of gateway appliance and AWS storage is encrypted using SSL. By default, all data stored by AWS Storage Gateway in S3 is encrypted server-side with Amazon S3-Managed Encryption Keys (SSE-S3). Also, you can optionally configure different gateway types to encrypt stored data with AWS Key Management Service (KMS) via the Storage Gateway API. See below for specifics on KMS support by File Gateway, Tape Gateway, and Volume Gateway.

Q: Is AWS Storage Gateway HIPAA eligible?

Yes. AWS Storage Gateway is HIPAA eligible. If you have an executed Business Associate Agreement (BAA) with AWS, you can use Storage Gateway to store, back up, and archive protected health information (PHI) on scalable, cost-effective, and secure AWS storage services, including Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Amazon FSx for Windows File Server, and Amazon EBS, which are also HIPAA eligible.

Information on HIPAA eligible services on AWS can be found on our HIPAA Compliance page, and you can also enter into a BAA with AWS on that page. HIPAA eligibility for Storage Gateway

applies to all gateway types (File, Volume, and Tape).

Q: Is AWS Storage Gateway PCI compliant?

Yes, AWS Storage Gateway is compliant with the Payment Card Industry Data Security Standard (PCI DSS) based on recent assessments. Existing customers can download the Attestation of Compliance (AOC) and PCI Responsibility Summary reports in the AWS Management Console with AWS Artifact. Prospective customers can request the reports by working with the AWS sales team.

Q: Is AWS Storage Gateway FedRAMP compliant?

Yes, AWS Storage Gateway is FedRAMP compliant with High authorization level in the AWS GovCloud (US) Regions, and Moderate authorization level in the AWS US Commercial Regions. More information can be found on the AWS FedRAMP compliance page.

Q: Does AWS Storage Gateway support FIPS 140-2 compliant endpoints?

The S3 File Gateway, Amazon FSx File Gateway, Volume Gateway, and Tape Gateway support FIPS 140-2 compliant endpoints.

Q: Which Regions support AWS Storage Gateway FIPS 140-2 compliant endpoints?

AWS Storage Gateway supports FIPS 140-2 compliant endpoints in the following AWS Regions: US East (N. Virginia), US East (Ohio), US West (N. California), US West (Oregon), Canada (Central), GovCloud (US-West), and GovCloud (US-East).

Q: What are the FIPS endpoints for AWS Storage Gateway?

For a list of the FIPS endpoints available for AWS Storage Gateway, refer to the AWS Storage Gateway endpoints reference guide or the AWS GovCloud (US) user guide.

Q: Is AWS Storage Gateway Hardware Appliance FIPS 140-2 compliant?

No, AWS Storage Gateway Hardware Appliance is not FIPS 140-2 compliant.

Q: Does File Gateway provide logging to monitor client file access operations?

Yes, File Gateway audit logs can be used to monitor client operations for folders and files within SMB file shares.

Q: Can I monitor client activity for individual file shares?

You can configure File Gateway audit logs to monitor user operations for folders and files at the share level for each SMB share.

Q: What types of file shares are supported by File Gateway audit logs?

File Gateway audit logs support SMB shares.

Q: What file operations will I see in File Gateway audit logs?

You will see details about the following operations logged for files and directories: open, delete, read, write, rename, change of permissions, and file operation success. User information for each operation, including timestamp, Active Directory domain, user name, and client IP address, is also logged.

Q: How do I access File Gateway audit logs?

You can access the File Gateway audit logs in Amazon CloudWatch. Audit logs can also be sent from CloudWatch to the Amazon S3 bucket of your choice. Audit logs can be viewed from Amazon S3 using Amazon Athena and can also be exported to third party security information and event management applications (SIEM) for analysis within those tools.

Q: Does Tape Gateway support Write Once Read Many (WORM) capability?

Yes, when creating new virtual tapes manually or using automatic tape creation configuration on Tape Gateway, you can select the WORM tape type. Data on WORM virtual tapes cannot be erased intentionally or accidentally from the backup application. In addition, Tape Gateway's Tape Retention Lock capability prevents archived virtual tapes from being deleted for a fixed amount of time, or even indefinitely.

Networking

Q: Can I use 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 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 Gateway supports configuration of a

HyperText Transfer Protocol (HTTP) proxy.

Q: Can I deploy a Storage Gateway on my private non-routable network? Does Storage Gateway support AWS PrivateLink?

Yes. You can deploy a Storage Gateway on a private, non-routable network if that network is connected to your Amazon VPC via DX or VPN. Storage Gateway traffic will be routed via VPC endpoints powered by AWS PrivateLink, a technology that enables private connectivity between AWS services using Elastic Network Interfaces (ENI) with private IPs in your VPCs. To learn more about PrivateLink, visit the PrivateLink documentation. To set up AWS PrivateLink for Storage Gateway, visit the AWS PrivateLink for Storage Gateway documentation.

Q: Does Storage Gateway support AWS PrivateLink for all types of gateways?

Yes, the service supports PrivateLink for all gateway types (File/Volume/Tape).

Q: What is the cost for using VPC endpoints with Storage Gateway?

You will be billed for each hour that your VPC endpoint remains provisioned. Data processing charges also apply for each Gigabyte processed through the VPC endpoint regardless of the traffic's source or destination.

Q: How do I activate gateways that are connected to AWS via AWS PrivateLink?

PrivateLink enabled gateways can be activated through the AWS Console if your web browser has access to both the internet and your private network, or via the CLI in the region that they are based.

Q: How can I use PrivateLink with File Gateway?

To use File Gateway on-premises with PrivateLink and private virtual interfaces (VIFs) to access your Amazon S3 buckets, you will need to set up an Amazon EC2 based proxy server. In order to access Amazon S3 over a private network, you need to use S3's gateway endpoints, and these endpoints are not directly accessible from on-premises environments. The proxy server will provide access through the VPC endpoint for S3, making it accessible to an on-premises File Gateway. We recommend using an EC2 instance family that is optimized for network bandwidth.

Q: Can a File Gateway use a VPC endpoint in one region and access an S3 bucket in another region?

No.

Q: How can I use PrivateLink with Volume Gateways and Tape Gateways?

Volume and Tape Gateways connect directly to AWS services through the Storage Gateway VPC endpoint without the need for a proxy to S3.

Q: Can I use AWS PrivateLink with my Storage Gateway Hardware Appliance?

Yes, but the appliance must be activated before it is moved to the private network.

Performance, Monitoring, and Management

Q: What performance can I expect?

The AWS Storage Gateway sits between your applications and Amazon storage services. The performance you experience depends on the host platform (hardware appliance, virtual machine, Amazon EC2 instance) you are using to run Storage Gateway software, along with a number of other 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 AWS Storage Gateway environment for best performance.

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

For running AWS Storage Gateway on a virtual machine or an Amazon EC2 instance, see the requirements section in the AWS Storage Gateway User Guide. AWS Storage Gateway is also available as a Hardware Appliance with pre-validated specifications.

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 AWS Storage Gateway support network bandwidth throttling?

Yes, you can throttle network bandwidth used by the gateway to synchronize data with AWS based on a schedule for Volume and Tape Gateways. You can specify day of the week, time, and bandwidth rates for inbound and outbound traffic.

Q: How do I monitor my gateway?

You can use Amazon CloudWatch to monitor the performance metrics and alarms for your gateway, giving you insight into storage, bandwidth, throughput, and latency. These metrics and alarms are accessible directly from CloudWatch; or by following links in the AWS Storage Gateway Console, which take you directly to the CloudWatch metrics or alarms 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 can I create CloudWatch Alarms for my gateway?

You can create alarms for your gateway in the Amazon CloudWatch console.

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.

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 on an archived virtual tape?

You are charged, when retrieving a virtual tape that has been archived in S3 Glacier, 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 x 100GB x $0.01 = $5.00.

Q: How will I be charged for deleting an archived virtual tape?

If a virtual tape is deleted within three months of being archived in S3 Glacier or within six months of being archived in S3 Glacier Deep Archive, you will be charged an early deletion fee. If the virtual tape has been stored for three months or longer in S3 Glacier or for six months or longer in S3 Glacier Deep Archive, 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 archiving it in S3 Glacier, 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 am I charged for virtual tapes I store in S3 Glacier Deep Archive?

Virtual tapes stored in S3 Glacier Deep Archive will be charged S3 Glacier Deep Archive storage class rate. You can visit Storage Gateway pricing webpage to review Tape Gateway pricing.

Q: How will the virtual tapes I store in Deep Archive Pool, associated with S3 Glacier Deep Archive storage class, show up on my AWS bill and in the AWS Cost Management tool?

The usage and cost for virtual tapes you store in Deep Archive Pool will show up as an independent service line item on your monthly AWS bill under AWS Storage Gateway Deep Archive, separate from your AWS Storage Gateway and costs. However, if you are using the AWS Cost Management tool, usage and cost for virtual tapes you store in Deep Archive Pool will be included under AWS Storage Gateway in your detailed monthly spend reports, and not broken out as a separate service line item.

Q: How will I be charged for moving a virtual tape archived in S3 Glacier to S3 Glacier Deep Archive?

For AWS US East (N. Virginia) region, you are charged, when moving a virtual tape that has been archived in S3 Glacier to S3 Glacier Deep Archive, at a rate of $0.032 per GB of data stored on the tape. For example, moving a 100 GB tape archived in S3 Glacier to S3 Glacier Deep Archive will cost 100 GB x $0.032/GB = $3.2. If you move a tape that's archived for less than 90 days in S3 Glacier to S3 Glacier Deep Archive, you are also charged for early deletion fee for tape storage in S3 Glacier.

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: Will I incur CloudWatch charges when using File Gateway audit logs?

You will be charged standard rates for Amazon CloudWatch Logs, Amazon CloudWatch Events, and Amazon CloudWatch Metrics if you configure File Gateway audit logs.

Q: When does each monthly billing cycle begin?

The billing system follows Coordinated Universal Time (UTC). The calendar month begins at 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.

Q: How much does the hardware appliance cost?

Please refer to the Storage Gateway pricing page for the current pricing. You may also request a sales quote from the AWS Storage Gateway console.

Q: How do I pay for the hardware appliance?

You purchase the hardware appliance through a streamlined procurement process that is integrated in the AWS Console. You will need to submit a purchase order after receiving a sales quote, or you can arrange for pre-payment.

Q: Can I lease or rent the hardware appliance?

No. You pay the full price at the time of purchase.

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.

Q: Who do I call for support related to the hardware appliance?

You contact AWS Support, who provides AWS Storage Gateway software and service support. AWS Support also coordinates all hardware related cases with the hardware manufacturer's support team. We recommend that you purchase AWS Premium Support.

Q: Where do I find the service tag for the hardware appliance (also known as the serial number)?

The service tag for the hardware appliance can be found in the Hardware view of the AWS Storage Gateway console.

Q: What if there is a hardware problem with the hardware appliance?

AWS Support works with the hardware manufacturer for hardware support. Hardware support is included with your appliance purchase and includes 36 months of 24/7 phone support and next-business-day, on-site service for parts replacement.

Q: What are the warranty terms of the hardware appliance?

The hardware appliance comes with 3 years of warranty and next business day onsite service for parts replacement provided by the hardware manufacturer. You can find warranty information here.

Learn more about AWS Storage Gateway pricing

Visit the pricing page

Ready to build?

Get started with AWS Storage Gateway

Have more questions?
Contact us

AWS for the Edge

Bringing data processing and analysis closer to end-points

What's New with AWS

Learn about the latest products, services, and more

Learn Cloud Fundamentals in 3 Hours | 9 June, 2022

Get started with AWS Cloud through step-by-step guides and video tutorials. Register now »

AWSOME DAY
ONLINE CONFERENCE

Sign In to the Console

Learn About AWS

- What Is AWS?
- What Is Cloud Computing?
- AWS Inclusion, Diversity & Equity
- What Is DevOps?
- What Is a Container?
- What Is a Data Lake?
- AWS Cloud Security
- What's New
- Blogs
- Press Releases

Resources for AWS

- Getting Started
- Training and Certification
- AWS Solutions Portfolio
- Architecture Center
- Product and Technical FAQs
- Analyst Reports
- AWS Partners

Developers on AWS

- Developer Center
- SDKs & Tools
- .NET on AWS
- Python on AWS
- Java on AWS
- PHP on AWS
- JavaScript on AWS

Help

Contact Us

File a Support Ticket

Knowledge Center

AWS re:Post

AWS Support Overview

Legal

AWS Careers

Sign In to the Console

Amazon is an Equal Opportunity Employer: *Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.*

Language

عربي |
Bahasa Indonesia |
Deutsch |
English |
Español |
Français |
Italiano |
Português |
Tiếng Việt |
Türkçe |
Русский |
ไทย |
日本語 |
한국어 |
中文 (简体) |
中文 (繁體)

Privacy
|
Site Terms
|
Cookie Preferences
|