S3

Q: How much data can I store in Amazon S3?

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes. For objects larger than 100 megabytes, customers should consider using the [Multipart Upload](https://docs.aws.amazon.com/AmazonS3/latest/dev/UploadingObjects.html) capability.

Q: How is Amazon S3 data organized?

Amazon S3 is a simple key-based object store. When you store data, you assign a unique object key that can later be used to retrieve the data. Keys can be any string, and they can be constructed to mimic hierarchical attributes. Alternatively, you can use S3 Object Tagging to organize your data across all of your S3 buckets and/or prefixes.

Q: What is the consistency model for Amazon S3?

Amazon S3 delivers strong read-after-write consistency automatically, without changes to performance or availability, without sacrificing regional isolation for applications, and at no additional cost.

After a successful write of a new object or an overwrite of an existing object, any subsequent read request immediately receives the latest version of the object. S3 also provides strong consistency for list operations, so after a write, you can immediately perform a listing of the objects in a bucket with any changes reflected.

Q: Why does strong read-after-write consistency help me?

Strong read-after-write consistency helps when you need to immediately read an object after a write. For example, strong read-after-write consistency when you often read and list immediately after writing objects. High-performance computing workloads also benefit in that when an object is overwritten and then read many times simultaneously, strong read-after-write consistency provides assurance that the latest write is read across all reads. These applications automatically and immediately benefit from strong read-after-write consistency. S3 strong consistency also reduces costs by removing the need for extra infrastructure to provide strong consistency.

Q: What are Amazon S3 Event Notifications?

Amazon S3 event notifications can be sent in response to actions in Amazon S3 like PUTs, POSTs, COPYs, or DELETEs. Notification messages can be sent through either [Amazon SNS](https://aws.amazon.com/sns/), [Amazon SQS](https://aws.amazon.com/sqs/), or directly to [AWS Lambda](https://aws.amazon.com/lambda/).

Q:  What can I do with Amazon S3 event notifications?

Amazon S3 event notifications enable you to run workflows, send alerts, or perform other actions in response to changes in your objects stored in S3. You can use S3 event notifications to set up triggers to perform actions including transcoding media files when they are uploaded, processing data files when they become available, and synchronizing S3 objects with other data stores. You can also set up event notifications based on object name prefixes and suffixes. For example, you can choose to receive notifications on object names that start with “images/."

Q:  What is S3 Transfer Acceleration?

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration leverages Amazon CloudFront’s globally distributed AWS Edge Locations. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path.

Q:     Can I use S3 Transfer Acceleration with multipart uploads?

Yes, S3 Transfer Acceleration supports all bucket level features including multipart uploads.

Q:      How should I choose between S3 Transfer Acceleration and Amazon CloudFront’s PUT/POST?

S3 Transfer Acceleration optimizes the TCP protocol and adds additional intelligence between the client and the S3 bucket, making S3 Transfer Acceleration a better choice if a higher throughput is desired. If you have objects that are smaller than 1GB or if the data set is less than 1GB in size, you should consider using Amazon CloudFront's PUT/POST commands for optimal performance.

Q:  How secure is my data in Amazon S3?

Amazon S3 is secure by default. Upon creation, only the resource owners have access to Amazon S3 resources they create. Amazon S3 supports user authentication to control access to data. You can use access control mechanisms such as bucket policies and Access Control Lists (ACLs) to selectively grant permissions to users and groups of users. The Amazon S3 console highlights your publicly accessible buckets, indicates the source of public accessibility, and also warns you if changes to your bucket policies or bucket ACLs would make your bucket publicly accessible. You should enable Block Public Access for all accounts and buckets that you do not want publicly accessible.

You can securely upload/download your data to Amazon S3 via SSL endpoints using the HTTPS protocol. If you need extra security you can use the Server-Side Encryption (SSE) option to encrypt data stored at rest. You can configure your Amazon S3 buckets to automatically encrypt objects before storing them if the incoming storage requests do not have any encryption information. Alternatively, you can use your own encryption libraries to encrypt data before storing it in Amazon S3.

Q:  How can I control access to my data stored on Amazon S3?

Customers may use four mechanisms for controlling access to Amazon S3 resources: Identity and Access Management (IAM) policies, bucket policies, Access Control Lists (ACLs), and Query String Authentication. IAM enables organizations with multiple employees to create and manage multiple users under a single AWS account. With IAM policies, customers can grant IAM users fine-grained control to their Amazon S3 bucket or objects while also retaining full control over everything the users do. With bucket policies, customers can define rules which apply broadly across all requests to their Amazon S3 resources, such as granting write privileges to a subset of Amazon S3 resources. Customers can also restrict access based on an aspect of the request, such as HTTP referrer and IP address. With ACLs, customers can grant specific permissions (i.e. READ, WRITE, FULL\_CONTROL) to specific users for an individual bucket or object. With Query String Authentication, customers can create a URL to an Amazon S3 object which is only valid for a limited time. For more information on the various access control policies available in Amazon S3, please refer to the [Access Control topic](http://docs.amazonwebservices.com/AmazonS3/latest/dev/index.html?UsingAuthAccess.html) in the [Amazon S3 Developer Guide](http://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html).

Q: What is Access Analyzer for S3?

Access Analyzer for S3 is a feature that monitors your access policies, ensuring that the policies provide only the intended access to your S3 resources. Access Analyzer for S3 evaluates your bucket access policies and enables you to discover and swiftly remediate buckets with potentially unintended access.

Q. How do I enable Access Analyzer for S3?

To get started with Access Analyzer for S3, visit the IAM console to enable the [AWS Identity and Access Management (IAM) Access Analyzer](https://aws.amazon.com/iam/features/analyze-access/). When you do this, Access Analyzer for S3 will automatically be visible in the S3 Management Console.

Access Analyzer for S3 is available at no additional cost in the S3 Management Console.

Q: How do I configure Block Public Access (BPA) settings on my access point?

You can configure the Block Public Access (BPA) settings uniquely on each access point at creation time. We are currently working to support changing BPA settings after creation time. Amazon S3 applies the most restrictive combination of the access point-level, bucket-level, and account-level settings.

Q: Can I completely disable direct access to a bucket using the bucket hostname?

Not currently, but you can attach a bucket policy that rejects requests not made using an access point. Refer to the S3 Documentation for more details.

Q: Will I be able to view metrics on operations performed through an access point?

You can monitor and aggregate request metrics on operations performed through an access point using CloudTrail logs and S3 Server Access Logs, and bucket level CloudWatch metrics include requests made through access points.

Q:  How does Versioning protect me from accidental deletion of my objects?

When a user performs a DELETE operation on an object, subsequent simple (un-versioned) requests will no longer retrieve the object. However, all versions of that object will continue to be preserved in your Amazon S3 bucket and can be retrieved or restored. Only the owner of an Amazon S3 bucket can permanently delete a version. You can set [Lifecycle rules](http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html) to manage the lifetime and the cost of storing multiple versions of your objects.

Q:  How can I ensure maximum protection of my preserved versions?

Versioning’s [Multi-Factor Authentication (MFA)](https://aws.amazon.com/mfa/) Delete capability can be used to provide an additional layer of security. By default, all requests to your Amazon S3 bucket require your AWS account credentials. If you enable Versioning with MFA Delete on your Amazon S3 bucket, two forms of authentication are required to permanently delete a version of an object: your AWS account credentials and a valid six-digit code and serial number from an authentication device in your physical possession. To learn more about enabling Versioning with MFA Delete, including how to purchase and activate an authentication device, please refer to the [Amazon S3 Technical Documentation](http://docs.amazonwebservices.com/AmazonS3/latest/dev/Versioning.html).

Q:  What are S3 object tags?

S3 object tags are key-value pairs applied to S3 objects which can be created, updated or deleted at any time during the lifetime of the object. With these, you’ll have the ability to create Identity and Access Management (IAM) policies, setup S3 Lifecycle policies, and customize storage metrics. These object-level tags can then manage transitions between storage classes and expire objects in the background.

Q:  How do I apply object tags to my objects?

You can add tags to new objects when you upload them or you can add them to existing objects. Up to ten tags can be added to each S3 object and you can use either the AWS Management Console, the REST API, the AWS CLI, or the AWS SDKs to add object tags.

Q:  Why should I use object tags?

Object tags are a tool you can use to enable simple management of your S3 storage. With the ability to create, update, and delete tags at any time during the lifetime of your object, your storage can adapt to the needs of your business. These tags allow you to control access to objects tagged with specific key-value pairs, allowing you to further secure confidential data for only a select group or user. Object tags can also be used to label objects that belong to a specific project or business unit, which could be used in conjunction with S3 Lifecycle policies to manage transitions to other storage classes (S3 Standard-IA, S3 One Zone-IA, and S3 Glacier) or with S3 Replication to selectively replicate data between AWS Regions.

Q:  Will my object tags be replicated if I use Cross-Region Replication?

Object tags can be replicated across AWS Regions using Cross-Region Replication. For customers with Cross-Region Replication already enabled, new permissions are required in order for tags to replicate. For more information about setting up Cross-Region Replication, please visit [How to Set Up Cross-Region Replication](http://docs.aws.amazon.com/AmazonS3/latest/dev/crr-how-setup.html) in the [Amazon S3 Developer Guide](http://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html).

Q: What is Amazon S3 Object Lock?

Amazon S3 Object Lock is a new Amazon S3 feature that blocks object version deletion during a customer-defined retention period so that you can enforce retention policies as an added layer of data protection or for regulatory compliance. You can migrate workloads from existing write-once-read-many (WORM) systems into Amazon S3, and configure S3 Object Lock at the object- and bucket-levels to prevent object version deletions prior to pre-defined Retain Until Dates or Legal Hold Dates. S3 Object Lock protection is maintained regardless of which storage class the object resides in and throughout S3 Lifecycle transitions between storage classes.

Q: Why should you use Amazon S3 Object Lock?

You should use S3 Object Lock if you have regulatory requirements that specify that data must be WORM protected, or if you want to add an additional layer of protection to data in Amazon S3. S3 Object Lock can help you to meet regulatory requirements that specify that data should be stored in an immutable format, and also can protect against accidental or malicious deletion for data in Amazon S3.

Q:  How do I get started with S3 CloudWatch Metrics?

You can use the AWS Management Console to enable the generation of 1-minute CloudWatch request metrics for your S3 bucket or configure filters for the metrics using a prefix or object tag. Alternatively, you can call the S3 PUT Bucket Metrics API to enable and configure publication of S3 storage metrics. CloudWatch Request Metrics will be available in CloudWatch within 15 minutes after they are enabled. CloudWatch Storage Metrics are enabled by default for all buckets, and reported once per day.

Q:  What alarms can I set on my storage metrics?

You can use CloudWatch to set thresholds on any of the storage metrics counts, timers, or rates and trigger an action when the threshold is breached. For example, you can set a threshold on the percentage of 4xx Error Responses and when at least 3 data points are above the threshold trigger a CloudWatch alarm to alert a DevOps engineer.

Q: What features are available to analyze my storage usage on Amazon S3?

S3 Storage Lens delivers organization-wide visibility into object storage usage, activity trends, and makes actionable recommendations to improve cost-efficiency and apply data protection best practices. S3 Storage Class Analysis enables you to monitor access patterns across objects to help you decide when to transition data to the right storage class to optimize costs. You can then use this information to configure an S3 Lifecycle policy that makes the data transfer. Amazon S3 Inventory provides a report of your objects and their corresponding metadata on a daily or weekly basis for an S3 bucket or prefix. This report can be used to help meet business, compliance, and regulatory needs by verifying the encryption, and replication status of your objects.

Q:  What is "Query in Place" functionality?

Amazon S3 allows customers to run sophisticated queries against data stored without the need to move data into a separate analytics platform. The ability to query this data in place on Amazon S3 can significantly increase performance and reduce cost for analytics solutions leveraging S3 as a data lake. S3 offers multiple query in place options, including S3 Select, Amazon Athena, and Amazon Redshift Spectrum, allowing you to choose one that best fits your use case. You can even use Amazon S3 Select with AWS Lambda to build serverless apps that can take advantage of the in-place processing capabilities provided by S3 Select.

Q:  What is S3 Select?

S3 Select is an Amazon S3 feature that makes it easy to retrieve specific data from the contents of an object using simple SQL expressions without having to retrieve the entire object. You can use S3 Select to retrieve a subset of data using SQL clauses, like SELECT and WHERE, from objects stored in CSV, JSON, or Apache Parquet format. It also works with objects that are compressed with GZIP or BZIP2 (for CSV and JSON objects only), and server-side encrypted objects.

Q:  Why should I use S3 Select?

S3 Select provides a new way to retrieve specific data using SQL statements from the contents of an object stored in Amazon S3 without having to retrieve the entire object. S3 Select simplifies and improves the performance of scanning and filtering the contents of objects into a smaller, targeted dataset by up to 400%. With S3 Select, you can also perform operational investigations on log files in Amazon S3 without the need to operate or manage a compute cluste

Q:  What is Amazon Athena?

Amazon Athena is an interactive query service that makes it easy to [analyze data in Amazon S3 using standard SQL queries](https://aws.amazon.com/athena/). Athena is serverless, so there is no infrastructure to setup or manage, and you can start analyzing data immediately. You don’t even need to load your data into Athena, it works directly with data stored in any S3 storage class. To get started, just log into the Athena Management Console, define your schema, and start querying. Amazon Athena uses Presto with full standard SQL support and works with a variety of standard data formats, including CSV, JSON, ORC, Apache Parquet and Avro. While Athena is ideal for quick, ad-hoc querying and integrates with Amazon QuickSight for easy visualization, it can also handle complex analysis, including large joins, window functions, and arrays.

Q: Can I use S3 Replication to replicate to more than one destination bucket?  
  
Yes. S3 Replication allows customers to replicate their data to multiple destination buckets in the same, or different AWS Regions. When setting up, you simply specify the new destination bucket in your existing replication configuration or create a new replication configuration with multiple destination buckets. For each new destination you specify, you have the flexibility to choose storage class of destination bucket, encryption type, replication metrics and notifications, Replication Time Control (RTC), and other properties.

Q: Can I use S3 Replication to setup two-way replication between S3 buckets?  
  
Yes. To setup two-way replication, you create a replicate rule from bucket A to bucket B and setup another replication rule from bucket B to bucket A. Make sure to enable replica modification sync on both buckets A and B to replicate replica metadata changes like object access control lists (ACLs), object tags, or object locks on the replicated objects.

* **SES + S3** - The combination of these services only provide email and object storage services.
* Store the session state in Amazon S3" is incorrect as though you can store session data in Amazon S3 and replicate the data to another bucket, this would result in a service interruption if the S3 bucket was not accessible.
* 