S3 Storage Class

S3 Overview

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

Note:
Let's define durability (with respect to an object stored in S3) as the probability that the object will remain intact and accessible after a period of one year. 100% durability would mean that there's no possible way for the object to be lost, 90% durability would mean that there's a 1-in-10 chance, and so forth

Amazon S3 offers a range of storage classes designed for different use cases. These include

S3 Standard

- For general purpose storage of frequently accessed data;

S3 Intelligent-Tiering

- For data with unknown or changing access patterns;

S3 Standard-Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone-IA)

- For long-lived, but less frequently accessed data

Amazon S3 Glacier (S3 Glacier) and Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)

- For long-term archive and digital preservation. Amazon S3 also offers capabilities to manage your data throughout its lifecycle.

Note: Once an S3 Lifecycle policy is set, your data will automatically transfer to a different storage class without any changes to your application.

General purpose

Amazon S3 Standard (S3 Standard)

S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.
S3 Storage Classes can be configured at the object level and a single bucket can contain objects stored across S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA.

You can also use S3 Lifecycle policies to automatically transition objects between storage classes without any application changes.

Key Features:

- Low latency and high throughput performance
- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Resilient against events that impact an entire Availability Zone
- Designed for 99.99% availability over a given year
- Backed with the Amazon S3 Service Level Agreement for availability
- Supports SSL for data in transit and encryption of data at rest
- S3 Lifecycle management for automatic migration of objects to other S3 Storage Classes

Unknown or changing access

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access.

For a small monthly monitoring and automation fee per object, Amazon S3 monitors access patterns of the objects in S3 Intelligent-Tiering, and moves the ones that have not been accessed for 30 consecutive days to the infrequent access tier. If an object in the infrequent access tier is accessed, it is automatically moved back to the frequent access tier. There are no retrieval fees when using the S3 Intelligent-Tiering storage class, and no additional tiering fees when objects are moved between access tiers. It is the ideal storage class for long-lived data with access patterns that are unknown or unpredictable.

S3 Storage Classes can be configured at the object level and a single bucket can contain objects stored in S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA. You can upload objects directly to S3 Intelligent-Tiering, or use S3 Lifecycle policies to transfer objects from S3 Standard and S3 Standard-IA to S3 Intelligent-Tiering. You can also archive objects from S3 Intelligent-Tiering to S3 Glacier.

Key Features:

- Same low latency and high throughput performance of S3 Standard
- Small monthly monitoring and auto-tiering fee
- Automatically moves objects between two access tiers based on changing access patterns
- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Resilient against events that impact an entire Availability Zone
- Designed for 99.9% availability over a given year
- Backed with the Amazon S3 Service Level Agreement for availability
- Supports SSL for data in transit and encryption of data at rest
- S3 Lifecycle management for automatic migration of objects to other S3 Storage Classes

Infrequent access

Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and **per GB retrieval fee**. This combination of low cost and high performance makes S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files.

Key Features:

- Same low latency and high throughput performance of S3 Standard
- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Resilient against events that impact an entire Availability Zone
- Data is resilient in the event of one entire Availability Zone destruction
- Designed for 99.9% availability over a given year
- Backed with the Amazon S3 Service Level Agreement for availability
- Supports SSL for data in transit and encryption of data at rest
- S3 Lifecycle management for automatic migration of objects to other S3 Storage Classes

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum **of three Availability Zones (AZs)**, S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA.

S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. It's a good choice for storing secondary backup copies of on-premises data or easily re-creatable data. You can also use it as cost-effective storage for data that is replicated from another AWS Region using S3 Cross-Region Replication.
S3 One Zone-IA offers the same high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee.

Key Features:

- Same low latency and high throughput performance of S3 Standard
- Designed for durability of 99.999999999% of objects in a single Availability Zone†
- Designed for 99.5% availability over a given year
- Backed with the Amazon S3 Service Level Agreement for availability
- Supports SSL for data in transit and encryption of data at rest
- S3 Lifecycle management for automatic migration of objects to other S3 Storage Classes
- Because S3 One Zone-IA stores data in a single AWS Availability Zone, data stored in this storage class will be lost in the event of Availability Zone destruction.

Archive

Amazon S3 Glacier (S3 Glacier)

S3 Glacier is a secure, durable, and low-cost storage class for data archiving. You can reliably store any amount of data at costs that are competitive with or cheaper than on-premises solutions. To keep costs low yet suitable for varying needs, S3 Glacier provides three retrieval options that range from a few

minutes to hours. You can upload objects directly to S3 Glacier, or use S3 Lifecycle policies to transfer data between any of the S3 Storage Classes for active data (S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA) and S3 Glacier.

Amazon S3 Glacier and S3 Glacier Deep Archive are a secure, durable, and extremely low-cost Amazon S3 cloud storage classes for data archiving and long-term backup. They are designed to deliver 99.999999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. Customers can store data for as little as $1 per terabyte per month, a significant savings compared to on-premises solutions. To keep costs low yet suitable for varying retrieval needs, Amazon S3 Glacier provides three options for access to archives, from a few minutes to several hours, and S3 Glacier Deep Archive provides two access options ranging from 12 to 48 hours.

Key Features:

- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Data is resilient in the event of one entire Availability Zone destruction
- Supports SSL for data in transit and encryption of data at rest
- Low-cost design is ideal for long-term archive
- Configurable retrieval times, from minutes to hours
- S3 PUT API for direct uploads to S3 Glacier, and S3 Lifecycle management for automatic migration of objects

Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)

S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements.

S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases, and is a cost-effective and easy-to-manage alternative to magnetic tape systems, whether they are on-premises libraries or off-premises services.

S3 Glacier Deep Archive complements Amazon S3 Glacier, which is ideal for archives where data is regularly retrieved and some of the data may be needed in minutes. All objects stored in S3 Glacier Deep Archive are replicated and stored across at least three geographically-dispersed Availability Zones, protected by 99.999999999% of durability, and can be restored within **12 hours**.

Key Features:

- Designed for durability of 99.999999999% of objects across multiple Availability Zones
- Lowest cost storage class designed for long-term retention of data that will be retained for 7-10 years
- Ideal alternative to magnetic tape libraries
- Retrieval time within 12 hours
- S3 PUT API for direct uploads to S3 Glacier Deep Archive, and S3 Lifecycle management for automatic migration of objects

Performance across the S3 Storage Classes

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99.9%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128KB	128KB	40KB	40KB
Minimum storage duration charge	N/A	30 days	30 days	30 days	90 days	180 days
Retrieval fee	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	select minutes or hours	select hours
Storage type	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes

- Because S3 One Zone-IA stores data in a single AWS Availability Zone, data stored in this storage class will be lost in the event of Availability Zone destruction.
- S3 Intelligent-Tiering charges a small tiering fee and has a minimum eligible object size of 128KB for auto-tiering.
- Smaller objects may be stored but will always be charged at the Frequent Access tier rates. See the Amazon S3 Pricing for more information.

FAQ

General

Q: What is Amazon S3?

Amazon S3 is object storage built to store and retrieve any amount of data from anywhere on the Internet. It's a simple storage service that offers an extremely durable, highly available, and infinitely scalable data storage infrastructure at very low costs.

Q: What can I do with Amazon S3?

Amazon S3 provides a simple web service interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web. Using this web service, you can easily build applications that make use of Internet storage. Since Amazon S3 is highly scalable and you only pay for what you use, you can start small and grow your application as you wish, with no compromise on performance or reliability.

Amazon S3 is also designed to be highly flexible. Store any type and amount of data that you want; read the same piece of data a million times or only for emergency disaster recovery; build a simple FTP

application, or a sophisticated web application such as the Amazon.com retail web site. Amazon S3 frees developers to focus on innovation instead of figuring out how to store their data.

Q: How can I get started using Amazon S3?

To sign up for Amazon S3, click this link. You must have an Amazon Web Services account to access this service; if you do not already have one, you will be prompted to create one when you begin the Amazon S3 sign-up process. After signing up, please refer to the Amazon S3 documentation and sample code in the Resource Center to begin using Amazon S3.

Q: What can developers do with Amazon S3 that they could not do with an on-premises solution?

Amazon S3 enables any developer to leverage Amazon's own benefits of massive scale with no up-front investment or performance compromises. Developers are now free to innovate knowing that no matter how successful their businesses become, it will be inexpensive and simple to ensure their data is quickly accessible, always available, and secure.

Q: What kind of data can I store in Amazon S3?

You can store virtually any kind of data in any format. Please refer to the Amazon Web Services Licensing Agreement for details.

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 capability. The multipart upload API is designed to improve the upload experience for larger objects. You can upload objects in parts. These object parts can be uploaded independently, in any order, and in parallel. You can use a multipart upload for objects from 5 MB to 5 TB in size.

Q: What storage classes does Amazon S3 offer?

Amazon S3 offers a range of storage classes designed for different use cases. These include S3 Standard for general-purpose storage of frequently accessed data; S3 Intelligent-Tiering for data with unknown or changing access patterns; S3 Standard-Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone-IA) for long-lived, but less frequently accessed data; and Amazon S3 Glacier (S3 Glacier) and Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive) for long-term archive and digital preservation. You can learn more about these storage classes on the Amazon S3 Storage Classes page.

Q: What does Amazon do with my data in Amazon S3?

Amazon will store your data and track its associated usage for billing purposes. Amazon will not otherwise access your data for any purpose outside of the Amazon S3 offering, except when required to do so by law. Please refer to the Amazon Web Services Licensing Agreement for details.

Q: Does Amazon store its own data in Amazon S3?

Yes. Developers within Amazon use Amazon S3 for a wide variety of projects. Many of these projects use Amazon S3 as their authoritative data store and rely on it for business-critical operations.

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: How do I interface with Amazon S3?

Amazon S3 provides a simple, standards-based REST web services interface that is designed to work with any Internet-development toolkit. The operations are intentionally made simple to make it easy to add new distribution protocols and functional layers.

Q: How reliable is Amazon S3?

Amazon S3 gives any developer access to the same highly scalable, highly available, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites. The S3 Standard storage class is designed for 99.99% availability, the S3 Standard-IA storage class is designed for 99.9% availability, the S3 One Zone-IA storage class is designed for 99.5% availability, and the S3 Glacier and S3 Glacier Deep Archive class are designed for 99.99% availability and SLA of 99.9%. All of these storage classes are backed by the Amazon S3 Service Level Agreement.

Q: How will Amazon S3 perform if traffic from my application suddenly spikes?

Amazon S3 was designed from the ground up to handle traffic for any Internet application. Pay-as-you-go pricing and unlimited capacity ensures that your incremental costs don't change and that your service is not interrupted. Amazon S3's massive scale enables us to spread load evenly, so that no individual application is affected by traffic spikes.

Q: Does Amazon S3 offer a Service Level Agreement (SLA)?

Yes. The Amazon S3 SLA provides for a service credit if a customer's monthly uptime percentage is below our service commitment in any billing cycle.

Q: What is a Provisioned Capacity Unit (PCU) and when should it use PCU?

Provisioned Capacity guarantees that your retrieval capacity for Expedited retrievals will be available when you need it. Each unit of capacity ensures that at least 3 expedited retrievals can be performed every 5 minutes and provides up to 150MB/s of retrieval throughput. Retrieval capacity can be provisioned if you have specific Expedited retrieval rate requirements that need to be met. Without provisioned capacity, Expedited retrieval requests will be accepted if capacity is available at the time the request is made. You can purchase provisioned capacity using the console, SDK, or the CLI. Each unit of provisioned capacity costs $100 per month from the date of purchase.

AWS Regions

Q: Where is my data stored?

You specify an AWS Region when you create your Amazon S3 bucket. For S3 Standard, S3 Standard-IA, and S3 Glacier storage classes, your objects are automatically stored across multiple devices spanning a

minimum of three Availability Zones, each separated by miles across an AWS Region. Objects stored in the S3 One Zone-IA storage class are stored redundantly within a single Availability Zone in the AWS Region you select. Please refer to Regional Products and Services for details of Amazon S3 service availability by AWS Region.

Q: What is an AWS Region?

An AWS Region is a geographic location where AWS provides multiple, physically separated and isolated Availability Zones which are connected with low latency, high throughput, and highly redundant networking.

Q: What is an AWS Availability Zone (AZ)?

An AWS Availability Zone is a physically isolated location within an AWS Region. Within each AWS Region, S3 operates in a minimum of three AZs, each separated by miles to protect against local events like fires, floods, etc.
Amazon S3 Standard, S3 Standard-Infrequent Access, and S3 Glacier storage classes replicate data across a minimum of three AZs to protect against the loss of one entire AZ.

This remains true in Regions where fewer than three AZs are publicly available. Objects stored in these storage classes are available for access from all of the AZs in an AWS Region.
The Amazon S3 One Zone-IA storage class replicates data within a single AZ. Data stored in this storage class is susceptible to loss in an AZ destruction event.

Q: How do I decide which AWS Region to store my data in?

There are several factors to consider based on your specific application. You may want to store your data in a Region that…
...is near to your customers, your data centers, or your other AWS resources in order to reduce data access latencies.
...is remote from your other operations for geographic redundancy and disaster recovery purposes.
...enables you to address specific legal and regulatory requirements.
...allows you to reduce storage costs. You can choose a lower priced region to save money

Q: In which parts of the world is Amazon S3 available?

Amazon S3 is available in AWS Regions worldwide, and you can use Amazon S3 regardless of your location. You just have to decide which AWS Region(s) you want to store your Amazon S3 data. See the AWS Regional Availability Table for a list of AWS Regions in which S3 is available today.

Billing

Q: How much does Amazon S3 cost?

With Amazon S3, you pay only for what you use. There is no minimum fee. You can estimate your monthly bill using the AWS Pricing Calculator.
We charge less where our costs are less. Some prices vary across Amazon S3 Regions. Billing prices are based on the location of your bucket. There is no Data Transfer charge for data transferred within an Amazon S3 Region via a COPY request. Data transferred via a COPY request between AWS Regions is charged at rates specified in the pricing section of the Amazon S3 detail page. There is no Data Transfer charge for data transferred between Amazon EC2 and Amazon S3 within the same region, for example, data transferred within the US East (Northern Virginia) Region. However, data transferred between

Amazon EC2 and Amazon S3 across all other regions is charged at rates specified on the Amazon S3 pricing page, for example, data transferred between Amazon EC2 US East (Northern Virginia) and Amazon S3 US West (Northern California).

Q: Why do prices vary depending on which Amazon S3 Region I choose?

We charge less where our costs are less. For example, our costs are lower in the US East (Northern Virginia) Region than in the US West (Northern California) Region.

Q: How am I charged for using Versioning?

Normal Amazon S3 rates apply for every version of an object stored or requested. For example, let's look at the following scenario to illustrate storage costs when utilizing Versioning (let's assume the current month is 31 days long):

1) Day 1 of the month: You perform a PUT of 4 GB (4,294,967,296 bytes) on your bucket.
2) Day 16 of the month: You perform a PUT of 5 GB (5,368,709,120 bytes) within the same bucket using the same key as the original PUT on Day 1.

When analysing the storage costs of the above operations, please note that the 4 GB object from Day 1 is not deleted from the bucket when the 5 GB object is written on Day 15. Instead, the 4 GB object is preserved as an older version and the 5 GB object becomes the most recently written version of the object within your bucket. At the end of the month:

Total Byte-Hour usage
[4,294,967,296 bytes x 31 days x (24 hours / day)] + [5,368,709,120 bytes x 16 days x (24 hours / day)] = 5,257,039,970,304 Byte-Hours.

Conversion to Total GB-Months
5,257,039,970,304 Byte-Hours x (1 GB / 1,073,741,824 bytes) x (1 month / 744 hours) = 6.581 GB-Month

The fee is calculated based on the current rates for your region on the Amazon S3 Pricing page.

Q: How am I charged for accessing Amazon S3 through the AWS Management Console?

Normal Amazon S3 pricing applies when accessing the service through the AWS Management Console. To provide an optimized experience, the AWS Management Console may proactively execute requests. Also, some interactive operations result in more than one request to the service.

Q: How am I charged if my Amazon S3 buckets are accessed from another AWS account?

Normal Amazon S3 pricing applies when your storage is accessed by another AWS Account. Alternatively, you may choose to configure your bucket as a Requester Pays bucket, in which case the requester will pay the cost of requests and downloads of your Amazon S3 data.

You can find more information on Requester Pays bucket configurations in the Amazon S3 Documentation.

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 AWS services is subject to Japanese Consumption Tax.

Learn more about taxes on AWS services »

Security

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 in the Amazon S3 Developer Guide.

Q: Does Amazon S3 support data access auditing?

Yes, customers can optionally configure an Amazon S3 bucket to create access log records for all requests made against it. Alternatively, customers who need to capture IAM/user identity information in their logs can configure AWS CloudTrail Data Events.

These access log records can be used for audit purposes and contain details about the request, such as the request type, the resources specified in the request, and the time and date the request was processed.

Q: What options do I have for encrypting data stored on Amazon S3?

You can choose to encrypt data using SSE-S3, SSE-C, SSE-KMS, or a client library such as the Amazon S3 Encryption Client. All four enable you to store sensitive data encrypted at rest in Amazon S3.

SSE-S3 provides an integrated solution where Amazon handles key management and key protection using multiple layers of security. You should choose SSE-S3 if you prefer to have Amazon manage your keys.

SSE-C enables you to leverage Amazon S3 to perform the encryption and decryption of your objects while retaining control of the keys used to encrypt objects. With SSE-C, you don't need to implement or use a client-side library to perform the encryption and decryption of objects you store in Amazon S3, but you do need to manage the keys that you send to Amazon S3 to encrypt and decrypt objects. Use SSE-C if you

want to maintain your own encryption keys, but don't want to implement or leverage a client-side encryption library.

SSE-KMS enables you to use AWS Key Management Service (AWS KMS) to manage your encryption keys. Using AWS KMS to manage your keys provides several additional benefits. With AWS KMS, there are separate permissions for the use of the master key, providing an additional layer of control as well as protection against unauthorized access to your objects stored in Amazon S3. AWS KMS provides an audit trail so you can see who used your key to access which object and when, as well as view failed attempts to access data from users without permission to decrypt the data. Also, AWS KMS provides additional security controls to support customer efforts to comply with PCI-DSS, HIPAA/HITECH, and FedRAMP industry requirements.

Using an encryption client library, such as the Amazon S3 Encryption Client, you retain control of the keys and complete the encryption and decryption of objects client-side using an encryption library of your choice. Some customers prefer full end-to-end control of the encryption and decryption of objects; that way, only encrypted objects are transmitted over the Internet to Amazon S3. Use a client-side library if you want to maintain control of your encryption keys, are able to implement or use a client-side encryption library, and need to have your objects encrypted before they are sent to Amazon S3 for storage.

For more information on using Amazon S3 SSE-S3, SSE-C, or SSE-KMS, please refer to the topic on Using Encryption in the Amazon S3 Developer Guide.

Q: Can I comply with EU data privacy regulations using Amazon S3?

Customers can choose to store all data in the EU by using the EU (Frankfurt), EU (Ireland), EU (London), or EU (Paris) region. It is your responsibility to ensure that you comply with EU privacy laws. Please see the AWS GDPR Center for more information.

Q: Where can I find more information about security on AWS?

For more information on security on AWS please refer to the AWS security page.

Q: What is an Amazon VPC Endpoint for Amazon S3?

An Amazon VPC Endpoint for Amazon S3 is a logical entity within a VPC that allows connectivity only to S3. The VPC Endpoint routes requests to S3 and routes responses back to the VPC. For more information about VPC Endpoints, read Using VPC Endpoints.

Q: Can I allow a specific Amazon VPC Endpoint access to my Amazon S3 bucket?

You can limit access to your bucket from a specific Amazon VPC Endpoint or a set of endpoints using Amazon S3 bucket policies. S3 bucket policies now support a condition, aws:sourceVpce, that you can use to restrict access. For more details and example policies, read Using VPC Endpoints.

Q: What is Amazon Macie?

Amazon Macie is an AI-powered security service that helps you prevent data loss by automatically discovering, classifying, and protecting sensitive data stored in Amazon S3. Amazon Macie uses machine learning to recognize sensitive data such as personally identifiable information (PII) or intellectual property, assigns a business value, and provides visibility into where this data is stored and how it is being used in your organization. Amazon Macie continuously monitors data access activity for anomalies, and delivers alerts when it detects risk of unauthorized access or inadvertent data leaks.

Q: What can I do with Amazon Macie?

You can use Amazon Macie to protect against security threats by continuously monitoring your data and account credentials. Amazon Macie gives you an automated and low touch way to discover and classify your business data. It provides controls via templated Lambda functions to revoke access or trigger password reset policies upon the discovery of suspicious behavior or unauthorized data access to entities or third-party applications. When alerts are generated, you can use Amazon Macie for incident response, using Amazon CloudWatch Events to swiftly take action to protect your data.

Q: How does Amazon Macie secure your data?

As part of the data classification process, Amazon Macie identifies customers' objects in their S3 buckets, and streams the object contents into memory for analysis. When deeper analysis is required for complex file formats, Amazon Macie will download a full copy of the object, only keeping it for the short time it takes to fully analyze the object. Immediately after Amazon Macie has analyzed the file content for data classification, it deletes the stored content and only retains the metadata required for future analysis. At any time, customers can revoke Amazon Macie access to data in the Amazon S3 bucket. For more information, go to the Amazon Macie User Guide.

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 does Access Analyzer for S3 work?

Access Analyzer for S3 alerts you when you have a bucket that is configured to allow access to anyone on the internet or that is shared with other AWS accounts. You receive insights or 'findings' into the source and level of public or shared access. For example, Access Analyzer for S3 will proactively inform you if read or write access were unintendedly provided through an access control list (ACL) or bucket policy. With these insights, you can immediately set or restore the intended access policy.

When reviewing results that show potentially shared access to a bucket, you can Block All Public Access to the bucket with a single click in the S3 Management console. You can also drill down into bucket level permission settings to configure granular levels of access.

For specific and verified use cases that require public access, such as static website hosting, you can acknowledge and archive the findings on a bucket to record that you intend for the bucket to remain public or shared. You can revisit and modify these bucket configurations at any time. For auditing purposes, Access Analyzer for S3 findings can be downloaded as a CSV report.

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. 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.

S3 Access Points

Q: What is Amazon S3 Access Points?

Today, customers manage access to their S3 buckets using a single bucket policy that controls access for hundreds of applications with different permission levels.

Amazon S3 Access Points simplifies managing data access at scale for applications using shared data sets on S3. With S3 Access Points, you can now easily create hundreds of access points per bucket, representing a new way of provisioning access to shared data sets. Access Points provide a customized path into a bucket, with a unique hostname and access policy that enforces the specific permissions and network controls for any request made through the access point.

Q: How do S3 Access Points work?

Each S3 Access Point is configured with an access policy specific to a use case or application, and a bucket can have hundreds of access points. For example, you can create an access point for your S3 bucket that grants access for groups of users or applications for your data lake. An Access Point could support a single user or application, or groups of users or applications, allowing separate management of each access point. Each access point is associated with a single bucket and contains a network origin control, and a Block Public Access control. For example, you can create an access point with a network origin control that only permits storage access from your Virtual Private Cloud, a logically isolated section of the AWS Cloud. You can also create an access point with the access point policy configured to only allow access to objects with a defined prefix, such as “finance”.

Because each access point contains a unique DNS name, you can now address existing and new buckets with any name of your choice that is unique within the AWS account and region. Using access points that are restricted to a VPC, you can now have an easy, auditable way to make sure S3 data stays within your VPC. Additionally, you can now use AWS Service Control Policies to require any new access point in their organization to be restricted to VPC only access.

Q: What is the difference between a bucket and an access point?

A bucket is the logical storage container for your objects while an access point provides access to the bucket and its contents. An access point is a separate Amazon resource created for a bucket with an Amazon Resource Name (ARN), hostname (in the format of https://[access_point_name]-[account ID].s3-accesspoint.[region].amazonaws.com), an access control policy, and a network origin control.

Q: Why should I use an access point?

S3 Access Points simplify how you manage data access for your application set to your shared data sets on S3. You no longer have to manage a single, complex bucket policy with hundreds of different permission rules that need to be written, read, tracked, and audited. With S3 Access Points, you can now create application-specific access points permitting access to shared data sets with policies tailored to the specific application.

Using Access Points, you can decompose one large bucket policy into separate, discrete access point policies for each application that needs to access the shared data set. This makes it simpler to focus on building the right access policy for an application, while not having to worry about disrupting what any other application is doing within the shared data set. You can also create a Service Control Policy (SCP) and require that all access points be restricted to a Virtual Private Cloud (VPC), firewalling your data to within your private networks. Using access points, you can easily test new access control policies before migrating applications to the access point, or copying the policy to an existing access point. With S3 Access Points you can specify VPC Endpoint policies that permit access only to access points (and thus buckets) owned by specific account IDs. This simplifies the creation of access policies that permit access to buckets within the same account, while rejecting any other S3 access via the VPC Endpoint. S3 Access points allow you to specify any name that is unique within the account and region. For example, you can now have a “test” access point in every account and region.

Q: How do I get started with S3 Access Points?

You can start creating Access Points on new buckets as well as your existing buckets through the AWS Management Console, the AWS Command Line Interface (CLI), the Application Programming Interface (API), and the AWS Software Development Kit (SDK) client. For example, if your bucket is in the Northern California region under AWS account ID 123456789012 and you want to give data access only to your applications running within VPC 'vpc-1a2b3c4d,' you can now set up a new access point "foo" with a "network origin control" value of vpc using the following command:

aws s3control create-access-point --bucket [bucket name] --name foo --account-id 123456789012 --vpc-configuration VpcId= vpc-1a2b3c4d

If your software uses a hostname to connect to your bucket, specify the new access point hostname ("foo-123456789012.s3-accesspoint.us-west-1.amazonaws.com") and you will begin using the access point. If your software uses a bucket name, after updating to the latest AWS SDK release specify, the access point ARN ('arn:aws:s3:us-west-1: 123456789012:accesspoint/foo') as the bucket name to make requests to your data through this access point. Note that access points do not support the CopyObject API to create a copy of an object that is already stored in S3. We are currently working to support CopyObject with access points.

Q: How do I manage access points?

You can add, view, and delete access points as well as edit access point policies through the S3 console and the CLI. You will also be able to use CloudFormation templates to get started with access points. You can monitor and audit access point operations such as "create access point" and "delete access point" through AWS CloudTrail logs. You can control access point usage using AWS Organizations support for AWS SCPs.

Q: Does this change how I create buckets?

No. When you create a bucket, there will be no access points attached to the bucket.

Q: What happens to my existing S3 buckets that do not have any access points attached to them?

You can continue to access existing buckets directly using the bucket hostname. These buckets without access points will continue to function the same way as they always have. No changes are needed to manage them.

Q: When using an access point, how are requests authorized?

S3 access points have their own IAM access point policy. You write access point policies like you would a bucket policy, using the access point ARN as the resource. Access point policies can grant or restrict access to the S3 data requested through the access point. Amazon S3 evaluates all the relevant policies, including those on the user, bucket, access point, VPC Endpoint, and service control policies as well as Access Control Lists, to decide whether to authorize the request.

Q: How do I write access point policies?

You can write an access point policies just like a bucket policy, using IAM rules to govern permissions and the access point ARN in the policy document.

Q: How is restricting access to specific VPCs using network origin controls on access points different from restricting access to VPCs using the bucket policy?

You can continue to use bucket policies to limit bucket access to specified VPCs. Access points provide an easier, auditable way to lock down all or a subset of data in a shared data set to VPC-only traffic for all

applications in your organization using API controls. You can use an AWS Organizations Service Control Policy (SCP) to mandate that any access point created in your organization set the "network origin control" API parameter value to "vpc". Then, any new access point created automatically restricts data access to VPC-only traffic. No additional access policy is required to make sure that data requests are processed only from specified VPCs.

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 enforce a "No Internet data access" policy for all access points in my organization?

Yes. To enforce a "No Internet data access" policy for access points in your organization, you would want to make sure all access points enforce VPC only access. To do so, you will write an AWS SCP that only supports the value "vpc" for the "network origin control" parameter in the create_access_point() API. If you had any Internet facing access points that you created previously, they can be removed. You will also need to modify the bucket policy in each of your buckets to further restrict Internet access directly to your bucket through the bucket hostname. Since other AWS services may be directly accessing your bucket, make sure you setup access to allow the AWS services you want by modifying the policy to permit these AWS services. Refer to the S3 documentation for examples of how to do this.

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: Can I replace or remove an access point from a bucket?

Yes. When you remove an access point, any access to the associated bucket through other access points, and through the bucket hostname, will not be disrupted.

Q: How can I control access to access point management APIs (creating new access points, deleting access points)?

Similar to controlling access to bucket management APIs, you can control the use of access point management APIs through IAM user, group, and role policies permissions.

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: Is there a quota on how many access points I can create?

By default, each account can create 1,000 access points per region. Please visit AWS Service Quotas to request an increase in this quota.

Q: Can other AWS services and features use access points?

Yes, some AWS services support using access points, please refer to the S3 documentation for the current list. AWS services and features that currently do not support S3 Access Points can continue to use the bucket hostname to access your bucket. Note we are currently working to support Amazon EMR and the Apache Hadoop S3A client.

Q: What is the cost of Amazon S3 Access Points?

There is no additional charge for access points or buckets that use access points. Usual Amazon S3 request rates apply.

S3 Intelligent-Tiering

Q: What is S3 Intelligent-Tiering?

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) is an S3 storage class for data with unknown access patterns or changing access patterns that are difficult to learn. It is the first cloud storage class that delivers automatic cost savings by moving objects between two access tiers when access patterns change. One tier is optimized for frequent access and the other lower-cost tier is designed for infrequent access.

Objects uploaded or transitioned to S3 Intelligent-Tiering are automatically stored in the frequent access tier. S3 Intelligent-Tiering works by monitoring access patterns and then moving the objects that have not been accessed in 30 consecutive days to the infrequent access tier. If the objects are accessed later, S3 Intelligent-Tiering moves the object back to the frequent access tier. This means all objects stored in S3 Intelligent-Tiering are always available when needed. There are no retrieval fees, so you won't see unexpected increases in storage bills when access patterns change.

Q: Why would I choose to use S3 Intelligent-Tiering?

S3 Intelligent-Tiering is for data with unknown access patterns or changing access patterns that are difficult to learn. It is ideal for data sets where you may not be able to anticipate access patterns. S3 Intelligent-Tiering can also be used to store new data sets where, shortly after upload, access is frequent, but decreases as the data set ages. Then you can move the data set to S3 One Zone-IA or archive it to S3 Glacier.

Q: What performance does S3 Intelligent-Tiering offer?

S3 Intelligent-Tiering provides the same performance as S3 Standard storage.

Q: How durable and available is S3 Intelligent-Tiering?

S3 Intelligent-Tiering is designed for the same 99.999999999% durability as S3 Standard. S3 Intelligent-Tiering is designed for 99.9% availability, and carries a service level agreement providing service credits if availability is less than our service commitment in any billing cycle.

Q: How do I get my data into S3 Intelligent-Tiering?

There are two ways to get data into S3 Intelligent-Tiering. You can directly PUT into S3 Intelligent-Tiering by specifying INTELLIGENT_TIERING in the x-amz-storage-class header or set lifecycle policies to transition objects from S3 Standard or S3 Standard-IA to S3 INTELLIGENT_TIERING.

Q: Are my S3 Intelligent-Tiering objects backed by the Amazon S3 Service Level Agreement?

Yes, S3 Intelligent-Tiering is backed with the Amazon S3 Service Level Agreement, and customers are eligible for service credits if availability is less than our service commitment in any billing cycle.

Q: How will my latency and throughput performance be impacted as a result of using S3 Intelligent-Tiering

You should expect the same latency and throughput performance as S3 Standard when using S3 Intelligent-Tiering.

Q: Is there a minimum duration for S3 Intelligent-Tiering?

S3 Intelligent-Tiering has a minimum storage duration of 30 days, which means that data that is deleted, overwritten, or transitioned to a different S3 Storage Class before 30 days will incur the normal usage charge plus a pro-rated charge for the remainder of the 30-day minimum.

Q: Is there a minimum object size for S3 Intelligent-Tiering?
S3 Intelligent-Tiering has no minimum billable object size, but objects smaller than 128KB are not eligible for auto-tiering and will always be stored at the frequent access tier rate.
Q: Can I tier objects from S3 Intelligent-Tiering to the Amazon S3 Glacier storage class?
Yes. In addition to using lifecycle policies to migrate objects from S3 Intelligent-Tiering to S3 One Zone-IA, you can also set up lifecycle policies to archive objects to S3 Glacier.
Q: Can I have a bucket that has different objects in different storage classes?
Yes, you can have a bucket that has different objects stored in S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA.
Q: Is S3 Intelligent-Tiering available in all AWS Regions in which Amazon S3 operates?
Yes

S3 Standard-Infrequent Access (S3 Standard-IA)

Q: What is S3 Standard-Infrequent Access?
Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. S3 Standard-IA offers the high durability, throughput, and low latency of the Amazon S3 Standard storage class, with a low per-GB storage price and per-GB retrieval fee. This combination of low cost and high performance make S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery. The S3 Standard-IA storage class is set at the object level and can exist in the same bucket as the S3 Standard or S3 One Zone-IA storage classes, allowing you to use S3 Lifecycle policies to automatically transition objects between storage classes without any application changes.
Q: Why would I choose to use S3 Standard-IA?
S3 Standard-IA is ideal for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA is ideally suited for long-term file storage, older sync and share storage, and other aging data.
Q: What performance does S3 Standard-IA offer?
S3 Standard-IA provides the same performance as the S3 Standard and S3 One Zone-IA storage classes.

Q: How durable and available is S3 Standard-IA?
S3 Standard-IA is designed for the same 99.999999999% durability as the S3 Standard and S3 Glacier storage classes. S3 Standard-IA is designed for 99.9% availability, and carries a service level agreement providing service credits if availability is less than our service commitment in any billing cycle.
Q: How do I get my data into S3 Standard-IA?
There are two ways to get data into S3 Standard-IA. You can directly PUT into S3 Standard-IA by specifying STANDARD_IA in the x-amz-storage-class header. You can also set Lifecycle policies to transition objects from the S3 Standard to the S3 Standard-IA storage class.
Q: Are my S3 Standard-IA objects backed by the Amazon S3 Service Level Agreement?
Yes, S3 Standard-IA is backed with the Amazon S3 Service Level Agreement, and customers are eligible for service credits if availability is less than our service commitment in any billing cycle.
Q: How will my latency and throughput performance be impacted as a result of using S3 Standard-IA?
You should expect the same latency and throughput performance as the S3 Standard storage class when using S3 Standard-IA.
Q: How am I charged for using S3 Standard-IA?
Please see the Amazon S3 pricing page for general information about S3 Standard-IA pricing.
Q: What charges will I incur if I change the storage class of an object from S3 Standard-IA to S3 Standard with a COPY request?
You will incur charges for an S3 Standard-IA COPY request and an S3 Standard-IA data retrieval.

Q: Is there a minimum storage duration charge for S3 Standard-IA?

S3 Standard-IA is designed for long-lived but infrequently accessed data that is retained for months or years. Data that is deleted from S3 Standard-IA within 30 days will be charged for a full 30 days. Please see the Amazon S3 pricing page for information about S3 Standard-IA pricing.

Q: Is there a minimum object storage charge for S3 Standard-IA?

S3 Standard-IA is designed for larger objects and has a minimum object storage charge of 128KB. Objects smaller than 128KB in size will incur storage charges as if the object were 128KB. For example, a 6KB object in S3 Standard-IA will incur S3 Standard-IA storage charges for 6KB and an additional minimum object size fee equivalent to 122KB at the S3 Standard-IA storage price. Please see the Amazon S3 pricing page for information about S3 Standard-IA pricing.

Q: Can I tier objects from S3 Standard-IA to S3 One Zone-IA or S3 Glacier?

Yes. In addition to using Lifecycle policies to migrate objects from S3 Standard to S3 Standard-IA, you can also set up Lifecycle policies to tier objects from S3 Standard-IA to S3 One Zone-IA or S3 Glacier.

S3 One Zone-Infrequent Access (S3 One Zone-IA)

Q: What is S3 One Zone-IA storage class?

S3 One Zone-IA storage class is an Amazon S3 storage class that customers can choose to store objects in a single availability zone. S3 One Zone-IA storage redundantly stores data within that single Availability Zone to deliver storage at 20% less cost than geographically redundant S3 Standard-IA storage, which stores data redundantly across multiple geographically separate Availability Zones.

S3 One Zone-IA offers a 99% available SLA and is also designed for eleven 9's of durability within the Availability Zone. But, unlike the S3 Standard and S3 Standard-IA storage classes, data stored in the S3 One Zone-IA storage class will be lost in the event of Availability Zone destruction.

S3 One Zone-IA storage offers the same Amazon S3 features as S3 Standard and S3 Standard-IA and is used through the Amazon S3 API, CLI and console. S3 One Zone-IA storage class is set at the object level and can exist in the same bucket as S3 Standard and S3 Standard-IA storage classes. You can use S3 Lifecycle policies to automatically transition objects between storage classes without any application changes.

Q: What use cases are best suited for S3 One Zone-IA storage class?

Customers can use S3 One Zone-IA for infrequently-accessed storage, like backup copies, disaster recovery copies, or other easily re-creatable data.

Q: What performance does S3 One Zone-IA storage offer?

S3 One Zone-IA storage class offers the same performance as S3 Standard and S3 Standard-Infrequent Access storage.

Q: How durable is the S3 One Zone-IA storage class?

S3 One Zone-IA storage class is designed for 99.999999999% of durability within an Availability Zone. However, S3 One Zone-IA storage is not designed to withstand the loss of availability or total destruction of an Availability Zone, in which case data stored in S3 One Zone-IA will be lost. In contrast, S3 Standard, S3 Standard-Infrequent Access, and S3 Glacier storage are designed to withstand loss of availability or the destruction of an Availability Zone. S3 One Zone-IA can deliver the same or better durability and availability than most modern, physical data centers, while providing the added benefit of elasticity of storage and the Amazon S3 feature set.

Q: What is the availability SLA for S3 One Zone-IA storage class?

S3 One Zone-IA offers a 99% availability SLA. For comparison, S3 Standard offers a 99.9% availability SLA and S3 Standard-Infrequent Access offers a 99% availability SLA. As with all S3 storage classes, S3 One Zone-IA storage class carries a service level agreement providing service credits if availability is less than our service commitment in any billing cycle. See the Amazon S3 Service Level Agreement.

Q: How will using S3 One Zone-IA storage affect my latency and throughput?

You should expect the same latency and throughput in S3 One Zone-IA storage class to Amazon S3 Standard and S3 Standard-IA storage classes.

Q: How am I charged for using S3 One Zone-IA storage class?

Like S3 Standard-IA, S3 One Zone-IA charges for the amount of storage per month, bandwidth, requests, early delete and small object fees, and a data retrieval fee. Amazon S3 One Zone-IA storage is 20% cheaper than Amazon S3 Standard-IA for storage by month, and shares the same pricing for bandwidth, requests, early delete and small object fees, and the data retrieval fee.

As with S3 Standard-Infrequent Access, if you delete a S3 One Zone-IA object within 30 days of creating it, you will incur an early delete charge. For example, if you PUT an object and then delete it 10 days later, you are still charged for 30 days of storage.

Like S3 Standard-IA, S3 One Zone-IA storage class has a minimum object size of 128KB. Objects smaller than 128KB in size will incur storage charges as if the object were 128KB. For example, a 6KB object in a S3 One Zone-IA storage class will incur storage charges for 6KB and an additional minimum object size fee equivalent to 122KB at the S3 One Zone-IA storage price. Please see the pricing page for information about S3 One Zone-IA pricing.

Q: Is an S3 One Zone-IA "Zone" the same thing as an AWS Availability Zone?

Yes. Each AWS Region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones. The Amazon S3 One Zone-IA storage class uses an individual AWS Availability Zone within the region.

Q: Are there differences between how Amazon EC2 and Amazon S3 work with Availability Zone-specific resources?

Yes. Amazon EC2 provides you the ability to pick the AZ to place resources, such as compute instances, within a region. When you use S3 One Zone-IA, S3 One Zone-IA assigns an AWS Availability Zone in the region according to available capacity.

Q: Can I have a bucket that has different objects in different storage classes and Availability Zones?

Yes, you can have a bucket that has different objects stored in S3 Standard, S3 Standard-IA and S3 One Zone-IA.

Q: Is S3 One Zone-IA available in all AWS Regions in which S3 operates?

Yes.

Q: How much disaster recovery protection do I forgo by using S3 One Zone-IA?

Each Availability Zone uses redundant power and networking. Within an AWS Region, Availability Zones are on different flood plains, earthquake fault zones, and geographically separated for fire protection. S3 Standard and S3 Standard-IA storage classes offer protection against these sorts of disasters by storing your data redundantly in multiple Availability Zones. S3 One Zone-IA offers protection against equipment failure within an Availability Zone, but it does not protect against the loss of the Availability Zone, in which case, data stored in S3 One Zone-IA would be lost. Using S3 One Zone-IA, S3 Standard, and S3 Standard-IA options, you can choose the storage class that best fits the durability and availability needs of your storage.

Amazon S3 Glacier

Q: Why is Amazon Glacier now called Amazon S3 Glacier?

Customers have long thought of Amazon Glacier, our backup and archival storage service, as a storage class of Amazon S3. In fact, a very high percentage of the data stored in Amazon Glacier today comes directly from customers using S3 Lifecycle policies to move cooler data into Amazon Glacier. Now, Amazon Glacier is officially part of S3 and will be known as Amazon S3 Glacier (S3 Glacier). All of the existing Glacier direct APIs continue to work just as they have, but we've now made it even easier to use the S3 APIs to store data in the S3 Glacier storage class.

Q: Does Amazon S3 provide capabilities for archiving objects to lower cost storage classes?

Yes, Amazon S3 enables you to utilize Amazon S3 Glacier's extremely low-cost storage service for data archival. Amazon S3 Glacier stores data for as little as $0.004 per gigabyte per month. To keep costs low yet suitable for varying retrieval needs, Amazon S3 Glacier provides three options for access to archives, ranging from a few minutes to several hours. Some examples of archive uses cases include digital media archives, financial and healthcare records, raw genomic sequence data, long-term database backups, and data that must be retained for regulatory compliance.

Q: How can I store my data using the Amazon S3 Glacier storage class?

If you have storage which should be immediately archived without delay, or if you make business decisions about when to transition objects to S3 Glacier that can't be expressed through an Amazon S3 Lifecycle policy, S3 PUT to Glacier allows you to use S3 APIs to upload to the S3 Glacier storage class on an object-by-object basis. There are no transition delays and you control the timing. This is also a good option if you want your application to make storage class decisions without having to set a bucket-level policy.

You can use Lifecycle rules to automatically archive sets of Amazon S3 objects to S3 Glacier based on object age. Use the Amazon S3 Management Console, the AWS SDKs, or the Amazon S3 APIs to define rules for archival. Rules specify a prefix and time period. The prefix (e.g. "logs/") identifies the object(s) subject to the rule. The time period specifies either the number of days from object creation date (e.g. 180 days) or the specified date after which the object(s) should be archived. Any S3 Standard, S3 Standard-IA, or S3 One Zone-IA objects which have names beginning with the specified prefix and which have aged past the specified time period are archived to S3 Glacier. To retrieve Amazon S3 data stored in S3 Glacier, initiate a retrieval job via the Amazon S3 APIs or Management Console. Once the retrieval job is complete, you can access your data through an Amazon S3 GET object request.

For more information on using Lifecycle rules for archival to S3 Glacier, please refer to the Object Archival topic in the Amazon S3 Developer Guide.

Q: Can I use the Amazon S3 APIs or Management Console to list objects that I've archived to Amazon S3 Glacier?

Yes, like Amazon S3's other storage classes (S3 Standard, S3 Standard-IA, and S3 One Zone-IA), S3 Glacier objects stored using Amazon S3's APIs or Management Console have an associated user-defined name. You can get a real-time list of all of your Amazon S3 object names, including those stored using the S3 Glacier storage class, using the S3 LIST API or the S3 Inventory report.

Q: Can I use Amazon Glacier direct APIs to access objects that I've archived to Amazon S3 Glacier?

No. Because Amazon S3 maintains the mapping between your user-defined object name and Amazon S3 Glacier's system-defined identifier, Amazon S3 objects that are stored using the S3 Glacier storage class are only accessible through the Amazon S3 APIs or the Amazon S3 Management Console.

Q: How can I retrieve my objects that are archived in Amazon S3 Glacier and will I be notified when the object is restored?

To retrieve Amazon S3 data stored in the S3 Glacier storage class, initiate a retrieval request using the Amazon S3 APIs or the Amazon S3 Management Console. The retrieval request creates a temporary copy of your data in the S3 RRS or S3 Standard-IA storage class while leaving the archived data intact in S3 Glacier. You can specify the amount of time in days for which the temporary copy is stored in S3. You can then access your temporary copy from S3 through an Amazon S3 GET request on the archived object.

With restore notifications, you can now be notified with an S3 Event Notification when an object has successfully restored from S3 Glacier and the temporary copy is made available to you. The bucket owner (or others, as permitted by an IAM policy) can arrange for notifications to be issued to Amazon Simple Queue Service (SQS) or Amazon Simple Notification Service (SNS). Notifications can also be delivered to AWS Lambda for processing by a Lambda function.

Q: How long will it take to restore my objects archived in S3 Glacier and can I upgrade an in-progress request to a faster restore speed?

When processing a retrieval job, Amazon S3 first retrieves the requested data from S3 Glacier, and then creates a temporary copy of the requested data in S3 (which typically takes a few minutes). The access time of your request depends on the retrieval option you choose: Expedited, Standard, or Bulk retrievals. For all but the largest objects (250MB+), data accessed using Expedited retrievals are typically made available within 1-5 minutes. Objects retrieved using Standard retrievals typically complete between 3-5 hours. Bulk retrievals typically complete within 5-12 hours. For more information about S3 Glacier retrieval options, please refer to the S3 Glacier FAQs.

S3 Restore Speed Upgrade is an override of an in-progress restore to a faster restore tier if access to the data becomes urgent. You can use S3 Restore Speed Upgrade by issuing another restore request to the same object with a new "tier" job parameter. When issuing an S3 Restore Speed Upgrade, you must choose a faster restore speed than the in-progress restore. Other parameters such as Object Expiry Time will not be changed. You can update the Object Expiry Time after the restore is complete. You pay for each restore request and the per-GB retrieval charge for the faster restore tier. For example, if you issued a Bulk tier restore and then issued an S3 Restore Speed Upgrade request at the Expedited tier to override the in-progress Bulk tier restore, you would be charged for two requests and the per-GB retrieval charge for the Expedited tier.

Q: What am I charged for archiving objects in Amazon S3 Glacier?

Amazon S3 Glacier storage class is priced based on monthly storage capacity and the number of Lifecycle transition requests into Amazon S3 Glacier. Objects that are archived to Amazon S3 Glacier have a minimum of 90 days of storage, and objects deleted before 90 days incur a pro-rated charge equal to the storage charge for the remaining days. See the Amazon S3 pricing page for current pricing.

Q: How is my storage charge calculated for Amazon S3 objects archived to Amazon S3 Glacier?

The volume of storage billed in a month is based on average storage used throughout the month, measured in gigabyte-months (GB-Months). Amazon S3 calculates the object size as the amount of data you stored plus an additional 32KB of Amazon S3 Glacier data plus an additional 8KB of S3 Standard storage class data. Amazon S3 Glacier requires an additional 32KB of data per object for Glacier's index and metadata so you can identify and retrieve your data. Amazon S3 requires 8KB to store and maintain the user-defined name and metadata for objects archived to Amazon S3 Glacier. This enables you to get a real-time list of all of your Amazon S3 objects, including those stored using the Amazon S3 Glacier storage class, using the Amazon S3 LIST API or the S3 Inventory report. For example, if you have archived 100,000 objects that are 1GB each, your billable storage would be:

1.000032 gigabytes for each object x 100,000 objects = 100,003.2 gigabytes of Amazon S3 Glacier storage.

0.000008 gigabytes for each object x 100,000 objects = 0.8 gigabytes of Amazon S3 Standard storage.

The fee is calculated based on the current rates for your AWS Region on the Amazon S3 Pricing Page.

Q: How much data can I retrieve from Amazon S3 Glacier for free?

You can retrieve 10GB of your Amazon S3 Glacier data per month for free with the AWS free tier. The free tier allowance can be used at any time during the month and applies to Amazon S3 Glacier Standard retrievals.

Q: How am I charged for deleting objects from Amazon S3 Glacier that are less than 90 days old?

Amazon S3 Glacier is designed for use cases where data is retained for months, years, or decades. Deleting data that is archived to Amazon S3 Glacier is free if the objects being deleted have been archived in Amazon S3 Glacier for 90 days or longer. If an object archived in Amazon S3 Glacier is deleted or overwritten within 90 days of being archived, there will be an early deletion fee. This fee is prorated. If you delete 1GB of data 30 days after uploading it, you will be charged an early deletion fee for 60 days of

Amazon S3 Glacier storage. If you delete 1 GB of data after 60 days, you will be charged for 30 days of Amazon S3 Glacier storage.

Q: How much does it cost to retrieve data from Amazon S3 Glacier?

There are three ways to restore data from Amazon S3 Glacier – Expedited, Standard, and Bulk Retrievals - and each has a different per-GB retrieval fee and per-archive request fee (i.e. requesting one archive counts as one request). For detailed S3 Glacier pricing by AWS Region, please visit the Amazon S3 Glacier pricing page.

Q: What is the backend infrastructure supporting the S3 Glacier storage class?

We prefer to focus on the customer outcomes of performance, durability, availability, and security. However, this question is often asked by our customers. We use a number of different technologies which allow us to offer the prices we do to our customers. Our services are built using common data storage technologies specifically assembled into purpose-built, cost-optimized systems using AWS-developed software. S3 Glacier benefits from our ability to optimize the sequence of inputs and outputs to maximize efficiency accessing the underlying storage.

Amazon S3 Glacier Deep Archive

Q: What is S3 Glacier Deep Archive?

S3 Glacier Deep Archive is a new Amazon S3 storage class that provides secure and durable object storage for long-term retention of data that is accessed once or twice in a year. From just $0.00099 per GB-month (less than one-tenth of one cent, or about $1 per TB-month), S3 Glacier Deep Archive offers the lowest cost storage in the cloud, at prices significantly lower than storing and maintaining data in on-premises magnetic tape libraries or archiving data off-site.

Q: What use cases are best suited for S3 Glacier Deep Archive?

S3 Glacier Deep Archive is an ideal storage class to provide offline protection of your company's most important data assets, or when long-term data retention is required for corporate policy, contractual, or regulatory compliance requirements. Customers find S3 Glacier Deep Archive to be a compelling choice to protect core intellectual property, financial and medical records, research results, legal documents, seismic exploration studies, and long-term backups, especially in highly regulated industries, such as Financial Services, Healthcare, Oil & Gas, and Public Sectors. In addition, there are organizations, such as media and entertainment companies, that want to keep a backup copy of core intellectual property. Frequently, customers using S3 Glacier Deep Archive are able to reduce or discontinue the use of on-premises magnetic tape libraries and off-premises tape archival services.

Q: How does S3 Glacier Deep Archive differ from S3 Glacier?

S3 Glacier Deep Archive expands our data archiving offerings, enabling you to select the optimal storage class based on storage and retrieval costs, and retrieval times. Choose S3 Glacier when you need to retrieve archived data typically in 1-5 minutes using Expedited retrievals. S3 Glacier Deep Archive, in contrast, is designed for colder data that is very unlikely to be accessed, but still requires long-term, durable storage. S3 Glacier Deep Archive is up to 75% less expensive than S3 Glacier and provides retrieval within 12 hours using the Standard retrieval speed. You may also reduce retrieval costs by selecting Bulk retrieval, which will return data within 48 hours.

Q: How durable and available is S3 Glacier Deep Archive?

S3 Glacier Deep Archive is designed for the same 99.999999999% durability as the S3 Standard and S3 Glacier storage classes. S3 Glacier Deep Archive is designed for 99.99% availability, and carries a service level agreement for 99.9% availability that provides service credits if availability is less than our service commitment in any billing cycle.

Q: Are my S3 Glacier Deep Archive objects backed by Amazon S3 Service Level Agreement?

Yes, S3 Glacier Deep Archive is backed with the Amazon S3 Service Level Agreement, and customers are eligible for service credits if availability is less than our service commitment in any billing cycle.

Q: How do I get started using S3 Glacier Deep Archive?

The easiest way to store data in S3 Glacier Deep Archive is to use the S3 API to upload data directly. Just specify "S3 Glacier Deep Archive" as the storage class. You can accomplish this using the AWS Management Console, S3 REST API, AWS SDKs, or AWS Command Line Interface.

You can also begin using S3 Glacier Deep Archive by creating policies to migrate data using S3 Lifecycle, which provides the ability to define the lifecycle of your object and reduce your cost of storage. These policies can be set to migrate objects to S3 Glacier Deep Archive based on the age of the object. You can specify the policy for an S3 bucket, or for specific prefixes. Lifecycle transitions are billed at the S3 Glacier Deep Archive Upload price.

Tape Gateway, a cloud-based virtual tape library feature of AWS Storage Gateway, now integrates with S3 Glacier Deep Archive, enabling you to store your virtual tape-based, long-term backups and archives in S3 Glacier Deep Archive, thereby providing the lowest cost storage for this data in the cloud. To get started, create a new virtual tape using AWS Storage Gateway Console or API, and set the archival storage target either to S3 Glacier or S3 Glacier Deep Archive. When your backup application ejects the tape, the tape will be archived to your selected storage target.

Q: How do you recommend migrating data from my existing tape archives to S3 Glacier Deep Archive?

There are multiple ways to migrate data from existing tape archives to S3 Glacier Deep Archive. You can use the AWS Tape Gateway to integrate with existing backup applications using a virtual tape library (VTL) interface. This interface presents virtual tapes to the backup application. These can be immediately used to store data in Amazon S3, S3 Glacier, and S3 Glacier Deep Archive.

You can also use AWS Snowball or Snowmobile to migrate data. Snowball and Snowmobile accelerate moving terabytes to petabytes of data into and out of AWS using physical storage devices designed to be secure for transport. Using Snowball and Snowmobile helps to eliminate challenges that can be encountered with large-scale data transfers including high network costs, long transfer times, and security concerns.

Finally, you can use AWS Direct Connect to establish dedicated network connections from your premises to AWS. In many cases, Direct Connect can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

Q: How can I retrieve my objects stored in S3 Glacier Deep Archive?

To retrieve data stored in S3 Glacier Deep Archive, initiate a "Restore" request using the Amazon S3 APIs or the Amazon S3 Management Console. The Restore creates a temporary copy of your data in the S3 One Zone-IA storage class while leaving the archived data intact in S3 Glacier Deep Archive. You can specify the amount of time in days for which the temporary copy is stored in S3. You can then access your temporary copy from S3 through an Amazon S3 GET request on the archived object.

When restoring an archived object, you can specify one of the following options in the Tier element of the request body: Standard is the default tier and lets you access any of your archived objects within 12 hours, and Bulk lets you retrieve large amounts, even petabytes of data inexpensively and typically completes within 48 hours.

Q: How am I charged for using S3 Glacier Deep Archive?

S3 Glacier Deep Archive storage is priced based on the amount of data you store in GBs, the number of PUT/lifecycle transition requests, retrievals in GBs, and number of restore requests. This pricing model is similar to S3 Glacier. Please see the Amazon S3 pricing page for information about S3 Glacier Deep Archive pricing.

Q: How will S3 Glacier Deep Archive usage show up on my AWS bill and in the AWS Cost Management tool?

S3 Glacier Deep Archive usage and cost will show up as an independent service line item on your monthly AWS bill, separate from your Amazon S3 usage and costs. However, if you are using the AWS Cost

Management tool, S3 Glacier Deep Archive usage and cost will be included under the Amazon S3 usage and cost in your detailed monthly spend reports, and not broken out as a separate service line item.

Q: Are there minimum storage duration and minimum object storage charges for S3 Glacier Deep Archive?
S3 Glacier Deep Archive is designed for long-lived but rarely accessed data that is retained for 7-10 years or more. Objects that are archived to S3 Glacier Deep Archive have a minimum of 180 days of storage, and objects deleted before 180 days incur a pro-rated charge equal to the storage charge for the remaining days. Please see the Amazon S3 pricing page for information about S3 Glacier Deep Archive pricing.
S3 Glacier Deep Archive has a minimum billable object storage size of 40KB. Objects smaller than 40KB in size may be stored but will be charged for 40KB of storage. Please see the Amazon S3 pricing page for information about S3 Glacier Deep Archive pricing.

Q: How does S3 Glacier Deep Archive integrate with other AWS Services?
Deep Archive is integrated with Amazon S3 features including S3 Storage Class Analysis, S3 Object Tagging, S3 Lifecycle policies, Composable objects, S3 Object Lock, and S3 Replication. With S3 storage management features, you can use a single Amazon S3 bucket to store a mixture of S3 Glacier Deep Archive, S3 Standard, S3 Standard-IA, S3 One Zone-IA, and S3 Glacier data. This allows storage administrators to make decisions based on the nature of the data and data access patterns. Customers can use Amazon S3 Lifecycle policies to automatically migrate data to lower-cost storage classes as the data ages, or S3 Cross-Region Replication or Same-Region Replication policies to replicate data to the same or a different region.
AWS Storage Gateway service integrates Tape Gateway with S3 Glacier Deep Archive storage class, allowing you to store virtual tapes in the lowest-cost Amazon S3 storage class, reducing the monthly cost to store your long-term data in the cloud by 75%. With this feature, Tape Gateway supports archiving your new virtual tapes directly to S3 Glacier and S3 Glacier Deep Archive, helping you meet your backup, archive, and recovery requirements. Tape Gateway helps you move tape-based backups to AWS without making any changes to your existing backup workflows. Tape Gateway supports most of the leading backup applications such as Veritas, Veeam, Commvault, Dell EMC NetWorker, IBM Spectrum Protect (on Windows OS), and Microsoft Data Protection Manager.
Q: What is the backend infrastructure supporting the S3 Glacier Deep Archive storage class?
In general, AWS does not disclose the backend infrastructure and architecture for our compute, networking, and storage services, as we are more focused on the customer outcomes of performance, durability, availability, and security. However, this question is often asked by our customers. We use a number of different technologies which allow us to offer the prices we do to our customers. Our services are built using common data storage technologies specifically assembled into purpose-built, cost-optimized systems using AWS-developed software. S3 Glacier Deep Archive benefits from our ability to optimize the sequence of inputs and outputs to maximize efficiency accessing the underlying storage.

Query in Place

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: What can I do with S3 Select?

You can use S3 Select to retrieve a smaller, targeted data set from an object using simple SQL statements. You can use S3 Select with AWS Lambda to build serverless applications that use S3 Select to efficiently and easily retrieve data from Amazon S3 instead of retrieving and processing entire object. You can also use S3 Select with Big Data frameworks, such as Presto, Apache Hive, and Apache Spark to scan and filter the data in Amazon S3.

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 cluster.

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. 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: What is Amazon Redshift Spectrum?

Amazon Redshift Spectrum is a feature of Amazon Redshift that enables you to run queries against exabytes of unstructured data in Amazon S3 with no loading or ETL required. When you issue a query, it goes to the Amazon Redshift SQL endpoint, which generates and optimizes a query plan. Amazon Redshift determines what data is local and what is in Amazon S3, generates a plan to minimize the amount of Amazon S3 data that needs to be read, requests Redshift Spectrum workers out of a shared resource pool to read and process data from Amazon S3.

Redshift Spectrum scales out to thousands of instances if needed, so queries run quickly regardless of data size. And, you can use the exact same SQL for Amazon S3 data as you do for your Amazon Redshift queries today and connect to the same Amazon Redshift endpoint using the same BI tools. Redshift Spectrum lets you separate storage and compute, allowing you to scale each independently. You can setup as many Amazon Redshift clusters as you need to query your Amazon S3 data lake, providing high availability and limitless concurrency. Redshift Spectrum gives you the freedom to store your data where you want, in the format you want, and have it available for processing when you need it.

Event Notification

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, Amazon SQS, or directly to AWS 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 included in an Amazon S3 event notification?

For a detailed description of the information included in Amazon S3 event notification messages, please refer to the Configuring Amazon S3 Event Notifications topic in the Amazon S3 Developer Guide.

Q: How do I set up Amazon S3 event notifications?

For a detailed description of how to configure event notifications, please refer to the Configuring Amazon S3 event notifications topic in the Amazon S3 Developer Guide. You can learn more about AWS messaging services in the Amazon SNS Documentation and the Amazon SQS Documentation.

Q: What does it cost to use Amazon S3 event notifications?

There are no additional charges for using Amazon S3 for event notifications. You pay only for use of Amazon SNS or Amazon SQS to deliver event notifications, or for the cost of running an AWS Lambda function. Visit the Amazon SNS, Amazon SQS, or AWS Lambda pricing pages to view the pricing details for these services.

Amazon S3 Transfer Acceleration

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: How do I get started with S3 Transfer Acceleration?

To get started with S3 Transfer Acceleration enable S3 Transfer Acceleration on an S3 bucket using the Amazon S3 console, the Amazon S3 API, or the AWS CLI. After S3 Transfer Acceleration is enabled, you can point your Amazon S3 PUT and GET requests to the s3-accelerate endpoint domain name. Your data transfer application must use one of the following two types of endpoints to access the bucket for faster data transfer: .s3-accelerate.amazonaws.com or .s3-accelerate.dualstack.amazonaws.com for the “dual-stack” endpoint. If you want to use standard data transfer, you can continue to use the regular endpoints. There are certain restrictions on which buckets will support S3 Transfer Acceleration. For details, please refer the Amazon S3 developer guide.

Q: How fast is S3 Transfer Acceleration?

S3 Transfer Acceleration helps you fully utilize your bandwidth, minimize the effect of distance on throughput, and is designed to ensure consistently fast data transfer to Amazon S3 regardless of your client’s location. The amount of acceleration primarily depends on your available bandwidth, the distance between the source and destination, and packet loss rates on the network path. Generally, you will see more acceleration when the source is farther from the destination, when there is more available bandwidth, and/or when the object size is bigger.

One customer measured a 50% reduction in their average time to ingest 300 MB files from a global user base spread across the US, Europe, and parts of Asia to a bucket in the Asia Pacific (Sydney) region. Another customer observed cases where performance improved in excess of 500% for users in South East

Asia and Australia uploading 250 MB files (in parts of 50MB) to an S3 bucket in the US East (N. Virginia) region.

Try the speed comparison tool to get a preview of the performance benefit from your location!

Q: Who should use S3 Transfer Acceleration?

S3 Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets. If you are uploading to a centralized bucket from geographically dispersed locations, or if you regularly transfer GBs or TBs of data across continents, you may save hours or days of data transfer time with S3 Transfer Acceleration.

Q: How secure is S3 Transfer Acceleration?

S3 Transfer Acceleration provides the same security as regular transfers to Amazon S3. All Amazon S3 security features, such as access restriction based on a client's IP address, are supported as well. S3 Transfer Acceleration communicates with clients over standard TCP and does not require firewall changes. No data is ever saved at AWS Edge Locations.

Q: What if S3 Transfer Acceleration is not faster than a regular Amazon S3 transfer?

Each time you use S3 Transfer Acceleration to upload an object, we will check whether S3 Transfer Acceleration is likely to be faster than a regular Amazon S3 transfer. If we determine that S3 Transfer Acceleration is not likely to be faster than a regular Amazon S3 transfer of the same object to the same destination AWS Region, we will not charge for the use of S3 Transfer Acceleration for that transfer, and we may bypass the S3 Transfer Acceleration system for that upload.

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 should I choose between S3 Transfer Acceleration and AWS Snow Family (Snowball, Snowball Edge, and Snowmobile)?

The AWS Snow Family is ideal for customers moving large batches of data at once. The AWS Snowball has a typical 5-7 days turnaround time. As a rule of thumb, S3 Transfer Acceleration over a fully-utilized 1 Gbps line can transfer up to 75 TBs in the same time period. In general, if it will take more than a week to transfer over the Internet, or there are recurring transfer jobs and there is more than 25Mbps of available bandwidth, S3 Transfer Acceleration is a good option. Another option is to use both: perform initial heavy lift moves with an AWS Snowball (or series of AWS Snowballs) and then transfer incremental ongoing changes with S3 Transfer Acceleration.

Q: Can S3 Transfer Acceleration complement AWS Direct Connect?

AWS Direct Connect is a good choice for customers who have a private networking requirement or who have access to AWS Direct Connect exchanges. S3 Transfer Acceleration is best for submitting data from distributed client locations over the public Internet, or where variable network conditions make throughput poor. Some AWS Direct Connect customers use S3 Transfer Acceleration to help with remote office transfers, where they may suffer from poor Internet performance.

Q: Can S3 Transfer Acceleration complement the AWS Storage Gateway or a 3rd party gateway?

If you can configure the bucket destination in your 3rd party gateway to use an S3 Transfer Acceleration endpoint domain name you will see the benefit.

Visit this File section of the Storage Gateway FAQ to learn more about the AWS implementation.

Q: Can S3 Transfer Acceleration complement 3rd party integrated software?

Yes. Software packages that connect directly into Amazon S3 can take advantage of S3 Transfer Acceleration when they send their jobs to Amazon S3.

Learn more about Storage Partner Solutions »

Q: Is S3 Transfer Acceleration HIPAA eligible?

Yes, AWS has expanded its HIPAA compliance program to include Amazon S3 Transfer Acceleration as a HIPAA eligible service. If you have an executed Business Associate Agreement (BAA) with AWS, you can use Amazon S3 Transfer Acceleration to enable fast, easy, and secure transfers of files including protected health information (PHI) over long distances between your client and your Amazon S3 bucket.

Learn more about HIPAA Compliance »

Storage Management

S3 Object Tagging

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: How can I update the object tags on my objects?

Object tags can be changed at any time during the lifetime of your S3 object, you can use either the AWS Management Console, the REST API, the AWS CLI, or the AWS SDKs to change your object tags. Note that all changes to tags outside of the AWS Management Console are made to the full tag set. If you have five tags attached to a particular object and want to add a sixth, you need to include the original five tags in that request.

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 in the Amazon S3 Developer Guide.

Q: How much do object tags cost?

Object tags are priced based on the quantity of tags and a request cost for adding tags. The requests associated with adding and updating Object Tags are priced the same as existing request prices. Please see the Amazon S3 pricing page for more information.

Storage Class Analysis

Q: What is Storage Class Analysis?

With Storage Class Analysis, you can analyze storage access patterns and transition the right data to the right storage class. This new S3 feature automatically identifies infrequent access patterns to help you

transition storage to S3 Standard-IA. You can configure a Storage Class Analysis policy to monitor an entire bucket, prefix, or object tag. Once an infrequent access pattern is observed, you can easily create a new S3 Lifecycle age policy based on the results. Storage Class Analysis also provides daily visualizations of your storage usage on the AWS Management Console that you can export to an S3 bucket to analyze using business intelligence tools of your choice such as Amazon QuickSight.

Q: How do I get started with Storage Class Analysis?

You can use the AWS Management Console or the S3 PUT Bucket Analytics API to configure a Storage Class Analysis policy to identify infrequently accessed storage that can be transitioned to the S3 Standard-IA or S3 One Zone-IA storage class or archived to the S3 Glacier storage class. You can navigate to the "Management" tab in the S3 Console to manage Storage Class Analysis, S3 Inventory, and S3 CloudWatch metrics.

Q: How am I charged for using Storage Class Analysis?

Please see the Amazon S3 pricing page for general information about Storage Class Analysis pricing.

Q: How often is the Storage Class Analysis updated?

Storage Class Analysis is updated on a daily basis in the S3 Management Console. Additionally, you can configure Storage Class Analysis to export your report to an S3 bucket of your choice.

S3 Inventory

Q: What is S3 Inventory?

The S3 Inventory report provides a scheduled alternative to Amazon S3's synchronous List API. You can configure S3 Inventory to provide a CSV, ORC, or Parquet file output of your objects and their corresponding metadata on a daily or weekly basis for an S3 bucket or prefix. You can simplify and speed up business workflows and big data jobs with S3 Inventory. You can also use S3 inventory to verify encryption and replication status of your objects to meet business, compliance, and regulatory needs.

Q: How do I get started with S3 Inventory?

You can use the AWS Management Console or the PUT Bucket Inventory API to configure a daily or weekly inventory report for all the objects within your S3 bucket or a subset of the objects under a shared prefix. As part of the configuration, you can specify a destination S3 bucket for your S3 Inventory report, the output file format (CSV, ORC, or Parquet), and specific object metadata necessary for your business application, such as object name, size, last modified date, storage class, version ID, delete marker, noncurrent version flag, multipart upload flag, replication status, or encryption status.

Q: Can S3 Inventory report files be encrypted?

Yes, you can configure encryption of all files written by S3 inventory to be encrypted by SSE-S3 or SSE-KMS. For more information, refer to the user guide.

Q: How do I use S3 Inventory?

You can use S3 Inventory as a direct input into your application workflows or Big Data jobs. You can also query S3 Inventory using Standard SQL language with Amazon Athena, Amazon Redshift Spectrum, and other tools such as Presto, Hive, and Spark.

Learn more about querying S3 Inventory with Athena »

Q: How am I charged for using S3 Inventory?

Please see the Amazon S3 pricing page for S3 Inventory pricing. Once you configure encryption using SSE-KMS, you will incur KMS charges for encryption, refer to the KMS pricing page for detail.

S3 Batch Operations

Q: What is S3 Batch Operations?

S3 Batch Operations is a feature that you can use to automate the execution, management, and auditing of a specific S3 request or Lambda function across many objects stored in Amazon S3. You can use S3 Batch Operations to automate replacing tag sets on S3 objects, updating access control lists (ACL) for S3 objects, copying storage between buckets, initiating a restore from Glacier to S3, or performing custom

operations with Lambda functions. S3 Batch Operations can be used from the S3 console, or through the AWS CLI and SDK.

Q: Why should I use S3 Batch Operations?

You should use S3 Batch Operations if you want to automate the execution of a single operation (like copying an object, or executing an AWS Lambda function) across many objects. With S3 Batch Operations, you can, with a few clicks in the S3 console or a single API request, make a change to billions of objects without having to write custom application code or run compute clusters for storage management applications. Not only does S3 Batch Operations administer your storage operation across many objects, S3 Batch Operations manages retries, displays progress, delivers notifications, provides a completion report, and sends events to AWS CloudTrail for all operations performed on your target objects. If you are interested in learning more about S3 Batch Operations, go to the Amazon S3 features page.

Q: How do I get started with S3 Batch Operations?

You can get started with S3 Batch Operations by going into the Amazon S3 console or using the AWS CLI or SDK to create your first S3 Batch Operations job. A S3 Batch Operations job consists of the list of objects to act upon and the type of operation to be performed. Start by selecting an S3 Inventory report or providing your own custom list of objects for S3 Batch Operations to act upon. An S3 Inventory report is a file listing all objects stored in an S3 bucket or prefix. Next, you choose from a set of S3 operations supported by S3 Batch Operations, such as replacing tag sets, changing ACLs, copying storage from one bucket to another, or initiating a restore from Glacier to S3. You can then customize your S3 Batch Operations jobs with specific parameters such as tag values, ACL grantees, and restoration duration. To further customize your storage actions, you can write your own Lambda function and invoke that code through S3 Batch Operations.

Once you create your S3 Batch Operations job, S3 Batch Operations will process your list of objects and send the job to the “awaiting confirmation” state if required. After you confirm the job details, S3 Batch Operations will begin executing the operation you specified. You can view your job’s progress programmatically or through the S3 console, receive notifications on completion, and review a completion report that itemizes the changes made to your storage.

If you are interested in learning more about S3 Batch Operations watch the tutorials videos and visit the documentation.

S3 Object Lock

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 does Amazon S3 Object Lock work?

Amazon S3 Object Lock blocks deletion of an object for the duration of a specified retention period. Coupled with S3 Versioning, which protects objects from being overwritten, you’re able to ensure that

objects remain immutable for as long as WORM protection is applied. You can apply WORM protection by either assigning a Retain Until Date or a Legal Hold to an object using the AWS SDK, CLI, REST API, or the S3 Management Console. You can apply retention settings within a PUT request, or apply them to an existing object after it has been created.

The Retain Until Date defines the length of time for which an object will remain immutable. Once a Retain Until Date has been assigned to an object, that object cannot be modified or deleted until the Retain Until Date has passed. If a user attempts to delete an object before its Retain Until Date has passed, the operation will be denied.

S3 Object Lock can be configured in one of two Modes. When deployed in Governance Mode, AWS accounts with specific IAM permissions are able to remove WORM protection from an object. If you require stronger immutability in order to comply with regulations, you can use Compliance Mode. In Compliance Mode, WORM protection cannot be removed by any user, including the root account.

Alternatively, you can make an object immutable by applying a Legal Hold to that object. A Legal Hold places indefinite S3 Object Lock protection on an object, which will remain until it is explicitly removed. In order to place and remove Legal Holds, your AWS account must have write permission for the PutObjectLegalHold action. Legal Hold can be applied to any object in an S3 Object Lock enabled bucket, whether or not that object is currently WORM-protected by a retention period.

Q: What AWS electronic storage services have been assessed based on financial services regulations?

For customers in the financial services industry, S3 Object Lock provides added support for broker-dealers who must retain records in a non-erasable and non-rewritable format to satisfy regulatory requirements of SEC Rule 17a-4(f), FINRA Rule 4511, or CFTC Regulation 1.31. You can easily designate the records retention time frame to retain regulatory archives in the original form for the required duration, and also place legal holds to retain data indefinitely until the hold is removed.

Q: What AWS documentation supports the SEC 17a-4(f)(2)(i) and CFTC 1.31(c) requirement for notifying my regulator?

Provide notification to your regulator or “Designated Examining Authority (DEA)” of your choice to use Amazon S3 for electronic storage along with a copy of the Cohasset Assessment. For the purposes of these requirements, AWS is not a designated third party (D3P). Be sure to select a D3P and include this information in your notification to your DEA.

S3 CloudWatch Metrics

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: Can I align S3 CloudWatch request metrics to my applications or business organizations?

Yes, you can configure S3 CloudWatch request metrics to generate metrics for your S3 bucket or configure filters for the metrics using a prefix or object tag.

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: How am I charged for using S3 CloudWatch Metrics?

CloudWatch storage metrics are provided free. Cloudwatch request metrics are priced as custom metrics for Amazon CloudWatch. Please see the Amazon CloudWatch pricing page for general information about S3 CloudWatch metrics pricing.

S3 Lifecycle Management

Q: What is S3 Lifecycle management?

S3 Lifecycle management provides the ability to define the lifecycle of your object with a predefined policy and reduce your cost of storage. You can set a lifecycle transition policy to automatically migrate objects stored in the S3 Standard storage class to the S3 Standard-IA, S3 One Zone-IA, and/or S3 Glacier storage classes based on the age of the data. You can also set lifecycle expiration policies to automatically remove objects based on the age of the object. You can set a policy for multipart upload expiration, which expires incomplete multipart uploads based on the age of the upload.

Q: How do I set up an S3 Lifecycle management policy?

You can set up and manage Lifecycle policies in the AWS Management Console, S3 REST API, AWS SDKs, or AWS Command Line Interface (CLI). You can specify the policy at the prefix or at the bucket level.

Q: How much does it cost to use S3 Lifecycle management?

There is no additional cost to set up and apply Lifecycle policies. A transition request is charged per object when an object becomes eligible for transition according to the Lifecycle rule. Refer to the S3 Pricing page for pricing information.

Q: What can I do with Lifecycle management policies?

As data matures, it can become less critical, less valuable, and/or subject to compliance requirements. Amazon S3 includes an extensive library of policies that help you automate data migration processes between storage classes. For example, you can set infrequently accessed objects to move into lower cost storage classes (like S3 Standard-IA or S3 One Zone-IA) after a period of time. After another period, those objects can be moved into Amazon S3 Glacier for archive and compliance. If policy allows, you can also specify a lifecycle policy for object deletion. These rules can invisibly lower storage costs and simplify management efforts. These policies also include good stewardship practices to remove objects and attributes that are no longer needed to manage cost and optimize performance.

Q: How can I use Amazon S3 Lifecycle management to help lower my Amazon S3 storage costs?

With Amazon S3 Lifecycle policies, you can configure your objects to be migrated to from the S3 Standard storage class to S3 Standard-IA or S3 One Zone-IA and/or archived to S3 Glacier. You can also specify an S3 Lifecycle policy to delete objects after a specific period of time. You can use this policy-driven automation to quickly and easily reduce storage costs as well as save time. In each rule you can specify a prefix, a time period, a transition to S3 Standard-IA, S3 One Zone-IA, or S3 Glacier, and/or an expiration. For example, you could create a rule that archives into S3 Glacier all objects with the common prefix “logs/” 30 days from creation and expires these objects after 365 days from creation. You can also create a separate rule that only expires all objects with the prefix “backups/” 90 days from creation. S3 Lifecycle policies apply to both existing and new S3 objects, helping you optimize storage and maximize cost savings for all current data and any new data placed in S3 without time-consuming manual data review and migration. Within a lifecycle rule, the prefix field identifies the objects subject to the rule. To apply the rule to an individual object, specify the key name. To apply the rule to a set of objects, specify their common prefix (e.g. “logs/”). You can specify a transition action to have your objects archived and an expiration action to have your objects removed. For time period, provide the creation date (e.g. January 31, 2015) or the number of days from creation date (e.g. 30 days) after which you want your objects to be archived or removed. You may create multiple rules for different prefixes.

Q: How can I configure my objects to be deleted after a specific time period?

You can set an S3 Lifecycle expiration policy to remove objects from your buckets after a specified number of days. You can define the expiration rules for a set of objects in your bucket through the Lifecycle configuration policy that you apply to the bucket.

Learn more about S3 Lifecycle expiration policies »

Q: Why would I use an S3 Lifecycle policy to expire incomplete multipart uploads?

The S3 Lifecycle policy that expires incomplete multipart uploads allows you to save on costs by limiting the time non-completed multipart uploads are stored. For example, if your application uploads several multipart object parts, but never commits them, you will still be charged for that storage. This policy can lower your S3 storage bill by automatically removing incomplete multipart uploads and the associated storage after a predefined number of days.

Learn more about using S3 Lifecycle to expire incomplete mulitpart uploads »

Replication

Q: What is Amazon S3 Replication?

Amazon S3 Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions (S3 Cross-Region Replication), or within the same AWS Region (S3 Same-Region Replication).

Q: What is Amazon S3 Cross-Region Replication (CRR)?

CRR is an Amazon S3 feature that automatically replicates data between buckets across different AWS Regions. With CRR, you can set up replication at a bucket level, a shared prefix level, or an object level using S3 object tags. You can use CRR to provide lower-latency data access in different geographic regions. CRR can also help if you have a compliance requirement to store copies of data hundreds of miles apart. You can use CRR to change account ownership for the replicated objects to protect data from accidental deletion. To learn more about CRR, please visit the replication developer guide.

Q: What is Amazon S3 Same-Region Replication (SRR)?

SRR is an Amazon S3 feature that automatically replicates data between buckets within the same AWS Region. With SRR, you can set up replication at a bucket level, a shared prefix level, or an object level using S3 object tags. You can use SRR to make a second copy of your data in the same AWS Region. SRR helps you address data sovereignty and compliance requirements by keeping a copy of your data in a separate AWS account in the same region as the original. You can use SRR to change account ownership for the replicated objects to protect data from accidental deletion. You can also use SRR to easily aggregate logs from different S3 buckets for in-region processing, or to configure live replication between test and development environment. To learn more about SRR, please visit the replication developer guide.

Q: How do I enable Amazon S3 Replication (Cross-Region Replication and Same-Region Replication)?

Amazon S3 Replication (CRR and SRR) is configured at the S3 bucket level, a shared prefix level, or an object level using S3 object tags. You add a replication configuration on your source bucket by specifying a destination bucket in the same or different AWS region for replication.

You can use either the AWS Management Console, the REST API, the AWS CLI, or the AWS SDKs to enable replication. Versioning must be enabled for both the source and destination buckets to enable replication. To learn more, please visit overview of setting up Replication in the Amazon S3 Developer Guide.

Q: Can I use S3 Replication (CRR and SRR) with S3 Lifecycle rules?

With S3 Replication (CRR and SRR), you can establish replication rules to make copies of your objects into another storage class, in the same or a different region. Lifecycle actions are not replicated, and if you want the same lifecycle configuration applied to both source and destination buckets, enable the same lifecycle configuration on both.

For example, you can configure a lifecycle rule to migrate data from the S3 Standard storage class to the S3 Standard-IA or S3 One Zone-IA storage class or archive data to S3 Glacier on the destination bucket.
You can find more information about lifecycle configuration and replication on the S3 Replication developer guide.

Q: Can I use replication with objects encrypted by AWS Key Management Service (KMS)?

Yes, you can replicate KMS-encrypted objects by providing a destination KMS key in your replication configuration.

Learn more about replicating KMS-encrypted objects »

Q: Are objects securely transferred and encrypted throughout replication process?

Yes, objects remain encrypted throughout the replication process. The encrypted objects are transmitted securely via SSL from the source region to the destination region (CRR) or within the same region (SRR).

Q: Can I use replication across AWS accounts to protect against malicious or accidental deletion?

Yes, for CRR and SRR, you can set up replication across AWS accounts to store your replicated data in a different account in the target region. You can use Ownership Overwrite in your replication configuration to maintain a distinct ownership stack between source and destination, and grant destination account ownership to the replicated storage.

Q: What is Amazon S3 Replication Time Control?

Amazon S3 Replication Time Control is a feature of S3 Replication that helps you meet compliance or business requirements for predictable replication times. S3 Replication Time Control is designed to replicate most objects in seconds, 99% of objects within 5 minutes, and 99.99% of objects within 15 minutes. S3 Replication Time Control is backed by a Service Level Agreement (SLA) commitment that 99.9% of objects will be replicated in 15 minutes for each replication region pair during any billing month. Replication Time works with all S3 Replication features. To learn more, please visit the replication developer guide.

Q: How do I enable Amazon S3 Replication Time Control?

Amazon S3 Replication Time Control is enabled as an option in your S3 Replication configuration. You can create a new S3 Replication policy with S3 Replication Time Control, or enable the feature on an existing policy.

You can use either the S3 Management Console, the REST API, the AWS CLI, or the AWS SDKs to configure replication. To learn more, please visit overview of setting up Replication in the Amazon S3 Developer Guide.

Q: What are Amazon S3 Replication metrics and events?

Amazon S3 Replication metrics and events provides visibility into Amazon S3 Replication Time Control activity. With S3 Replication metrics, you can monitor the total number and size of objects that are pending replication, and the maximum replication time for each S3 Replication rule configured with S3 Replication Time Control. Replication metrics are available through the Amazon S3 Management Console and through Amazon CloudWatch. S3 Replication events will notify you in the rare instance when an object takes more than 15 minutes to replicate, and also when that object replicates successfully to their destination. Like other Amazon S3 events, S3 Replication events are available through Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS), or AWS Lambda.

Q: How do I enable Amazon S3 Replication Time Control metrics and events?

Amazon S3 Replication metrics and events are enabled automatically for each S3 Replication rule configured with S3 Replication Time Control. Once you enable Replication Time Control, you can access metrics through the Amazon S3 Management Console and Amazon CloudWatch. Like other Amazon S3 events, S3 Replication events are available through Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS), or AWS Lambda. To learn more, please visit enabling Replication metrics in the Amazon S3 Developer Guide.

Q: What is the Amazon S3 Replication Time Control Service Level Agreement (SLA)?
Amazon S3 Replication Time Control is designed to replicate 99.99% of your objects within 15 minutes, and is backed by a service level agreement. If fewer than 99.9% of your objects are replicated in 15 minutes for each replication region pair during a monthly billing cycle, the S3 RTC SLA provides for a service credit on any object that took longer than 15 minutes to replicate. The service credit covers a percentage of all replication-related charges associated with the objects that did not meet the SLA, including the RTC fee, replication bandwidth and request charges, and the cost associated with storing your replica in the destination region in the monthly billing cycle affected. To learn more, read the S3 Replication Time Control SLA.
Q: How do I know if I qualify for an Amazon S3 Replication Time Control SLA service credit?
You are eligible for an SLA credit for Amazon S3 Replication Time Control, if fewer than 99.9% of your objects are replicated in 15 minutes for each replication region pair during a monthly billing cycle. For full details on all of the terms and conditions of the SLA, as well as details on how to submit a claim, please see the S3 Replication Time Control SLA.
Q: What is the pricing for S3 Replication and S3 Replication Time Control?
For CRR and SRR, you pay the Amazon S3 charges for storage in the destination S3 storage class you select, in addition to the storage charges for the primary copy, replication PUT requests, and applicable infrequent access storage retrieval fees. For CRR, you also pay for inter-region Data Transfer OUT From Amazon S3 to your destination region. Pricing for the replicated copy of storage and the requests are based on the destination AWS Region, while pricing for inter-region data transfer is based on the source AWS Region. For S3 Replication Time Control, you pay an additional Data Transfer fee and S3 Replication Metrics charges that are billed at the same rate as Amazon CloudWatch custom metrics. For more information, please visit the S3 pricing page.
If the source object is uploaded using the multipart upload feature, then it is replicated using the same number of parts and part size. For example, a 100 GB object uploaded using the multipart upload feature (800 parts of 128 MB each) will incur request cost associated with 802 requests (800 Upload Part requests + 1 Initiate Multipart Upload request + 1 Complete Multipart Upload request) when replicated. You will incur a request charge of $0.00401 (802 requests x $0.005 per 1,000 requests) and (if the replication was between different AWS regions) a charge of $2.00 ($0.020 per GB transferred x 100 GB) for inter-region data transfer. After replication, the 100 GB will incur storage charges based on the destination region.

Amazon S3 and IPv6

Q: What is IPv6?
Every server and device connected to the Internet must have a unique address. Internet Protocol Version 4 (IPv4) was the original 32-bit addressing scheme. However, the continued growth of the Internet means that all available IPv4 addresses will be utilized over time. Internet Protocol Version 6 (IPv6) is the new addressing mechanism designed to overcome the global address limitation on IPv4.

Q: What can I do with IPv6?
Using IPv6 support for Amazon S3, applications can connect to Amazon S3 without the need for any IPv6 to IPv4 translation software or systems. You can meet compliance requirements, more easily integrate with existing IPv6-based on-premises applications, and remove the need for expensive networking equipment to handle the address translation. You can also now utilize the existing source address

filtering features in IAM policies and bucket policies with IPv6 addresses, expanding your options to secure applications interacting with Amazon S3.

Q: How do I get started with IPv6 on Amazon S3?
You can get started by pointing your application to Amazon S3's new "dual-stack" endpoint, which supports access over both IPv4 and IPv6. In most cases, no further configuration is required for access over IPv6, because most network clients prefer IPv6 addresses by default.

Q: Should I expect a change in Amazon S3 performance when using IPv6?
No, you will see the same performance when using either IPv4 or IPv6 with Amazon S3.

Q: What can I do if my clients are impacted by policy, network, or other restrictions in using IPv6 for Amazon S3?
Applications that are impacted by using IPv6 can switch back to the standard IPv4-only endpoints at any time.

Q: Can I use IPv6 with all Amazon S3 features?
No, IPv6 support is not currently available when using Website Hosting and access via BitTorrent. All other features should work as expected when accessing Amazon S3 using IPv6.

Q: Is IPv6 supported in all AWS Regions?
Yes, you can use IPv6 with Amazon S3 in all commercial AWS Regions, including AWS China (Beijing) Region, operated by Sinnet and AWS China (Ningxia) Region, operated by NWCD. You can also use IPv6 with Amazon S3 in the AWS GovCloud (US) Region.

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html