**Amazon S3 Reduced Redundancy Storage**

Reduced Redundancy Storage (RRS) is an Amazon S3 storage option that enables customers to store noncritical, reproducible data at lower levels of redundancy than Amazon S3’s standard storage. It provides a highly available solution for distributing or sharing content that is durably stored elsewhere, or for storing thumbnails, transcoded media, or other processed data that can be easily reproduced. The RRS option stores objects on multiple devices across multiple facilities, providing 400 times the durability of a typical disk drive, but does not replicate objects as many times as standard Amazon S3 storage.

Reduced Redundancy Storage is:

Backed with the Amazon S3 Service Level Agreement for availability.

Designed to provide 99.99% durability and 99.99% availability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.01% of objects.

Designed to sustain the loss of data in a single facility.

**Pre-signed url by cloudfront**

When you create a pre-signed URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method (GET to download the object) and expiration date and time. The pre-signed URLs are valid only for the specified duration.

Anyone who receives the pre-signed URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a pre-signed URL

Reduced Redundancy Storage (RRS) is an Amazon S3 storage option that enables customers to store noncritical, reproducible data at lower levels of redundancy than Amazon S3’s standard storage. It provides a highly available solution for distributing or sharing content that is durably stored elsewhere, or for storing thumbnails, transcoded media, or other processed data that can be easily reproduced.

The difference between them is: Concurrent facility fault tolerance and Durability

S3- IA provide 99.9x9% while RRS provide only 99.99%.

Amazon 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 perfect for a wide variety of use cases including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and Big Data analytics. S3 Lifecycle management offers configurable policies to automatically migrate objects to the most appropriate storage class.

Key Features:

* Low latency and high throughput performance
* Designed for durability of 99.999999999% of objects across multiple Availability Zones
* Data is resilient in the event of one entire Availability Zone destruction
* Designed for 99.99% availability over a given year
* Backed with the [Amazon S3 Service Level Agreement](https://aws.amazon.com/s3/sla/?nc=hl&pg=sc&pos=1) for availability
* Supports SSL for data in transit and encryption of data at rest
* Lifecycle management for automatic migration of objects

Infrequent Access

Amazon 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, 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 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 S3 Standard, allowing you to use S3 Lifecycle Policies to automatically transition objects between storage classes without any application changes.

Key Features:

* Same low latency and high throughput performance of S3 Standard
* Designed for durability of 99.999999999% of objects across multiple Availability Zones
* 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](https://aws.amazon.com/s3/sla/?nc=hl&pg=sc&pos=2) for availability
* Supports SSL for data in transit and encryption of data at rest
* Lifecycle management for automatic migration of objects

Amazon S3 One Zone-Infrequent Access

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is an Amazon S3 storage class for data that is accessed less frequently, but requires rapid access when needed. Unlike other Amazon object storage classes, which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ. Because of this, storing data in S3 One Zone-IA costs 20% less than storing it in 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 storage. It’s a good choice, for example, for storing secondary backup copies of on-premises data or easily re-creatable data, or for storage used as an S3 Cross-Region Replication target from another AWS Region.

S3 One Zone-IA offers the same high durability†, high throughput, and low latency of Amazon S3 Standard and S3 Standard-IA, with a low per GB storage price and per GB retrieval fee. The 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, allowing you to use S3 Lifecycle Policies to automatically transition objects between storage classes without any application changes.

Key Features:

* Same low latency and high throughput performance of S3 Standard and S3 Standard-IA
* Designed for durability of 99.999999999% of objects in a single Availability Zone, but data will be lost in the event of Availability Zone destruction
* Designed for 99.5% availability over a given year
* Backed with the [Amazon S3 Service Level Agreement](https://aws.amazon.com/s3/sla/?nc=hl&pg=sc&pos=3) for availability
* Supports SSL for data in transit and encryption of data at rest
* Lifecycle management for automatic migration of objects

† 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 Glacier

Amazon Glacier is a secure, durable, and extremely low-cost storage service 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 retrieval needs, Amazon Glacier provides three options for access to archives, from a few minutes to several hours. Amazon Glacier supports S3 Lifecycle Policies for automatic migration between S3 & Amazon Glacier storage classes. Please see the [Amazon Glacier page](https://aws.amazon.com/glacier/?nc=hl&pg=sc&p=s3) for more details.

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
* Extremely low cost design is ideal for long-term archive
* Lifecycle management for automatic migration of objects

Multiprotocol Label Switching (MPLS)

By default, you can create up to 100 buckets in each of your AWS accounts. If you need additional buckets, you can increase your bucket limit by submitting a service limit increase.

* **Upload objects in a single operation—**With a single PUT operation, you can upload objects up to 5 GB in size.

For more information, see [Uploading Objects in a Single Operation](https://docs.aws.amazon.com/AmazonS3/latest/dev/UploadInSingleOp.html).

* **Upload objects in parts—**Using the multipart upload API, you can upload large objects, up to 5 TB.

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.

Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with [Amazon EC2](https://aws.amazon.com/ec2-sla/) instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability.

Amazon EBS is designed for application workloads that benefit from fine tuning for performance, cost and capacity. Typical use cases include Big Data analytics engines (like the Hadoop/HDFS ecosystem and [Amazon EMR](https://aws.amazon.com/emr/) clusters), relational and NoSQL databases (like Microsoft SQL Server and MySQL or Cassandra and MongoDB), stream and log processing applications (like Kafka and Splunk), and data warehousing applications (like Vertica and Teradata).

Every computer needs a drive and virtual machine is not an exception. Amazon EBS is a storage for the drives of your virtual machines. It stores data as blocks of the same size and organizes them through the hierarchy similar to a traditional file system. EBS is not a standalone storage service like Amazon S3 so you can use it only in combination with Amazon EC2, a cloud computing service by AWS.

Amazon EBS is designed to store data in volumes of a provisioned size attached to an Amazon EC2 instance, similar to a local disk drive on your physical machine. Amazon EBS only allows to attach the volume to another EC2 instance or keep it in a standby mode. It’s important as once you configure the volume in Amazon EBS, it can’t be easily scaled. If you need more storage space, you will need to buy and configure a new volume of a bigger size.

## Amazon EBS volume types

There are three types of volumes in Amazon EBS. To understand the difference, you need to know what IOPS is. “IOPS” stands for input/output operations per second or, put it simply, the maximum amount of read/write operations you are able to perform per second. To choose the right Amazon EBS volume type you need to know IOPS requirements for your application.

### General Purpose (SSD) Volumes

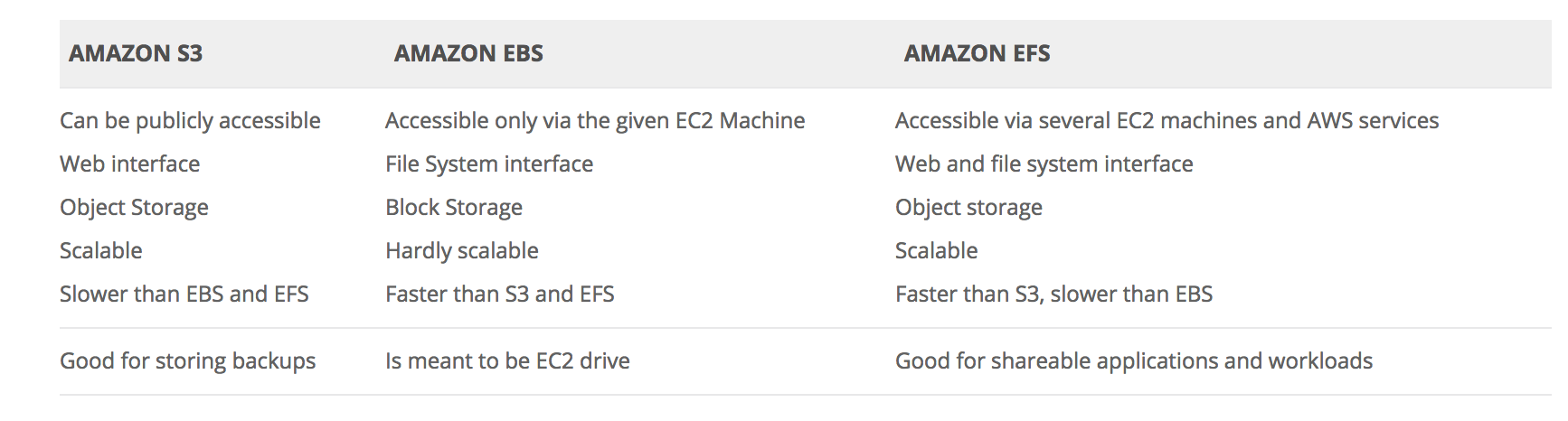
Designed for a broad range of tasks, General Purpose Volumes are backed with Solid State Drive (SSD). The baseline performance of 3 IOPS/GB and a possibility to burst up to 10,000 IOPS makes them a good fit for [AWS databases](http://www.cloudberrylab.com/blog/aws-database-services-complete-overview-rds-vs-redshift-vs-dynamodb-vs-simpledb/) that need a lot of read and write operations, like PostgreSQL, MS SQL or Oracle databases.

### Provisioned IOPS (SSD) Volumes

By expanding the bandwidth bottleneck, Provisioned IOPS Volumes allow to buy read/write operations on demand regardless of the volume capacity. This type of EBS volumes is backed with the same SSD but designed for heavy workloads from 30 IOPS/GB up to 20,000 IOPS. Multiple Provisioned IOPS volumes can be striped thus ensuring up to 48,000 IOPS or 800 MBps of throughput.

### Magnetic Volumes

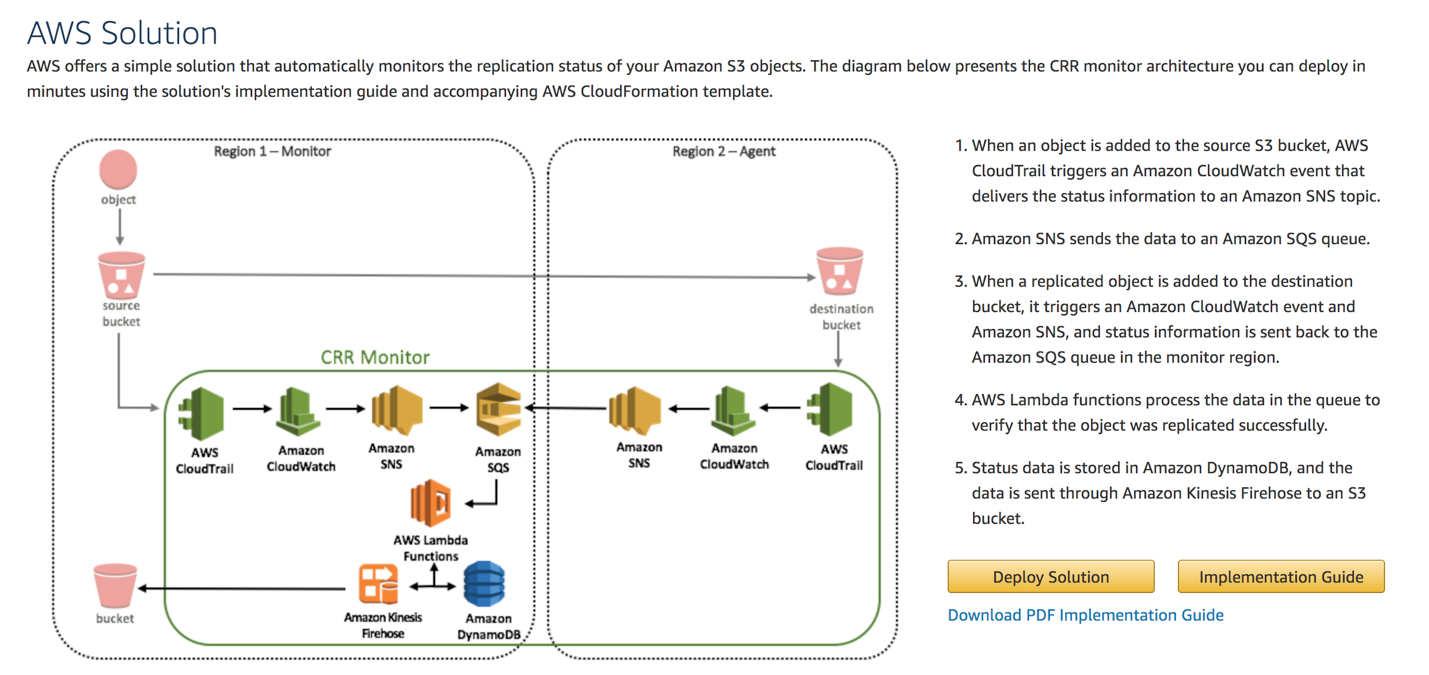
The best way to think of the Magnetic Volumes type is as of a low-cost volume that can be used with testing and development environments on Amazon EC2. It can also be used with applications that don’t require a lot of read/write operations. Instead of SSD, this type is based on magnetic HDD drives, thus the IOPS baseline is within the range of 100 up to hundreds of IOPS. Magnetic Volumes can also become a starting point in working with Amazon EC2 — once you understand your IOPS demands, you can select the type of volume that fits best.



Full S3 is quite expensive at around $0.023 per GB for the lowest band. S3 standard IA is $0.0125 per GB, S3 One-Zone-IA is $0.01 per GB, and Legacy S3-RRS is around $0.024 per GB for the lowest band. Of the offered solutions S3-IA is the cheapest suitable option. Glacier cannot be considered as it is not intended for direct access, however it comes in at around $0.004 per GB.

S3 One Zone has the same Durability but reduced Availability and reduced cost. RRS, is deprecated and new uses are strongly discouraged by AWS.

To help customers more proactively monitor the replication status of their Amazon S3 objects, AWS offers the Cross-Region Replication Monitor (CRR Monitor) solution.



Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buckets in different AWS Regions. We refer to these buckets as *source* bucket and *destination* bucket. These buckets can be owned by different AWS accounts.

* Replicas have the same key names and the same metadata—for example, creation time, user-defined metadata, and version ID.

* Amazon S3 stores object replicas using the same storage class as the source object, unless you explicitly specify a different storage class in the replication configuration.

* Assuming that the object replica continues to be owned by the source object owner, when Amazon S3 initially replicates objects, it also replicates the corresponding object access control list (ACL).

Amazon S3 encrypts all data in transit across AWS Regions using Secure Sockets Layer (SSL).

You can replicate objects from a source bucket to only one destination bucket. After Amazon S3 replicates an object, the object cannot be replicated again.

* SSE-S3 requires that Amazon S3 manage the data and master encryption keys. For more information about SSE-S3, see [Protecting Data Using Server-Side Encryption with AWS-Managed Encryption Keys.](http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html)
* SSE-C requires that you manage the encryption key. For more information about SSE-C, see [Protecting Data Using Server-Side Encryption with Customer-Provided Encryption Keys (SSE-C).](http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerSideEncryptionCustomerKeys.html)
* SSE-KMS requires that AWS manage the data key but you manage the master key in AWS KMS. The remainder of this topic discusses how to protect data by using server-side encryption with AWS KMS-managed keys (SSE-KMS).

Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

If you need server-side encryption for all of the objects that are stored in a bucket, use a bucket policy.

Server-side encryption is about protecting data at rest. Using server-side encryption with customer-provided encryption keys (SSE-C) allows you to set your own encryption keys. With the encryption key you provide as part of your request, Amazon S3 manages both the encryption, as it writes to disks, and decryption, when you access your objects. Therefore, you don't need to maintain any code to perform data encryption and decryption. The only thing you do is manage the encryption keys you provide.

If you choose to encrypt your data, AWS KMS and Amazon S3 perform the following actions:

* Amazon S3 requests a plaintext data key and a copy of the key encrypted by using the specified customer-managed master key or the AWS-managed master key.
* AWS KMS creates a data key, encrypts it by using the master key, and sends both the plaintext data key and the encrypted data key to Amazon S3.
* Amazon S3 encrypts the data using the data key and removes the plaintext key from memory as soon as possible after use.
* Amazon S3 stores the encrypted data key as metadata with the encrypted data.

Amazon S3 and AWS KMS perform the following actions when you request that your data be decrypted.

* Amazon S3 sends the encrypted data key to AWS KMS.
* AWS KMS decrypts the key by using the appropriate master key and sends the plaintext key back to Amazon S3.
* Amazon S3 decrypts the ciphertext and removes the plaintext data key from memory as soon as possible.

You can use the Amazon S3 encryption client in the AWS SDK from your own application to encrypt objects and upload them to Amazon S3. This method allows you to encrypt your data locally to ensure its security as it passes to the Amazon S3 service. The S3 service receives your encrypted data and does not play a role in encrypting or decrypting it.