The ABCs of AWS

S3: Simple Storage Service

Presented @macbrained_yvr March 2nd 2017

Mark Cohen

“AWS makes it ever easier to experiment with technology and try new solutions that would be prohibitively costly or outright impossible for most companies to even consider.”

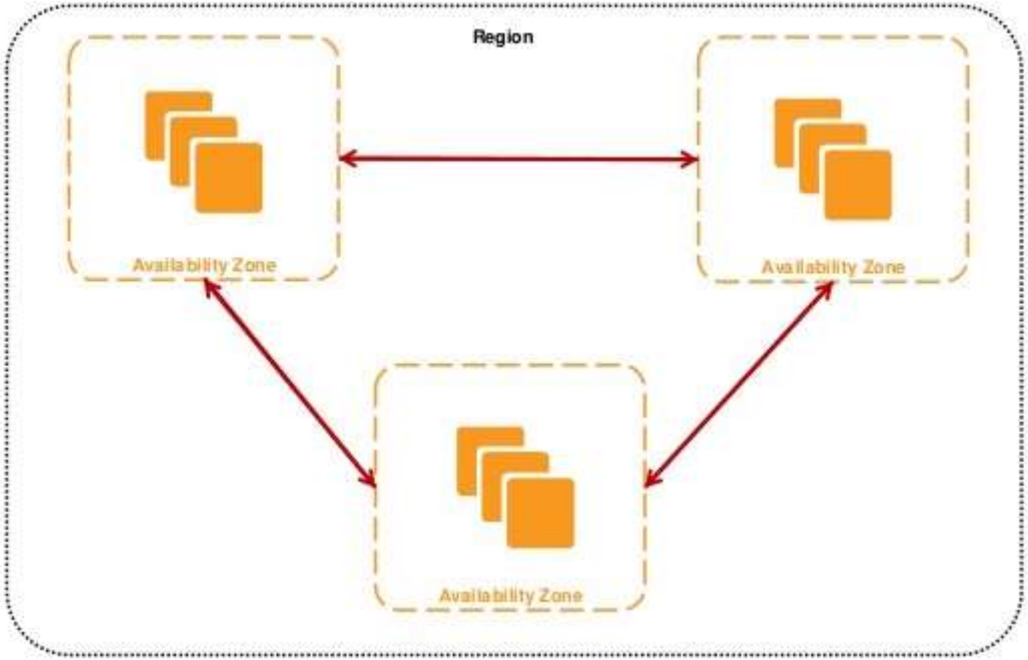
https://aws.amazon.com/free/

AWS Fundamental constructs:

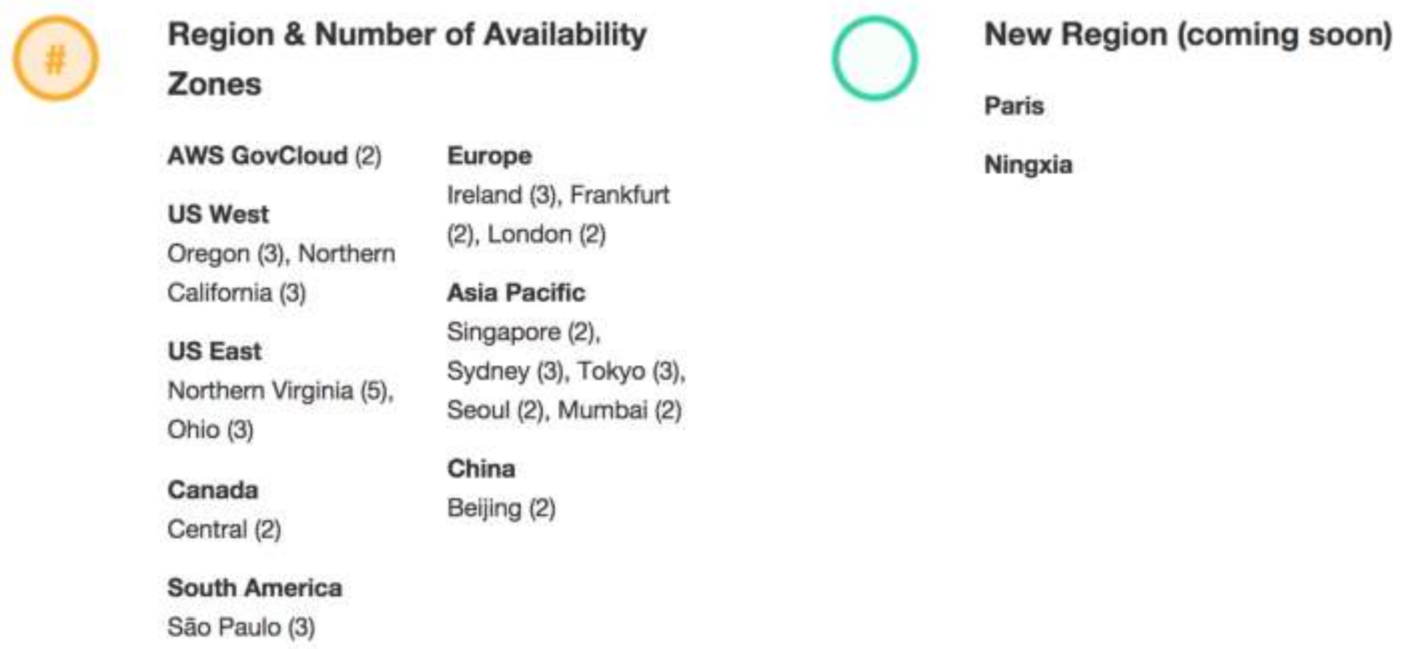
Regions and Availability Zones:

- ❑ A *Region* is a geographical area. Each region has multiple, isolated locations within it known as *Availability Zones*.
- ❑ Availability Zones consist of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities.
- ❑ AWS provides regional assurance, in that data won’t leave the region it’s placed in.
- ❑ Region choice should be determined based on latency (locating objects geographically closer to end users), price (minimize costs), address regulatory requirements (ie: data residency).

AWS Fundamental constructs:



AWS Global Infrastructure:



Region & Number of Availability Zones

AWS GovCloud (2)

US West
Oregon (3), Northern California (3)

US East
Northern Virginia (5), Ohio (3)

Canada
Central (2)

South America
São Paulo (3)

Europe
Ireland (3), Frankfurt (2), London (2)

Asia Pacific
Singapore (2), Sydney (3), Tokyo (3), Seoul (2), Mumbai (2)

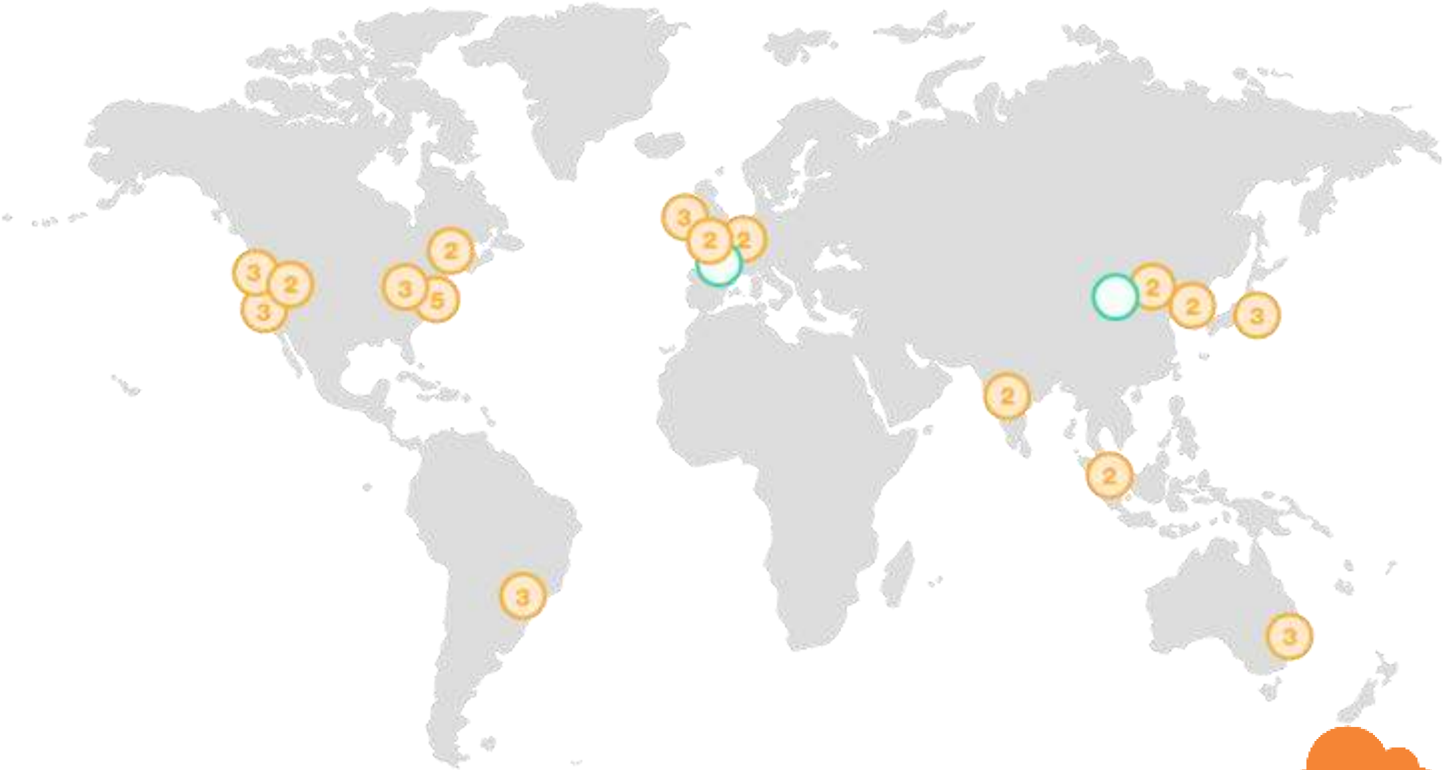
China
Beijing (2)

○ New Region (coming soon)

Paris

Ningxia

AWS Global Infrastructure:



S3: Simple Storage Service

So, what is S3, anyway ?

Internet-scale storage
Grow without limits

Built-in redundancy
Designed for 99.999999999% durability and 99.99% availability

Low price per GB per month
No commitment
No up-front cost

Benefit from AWS's massive security investments

S3: Simple Storage Service

Overview:

- ❑ Object storage, not file/block storage. A representation of (looks like) a file system, but more like a database.
- ❑ One of the earliest services available on AWS, introduced in 2006.
- ❑ Delivered managed service.
- ❑ Highly secure, durable, scalable. Designed to sustain the loss of data in 2 facilities (implies data is replicated across at least 3 facilities).
- ❑ No minimum commitments, no upfront fees. Pay only for what you use; storage, bandwidth.
- ❑ S3 Integrates tightly with other AWS services; Compute (EC2), CDN (CloudFront), Database (RDS), etc…

S3: Simple Storage Service

Access:

- Management console: https://console.aws.amazon.com
- CLI: Windows, Mac, Linux, Powershell
- API: REST, SOAP over HTTP is deprecated, still available over HTTPS.
- SDK: Java, .NET, node.JS, PHP, Python, Ruby, Go, C++....

S3 Fundamental constructs:

Buckets and Objects:

❑ Amazon S3 stores data as *objects* within *buckets*. An object consists of a file and optionally any metadata that describes that file.

S3 Fundamental constructs:

Buckets:

- ❑ Containers for objects.
- ❑ Organize the namespace. Bucket names must be:
  - globally unique.
  - Between 3 and 63 characters.
  - adhere to DNS naming conventions (* except for US East)
- ❑ > 100 buckets/account (soft limit, can be increased via support)

S3 Fundamental constructs:

Objects:

❑ An object is comprised of the data (file), and its meta-data (a name-value pair that describes the object).

❑ Objects are uniquely identified by a single key (name) and version ID.

❑ Unlimited # of objects/bucket.

❑ Objects can be > 5TB in size.

❑ Objects of differing storage classes can exist in the same bucket.

❑ Storage Inventory: flat-file output of your objects and their corresponding metadata (JSON, CSV).

S3 Fundamental constructs:

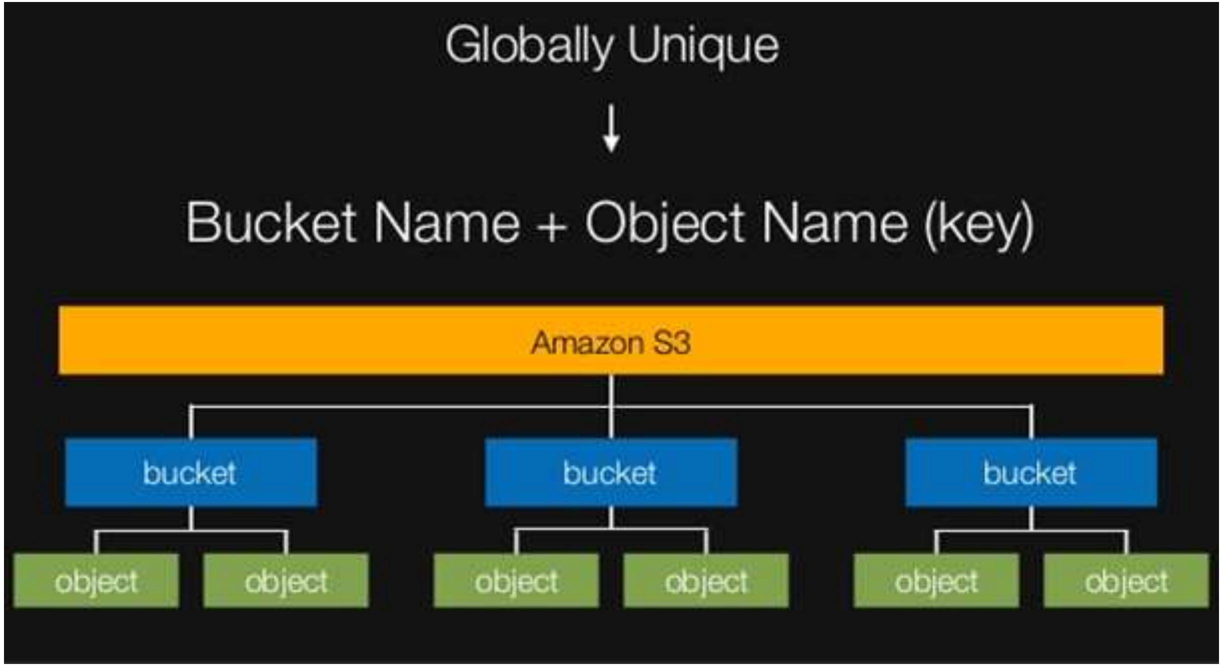
Keys:

❑ Unique identifier for an object within a bucket.

❑ Maximum 1024 bytes (including path prefix).

S3 Fundamental constructs:

Structure:



S3: Storage Classes

Standard:

- ❑ Active/”hot” data and/or temp data. Applications, dynamic websites, content distribution, mobile, gaming applications, big data analytics.
- ❑ Low latency and high throughput.
- ❑ 99.999999999% durability (average annual expected loss of 0.000000001% of objects).
- ❑ 99.99% availability.
- ❑ No minimum storage duration.

S3: Storage Classes

Standard IA (Infrequent Access)**:**

- ❑ High performance, infrequent access, ideal for long-term storage, backups, data store for disaster recovery.
- ❑ Low latency and high throughput.
- ❑ 99.999999999% durability.
- ❑ 99.9% availability.
- ❑ Lower cost (than Standard), per GB retrieval fee.
- ❑ Minimum storage duration 30 days.

S3: Storage Classes

Standard RRS (Reduced Redundancy Storage)**:**

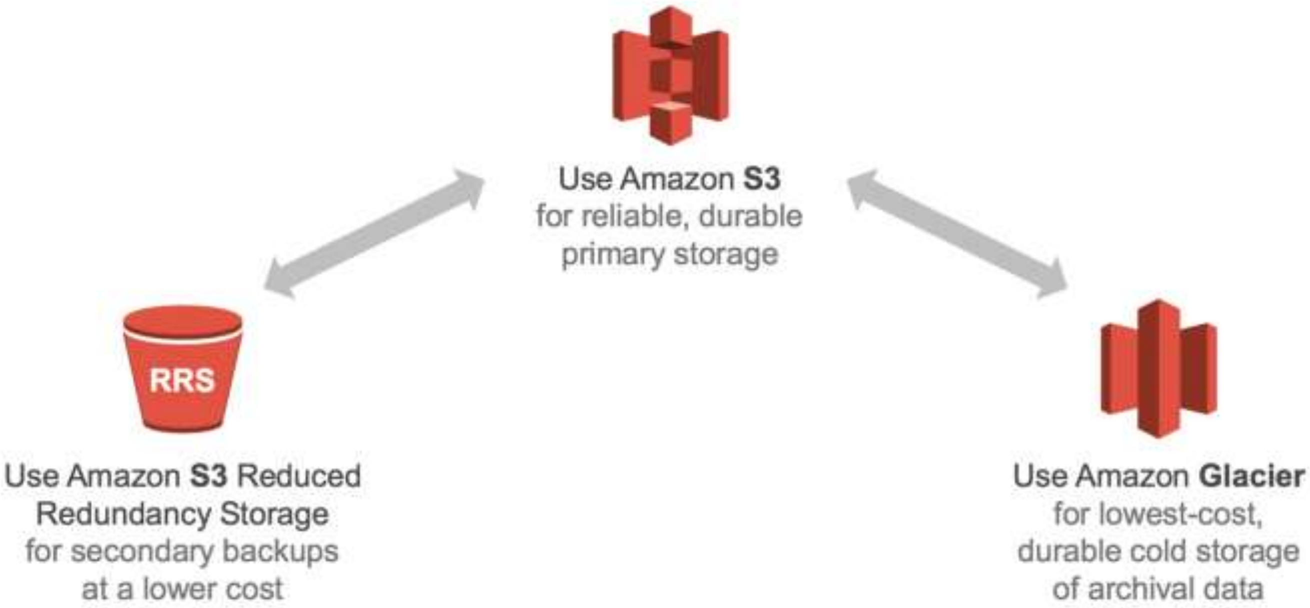
- ❑ For distributing or sharing noncritical, reproducible data that is durably stored elsewhere.
- ❑ Designed to sustain the loss of data in a single facility.
- ❑ 99.99% durability (average annual expected loss of 0.01% of objects).
- ❑ 99.99% availability.

S3: Storage Classes

Glacier:

- ❑ Cold storage, long term archive/retention.
- ❑ Data is stored in “archives”, archives are stored in “vaults”.
- ❑ 99.999999999% durability.
- ❑ 99.99% availability
- ❑ Data retrieval policies: Expedited (1-5 mins), Standard (3-5 hrs), Bulk (5-12 hrs).
- ❑ Vault lock: Compliance, storing your data as immutable objects
- ❑ Minimum storage duration 90 days.

S3: Storage Classes



Use Amazon **S3** for reliable, durable primary storage

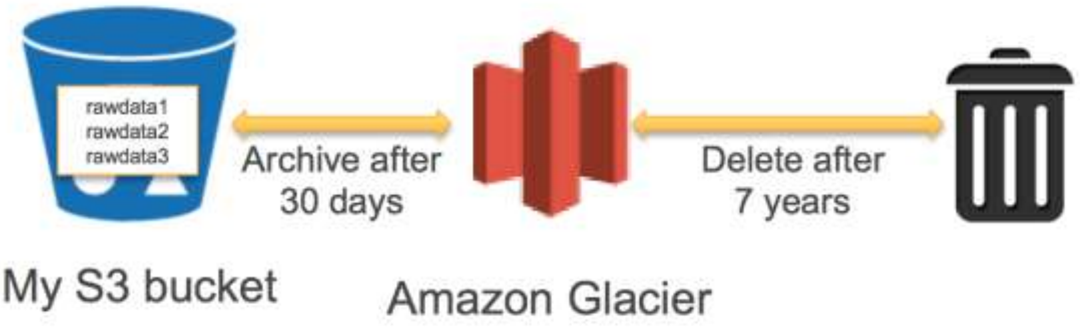
Use Amazon **S3** Reduced Redundancy Storage for secondary backups at a lower cost

Use Amazon **Glacier** for lowest-cost, durable cold storage of archival data

S3: Simple Storage Service

Lifecycle Policies:

- Automatically transition objects to another storage class, ie: from “hot” (Standard), to “warm” (IA), to “cold” (Glacier).
- Automatically expire (delete) objects after x amount of days.

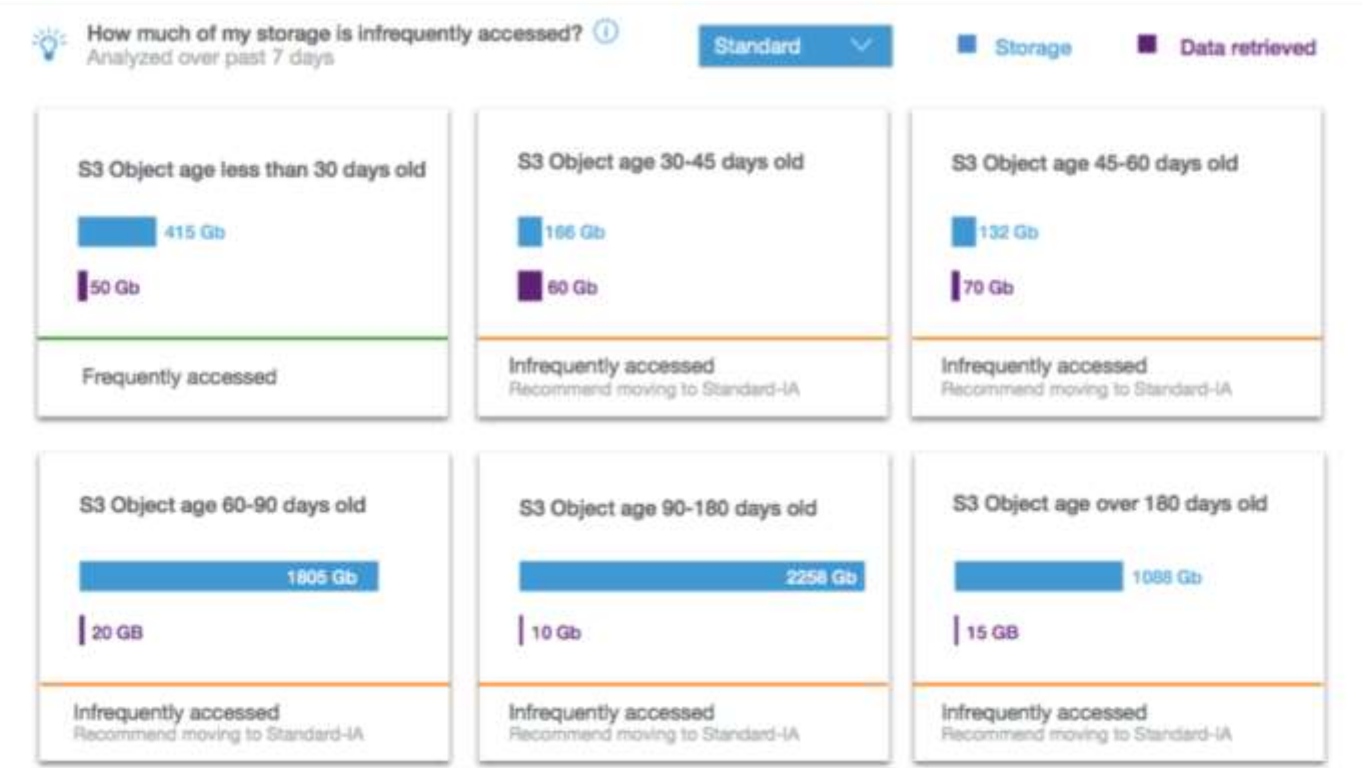


S3: Simple Storage Service

Lifecycle Policies:

- Actions can be combined/staged; ie: archive, then delete. Separate actions for current versions, previous versions.
- Can be applied to entire bucket, or object prefix (ie: “logs-” prefix).

S3: Analytics



How much of my storage is infrequently accessed?

Analyzed over past 7 days

Standard

■ Storage ■ Data retrieved

S3 Object age less than 30 days old

415 Gb

50 Gb

Frequently accessed

S3 Object age 30-45 days old

166 Gb

60 Gb

Infrequently accessed

Recommend moving to Standard-IA

S3 Object age 45-60 days old

132 Gb

70 Gb

Infrequently accessed

Recommend moving to Standard-IA

S3 Object age 60-90 days old

1805 Gb

20 GB

Infrequently accessed

Recommend moving to Standard-IA

S3 Object age 90-180 days old

2258 Gb

10 Gb

Infrequently accessed

Recommend moving to Standard-IA

S3 Object age over 180 days old

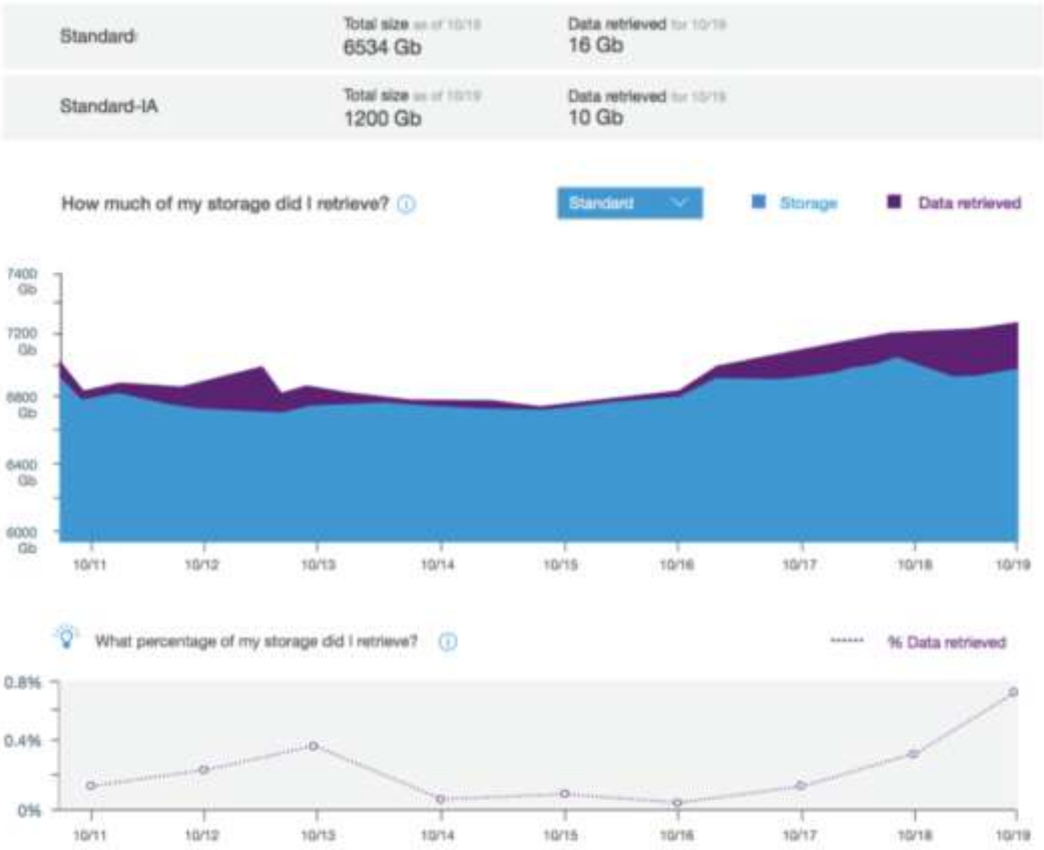
1088 Gb

15 GB

Infrequently accessed

Recommend moving to Standard-IA

S3: Analytics



Standard	Total size as of 10/19 6534 Gb	Data retrieved for 10/19 16 Gb
Standard-IA	Total size as of 10/19 1200 Gb	Data retrieved for 10/19 10 Gb

How much of my storage did I retrieve?

What percentage of my storage did I retrieve?

S3: Simple Storage Service

Data ingress:

- ❑ Buckets can be set up for internet upload (anonymously, or via time limited auth).
- ❑ VPC endpoints (transfer data to/from S3 buckets privately, without going through the public internet)
- ❑ Direct Connect
- ❑ AWS Storage Gateway
- ❑ File Gateway (NFS4)
- ❑ Snowball/Snowmobile (Petabytes, Exabytes)
- ❑ 3rd party solutions: NetApp, CommVault, Veritas, etc…
- ❑ S3 Transfer Acceleration (shortens distance to AWS over internet using AWS Edge network)

S3: Simple Storage Service

Data egress:

❑ Static web hosting (images, video, html).

❑ Single, durable origin for multiple CDNs (Cloudfront).

❑ * No cost to move data between S3 and CloudFront.

❑ * No cost to move data between S3 and EC2.

S3: Simple Storage Service

Security:

- ❑ Encrypt data in transit via SSL, client side encryption.
- ❑ Data is encrypted at rest (using AES 256), via:
  - SSE-S3: server side (AWS manages the encryption/keys)
  - SSE-KMS (AWS manages the encryption, customer keys and access permissions centrally managed via KMS service).
  - SSE-C (AWS manages the encryption, customer manages keys)
  - Client side (you manage the encryption/keys)

S3: Simple Storage Service

Security:

- □ Permissions/Policies:
  - IAM policies (fine grained access control, centralized management)
  - Bucket policies (access to users outside of AWS)
  - ACLs (legacy); course grained, limited, can only grant permissions to other AWS accounts.
- □ Time limited access to objects via pre-signed URLs (query string auth).
- □ MFA delete: can only change object state/delete object via MFA, enabled per bucket.
- □ (Object) Tags ! Key value pairs, > 10 tags/object, classify storage/manage access via IAM policies.

S3: Simple Storage Service

Security:

❑ Auditing:

- Cloudtrail records API calls (changes to policies, modifications of access, creation/deletion), captures bucket level and object level events (to logs).

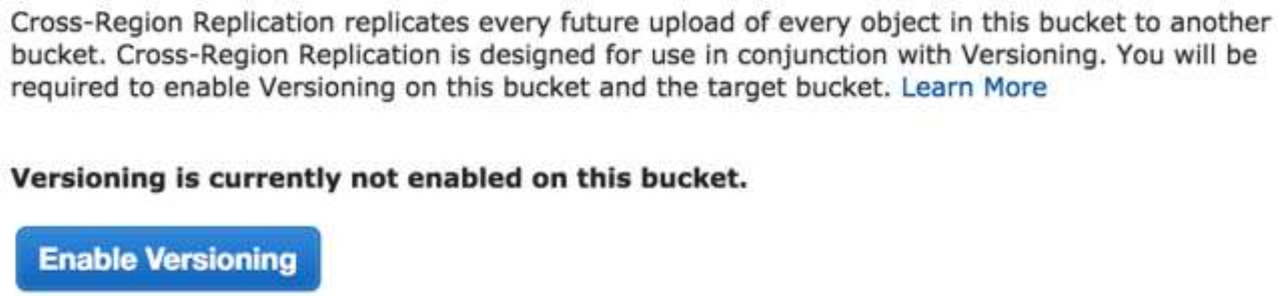
❑ Alerting/Monitoring:

- Cloudwatch metrics provide visibility into storage performance
- Cloudwatch alarms provide alerting.

S3: Simple Storage Service

Security:

- ❑ Cross Region Replication: automatic asynchronous copying of objects across buckets in different regions. Useful to adhere to regulatory/compliance requirements, address security concerns (separate buckets/owners), locate objects closer to end users, lower costs (ie: leverage Spot instances, lower priced regions).

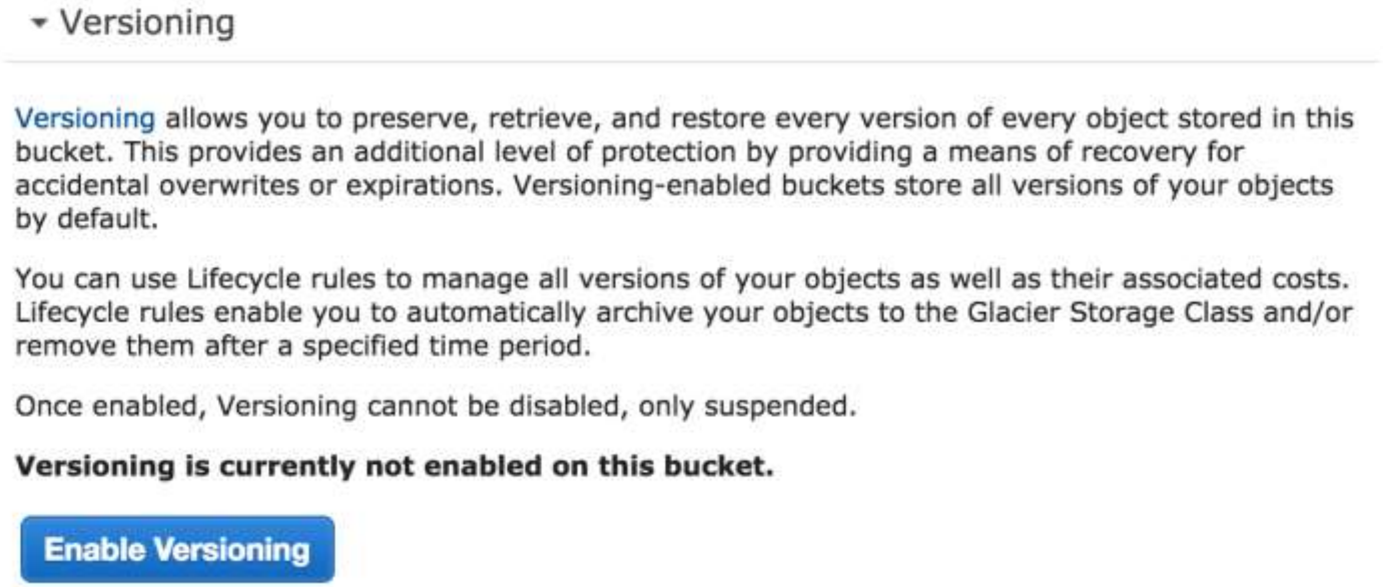


Cross-Region Replication replicates every future upload of every object in this bucket to another bucket. Cross-Region Replication is designed for use in conjunction with Versioning. You will be required to enable Versioning on this bucket and the target bucket. Learn More

Versioning is currently not enabled on this bucket.

S3: Buckets

Versioning:



Versioning allows you to preserve, retrieve, and restore every version of every object stored in this bucket. This provides an additional level of protection by providing a means of recovery for accidental overwrites or expirations. Versioning-enabled buckets store all versions of your objects by default.

You can use Lifecycle rules to manage all versions of your objects as well as their associated costs. Lifecycle rules enable you to automatically archive your objects to the Glacier Storage Class and/or remove them after a specified time period.

Once enabled, Versioning cannot be disabled, only suspended.

Versioning is currently not enabled on this bucket.

S3: Buckets

Versioning:

- ❑ 3 modes: Versioning off (default), Versioning-enabled: multiple versions, Versioning-suspended: existing versions are retained, new versions are not created.
- ❑ When an object is deleted/re-written, a delete marker is added to the current version, and the object is retained as a previous version.
- ❑ Once enabled (on a bucket), versioning cannot be disabled, only suspended. Must then use lifecycle expiration policies, to transition objects (to another storage class), or expire objects (ie: delete after x amount of time). Applies only to current version.
- ❑ Removing expired markers can improve performance (ie: when listing bucket contents).

S3: Simple Storage Service

Events, Notifications:

- ❑ PUT command (new object created) can generate event notifications to SNS, SQS, Lambda (“event based computing”). Example: an image or video file is uploaded, which kicks off a transcoding workflow…
- ❑ Highly reliable, “nine 9s” of reliability, with at least once delivery.
- ❑ Destination service must be in same region as S3 bucket (reliability, perf reasons)
- ❑ No charge for event notifications, pay only for use of services (Lambda, SNS, SQS, etc...)

Thank you !

@_markcohen