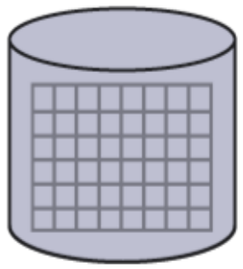
AWS Solutions Architect Associate

Session 301

Storage: S3

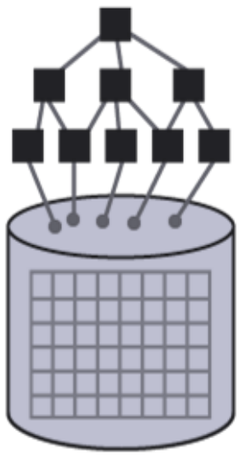
July/2024

AWS Storage



Block Storage
Raw Storage
Data organized as an array of unrelated blocks
Host File System places data on disk
E.g.: Microsoft NTFS, Unix ZFS

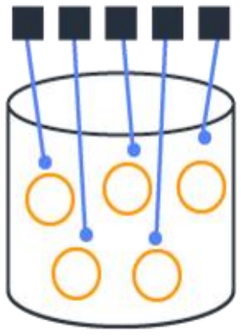
EBS



File Storage
Unrelated data blocks managed by a file (serving) system
Native file system places data on disk

EFS

FSx



Object Storage
Stores Virtual containers that encapsulate the data, data attributes, metadata and Object ID
API Access to data
Metadata Driven, Policy-based, etc.

S3

Simple Storage Service – S3

Amazon Simple Storage Service

Bucket

Bucket with objects

- (..) 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.
- It’s one of the oldest service offered by Amazon (2006): mature.

- Object Storage. Simple element: Bucket
- No system-boot volume.
- Unlimited storage per bucket, however object size range from 0 to 5 TB (Single PUT 5GB). Via Web Console, upto 160 GB in a file.
- Automatic S3 replication minimum for 3 AZ's where the region allow it, a single exception (S3 One-Zone IA).
- HTTP Code is 200 when an object upload is successful
- Bucket name must be an unique DNS-Compliant name
- Path-Styled Request (Depreciated on 30/Sept/2020) https://s3.Region.amazonaws.com/bucket-name/keyname
- Virtual-Hosted Style: https://bucket-name.s3.Region.amazonaws.com/keyname

Taken from https://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html and https://aws.amazon.com/blogs/aws/amazon-s3-path-deprecation-plan-the-rest-of-the-story/ (17/07/2024)

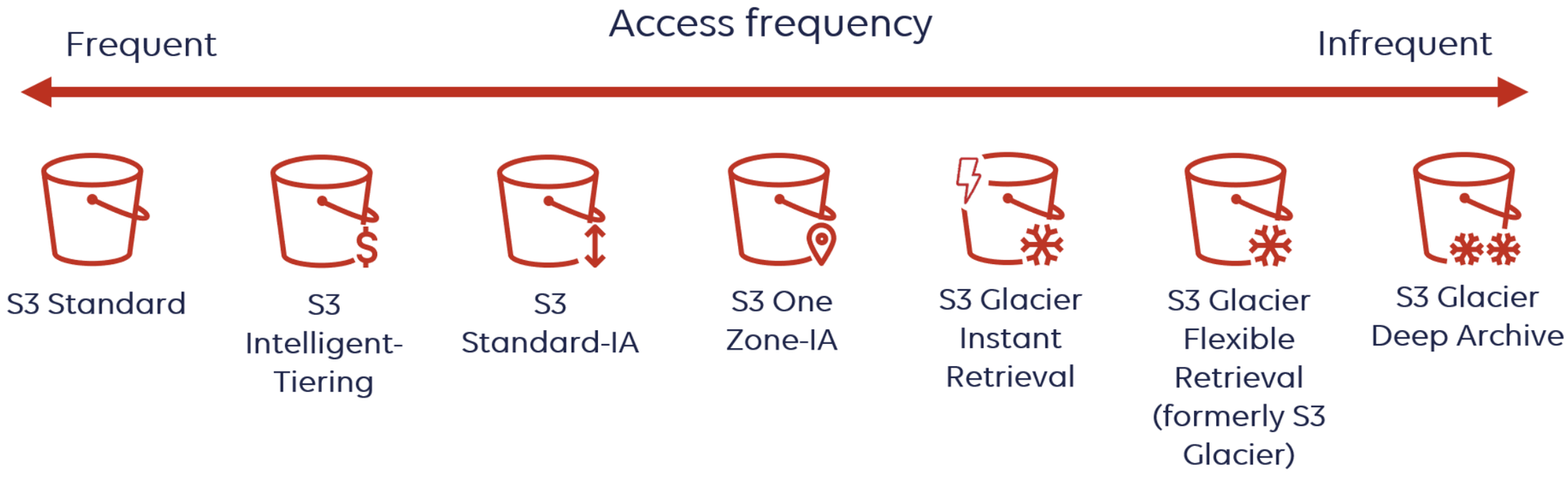
Consistency Model

- Strong Consistency (Read-after-write) for new objects after PUT.
- Eventual consistency for previous objects for PUT (Rewrite) and DELETE due to propagation.
- As S3 is object-based storage, its compose by:
  - **Key:** Object Name.
  - **Value: Object itself.**
  - **Version ID:** Important if version is activated.
  - **Metadata:** Store tags.

Storage Classes

Class	Description
S3 Standard	Base configuration
S3 Standard - Infrequent Access (IA)	Similar to Standard, however it costs retrieval access.
S3 One Zone - Infrequent Access	Reduced Redundancy Storage
Glacier Instant Retrieval	Lower cost with a retrieval at least in quarter, same latency for Standard
Glacier Flexible Retrieval	Historic files, long retrieval time. • Expedited retrievals (restore in 1–5 minutes). • Standard retrievals (restore in 3–5 hours). • Bulk retrievals (restore in 5–12 hours). Bulk retrievals are available at no additional charge.
Glacier Deep Archive	Longest retrieval time. Longer time to move there.
S3 – Intelligent Tier	Similar to Standard, it has intelligent to move between 2 tiers: frequent and infrequent.

Buckets has default Standard storage class for all objects, but you can modify it per object.



Comparative for S3 Storage Classes

	S3 Standard	S3 Intelligent-Tiering*	S3 Express One Zone**	S3 Standard-IA	S3 One Zone-IA**	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval***	S3 Glacier Deep Archive***
Use cases	General purpose storage for frequently accessed data	Automatic cost savings for data with unknown or changing access patterns	High performance storage for your most frequently accessed data	Infrequently accessed data that needs millisecond access	Re-creatable infrequently accessed data	Long-lived data that is accessed a few times per year with instant retrievals	Backup and archive data that is rarely accessed and low cost	Archive data that is very rarely accessed and very low cost
First byte latency	milliseconds	milliseconds	single-digit milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Durability	Amazon S3 provides the most durable storage in the cloud. Based on its unique architecture, S3 is designed to exceed **99.999999999% (11 nines)** data durability. Additionally, S3 stores data redundantly across a minimum of 3 Availability Zones by default, providing built-in resilience against widespread disaster. Customers can store data in a single AZ to minimize storage cost or latency, in multiple AZs for resilience against the permanent loss of an entire data center, or in multiple AWS Regions to meet geographic resilience requirements.							
Designed for availability	99.99%	99.9%	99.95%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99.9%	99%	99%	99%	99.9%	99.9%
Availability Zones	≥3	≥3	1	≥3	1	≥3	≥3	≥3
Minimum storage duration charge	N/A	N/A	1 hour	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
Lifecycle transitions	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes

Taken from https://aws.amazon.com/s3/storage-classes/#Performance_across_the_S3_storage_classes (12/07/2024)

Pricing: Storage

Its based on Storage, Requests, Data Transfers, and Management and Replication.
We will see, for us-east-1 as example.

	Storage pricing
S3 Standard - General purpose storage for any type of data, typically used for frequently accessed data	
First 50 TB / Month	$0.023 per GB
Next 450 TB / Month	$0.022 per GB
Over 500 TB / Month	$0.021 per GB
S3 Intelligent - Tiering* - Automatic cost savings for data with unknown or changing access patterns	
Monitoring and Automation, All Storage / Month (Objects > 128 KB)	$0.0025 per 1,000 objects
Frequent Access Tier, First 50 TB / Month	$0.023 per GB
Frequent Access Tier, Next 450 TB / Month	$0.022 per GB
Frequent Access Tier, Over 500 TB / Month	$0.021 per GB
Infrequent Access Tier, All Storage / Month	$0.0125 per GB
Archive Instant Access Tier, All Storage / Month	$0.004 per GB
S3 Intelligent - Tiering* - Optional asynchronous Archive Access tiers	
Archive Access Tier, All Storage / Month	$0.0036 per GB
Deep Archive Access Tier, All Storage / Month	$0.00099 per GB
S3 Standard - Infrequent Access** - For long lived but infrequently accessed data that needs millisecond access	
All Storage / Month	$0.0125 per GB
S3 One Zone - Infrequent Access** - For re-createable infrequently accessed data that needs millisecond access	
All Storage / Month	$0.01 per GB
S3 Glacier Instant Retrieval*** - For long-lived archive data accessed once a quarter with instant retrieval in milliseconds	
All Storage / Month	$0.004 per GB
S3 Glacier Flexible Retrieval (Formerly S3 Glacier)*** - For long-term backups and archives with retrieval option from 1 minute to 12 hours	
All Storage / Month	$0.0036 per GB
S3 Glacier Deep Archive*** - For long-term data archiving that is accessed once or twice in a year and can be restored within 12 hours	
All Storage / Month	$0.00099 per GB

Taken from https://aws.amazon.com/s3/pricing/?nc=sn&loc=4 (12/07/2024)

Pricing: Requests

Example, for us-east-1

	PUT, COPY, POST, LIST requests (per 1,000 requests)	GET, SELECT, and all other requests (per 1,000 requests)	Lifecycle Transition requests into (per 1,000 requests)	Data Retrieval requests (per 1,000 requests)	Data retrievals (per GB)
S3 Standard	$0.005	$0.0004	n/a	n/a	n/a
S3 Intelligent - Tiering *	$0.005	$0.0004	$0.01	n/a	n/a
Frequent Access	n/a	n/a	n/a	n/a	n/a
Infrequent Access	n/a	n/a	n/a	n/a	n/a
Archive Instant	n/a	n/a	n/a	n/a	n/a
Archive Access, Standard	n/a	n/a	n/a	n/a	n/a
Archive Access, Bulk	n/a	n/a	n/a	n/a	n/a
Archive Access, Expedited	n/a	n/a	n/a	$10.00	$0.03
Deep Archive Access, Standard	n/a	n/a	n/a	n/a	n/a
Deep Archive Access, Bulk	n/a	n/a	n/a	n/a	n/a
S3 Standard - Infrequent Access **	$0.01	$0.001	$0.01	n/a	$0.01
S3 One Zone - Infrequent Access **	$0.01	$0.001	$0.01	n/a	$0.01
S3 Glacier Instant Retrieval ***	$0.02	$0.01	$0.02	n/a	$0.03
S3 Glacier Flexible Retrieval ***	$0.03	$0.0004	$0.03	See below	See below
Expedited	n/a	n/a	n/a	$10.00	$0.03
Standard	n/a	n/a	n/a	$0.05	$0.01
Bulk ***	n/a	n/a	n/a	n/a	n/a
Provisioned Capacity Unit ****	n/a	n/a	n/a	n/a	$100.00 per unit
S3 Glacier Deep Archive ***	$0.05	$0.0004	$0.05	See below	See below
Standard	n/a	n/a	n/a	$0.10	$0.02
Bulk	n/a	n/a	n/a	$0.025	$0.0025

Taken from https://aws.amazon.com/s3/pricing/?nc=sn&loc=4 (12/07/2024)

Lifecycle

Lifecycle

90 days

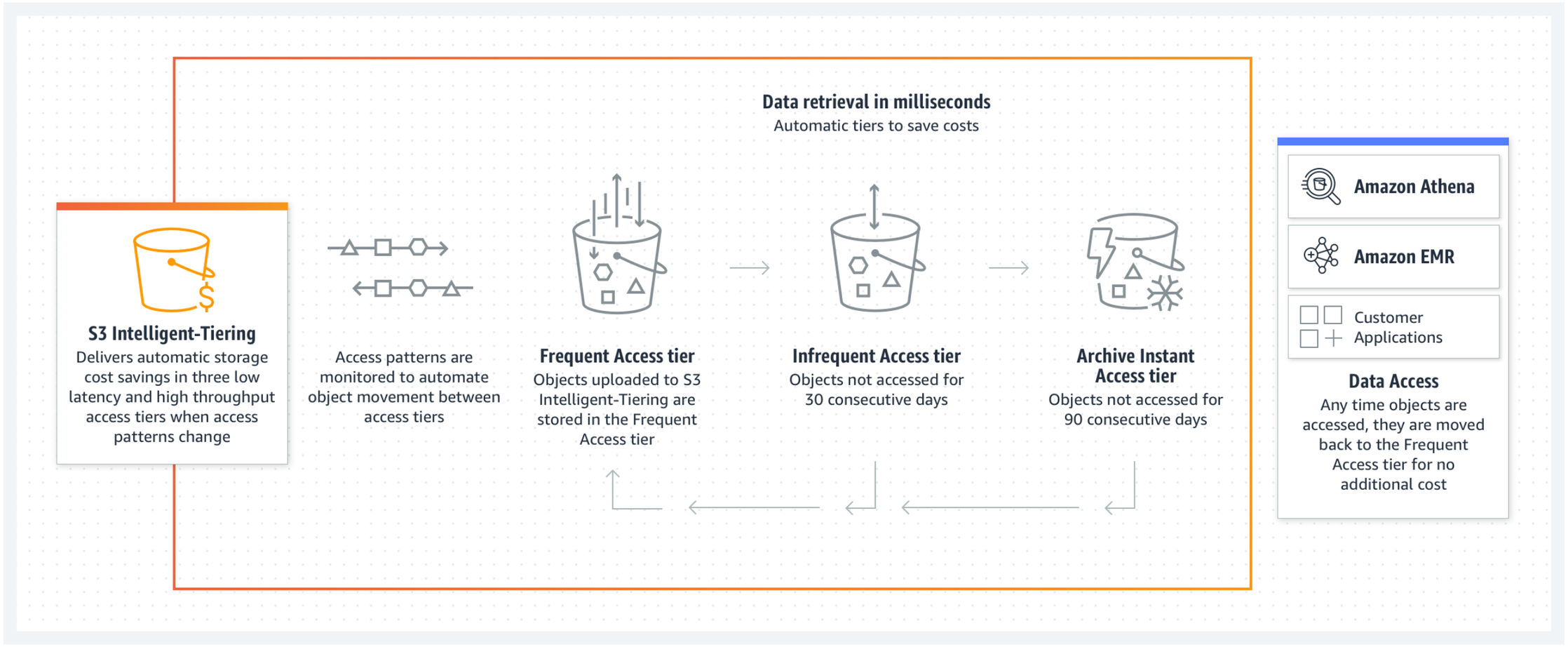
1 year

Amazon S3 Standard

Amazon S3 Infrequent Access

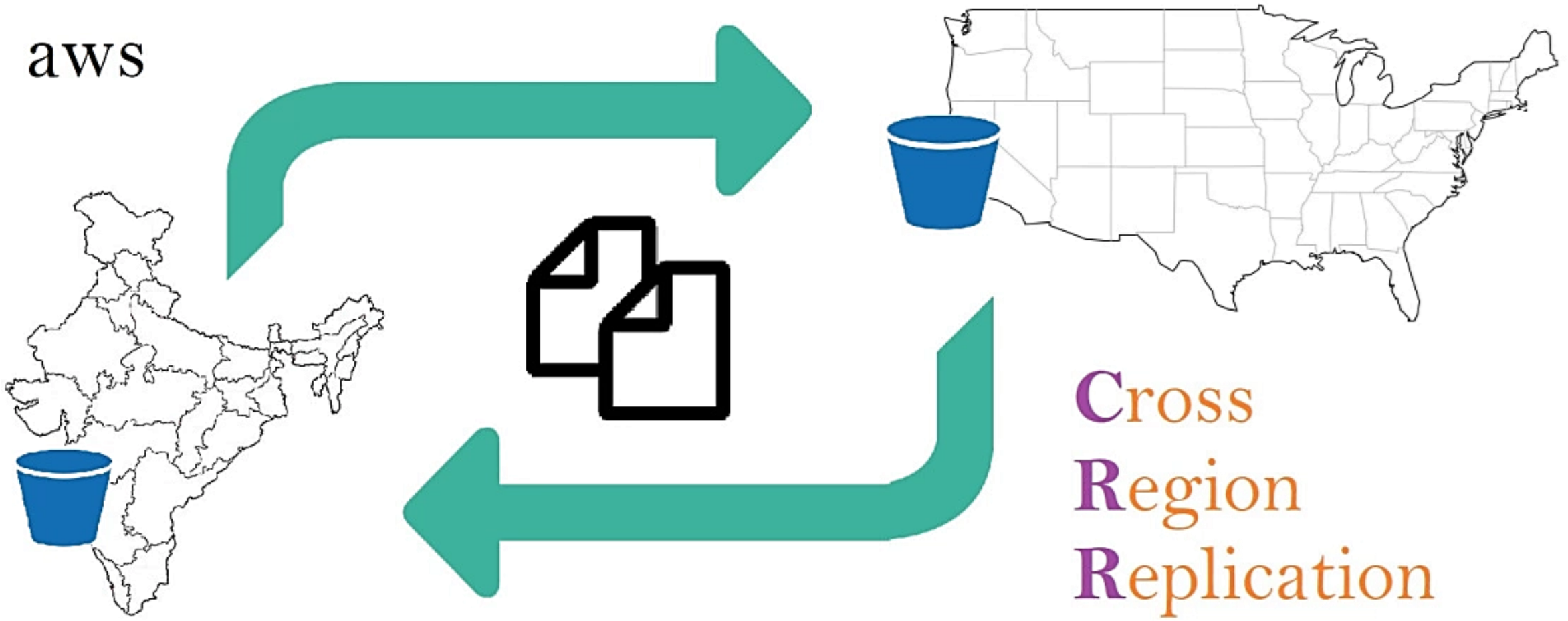
Amazon Glacier

Intelligent Tiering



Taken from https://aws.amazon.com/s3/storage-classes/intelligent-tiering/ (12/07/2024)

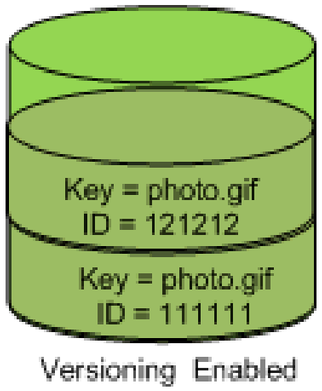
Cross-Region Replication

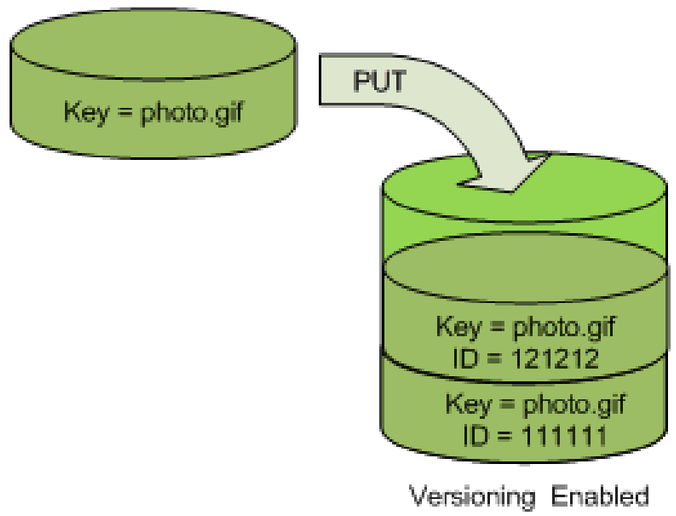


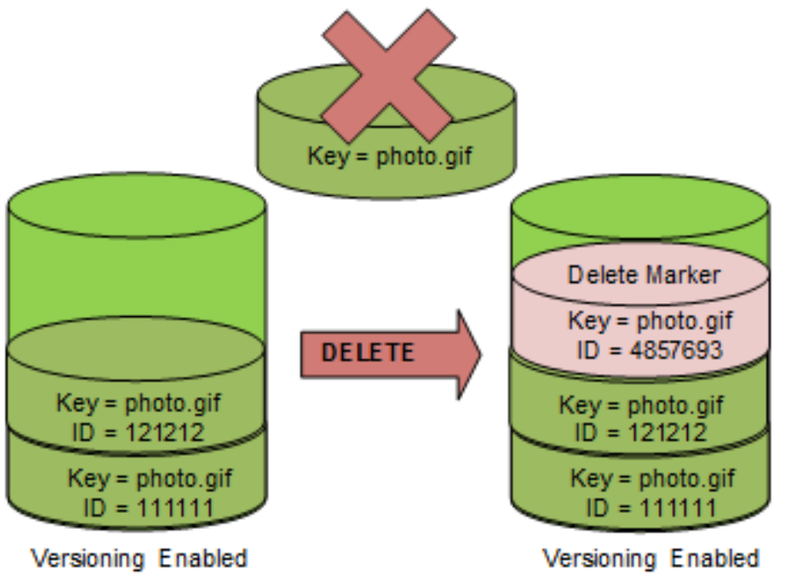
- Regulatory law or administrative requirement (DRP).
- Reduce latency.
- Operational requests.
- Keep copied objects in several accounts.

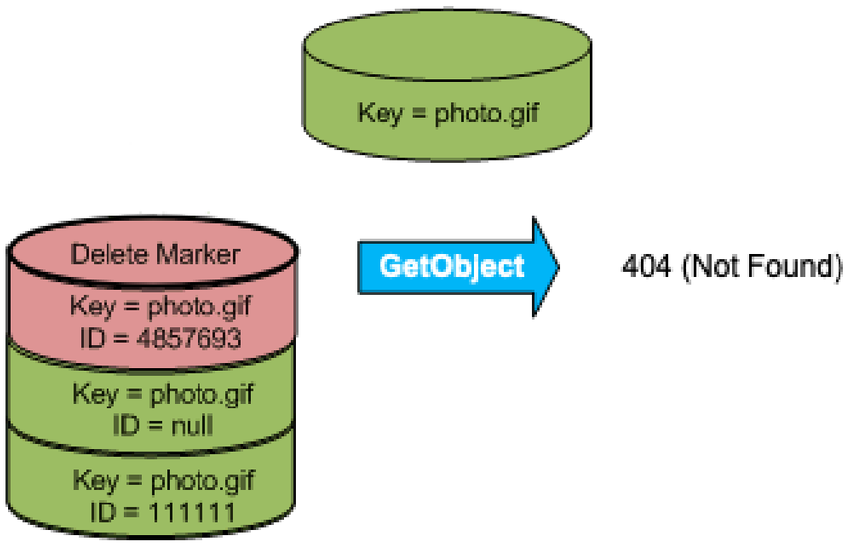
Taken from https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-example-walkthroughs.html (12/07/2024)

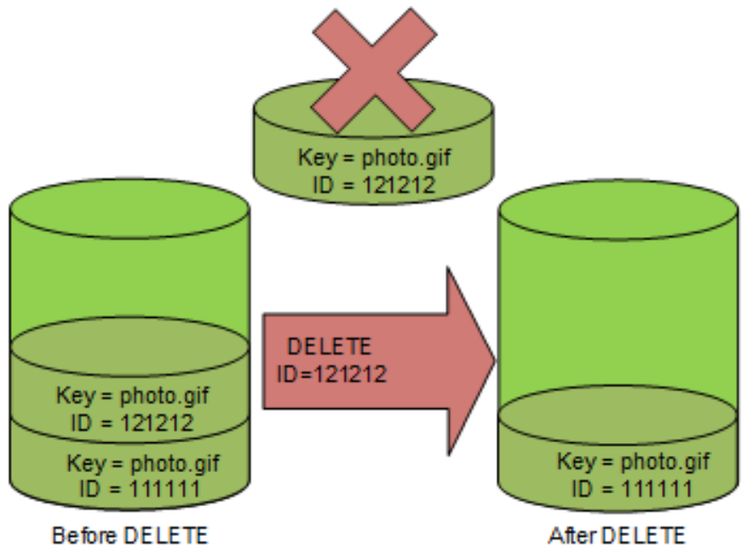
Versioning











Taken from https://docs.aws.amazon.com/AmazonS3/latest/userguide/versioning-workflows.html (12/07/2024)

Overview | Properties | Permissions (Public)

Access Control List (Public) | Bucket Policy | CORS configuration

CORS configuration editor ARN: [redacted]

Add a new cors configuration or edit an existing one in the text area below.

```
<?xml version="1.0" encoding="UTF-8"?>
<CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>PUT</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedMethod>HEAD</AllowedMethod>
    <ExposeHeader>ETag</ExposeHeader>
    <AllowedHeader>*</AllowedHeader>
</CORSRule>
</CORSConfiguration>
```

AWS Glacier - Archives


Amazon S3 Glacier


Vault


Archive

- Data is stored in Amazon S3 Glacier in "archives" and its similar to S3 Buckets are called “vaults”.
- A single archive can be as large as **40 TB**.
- Each archive is assigned a unique archive ID at the time of creation, and the content of the archive is immutable, meaning that after an archive is created it cannot be updated.

AWS Glacier - Vaults

- Amazon S3 Glacier uses **"vaults" as containers to store archives**.

- You can view a list of your vaults in the AWS Console and use the **SDKs** to perform a variety of vault operations.

- You can also set access policies for each vault to grant or deny specific activities to users.

- Under a single AWS account → 1000 vaults.

AWS Glacier – Deep Archive

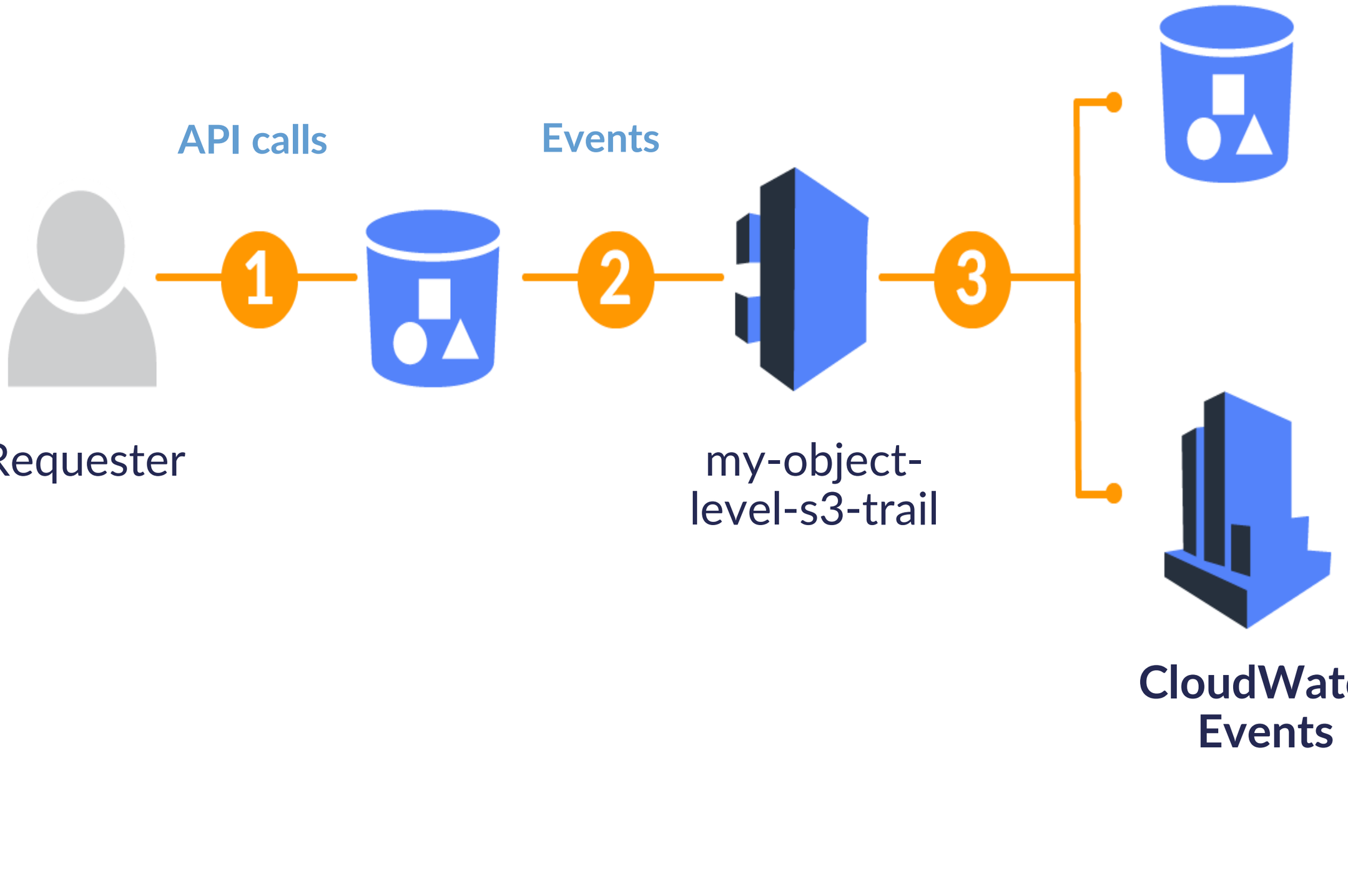
Many AWS customers collect and store large volumes (**often a petabyte or more**) of important data but **seldom access it**. In some cases raw data is collected and immediately processed, then stored **for years or decades** just in case there's a need for further processing or analysis.

In other cases, the data is retained for compliance or auditing purposes

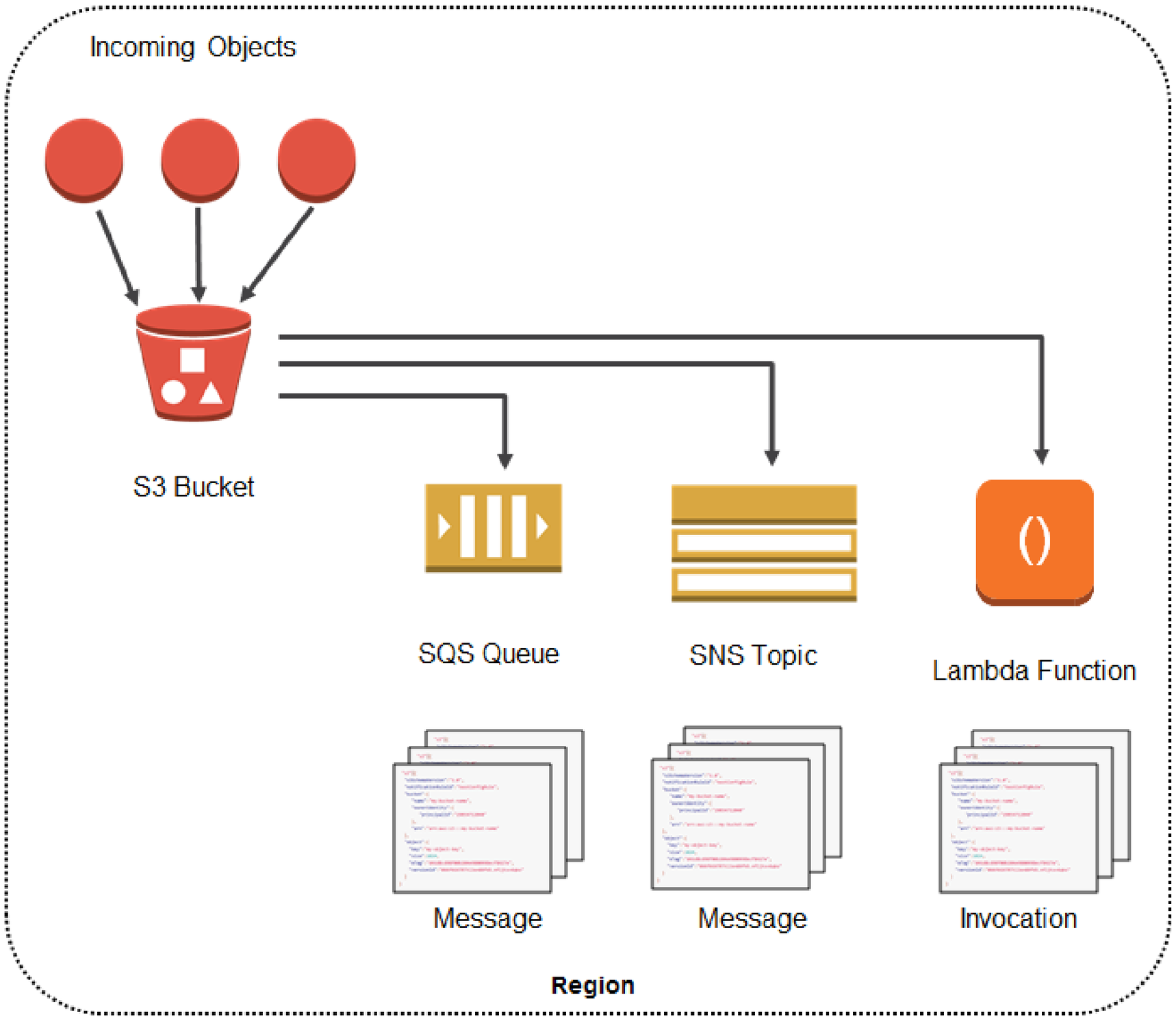
- **$0.00099 Per GB per Month**

https://calculator.aws/#/

S3 Logging



S3 Event Notification



Transfer Acceleration

San Francisco

(US-WEST-1) 720% faster

S3 Direct Upload Speed

Upload complete

S3 Accelerated Transfer Upload Speed

Upload complete

Oregon

(US-WEST-2) 1362% faster

S3 Direct Upload Speed

Upload complete

S3 Accelerated Transfer Upload Speed

Upload complete

Frankfurt

(EU-CENTRAL-1) 206% faster

S3 Direct Upload Speed

Upload complete

S3 Accelerated Transfer Upload Speed

Upload complete

Tokyo

(AP-NORTHEAST-1) 48% slower

S3 Direct Upload Speed

Upload complete

S3 Accelerated Transfer Upload Speed

Upload complete

S3 Transfer Acceleration is not supported for buckets with periods (.) in their names

Using Cloudfront Edge Location.
Change accelerated endpoint.
It can be an option instead of Snowball

Taken from S3 FAQs (https://aws.amazon.com/s3/faqs/#Amazon_S3_Transfer_Acceleration) on (10/05/2020)

S3 Events

Name	Events	Filter	Type

New event

Name

e.g. MyEmailEventForPut

Events

- RRSObjectLost
- Put
- Post
- Copy
- Complete Multipa
- Delete
- Delete Marker Created
- ObjectCreate (All)
- ObjectDelete (All)

Prefix

e.g. images/

Suffix

e.g. .jpg

Send to

Select notification d

Send to

Select notification destination

- SNS Topic
- SQS Queue
- Lambda Function

Amazon S3 > fmorenod > Create event notification

Create event notification

The notification configuration identifies the events you want Amazon S3 to publish and the Amazon S3 to send the notifications. Learn more

General configuration

Event name

Event name

Event name can contain up to 255 characters.

Prefix - *optional*

Limit the notifications to objects with key starting with specified characters.

images/

Suffix - *optional*

Limit the notifications to objects with key ending with specified characters.

.jpg

Event types

Specify at least one type of event for which you want to receive notifications. Learn more

- All object create events
  s3:ObjectCreated:*
  - Put
    s3:ObjectCreated:Put
  - Post
    s3:ObjectCreated:Post

Destination

Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. Learn more

Destination

Choose a destination to publish the event. Learn more

- Lambda function
  Run a Lambda function script based on S3 events.
- SNS topic
  Send notifications to email, SMS, or an HTTP endpoint.
- SQS queue
  Send notifications to an SQS queue to be read by a server.

Specify Lambda function

- Choose from your Lambda functions
- Enter Lambda function ARN

Lambda function

Choose Lambda function

Cancel | Save changes

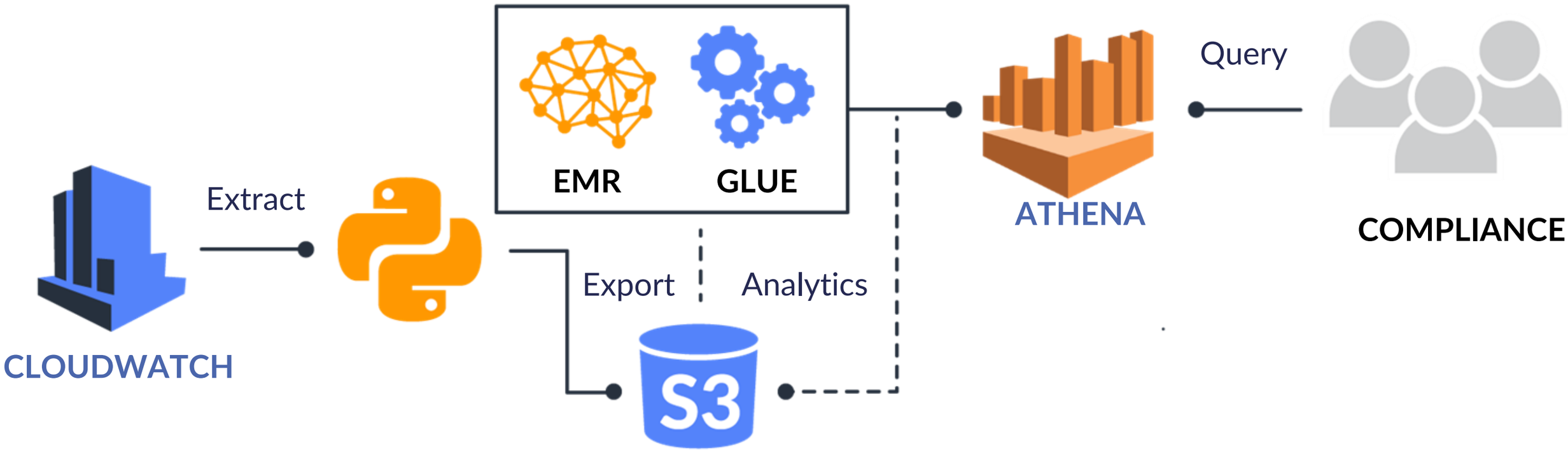
It seems that AWS UI/UX is working every year!

Multiload Parts

>100MB	CLI Usage on shell as separated components: s3cmd, s3ftp
SDK	Multipart upload. “Divide and conquer”, upload small parts simultaneously, as 5 MB to 5GB.
AWS CLI	Java, .NET, Python, Node JS, Ruby, PHP and C++ (Mobile); bit Torrent.

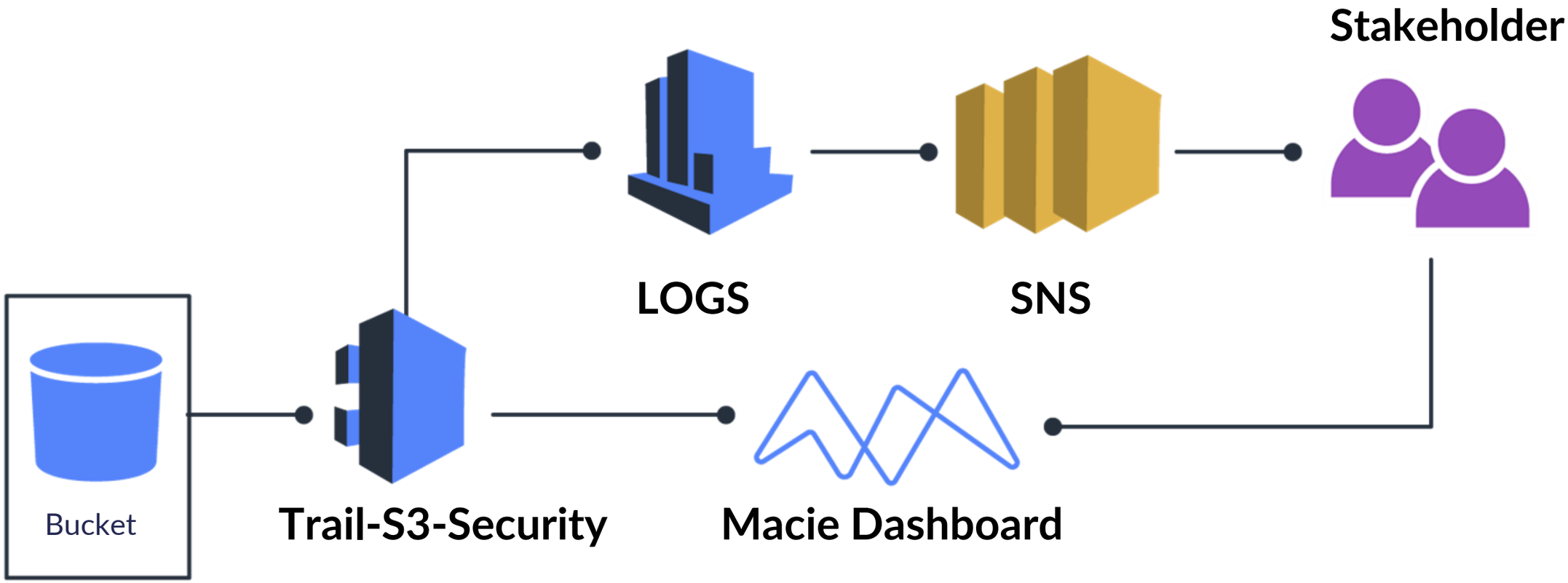
More info at https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html (12/07/2024)

Use Case: Big Data



Data ingestion and storage to receive logs (millions) using SDKs or Cloudwatch.

Use Case: Auditing



Object-Level-Logging

- Detect object changes under mission-critical bucket.
- Protect and audit important information.

Server Side Encryption (SSE)

- SSE-S3: S3 provide CMK.
- SSE-KMS: KMS manage CMK.
- SSE-C: Customer provide Encryption Key.

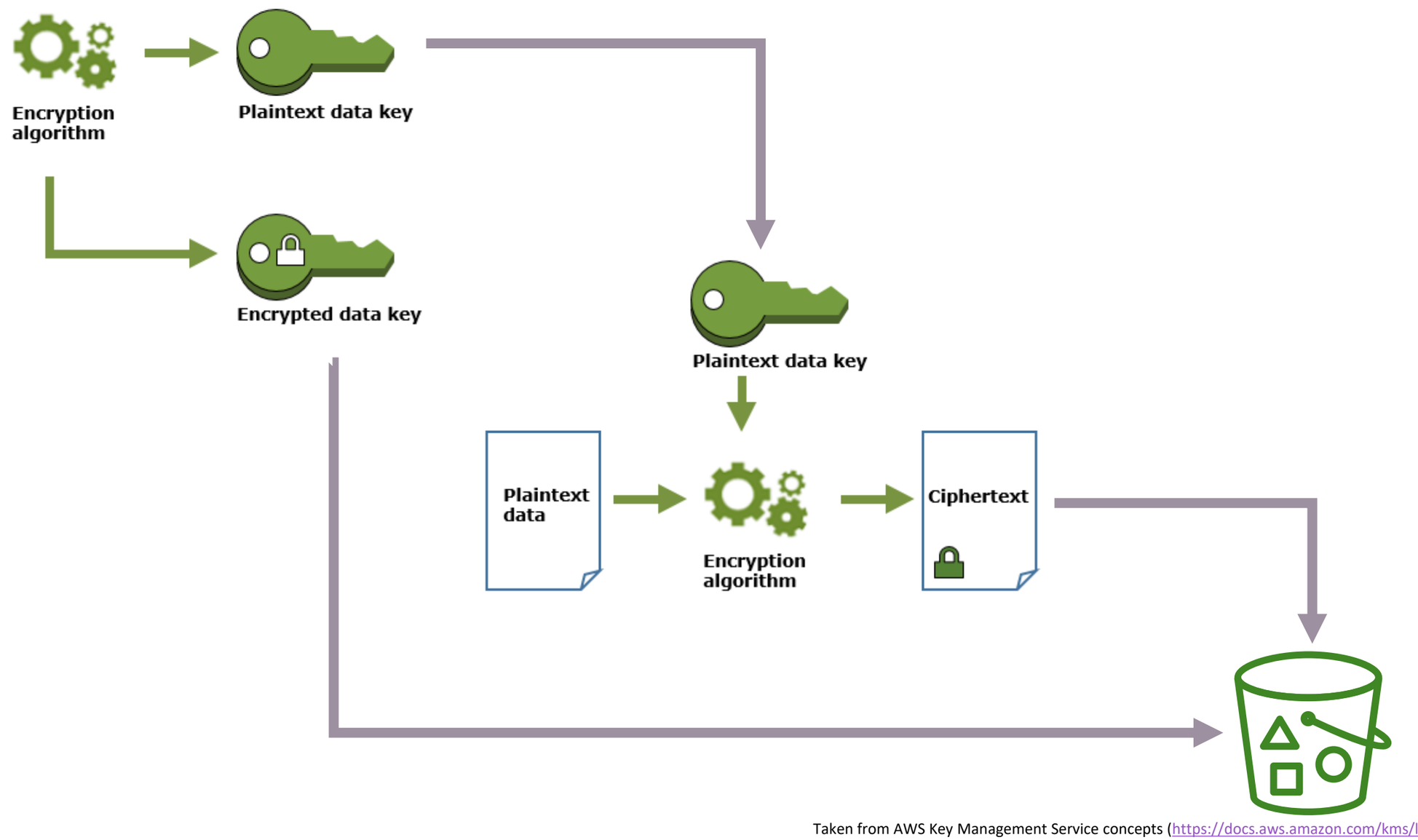
Client Side Encryption

Customer use CMK stored on KMS.
Encryption Key on your application.

Note: It’s only symmetric CMK.

Encryption

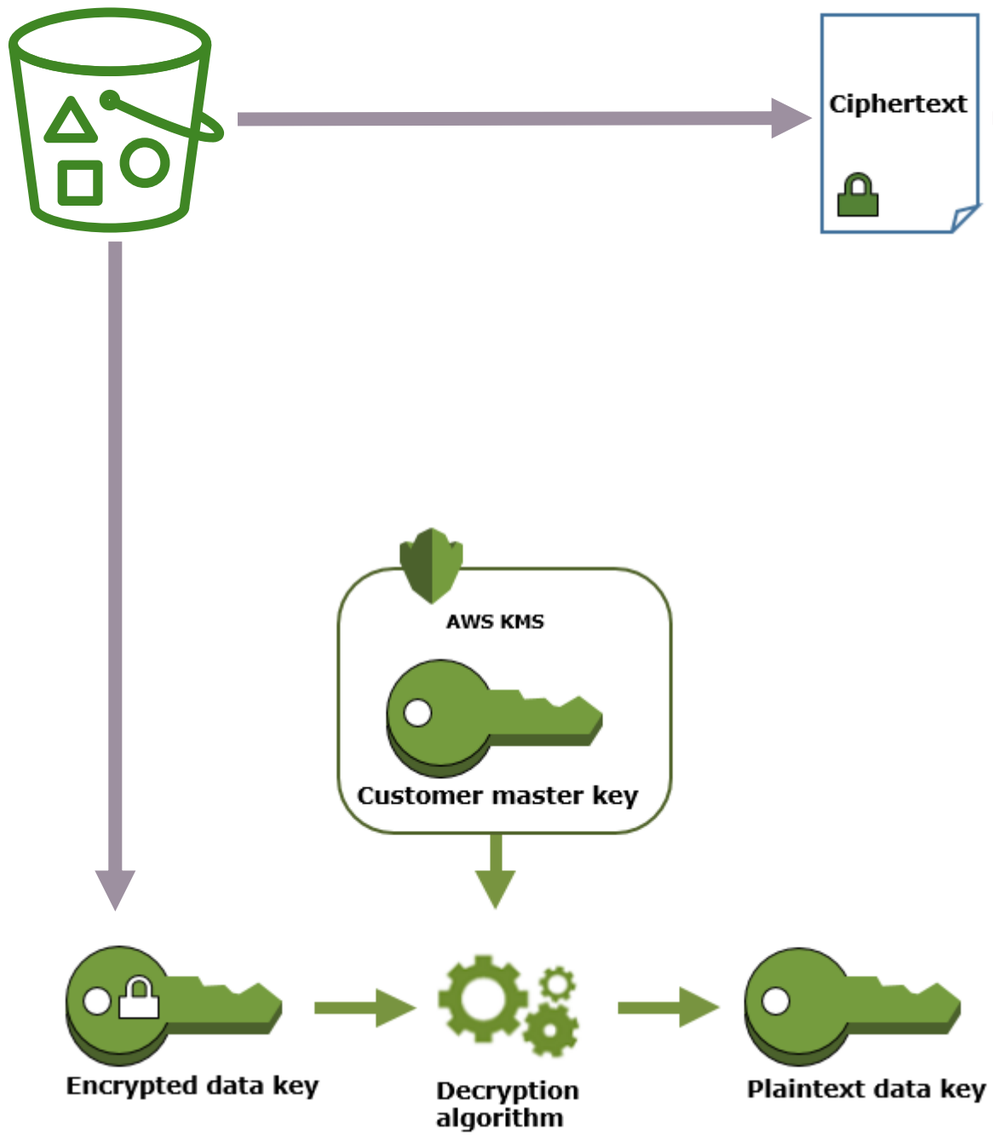
For SSE-S3 and -KMS using CMK
For SSE-C, Customer using Encryption Key



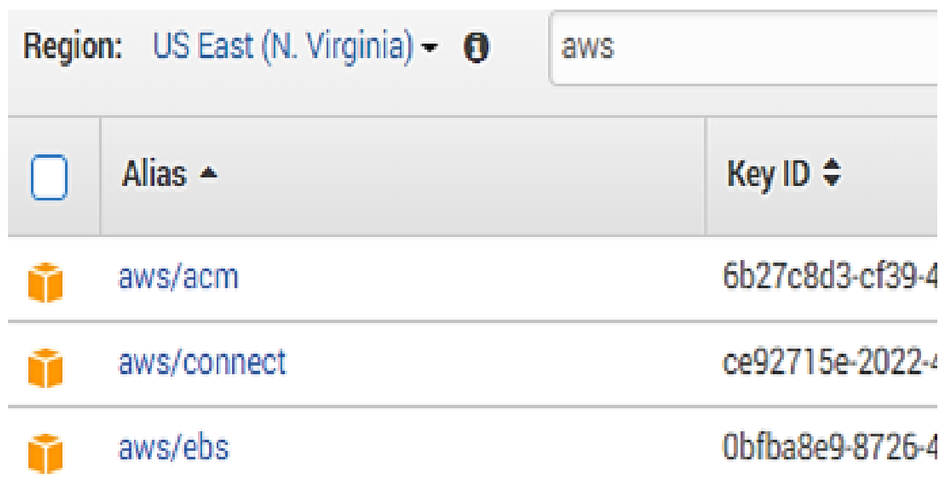
For SSE-C don’t store data key

Taken from AWS Key Management Service concepts (https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html) on (10/05/2020)

Decryption



For SSE-C, the encrypted data key is provided for customer



Taken from AWS Key Management Service concepts (https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html) on (10/05/2020)

Encryption Notes

Encryption Scope:	Only the value (Object), no metadata
Role to apply:	Using IAM Roles to allow to get actions on KMS
Keys:	using AES256 (Advanced Encryption Standard 256 bits)
Key Scope:	Region – Dependent, so Cross-Account or Replication depends only on generator.
Key Management:	Depend on creator (S3, KMS or Customer); for instanceKey Rotation.
KMS Advantages:	Auditing using CloudTrail, managed users using IAM

Type of CMK	Can view CMK metadata	Can manage CMK	Used only for my AWS account	Automatic rotation
Customer managed CMK	Yes	Yes	Yes	Optional. Every 365 days (1 year).
AWS managed CMK	Yes	No	Yes	Required. Every 1095 days (3 years).
AWS owned CMK	No	No	No	Varies

Taken from AWS Key Management Service concepts (https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html) on (10/05/2020)

KMS - Overview

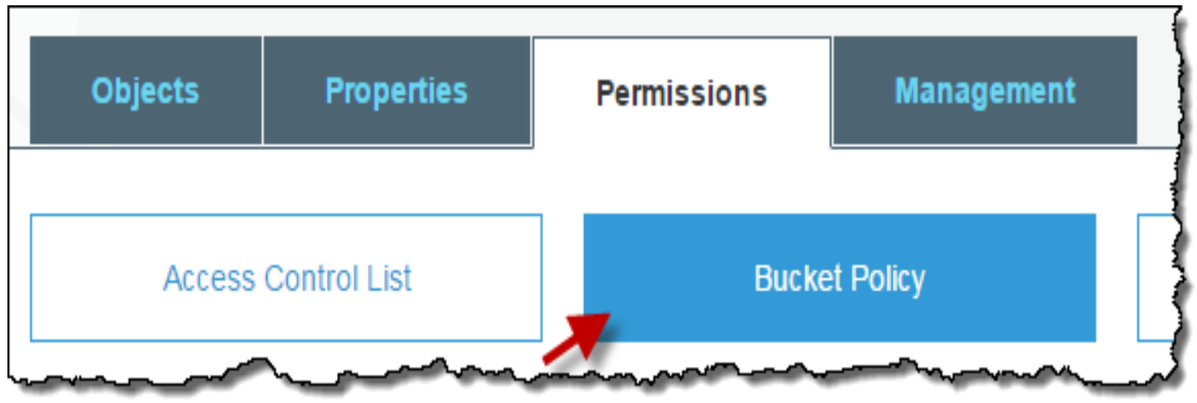
Key Management System :

- SECURE (Backup by CloudHSM – S11C1)
- Centralized Government
- Integrated with AWS Services (Approx. 83 services)
- Audit Capabilities (Cloud Trail)
- Scalability, Durability and HA
- Custom Key Store (CMK), backup by CloudHSM Cluster.
- Asymmetric Key Store
- Compliance:

Taken from https://aws.amazon.com/kms/features/ (09/06/2021)

Bucket Policies

- User/Role –based permissions.
- JSON-format file



Label	M/O	Description
Version	O	Specific language syntax. i.e. 2012-10-17
Statement	M	Contain the following elements.
Sid	O	Unique identifier.
Effect	M	Allow or Deny
Principal	M	Who (User/Role) using ARN format.
Action	M	Verbs to apply, i.e. s3GetObject
Resource	M	Resource ARN, scope.
Condition	O	Operations to fulfill.

Mandatory/Optional

Bucket Policies – Examples I

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AddPerm",
         "Effect":"Allow",
         "Principal": "*",
         "Action":["s3:GetObject"],
         "Resource":["arn:aws:s3:::examplebucket/*"]
      }
   ]
}
```

Bucket Policies – Examples II

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
      }
    }
  ]
}
```

Bucket Policies – Examples III

```
{
   "Version": "2012-10-17",
   "Id": "http referer policy example",
   "Statement": [
     {
       "Sid": "Allow get requests referred by www.example.com and example.com.",
       "Effect": "Allow",
       "Principal": "*",
       "Action": "s3:GetObject",
       "Resource": "arn:aws:s3:::examplebucket/*",
       "Condition": {
         "StringLike": {"aws:Referer": ["http://www.example.com/*","http://example.com/*"]}
       }
     },
      {
       "Sid": "Explicit deny to ensure requests are allowed only from specific referer.",
       "Effect": "Deny",
       "Principal": "*",
       "Action": "s3:*",
       "Resource": "arn:aws:s3:::examplebucket/*",
       "Condition": {
         "StringNotLike": {"aws:Referer": ["http://www.example.com/*","http://example.com/*"]}
       }
     }
   ]
}
```

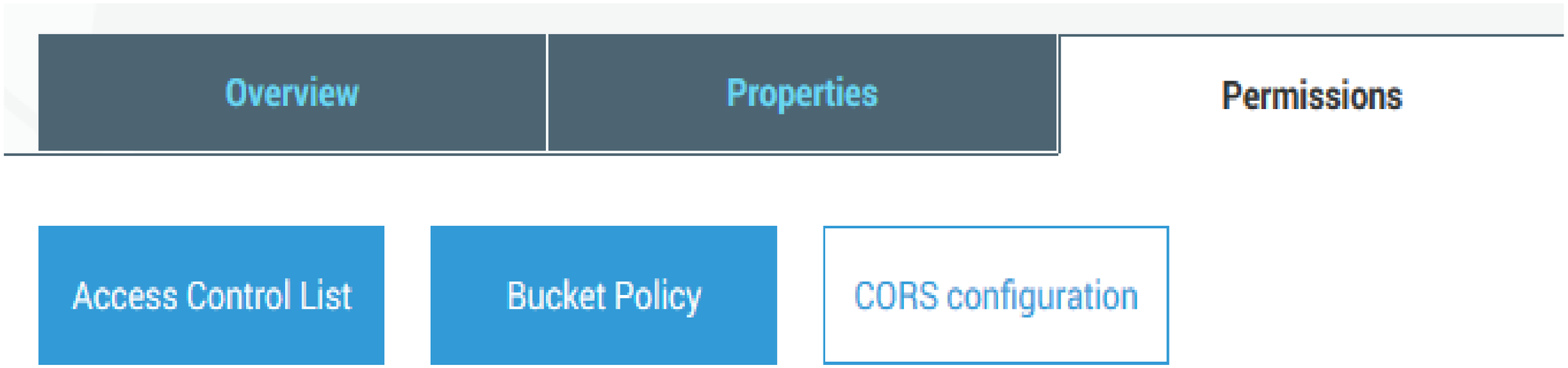
Bucket ACL

Bucket and Object permissions.

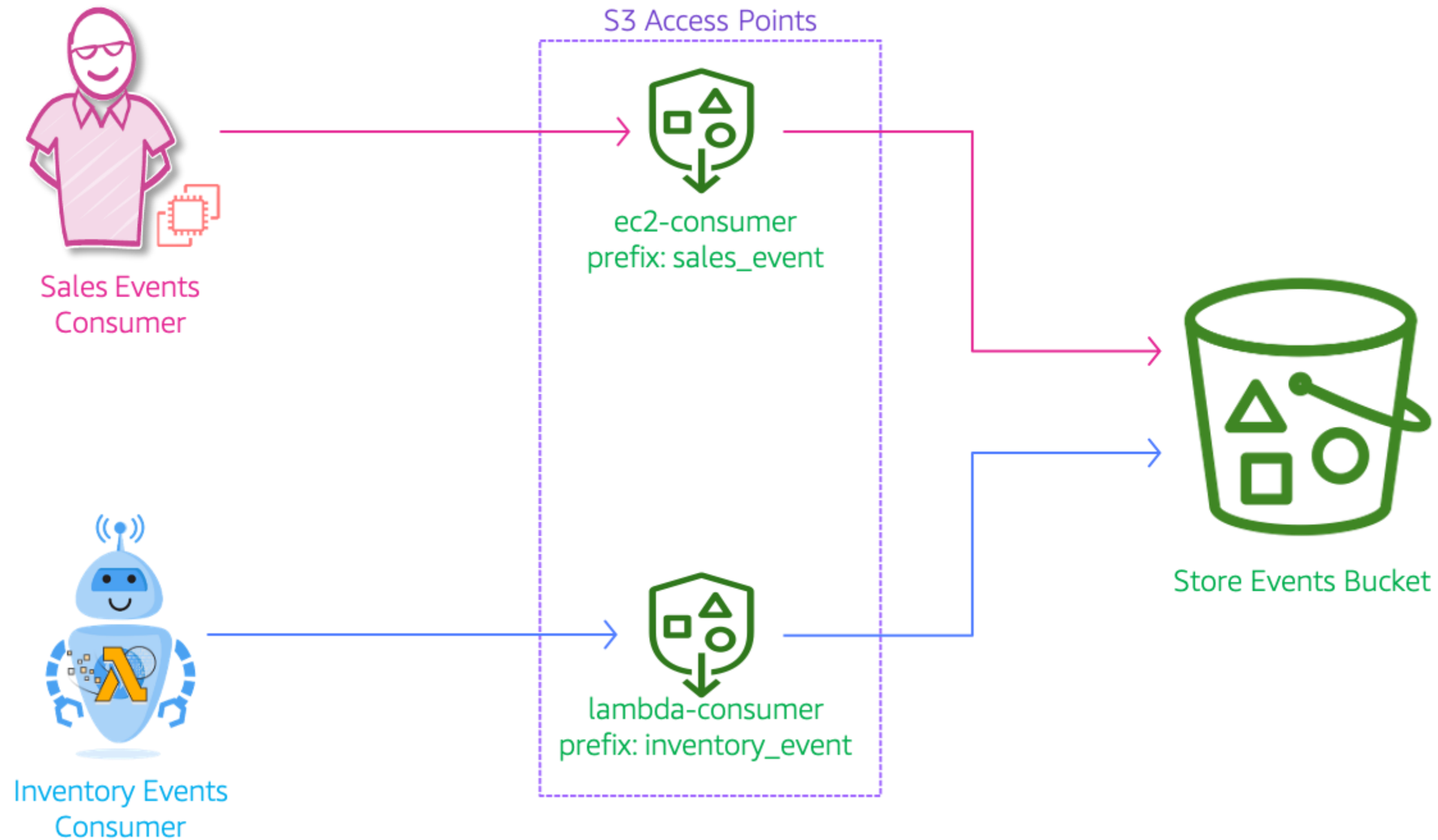
XML-format file.

Cross-Account Permissions.

Default permissions to account owner.



S3 Access Point



Each access point has:
A unique Domain Name System (DNS) name and Amazon Resource Name (ARN)
Distinct permissions and network controls

More info at https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-points.html (12/07/2024)