Storage y CDN

examen

- https://aws.amazon.com/s3/faqs
- https://aws.amazon.com/s3/storage-classes
- https://docs.aws... versioning
- aws dynamoDB

servicios

- S3 = Simple Storage Service
- Glacier
- Storage Gateway
- CloudFront = cacheado por región → CDN [1)]

S3

- object storage key-based
- escalable (no hay que especificar tamaño) infinitamente
- barato
- durabilidad
  - el objeto se guarda en los Availability Zones de la región (suelen ser 3 - datacenters -, pero depende de la region)
  - existe un servicio que no replica - más barato
- disponibilidad (SLA):
  - 99,99% availability
  - 99,999999999% durabilidad
- individual Amazons S3 objects:
  - 0 - 5TB
  - objeto enviable en un único PUT: 5GB
  - objetos de más de 100MB, se debería usar el Multipart Upload ← no accesible por la consola
- buckets ≡ directorios
  - por defecto privados
  - se crean en una región
  - global : nombres únicos
  - acceso: **https://s3.<region>.amazonaws.com/<bucket>**
  - web estática : convertir bucket en página web: **http://<bucket>.s3-website-<region>.amazonaws.com**
- se puede subir desde la consola
- objeto (key-based):
  - key
  - value : cadena de bits
  - version ID
  - metadata
  - ACL
- tired storage available
  - S3 Standard : normal
  - S3 Standard-IA (Infrequent Access) : acceso esporádico
    - recuperación más cara

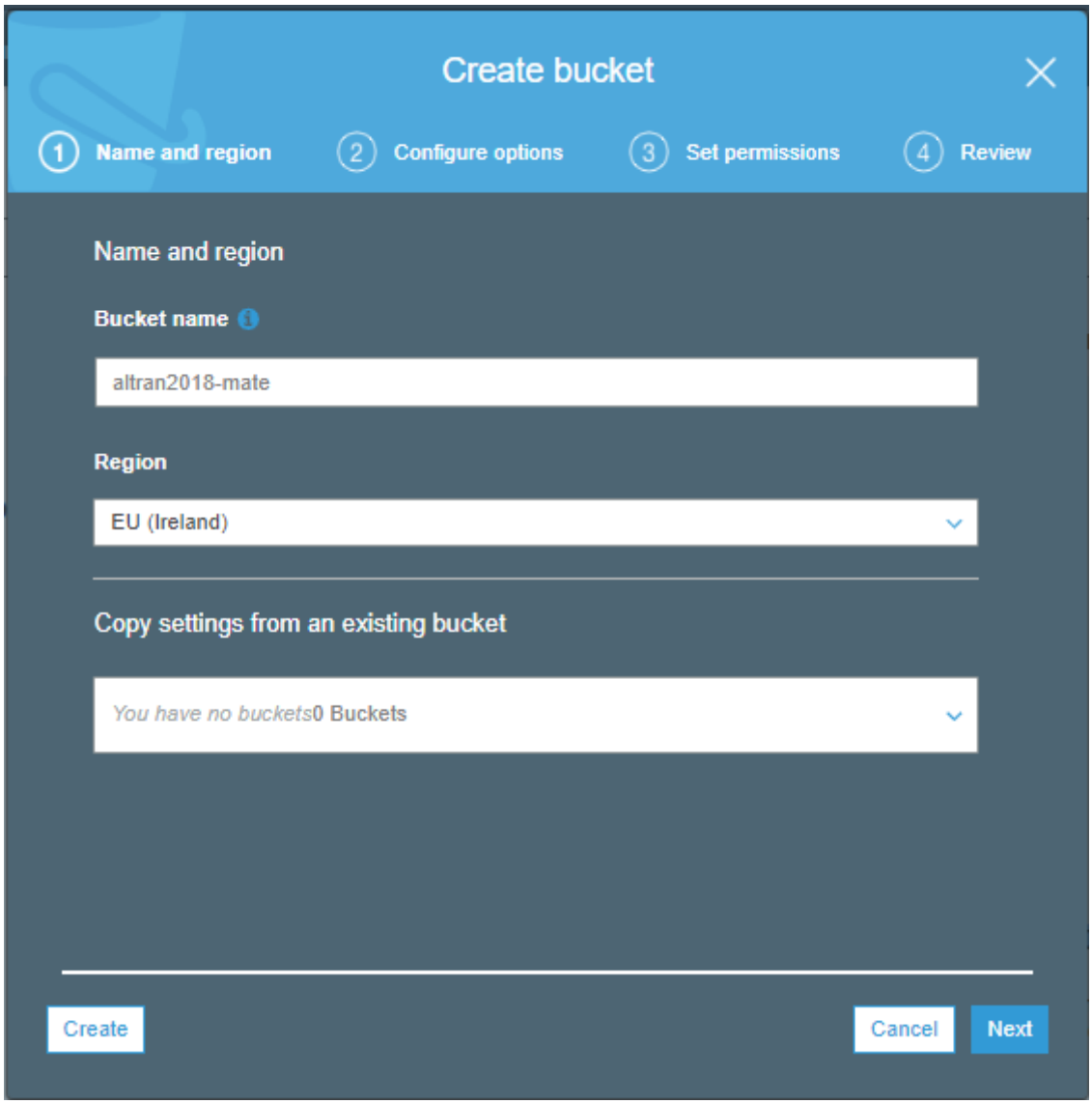
        - almacenamiento más barato
    - S3 Standard-One Z IA : idem anterior, pero en solo 1 zona
    - reduced Redundancy : to be deprecated
    - Glacier : recuperación entre 3-5 horas, mejorando
        - expedited : recuperación inmediata, muy caro recuperar
        - standard : 3-5 horas
        - bulk : 5-12 horas

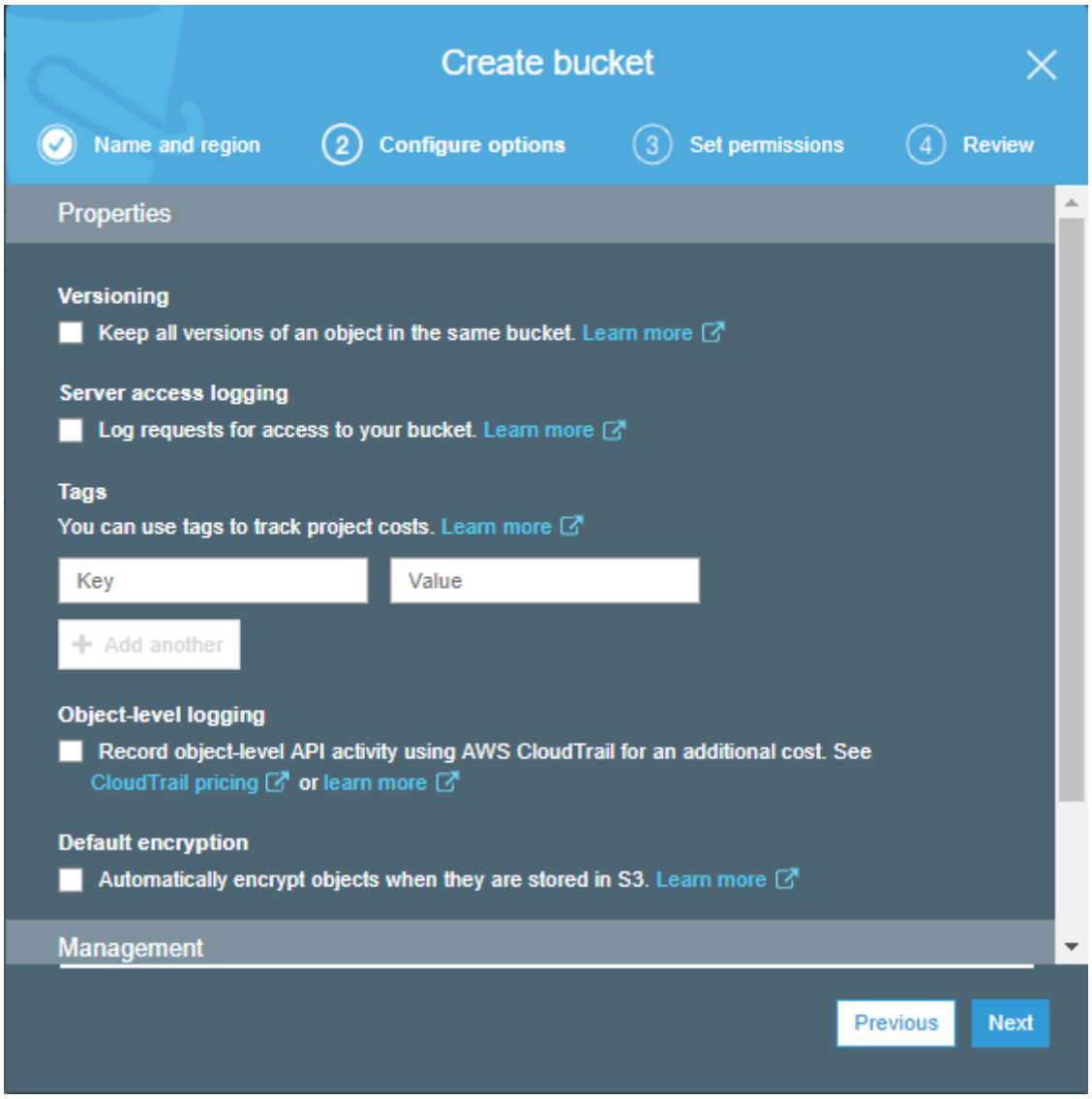
	S3 Estándar	S3 Estándar – Acceso poco frecuente	S3 Única zona – Acceso poco frecuente	Amazon Glacier
Diseñado para ofrecer durabilidad	99,999999999%	99,999999999%	99,999999999%†	99,999999999%
Diseñado para ofrecer disponibilidad	99,99%	99,9%	99,5%	N/D
SLA de disponibilidad	99,9%	99%	99%	N/D
Zonas de disponibilidad	≥3	≥3	1	≥3
Cargo mínimo de capacidad por objeto	N/D	128 KB*	128 KB*	N/D
Cargo mínimo por duración de almacenamiento	N/D	30 días	30 días	90 días
Tarifa de recuperación	N/D	por GB recuperado	por GB recuperado	por GB recuperado**
Latencia del primer byte	milisegundos	milisegundos	milisegundos	minutos u horas seleccionados***
Tipo de almacenamiento	Objeto	Objeto	Objeto	Objeto
Transiciones del ciclo de vida	Sí	Sí	Sí	Sí

- Versioning.
    - al sobreescribir/borrar guarda la versión anterior
    - MFA((Multi Factor Authentication) en borrado de ficheros
    - una vez activo no se puede desactivar, solo suspender
- Livecycle Management
    - reglas de ciclo de vida para mover entre los diferentes tipos de S3
    - de Standard → 30 días → IA → 30 días → Glacier
    - o borrar
- Securing buckets
    - ACL : Access Control List
        - a nivel de bucket o de objeto dentro de bucket
        - entidades en otras cuentas o en internet
    - Bucket Policies
        - a nivel de bucket
        - nivel «interno», nuestra cuenta.
    - access logs de todo lo que se hace
        - se puede guardar en el mismo bucket o en otro
    - encriptación
        - en tránsito SSL/TLS (por defecto)
        - encriptación en la lado cliente
        - al resto (en Amazon, Server Side)

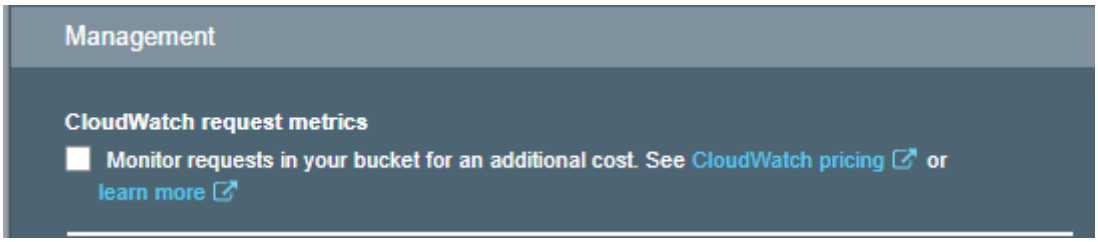
            - AES-256, server-side encryption con Amazon S3-Managed Keys (SSE-S3) ← gratuita
            - AWS-KMS, server-sice encruption con AWS KMS-Managed Keys (SSE-KMS)
                - se genera llave maestra que genera otras y hay un log de uso
                - auditado
            - server side encryption con Costumer Provided Keys (SSE-C) ← no dispoble en consola
        - el encriptado si es activado a posteriori, no encripta los elementos que ya están guardados, solo los nuevos
    - Data Consystency Model
        - PUTS : envío ficheros → Read-after-write ← al recibir el 200 (OK) ya está asegurada la consistencia)
        - PUTS overwrites y DELETES : consistencia eventual (lapso en el cual la misma petición podría dar resultados diferentes mientras se «sincroniza»)
    - costes:
        - almacenamiento
        - peticiones
        - storage management pricing (tags/metadata)
        - data transfer pricing (repicación inter-zona)
        - Transfer Acceleration
            - infraestructura cloudfront para acelerar el ratio

Laboratorio

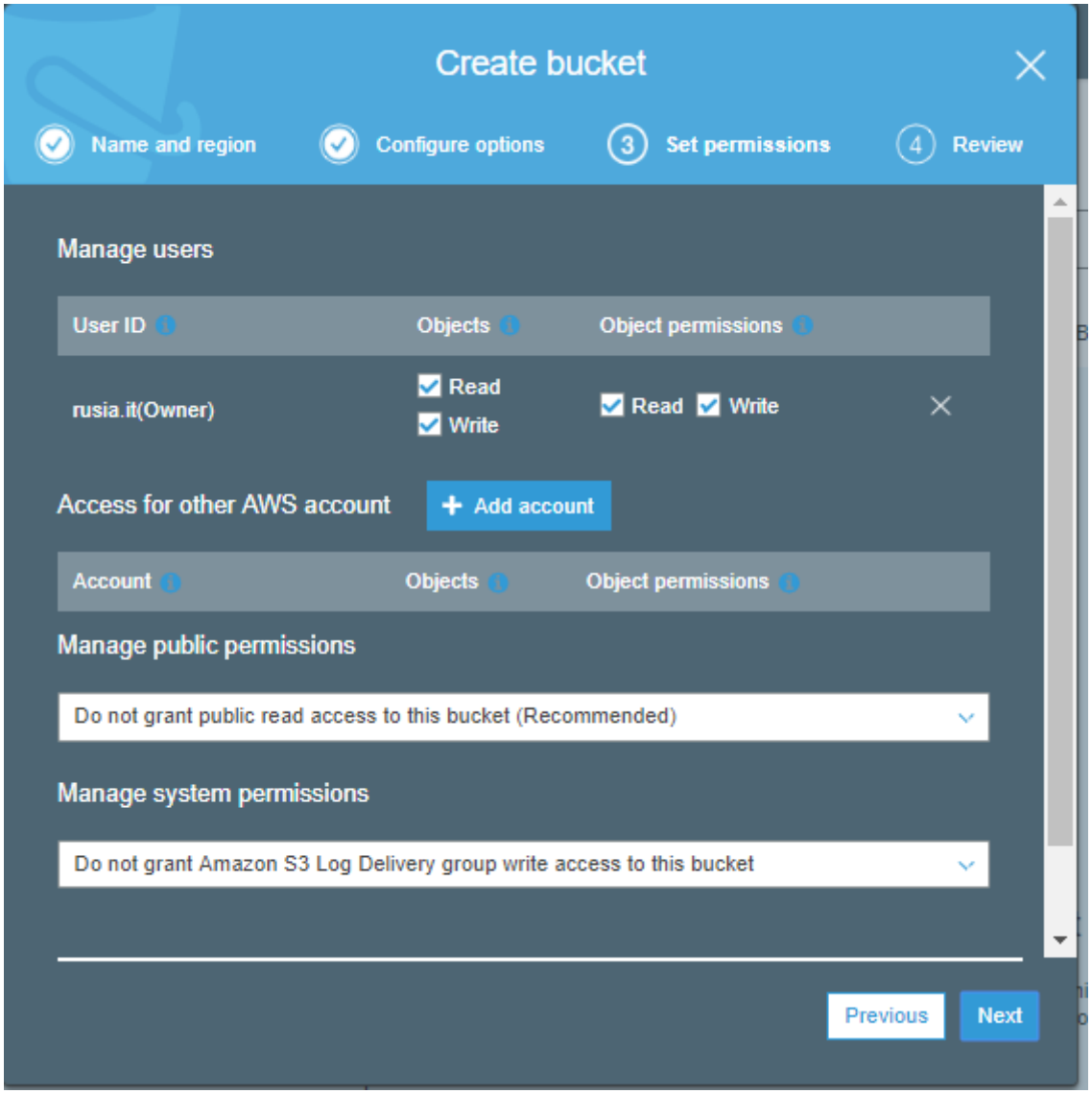




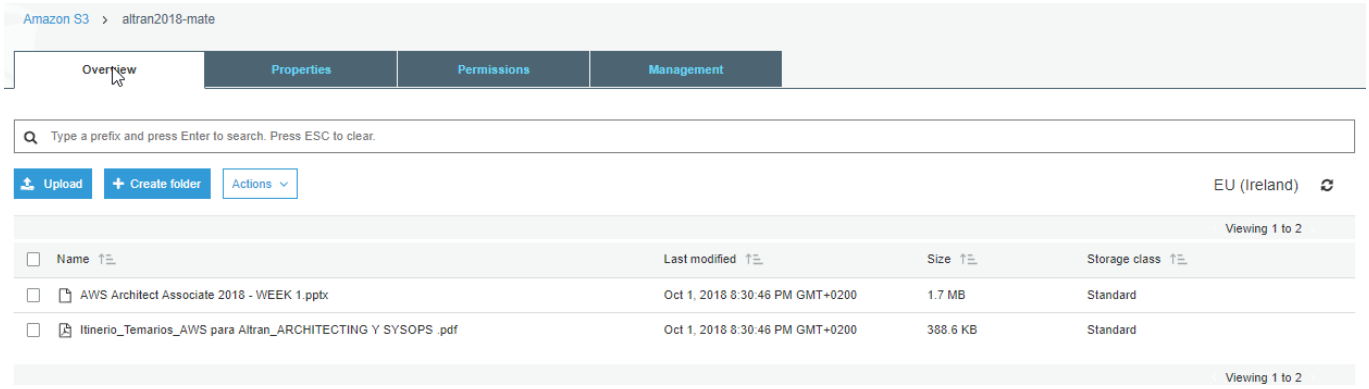
- tags:
  - para asociar a facturación
  - para establecer permisos
  - organización, agrupación
- CloudTrail : cualquier petición de usuario queda registrado

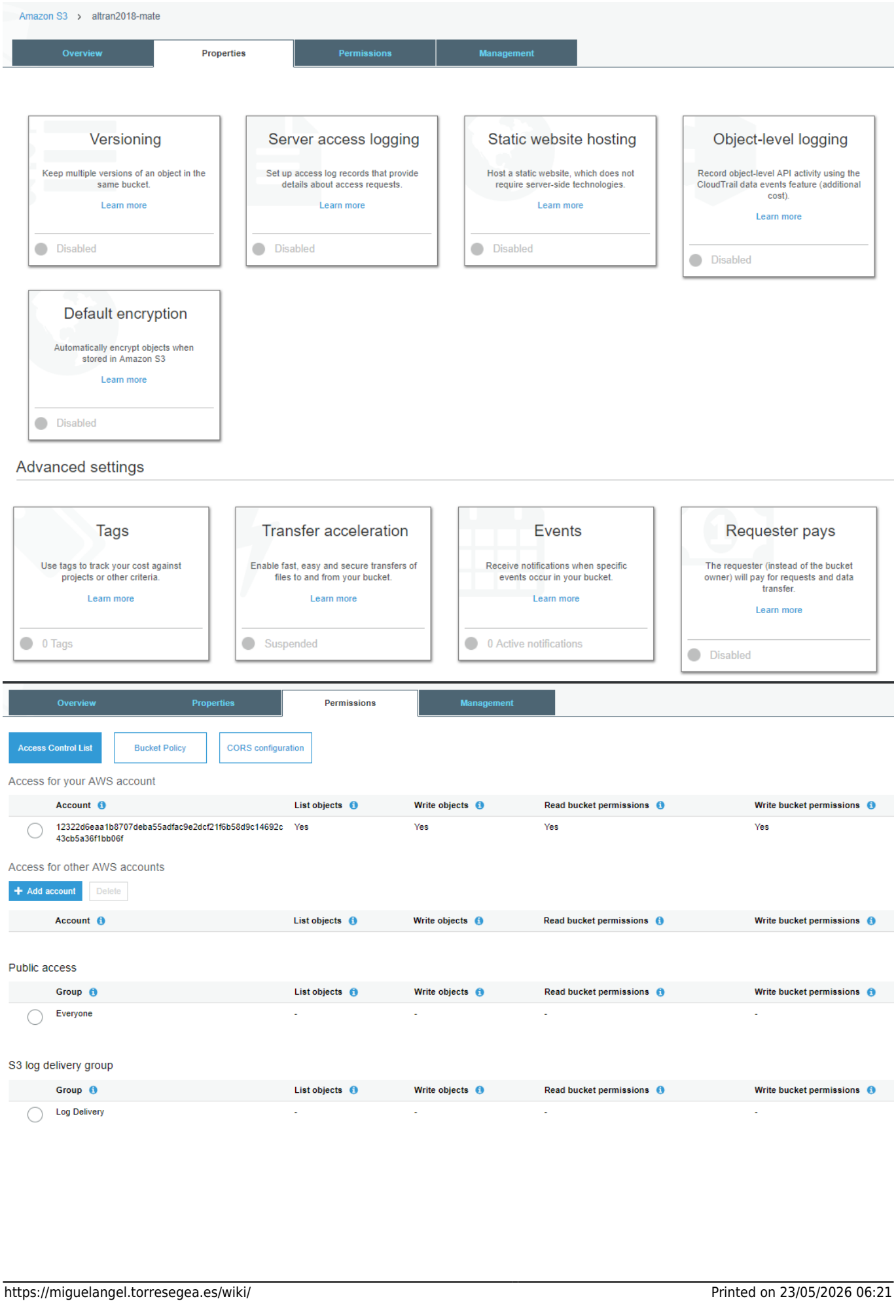


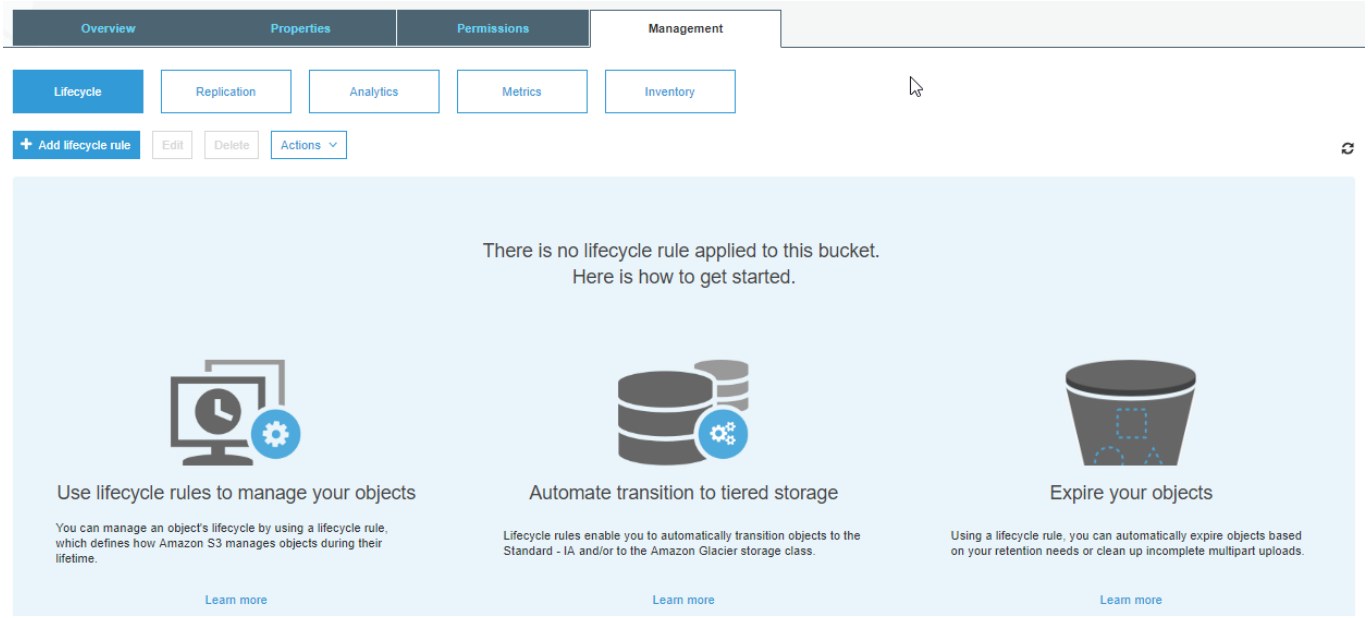
- CloudWatch : métricas, monitorización



- manage system permissions : hay que darle permiso explícito para que **S3 Log Delivery** deje los logs de otros buckets




Amazon S3 › altran2018-mate
Overview
Properties
Permissions
Management
Versioning
Keep multiple versions of an object in the same bucket.
Learn more
Disabled
Server access logging
Set up access log records that provide details about access requests.
Learn more
Disabled
Static website hosting
Host a static website, which does not require server-side technologies.
Learn more
Disabled
Object-level logging
Record object-level API activity using the CloudTrail data events feature (additional cost).
Learn more
Disabled
Default encryption
Automatically encrypt objects when stored in Amazon S3
Learn more
Disabled
Advanced settings
Tags
Use tags to track your cost against projects or other criteria.
Learn more
0 Tags
Transfer acceleration
Enable fast, easy and secure transfers of files to and from your bucket.
Learn more
Suspended
Events
Receive notifications when specific events occur in your bucket.
Learn more
0 Active notifications
Requester pays
The requester (instead of the bucket owner) will pay for requests and data transfer.
Learn more
Disabled
Overview
Properties
Permissions
Management
Access Control List
Bucket Policy
CORS configuration
Access for your AWS account
Account
List objects
Write objects
Read bucket permissions
Write bucket permissions
12322d6eaa1b8707deba55adfac9e2dcf21f6b58d9c14692c43cb5a36f1bb06f
Yes
Yes
Yes
Yes
Access for other AWS accounts
Add account
Delete
Account
List objects
Write objects
Read bucket permissions
Write bucket permissions
Public access
Group
List objects
Write objects
Read bucket permissions
Write bucket permissions
Everyone
S3 log delivery group
Group
List objects
Write objects
Read bucket permissions
Write bucket permissions
Log Delivery



- diferentes permisos si seleccionas el bucket o un archivo
- las carpetas que se crean no son al uso, son «virtuales»

CloudFront (CDN)

- distribuir contenido con latencia baja y gran velocidad de transferencia
- edge locations ≡ CDN servers
    - no tiene nada que ver con las AZ o regiones
    - existen las **Regional Edge Caches**
- ficheros, media streaming
- los **orígenes** pueden ser:
    - S3 Bucket
    - EC2 instance
    - Elastic Load Balancer
    - Route 53
    - Media Package : sirve el contenido adecuado para el dispositivo
    - AWS Elemental MediaStore : ayuda a optimizar la descarga
- la **distribución**
    - CDN - Edge Locations
    - web distribution → websites
    - RTMP - media streaming
- tanto para servir (cache) como para recoger (red más optimizada)
- TTL = Time To Live
- se pueden invalidar los objetos en caché ($)
    - si quieres cambiar el contenido, usar URLs con cadenas random para que al actualizar la URL y el contenido asociado

Laboratorio

- si restringimos el acceso al bucket, solo se podrá acceder via CloudFront, no vía http/bucket
- (!) para hace restricción sobre la URL del CloudFront generado, podemos usar:
    - Signed URLs
    - Signed Cookies

Storage Gateway

File Gateway

- S3
- NFS / SMB

Volume Gateway

- volúmenes iSCSI
  - cached volumes : almacenamiento principal en Amazon, cacheado en el server
    - 1GB - 32TB
  - stored volumes : almacenamiento principal en mi datacenter, cacheado / replicado en Amazon

Tape Gateway

- almacena en Glacier
- estructura virtual de cintas de backup

Snowball

- import / export data to S3
- dispositivo físico para mover gran cantidad de información
- 3 tipos:
  - snowball : 80TB
  - snowball edge:..
  - ...

1)
Content Delivery Network