



MTIG

MAGÍSTER EN TECNOLOGÍAS
DE INFORMACIÓN Y GESTIÓN

INF3591

Cloud Computing

Clase 3

Almacenamiento de datos

Cristian Daniel Ruz - cruz@ing.puc.cl

Germán Leandro Contreras Sagredo - glcontreras@uc.cl

Planificación

Se actualizó el calendario

Fecha	Temario	Evaluación
Jueves 24 de marzo	Clase 1. Introducción; Conceptos básicos de Cloud Computing.	-
Jueves 31 de marzo	Clase 2. Casos de uso, seguridad, <i>billing</i> .	-
Jueves 7 de abril	Clase 3. Almacenamiento de datos en la nube.	-
Miércoles 13 de abril	Clase 4. Bases de datos en la nube.	Taller evaluado 1
Jueves 21 de abril	Clase 5. Repaso con casos reales.	Control 1
Jueves 28 de abril	Clase 6. Cloud Computing con servidor.	Taller evaluado 2
Jueves 5 de mayo	Clase 7. Cloud Computing sin servidor.	Taller evaluado 3
Jueves 12 de mayo	Clase 8. Virtualización.	Taller evaluado 4
Jueves 19 de mayo	Clase 9. Repaso con casos reales.	Control 2

Almacenamiento de objetos en AWS - S3

S3 (*Simple Storage Service*) consiste en el servicio de almacenamiento de **objetos** ofrecido por Amazon Web Services.

Es **seguro**: además de poder configurar los permisos de acceso, podemos habilitar el **control de versiones** para mantener respaldo de nuestros archivos.

Es **rentable**: S3 nos ofrece distintos tipos de almacenamiento, permitiendo ajustarnos a nuestro presupuesto.

Almacenamiento de objetos en AWS - S3

También es importante hacer mención de **S3 Glacier**.

S3 Glacier nace a partir de AWS Glacier, servicio previo de la nube de Amazon enfocado en el almacenamiento de archivos y copia de seguridad.

A diferencia de S3, S3 Glacier cuenta con costos de almacenamiento **mucho más bajos**: 0,023 USD por GB en S3 vs. 0,004 USD por GB en S3 Glacier.

Almacenamiento de objetos en AWS - S3

¿Cuándo usar S3 y cuándo usar S3 Glacier? Algunos puntos a considerar:

- **Tamaño de archivo máximo:** 5 TB en S3, 40 TB en S3 Glacier.
- **Extracción:** S3 Glacier tiene un **costo adicional** por GB de extracción de datos; S3 no.
- **Acceso a los datos:** Los accesos a objetos de S3 suelen estar en el rango de milisegundos y minutos... en S3 Glacier pueden ser horas.
- **Control de versiones:** Solo disponible en S3.
- **Página web estática:** Solo disponible en S3.

Almacenamiento de objetos en AWS - S3

Entonces... con ¿cuál me quedo?



Almacenamiento de objetos en AWS - S3

Algunas ventajas de usar S3 y S3 Glacier en conjunto:

- **Control de versiones:** Versiones más antiguas de un objeto en S3 se pueden transferir a S3 Glacier.
- **Costos:** Si tenemos una empresa con un volumen de datos significativamente alto, dejar los archivos menos accedidos en S3 Glacier nos puede ayudar a reducir costos.

También existen más tipos de almacenamiento de niveles intermedios.

Almacenamiento de objetos en AWS - S3

Para efectos de este curso, veremos S3 Estándar. Algunos precios...

Capa gratuita de AWS

Como parte de la [capa gratuita de AWS](#), puede comenzar a utilizar Amazon S3 sin cargo. Cuando se registran, los clientes de AWS nuevos reciben 5 GB de almacenamiento de Amazon S3 en la clase de almacenamiento S3 Estándar, 20 000 solicitudes GET, 2000 solicitudes PUT, COPY, POST o LIST y 15 GB de transferencia de datos de salida al mes durante un año.

El uso de la capa gratuita se calcula mensualmente en todas las regiones de AWS, excepto en la región de AWS GovCloud, y se aplica a su factura de manera automática; no se acumulará el uso mensual no consumido. Se aplican restricciones; consulte las [condiciones de la oferta](#) para obtener más detalles.

Almacenamiento de objetos en AWS - S3

Para efectos de este curso, veremos S3 Estándar. Algunos precios...

Precios de almacenamiento	
S3 Estándar: almacenamiento de propósito general para cualquier clase de datos que se utiliza generalmente para datos a los que se accede con frecuencia	
Primeros 50 TB/mes	0,023 USD por GB
Siguientes 450 TB/mes	0,022 USD por GB
Más de 500 TB/mes	0,021 USD por GB

	Solicitudes PUT, COPY, POST LIST (por 1000 solicitudes)	GET, SELECT y el resto de las solicitudes (por 1000 solicitudes)	Solicitudes de transición de ciclo de vida (por 1000 solicitudes)	Solicitudes de recuperación de datos (por 1000 solicitudes)	Recuperaciones de datos (por GB)
S3 Estándar	0,005 USD	0,0004 USD	n/d	n/d	n/d

Almacenamiento de objetos en AWS - S3

Para efectos de este curso, veremos S3 Estándar. Algunos precios...

Región:	EE.UU. Este (Ohio) ↕
	Precio
Transferencia ENTRANTE de datos a Amazon S3 desde Internet	
Todas las transferencias entrantes de datos	0,00 USD por GB
Transferencia SALIENTE de datos desde Amazon S3 a Internet	
Hasta 1 GB al mes	0,00 USD por GB
Siguientes 9,999 TB/mes	0,09 USD por GB
Siguientes 40 TB/mes	0,085 USD por GB
Siguientes 100 TB/mes	0,07 USD por GB
Superior a 150 TB/mes	0,05 USD por GB

Importante destacar que **pueden** variar según región.

Más información: <https://aws.amazon.com/es/s3/pricing/>

Almacenamiento de objetos en AWS - S3

¿Cómo se utiliza?

Los datos se almacenan en ***buckets***, los que corresponden a contenedores datos.

Podemos tener varios *buckets* en nuestra cuenta, con distintas configuraciones y propósitos.

¡Comencemos creando un *bucket*!

Almacenamiento de objetos en AWS - S3

Buscamos en la consola por el nombre del servicio.

Resultados de búsqueda de "s3"

Servicios (7)

Características (10)





Documentación (397.058)

Artículos de conocimiento (30)

Marketplace (632)

Servicios

[Ver todos los 7 resultados ►](#)

-  **S3**
Almacenamiento escalable en la nube
-  **S3 Glacier**
Almacenamiento de archivos en la nube
-  **Athena**
Consulta de datos en S3 con SQL
-  **AWS Snow Family**
Transporte de datos a gran escala

Almacenamiento de objetos en AWS - S3

Panel principal de S3. Vamos directo a crear un *bucket*.

Amazon S3

Buckets

Puntos de acceso

Puntos de acceso del objeto Lambda

Operaciones por lotes

Analizador de acceso para S3

Configuración de bloqueo de acceso público correspondiente a esta cuenta

Storage Lens

Paneles

Configuración de AWS Organizations

Características destacadas 3

AWS Marketplace para S3

Amazon S3

Instantánea de la cuenta

Storage Lens ofrece visibilidad sobre el uso del almacenamiento y las tendencias de la actividad. [Más información](#)

Ver panel de Storage Lens

Buckets (1) Info

Los buckets son contenedores de datos almacenados en S3. [Más información](#)

Buscar buckets por nombre

Nombre

Región de AWS

Acceso

Fecha de creación

introduccion-herramientas-nube-actividad-1

EE. UU. Este (Norte de Virginia) us-east-1

Bucket y objetos que no son públicos

21 Jul 2021 9:11:14 AM -04

Crear bucket

Almacenamiento de datos

61/79

Almacenamiento de objetos en AWS - S3

Configuración inicial: nombre y **región**.

Amazon S3 > Crear bucket

Crear bucket [Info](#)

Los buckets son contenedores de datos almacenados en S3. [Más información](#)

Configuración general

Nombre del bucket

myawsbucket

El nombre del bucket debe ser único y no debe contener espacios ni letras mayúsculas. [Consulte las reglas para la denominación de los buckets](#)

Región de AWS

EE. UU. Este (Norte de Virginia) us-east-1

Copiar la configuración del bucket existente: *opcional*
Solo se copia la configuración del bucket en los siguientes ajustes.

[Elegir el bucket](#)

Regiones en AWS

- Independientes entre sí.
- Optimización de latencia y costos por ubicación.
- Mayor protección con replicación de datos en distintas regiones.
- Interacción entre recursos de distintas regiones.

Almacenamiento de objetos en AWS - S3

Configuración de acceso al *bucket*.
Se puede otorgar de distintas formas:

- **Access Control Lists:** Recurso XML. Solo para cuentas AWS y grupos predeterminados; solo permisos de lectura/escritura.
- **Access Points:** Puntos de acceso Ideal para *buckets* accedidos por varias aplicaciones. Solo facilita permisos para manipular objetos.

Configuración de bloqueo de acceso público para este bucket

Se concede acceso público a los buckets y objetos a través de listas de control de acceso (ACL), políticas de bucket, políticas de puntos de acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos, active Bloquear todo el acceso público. Esta configuración se aplica exclusivamente a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo el acceso público, pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que las aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a los buckets u objetos, puede personalizar la configuración individual a continuación para adaptarla a sus casos de uso de almacenamiento específicos. [Más información](#)

☐ Bloquear todo el acceso público

Activar esta configuración equivale a activar las cuatro opciones que aparecen a continuación. Cada uno de los siguientes ajustes son independientes entre sí.

☐ Bloquear el acceso público a buckets y objetos concedido a través de nuevas listas de control de acceso (ACL)

S3 bloqueará los permisos de acceso público aplicados a objetos o buckets agregados recientemente, y evitará la creación de nuevas ACL de acceso público para buckets y objetos existentes. Esta configuración no cambia los permisos existentes que permiten acceso público a los recursos de S3 mediante ACL.

☐ Bloquear el acceso público a buckets y objetos concedido a través de cualquier lista de control de acceso (ACL)

S3 ignorará todas las ACL que conceden acceso público a buckets y objetos.

☐ Bloquear el acceso público a buckets y objetos concedido a través de políticas de bucket y puntos de acceso públicas nuevas

S3 bloqueará las nuevas políticas de buckets y puntos de acceso que concedan acceso público a buckets y objetos. Esta configuración no afecta a las políticas ya existentes que permiten acceso público a los recursos de S3.

☐ Bloquear el acceso público y entre cuentas a buckets y objetos concedido a través de cualquier política de bucket y puntos de acceso pública

S3 ignorará el acceso público y entre cuentas en el caso de buckets o puntos de acceso que tengan políticas que concedan acceso público a buckets y objetos.



Desactivar el bloqueo de todo acceso público puede provocar que este bucket y los objetos que contiene se vuelvan públicos

AWS recomienda que active la opción para bloquear todo el acceso público, a menos que se requiera acceso público para casos de uso específicos y verificados, como el alojamiento de sitios web estáticos.

- ☐ Reconozco que la configuración actual puede provocar que este bucket y los objetos que contiene se vuelvan públicos.

Almacenamiento de objetos en AWS - S3

Configuración de acceso al *bucket*.
Se puede otorgar de distintas formas:

- **Etiquetas:** Podemos añadir *tags* a los *buckets* que permitan que puedan ser accedidos por usuarios con etiquetas coincidentes.
- **Políticas/Roles:** Lo más tradicional, entregar políticas o roles a usuarios para que puedan acceder.

Configuración de bloqueo de acceso público para este bucket

Se concede acceso público a los buckets y objetos a través de listas de control de acceso (ACL), políticas de bucket, políticas de puntos de acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos, active Bloquear todo el acceso público. Esta configuración se aplica exclusivamente a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo el acceso público, pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que las aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a los buckets u objetos, puede personalizar la configuración individual a continuación para adaptarla a sus casos de uso de almacenamiento específicos. [Más información](#)

☐ Bloquear todo el acceso público

Activar esta configuración equivale a activar las cuatro opciones que aparecen a continuación. Cada uno de los siguientes ajustes son independientes entre sí.

☐ Bloquear el acceso público a buckets y objetos concedido a través de nuevas listas de control de acceso (ACL)

S3 bloqueará los permisos de acceso público aplicados a objetos o buckets agregados recientemente, y evitará la creación de nuevas ACL de acceso público para buckets y objetos existentes. Esta configuración no cambia los permisos existentes que permiten acceso público a los recursos de S3 mediante ACL.

☐ Bloquear el acceso público a buckets y objetos concedido a través de cualquier lista de control de acceso (ACL)

S3 ignorará todas las ACL que conceden acceso público a buckets y objetos.

☐ Bloquear el acceso público a buckets y objetos concedido a través de políticas de bucket y puntos de acceso públicas nuevas

S3 bloqueará las nuevas políticas de buckets y puntos de acceso que concedan acceso público a buckets y objetos. Esta configuración no afecta a las políticas ya existentes que permiten acceso público a los recursos de S3.

☐ Bloquear el acceso público y entre cuentas a buckets y objetos concedido a través de cualquier política de bucket y puntos de acceso pública

S3 ignorará el acceso público y entre cuentas en el caso de buckets o puntos de acceso que tengan políticas que concedan acceso público a buckets y objetos.



Desactivar el bloqueo de todo acceso público puede provocar que este bucket y los objetos que contiene se vuelvan públicos

AWS recomienda que active la opción para bloquear todo el acceso público, a menos que se requiera acceso público para casos de uso específicos y verificados, como el alojamiento de sitios web estáticos.

- ☐ Reconozco que la configuración actual puede provocar que este bucket y los objetos que contiene se vuelvan públicos.

Almacenamiento de objetos en AWS - S3

Otras configuraciones a considerar:

- **Control de versiones:** Si queremos mantener registro de los cambios sobre los objetos en el *bucket*.
- **Cifrado:** Si queremos que los objetos almacenados sean encriptados por el lado del servidor.

Control de versiones de buckets

El control de versiones es una forma de mantener múltiples variantes de un objeto dentro del mismo bucket. Puede utilizar el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. Con el control de versiones, puede recuperarse con facilidad de las acciones involuntarias de los usuarios y de los errores en las aplicaciones. [Más información](#)

Control de versiones de buckets

☒ Desactivar

☐ Habilitar

Etiquetas (0) - opcional

Para realizar un seguimiento del costo del almacenamiento u otros criterios, etiquete el bucket. [Más información](#)

No hay etiquetas asociadas a este bucket.

Agregar etiqueta

Cifrado predeterminado

Cifre automáticamente los nuevos objetos almacenados en este bucket. [Más información](#)

Cifrado del lado del servidor

☒ Desactivar

☐ Habilitar

Almacenamiento de objetos en AWS - S3

El método sugerido para encriptar nuestros objetos dentro de un *bucket* es el de “clave de *bucket*”, haciendo uso de una llave proveniente de AWS KMS (*Key Management Service*).

Si bien AWS KMS tiene un costo adicional, posee también cuotas de capa gratuita (20.000 solicitudes al mes).

Cifrado predeterminado
Cifre automáticamente los nuevos objetos almacenados en este bucket. [Más información](#)

Cifrado del lado del servidor
☐ Desactivar
☒ Habilitar

Tipo de clave de cifrado
Para cargar un objeto con una clave de cifrado proporcionada por el cliente (SSE-C), utilice la CLI de AWS, el SDK de AWS o la API REST de Amazon S3.
☐ Clave de Amazon S3 (SSE-S3)
Una clave de cifrado que Amazon S3 crea, administra y utiliza por usted. [Más información](#)
☒ Clave de AWS Key Management Service (SSE-KMS)
Una clave de cifrado protegida por AWS Key Management Service (AWS KMS). [Más información](#)

Clave de AWS KMS
☒ Clave administrada por AWS (aws/s3)
arn:aws:kms:us-east-1:319619190679:alias/aws/s3
☐ Elija entre sus claves de AWS KMS
☐ Introducir el ARN de la clave de AWS KMS

Clave de bucket
Reduzca los costos de cifrado disminuyendo las llamadas a AWS KMS para nuevos objetos en este bucket. Para especificar una configuración de la clave del bucket para un objeto, utilice la CLI de AWS, el SDK de AWS o la API de REST de Amazon S3. [Más información](#)
☐ Desactivar
☒ Habilitar

Uso de la clave
El costo de cada solicitud a las API realizada a AWS Key Management Service (una vez excedida la capa gratuita) es:
Región: EE.UU. Este (Norte de Virginia) •

- 0,03 USD por cada 10 000 solicitudes
- 0,03 USD por cada 10 000 solicitudes que involucren claves RSA 2048
- 0,10 USD por cada 10 000 solicitudes de ECC GenerateDataKeyPair
- 0,15 USD por cada 10 000 solicitudes asimétricas excepto RSA 2048
- 0,10 USD por cada 10 000 solicitudes de RSA GenerateDataKeyPair

Almacenamiento de objetos en AWS - S3

¡*Bucket* creado correctamente! ¿Cómo se ve?

Amazon S3 ×

✓ El bucket "ejemplo-clase-2" se creó correctamente
Para cargar archivos y carpetas, o para configurar ajustes adicionales del bucket, elija [Ver detalles](#).

Amazon S3

Ver panel de Storage Lens

Buckets (2) Info

Los buckets son contenedores de datos almacenados en S3. [Más información](#)

Buscar buckets por nombre

	Nombre	Región de AWS	Acceso	Fecha de creación
<input type="radio"/>	ejemplo-clase-2	EE. UU. Este (Norte de Virginia) us-east-1	Bucket y objetos que no son públicos	28 Jul 2021 1:58:53 AM -04
<input type="radio"/>	introduccion-herramientas-nube-actividad-1	EE. UU. Este (Norte de Virginia) us-east-1	Bucket y objetos que no son públicos	21 Jul 2021 9:11:14 AM -04

Almacenamiento de objetos en AWS - S3

¡*Bucket* creado correctamente! ¿Cómo se ve?

The screenshot shows the Amazon S3 console interface for a bucket named 'ejemplo-clase-2'. The breadcrumb navigation at the top indicates the path 'Amazon S3 > ejemplo-clase-2'. Below the bucket name, there are tabs for 'Objetos', 'Propiedades', 'Permisos', 'Métricas', 'Administración', and 'Puntos de acceso', with 'Objetos' being the active tab.

Under the 'Objetos' tab, the heading 'Objetos (0)' is followed by a descriptive paragraph: 'Los objetos son las entidades fundamentales que se almacenan en Amazon S3. Puede utilizar el [inventario de Amazon S3](#) para obtener una lista de todos los objetos de su bucket. Para que otras personas obtengan acceso a sus objetos, tendrá que concederles permisos de forma explícita. [Más información](#)'. Below this text is a row of action buttons: 'Recargar', 'Copiar URI de S3', 'Copiar URL', 'Descargar', 'Abrir', 'Eliminar', 'Acciones', 'Crear carpeta', and 'Cargar'.

Below the buttons is a search bar with the placeholder text 'Buscar objetos por prefijo'. To the right of the search bar are navigation controls showing '< 1 >' and a settings gear icon.

Below the search bar is a table header with columns: 'Nombre', 'Tipo', 'Última modificación', 'Tamaño', and 'Clase de almacenamiento'. The table body is empty, displaying the message 'No hay objetos' and 'No tiene objetos en este bucket.' with a 'Cargar' button below it.

Almacenamiento de objetos en AWS - S3

Si quisiéramos, podríamos configurar las políticas de acceso.

Editar la política del bucket Info

Política de bucket

La política del bucket, escrita en JSON, proporciona acceso a los objetos almacenados en el bucket. Las políticas de bucket no se aplican a los objetos que pertenecen a otras cuentas. [Más información](#)

Ejemplos de políticas

Generador de políticas

ARN del bucket

arn:aws:s3:::ejemplo-clase-2

Política

1

Vista previa del acceso externo

Obtenga una vista previa y valide los resultados de Access Analyzer para obtener acceso externo a su recurso. [Más información](#)

Vista previa del acceso externo a su bucket con Access Analyzer

Access Analyzer analiza su política de bucket junto con los permisos de bucket existentes para obtener una vista previa de los resultados de acceso externo a su bucket. Esto le ayuda a validar el acceso público y entre cuentas a su bucket antes de guardar su política. Elija un analizador y seleccione la vista previa para comenzar.

[Más información sobre Access Analyzer](#)

No hay analizadores

Para obtener una vista previa del acceso externo al bucket, cree un analizador de en la región del bucket

Ir a Access Analyzer

Cancelar

Guardar cambios

amazon

web services

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy

SQS Queue Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect

Allow

Deny

Principal

Use a comma to separate multiple values.

AWS Service

Amazon SQS

All Services (*)

Use multiple statements to add permissions for more than one service.

Actions

-- Select Actions --

All Actions (*)

Amazon Resource Name (ARN)

ARN should follow the following format: `arn:aws:sqs:<region>:<account_ID>:<queue_name>`.
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.

Almacenamiento de datos

69/79

Almacenamiento de objetos en AWS - S3

¿Y si quisiéramos dar acceso público a cualquier tipo de acceso?
¿Basta con desbloquearlo en la configuración?

Bloquear acceso público (configuración del bucket)

Se concede acceso público a buckets y objetos a través de listas de control de acceso (ACL), políticas de bucket, políticas de puntos de acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos de S3, active Bloquear todo acceso público. Esta configuración se aplica en exclusiva a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo acceso público pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que sus aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a sus buckets u objetos, puede personalizar los valores de configuración individuales a continuación para que se ajusten mejor a sus necesidades específicas de almacenamiento.

[Más información](#)

Editar

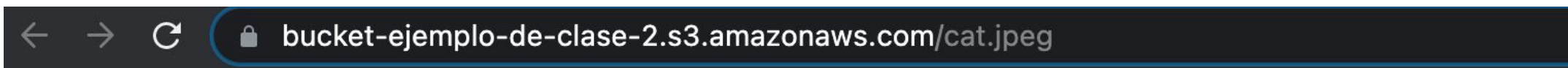
Bloquear todo el acceso público

⚠ Desactivado

- Bloquear el acceso público a buckets y objetos concedido a través de *nuevas* listas de control de acceso (ACL)
⚠ Desactivado
- Bloquear el acceso público a buckets y objetos concedido a través de *cualquier* lista de control de acceso (ACL)
⚠ Desactivado
- Bloquear el acceso público a buckets y objetos concedido a través de políticas de bucket y puntos de acceso públicas *nuevas*
⚠ Desactivado
- Bloquear el acceso público y entre cuentas a buckets y objetos concedido a través de *cualquier* política de bucket y puntos de acceso pública
⚠ Desactivado

Almacenamiento de objetos en AWS - S3

No... debemos hacer algo más: **habilitarlo mediante políticas.**



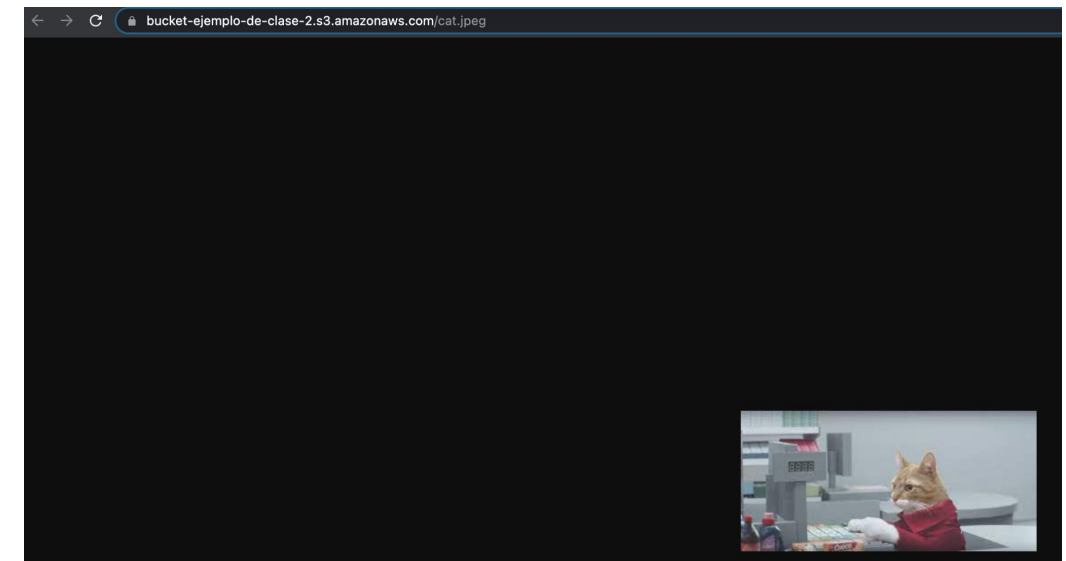
```
▼<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>B9JWYE51HDQHYG2K</RequestId>
  <HostId>t8A78LqI8gPFmv/SbGOCMGofEttOq01Ka9Zq2hlwBxJ0adTNhkjxcqIB364TDLWFdJfMOGum9I4=</HostId>
</Error>
```


Almacenamiento de objetos en AWS - S3

¿Y si quisiéramos dar acceso público a cualquier tipo de acceso?

Política

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": "*",  
7       "Action": "s3:GetObject",  
8       "Resource": "arn:aws:s3:::bucket-ejemplo-de-clase-2/*"  
9     }  
10  ]  
11 }
```



Almacenamiento de objetos en AWS - S3

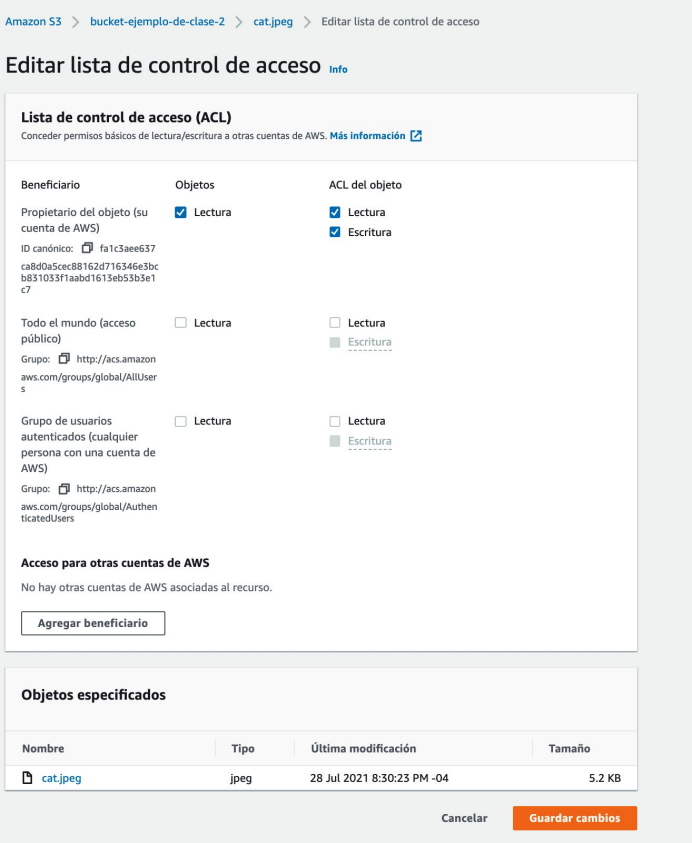
También podemos dar acceso público a **algunos objetos** a través de etiquetas.

Política

```
1  {  
2    "Version": "2012-10-17",  
3    "Statement": [  
4      {  
5        "Effect": "Allow",  
6        "Principal": "*",  
7        "Action": "s3:GetObject",  
8        "Resource": "arn:aws:s3:::bucket-ejemplo-de-clase-2/*",  
9        "Condition": {  
10       "StringEquals": {  
11         "s3:ExistingObjectTag/publico": "si"  
12       }  
13     }  
14   ]  
15 }  
16 }
```

Almacenamiento de objetos en AWS - S3

O simplemente modificarlo a través de la consola con listas de control de acceso.



Recursos útiles

S3 vs. S3 Glacier

<https://luneba.com/blog/amazon-s3-vs-amazon-glacier>

Control de versiones en S3

<https://aws.amazon.com/es/blogs/aws/amazon-s3-lifecycle-management-update/>

S3 Access Points

<https://tutorialsdojo.com/amazon-s3-access-points/>

Recursos útiles

Encriptación en S3

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-key.html>

Sitio web estático en S3

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/HostingWebsiteOnS3Setup.html>

Recursos útiles

Símil de S3 en Google Cloud Platform: Cloud Storage

<https://hackersandslackers.com/manage-files-in-google-cloud-storage-with-python/>

https://www.youtube.com/watch?v=pEbL_TT9cHg

Símil de S3 en Microsoft Azure: Azure Blob Storage

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-quickstart-blobs-python>

<https://www.youtube.com/watch?v=z-trZhXOawg>





MTIG

MAGÍSTER EN TECNOLOGÍAS
DE INFORMACIÓN Y GESTIÓN

INF3591

Cloud Computing

Clase 3

Almacenamiento de datos

Cristian Daniel Ruz - cruz@ing.puc.cl

Germán Leandro Contreras Sagredo - glcontreras@uc.cl