

Este trabajo tiene licencia CC BY-NC-SA 4.0. Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nc-sa/4.0/>

U7P01- Amazon S3. Creación y gestión de buckets-1

1. Descripción

Amazon Simple Storage Service, más conocido como **S3** (<https://aws.amazon.com/es/s3/>) es un servicio de almacenamiento persistente de objetos creado para almacenar y recuperar cualquier cantidad de datos desde cualquier lugar.

Los datos se almacenan por lo tanto como objetos dentro de recursos conocidos como ***buckets***.

En esta práctica se realizarán varias tareas Amazon S3.

- Crear un *bucket* en AWS S3 y analizar sus propiedades y posibles configuraciones.
- Subir archivos (objetos) al *bucket* y analizar sus propiedades y posibles configuraciones.
- Configurar los permisos del *bucket*/objetos para permitir su acceso en diferentes contextos.

2. Formato de entrega

- Realiza la opción que indique el profesor
 - MOSTRAR: muestra en la clase tu configuración al profesor.
 - ENTREGAR: Entrega un documento que incluya capturas de pantalla de los diferentes pasos realizados a lo largo de la práctica.

3. Trabajo a realizar

3.1. Crear un bucket

1. Inicia su entorno **Learner Lab** y accede a la consola de administración de AWS.
2. Accede a la consola de **S3**.
3. Selecciona en el menú lateral la opción **Buckets de uso general** y se presiona el botón de la derecha **Crear bucket**.
4. Configura los siguientes campos:
 - Tipo de bucket: **uso general**
 - Nombre del bucket: Introduce un nombre único: **1dam/1daw-ldvXX** (XX es tu número de prácticas),
 - Propiedad de objetos: **ACL deshabilitadas (recomendado)**.
 - Deja seleccionado **el Bloqueo de acceso público**.
 - Deja **desactivado el control de versiones**.
 - Deja **el tipo de cifrado que esta seleccionado por defecto**

Pincha en **Crear Bucket**. El **bucket** se creará en la región en la que estamos **us-east-1**.

5. Observa que se ha creado el **bucket** en la región **EE.UU. Este (Norte de Virginia) us-east-1**.

3.2. Propiedades un bucket

1. Pincha sobre el **bucket** y observa sus propiedades. Hay diferentes pestañas a las que puedes ir accediendo.

- **Objects (Objetos)**
 - Muestra los archivos almacenados en el bucket. Ahora está vacío.
 - Se pueden cargar, eliminar, mover y organizar los archivos dentro de carpetas virtuales.
 - Permite realizar búsquedas y aplicar filtros.
- **Metadata (Metadatos)**
 - Permite añadir metadatos a los objetos para poder clasificarlos, hacer búsquedas, etc.
- **Properties (Propiedades)**
 - Contiene configuraciones generales del bucket, como la región, el control de versiones y el almacenamiento inteligente.
 - Aquí se configuran aspectos como la replicación, el cifrado, eventos, notificaciones, etc.
- **Permissions (Permisos)**
 - Permite gestionar los permisos de acceso al bucket y sus objetos.
 - Incluye diferentes opciones para configurar permisos.
 - Controla el acceso público y el acceso mediante usuarios de IAM.
- **Metrics (Métricas)**
 - Muestra estadísticas sobre el uso del bucket, como el tamaño total y la cantidad de objetos.
 - Se pueden habilitar métricas detalladas con **Amazon CloudWatch**.
- **Management (Administración)**
 - Permite gestionar reglas de ciclo de vida para automatizar la transición y eliminación de objetos.
 - Configuración de registros de acceso y almacenamiento inteligente.
- **Access points (Puntos de acceso)**
 - Configuración de puntos de acceso específicos que permitan acceder al bucket y sus objetos a diferentes aplicaciones o usuarios.

- Permite gestionar políticas de acceso independientes del **bucket** principal.

3.3. Subir archivos (objetos) al **bucket**

Vamos a subir varios archivos al bucket que hemos creado.

1. Dentro del **bucket** recién creado accede a la pestaña objetos y haz clic en Cargar.
2. En la sección **Archivos y carpetas**, haz clic en **Agregar archivos** y selecciona un par de archivos (una imagen y un documento) para subirlos al **bucket**.
3. Un poco más abajo consulta la sección **Permisos** y observa que los permisos de los objetos dependen de los permisos globales del **bucket**.
4. En la sección **Clase de almacenamiento** observa que puedes elegir que clase quieres para los objetos que has subido. Vamos a dejar la **clase estándar**.
5. Observa otras configuraciones adicionales.
 - **Cifrado**
 - **Metadatos.**
 - **Sumas de comprobación**
 - **Etiquetas.**
6. Pincha en **Cargar** para subir los archivos.
7. Observa los archivos subidos y pincha en Cerrar (arriba a la derecha) para volver a las propiedades del **bucket**.

3.4. Propiedades un objeto

1. Pincha sobre uno de los archivos subidos.
2. Puedes acceder a las diferentes pestañas para ver las propiedades del objeto.
 - **Properties (Propiedades)**
 - Se pueden consultar sus propiedades generales y modificar algunas de sus configuraciones (clase de almacenamiento, cifrado, metadatos, etiquetas, ...)
 - Aquí puedes consultar diferentes identificadores del objeto.
 - **URI de S3**
 - Es un identificador estándar para referirse al objeto dentro de Amazon S3.
 - Se usa en herramientas de **AWS como la CLI o en scripts para acceder a los objetos.**
 - **Formato: s3://{nombre-del-bucket}/{ruta-del-objeto}.**
 - **Nombre de recurso de Amazon (ARN)**
 - Es el identificador único global del recurso en AWS.
 - Se usa en políticas de IAM, permisos y configuraciones dentro de AWS.
 - **Formato: arn:aws:s3:::{nombre-del-bucket}/{ruta-del-objeto}.**

- **Etiqueta de entidad (ETag)**
 - Es un hash MD5 del contenido del archivo (si no está cifrado).
 - Se usa para verificar la integridad del objeto al subirlo o descargarlo.
 - Si el objeto cambia, el ETag también cambiará.
- **URL del objeto**
 - Es el enlace HTTP público o privado para acceder al archivo.
 - Puede usarse en navegadores, APIs y aplicaciones para descargar el objeto.
 - **Si el bucket no es público, esta URL solo funcionará con los permisos adecuados.**
- **Permissions (Permisos)**
 - Permisos del objeto.
- **Versions (Versiones)**
 - Se podrían ver las diferentes versiones del objeto si estuviera habilitado.

3.5. Accede a un objeto

1. Para acceder a un objeto de forma privada puedes pinchar en:

- **Descargar:** para descargar el archivo correspondiente.
- **Abrir:** crear una **URL prefirmada** que permite acceder al objeto durante un tiempo limitado.

Prueba las dos opciones con los dos objetos que ha subido.

2. Es posible crear una **URL prefirmada** para compartir temporalmente el acceso a un objeto aunque sus el bucket y sus permisos sean privados.

- En el menú superior derecho **Acciones de objetos** y pincha en “**Compartir con una URL prefirmada**”
- Selecciona el tiempo que consideres y pincha en crear.
- Pincha en “**Copiar URL prefirmada**”.
- La puedes abrir en otro navegador o enviársela a un compañero para probar.

3.6. Hacer que los objetos de un bucket sean accesible públicamente

Aunque no es una configuración recomendada vamos a hacer accesible públicamente los objetos que hemos subido.

1. Accede a las propiedades del **bucket** que hemos creado.

2. Accede a la pestaña **Permisos**.

3. Sobre la opción **Bloquear acceso público (configuración del bucket)** pincha en **Editar**.

4. Desmarca la opción “**Bloquear todo el acceso público**” y **Guarda los cambios**.
Observa el aviso de seguridad es escribe **confirmar** para **Confirmar** la configuración.

5. Accede a uno de los archivos subidos.

6. Pincha en la URL del objeto y observa que sale un mensaje de error al acceder.

El error anterior se debe a que, si bien el *bucket* se ha configurado como público, los objetos del bucket no son públicos. Para hacer los objetos del *bucket* públicos existen varias formas; sin embargo, AWS recomienda que se utilicen las políticas de *buckets* de Amazon S3, ya que permiten un control muy detallado sobre los niveles de permisos necesarios para el acceso a los objetos de los *buckets*.

7. Pincha en permisos y observa que aunque el **bucket** es de acceso público el archivo no tiene permisos de lectura para todos el mundo. Hay que crear una política para permitir el acceso.

Las **políticas de bucket** son documentos escritos en un lenguaje de acceso basado en JSON que permiten especificar el nivel de permisos de acceso a un *bucket* de S3. Para poder elaborar la política, necesitamos el **ARN** del **bucket** de S3. El ARN (Amazon Resource Name) de un recurso es un identificador que referencia al recurso globalmente de manera unívoca. Podemos encontrar el **ARN** en la pestaña **Propiedades**.

8. Vuelve a las propiedades del **bucket**. Ve a la sección de **Permisos** dentro del **bucket**.

9. En **Política de bucket** pincha en **Editar** y añade la siguiente política. Reemplaza **<ARN_Bucket>** por el de tu **bucket**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "<ARN_Bucket>/*"
    }
  ]
}
```

Pincha en **Guardar Cambios**.

Una breve explicación sobre la política

- **"Version": "2012-10-17"**
 - Es la versión de la sintaxis de la política.
 - "2012-10-17" es la más reciente y recomendada para políticas de S3.

- **"Statement": [...]**
 - Es una lista de reglas (puede haber varias).
 - En este caso, tenemos una sola regla que otorga permisos públicos.
- **"Effect": "Allow"**
 - Define si la acción está permitida (Allow) o denegada (Deny).
 - Aquí se está permitiendo (Allow) el acceso.
- **"Principal": "*"**
 - "*" significa "cualquiera" → Es decir, todos los usuarios pueden acceder al objeto.
 - Si quisieras limitar el acceso a usuarios específicos de AWS, aquí pondrías su ARN o ID de usuario.
- **"Action": "s3:GetObject"**
 - Especifica la acción que se permite.
 - "s3:GetObject" → Permite leer (descargar) los objetos del bucket.
 - No permite subir, borrar ni modificar archivos, solo lectura.
- **"Resource": "<ARN_Bucket>/*"**
 - Define a qué recursos se aplica esta política.
 - Por ejemplo "arn:aws:s3:::1daw-ldv01/*" significa:
 - "arn:aws:s3:::" → Es el identificador de Amazon S3.
 - "1daw-ldv01" → Es el nombre del bucket.
 - "*" → Se aplica a todos los objetos dentro del bucket.
 - Si quisieras aplicar la política solo a un archivo específico, en lugar de "*" pondrías el nombre del objeto, por ejemplo "arn:aws:s3:::1daw-ldv01/foto.png".

10. Regresa a uno de los archivos del bucket copia su URL de objeto y ábrela en el navegador. Si la configuración es correcta, el archivo será accesible públicamente.

3.7. Vaciar y eliminar el *bucket*

1. **Vacía el *bucket*.** Para ello, desde la consola de Amazon S3, selecciona la opción **Buckets de uso general** del menú lateral, marca el botón de radio del *bucket* y selecciona la opción **Vaciar**. Realiza las acciones indicadas para vaciarlo.

2. **Eliminar el *bucket*.** Una vez que el *bucket* este vacío lo puedes eliminar, selecciona la opción **Buckets de uso general** del menú lateral, marca el botón de radio del *bucket* y selecciona la opción **Eliminar**. Realiza las acciones indicadas para eliminarlo.