¿Qué es Amazon S3?

Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector. Los clientes de todos los tamaños y sectores pueden utilizar Amazon S3 para almacenar y proteger cualquier cantidad de datos para diversos casos de uso, tales como lagos de datos, sitios web, aplicaciones móviles, copia de seguridad y restauración, archivado, aplicaciones empresariales, dispositivos IoT y análisis de big data

# Amazon S3 Overview

Buckets

* Los buckets deben tener un nombre único globalmente (a través de todas las regiones y todas las cuentas)
* Los buckets están definidos a nivel regional
* S3 es un servicio global pero los buckets son creados en una región

Objetos

* Los objetos (files) tiene una llave (key)
* La llave es la ruta completa hacia el archivo:
  + S3://my-bucket/my-file.txt
  + S3://my-bucket/my-folder1/another\_folder/my-file.txt
* El máximo tamaño de un objeto es de 5TB, excedido ese tamaño, se debe hacer una carga Multi-part (dividir el archivo en partes mas pequeñas)
* La metadata de un objeto es una lista de pares key/value – metadata de sistema o de usuario
* Tags (key/value pair) muy útil para seguridad y políticas de lifecycle
* Versión de ID (si el versionado está habilitado)

Amazon S3 Websites

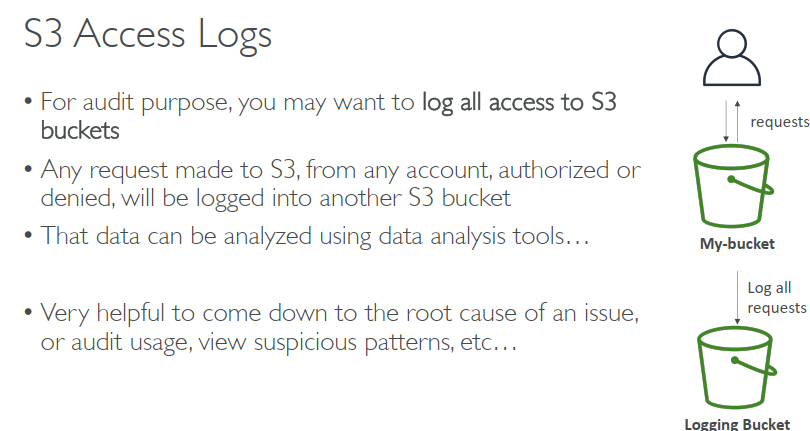
S3 puede hospedar sitios web estáticos y tenerlos accesibles en la WWW

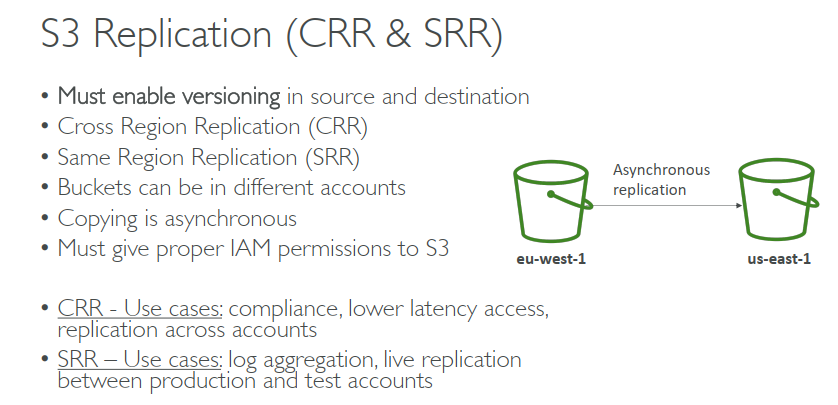
La URL del sitio web sería:

<bucket-name>.s3-website-<AWS-region>.amazonaws.com

<bucket-name>.s3-website.<AWS-region>.amazonaws.com

Amazon S3 – Versioning

* Los archivos de S3 se pueden versionar
* El versionado está habilitado a nivel de bucket
* La sobreescritura en una misma key, provocará un incremento en el versionado: 1,2,3..
* Es una buena práctica versionar los buckets
  + Protege contra eliminaciones no intencionadas
  + Fácil rollback hacia una versión anterior



Clases de almacenamiento

Amazon S3 ofrece varios tipos de almacenamiento diseñados para distintos casos de uso. Por ejemplo, puede almacenar **datos de producción críticos en S3 Standard para obtener acceso frecuente**, ahorrar costos al almacenar **datos a los que se accede con poca frecuencia en S3 Standard-IA o S3 One Zone-IA**, y **archivar datos con los costos más bajos en S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval y S3 Glacier Deep Archive**. Puede almacenar **datos con patrones de acceso cambiantes o desconocidos en S3 Intelligent-Tiering**, que optimiza los costos de almacenamiento moviendo automáticamente los datos entre cuatro niveles de acceso cuando cambian los patrones de acceso**. Funciona con el almacenamiento de objetos en cuatro capas de acceso: dos de acceso de baja latencia optimizadas para el acceso frecuente y poco frecuente y dos de acceso a archivos opcionales diseñados para el acceso asíncrono, las cuales están optimizadas para accesos inusuales.**

Administrar el almacenamiento

Amazon S3 cuenta con funciones de gestión del almacenamiento que puede utilizar para gestionar los costes, cumplir los requisitos normativos, reducir la latencia y guardar varias copias distintas de sus datos para cumplir los requisitos de cumplimiento.

Ciclo de vida de S3: Puede realizar la transición de objetos a otras clases de almacenamiento de S3 o caducar objetos que alcancen el final de su vida útil.

S3 Object Lock: evite que se eliminen o se sobrescriban objetos de Amazon S3 durante un período de tiempo determinado o de manera indefinida. Object Lock se puede utilizar para cumplir con los requisitos normativos que requieren almacenamiento de escritura única y lectura múltiple (WORM) o simplemente para agregar otra capa de protección para evitar cambios y eliminaciones de objetos

Replicación de S3— Replique objetos y sus respectivos metadatos y etiquetas de objeto en uno o más buckets de destino en el mismo o en diferentes Regiones de AWS para reducir la latencia, el cumplimiento normativo, la seguridad y otros casos de uso.

Operaciones por lotes de S3: gestione miles de millones de objetos a escala con una sola solicitud de API de S3 o con unos pocos clics en la consola de Amazon S3. Puede utilizar Operaciones Batch para realizar operaciones como Copy (Copiar), Invocación AWS Lambda Function, y Restauraren millones o miles de millones de objetos.

Administración de accesos

Amazon S3 proporciona funciones para auditar y gestionar el acceso a sus buckets y objetos. **De forma predeterminada, los buckets y los objetos de S3 son privados. Solo tiene acceso a los recursos de S3 que cree.**

Bloqueo del acceso público de S3: bloquea el acceso público a los buckets y objetos de S3. De forma predeterminada, la configuración de Bloquear acceso público se activa en el nivel de cuenta y bucket.

AWS Identity and Access Management (IAM)— Cree usuarios de IAM para su Cuenta de AWS Para administrar el acceso a sus recursos de Amazon S3. Por ejemplo, puede usar IAM con Amazon S3 para controlar el tipo de acceso que tiene un usuario o un grupo de usuarios a partes concretas de un bucket de Amazon S3 que es propiedad de su Cuenta deAWS.

Políticas de buckets: utilice el lenguaje de políticas basado en IAM para configurar permisos basados en recursos para los buckets de S3 y los objetos en ellos.  
  
Puntos de acceso de Amazon S3: configure los puntos de acceso de la red con nombre con políticas de acceso dedicadas para administrar el acceso a los datos a escala para los conjuntos de datos compartidos en Amazon S3

Listas de control de acceso (ACL): se recomienda utilizar políticas basadas en  
recursos de S3 (políticas de bucket y políticas de punto de acceso) o políticas de IAM para el control de acceso en lugar de ACL

S3 Object Ownership: desactive las ACL y tome posesión de todos los objetos del bucket, lo que simplifica la administración del acceso de los datos almacenados en Amazon S3. Como propietario del bucket, tiene automáticamente la propiedad y el control total sobre cada objeto del bucket; además, el control de acceso de los datos se basa en políticas.

Analizador de acceso para S3: evalúe y monitoree sus políticas de acceso a bucket de S3, asegurándose de que las políticas solo proporcionen el acceso previsto a sus recursos de S3.

Procesamiento de datos

Para transformar datos y activar flujos de trabajo para automatizar una variedad de otras actividades de procesamiento a escala, puede utilizar las siguientes características.

S3 Object Lambda: agregue su propio código a las solicitudes GET de Amazon S3 para modificar y procesar los datos a medida que vuelven a una aplicación. Filtra filas, redimensiona dinámicamente las imágenes, redacta datos confidenciales y mucho más.

Notificaciones de eventos: active flujos de trabajo que utilizan Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) y AWS Lambda cuando se realiza un cambio en los recursos de S3.

Cómo funciona Amazon S3

Amazon S3 es un servicio de almacenamiento de objetos que almacena datos como objetos dentro de buckets. Un objeto es un archivo y cualquier metadato que describa ese archivo. Un bucket es un contenedor de objetos.

Para almacenar datos en Amazon S3**, primero debe crear un bucket y especificar un nombre de bucket y Región de AWS**. A continuación, cargue datos a ese bucket como objetos en Amazon S3. Cada objeto tiene una clave (o Nombre de clave), que es el identificador único del objeto dentro del bucket.

* S3 proporciona funciones que puede configurar para **admitir su caso de uso específico.**
* Puede utilizar **S3 Versioning** para mantener varias versiones de un objeto en un bucket y restaurar objetos que se eliminan o sobrescriben accidentalmente.

Buckets

Un bucket es un contenedor para objetos almacenados en Amazon S3. Puede almacenar cualquier cantidad de objetos en un bucket y puede tener hasta 100 buckets en su cuenta.

Cada objeto está almacenado en un bucket. Por ejemplo, si el objeto denominado photos/puppy.jpg se almacena en el bucket DOC-EXAMPLE-BUCKET en la región EE. UU. Oeste (Oregón), es direccionable mediante la URL https://DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com/photos/puppy.jpg.

Cuando crea un bucket, introduzca un nombre de bucket y elija la opción Región de AWS donde residirá el cubo**. Después de crear un bucket, no se puede cambiar su nombre ni su región.**

* **Los nombres de los buckets deben ser únicos en todas las Cuentas de AWS de todas las Regiones de AWS de una partición**. Una partición es una agrupación de regiones. AWS actualmente tiene tres particiones: aws (regiones estándar), aws-cn (regiones de China) y aws-us-gov (AWS GovCloud (US)).
* **Otra Cuenta de AWS de la misma partición no puede utilizar el mismo nombre de bucket hasta que se elimine el bucket**.

Objetos

Los objetos son las entidades fundamentales almacenadas en Amazon S3. **Los objetos se componen de datos de objetos y metadatos.** Los metadatos son conjuntos de pares nombre-​valor que describen el objeto. **Incluyen algunos metadatos predeterminados**, como la fecha de la última modificación y los metadatos HTTP estándar, como Content-Type. También puede especificar metadatos personalizados en el momento en que se almacena el objeto.

**Un objeto se identifica de forma exclusiva dentro de un bucket con una**[**clave (nombre)**](https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/Welcome.html#BasicsKeys)**y un**[**ID de versión**](https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/Welcome.html#BasicsVersionID)**(si el control de versiones de S3 está habilitado en el bucket).**

Claves

Una *clave de objeto* (o *nombre de clave*) es el identificador único de un objeto dentro de un bucket. Cada objeto de un bucket tiene exactamente una clave. **La combinación de un bucket, clave de objeto y, opcionalmente, el ID de versión (si el control de versiones de S3 está habilitado para el bucket) identifica de forma única cada objeto.** Por tanto, puede pensar en Amazon S3 como una asignación de datos básica entre **"bucket + clave + versión"** y el objeto en sí.

Se puede acceder a cada objeto de Amazon S3 de forma exclusiva a través de la combinación de punto de enlace de servicio web, nombre del bucket, clave, y de forma opcional, una versión. Por ejemplo, en la URL https://DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com/photos/puppy.jpg, **DOC-EXAMPLE-BUCKET es el nombre del bucket** **y photos/puppy.jpg es la clave.**

ID de versión.

Si activa el control de versiones de S3 en un bucket**, Amazon S3 genera un ID de versión único para cada objeto agregado al bucket. Los objetos que ya existían en el bucket** en el momento en que habilita el control de versiones **tienen un ID de versión de null**. **Si modifica estos objetos (o cualquier otro) con otras operaciones, como [CopyObject](https://docs.aws.amazon.com/AmazonS3/latest/API/API_CopyObject.html) y [PutObject](https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutObject.html), los objetos nuevos obtienen un ID de versión único.**

Política de bucket

Una política de bucket es una política AWS Identity and Access Management basada en recursos (IAM) que puede utilizar para conceder permisos de acceso al bucket y a los objetos que contiene. Solo el propietario del bucket puede asociar una política a un bucket. Los permisos asociados a un bucket se aplican a todos los objetos del bucket que son propiedad de la cuenta de propietario del bucket. Las políticas de bucket tienen un límite de tamaño de 20 KB.

Puntos de acceso de S3

Los puntos de acceso de Amazon S3 se denominan **endpoints de red con políticas de acceso dedicadas que describen cómo se puede acceder a los datos mediante ese endpoint.** Los puntos de acceso están asociados a los buckets que se pueden utilizar para realizar operaciones con objetos de S3, como **GetObject y PutObject**. Los puntos de acceso simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en Amazon S3.

Cada punto de acceso tiene su propia política de puntos de acceso. También puede configurar los parámetros de [Bloquear acceso público](https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/access-control-block-public-access.html) para cada punto de acceso. **Puede configurar cualquier punto de acceso para que acepte solo las solicitudes procedentes de una nube virtual privada (VPC) c**on el fin de restringir el acceso a los datos de Amazon S3 a una red privada.

Listas de control de acceso (ACL)

**La mayoría de los casos de uso modernos de Amazon S3 ya no requieren el uso de ACL. Le recomendamos desactivar las ACL, excepto en circunstancias inusuales** en las que necesite controlar el acceso de cada objeto de manera individual. Con la propiedad de objetos, puede desactivar las ACL y confiar en políticas para el control de acceso. Al desactivar las ACL, puede mantener fácilmente un bucket con objetos cargados por diferentes Cuentas de AWS.

Regiones

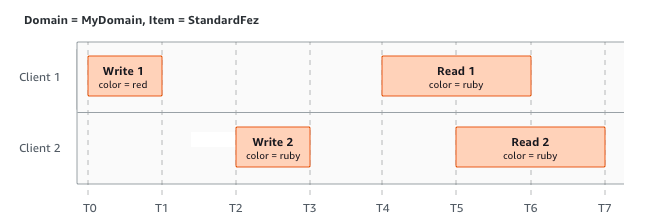
**Puede elegir la Región de AWS geográfica donde Amazon S3 almacenará los buckets que usted cree**. Puede elegir una región para **optimizar la latencia,** **minimizar los costos o cumplir con requisitos legales**. Los objetos almacenados en una Región de AWS nunca abandonan la región, a menos que se transfieran o repliquen expresamente a otra región

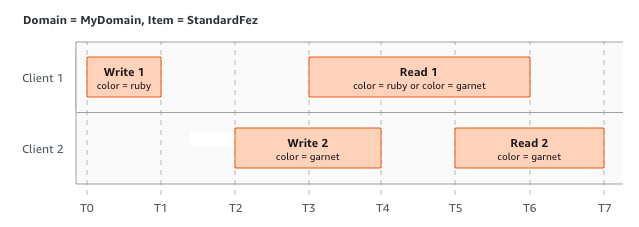
Modelo de consistencia de datos de Amazon S3

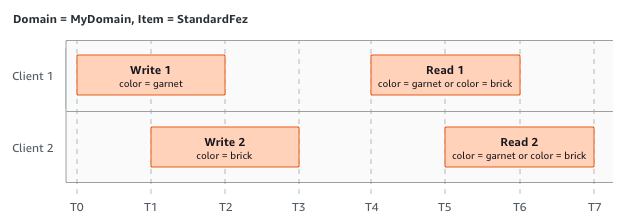
**Amazon S3 proporciona una sólida coherencia de lectura tras escritura para las operaciones PUT y DELETE de objetos del bucket de Amazon S3 en todas las Regiones de AWS**. Esto se aplica tanto a las escrituras en objetos nuevos como a las solicitudes PUT que sobrescriben objetos existentes y las solicitudes DELETE. Además, las operaciones de lectura en Amazon S3 Select, las listas de control de acceso de Amazon S3, las etiquetas de objeto de Amazon S3 y los metadatos de objetos (p. ej., el objeto HEAD) son muy consistentes.

**Amazon S3 consigue una alta disponibilidad mediante la reproducción de los datos de varios servidores ubicados en los centros de datos de AWS**. Si una solicitud PUT se realiza correctamente, sus datos se almacenan de forma segura. Cualquier lectura (solicitud GET o LIST) que se inicie después de recibir una respuesta PUT exitosa devolverá los datos escritos por la solicitud PUT.

Aplicaciones simultáneas







Clases de almacenamiento para objetos a los que se  
obtiene acceso con frecuencia

Para casos de uso sensibles al desempeño (aquellos que necesitan un tiempo de acceso de milisegundos) y datos a los que se obtiene acceso frecuentemente, Amazon S3 proporciona las siguientes clases de almacenamiento:

* **S3 Standard**: la clase de almacenamiento predeterminada. Si no se especifica una clase de almacenamiento al cargar un objeto, Amazon S3 asigna la clase de almacenamiento S3 Standard.
* **Redundancia reducida**: la clase de almacenamiento de redundancia reducida (RRS) se ha diseñado para los datos no críticos y reproducibles que se pueden almacenar con menor redundancia que la clase de almacenamiento S3 Standard.

**Importante**

Recomendamos que no utilice esta clase de almacenamiento. La clase de almacenamiento S3 Standard es más económica.

Clase de almacenamiento para optimizar automáticamente los datos con patrones de acceso cambiantes o desconocidos

**S3 Intelligent-Tiering es una clase de almacenamiento Amazon S3 diseñada para optimizar los costos de almacenamiento mediante el traslado automático de los datos a la capa de acceso más rentable sin que se produzca un impacto en el rendimiento o una sobrecarga operativa.** Es la única clase de almacenamiento en la nube que ofrece un ahorro automático en los costos mediante la migración de datos a nivel de objeto granular entre capas de acceso cuando los patrones de acceso cambian. S3 Intelligent-Tiering es la clase de almacenamiento perfecta cuando desea optimizar los costos de almacenamiento de datos con patrones de acceso desconocidos o cambiantes. S3 Intelligent-Tiering no tiene tarifas de recuperación.

**Por una pequeña tarifa mensual de monitoreo y automatización de objetos,** S3 Intelligent-Tiering monitorea los patrones de acceso y traslada automáticamente los objetos a los que no se ha accedido para reducir los niveles de acceso de costos. S3 Intelligent-Tiering ofrece ahorros automáticos en los costos de almacenamiento en dos niveles de acceso de baja latencia y alto rendimiento.

**S3 Intelligent-Tiering almacena automáticamente objetos en tres capas de acceso: una capa de acceso frecuente**, una capa de **acceso poco frecuente** y una capa **de acceso instantáneo a archivos**.

1. Los objetos cargados en S3 Intelligent-Tiering o migrados allí se almacenan de forma automática en la capa de **acceso frecuente.**
2. S3 Intelligent-Tiering monitorea los patrones de acceso y después traslada a la capa de **acceso poco frecuente** aquellos objetos a los que no se accedió **en 30 días consecutivos.**
3. Con S3 Intelligent-Tiering, cualquier objeto existente al que no se haya accedido **durante 90 días consecutivos** pasará automáticamente a la capa de **acceso instantáneo a archivos**

Clases de almacenamiento para objetos a los que se  
obtiene acceso con poca frecuencia

Las clases de almacenamiento **S3 Standard-IA** y **S3 One Zone-IA** están diseñadas para datos de larga duración y acceso poco frecuente. (IA significa acceso poco frecuente, infrequent access). Los objetos S3 Standard-IA y S3 One Zone-IA **están disponibles para acceder en milisegundos** (de modo similar a la clase de almacenamiento S3 Standard**). Amazon S3 cobra una tarifa de recuperación para estos objetos, por lo que son más adecuados para los datos a los que se obtiene acceso con poca frecuencia.**

Por ejemplo, puede elegir que las clases S3 Standard-IA y S3 One Zone-IA hagan lo siguiente:

* Para almacenar copias de seguridad.
* Para datos más antiguos a los que se obtiene acceso con poca frecuencia, pero que todavía necesitan acceso en milisegundos. Por ejemplo, cuando cargue datos, puede elegir la clase de almacenamiento S3 Standard y utilizar la configuración del ciclo de vida para indicar a Amazon S3 que realice la transición de los objetos a la clase S3 Standard-IA o S3 One Zone-IA.

Estas clases de almacenamiento se diferencian en lo siguiente:

* **S3 Standard-IA**: **Amazon S3 almacena los datos de los objetos de forma redundante en varias zonas de disponibilidad separadas geográficamente** (de forma similar a la clase de almacenamiento S3 Standard). Los objetos S3 Standard-IA resisten a la pérdida de una zona de disponibilidad. Esta clase de almacenamiento **ofrece mayor disponibilidad y resistencia que la clase S3 One Zone-IA.**
* **S3 One Zone-IA**: **Amazon S3 almacena los datos de los objetos en una sola zona de disponibilidad**, lo que resulta más económico que la clase S3 Standard-IA. Sin embargo, los datos no son resistentes a la pérdida física de la zona de disponibilidad como consecuencia de desastres, como terremotos e inundaciones**. La clase de almacenamiento S3 One Zone-IA es tan duradera como la clase Standard-IA, pero tiene menor disponibilidad y resistencia.**

Le recomendamos lo siguiente:

* S3 Standard-IA: utilice esta clase para su copia principal o única de los datos que no se puedan volver a crear.
* S3 One Zone-IA - Acceso poco frecuente: utilice esta clase si puede volver a crear los datos cuando la zona de disponibilidad falla y para las réplicas de objetos cuando configura la replicación entre regiones de S3 (CRR).

¿Qué es Amazon S3 Glacier?

Amazon S3 Glacier es una clase de almacenamiento de Amazon S3 segura, duradera y de bajo costo para archivar los datos y hacer copias de seguridad a largo plazo.

Con S3 Glacier, los **clientes pueden almacenar sus datos por un precio muy económico durante meses, años e incluso décadas**. S3 Glacier permite a los clientes descargar las cargas administrativas de operar y escalar el almacenamiento a AWS, por lo que no tienen que preocuparse por la planificación de la capacidad, el aprovisionamiento de hardware, la replicación de los datos, la detección y reparación de errores de hardware o las laboriosas migraciones de hardware

Almacén

En S3 Glacier, un almacén es un contenedor para guardar archivos. Cuando crea un almacén, debe especificar un nombre y elegir un AWSRegión en la que desea crear el almacén.

Cada recurso de almacén tiene una dirección única. El formato general es:

https://*<region-specific endpoint>*/*<account-id>*/vaults/*<vaultname>*

Por ejemplo, supongamos que crea un almacén (examplevault) en la región EE.UU. Oeste (Oregón). Se puede obtener acceso a este almacén mediante el siguiente URI:

https://glacier.us-west-2.amazonaws.com/111122223333/vaults/examplevault

En el URI,

* glacier.us-west-2.amazonaws.comidentifica la región EE.UU. Oeste (Oregón).
* 111122223333 es la Cuenta de AWS ID que es la propietaria de la cámara.
* vaultshace referencia a la colección de almacenes propiedad de la Cuenta de AWS.
* Example vault identifica un almacén concreto de una colección de almacenes.

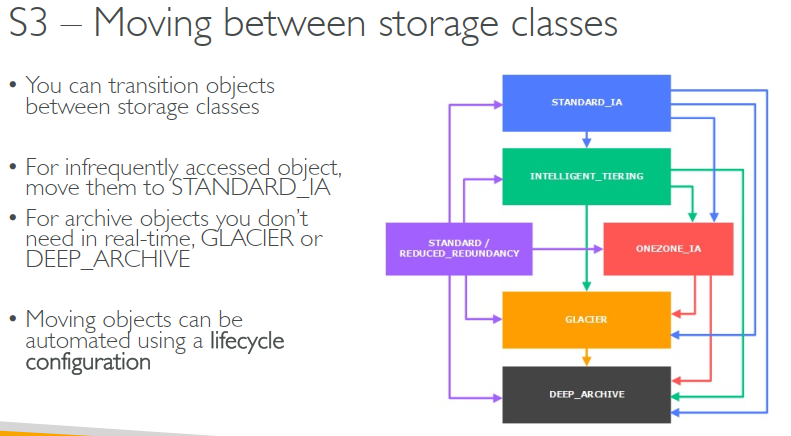
Clases de almacenamiento para el archivado de  
objetos

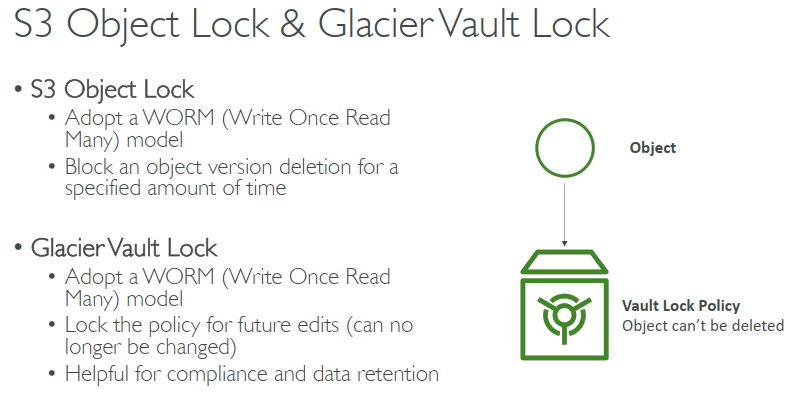
Las clases de almacenamiento **S3 Glacier Instant Retrieval**, **S3 Glacier Flexible Retrieval** y **S3 Glacier Deep Archive** están diseñadas para archivar datos de forma económica. Estas clases de almacenamiento ofrecen la misma durabilidad y resistencia que las clases de almacenamiento S3 Standard y S3 Standard-IA.

Estas clases de almacenamiento se diferencian en lo siguiente:

* **S3 Glacier Instant Retrieval**: se utiliza para archivar **datos a los que se accede con poca frecuencia** **y requieren recuperación en milisegundos**. Los datos almacenados en la clase de almacenamiento **S3 Glacier Instant** **Retrieval ofrecen un ahorro de costos en comparación con la clase de almacenamiento S3 Standard-IA**, **con la misma latencia y rendimiento que la clase de almacenamiento S3 Standard-IA**. **S3 Glacier Instant Retrieval tiene costos de acceso a datos más altos que S3 Standard-IA.**
* **S3 Glacier Flexible Retrieval**: se utiliza para archivos en los que **puede ser necesario recuperar partes de los datos en cuestión de minutos.** Los datos almacenados en la clase S3 Glacier Flexible Retrieval **tienen un periodo mínimo de almacenamiento de 90 días y se puede obtener acceso a ellos en un plazo comprendido entre 1 y 5 minutos mediante la recuperación rápida**. El tiempo de recuperación es flexible y puede solicitar recuperaciones masivas gratuitas en un máximo de 5 a 12 horas. Si ha eliminado, sobrescrito o movido a una clase de almacenamiento diferente un objeto antes del periodo mínimo de 90 días, se le cobrarán los 90 días.
* **S3 Glacier Deep Archive**: se usa para archivar datos a los que se necesita obtener acceso en contadas ocasiones. Los datos almacenados en la clase S3 Glacier Deep Archive tienen **un periodo mínimo de almacenamiento de 180 días y un tiempo predeterminado de recuperación de 12 horas**. Si ha eliminado, sobrescrito o movido a una clase de almacenamiento diferente un objeto antes del periodo mínimo de 180 días, se le cobrarán los 180 días.

S3 Glacier Deep Archive es la opción de almacenamiento más económica de AWS. Los costos de almacenamiento de S3 Glacier Deep Archive son menores que los de la clase de almacenamiento S3 Glacier Flexible Retrieval. **Se pueden reducir los costos de recuperación de S3 Glacier Deep Archive si se utiliza la recuperación en bloque, que devuelve los datos en menos de 48 horas.**

****

****Seguridad en Amazon S3

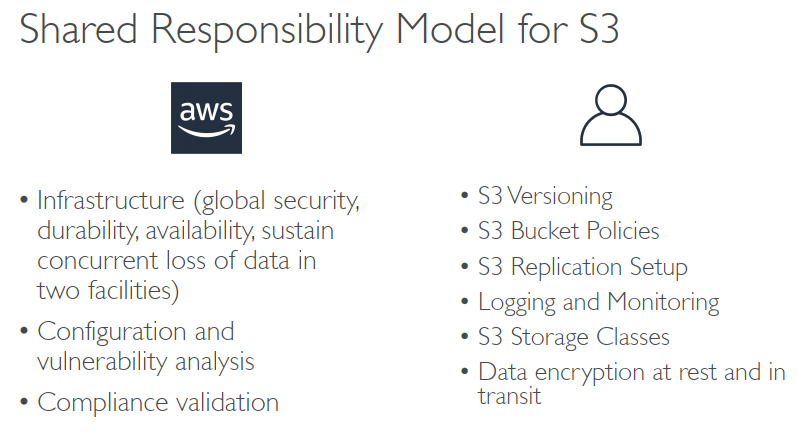
La seguridad es una responsabilidad compartida entre AWS y usted. El [modelo de responsabilidad compartida](http://aws.amazon.com/compliance/shared-responsibility-model/) la describe como seguridad *de* la nube y seguridad *en* la nube:

**Seguridad de la nube**

AWS es responsable de proteger la infraestructura que ejecuta servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura.

**Seguridad en la nube**

Su responsabilidad la determina el servicio de AWS que utilice. Usted también es responsable de otros factores incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables. Para Amazon S3, las siguientes áreas son su responsabilidad:

* Gestión de los datos, incluida la [propiedad del objeto](https://docs.aws.amazon.com/AmazonS3/latest/userguide/about-object-ownership.html) y el [cifrado](https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html).
* Clasificación de sus activos
* [Administración del acceso](https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-access-control.html) a los datos con [roles de IAM](https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html#roles) y otras configuraciones de servicio para aplicar los permisos adecuados.
* Habilitación de controles detectives, como [AWS CloudTrail](https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudtrail-logging.html) o [Amazon GuardDuty](https://docs.aws.amazon.com/guardduty/latest/ug/s3_detection.html) para Amazon S.

