Jonathan A nderson

AWS

Certified Solutions Architect

Associate

The ultimate guide for the

SAA-C03

Imagen que contiene lego, juguete

Descripción generada automáticamenteE X A M

**Event Notifications**

En respuesta a las acciones realizadas en los elementos cargados o almacenados en Amazon S3, se pueden enviar notificaciones de eventos de Amazon S3. En respuesta a los cambios realizados en los objetos almacenados en Amazon S3, las notificaciones de eventos le permiten ejecutar flujos de trabajo, enviar advertencias o realizar otras acciones. Puede utilizar alertas de eventos de Amazon S3 para configurar desencadenadores para que realicen acciones cuando se descarguen, como transcodificar archivos multimedia, procesar archivos de datos cuando estén disponibles y sincronizar objetos relacionados con Amazon S3 con otros almacenes de datos.

Las notificaciones de eventos de Amazon S3 se configuran a nivel de bucket y se pueden configurar a través de la consola de Amazon S3, a través de la API de REST o mediante un SDK de AWS. Amazon S3 puede publicar notificaciones cuando se crean nuevos objetos (mediante una carga PUT, POST, COPY o de varias partes), cuando se eliminan objetos (mediante un DELETE) o cuando Amazon S3 detecta que se ha perdido un objeto RRS. También puede configurar notificaciones de eventos basadas en prefijos y sufijos de nombres de objetos. Los mensajes de notificación se pueden enviar a través de Amazon Simple Notification Service (Amazon SNS) o Amazon Simple Queue Service (Amazon SQS) o directamente a AWS Lambda para invocar funciones de AWS Lambda.

**Best Practices, Models And Performance**

Es común utilizar el almacenamiento de Amazon S3 en aplicaciones y entornos informáticos híbridos. Por ejemplo, los datos de los sistemas de archivos locales, las bases de datos y los archivos de conformidad se pueden respaldar fácilmente a través de Internet en Amazon Glacier o Amazon S3, mientras que la aplicación principal o el almacenamiento de la base de datos permanece en las instalaciones.

Otro modelo común consiste en utilizar Amazon S3 como almacenamiento masivo de "blobs" para datos, mientras que un índice de esos datos se mantiene en otro servicio, como Amazon DynamoDB o Amazon RDS. Esto permite búsquedas rápidas y complejas de nombres de claves sin enumerar constantemente las claves.

Amazon S3 se escala automáticamente para admitir tasas de solicitud muy rápidas, reparticionando automáticamente los buckets según sea necesario. Consulte las directrices de prácticas recomendadas de Amazon S3 en la Guía para desarrolladores si necesita tasas de solicitud superiores a 100 solicitudes por segundo. Además, es mejor mantener un grado de distribución de claves aleatorias, por ejemplo, utilizando un hash como prefijo para los nombres de clave, para admitir tasas de solicitud más altas.

Supongamos que está ejecutando Amazon S3 en un modo intensivo de GET, como el alojamiento de sitios web estáticos, para obtener el mejor rendimiento. En este caso, debe considerar el uso de una distribución de Amazon CloudFront como nivel de almacenamiento en caché para su bucket de Amazon S3.

## Archives

Los datos se guardan en los archivos del glaciar Amazonas. Un archivo puede contener hasta

40 TB de datos, y puede poseer un número infinito de archivos. Tras la creación, a cada archivo se le asigna un ID de archivo único (no puede definir un nombre de archivo descriptivo, a diferencia de una clave de objeto de Amazon S3).

**Vaults**

Los contenedores para bibliotecas se conocen como cofres. Puede haber hasta 1000 almacenes en cada cuenta de AWS. Mediante el uso de políticas de IAM o políticas de acceso al almacén, puede supervisar el acceso a los almacenes y las acciones permitidas.

**Vault Locks**

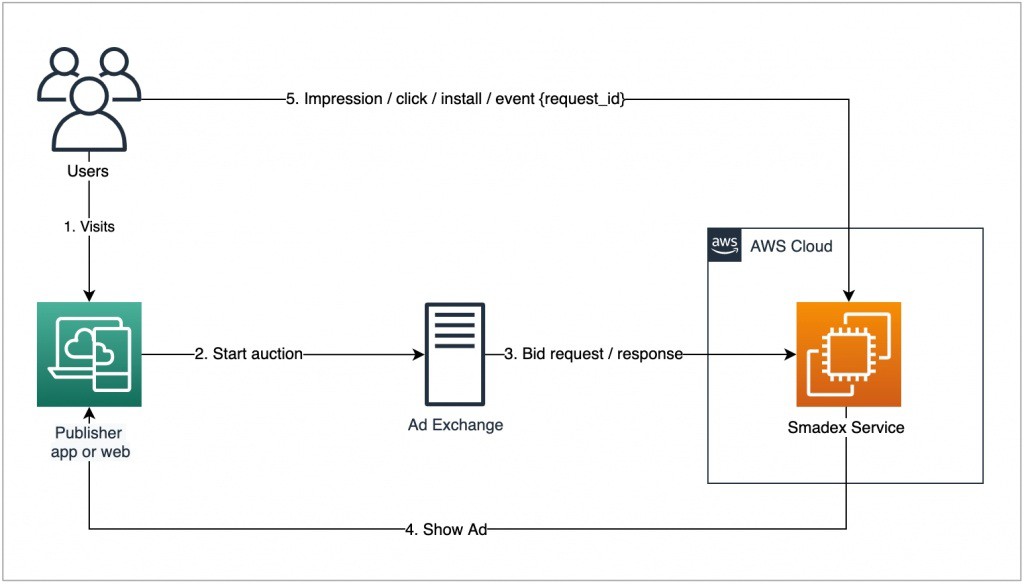
Puede implementar y aplicar fácilmente comprobaciones de conformidad para almacenes individuales de Amazon Glacier con una política de bloqueo de almacén. Puede crear controles de especificación como Escribir una vez leído muchos (WORM) en una directiva de bloqueo del almacén y bloquear dicha directiva contra cambios futuros. Una vez bloqueada, la directiva no se puede cambiar.

**Data Recovery**

Puede obtener hasta el 5 % de sus datos almacenados en Amazon Glacier diariamente de forma gratuita todos los meses. Si recupera más del 5%, tendrá que pagar una tarifa de recuperación basada en su tasa de recuperación máxima. Para eliminar o minimizar estos costos, puede establecer una política de recuperación de datos para un almacén para limitar sus acciones de recuperación a un nivel libre o a una determinada velocidad de datos.

**Amazon Glacier and Amazon Simple Storage Service (Amazon S3)**

Amazon Glacier es similar a Amazon S3, pero difiere en varios aspectos importantes. Amazon Glacier admite archivos de 40 TB frente a objetos de 5 TB en Amazon S3. Los archivos de Amazon Glacier se identifican mediante identificadores de archivo generados por el sistema, aunque Amazon S3 le permite utilizar nombres de clave que son "seguros". Los archivos de Amazon Glacier se cifran automáticamente, mientras que el resto del cifrado es opcional para Amazon S3. Sin embargo, al utilizar Amazon Glacier como una clase de almacenamiento de Amazon S3 con política de ciclo de vida de objetos, puede utilizar la interfaz de Amazon S3 para aprovechar al máximo los beneficios de Amazon Glacier sin aprender nada nuevo. interfaz.



Amazon S3 es el principal servicio de almacenamiento de objetos en AWS y le permite almacenar una cantidad ilimitada de datos con una durabilidad muy alta.

Los casos de uso comunes para Amazon S3 incluyen copia de seguridad y archivado, contenido web, análisis de big data, alojamiento de sitios web estáticos, alojamiento de aplicaciones móviles y nativas de la nube, y recuperación ante desastres.

Otros servicios en la nube de AWS, incluidos AWS IAM, Amazon EBS, AWS KMS, Amazon EC2, Amazon EMR, Amazon DynamoDB, Amazon Redshift, Amazon SQS, AWS Lambda y Amazon CloudFront, están integrados en Amazon S3.

El almacenamiento de objetos difiere del almacenamiento tradicional de bloques y archivos. El almacenamiento en bloque administra los datos a nivel de dispositivo como bloques direccionables, mientras que el almacenamiento de archivos administra los datos a nivel del sistema operativo en forma de archivos y carpetas.

El almacenamiento de objetos maneja los datos como objetos a los que puede acceder una API, que contienen datos y metadatos.

Los buckets de Amazon S3 son contenedores utilizados para almacenar artículos en Amazon S3. A nivel mundial, los nombres de bucket suelen ser únicos. Cada bucket se genera en una región específica y, a menos que el usuario lo copie directamente, los datos no salen de la región.

Las URL prefirmadas permiten un permiso de tiempo limitado para descargar objetos y se pueden usar contra el "raspado de sitios" ilegal para proteger los medios y / u otro contenido web.

La carga de varias partes se utiliza para cargar elementos grandes y partes de un archivo de Amazon S3 o Amazon Glacier se pueden cargar con GET de rango.

Los registros de acceso al servidor se pueden habilitar como bucket para realizar un seguimiento del solicitante, el asunto, la acción y la respuesta.

Cuando se genera o elimina un objeto, las notificaciones de eventos de Amazon S3 se pueden utilizar para enviar un mensaje de Amazon SQS o Amazon SNS o activar una función de AWS Lambda.

En Amazon S3, Amazon Glacier se puede utilizar como un servicio independiente o una clase de almacenamiento.

**Exam Essentials**

1. Comprenda qué es Amazon s3 y para qué se usa comúnmente. Amazon S3 es un almacenamiento en la nube seguro, duradero y altamente escalable que se puede utilizar para almacenar cantidades ilimitadas de datos en casi cualquier formato mediante una interfaz de servicios web simple. Los casos de uso comunes incluyen copia de seguridad y archivado, almacenamiento y distribución de contenido, análisis de big data, alojamiento estático de sitios web, alojamiento en la nube de software nativo y recuperación ante desastres.
2. Comprenda cómo el almacenamiento de objetos varía del almacenamiento de bloques y datos. El almacenamiento de objetos en la nube de Amazon S3 administra los datos a nivel de aplicación como objetos mediante una API de REST basada en HTTP. Block Storage administra datos a nivel de sistema operativo en bloques direccionables numerados mediante protocolos como SCSI o Fiber Channel. El almacenamiento en disco maneja los datos mediante protocolos como CIFS o NFS como archivos compartidos a nivel de sistema operativo.
3. Comprender los conceptos básicos de Amazon S3. Amazon S3 almacena datos en datos y objetos que contienen metadatos. Una clave definida por el usuario identifica objetos y se almacena en una carpeta plana simple llamada compartimento. Las interfaces REST nativas, los SDK multilingües y la AWS CLI y una consola de administración de AWS se incluyen en las interfaces.
4. Saber cómo crear un bucket; cómo cargar, descargar y eliminar objetos; cómo hacer objetos públicos; y cómo abrir la URL de un objeto.
5. Comprenda el modelo de Amazon S3 de durabilidad, disponibilidad y consistencia de los datos. Amazon S3 Standard Storage está diseñado para durar 11 nueve y cuatro nueve objetos en un año. Las otras clases de almacenamiento difieren. Al final, Amazon S3 es estable, pero proporciona nuevos artefactos con compatibilidad de lectura después de escritura para PUTs.
6. Sepa cómo habilitar Amazon S3 para alojar sitios web estáticos. En Amazon S3, debe crear un bucket con el nombre de host del sitio web para crear un sitio web estático, cargar el contenido estático y hacerlo público, permitir el alojamiento estático de sitios web en el bucket y definir objetos de página de índice y error.
7. En Amazon S3, aprenda a proteger sus datos. Cifre los datos con HTTPS sobre la marcha y con SSE o cifrado del lado del cliente en reposo. Habilite las versiones para contener diferentes versiones de un objeto en el bucket.
8. Para protegerse contra la eliminación accidental, permita la eliminación de MFA, utilizando la política de bucket de ACL para Amazon S3 y la política de control de acceso para AWS IAM. Para el acceso de descarga temporal, utilice URL prefirmadas. Para copiar datos automáticamente a otra región, utilice la replicación entre regiones.
9. Familiarícese con el caso de uso de cada una de las clases de almacenamiento para Amazon S3. Los datos que requieren alta confiabilidad, alto rendimiento y acceso de baja latencia se usan comúnmente para fines generales. Standard-IA está disponible para datos de uso poco común, pero cuando se accede a él, exige el mismo rendimiento y disponibilidad. Para obtener datos fácilmente replicables, RRS ofrece una menor durabilidad a un costo menor. Cuando el tiempo de recuperación de tres a cinco horas es adecuado, Amazon Glacier permite almacenar datos de archivo utilizados con poca frecuencia a un costo menor.
10. Sepa cómo usar las leyes de configuración para el ciclo de vida. Puede configurar reglas de ciclo de vida en la consola de administración de AWS o en las API. Las reglas de configuración del ciclo de vida definen acciones para transferir objetos de una clase de almacenamiento a otra a lo largo del tiempo.
11. Conozca cómo utilizar las alertas de eventos de Amazon S3. Las notificaciones de eventos se envían a nivel de bucket y pueden desencadenar un mensaje de Amazon SNS o Amazon SQS o una acción de AWS Lambda en respuesta a la carga de un objeto o borrar.
12. Como operación independiente, usted conoce los conceptos básicos del glaciar Amazonas. Los datos se almacenan en archivos cifrados que pueden ser tan anchos como 40 TB. Por lo general, los archivos contienen archivos TAR o ZIP. Las bóvedas son contenedores de archivos y, para el cumplimiento, las bóvedas pueden estar cerradas.

**Review Questions**

1. You need a low-latency platform where you can store files to be mounted within multiple VPC-based instances. Which of the following AWS services is the best choice?
2. AWS Storage Gateway
3. AWS S3
4. Amazon Elastic File System
5. AWS Elastic Block Store
6. What is the maximum size of S3 object metadata?
7. 2 KB
8. 5 GB
9. 100 MB
10. 5 TB
11. When planning your data operations, it's important to understand the practical limitations you'll encounter. Which of the following will be available only in limited amounts?
    1. PUT requests/month against an S3 bucket
    2. The volume of data available per S3 bucket
    3. Account-wide S3 storage space
    4. The number of S3 buckets within a single account
12. You have a publicly available file called filename, stored in an S3 bucket named bucket name. Which of the following addresses will successfully retrieve the file using a web browser?
    1. https://s3.amazonaws.com/bucketname/filename
    2. https://filename/bucketname.s3.amazonaws.com
    3. s3://bucketname/filename
    4. s3://filename/bucketname
13. If you want the files stored in an S3 bucket to be accessible using a familiar directory hierarchy system, you'll need to specify prefixes and delimiters. What are prefixes and delimiters?
14. A prefix is the name common to the objects you want to group, and a delimiter is the bar character (|).
15. A prefix is the DNS name that precedes the amazonaws.com domain, and a delimiter is the name you want to give your file directory.
16. A prefix is the name common to the objects you want to group, and a delimiter is a forward slash character (/).
17. A prefix is the name common to the file type you want to identify, and a delimiter is a forward slash character (/).
18. You want to encrypt the objects at rest in an S3 bucket using keys provided by

AWS that also allows you to track related events. Which combination of tools would you use?

1. Server-side encryption with AWS KMS-Managed Keys
2. Service-side encryption with Amazon S3-Managed Keys
3. Client-side encryption with AWS KMS-Managed Keys
4. Client-side encryption with Amazon S3-Managed Keys
5. Which of the following operational details are likely to be included in S3- generated logs? (Choose three.)
6. Source bucket name
7. Action requested
8. Current bucket size
9. Response status
10. The S3 data durability guarantees cover which of the following possible threats? (Choose two.)
11. User misconfiguration
12. Account security breach
13. Infrastructural failure
14. Data center security breach
15. Which of these explains the difference in durability between S3's S3 One Zone-IA and Reduced Redundancy classes?
16. One Zone-IA is heavily replicated but only within a single availability zone, while reduced redundancy is only lightly replicated.
17. Reduced redundancy is heavily replicated but only within a single availability zone, while One Zone-IA is only lightly replicated.
18. One Zone-IA is replicated across AWS regions, while reduced redundancy data is restricted to a single region.
19. One Zone-IA data is automatically backed up to Amazon Glacier while reduced redundancy remains within S3.
20. Which of the following is the 12-month availability guarantee for the S3 Standard-IA class?
21. 99.99 per cent
22. 99.9 per cent
23. 99.999999999 per cent
24. 99.5 percent
25. For which of the following data operations would you not worry about eventual consistency?
26. Operations immediately preceding the deletion of an existing object
27. Operations subsequent to updating of an existing object
28. Operations subsequent to the deletion of an existing object
29. Operations subsequent to the creation of a new object
30. What must you do to protect objects in S3 buckets from being accidentally overwritten?
31. Nothing. S3 protects existing files by default.
32. Nothing. S3 saves older versions of your files by default.
33. Enable versioning.
34. Enable file overwrite protection.
35. How can you apply transitions between storage classes for certain objects within an S3 bucket?
36. By specifying particular prefixes when you define your lifecycle rules
37. This isn't possible. Lifecycle rules must apply to all the objects in a bucket.
38. By specifying particular prefixes when you create the bucket
39. By importing a predefined lifecycle rule template
40. Which of the following classes will make the most sense for long-term storage when included within a sequence of lifecycle rules?
41. Glacier
42. Reduced Redundancy
43. S3 One Zone-IA
44. S3 Standard-IA
45. Which of the following are the recommended methods for providing secured and controlled access to your buckets? (Choose two.)
46. S3 access control lists (ACLs)
47. S3 bucket policies
48. IAM policies
49. Security groups

## Answer to Review Questions

* 1. C. S3 can be used to share files, but it doesn't offer low-latency access—and its eventual consistency will not work well with file systems. Storage Gateway is designed to simplify backing up archives to the AWS cloud; it's not meant for sharing files. EBS volumes can only be used for a single instance at a time.
  2. A. Object metadata contains information used by S3 to manage an object's security profile, behaviour, and the manner in which it is exposed to client requests. Storing this information requires very little space—2 KB is normally more than enough.
  3. D. In theory, at least, there's no limit to the data you can upload to a single bucket or to all the buckets in your account or to the number of times you upload (using the PUT command). By default, however, you are allowed only 100 S3

buckets per account.

* 1. A. HTTP (web) requests must address the s3.amazon.aws.com domain along with the bucket and filenames.
  2. C. A The prefix is a name common to objects that you want to group, and it is possible to use a slash character (/) as a delimiter. The bar character) (will be viewed not as a delimiter, but as part of the name.While DNS names can have prefixes, they're not relevant to S3 naming.
  3. A. Client-side encryption addresses encryption before an object reaches the bucket (i.e., before it rests). Only AWS KMS-Managed Keys provide an audit trail.
  4. A, B, D. Since there is no limit to the size of an S3 bucket, there would be little to gain by reporting its current size.
  5. C, D. The S3 guarantee only covers the physical infrastructure owned by AWS.
  6. A. One Zone-IA can be heavily replicated but only within a single availability zone, while reduced redundancy is only lightly replicated.
  7. B. The S3 Standard-IA (Infrequent Access) class is guaranteed to be available 99.9 per cent of the time.
  8. D. S3 can't guarantee instant consistency across their infrastructure for changes made to existing objects, but there aren't such concerns for newly created objects.
  9. C. Object versioning must be manually enabled for each bucket before older versions of objects will be saved.
  10. A. S3 lifecycle rules can incorporate specifying objects by the prefix. There's no such thing as a lifecycle template.
  11. A. Glacier offers the least expensive and most resilient storage within the AWS ecosystem. Reduced Redundancy is not resilient, and same apply to S3 One Zone and S3 Standard.
  12. B, C. ACLs is a legacy feature that isn't as flexible as IAM or S3 bucket policies. Security groups are not used equally with S3 buckets.