S3

Pregunta:

1. **Explica las diferentes opciones de almacenamiento disponibles en AWS y sus casos de uso más comunes. ¿Cuáles son las diferencias clave entre el almacenamiento en bloque, almacenamiento de archivos y almacenamiento de objetos?**

AWS ofrece varias opciones de almacenamiento diseñadas para diferentes necesidades y casos de uso. Las principales categorías de almacenamiento en AWS son almacenamiento en bloque, almacenamiento de archivos y almacenamiento de objetos.

Almacenamiento en Bloque (Amazon Elastic Block Store - EBS)

- **Qué es:** Almacenamiento de datos a nivel de bloque, similar a un disco duro virtual que se puede adjuntar a instancias EC2.
- **Casos de uso:** Ideal para sistemas de archivos de alto rendimiento, bases de datos y aplicaciones que requieren acceso rápido y de baja latencia a los datos.

Almacenamiento de Archivos (Amazon Elastic File System - EFS)

- **Qué es:** Sistema de archivos escalable y elástico que se puede montar en múltiples instancias EC2, permitiendo el acceso concurrente a los datos.
- **Casos de uso:** Perfecto para aplicaciones con alta concurrencia de acceso a archivos, análisis de datos y aplicaciones basadas en microservicios.

Almacenamiento de Objetos (Amazon Simple Storage Service - S3)

- **Qué es:** Almacenamiento de objetos altamente escalables que permite almacenar y recuperar cualquier cantidad de datos desde cualquier lugar de la web.
- **Casos de uso:** Ideal para backups, almacenamiento de grandes volúmenes de datos no estructurados, hosting de sitios web estáticos, y distribución de contenido multimedia.

Diferencias Clave

- **Nivel de Acceso:**
  - **Bloque:** Acceso a nivel de bloque, necesita estar adjunto a una instancia EC2.
  - **Archivos:** Acceso a nivel de archivo, puede ser montado en múltiples instancias EC2 simultáneamente.
  - **Objetos:** Acceso a nivel de objeto, accesible desde cualquier lugar de la web.

- Uso Típico:

- Bloque: Aplicaciones de alto rendimiento, bases de datos.

- Archivos: Aplicaciones que necesitan compartir archivos entre múltiples instancias.

- Objetos: Almacenamiento masivo y no estructurado, backups, y distribución de contenido.

- Escalabilidad:

- Bloque: Escalable, pero dentro de los límites de la instancia EC2 a la que está adjunto.

- Archivos: Automáticamente escalable con el tamaño de los datos almacenados.

- Objetos: Altamente escalable, diseñado para manejar cantidades masivas de datos.

Pregunta:

2. **Describe cómo se gestionan los permisos de acceso en Amazon S3. ¿Qué son las políticas de bucket y las listas de control de acceso (ACL)?**

Políticas de Bucket

Definición

Son un conjunto de reglas escritas en formato JSON que definen qué acciones están permitidas o denegadas para ciertos usuarios o grupos en un bucket específico de S3 y sus objetos. Estas políticas se aplican a nivel de bucket y pueden especificar permisos para todo el bucket o para objetos específicos dentro del bucket.

Características

Las políticas de bucket están escritas en JSON, lo que permite una fácil lectura y modificación de las reglas de acceso. Estas políticas permiten un control granular sobre las acciones que los usuarios pueden realizar, como leer, escribir, eliminar o listar los objetos en el bucket. Además, las políticas de bucket pueden incluir condiciones específicas bajo las cuales se aplican los permisos, como restricciones basadas en la dirección IP del solicitante, el tipo de autenticación utilizada o la hora del día en que se realiza la solicitud. Estas políticas se integran con AWS Identity and Access Management (IAM), permitiendo definir permisos para usuarios y roles de IAM, lo que ofrece una gestión centralizada y segura de los permisos.

Ejemplo:

```
{
  "Version": "2020-10-",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::example-bucket/*"
    }
  ]
}
```

Listas de Control de Acceso (ACL)

Definición

Son un método más básico y tradicional de definir permisos en Amazon S3. Las ACL especifican qué cuentas de AWS (o usuarios específicos) tienen permisos sobre un bucket o un objeto. Las ACL se pueden aplicar tanto a nivel de bucket como de objeto.

Características

Las ACL son más simples y menos flexibles que las políticas de bucket, lo que las hace adecuadas para casos de uso menos complejos. Permiten asignar permisos a grupos predeterminados, como AuthenticatedUsers (usuarios autenticados) y AllUsers (todos los usuarios, incluidos los anónimos). Las ACL ofrecen un conjunto limitado de permisos, como READ, WRITE, READ_ACP, WRITE_ACP, y FULL_CONTROL. Aunque son menos potentes que las políticas de bucket, las ACL siguen siendo útiles para la compatibilidad con sistemas que ya utilizan este método de control de acceso.

Ejemplo:

```
<AccessControlPolicy>
  <Owner>
    <ID>CanonicalUserID</ID>
    <DisplayName>OwnerName</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CanonicalUser">
        <ID>GranteeUserID</ID>
        <DisplayName>GranteeUserName</DisplayName>
      </Grantee>
      <Permission>READ</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```