Solución - Evaluación escrita Nº 1

Pregunta 1. ¿Cómo nos pueden ayudar las herramientas de la nube para abordar problemas relativos a Big Data? Enfóquese en al menos dos ventajas que nos otorgan estas herramientas y describa un caso hipotético en el que se evidencien estas.

R. Existen muchas ventajas. Algunas de ellas son:

- Escalabilidad. Incremento o decremento automático de potencial de recursos según uso.
- Costos. Cobro "*on demand*" (por uso).
- Flexibilidad. Abstracción de infraestructura de servicios y distintas alternativas dentro de cada uno de estos (motores de bases de datos; tipos de almacenamiento; lenguajes de programación; entre otros).
- Confiabilidad. Respaldo de datos y capas de seguridad para el acceso a recursos (VPC, grupos de seguridad).

Caso hipotético: Una empresa paga considerablemente por un servidor *on premise* para el almacenamiento de sus datos. Usan la mitad de este pero les cobran por el servidor completo (el proveedor no tenía una opción intermedia que se ajustara a su necesidad). La empresa decide almacenar sus datos con un servicio de la nube y dan la posibilidad de que el tamaño de almacenamiento aumente si se supera cierto umbral. La empresa ahora paga por la cantidad de datos almacenados y no se preocupa de tener que hacer cambio de servidores ni migraciones.

Cualquier caso hipotético que evidencie dos ventajas de las herramientas de la nube es correcto. No importa si las ventajas descritas no están en el listado, siempre y cuando sean correctas y relacionadas a la nube en sí.

Pregunta 2. ¿En qué se diferencia un usuario IAM de un rol IAM?

R. Los usuarios IAM poseen credenciales de acceso de largo plazo y pueden acceder directamente a los recursos donde posean permisos. Por otra parte, los roles IAM no acceden por sí mismos a los recursos, sino que distintas entidades (usuarios, aplicaciones, entre otras) asumen un rol IAM (lo que genera un *token* de servicios de vencimiento de corto plazo), que otorga permisos de acceso a recursos determinados.

Pregunta 3. Suponga que mientras creaba la llave de acceso de un usuario olvidó almacenarla, por lo que perdió el "secreto" de la llave. ¿Qué implicancia tiene esto? ¿Cómo lo solucionaría?

R. El hecho de perder el secreto de una llave de acceso implica que el usuario no podrá tener acceso a partir de ella, por lo que se vuelve inservible. Lo más apropiado, en este caso, es desactivar la llave y crear una nueva.

Pregunta 4. En una política de IAM existen Statements que entregan ("Allow") o niegan ("Deny") permisos. Suponga que, para un usuario particular, crea una política con dos Statements: una que entrega acceso y otra que niega acceso a un mismo recurso. ¿Qué pasa con el acceso del usuario a este recurso?

R. Los permisos de Statement “Deny” tienen más peso que los Statement de tipo “Allow”, de hecho, todos los usuarios tienen por defecto los accesos negados a todos los recursos. Por lo tanto, en el caso planteado, el usuario no tendrá acceso al recurso.

Pregunta 5. Suponga que una empresa posee diversos proyectos y busca dar de baja los de menor rentabilidad según los costos generados en AWS. ¿Cómo podría esta empresa llevar a cabo esta decisión solo haciendo uso de la información entregada por AWS?

R. La empresa podría crear un presupuesto en AWS según los recursos que utilice cada proyecto (mediante etiquetas o filtros). Luego, la empresa puede ver la rentabilidad de cada proyecto teniendo en cuenta su costo mensual y las ganancias que generan, permitiendo así tomar una decisión informada.

Pregunta 6. Elabore un caso hipotético en el que nos puede servir agregar una etiqueta a recursos de AWS.

R. Un caso hipotético plausible es el de creación de presupuestos según etiqueta. Podemos entregarle ciertas etiquetas a nuestros recursos de forma que su costo sea considerado en presupuestos específicos. Otro caso de uso es el de entrega de permisos según etiqueta, por ejemplo, dando acceso a ciertos recursos si es que el usuario que intenta acceder tiene una etiqueta con el valor deseado.

Pregunta 7. ¿En qué se diferencia S3 de S3 Glacier? Describa al menos dos diferencias y elabore un caso hipotético en el que convenga hacer uso de S3 Glacier.

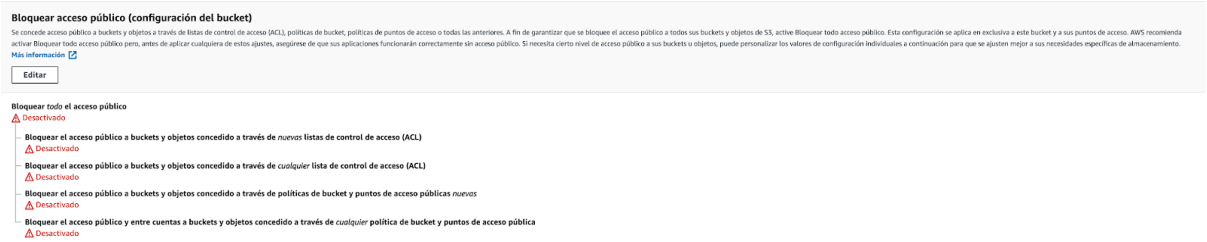
R. Existen varias diferencias. Entre ellas:

- Costo de almacenamiento significativamente menor en S3 Glacier.
- Tamaño de archivo máximo (5TB S3 vs. 40TB S3 Glacier).
- Control de versiones solo en S3.
- Páginas web estáticas solo en S3.
- Extracción de datos con costo adicional en S3 Glacier.
- Tiempo de respuesta promedio considerablemente más bajo en S3 Glacier.

Caso hipotético: Una empresa necesita almacenar gigas de reportes de todos los años, pero mientras más antiguo sea el reporte, menos probable es que se requiera su acceso inmediato. Se puede utilizar S3 Glacier para almacenar los archivos cuyo tiempo de vida promedio en S3 termine (según criterio de la empresa). De esta forma, no se pierden los reportes antiguos y tampoco utilizan espacio de los *buckets* principales de la empresa. La única desventaja es que tomaría tiempo poder acceder a los reportes antiguos, pero es un sacrificio menor considerando que su acceso de por sí será menor y que los costos de almacenamiento disminuirán drásticamente.

Cualquier caso hipotético que aluda a la conveniencia de Glacier por costos de almacenamiento y nula necesidad de acceso rápido o continuo está correcta.

Pregunta 8. Suponga que quiere permitir que los enlaces directos de los archivos dentro de un bucket en S3 sean públicos, es decir, que puedan ser accedidos a través del navegador con el enlace que les corresponde. ¿Basta con la configuración de la imagen? Justifique su respuesta.



R. No, la configuración descrita no basta ya que solo da acceso público al *bucket*, no a los objetos contenidos en este[1]. Existen varias formas de hacerlo: se puede dar acceso a todos los objetos de este mediante una política; se puede entregar acceso a los objetos manualmente a través de la consola; entre otras.

[1] En clases pudimos evidenciar que esto no era suficiente.

Pregunta 9. Suponga que una empresa que cuenta con varias áreas distintas posee la política de la imagen aplicada a todos sus usuarios en AWS para controlar los permisos de recursos en S3. ¿Qué es lo que hace precisamente esta política? Explique lo que hace cada Statement y el resultado final dentro de la empresa.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalTag/area": "desarrollo"
        }
      }
    }
  ]
}
```

R. El primer Statement permite realizar las acciones “s3:ListBucket” (listar *buckets*) y “s3:GetObject” (obtener un objeto dentro de un *bucket*) sobre todos los recursos. Esto implica que se pueden listar todos los *buckets* de S3 y se pueden obtener sus objetos, es decir, existen permisos de lectura para todos los usuarios. Por otra parte, el segundo Statement entrega todos los permisos de S3 sobre todos los recursos, siempre y cuando el usuario que trate de realizar la acción posea una etiqueta de llave “area” y valor “desarrollo”. Esto se traduce entonces en lo siguiente: todos los usuarios de la empresa tienen permiso de lectura sobre los *buckets* de S3, pero las personas del área de desarrollo (identificada según una etiqueta en el usuario) poseen permisos de administración sobre S3.

Pregunta 10. En la segunda actividad del curso, se tenía por objetivo crear distintas políticas y usuarios para poder acceder a distintos buckets en S3 y obtener archivos con algunas cuentas y no con otras, simulando así el control de accesos dentro de una empresa. No obstante lo anterior, hubo una persona que eliminó directamente los buckets, evitando que el resto de sus compañeros pudiera seguir con el desarrollo de la actividad. ¿Cuál fue el error del equipo docente? Desarrolle su respuesta aludiendo a los conceptos estudiados de IAM.

R. En la segunda actividad original del curso, se dio acceso a una llave de acceso que poseía permisos de administrador. Esto implicó que, con los comandos apropiados, cualquier estudiante del curso podía llevar a cabo la eliminación de los *buckets* de la actividad, siempre y cuando eliminara los objetos contenidos en estos con anterioridad.
No es necesario que sepan que el usuario posee permisos de administrador, pero sí deben indicar que tenían los suficientes para llevar a cabo la eliminación. Por otra parte, es importante que se indique que el acceso se entregó a través de una llave de acceso, no de un nombre de usuario y contraseña.