



Universidad Galileo

Carrera: Técnico universitario en desarrollo Full Stack

Curso: Introducción a la nube

Sede: Virtual

Servicio S3 en AWS

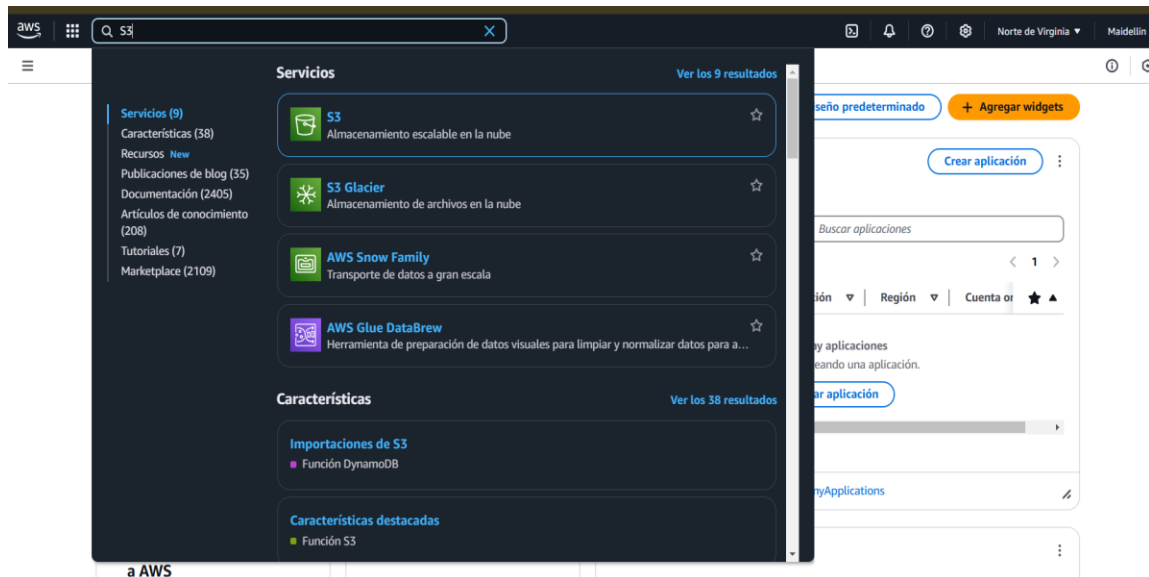
Nombre: Maidellin Suset Alvarado Cayax

Carné: 24011377

Sección: T

Fecha de entrega: 12/08/2024

Configuración de S3:



Voy a la sección de AWS y busco S3 y selecciono crear bucket

Almacenamiento

Amazon S3

Almacene y recupere cualquier cantidad de datos desde cualquier lugar

Amazon S3 es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes en el sector.

Creación de un bucket

Cada objeto en S3 se almacena en un bucket. Para subir archivos y carpetas a S3, tendrá que crear un bucket donde se almacenarán los objetos.

[Crear bucket](#)

Precios

Con S3, no hay cuotas mínimas. Sólo paga por lo que utiliza. Los precios se basan en la ubicación de su bucket de S3.

Realice una estimación de su factura mensual con la [calculadora de costo mensual de AWS](#)

[Ver detalles de precios](#)

Funcionamiento

[Introduction to Amazon S3](#)

[Copiar vínculo](#)

Configuración general

Región de AWS

EE.UU. Este (Norte de Virginia) us-east-1

Tipo de bucket [Información](#)

☒ Uso general

Recomendado para la mayoría de los casos de uso y patrones de acceso. Los buckets de uso general son del tipo de bucket de S3 original. Permiten una combinación de clases de almacenamiento que almacenan objetos de forma redundante en múltiples zonas de disponibilidad.

☐ Directorio

Recomendado para casos de uso de baja latencia. Estos buckets utilizan únicamente la clase de almacenamiento S3 Express One Zone, que proporciona un procesamiento más rápido de los datos dentro de una única zona de disponibilidad.

Nombre del bucket [Información](#)

mibucketSuset_Alvarado

El nombre del bucket debe ser único dentro del espacio de nombres global y seguir las reglas de nomenclatura del bucket. [Consulte las reglas para la asignación de nombres de buckets](#)

Copiar la configuración del bucket existente: *opcional*

Solo se copia la configuración del bucket en los siguientes ajustes.

[Elegir el bucket](#)

Formato: s3://bucket/prefijo

Propiedad de objetos [Información](#)

Controle la propiedad de los objetos escritos en este bucket desde otras cuentas de AWS y el uso de listas de control de acceso (ACL). La propiedad de los objetos determina quién puede especificar el acceso a los objetos.

☒ ACL deshabilitadas (recomendado)

Los objetos de este bucket no tienen propiedad de acceso desde otras cuentas de AWS. El acceso a este bucket...

☐ ACL habilitadas

Los objetos de este bucket tienen propiedad de acceso desde otras cuentas de AWS. El acceso a este bucket...

En este paso cuando creo mi bucket me aseguro de activar la opción bloquear todo el acceso público

✓ Se ha realizado la carga correctamente

Para obtener más información, consulte la tabla [Archivos y carpetas](#).

ⓘ Después de salir de esta página, la siguiente información ya no estará disponible.

Resumen

Destino

s3://mibucketsusetalvarado

Realizado correctamente

✓ 1 archivo, 14.3 KB (100.00%)

Con errores

⊖ 0 archivos, 0 B (0%)

Archivos y carpetas

Configuración

Archivos y carpetas (1 total, 14.3 KB)

🔍

< 1 >

Nombre	Carpeta	Tipo	Tamaño	Estado	Error
bucketTarea.docx	-	application/vnd.openx...	14.3 KB	✓ Realizado correctamente	-

Subir el archivo de texto, selecciona Add files (Agregar archivos). Y lo agregas a tu bucket.

Configuración de Políticas de IAM:

The screenshot displays the AWS IAM console interface. On the left, the navigation menu includes 'Identity and Access Management (IAM)' and a search bar. The main content area is titled 'Panel de IAM' and contains several sections:

- Recomendaciones de seguridad:** A section with two items: 'Agregar MFA para el usuario raíz' (with a warning icon and an 'Agregar MFA' button) and 'El usuario raíz no tiene claves de acceso activas' (with a checkmark icon).
- Recursos de IAM:** A table showing resources for the current account. The table has five columns: Grupos de usuarios, Usuarios, Roles, Políticas, and Proveedores de identidad. The values are 1, 2, 2, 1, and 0 respectively.
- Noticias:** A section with a link to 'Optimize the automation of the workflow of policy administration with reference information'.
- Cuenta de AWS:** A section showing account details: ID de cuenta (180294179475), Alias de cuenta (Crear), and URL de inicio de sesión para los usuarios de IAM de esta cuenta (https://180294179475.signin.aws.amazon.com/console).
- Quick Links:** A section with a link to 'Mis credenciales de seguridad'.
- Herramientas:** A section with a link to 'Simulador de políticas'.

The 'Políticas' link in the left navigation menu is highlighted in yellow.

ahora vamos a crear una nueva política

Identity and Access Management (IAM)

Buscar en IAM

Administración del acceso

Grupos de usuarios

Usuarios

Roles

Políticas

Proveedores de identidad

Configuración de cuenta

Not access management

Visibilidad

Formas de acceso

Access Analyzer

Permisos definidos en esta política Información

Copiar Editar Resumen JSON

Los permisos definidos en este documento de política especifican qué acciones se permiten o deniegan. Para definir permisos para una identidad de IAM (usuario, grupo de usuarios o rol), asíciela a una política

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:GetObject",
8         "s3:ListBucket"
9       ],
10      "Resource": [
11        "arn:aws:s3:::mibucketsusetalvarado",
12        "arn:aws:s3:::mibucketsusetalvarado/*"
13      ]
14    },
15    {
16      "Effect": "Deny",
17      "Action": [
18        "s3:PutObject"
19      ],
20      "Resource": [
21        "arn:aws:s3:::mibucketsusetalvarado/*"
22      ]
23    }
24  ]
25 }
```

En esta caso usamos un código Jason que investigamos donde :

La acción s3:GetObject permite la lectura de objetos (ver archivos).

La acción s3:PutObject está denegada para evitar la carga de archivos en el bucket.

En aws es muy importante la seguridad ósea que si hay un deny este se le dará prioridad a menos que tenga un full Access

IAM > Usuarios > UsuarioLectura > Agregar permisos

Paso 1
● Agregar permisos

Paso 2
○ Revisar

Agregar permisos

Agregue un usuario a un grupo existente o cree uno nuevo. El uso de grupos es una práctica recomendada para administrar los permisos de usuario según las funciones laborales. Más información

Opciones de permisos

☐ Agregar usuario al grupo
Agregue el usuario a un grupo existente o cree uno nuevo. Le recomendamos que utilice grupos para administrar los permisos de usuario según las funciones laborales.

☐ Copiar permisos
Copie todas las suscripciones a grupos, las políticas administradas adjuntas, las políticas insertadas y todos los límites de permisos existentes de un usuario existente.

☒ Adjuntar políticas directamente
Adjunte una política administrada a un usuario de manera directa. Como práctica recomendada, le sugerimos, en cambio, adjuntar políticas a un grupo. A continuación, agregue el usuario al grupo adecuado.

Políticas de permisos (1316)

Buscar

Filtrar por Tipo
Todos los tipos

Nombre de la política	Tipo	Entidades asociadas
accesopersonalizado	Administrada por el cliente	0
AccessAnalyzerServiceRolePolicy	Administrada por AWS	0
Administración de Acceso	Administrada por AWS: función de trabajo	1

Ahora aquí vamos a agregar permisos y luego elegimos adjuntar política directamente y seleccionamos la política que estaremos adjuntando

Identity and Access Management (IAM)

Buscar en IAM

Panel

Administración del acceso

Grupos de usuarios

Usuarios

Roles

Políticas

Proveedores de identidad

Configuración de cuenta

Root access management

Novedad

Informes de acceso

Access Analyzer

Acceso externo

Acceso no utilizado

Configuración del analizador

Usuarios (2) Información

Un usuario de IAM es una identidad con credenciales válidas a largo plazo que se utiliza para interactuar con AWS en una cuenta.

Eliminar Crear usuario

Buscar

	Nombre de usuario	Ruta	Grupo	Última actividad	MFA	Antigüedad de	Último inicio de sesión	ID
<input type="checkbox"/>	UsuarioAdmin	/	0	-	-	4 días	-	-
<input type="checkbox"/>	UsuarioLectura	/	1	-	-	4 días	-	-

ahora iremos a usuarios y ya tenemos creado nuestro usuario lectura, a este usuario le vamos a aplicar la política que hemos creado

Amazon S3

Buckets de uso general

Buckets de directorio

Buckets de tablas Nuevos

Concesiones de acceso

Puntos de acceso

Puntos de acceso del objeto Lambda

Puntos de acceso de varias regiones

Operaciones por lotes

Analizador de acceso de IAM para S3

Configuración de bloqueo de acceso público correspondiente a esta cuenta

Storage Lens

mibucketsusetalvarado Información

Objetos Metadatos Vista previa Propiedades Permisos Métricas Administración Puntos de acceso

Objetos (1) Información

Copiar URI de S3 Copiar URL Descargar Abrir Eliminar Acciones Crear carpeta Cargar

Los objetos son las entidades fundamentales que se almacenan en Amazon S3. Puede utilizar el [inventario de Amazon S3](#) para obtener una lista de todos los objetos de su bucket. Para que otras personas obtengan acceso a sus objetos, tendrá que concederles permisos de forma explícita. [Más información](#)

Buscar objetos por prefijo

	Nombre	Tipo	Última modificación	Tamaño	Clase de almacenamiento
<input type="checkbox"/>	bucketTarea.docx	docx	5 Dec 2024 8:18:02 PM CST	14.3 KB	Estándar

Ahora vamos a verificar los permisos cargando otro archivo a mibucket Suset en el usuario lectura

Arrastre y suelte aquí los archivos y carpetas que desee cargar, o seleccione **Add files** (Agregar archivos) o **Add folder** (Agregar carpeta).

Archivos y carpetas (0)

Eliminar Agregar archivos Agregar carpeta

Se cargarán todos los archivos y las carpetas de esta tabla.

Buscar por nombre

	Nombre	Carpeta	Tipo	Tamaño
No hay archivos ni carpetas				
No ha elegido ningún archivo ni carpeta para cargar.				

Destino Información

Destino

s3://mibucketsusetalvarado

Detalles del destino

Los ajustes del bucket que afectan a los objetos nuevos almacenados en el destino especificado.

Se ha realizado la carga correctamente
Para obtener más información, consulte la tabla Archivos y carpetas.

Después de salir de esta página, la siguiente información ya no estará disponible.

Resumen

Destino

s3://mibucketsusetalvarado

Realizado correctamente

1 archivo, 550.5 KB (100.00%)

Con errores

0 archivos, 0 B (0%)

Archivos y carpetas

Configuración

Archivos y carpetas (1 total, 550.5 KB)

Buscar por nombre

< 1 >

Nombre	Carpeta	Tipo	Tamaño	Estado	Error
scrum_scrums.docx	-	application/vnd.openxml...	550.5 KB	Realizado correctamente...	-

Pero si me dejo cargar el archivo en este caso la política no esta funcionando debemos verificar el código jason que usamos. Pero todo apuntaba a que mi código estaba bien con los permisos requeridos entonces busque ayuda en internet y encontré que:

IAM > Usuarios > UsuarioLectura

Identity and Access Management (IAM)

Buscar en IAM

Panel

Administración del acceso

Grupos de usuarios

Usuarios

Roles

Políticas

Proveedores de identidad

Configuración de cuenta

Root access management

Novedad

Informes de acceso

Access Analyzer

Acceso externo

Creado

December 01, 2024, 12:09 (UTC-06:00)

Último inicio de sesión en la consola

Nunca

Permisos

Grupos (1)

Etiquetas

Credenciales de seguridad

Last Accessed

Políticas de permisos (2)

Eliminar

Agregar permisos

Los permisos se definen mediante políticas asociadas al usuario directamente o a través de grupos.

Buscar

Filtrar por Tipo

Todos los tipos

< 1 >

Nombre de la política	Tipo	Adjuntado a través de
accesopersonalizado	Administrada por el cliente	Directamente
CustomReadOnlyAccess	Administrada por el cliente	Grupo LecturaOnly

Límite de permisos (no establecido)

Mi error fue haber subido el archivo desde mi usuario I am no había iniciado sesión en mi usuario lectura me Sali del usuario e inicie sesión en Usuario lectura

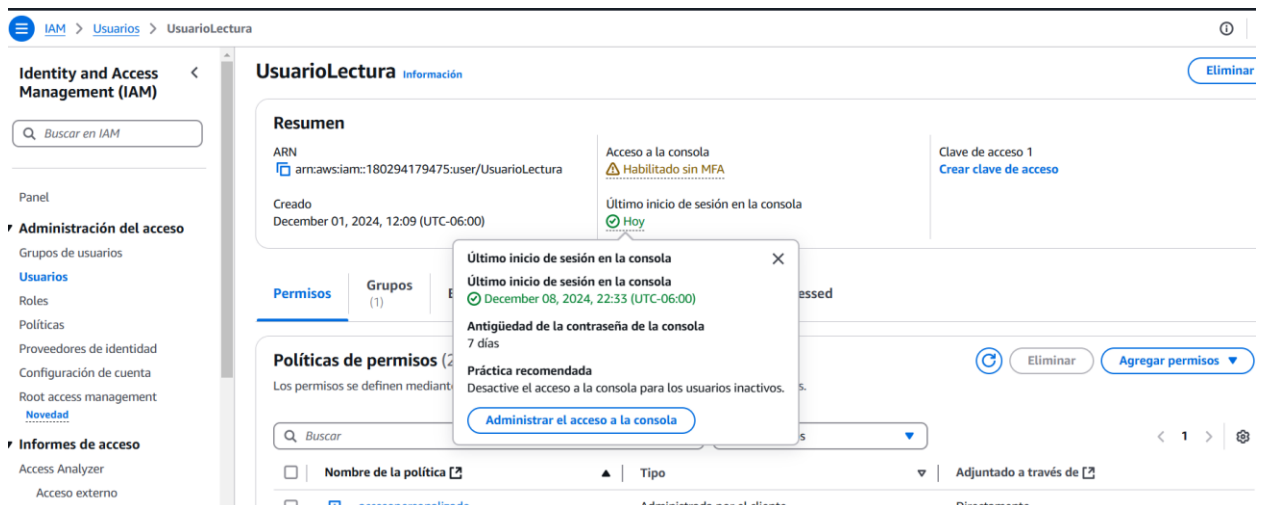
The screenshot shows the AWS IAM console interface. At the top, there is a red error banner that reads: "Error al cargar. Para obtener más información, consulte la columna Error de la tabla Archivos y carpetas." Below this, the "Cargar: estado" section shows a message: "Después de salir de esta página, la siguiente información ya no estará disponible." The "Resumen" section displays the upload status: "Destino: s3://mibucketsusetalvarado", "Realizado correctamente: 0 archivos, 0 B (0%)", and "Con errores: 1 archivo, 208.7 KB (100.00%)". The "Archivos y carpetas" section shows a table with one entry: "SCRUM_EXAMEN.docx" with a status of "Con errores" and a message "Acceso denegado".

Nombre	Carpeta	Tipo	Tamaño	Estado	Error
SCRUM_EXAMEN.docx	-	application/vnd.openxml...	208.7 KB	Con errores	Acceso denegado

Subi un archivo pero me dio error no tengo acceso a subir el archivo en el bucket desde mi usuario Lectura

The screenshot shows the AWS IAM console home page. The "Página de inicio de la Consola" section displays "Visitados recientemente" with links to IAM, S3, and EC2. The "Aplicaciones" section shows a list of applications with a message: "No hay aplicaciones. Comience creando una aplicación." and a "Crear aplicación" button.

y si regreso a mi usuario I am ya puedo subir archivos



Ahora me aparece que se inició sesión en el usuario lectura la ultima vez hoy y antes me aparecía que nunca había iniciado sesión

RESUMEN

No tuve ningún problema en crear el usuario ni el grupo ni siquiera en los permisos entendí el código json que permite a los usuarios listar los objetos del bucket y descargarlos.

Sin embargo, no pueden subir ni modificar objetos dentro del bucket.

El problema fue cuando comprobé subir los archivos al bucket me dejaba pero es que yo lo estaba haciendo desde mi usuario IAM y el propósito de la tarea si entendí bien era subir un archivo desde mi usuario lectura, esto es ideal para trabajar con un grupo este usuarioLectura pertenecida al grupo lecturaonly esto significa que los permisos eran lectura además si hay alguna persona que esta usando otro usuario y pertenece a otro grupo este puede tener otros permisos.

No tuve mayor problema que ese y en entender el código json ya que no es un lenguaje que manejo mucho, pero entendí que los permisos también tienen como prioridad la seguridad entonces si hay un deny solo puede descartarse cuando exista un fullaccess debemos de ver los permisos aplicados a cada usuario para que uno no esta descartado al otro por orden de jerarquía.