

Saturn Studio – Credencial AWS S3



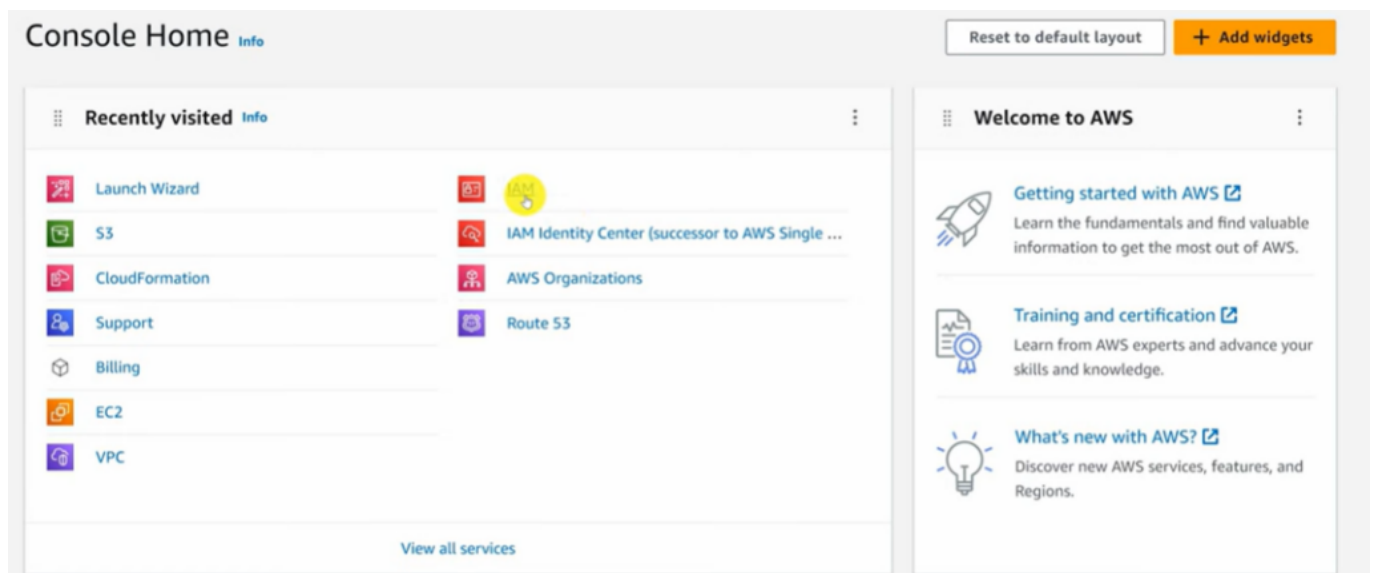
Amazon S3 (Simple Storage Service) es un servicio de almacenamiento en la nube que permite guardar, proteger y recuperar archivos y datos de forma segura y escalable. Su integración en **Saturn Studio** es fundamental para automatizar flujos que requieran el manejo persistente de activos digitales o copias de seguridad.

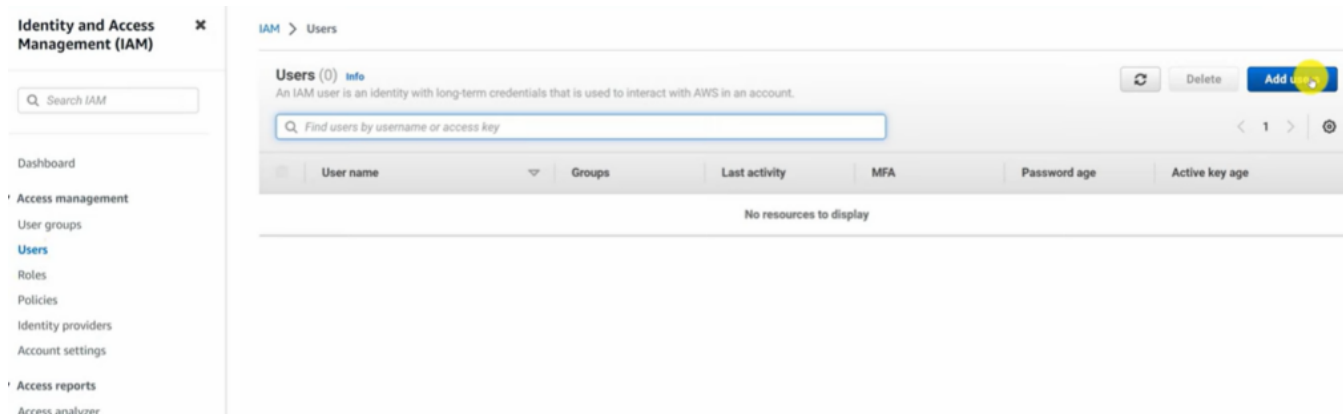
Cómo obtener las llaves de acceso (IAM)

El proceso de obtención de credenciales para S3 es idéntico al de otros servicios de AWS, variando únicamente el permiso específico que se le otorga al usuario.

1. Creación del Usuario en la Consola de AWS

- Inicia sesión en tu Consola de administración de AWS.
- En el buscador superior, selecciona el servicio **IAM**.
- En el menú lateral, dirígete a **Users** (Usuarios) y haz clic en el botón **Add Users**.

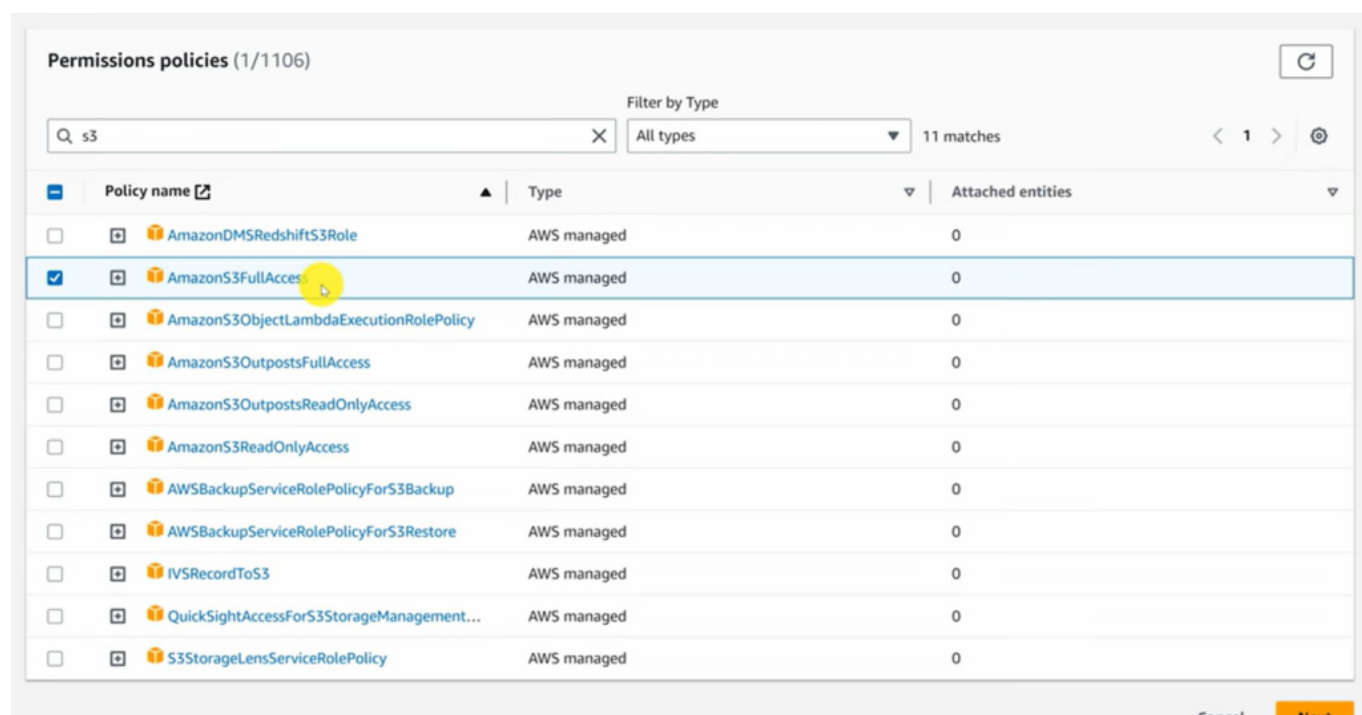




2. Configuración de Permisos

Para que Saturn Studio pueda gestionar tus archivos, el usuario debe tener acceso al servicio de almacenamiento:

- En la pantalla de **Set permissions**, selecciona la opción **Attach policies directly**.
- En el buscador de políticas, escribe **s3** y selecciona la casilla de **AmazonS3FullAccess**.
- Finaliza el proceso de creación del usuario.



3. Generación de las Access Keys

Una vez que el usuario esté creado, accede a su perfil para generar las llaves:

- Haz clic en la pestaña **Security credentials**.
- Desplázate hasta **Access keys** y haz clic en **Create access key**.

- Selecciona el caso de uso **Other** y asigna una descripción opcional (ej. Saturn_S3_Key).
- **IMPORTANTE:** Se mostrarán tu **Access key** y tu **Secret access key**. Debes copiarlas y pegarlas directamente en el módulo, ya que la llave secreta no volverá a mostrarse por seguridad.

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Create access key

No access keys

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

Create access key

IAM > Users > dev-user > Create access key

Step 1

Access key best practices & alternatives

Step 2 - optional

Set description tag

Step 3

Retrieve access keys

Retrieve access keys [info](#)

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key

AKIA3YGORTXJWJ23ZZBW

Secret access key

***** [Show](#)

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [Best practices for managing AWS access keys](#).

Download .csv file

Done

Vinculación en Saturn Studio

Para finalizar la configuración, abre la ventana de credenciales del módulo de **AWS S3** y completa los campos:

1. **Credential name:** Ingresa un nombre para identificar esta conexión.
2. **AWS Region:** Selecciona la región donde se encuentran tus buckets de S3 (ej. us-east-1).
3. **AWS Access Key ID:** Pega el identificador de acceso que copiaste de la consola de AWS.
4. **AWS Secret Access Key:** Pega la llave secreta correspondiente.
5. Haz clic en el botón **Check** para verificar que los permisos de S3 sean válidos.
6. Presiona **Save credentials** para guardar los cambios.