Conceptos básicos de AWS IAM

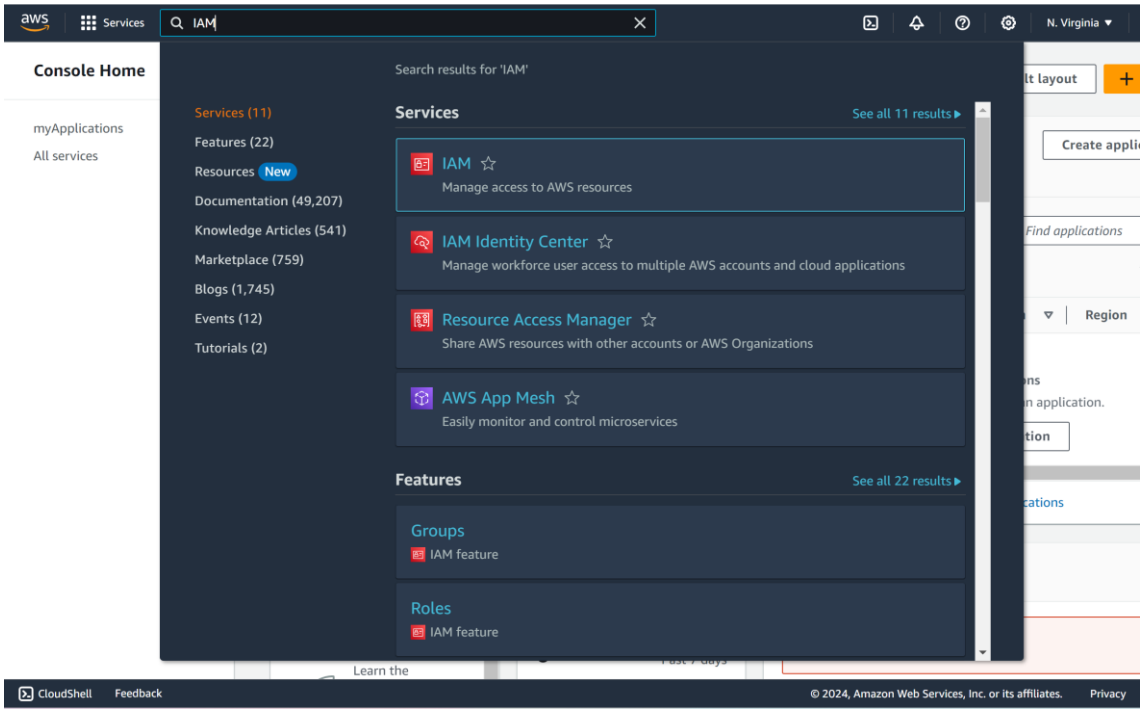
Información:

Este elemento incluye contenido que aún no se tradujo a tu idioma preferido.

Este elemento de lectura se basa en el vídeo anterior y contiene más información específica sobre AWS IAM.

¿Qué es IAM?

AWS IAM es un servicio web que le ayuda a administrar y controlar de forma segura el acceso a sus recursos y servicios de AWS. Con IAM, puede administrar de forma centralizada quién está autenticado en su cuenta y qué permisos de recursos tiene. Con IAM, puede compartir sus recursos sin compartir sus credenciales, y puede seleccionar acciones específicas a las que las personas pueden acceder a un nivel granular. Es un servicio global disponible sin coste adicional, lo que significa que puede ver y utilizar sus configuraciones de IAM desde cualquier región en la consola de administración de AWS.



¿Qué es un usuario IAM?

Cuando se crea una cuenta en AWS, se comienza con la identidad de "usuario raíz", que tiene acceso completo a todos los recursos y servicios de AWS de la cuenta. Se recomienda encarecidamente que no realice operaciones diarias utilizando esta cuenta. En su lugar, cree un usuario administrador para las tareas cotidianas. Tanto si eres el usuario raíz como si eres el usuario administrador, puedes crear otros usuarios en tu cuenta para permitir que otras personas de tu organización accedan a los recursos de AWS.

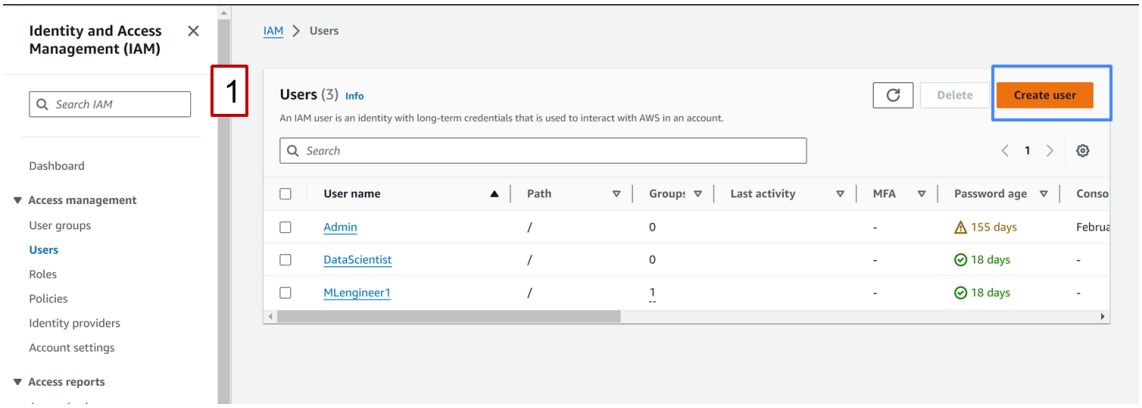
Los usuarios de IAM se crean bajo su cuenta de AWS, por lo que no necesita cuentas separadas para los usuarios de IAM. Cada usuario puede ser una persona o un servicio que interactúa con los recursos de AWS. Cuando crea un usuario, define a qué recursos puede acceder el usuario de IAM y qué acciones puede realizar. AWS generará entonces un conjunto de credenciales para ese usuario. Las credenciales pueden ser un nombre de usuario y una contraseña para

acceder a la consola de administración de AWS, o pueden ser claves de acceso para el acceso programático a los recursos de AWS. Las credenciales de usuario IAM son credenciales a largo plazo, ya que permanecen con el usuario hasta que el administrador las rota. Cuando proporcionas a los usuarios sus propias credenciales de acceso, ayudas a evitar que se compartan las credenciales. Puede añadir más usuarios a su cuenta, y todas las actividades de los usuarios se facturan a su cuenta.

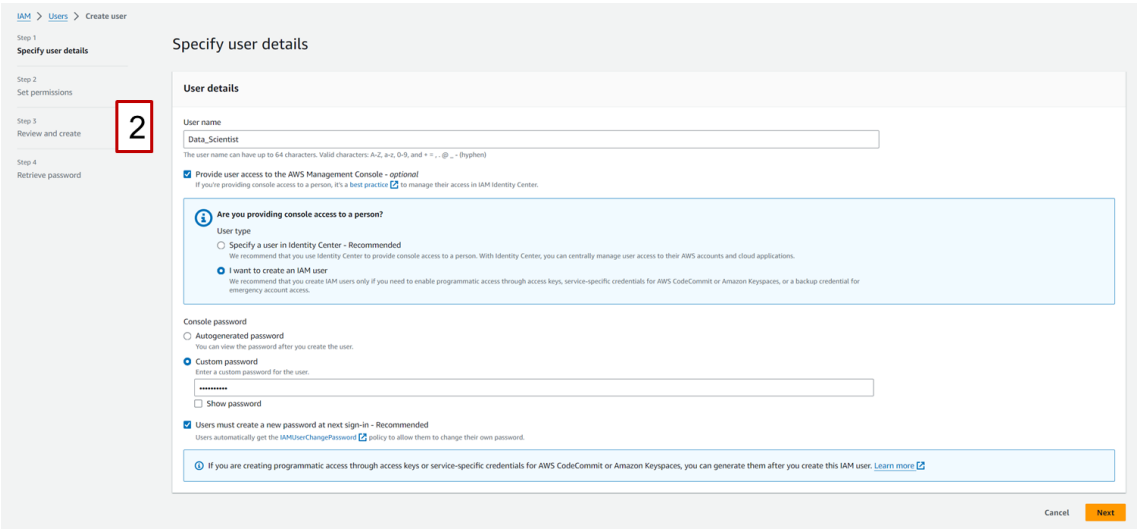
Por defecto, un usuario nuevo no tiene permiso para acceder a ningún recurso de AWS. Puede concederles acceso a los recursos de AWS adjuntándoles políticas. Una política especifica qué acciones están permitidas o denegadas para un recurso determinado (sólo lectura, sólo escritura, acceso total). Una política puede adjuntarse a varios usuarios, y un usuario puede tener varias políticas. Puede elegir políticas gestionadas por AWS o crear sus propias políticas personalizadas. Cada vez que un usuario realiza una solicitud, AWS evalúa sus políticas para determinar si esa solicitud está permitida.

Por ejemplo, supongamos que trabaja con un científico de datos y desea concederle acceso de solo lectura a un bucket de S3 para extraer el conjunto de datos de entrenamiento. Las siguientes figuras muestran los pasos para crear este usuario.

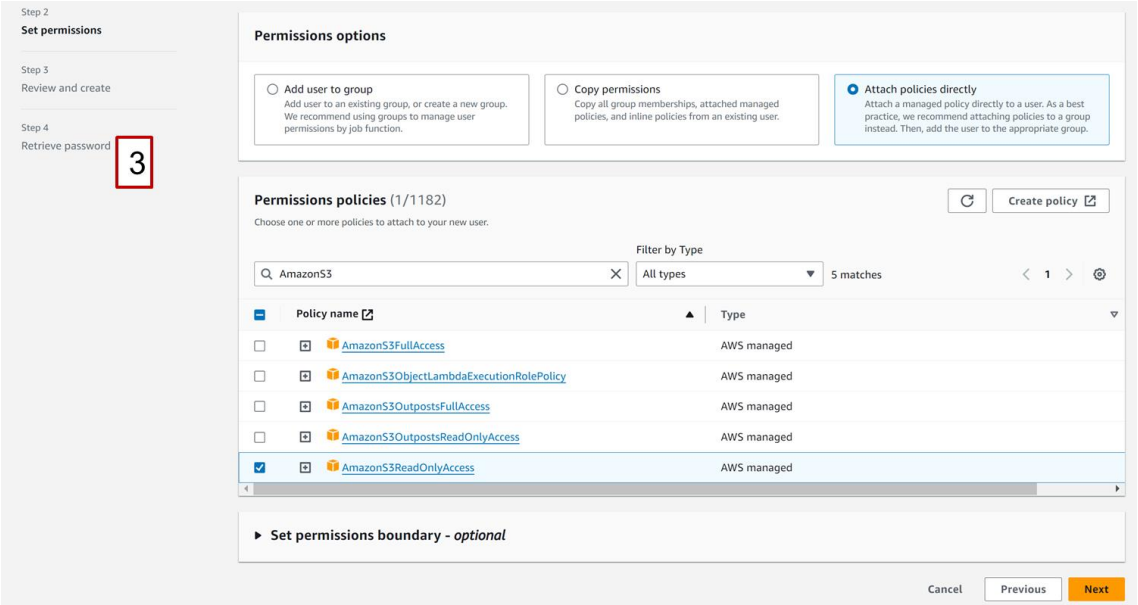
1. Crear un nuevo usuario



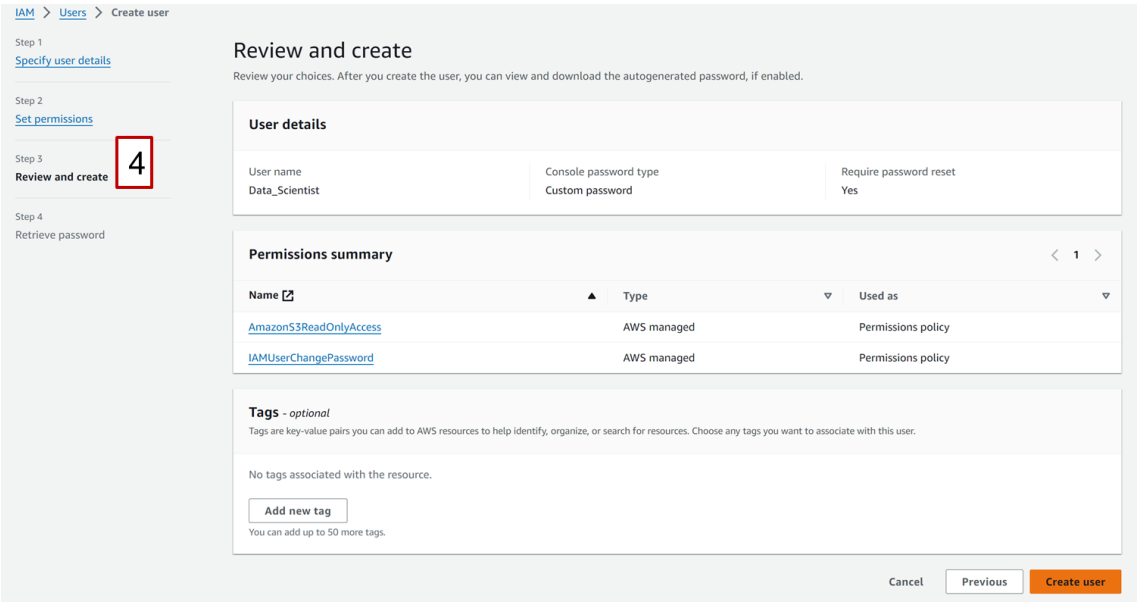
2. Crear las credenciales para este usuario



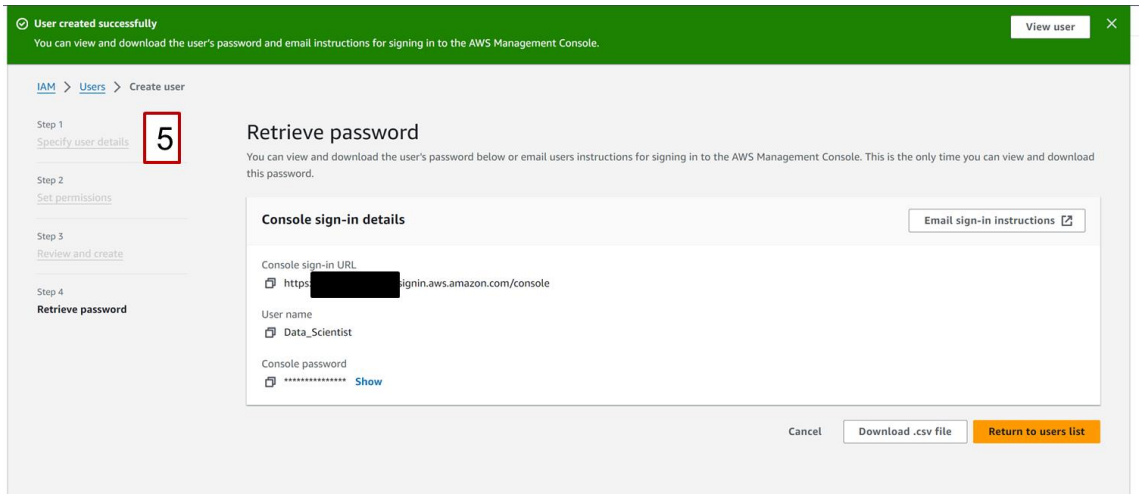
3. Establecer los permisos para este usuario adjuntando una política existente o creando una nueva. (Para obtener más información, consulte la sección ***¿Qué es una política de IAM*** ? a continuación)



4. Revise los detalles del usuario y cree el nuevo usuario IAM



5. Comparta las credenciales de inicio de sesión con el usuario



¿Qué es un grupo IAM?

Ahora, ¿qué pasa si desea conceder los mismos permisos a más de un usuario, tal vez un equipo de científicos de datos que quieren acceder a los mismos recursos con el mismo nivel de permisos. Usted podría adjuntar la misma política a cada usuario, pero podría ser difícil de manejar a medida que el equipo crece. En este caso, puede crear un grupo IAM, que es una colección de usuarios, y luego adjuntar la política al grupo en lugar de a los usuarios individuales. Cada usuario del grupo hereda los permisos del grupo. Piense en el grupo IAM como una forma de organizar los permisos. Estas son algunas de las características de los grupos IAM:

- Los grupos pueden tener múltiples usuarios
- Un usuario puede no pertenecer a ningún grupo, a un grupo o a varios grupos (hasta 10 grupos)
- Los grupos no pueden anidarse

¿Qué es un rol IAM?

La tercera identidad de IAM es un rol. Un rol IAM tiene permisos específicos con credenciales a corto plazo. Los roles pueden ser asumidos por entidades, como personas, aplicaciones o recursos de confianza de AWS. Los roles de IAM no tienen credenciales a largo plazo. En su lugar, proporcionan credenciales de seguridad temporales para la duración de la sesión del rol. Primero se crea un rol IAM y se le adjunta una política. A continuación, se especifica qué recurso puede asumir este rol. Esto otorga temporalmente permisos a los recursos de AWS.

Ejemplo 1: Supongamos que ejecuta un código en una instancia EC2 que necesita leer de S3. Por defecto, la instancia EC2 no tiene permiso para leer de S3. Puede transferir sus credenciales a EC2, pero esto no es seguro. Un mejor enfoque es crear un rol, adjuntar la política requerida para leer de S3, y permitir que la instancia EC2 asuma este rol.

Ejemplo 2: Supongamos que ejecutas un trabajo ETL de Glue y quieres que escriba los datos ingestados y transformados en S3. Puede crear una función con permisos para escribir en S3 y, a continuación, permitir que Glue ETL asuma esta función.

¿Qué es una política IAM?

Puede administrar el acceso en AWS creando políticas y adjuntándolas a usuarios, grupos o roles de IAM.

"Una política es un objeto en AWS que define los permisos del usuario o rol adjunto. AWS evalúa estas políticas cuando un usuario o rol de IAM realiza una solicitud. Los permisos de las políticas determinan si se permite o deniega la solicitud. La mayoría de las políticas se almacenan en AWS como documentos JSON" - Documentación de AWS IAM

Puede utilizar una política administrada por AWS o crear su propia política personalizada.

Ejemplo Política gestionada por AWS (AmazonS3FullAccess)

Esta es la política administrada *AmazonS3FullAccess* que concede acceso completo a S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "s3-object-lambda:*"
            ],
            "Resource": "*"
        }
    ]
}
```

- **Versión** - Especifique la versión del lenguaje de la política que desea utilizar.
- **Statement** - Utiliza este elemento como contenedor para los detalles de algunos permisos o denegaciones dados. Puede incluir más de una declaración en una política. Si una política incluye múltiples declaraciones, AWS aplica un OR lógico a través de las declaraciones cuando las evalúa.
    - **Sid** (Opcional) - Incluya un ID de sentencia para diferenciar entre sus sentencias.
    - **Efecto** - Utilice Permitir o Denegar para indicar si la política permite o deniega el acceso.
    - **Acción** - Incluya una lista de acciones que la política permite o deniega. En este ejemplo, las acciones permitidas en S3 son "*", lo que significa que todas las acciones de lectura y escritura en s3 están permitidas).
    - **Recurso** - Un objeto o una lista de objetos a los que se aplican las acciones. Por ejemplo, en el caso de S3, se puede especificar a qué bucket se permite o

deniega el acceso. En este ejemplo, el elemento resource es "*", que significa todos los recursos.

Ejemplo: Política gestionada por el cliente

Este es otro ejemplo de política que permite el acceso de lectura y escritura a todos los buckets de S3, excepto al bucket "confidencial", cuya eliminación está denegada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "statement2",
            "Effect": "Deny",
            "Action": [
                "s3:DeleteBucket"
            ],
            "Resource": "arn:aws:s3:::confidential"
        }
    ]
}
```

Más información

- Ejemplos de políticas de cubos de S3

 Guía del usuario de IAM (administración del acceso a los recursos de AWS

)

 ¿Qué es IAM?

-