Acceso a Bucket S3 para Clientes

Acceso a Bucket S3 para Clientes

Manual: Acceso a Bucket S3 para Clientes

Guía paso a paso para crear un bucket S3 exclusivo para un cliente, con acceso restringido mediante una política IAM y un usuario dedicado (Access Key), para que el cliente pueda subir/descargar sus archivos de forma segura.

> Reemplaza los nombres de ejemplo (`nxs-s3-cliente`, `nxs-user-cliente-app`, etc.) por la convención de nombres real del cliente que estás configurando.

Índice

---

1. Crear el bucket S3

1. Ir a **Amazon S3 → Buckets** y hacer clic en **Create bucket**.
2. **Bucket type:** `General purpose`.
3. **Bucket name:** usar convención `nxs-s3-<cliente>` (debe ser único a nivel global).
4. **AWS Region:** dejar la región estándar de la cuenta (ej. `US East (Ohio) us-east-2`).
5. **Object Ownership:** dejar `ACLs disabled` (recomendado).
6. **Block Public Access:** mantener **todo bloqueado** (bucket privado, sin acceso público).
7. **Bucket Versioning:** según necesidad del cliente (`Disable` u `Enable`).
8. **Default encryption:** `SSE-S3` (por defecto), `Bucket Key: Enable`.
9. Clic en **Create bucket**.

Crear bucket - datos generales Crear bucket - versionado y cifrado

---

2. Verificar el bucket creado

El bucket queda vacío y listo para recibir archivos (vía consola, CLI o API).

Bucket creado vacío

---

3. Revisar la pestaña de permisos del bucket

Entrar a la pestaña **Permissions** del bucket. En este flujo **no** se usa una Bucket Policy pública: el acceso se controla con una política IAM asociada a un usuario dedicado (pasos siguientes).

Bucket - tab de permisos

---

4. Crear la política IAM

1. Ir a **IAM → Policies → Create policy**.
2. Cambiar al editor **JSON** (arriba a la derecha).
3. Pegar el JSON de permisos (ver bloque abajo), reemplazando el nombre del bucket.

Crear política - acceso al servicio Crear política - editor JSON

JSON de permisos (copiar y pegar)

Da permisos de **subir, leer, listar y eliminar** objetos, limitado a un bucket específico:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "NxsS3AccessCliente",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::nxs-s3-cliente/*"
        },
        {
            "Sid": "NxsS3ListBucketCliente",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::nxs-s3-cliente"
        }
    ]
}
```

> ⚠ **Importante:** reemplazar `nxs-s3-cliente` por el nombre real del bucket creado en el paso 1, en **ambas** líneas (`Resource` con `/*` para objetos, y sin `/*` para el `ListBucket`).

JSON de la política

---

5. Nombrar y crear la política

1. En **Review and create**, asignar un nombre descriptivo, ej: `nxs-s3-cliente-policy`.
2. Verificar el resumen de permisos (S3: List, Read, Write).
3. Clic en **Create policy**.

Nombrar y revisar política

---

6. Crear el usuario IAM

1. Ir a **IAM → Users → Create user**.
2. **User name:** convención `nxs-user-<cliente>-app`.
3. **No** marcar "Provide user access to the AWS Management Console" (el cliente no necesita acceso a la consola, solo Access Key para API/CLI/SDK).
4. Clic en **Next**.

Crear usuario IAM

---

7. Asignar la política al usuario

1. En **Set permissions**, elegir **Attach policies directly**.
2. Buscar la política creada en el paso 5 (filtrar por el prefijo, ej: `nxs`).
3. Marcar el checkbox de la política correspondiente.
4. Clic en **Next** y luego **Create user**.

Asignar política al usuario

---

8. Generar el Access Key

1. Entrar al usuario creado → pestaña **Security credentials**.
2. En **Access keys**, clic en **Create access key**.

Crear access key

3. **Use case:** seleccionar `Application running outside AWS` (o `Command Line Interface (CLI)` si el cliente usará la CLI directamente). Clic en **Next**.

Caso de uso del access key

4. **Description tag (opcional):** se puede indicar el propósito de la key. Clic en **Create access key**.

Confirmación de creación

5. Se muestran el **Access key** y el **Secret access key**. Copiar ambos o descargar el archivo `.csv`. **El Secret access key solo se muestra una vez.**

Access key y secret key generados

> □□ Entregar estas credenciales al cliente por un canal seguro (gestor de contraseñas, no por correo o chat en texto plano).

---

9. Configuración del lado del cliente (AWS CLI)

En la máquina del cliente, con la AWS CLI instalada:

```
aws configure
```

```
AWS Access Key ID [None]: <ACCESS_KEY_ID>
AWS Secret Access Key [None]: <SECRET_ACCESS_KEY>
Default region name [None]: us-east-2
Default output format [None]: json
```

Prueba rápida de conexión (debe listar el contenido del bucket, vacío al inicio):

```
aws s3 ls s3://nxs-s3-cliente
```

Subir un archivo de prueba:

```
aws s3 cp archivo-prueba.txt s3://nxs-s3-cliente/
```

Configuración AWS CLI en el cliente

---

10. Buenas prácticas de seguridad

- Mantener **Block Public Access** activado en el bucket (privado, sin excepciones).
- Un **usuario IAM + una política dedicada por cliente** — nunca compartir credenciales entre clientes.
- No usar Bucket Policy pública salvo un requerimiento explícito y justificado.
- Rotar el Access Key periódicamente y desactivar/eliminar keys que ya no se usen.
- Habilitar **MFA** para usuarios humanos con acceso a la consola (no aplica a este flujo de solo Access Key).
- Documentar en un registro interno qué bucket, política y usuario corresponden a cada cliente.

Referencia rápida — plantilla JSON para copiar

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "NxsS3AccessCliente",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::NOMBRE_BUCKET/*"
        },
        {
            "Sid": "NxsS3ListBucketCliente",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::NOMBRE_BUCKET"
        }
    ]
}
```