

Amazon S3

Amazon S3 is probably the most well-known object storage in the world. It's very flexible and support a lot of settings and options. Explaining all of them here would be out of scope, so let us give you the links to the official documentation from Amazon/AWS regarding how to create a bucket and configure an access to it.

Step #1: in the AWS Console

First create your S3 bucket:

[Creating a general purpose S3 bucket](#) (opens in a new tab)

Then to create an Access Key and Secret pair:

1. Create an **IAM User**:
 1. Navigate to the IAM Console
 2. Select Users
 3. Click Create user.
2. **Attach Permissions**: In the permissions step, attach a policy granting S3 access (e.g., **AmazonS3FullAccess** or a custom policy restricting access to your specific bucket).
3. **Generate Keys**: After creating the user, click on the user name, go to the **Security credentials** tab, and select **Create access key**.
4. **Download Credentials**: Choose **Other** for the use case, add a description if desired, and click **Create access key**. **Download the .csv file immediately**, as the Secret Access Key is only displayed once.

That's it for the Amazon/AWS side. Now let's move to the SFTP.cloud side.

Step #2: in your SFTP.cloud Storage Connector

For **best performance** it is recommended that you deploy an SFTP.cloud Storage Connector as close as possible to the storage it handles, in this case **an EC2 VM or a container in Amazon ECS** are the ideal choices.

The first thing to do is to add a new **Virtual File System**. For Linode Object Storage in particular there are a few small (but extremely important) details to pay attention to:

- **Type**: **S3** (just like any other S3-compatible object stores)
- **Region**: whichever region you created the bucket in (ex: *us-east-1*)

- **Endpoint:** for Amazon/AWS leave this one empty

The screenshot shows the SFTP.cloud Connector interface. On the left is a sidebar with navigation links: Dashboard, STORAGE (Virtual file systems), ACCESS (Users, Folder sets), AUTOMATION (Scripts, Event handlers, Schedules, Transfers, Secrets), MONITORING (Activity, Log integrity), and SYSTEM (Settings, Network, Administrators, Updates). The main panel is titled 'Storage' and has two tabs: 'Virtual file systems' (active) and 'Encryption keys'. Below the tabs is a search bar and a table of virtual file systems. The table has columns for NAME, TYPE, and TARGET. It lists various imported systems like 'bulk', 'devfs', and 'imp94986hash' with their respective paths. At the bottom, it shows user-defined buckets: 'linode-bucket', 'my-minio', 'my-rustfs', and 'seed-000' through 'seed-002'. On the right, a 'Create virtual file system' modal is open. It contains fields for Name (my-amazon-s3), Type (S3), Connection (Bucket name), Path inside (optional), Region (us-east-1), and Endpoint (optional). There are sections for CREDENTIALS (Access key ID, Access secret with buttons for Configured, Replace, Remove) and TRANSFER SPEED (Parallel connections to your cloud site, set to Standard (one connection)). There is also an 'AT REST ENCRYPTION' section with a checkbox for 'Encrypt data at rest' and an 'Advanced' link. At the bottom right of the modal are 'Cancel' and 'Create' buttons.

NAME	TYPE	TARGET
bulk	Imported	/opt/Syncplify/sc-comm-data/devfs/legacy/bulk
devfs	Disk	/opt/Syncplify/sc-comm-data/devfs
imp94986hash	Imported	/opt/Syncplify/sc-comm-data/devfs/legacy/imp94986hash
imp94986keys	Imported	/opt/Syncplify/sc-comm-data/devfs/legacy/imp94986keys
imp94986none	Imported	/opt/Syncplify/sc-comm-data/devfs/legacy/imp94986none
imp94986plain	Imported	/opt/Syncplify/sc-comm-data/devfs/legacy/imp94986plain
imp95089hash	Imported	/opt/Syncplify/sc-comm-data/devfs/legacy/imp95089hash
imp95089keys	Imported	/opt/Syncplify/sc-comm-data/devfs/legacy/imp95089keys
imp95089none	Imported	/opt/Syncplify/sc-comm-data/devfs/legacy/imp95089none
imp95089plain	Imported	/opt/Syncplify/sc-comm-data/devfs/legacy/imp95089plain
linode-bucket	S3	s3://my-fancy-test-bucket
my-minio	S3	s3://my-minio-bucket
my-rustfs	S3	s3://my-rustfs-bucket
seed-000	Disk	/opt/Syncplify/sc-comm-data/devfs/seed/seed-000
seed-001	Disk	/opt/Syncplify/sc-comm-data/devfs/seed/seed-001
seed-002	Disk	/opt/Syncplify/sc-comm-data/devfs/seed/seed-002

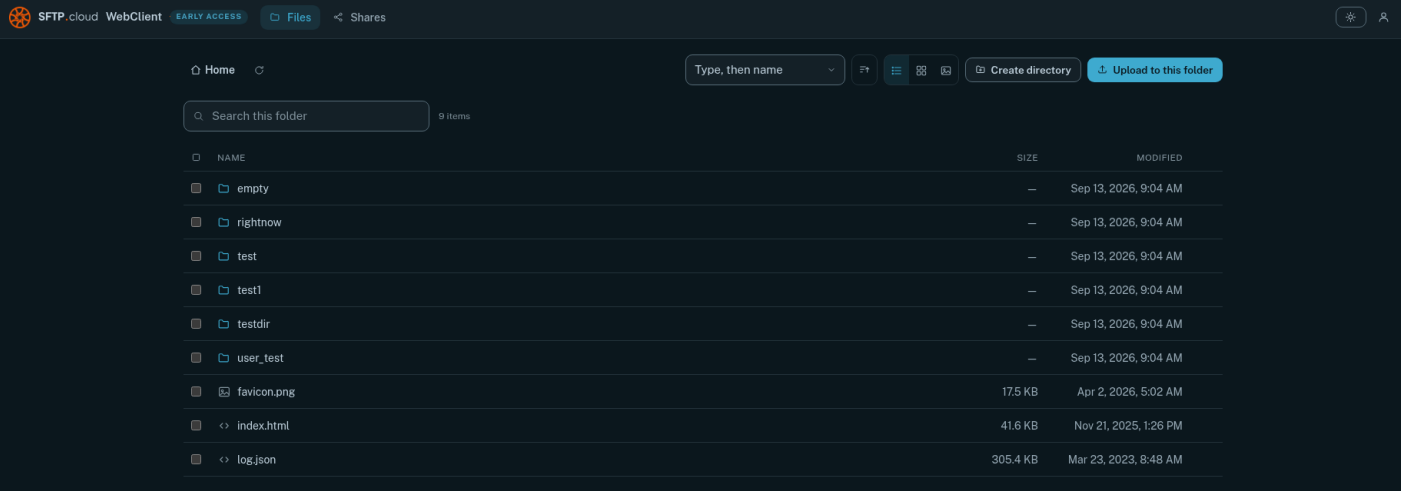
Do NOT forget to push the **Save** button next to the **Access secret** after you type it in, or it won't be saved, and nothing will work.

Then, still in the Storage Connector UI, go to the **Users** page, and give your user(s) the desired access to the newly created VFS:

The screenshot shows the 'Users' page in the SFTP.cloud Connector UI. The sidebar is the same as in the previous image. The main panel shows the user 'alice@devsite' with status 'Synced from Portal' and 'Active'. Above the user name are buttons: 'Edit access', 'Pause access', 'End all sessions', 'Revoke access', and 'Remove from this Connector'. Below the user name is a section titled 'Access on this Connector' with the text: 'Which of this Connector's folders this user may open, and what they can do in each one. Click a permission to change it; a folder without access stays closed.' There is a list of folders with their access levels: 'my-amazon-s3' (Full access), 'bulk' (No access), and 'devfs' (No access). Each folder has a trash icon to its right.

Finally

Test it out. Connect to it via your SFTP.cloud WebClient, create a folder, upload some files...



[Manual: [general information about storage back-ends](#)]

Revision #2
Created 13 September 2026 15:44:14 by DevTeam
Updated 13 September 2026 22:16:02 by DevTeam