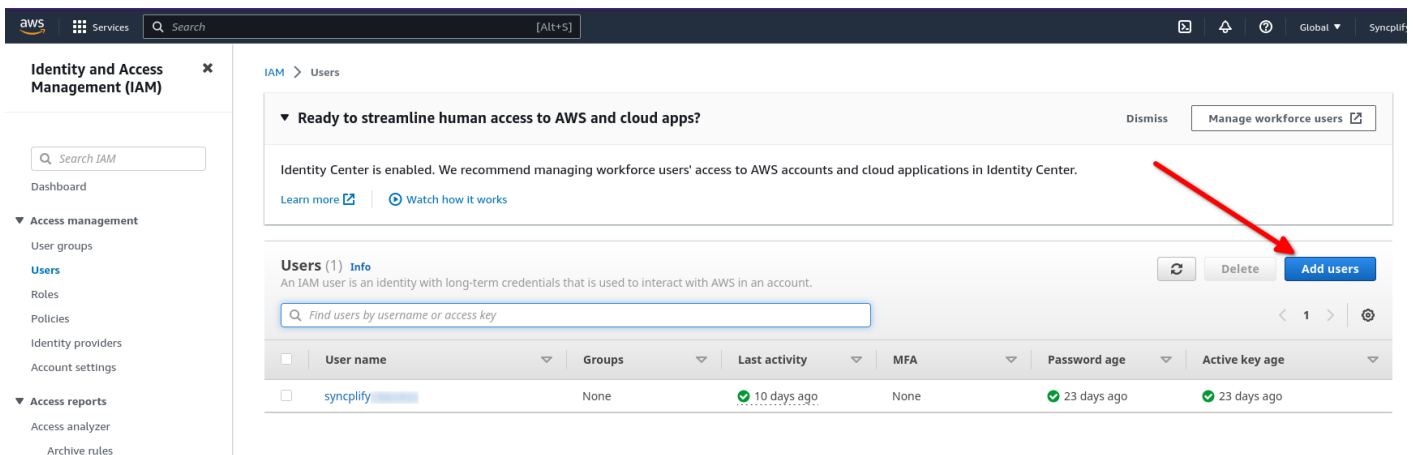


How to use the S3 Virtual File System (VFS)

Syncplify Server!, through its virtual file system (VFS) data storage layer, can store your SFTP server's data into various storage back-ends. This article explains how to use the **S3** VFS type that stores your server's data into an Amazon (AWS) S3 object storage bucket.

First of all you'll need an AWS IAM user account to access the S3 bucket. Head over to the IAM section of your AWS Console, and create one:



Make sure the newly created AWS user **has at least one Access Key**, and that it has the desired permissions to access your S3 buckets. In this picture we show an account that has *full access*, but for safety reasons you should always only grant the minimum set of permissions your workloads require.

Summary

ARN
arn:aws:iam::778330933654:user/syncplifyConsole access
Enabled without MFAAccess key 1
- Active
Used 10 days ago. 23 days old.Created
March 23, 2023, 08:35 (UTC-07:00)Last console sign-in
NeverAccess key 2
Not enabled

Permissions Groups Tags (1) Security credentials Access Advisor

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Find policies

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Directly

At this point you are ready to create your S3 bucket(s):

Amazon S3 Buckets

Account snapshot
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

View Storage Lens dashboard

Buckets (1) Info
Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Name	AWS Region	Access	Creation date
syncplify3testbucket	US East (N. Virginia) us-east-1	Bucket and objects not public	March 23, 2023, 08:47:00 (UTC-07:00)

Please make sure you deploy your S3 bucket in the AWS **region** you need it to be in, and make sure your security policies comply with the security requirements of your company/entity (typically you do not want your bucket to be publicly accessible, you probably want it to be accessible only by using the Access Key you created for the user profile above).

Now that everything is ready on the AWS side of the house, let's see how easy it is to create a Virtual File System (VFS) in Syncplify Server! v6 that uses your S3 bucket to store your SFTP server's data:

Editing VFS "Test-2-S3" (type: S3)

Target *

s3://syncplifys3test?region=us-east-1

Example: "s3://my-bucket?region=us-west-1&endpoint=string&disableSSL=true/false>&s3ForcePathStyle=true/false".

Target Payload

{"access_key":"AKIA3YREIUUNFGRU45B","access_secret":"wue386whgsbxv47"}

Example: {"access_key":"Server_Access_Key","access_secret":"Server_Access_Secret"}

Soft Quota

0

Hard Quota

0

Cancel

Edit

Make sure your S3 URL includes your bucket name and region, if the region is missing *us-east-1* will be assumed. Then input your **access_key** and **access_secret** as your Target Payload (in JSON format). No worries, Syncplify Server! uses strong encryption to store all secrets in its internal database. That's all there is to it. You can now assign this VFS to any User account in your Syncplify Server!, and its data will be stored in your S3 bucket.

Revision #4

Created 16 April 2023 14:22:23 by DevTeam

Updated 24 October 2024 10:18:02 by DevTeam