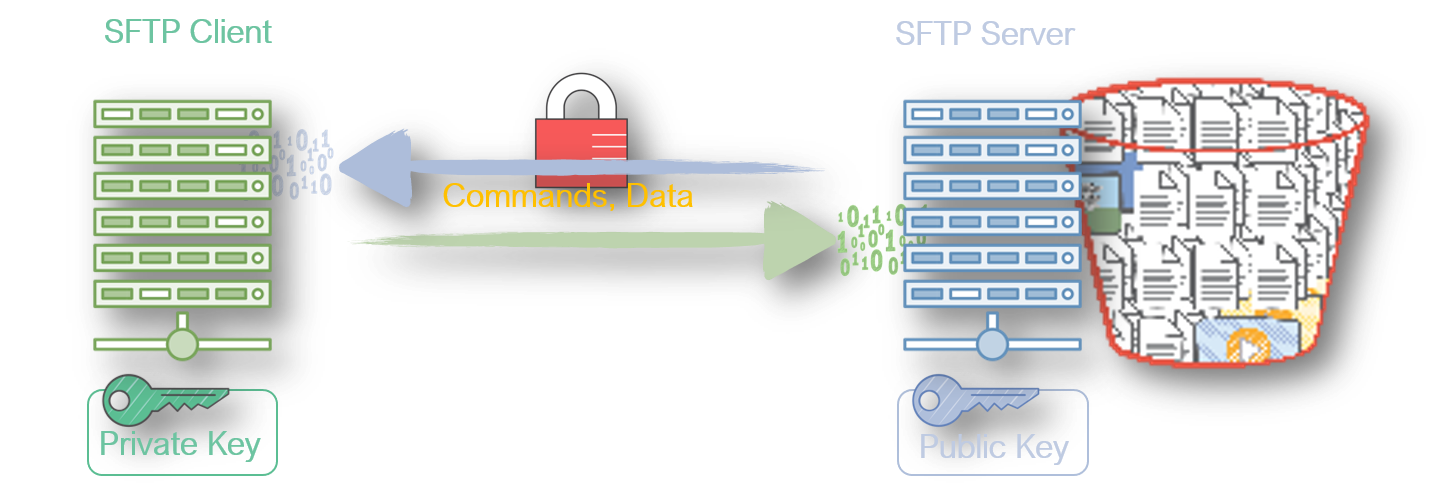
**SFTP Service for Amazon S3**

AWS Transfer for SFTP is a fully-managed, highly-available SFTP service.

Follow this article in **[Youtube](https://youtu.be/zuRPbqcaRcI)**

[](https://raw.githubusercontent.com/miztiik/AWS-Demos/master/How-To/setup-sftp-for-s3/images/sftp-for-s3-valaxy-miztiik.png)

**Prerequisites**

1. S3 Bucket - BucketName (*For ex:: sftp.dest.testbkt)*
   * *You will have to create your own bucket and use that name in the instructions*
2. SFTP Client
   * Preferably a linux machine as sftp client is available by default.
   * If you are using Windows, then you can use *WinSCP*
3. IAM Role for SFTP Users
   * Permissions - AmazonS3FullAccess
   * Updated Trust Relationship (*see below*)

**Setup IAM Role for Users**

Create a IAM Role with AmazonS3FullAccess (*You can restrict this to particular bucket/user*) with the following trust relationships.

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Principal": {

"Service": "transfer.amazonaws.com"

},

"Action": "sts:AssumeRole",

"Condition": {}

}

]

}

**Create the SFTP Server**

You can basically have have your custom endpoint with your domain name or can use the default endpoint

**Set up Users**

You will need a SSH Key pair, and upload the public key that the user will use when connecting to the SFTP server,

**Create SSH Keypair**

From linux server you can do this, (you can do the same in windows using putty-gen)

>ssh-keygen -P "" -f "sftp-test-key"

Copy the public key to the user configuration & save. **Note** : *The public key should not be multiline (or) have any special characters like enter*

**Connect to SFTP Server**

>sftp -i sftp-test-key testuser@YOUR-SFTP-END-POINT

# To list files

>ls

# To upload files

>mput YOUR-FILE-NAME

>ls