Virtual File System (VFS) Encryption

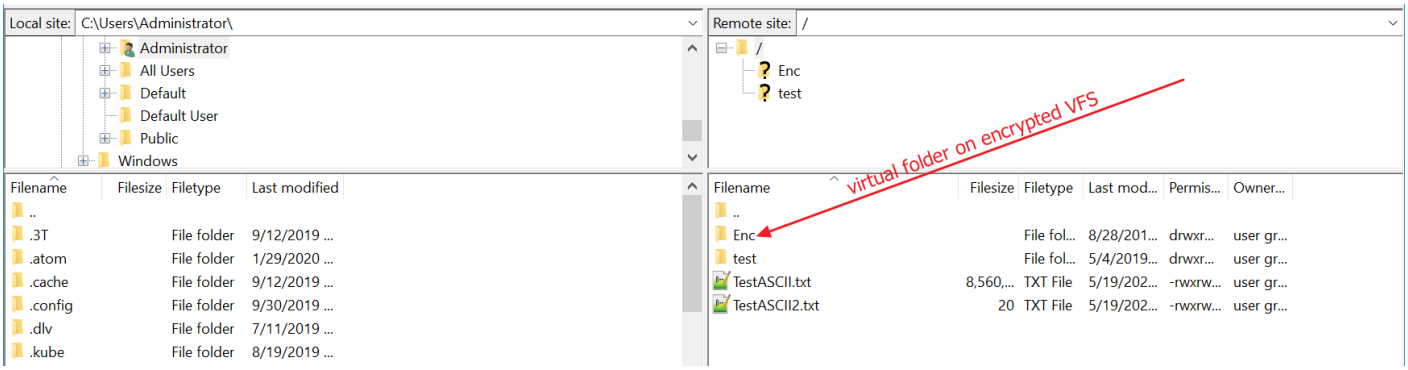
You may have notices that, depending on the Syncplify Server! edition you're running, you may be able to enable Encryption when you create a new Virtual File System (VFS).

This means that whatever you upload to that VFS will **automatically be stored in an encrypted form** on the server's storage, and it will be automatically decrypted when downloaded again by a client.

> Note: this has nothing to do with encryption over the network, which is always on, and is guaranteed by the file transfer protocols you're using - this article refers to what's known in the industry as "at-rest encryption".

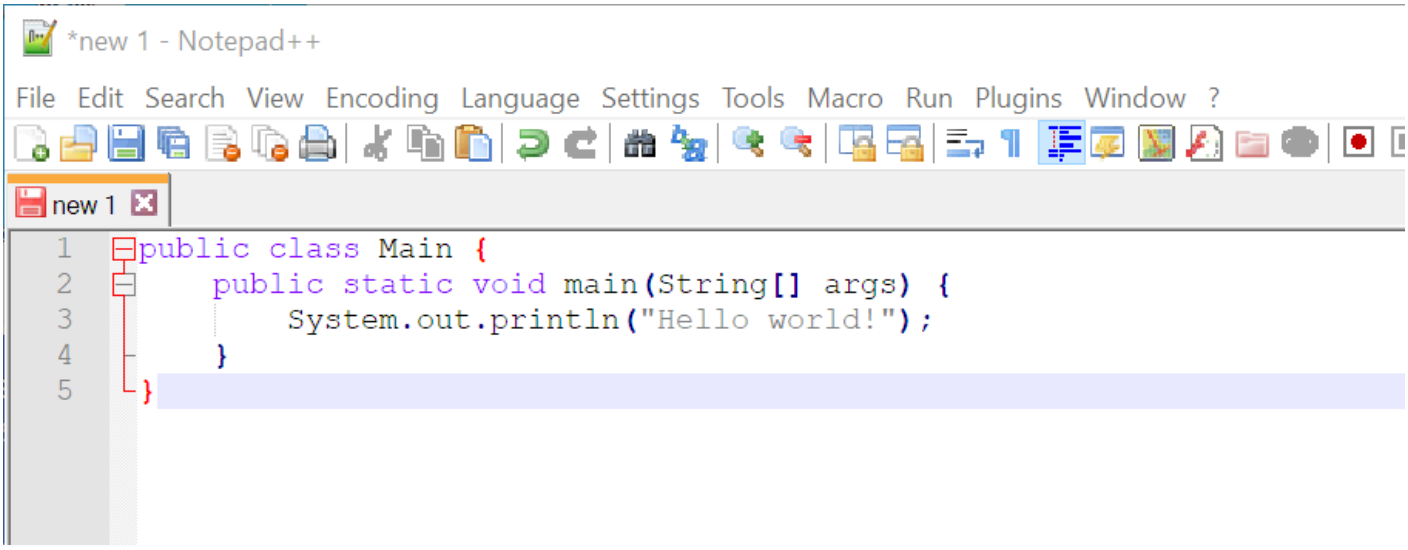
An encrypted VFS transparently encrypts and decrypts data on-the-fly during the interaction with the server machine/VM's storage medium, making sure that the files at-rest on the server-side are always encrypted. This way you can run your server externally, and still always be sure that whoever operates the server for you doesn’t have access to your files/backups. This is also a requirement in some cases when your company has to comply with the PCI/DSS or HIPAA regulations.

As long as an encrypted VFS is accessed via a secure file transfer client using a legitimate user account, a VFS will show us just like any other folder, and files in it can be downloaded in clear by the legitimate user.

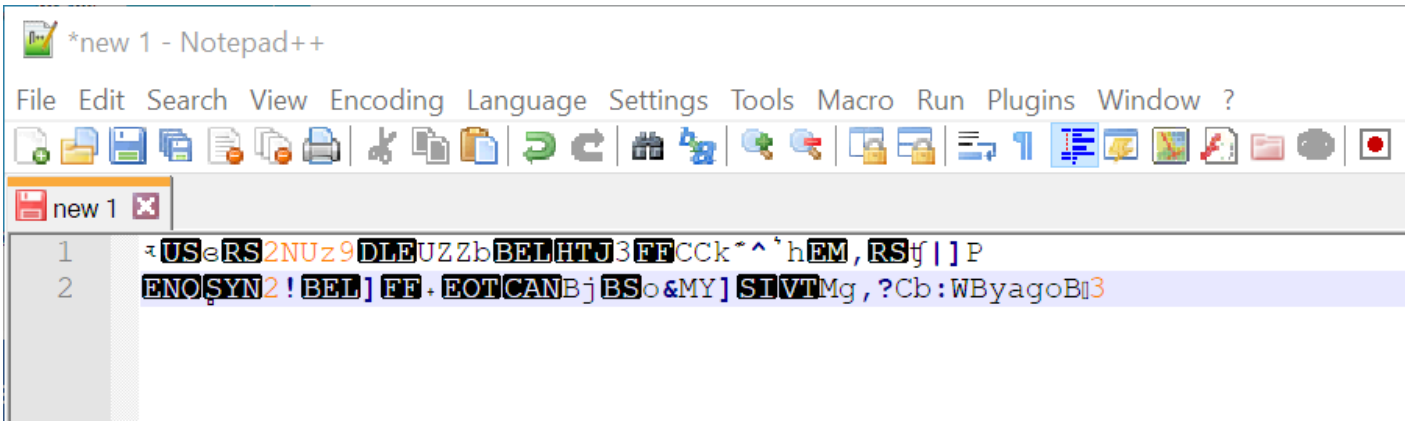


But let's say you have a text file on your client computer for example, and you want to upload it to a remote Syncplify Server! into an encrypted VFS...

The file on your client will look something like this:



Yet, once uploaded to the remote Syncplify Server!, should someone had raw direct access to the server's storage, all they would see is this:



Feel free to **run your SFTP server in the cloud**, or host it in any other insecure place, or delegate its management to an untrusted third party... whoever might have physical access to it, still won't be able to acquire your files, as they're all encrypted "at-rest" on the server's disk drive (or any other storage medium).

Revision #1
Created 7 February 2023 22:17:25 by DevTeam
Updated 7 February 2023 22:52:04 by DevTeam