

Using network shares (UNC paths) with Syncplify Server! v6+ on Windows

Windows does not allow system services running as SYSTEM (or LocalSystem) to access UNC paths. This is a design choice by Microsoft, so every system service of every vendor (not just Syncplify) is subject to it.

So what can you do when you need your system service to access those "network shares"? For example you may want to place your users home-VFSs on a different storage (this is practically mandatory in high-availability environments).

The correct and secure way to do it (according to Microsoft's Best Practices) is the following:

Step #1 - Create a Windows or Active Directory "service account"

A service account is just a user account which will be used to run your system service. This particular account will have to be given permissions onto the following directories/folders:

- `C:\ProgramData\Syncplify\ServerV6` (and all sub-dirs) - be wary that "ProgramData" is typically hidden in Windows, but it's there even if you don't see it
- All of the directories, folders, and UNC (network) paths where you intend to point your VFSs to

To avoid unattended-operation complications, it's best to set this account to never expire and to never have to change its own password. An Administrator should take care of that, from time to time, according to corporate policies.

Syncplify Properties

Member Of: Remote control: Remote Desktop Services Profile: Sessions: COM+

General: Address: Account: Profile: Telephones: Organization:

User logon name: sftp-service-account @AD9.local

User logon name (pre-Windows 2000): AD9\ sftp-service-account

Logon Hours... Log On To...

☒ Unlock account

Account options:

- ☐ User must change password at next logon
- ☒ User cannot change password
- ☒ Password never expires
- ☐ Store password using reversible encryption

Account expires:

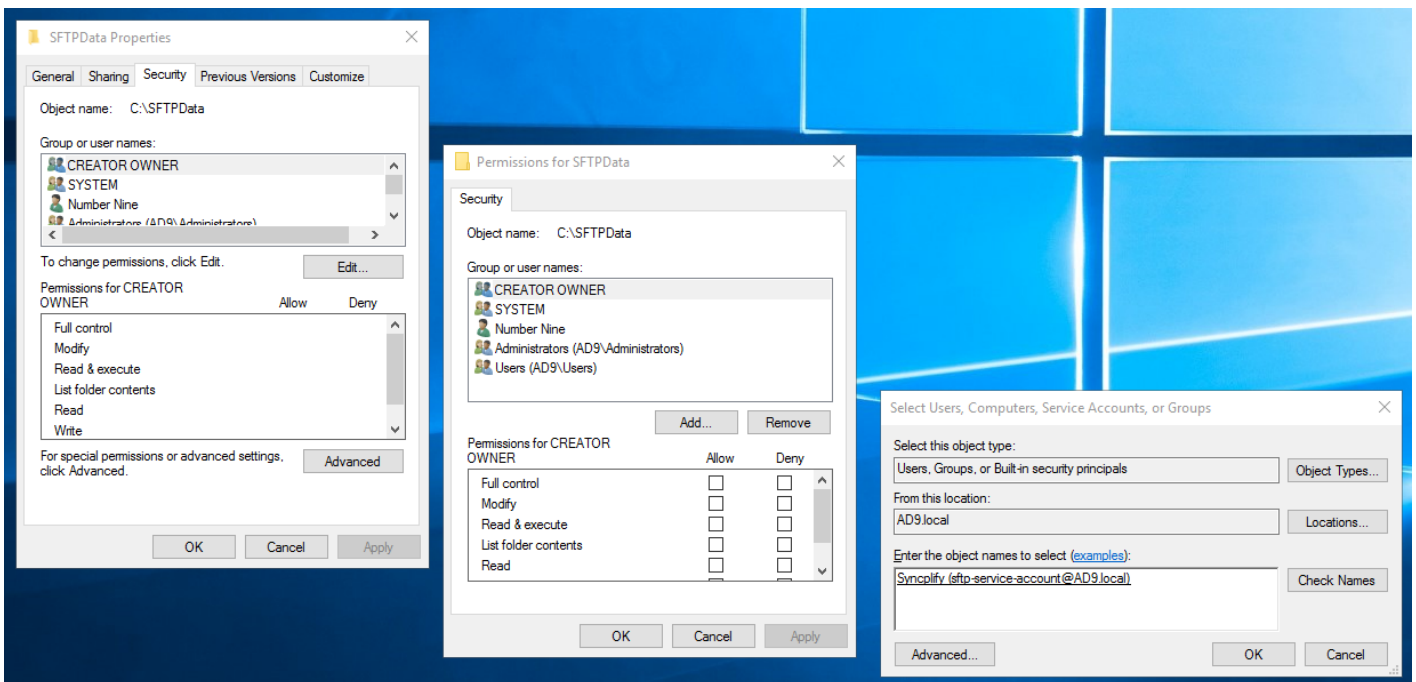
☒ Never

☐ End of: Tuesday, February 21, 2023

OK Cancel Apply Help

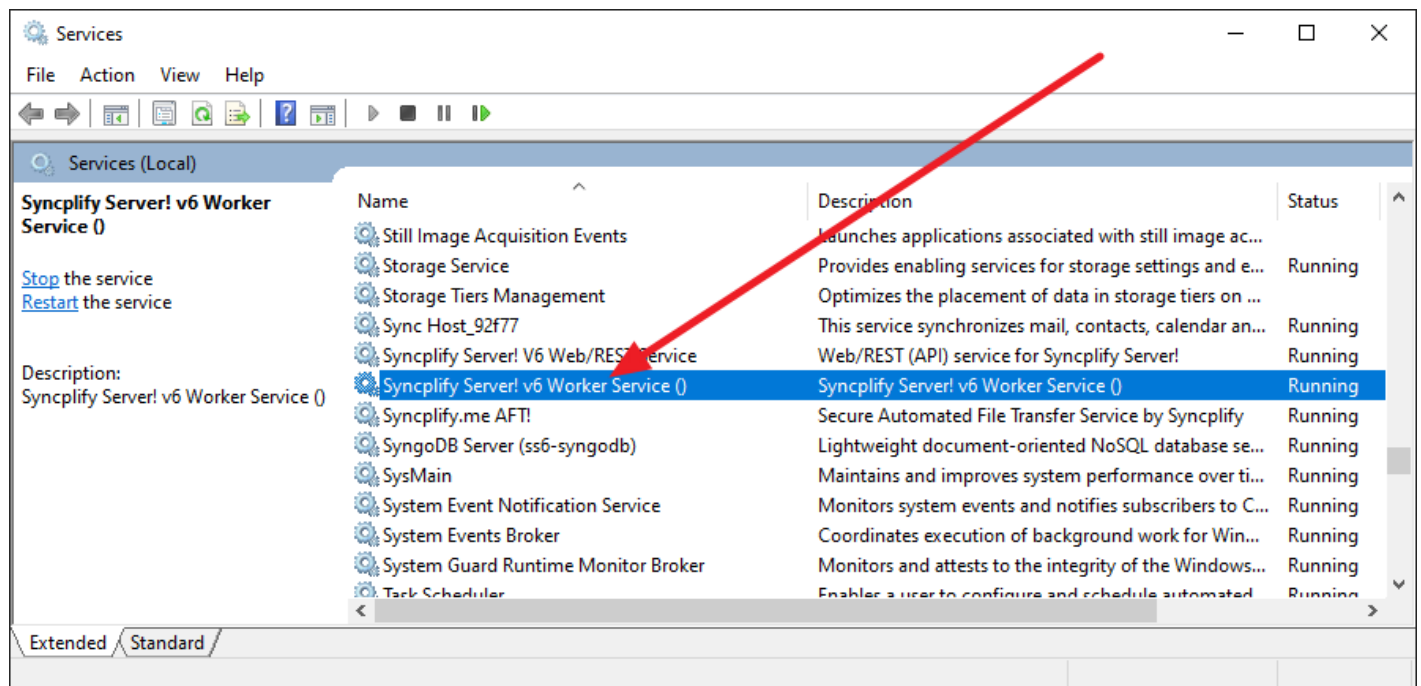
Step #2 - Grant the proper storage permissions to the service account

As already described above, this newly created service account will need to be granted access permissions to the folders and network paths listed above:

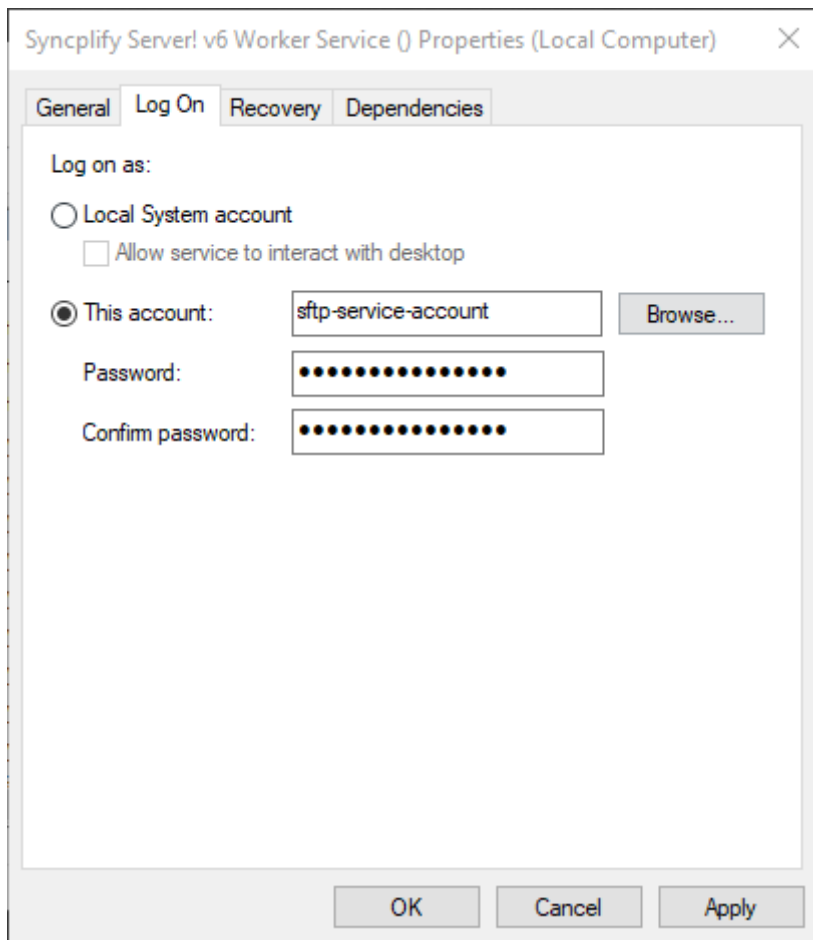


Step #3 - Run your virtual site's "worker" service impersonated with the above service account

Open Windows' SCM (Service Control Manager) and locate the "worker" (wrk) service for the virtual site you need to be able to access UNC paths:



Double click on it, and set it to run "as" the impersonation account you previously created:



Do not forget to **restart the virtual site's system service** for these changes to take effect

Once restarted, if you did everything correctly, the virtual site will now be able to access its users' home-VFSs located on the remote UNC paths (network shares) the service account has access to.

Revision #1

Created 3 February 2023 18:42:01 by DevTeam

Updated 7 February 2023 22:52:04 by DevTeam