



***Full credit is given to the above companies including the OS that this PDF file was generated!***

### ***Linux Ubuntu 22.4.5 Manual Pages on command 'virtfs-proxy-helper.1'***

**\$ man virtfs-proxy-helper.1**

VIRTFS-PROXY-HELPER.1(1)

VIRTFS-PROXY-HELPER.1(1)

#### **NAME**

virtfs-proxy-helper - QEMU 9p virtfs proxy filesystem helper

#### **SYNOPSIS**

virtfs-proxy-helper options

#### **DESCRIPTION**

Pass-through security model in QEMU 9p server needs root privilege to do few file operations (like chown, chmod to any mode/uid:gid). There are two issues in pass-through security model

1) TOCTTOU vulnerability: Following symbolic links in the server could provide access to files beyond 9p export path.

2) Running QEMU with root privilege could be a security issue.

To overcome above issues, following approach is used: A new filesystem type 'proxy' is introduced. Proxy FS uses chroot + socket combination for securing the vulnerability known with following symbolic links. Intention of adding a new filesystem type is to allow qemu to run in non-root mode, but doing privileged operations using socket IO.

Proxy helper(a stand alone binary part of qemu) is invoked with root privileges. Proxy helper chroots into 9p export path and creates a socket pair or a named socket based on the command line parameter. QEMU and proxy helper communicate using this socket. QEMU proxy fs driver sends filesystem request to proxy helper and receives the response from it.

The proxy helper is designed so that it can drop root privileges except for the capabilities needed for doing filesystem operations.

## OPTIONS

The following options are supported:

**-h** Display help and exit

**-p|--path** path

Path to export for proxy filesystem driver

**-f|--fd** socket-id

Use given file descriptor as socket descriptor for communicating with qemu proxy fs driver. Usually a helper like libvirt will create socketpair and pass one of the fds as parameter to **-f|--fd**

**-s|--socket** socket-file

Creates named socket file for communicating with qemu proxy fs driver

**-u|--uid** uid **-g|--gid** gid

uid:gid combination to give access to named socket file

**-n|--nodaemon**

Run as a normal program. By default program will run in daemon mode

## AUTHOR

M. Mohan Kumar

2022-12-08

VIRTFS-PROXY-HELPER.1(1)