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:

- TOCTTOU vulnerability: Following symbolic links in the server could provide access to files beyond 9p export path.
- 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 drier. Usually a helper like libvirt will create socketpair and pass one of the fds as parameter to this option.

−s, −−socket SOCKET_FILE
Creates named socket file for communicating with qemu proxy fs driver

−u, −−uid UID
uid to give access to named socket file; used in combination with −g.

−g, −−gid GID
gid to give access to named socket file; used in combination with −u.

−n, −−nodaemon
Run as a normal program. By default program will run in daemon mode

AUTHOR

M. Mohan Kumar

COPYRIGHT