



Red Hat Enterprise Linux Release 9.2 Manual Pages on 'setroubleshootd.8' command

\$ man setroubleshootd.8

setroubleshootd(8) setroubleshootd(8)

NAME

setroubleshootd - setroubleshoot daemon

SYNOPSIS

setroubleshootd [-d] [-f] [-h] [-c config]

DESCRIPTION

This manual page describes the setroubleshootd program.

setroubleshootd is the dbus service in the setroubleshoot system.

setroubleshoot is used to diagnose SELinux denials and attempts to provide

user friendly explanations for a SELinux denial (e.g. AVC) and

recommendations for how one might adjust the system to prevent the denial

in the future.

In a standard configuration setroubleshoot is composed of two components,

sealert and setroubleshootd.

setroubleshootd is a system daemon which runs under setroubleshoot user

and listens for audit events emitted from the kernel related to

SELinux. When the setroubleshootd daemon sees an SELinux AVC denial it

runs a series of analysis plugins which examine the audit data related

to the AVC. It records the results of the analysis and signals any

clients which have attached to the setroubleshootd daemon that a new

alert has been seen.

setroubleshootd is not persistent and only runs when there are new AVCs

to be analyzed. It is executed using setroubleshootd.service, which

also limits its priority and maximum RAM utilization to 1GB, in order to help with system responsiveness in case of large amounts of AVCs.

OPTIONS

`-f --nofork`

Do not fork the daemon

`-d --debug`

Do not exit after 10 seconds of inactivity

`-h --help`

Show this message

`-c --config`

`section.option=value` set a configuration value

AUTHOR

This man page was written by Dan Walsh <dwalsh@redhat.com>.

SEE ALSO

`sealert(8)`, `selinux(8)`

20100520

`setroubleshootd(8)`