Rocky Enterprise Linux 9.2 Manual Pages on command 'firewalld.lockdown-whitelist.5'

$ man firewalld.lockdown-whitelist.5

FIREWALLD.LOCKDOWN(5) firewalld.lockdown-whitelist FIREWALLD.LOCKDOWN(5)

NAME

firewalld.lockdown-whitelist - firewalld lockdown whitelist

configuration file

SYNOPSIS

/etc/firewalld/lockdown-whitelists.xml

DESCRIPTION

The firewalld lockdown-whitelist configuration file contains the

selinux contexts, commands, users and user ids that are white-listed

when firewalld lockdown feature is enabled (see firewalld.conf(5) and

firewall-cmd(1)).

This example configuration file shows the structure of an

lockdown-whitelist file:

```
<?xml version="1.0" encoding="utf-8"?>
<whitelist>
  <selinux context="selinuxcontext"/>
  <command name="commandline[*]"/>
  <user {name="username|id="userid"}/>
```

</whitelist>

OPTIONS

The config can contain these tags and attributes. Some of them are mandatory, others optional.

whitelist

The mandatory whitelist start and end tag defines the lockdown-whitelist. This tag can only be used once in a lockdown-whitelist configuration file. There are no attributes for this.

selinux

Is an optional empty-element tag and can be used several times to have more than one selinux contexts entries. A selinux entry has exactly one attribute:

context="string"

The context is the security (SELinux) context of a running application or service.

To get the context of a running application use ps -e --context and search for the application that should be white-listed.

Warning: If the context of an application is unconfined, then this will open access for more than the desired application.

command

Is an optional empty-element tag and can be used several times to have more than one command entry. A command entry has exactly one attribute:

name="string"

The command string is a complete command line including path and also attributes.

If a command entry ends with an asterisk '*', then all command lines starting with the command will match. If the '*' is not there the absolute command inclusive arguments must match.

Commands for user root and others is not always the same, the used path depends on the use of the PATH environment variable.

user

Is an optional empty-element tag and can be used several times to

white-list more than one user. A user entry has exactly one attribute of these:

name="string"

The user with the name string will be white-listed.

id="integer"

The user with the id userid will be white-listed.

SEE ALSO

firewall-applet(1), firewalld(1), firewall-cmd(1), firewall-config(1), firewalld.conf(5), firewalld.direct(5), firewalld.dbus(5), firewalld.icmptype(5), firewalld.lockdown-whitelist(5), firewall-offline-cmd(1), firewalld.richlanguage(5), firewalld.service(5), firewalld.zone(5), firewalld.zones(5), firewalld.policy(5), firewalld.policies(5), firewalld.ipset(5), firewalld.helper(5)

NOTES

firewalld home page:

http://firewalld.org

More documentation with examples:

http://fedoraproject.org/wiki/FirewallD

AUTHORS

Thomas Woerner <twoerner@redhat.com>

Developer

Jiri Popelka <jpopelka@redhat.com>

Developer

Eric Garver <eric@garver.life>

Developer