



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

Rocky Enterprise Linux 9.2 Manual Pages on command 'selinux_config.5'

\$ man selinux_config.5

selinux_config(5) SELinux configuration file selinux_config(5)

NAME

config - The SELinux sub-system configuration file.

DESCRIPTION

The SELinux config file controls the state of SELinux regarding:

1. The policy enforcement status - enforcing, permissive or disabled.
2. The policy name or type that forms a path to the policy to be loaded and its supporting configuration files.
3. How SELinux-aware login applications should behave if no valid SELinux users are configured.
4. Whether the system is to be relabeled or not.

The entries controlling these functions are described in the FILE FOR? MAT section.

The fully qualified path name of the SELinux configuration file is /etc/selinux/config.

If the config file is missing or corrupt, then no SELinux policy is loaded (i.e. SELinux is disabled).

The `sestatus (8)` command and the `libselinux` function `selinux_path (3)` will return the location of the config file.

FILE FORMAT

The config file supports the following parameters:

`SELINUX` = enforcing | permissive | disabled

`SELINUXTYPE` = policy_name

`REQUIRESEUSERS` = 0 | 1

`AUTORELABEL` = 0 | 1

Where:

SELINUX

This entry can contain one of three values:

enforcing

SELinux security policy is enforced.

permissive

SELinux security policy is not enforced but logs the warnings (i.e. the action is allowed to proceed).

disabled

No SELinux policy is loaded. This option was used to disable SELinux completely, which is now deprecated.

Use the `selinux=0` kernel boot option instead (see `selinux(8)`).

The entry can be determined using the `sestatus(8)` command or `selinux_getenforcemode(3)`.

SELINUXTYPE

The `policy_name` entry is used to identify the policy type, and becomes the directory name of where the policy and its configuration files are located.

The entry can be determined using the `sestatus(8)` command or `selinux_getpolicytype(3)`.

The `policy_name` is relative to a path that is defined within the SELinux subsystem that can be retrieved by using `selinux_path(3)`. An example entry retrieved by `selinux_path(3)`

is:

`/etc/selinux/`

The `policy_name` is then appended to this and becomes the 'policy root' location that can be retrieved by `selinux_policy_root_path(3)`. An example entry retrieved is:

`/etc/selinux/targeted`

The actual binary policy is located relative to this directory and also has a policy name pre-allocated. This information can be retrieved using `selinux_binary_policy_path(3)`. An example entry retrieved by `selinux_binary_policy_path(3)` is:

`/etc/selinux/targeted/policy/policy`

The binary policy name has by convention the SELinux policy version that it supports appended to it. The maximum policy version supported by the kernel can be determined using the `sestatus(8)` command or `security_policyvers(3)`. An example binary policy file with the version is:

`/etc/selinux/targeted/policy/policy.24`

REQUIRESEUSERS

This optional entry can be used to fail a login if there is no matching or default entry in the `seusers(5)` file or if the `seusers` file is missing.

It is checked by `getseuserbyname(3)` that is called by SELinux-aware login applications such as `PAM(8)`.

If set to 0 or the entry missing:

`getseuserbyname(3)` will return the GNU / Linux user name as the SELinux user.

If set to 1:

`getseuserbyname(3)` will fail.

The `getseuserbyname(3)` man page should be consulted for its use.

The format of the `seusers` file is shown in `seusers(5)`.

AUTORELABEL

This is an optional entry that allows the file system to be relabeled.

If set to 0 and there is a file called `.autorelabel` in the root

directory, then on a reboot, the loader will drop to a shell where a root login is required. An administrator can then manually relabel the file system.

If set to 1 or no entry present (the default) and there is a .autorelabel file in the root directory, then the file system will be automatically relabeled using fixfiles -F restore

In both cases the /.autorelabel file will be removed so that relabeling is not done again.

EXAMPLE

This example config file shows the minimum contents for a system to run SELinux in enforcing mode, with a policy_name of 'targeted':

```
SELINUX = enforcing
```

```
SELINUXTYPE = targeted
```

SEE ALSO

selinux(8), sestatus(8), selinux_path(3), selinux_policy_root_path(3), selinux_binary_policy_path(3), getseuserbyname(3), PAM(8), fixfiles(8), selinux_mkload_policy(3), selinux_getpolicytype(3), security_policy(8), selinux_getenforcemode(3), seusers(5)

Security Enhanced Linux 18 Nov 2011 selinux_config(5)