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

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

$ man selinux.8

selinux(8) SELinux Command Line documentation selinux(8)

NAME

SELinux - NSA Security-Enhanced Linux (SELinux)

DESCRIPTION

NSA Security-Enhanced Linux (SELinux) is an implementation of a flexi? ble mandatory access control architecture in the Linux operating sys? tem. The SELinux architecture provides general support for the en? forcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement?, Role- Based Access Control, and Multi-Level Security. Background information and techni? cal documentation about SELinux can be found at https://github.com/SELinuxProject.

The /etc/selinux/config configuration file controls whether SELinux is enabled or disabled, and if enabled, whether SELinux operates in per? missive mode or enforcing mode. The SELINUX variable may be set to any one of disabled, permissive, or enforcing to select one of these op? tions. The disabled disables most of the SELinux kernel and applica? tion code, leaving the system running without any SELinux protection.

The permissive option enables the SELinux code, but causes it to oper? ate in a mode where accesses that would be denied by policy are permit? ted but audited. The enforcing option enables the SELinux code and causes it to enforce access denials as well as auditing them. permis? sive mode may yield a different set of denials than enforcing mode,

both because enforcing mode will prevent an operation from proceeding past the first denial and because some application code will fall back to a less privileged mode of operation if denied access.

NOTE: Disabling SELinux by setting SELINUX=disabled in /etc/selinux/config is deprecated and depending on kernel version and configuration it might not lead to SELinux being completely disabled. Specifically, the SELinux hooks will still be executed internally, but the SELinux policy will not be loaded and no operation will be denied. In such state, the system will act as if SELinux was disabled, although some operations might behave slightly differently. To properly disable SELinux, it is recommended to use the selinux=0 kernel boot option in? stead. In that case SELinux will be disabled regardless of what is set in the /etc/selinux/config file.

The /etc/selinux/config configuration file also controls what policy is active on the system. SELinux allows for multiple policies to be in? stalled on the system, but only one policy may be active at any given time. At present, multiple kinds of SELinux policy exist: targeted, mls for example. The targeted policy is designed as a policy where most user processes operate without restrictions, and only specific services are placed into distinct security domains that are confined by the policy. For example, the user would run in a completely unconfined domain while the named daemon or apache daemon would run in a specific domain tailored to its operation. The MLS (Multi-Level Security) pol? icy is designed as a policy where all processes are partitioned into fine-grained security domains and confined by policy. MLS also sup? ports the Bell And LaPadula model, where processes are not only con? fined by the type but also the level of the data.

You can define which policy you will run by setting the SELINUXTYPE en? vironment variable within /etc/selinux/config. You must reboot and possibly relabel if you change the policy type to have it take effect on the system. The corresponding policy configuration for each such policy must be installed in the /etc/selinux/{SELINUXTYPE}/ directo? ries.

A given SELinux policy can be customized further based on a set of com? pile-time tunable options and a set of runtime policy booleans. system-config-selinux allows customization of these booleans and tun? ables.

Many domains that are protected by SELinux also include SELinux man pages explaining how to customize their policy.

FILE LABELING

All files, directories, devices ... have a security context/label asso? ciated with them. These context are stored in the extended attributes of the file system. Problems with SELinux often arise from the file system being mislabeled. This can be caused by booting the machine with a non SELinux kernel. If you see an error message containing file_t, that is usually a good indicator that you have a serious problem with file system labeling.

The best way to relabel the file system is to create the flag file /.autorelabel and reboot. system-config-selinux, also has this capa? bility. The restorecon/fixfiles commands are also available for rela? beling files.

Please note that using mount flag nosuid also disables SELinux domain transitions, unless permission nosuid_transition is used in the policy to allow this, which in turn needs also policy capability nnp_no? suid_transition.

AUTHOR

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

FILES

/etc/selinux/config

SEE ALSO

booleans(8), setsebool(8), sepolicy(8), system-config-selinux(8), togglesebool(8), restorecon(8), fixfiles(8), setfiles(8), semanage(8), sepolicy(8)

Every confined service on the system has a man page in the following format:

<servicename>_selinux(8)

For example, httpd has the httpd_selinux(8) man page.

man -k selinux

Will list all SELinux man pages.