

NAME

SELinux – NSA Security-Enhanced Linux (SELinux)

DESCRIPTION

NSA Security-Enhanced Linux (SELinux) is an implementation of a flexible mandatory access control architecture in the Linux operating system. The SELinux architecture provides general support for the enforcement 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 technical documentation about SELinux can be found at <http://www.nsa.gov/research/selinux>.

The */etc/selinux/config* configuration file controls whether SELinux is enabled or disabled, and if enabled, whether SELinux operates in permissive mode or enforcing mode. The **SELINUX** variable may be set to any one of disabled, permissive, or enforcing to select one of these options. The disabled option completely disables the SELinux kernel and application code, leaving the system running without any SELinux protection. The permissive option enables the SELinux code, but causes it to operate in a mode where accesses that would be denied by policy are permitted but audited. The enforcing option enables the SELinux code and causes it to enforce access denials as well as auditing them. Permissive 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.

The */etc/selinux/config* configuration file also controls what policy is active on the system. SELinux allows for multiple policies to be installed 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) policy is designed as a policy where all processes are partitioned into fine-grained security domains and confined by policy. MLS also supports the Bell And LaPadula model, where processes are not only confined by the type but also the level of the data.

You can define which policy you will run by setting the **SELINUXTYPE** environment 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}/* directories.

A given SELinux policy can be customized further based on a set of compile-time tunable options and a set of runtime policy booleans. **system-config-selinux** allows customization of these booleans and tunables.

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 associated 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 capability. The **restorcon/fixfiles** commands are also available for relabeling files.

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.