(/) **Wiki**

SELinux/Tutorials/How is the policy provided and loaded

From Gentoo Wiki

< SELinux (/wiki/SELinux) | Tutorials (/wiki/SELinux/Tutorials)

Contents

How is the policy provided and loaded?

We have been talking about SELinux policies for a while, and even seen as few of the supported statements (through the output of the **sesearch** command). Let's have a look at how policies are truly provided and loaded on the system.

SELinux uses policy modules

SELinux borrowed the concept of modules from the Linux kernel and implemented a similar approach for its policies. Just as you can dynamically add in (and remove) driver support in the Linux kernel through kernel modules, you can add in (and remove) policies using SELinux modules.

The list of SELinux modules that are currently loaded on a system can be obtained with **semodule -l**.

```
root # semodule -l
```

```
alsa    1.11.4
apache  2.6.10
apm     1.11.4
application     1.2.0
...
```

On some distributions, you can even get information about each module through automatically generated man pages, like with **man selinux_apache**. This isn't the case for Gentoo Linux (yet) though.

Modules can be loaded into and removed from memory using the same **semodule** tool, which we will see later in this tutorial.

The policy store

SELinux uses a *policy store* to keep track of its loaded policy modules and related settings. The active policy store name can be obtained from **sestatus** (look for the *Loaded policy name* line):

```
root # sestatus | grep Loaded
```

```
Loaded policy name:    strict
```

The policy store that should be active upon boot is configured in `/etc/selinux/config` through the *SELINUXTYPE* setting.

```
root # grep ^SELINUXTYPE /etc/selinux/config
```

```
SELINUXTYPE=strict
```

In the remainder of this tutorial, we will assume that the active policy is called "strict". When you see a command or path that uses "strict" inside, you might need to change that to the policy store name active on your system (which is either *targeted*, *mcs* or *mls* - most non-Gentoo distributions use *targeted*).

Installing the SELinux policy

Most binary distributions build the SELinux policy in advance, and provide packages that install the binary modules on the file system. Gentoo of course builds the policy through its package management, but in the end, the binary policy modules will be installed on the file system as well. Installing the files on the file system *does not enable* the policy. Unlike with Linux kernel modules, which can be automatically loaded (if needed) when they are located in the right directory, SELinux requires policy modules to be explicitly loaded (by the administrator or through its configuration).

On most systems, the policy files are stored in `/usr/share/selinux/strict`. If you take a look in this directory, you will find lots of files with the `.pp` suffix:

```
user $ ls /usr/share/selinux/targeted
```

```
alsa.pp
apache.pp
apm.pp
application.pp
...
```

These files are provided by the policy packages (in Gentoo, these are the packages in the *sec-policy* category). Each of these files might show up in the output of **semodule -l** *except* for the `base.pp` file. This is a special one: it is the base policy, comparable to the Linux kernel itself (if we compare modular design) as the kernel itself is also not displayed if you use **lsmod**.

Loading the SELinux policies

When SELinux is enabled, these files need to be loaded in memory. What happens is that these files are read in (through **semodule** again) and combined in the active policy. This policy is then loaded in memory (at which point in time the policy takes effect). The full binary policy as it is loaded in memory can be found at `/etc/selinux/strict/policy` and is usually called `policy.##` where ## is a version telling the management utilities which SELinux features are supported. Most of the time, you don't need to concern you with this version information.

The SELinux modules that are currently loaded are also to be found in the `/etc/selinux/strict` location: they are contained in the `modules/active/modules` subdirectory. Because they are copied there before loaded, it allows an administrator to verify if the policy modules installed by the package manager (in `/usr/share/selinux/strict`) are the ones that are loaded:

```
user $ sha1sum /usr/share/selinux/strict/alsa.pp
/etc/selinux/strict/modules/active/modules/alsa.pp
```

```
86e7c57920ad1a8c28d08dd97bfc5386ba13693b  /usr/share/selinux/strict/alsa.pp
86e7c57920ad1a8c28d08dd97bfc5386ba13693b  /etc/selinux/strict/modules/active/modules/alsa
```

Effectively loading the policies in memory is done through the distribution support of SELinux. In Gentoo, this is done at install time of the various sec-policy packages, which calls **semodule** with the proper arguments.

```
root # cd /usr/share/selinux/strict; semodule -i alsa.pp
```

Similarly, deinstalling the package removes the policy from memory (in this case, the module name is used, not the module file name).

```
root # semodule -r alsa
```

Sometimes an update requires the entire policy (including base policy) to be loaded. SELinux supports full reloads - all you need to do is add in **-b base.pp** to tell the management utilities where the base policy module can be found. But again, most of the time this is done through the distribution.

```
root # cd /usr/share/selinux
root # semodule -b base.pp -i alsa.pp -i apache.pp -i apm.pp -i application.pp -i ...
```

Disabling policy modules

You can also opt to disable policy modules. This way, the part of the policy that is provided by the policy module is not active anymore.

```
root # semodule -d alsa
root # semodule -l
```

```
alsa    1.11.4  Disabled
apache  2.6.10
...
```

What you need to remember

What you should remember from this tutorial is that

- SELinux uses a modular design for its policies, similar as how the Linux kernel uses modules
- a policy store is used to keep track of loaded policy modules and settings, and is governed through the *SELINUXTYPE* setting in `/etc/selinux/config`
- the **semodule** tool is used to load, unload, ... SELinux policies

Retrieved from "http://wiki.gentoo.org/index.php?title=SELinux/Tutorials/How_is_the_policy_provided_and_loaded&oldid=709148 (http://wiki.gentoo.org/index.php?title=SELinux/Tutorials/How_is_the_policy_provided_and_loaded&oldid=709148)"

Category (/wiki/Special:Categories): SELinux (/wiki/Category:SELinux)

- This page was last modified on 16 February 2018, at 15:53.