SE-LINXU

Tuesday, June 21, 2022 10:45 AM

SELinux is implemented to provide an additional layer of protection, increase the control over processes execution, and protects against exploits by using multi level security.

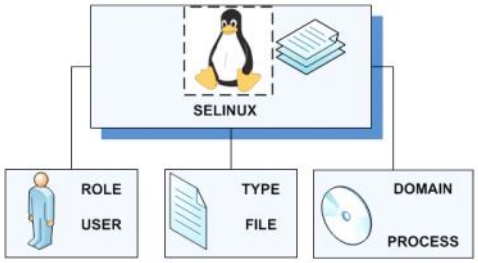
SELinux works by using Labels and Type Enforcement.This can be also described in the format :

[SELinux User =system_u]:[SELinux Role=object_r]:[SELinux Domain/Type label=ssh_exec_t]:[SELinux MCS/MLS Label=s0]

For example , “sshd” service executable configuration directory is labeled ssh_exec_t as seen below using the command utility ls -Z as shown below:

```
root@server:~$ ls -lZ /usr/bin/ssh
-rwxr-xr-x. root root system_u:object_r:ssh_exec_t:s0  /usr/bin/ssh
```

Type Enforcement its the part where the policy dictates if for example within ssh process context running label ssh_exec_t to interact with a ssh file label.



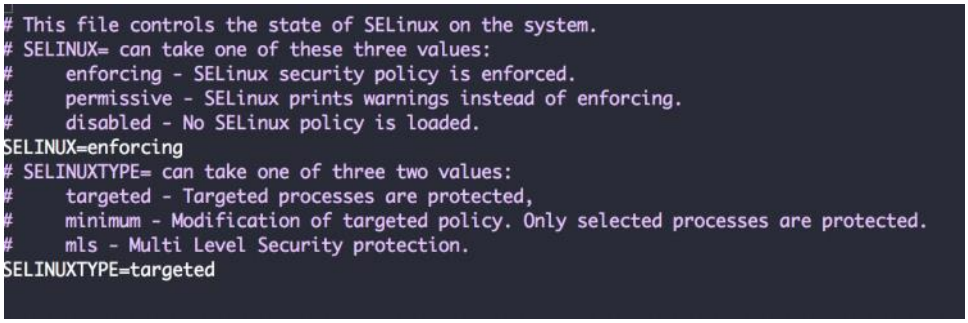
There are two policies that can be used :

Targeted Policy : The default policy
Minimum
Multi-Level/Multi Category Security-(MLS) Policy: Can be enabled.
SElinux has three modes of operation:

Enforcing
Disabled
Permissive
The modes of operation and the policy types are embedded inside “config” file which controls the state of the SELinux on the system.

The file can be accessed using vim tool at

vi /etc/selinux/config



SELinux Folder Structure

Below are some snippets of the SELinux folder structure and some of the files utilized by the application.

The /etc/selinux directory is the main location for all policy and configuration files.

Based on SELinux type on /etc/selinux/config we could also have addition folders. Since SElinuxType is set to Targeted a targeted folder is created.

The directory targeted or strict depending on your SElinuxType are the locations where their policy files are contained.