Beware of a funny side effect with SELinux.

Use case

We have to activate SSL/TLS on the Linux server, AlmaLinux in my case (RedHat variant).

SELinux (Security Enhanced Linux) in enabled by default.

I upload certificates and private key on /tmp directory, then I move these two files on the target directory /etc/ssl/certs/ (with the `mv` command).

When restarting httpd, it complaigns because it can’t access the two certificate files.
We can set all security flags that we want, « open all the doors », that will not run.

In fact, the solution is to re-label the certificate files because the SELinux inheritance rules are specific to the directory which contains certificates. Then, the two new files will be setup correctly.

```
restorecon -RvF /etc/ssl/certs/
```

Or… we can disable SELinux.
Display the status
`getenforce`

Disable SELInux until next reboot

```
sudo setenforce 0
```

This would not have happened if I had copied (and not moved) my certificate files because in this case, they would have automatically inherited the SELinux rules from the receiving directory

Author

- 

  Patrick

  GPM Factory