SE LINUX

SElinux provides a critical security purpose in Linux .which is more than a user and group permission, which enables features that support security policies for access control, including mandatory access control (MAC)

SElinux has three modes:

• Enforcing: SElinux is enforcing access control rules. Computers generally run in this mode.

• Permissive: SElinux is active but instead of enforcing access control rules, it is recording warnings that rules have been violated. This mode is used primarily for testing and troubleshooting

• Disabled: SElinux is turned off entirely: no SElinux violations are denied, nor even recorded. Discouraged!

SElinux is a set of security rules that determine which process can access which files, directories, and ports. Every file, process, directory, and port has a special security label called an SElinux context.

Changing SElinux mode

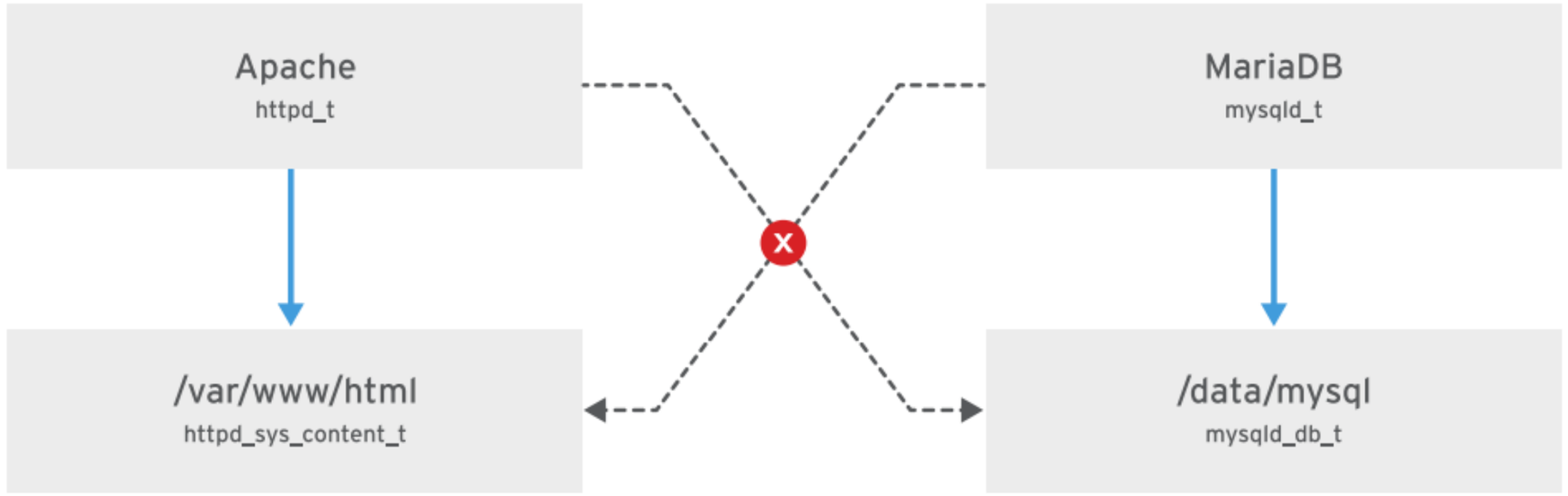
#getenforce

#setenforce 0 |1

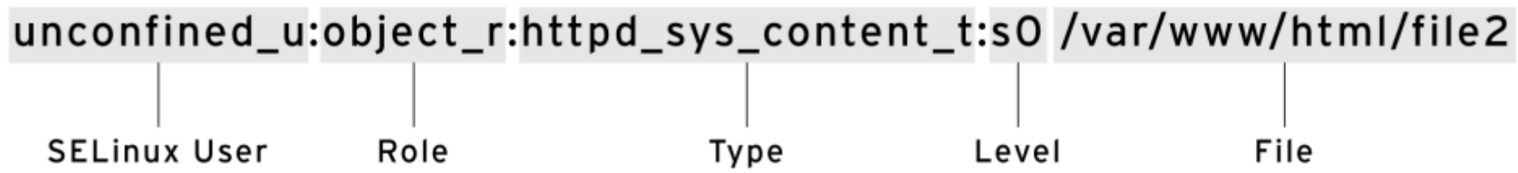
Or

/etc/selinux/config

/etc/sysconfig/selinux



CONTROLLING SELINUX FILE CONTEXTS



#chcon –t (this is fortemporary)

#restorecon (restore to defaults)

 # semanage fcontext (for permanent)

SELINUX BOOLEANS

A given SElinux policy can be customized by enabling or disabling a set of policy Booleans. Booleans allow parts of SELinux policy to be changed at run time, without any knowledge of SElinux policy writing. This allows changes without reloading or recompiling SELinux policy.

#semanage Boolean –l (list, status with description)

#getsebool –a (without description)

```
# setsebool [Boolean] on|off
```

/sys/fs/selinux Directory

You can also view and change the value of Booleans in the /sys/fs/selinux directory. The Boolean files are stored in the /sys/fs/selinux/booleans directory:

INVESTIGATING AND RESOLVING SELINUX ISSUES

TROUBLESHOOTING SELINUX ISSUES

1. **Need to check is it working?**
2. **Restorecon**
3. **Boolean**

MONITORING SELINUX VIOLATIONS

Install the setroubleshoot-server package to send SELinux messages to /var/log/messages. setroubleshoot-server

#sealetr –l uuid (to produce report)