What is SELinux?

SELinux is a label based security system

Every process has a label, every object on the system has a label

Files, Directories, network ports …

The SELinux policy controls how process labels interact with other labels on the system

The kernel enforces the policy rules

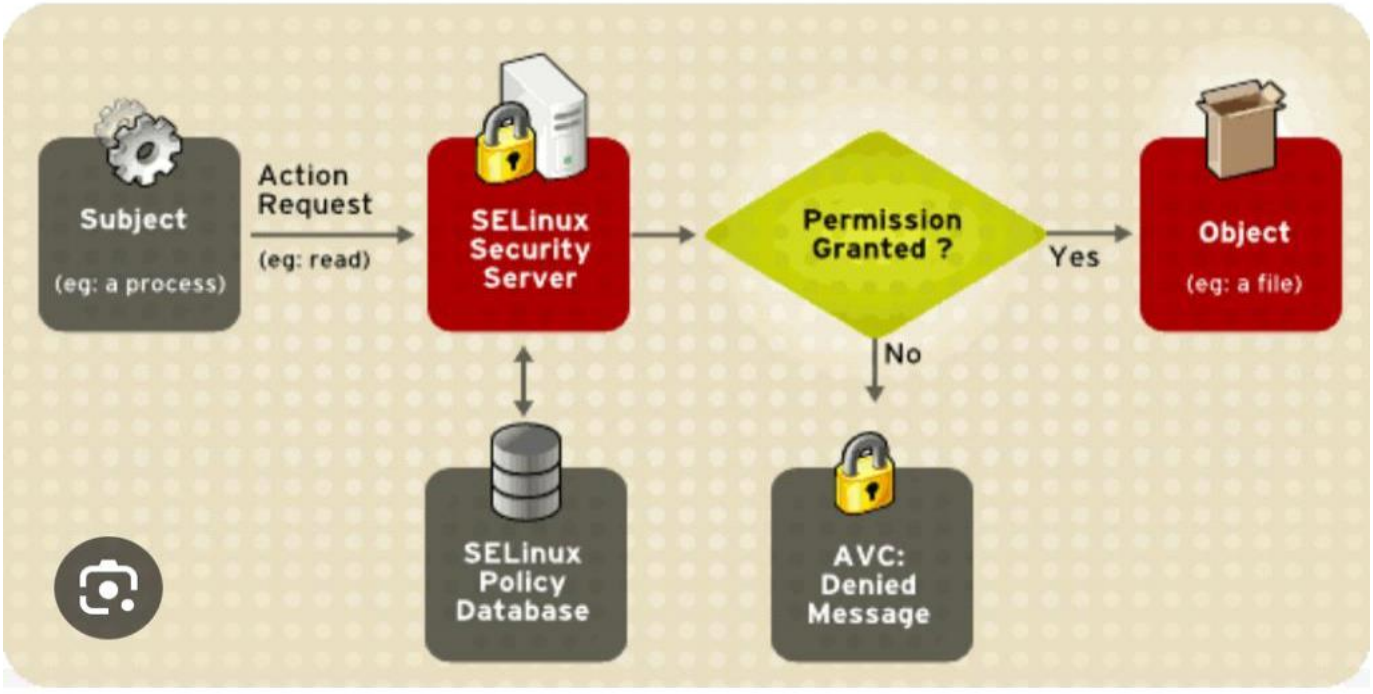
SELinux is set in three modes.

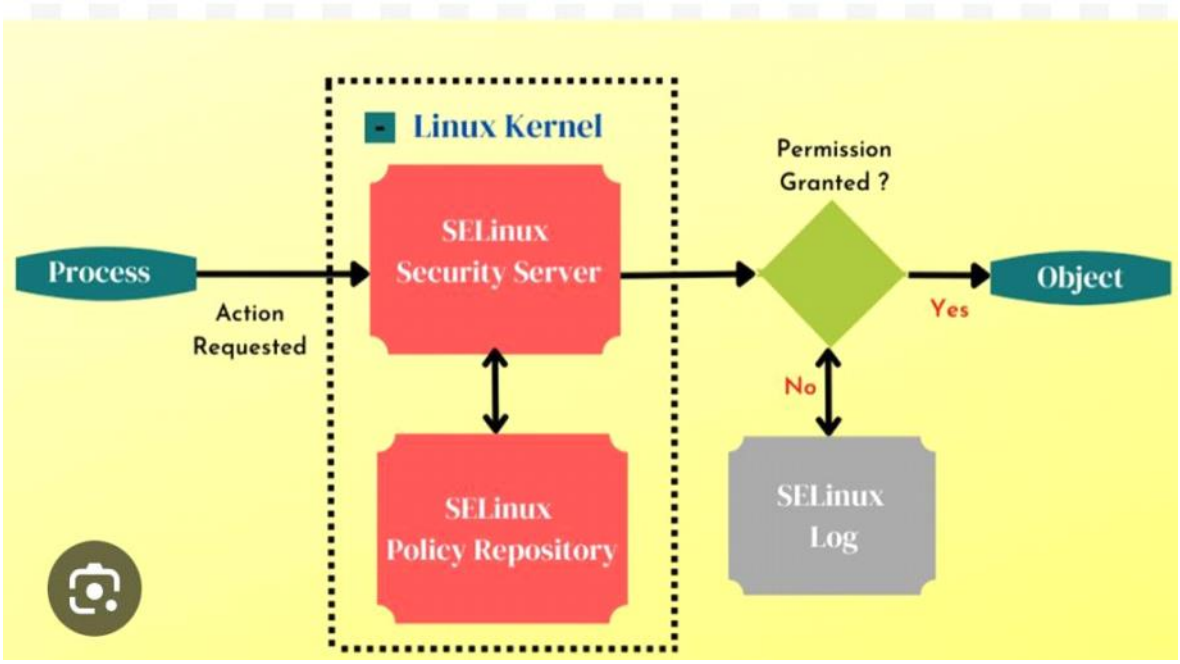
- **Enforcing** – SELinux security policy is enforced. IF this is set SELinux is enabled and will try to enforce the SELinux policies strictly
- **Permissive** – SELinux prints warnings instead of enforcing. This setting will just give warning when any SELinux policy setting is breached
- **Disabled** – No SELinux policy is loaded. This will totally disable SELinux policies.

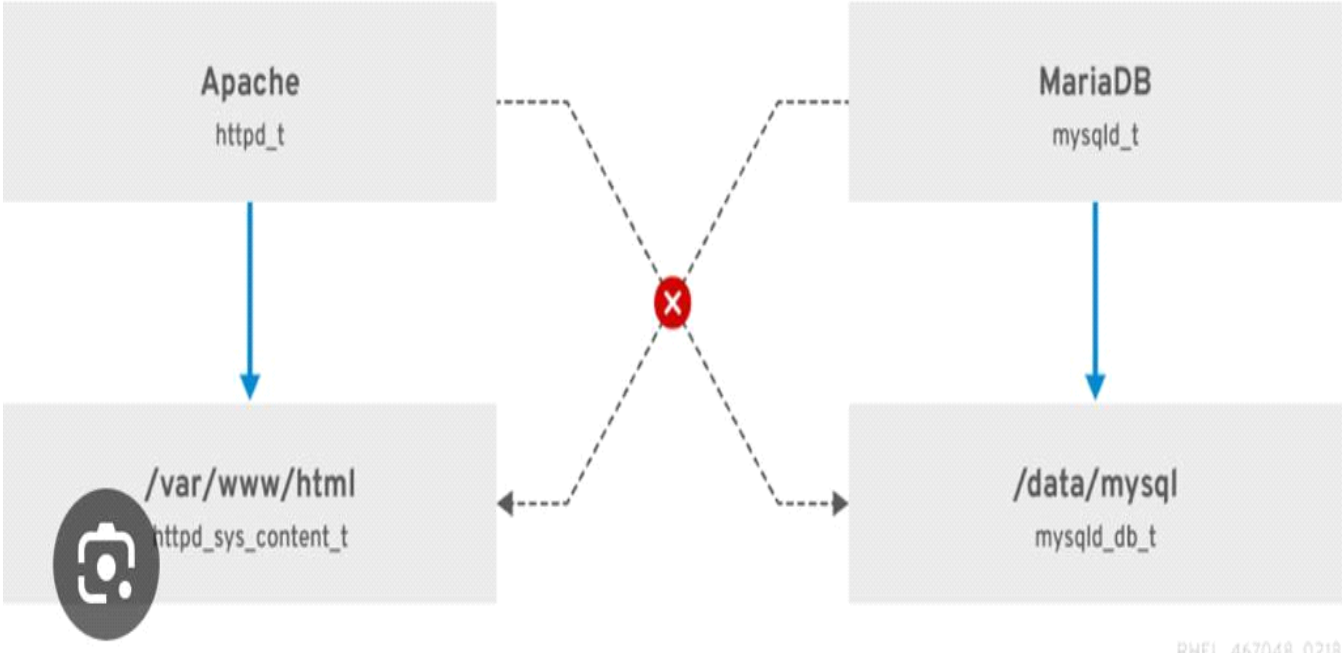
SELinux policies

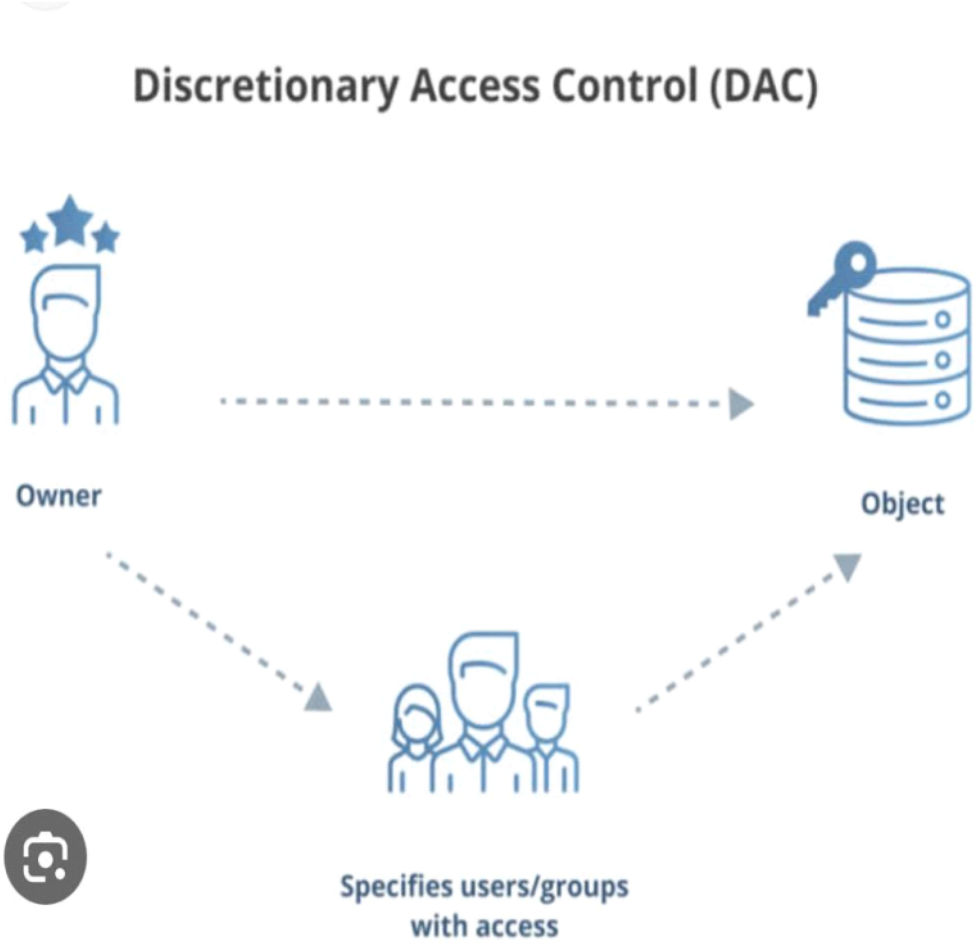
SELinux allows for multiple policies to be installed on the system, but only one policy may be active at any given time. At present, two kinds of SELinux policy exist

- **Targeted** – The targeted policy is designed as a policy where most processes operate without restrictions, and only specific ser-vices are placed into distinct security domains that are confined by the policy.
- **Strict** – The strict policy is designed as a policy where all processes are partitioned into fine-grained security domains and confined by policy.




Linux Kernel
Process
Action Requested
SELinux Security Server
SELinux Policy Repository
Permission Granted ?
Yes
No
Object
SELinux Log


Apache
httpd_t
MariaDB
mysqld_t
/var/www/html
httpd_sys_content_t
/data/mysql
mysqld_db_t
RHEL_467048_0218


Discretionary Access Control (DAC)
Owner
Object
Specifies users/groups
with access

DAC VERSUS MAC

DAC	MAC
A type of access control in which the owner of a resource restricts access to the resource based on the identity of the users	A type of access control that restricts the access to the resources based on the clearance of the subjects
Stands for Discretionary Access Control	Stands for Mandatory Access Control
Resource owner determines who can access and what privileges they have	Provides access to the users depending on the clearance level of the users. Access is determined by the system
More flexible	Less flexible
Not as secure as MAC	More secure
Easier to implement	Comparatively less easier to implement

Discretionary access control (DAC) vs. mandatory access control (MAC)

Traditionally, Linux and UNIX systems have used DAC. SELinux is an example of a MAC system for Linux.

With DAC, files and processes have owners. You can have the user own a file, a group own a file, or other, which can be anyone else. Users have the ability to change permissions on their own files.

The root user has full access control with a DAC system. If you have root access, then you can access any other user's files or do whatever you want on the system.

But on MAC systems like SELinux, there is administratively set policy around access. Even if the DAC settings on your home directory are changed, an SELinux policy in place to prevent another user or process from accessing the directory will keep the system safe.

SELinux policies let you be specific and cover a large number of processes. You can make changes with SELinux to limit access between users, files, directories, and more.