SELinux Reference

SELinux

What is SELinux?

SElinux is a Security-Enhanced Linux – a framework for securely managing processes, users and files on your **Red Hat Enterprise Linux OS**.

If you're using a Red Hat based system or one of the distros based on it – CentOS Linux or Fedora Linux desktop, you probably have **SELinux** enabled by default.

SELinux Basics

First of all, confirm **SELinux status**: it's going to be in one of these three modes:

- **enforcing** – normal operation of SELinux, meaning access is controlled and any access attempts are logged for later inspection. You can actively manage access and SELinux contexts for files .
- **permissive** – SELinux engine is active, but no controls are enforced – everything is allowed but captured in audit log files so that you can use the logs to later create SELinux policy before switching into SELinux Enforcing mode.
- **disabled** – SELinux is fully disabled, completely inactive. This means, among other things, that files created in this mode may not get any SELinux control assigned right away.

You may want to **enable SELinux** or **disable SELinux** depending on your scenario.

Working with SELinux

Everything under SELinux control is managed by SELinux policy and its objects. Processes, users and files have SELinux contexts. It's easy enough to **list SELinux contexts for files** and to show SELinux contexts for processes.

SELinux Context

SELinux context is the combination of such additional information:

- user
- role
- type
- level

You can **review audit logs for SELinux events** to understand requirements of a particular application and later use the same logs to create SELinux module – special set of rules that can be compiled and activated to expand existing SELinux policy.

SELinux has its own users – identities that you can create and map to existing real Linux users in your system.

Advanced SELinux Usage

Learn how to **use sestatus command for reporting SELinux state of key OS files** – you get a listing of important configuration files and indication whether their SELinux contexts are what they should be.

See Also

- Red Hat Enterprise Linux
- RHEL 8