SELinux Mandatory access control

CONCEPTS

Never disable SELinux to make something work. Switch to permissive, reproduce, read the denial, then fix the label, boolean or port.

Process domain, e.g. httpd_t
↓ wants access to
Object file or port type
↓ checked by
Policy allow rules + booleans
↓ no rule
Denied AVC in audit.log

Reading a context

Part	Example	Matters for
user	`system_u`	confined users
role	`object_r`	rarely
type	`etc_t`	almost every rule
level	`s0`	MLS/MCS, containers

Normal permissions are checked first; SELinux can only deny more, never grant what they forbid.

MODE AND STATUS

`getenforce`
Show the current mode

`sestatus`
Full status: mode, config, policy

`setenforce 0`
Switch to permissive until reboot

`setenforce 1`
Switch back to enforcing

`semanage permissive -a <domain>`
Make one domain permissive

`semanage permissive -d <domain>`
Enforce that domain again

`SELINUX=enforcing`
Boot mode in /etc/selinux/config

Modes

Mode	Effect
`enforcing`	denies and logs
`permissive`	logs only, allows
`disabled`	no checks, no labels kept

CONTEXTS

`ls -Z <path>`
Show file contexts

CONTEXTS (cont.)

`ls -dZ <dir>`
Context of the directory itself

`ps -eZ`
Show the domain of every process

`id -Z`
Your own user context

`matchpathcon -V <path>`
Check a label against the policy

mv keeps a file's old label; cp creates a new one from the target directory. Run restorecon after moving files into place.

FILE LABELS

`semanage fcontext -a -t <type> '<path>(/.*)?'`
Add a persistent label rule

`restorecon -Rv <path>`
Relabel files to match the rules

`restorecon -Rnv <path>`
Dry run: show what would change

`chcon -t <type> <file>`
Change a label temporarily

`semanage fcontext -a -e <src> <dst>`
Label dst like src (equivalence)

`semanage fcontext -l -C`
List your local label rules

`semanage fcontext -l | grep <path>`
Find the rule for a path

`semanage fcontext -d '<path>(/.*)?'`
Delete a local label rule

chcon or semanage?

Tool	After relabel
`chcon`	label lost: tests only
`semanage fcontext`	label kept: the real fix

BOOLEANS

`getsebool -a`
List all booleans and values

`getsebool <bool>`
Show one boolean

`setsebool -P <bool> on`
Set a boolean, persistently

BOOLEANS (cont.)

`setsebool <bool> on`
Set a boolean until reboot

`semanage boolean -l`
Booleans with descriptions

Common switches: httpd_can_network_connect, httpd_can_network_connect_db, httpd_use_nfs, httpd_enable_homedirs.

PORTS

`semanage port -l`
List port types

`semanage port -a -t <type> -p tcp <port>`
Allow a service on a port

`semanage port -d -t <type> -p tcp <port>`
Remove a local port rule

DENIALS

`ausearch -m AVC -ts recent`
Show denials of the last 10 minutes

`ausearch -m AVC -c <comm> -i`
Denials of one program, readable

`ausearch -m AVC -ts recent | audit2why`
Explain why access was denied

`sealert -l "*"`
Analysis with suggested fixes

`journalctl -t setroubleshoot`
setroubleshoot alerts in the journal

No AVC but still failing? Look for silenced denials (semodule -DB), then check plain permissions and the firewall.

POLICY MODULES

`ausearch -m AVC -ts recent | audit2allow -M <name>`
Build a module from denials

audit2allow is the last step: first rule out a wrong label, a boolean or a port type.

RELABEL AND USERS

`touch /.autorelabel`
Relabel everything at next boot