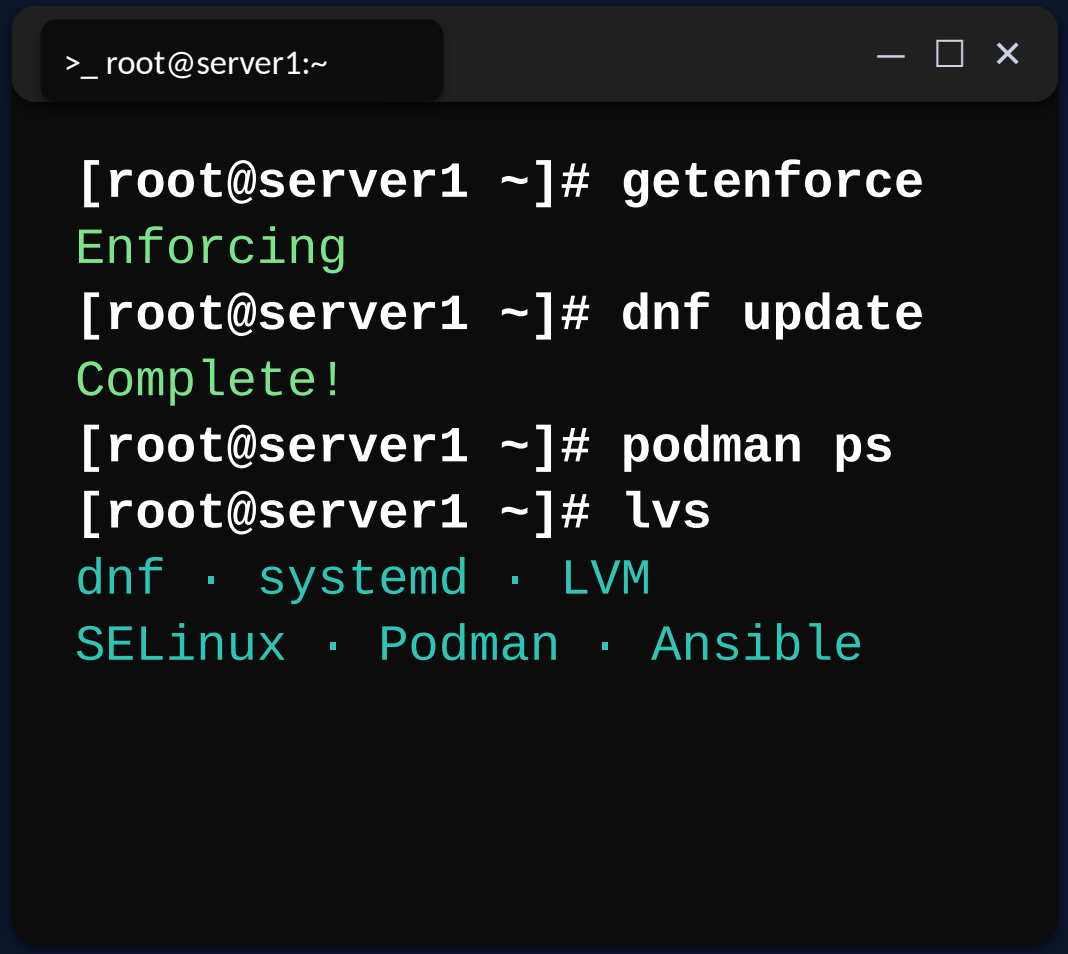


LESSON 9 OF 12

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

SELinux: Modes, Contexts, Booleans & Troubleshooting

Full Course · RHEL 10.3 & 9.9 (Nov 2026)

What You Will Learn in Lesson 9

- Why SELinux: mandatory access control
- Modes: enforcing, permissive, disabled
- Contexts: user, role, type, level
- Fixing file contexts: semanage fcontext and restorecon
- Booleans: switches for common needs
- Ports: semanage port
- Troubleshooting AVC denials: ausearch, sealert, audit2why

Why SELinux?

	Normal permissions (DAC)	SELinux (MAC)
Who decides	The owner of the file	A central policy from Red Hat
Based on	User, group, rwx	Labels (types) on processes and files
root	Bypasses everything	Is also limited by the policy
If a web server is hacked	Attacker gets all of apache's file access	Attacker is confined to web content types
Default in RHEL	Always on	Enforcing, targeted policy

Modes

```
[student@server1 ~]$ getenforce
Enforcing
[student@server1 ~]$ sestatus
SELinux status:                 enabled
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
[student@server1 ~]$ sudo setenforce 0      # permissive until reboot (testing only)
[student@server1 ~]$ sudo setenforce 1      # back to enforcing
[student@server1 ~]$ grep ^SELINUX= /etc/selinux/config
SELINUX=enforcing
```

Contexts: Labels on Everything

```
[student@server1 ~]$ ls -Z /var/www/html/index.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/index.html
[student@server1 ~]$ ls -Zd /home/student
unconfined_u:object_r:user_home_dir_t:s0 /home/student
[student@server1 ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0     1234 ?  00:00:01 httpd
[student@server1 ~]$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
# user : role : TYPE : level   — in the targeted policy, the TYPE matters most
```

The Classic Problem: Moved Files

```
[student@server1 ~]$ echo 'Hello from MyWebUniversity' > index.html
[student@server1 ~]$ sudo mv index.html /var/www/html/     # mv keeps the OLD label
[student@server1 ~]$ ls -Z /var/www/html/index.html
unconfined_u:object_r:user_home_t:s0 /var/www/html/index.html
[student@server1 ~]$ curl http://localhost/
<title>403 Forbidden</title>
[student@server1 ~]$ sudo restorecon -Rv /var/www/html
Relabeled /var/www/html/index.html from ...user_home_t:s0 to ...httpd_sys_content_t:s0
[student@server1 ~]$ curl http://localhost/
Hello from MyWebUniversity
```

Custom Locations: semanage fcontext

```
# Serve a web site from /srv/web (our LVM volume from Lesson 7)
[student@server1 ~]$ sudo semanage fcontext -a -t httpd_sys_content_t '/srv/web(/.*)?'
[student@server1 ~]$ sudo restorecon -Rv /srv/web
[student@server1 ~]$ ls -Zd /srv/web
system_u:object_r:httpd_sys_content_t:s0 /srv/web
[student@server1 ~]$ sudo semanage fcontext -l -C       # your local rules
[student@server1 ~]$ sudo semanage fcontext -l | grep '/var/www'
# chcon changes a label temporarily — a relabel or restorecon will undo it
```

Booleans: Policy Switches

```
[student@server1 ~]$ getsebool -a | grep httpd | head
httpd_can_network_connect --> off
httpd_can_sendmail --> off
httpd_enable_homedirs --> off
[student@server1 ~]$ sudo semanage boolean -l | grep httpd_can_network_connect
httpd_can_network_connect (off, off)  Allow httpd to can network connect
[student@server1 ~]$ sudo setsebool -P httpd_can_network_connect on   # -P = permanent
[student@server1 ~]$ sudo setsebool -P httpd_enable_homedirs on
[student@server1 ~]$ sudo semanage boolean -l -C        # booleans you changed
```

Ports: semanage port

```
[student@server1 ~]$ sudo semanage port -l | grep -w http_port_t
http_port_t     tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
# Run Apache on port 8888:
[student@server1 ~]$ sudo semanage port -a -t http_port_t -p tcp 8888
[student@server1 ~]$ sudo firewall-cmd --permanent --add-port=8888/tcp ; sudo firewall-cmd --reload
[student@server1 ~]$ sudo systemctl restart httpd

# SSH on port 2222 (from Lesson 8):
[student@server2 ~]$ sudo semanage port -a -t ssh_port_t -p tcp 2222
[student@server2 ~]$ sudo semanage port -l -C
```

Troubleshooting Denials

```
[student@server1 ~]$ sudo ausearch -m AVC -ts recent
type=AVC msg=audit(...): avc:  denied  { read } for  pid=1234 comm="httpd"
  name="index.html" scontext=system_u:system_r:httpd_t:s0
  tcontext=unconfined_u:object_r:user_home_t:s0 tclass=file permissive=0
[student@server1 ~]$ sudo ausearch -m AVC -ts recent | audit2why
[student@server1 ~]$ sudo dnf install -y setroubleshoot-server
[student@server1 ~]$ sudo journalctl -t setroubleshoot --since '10 min ago'
[student@server1 ~]$ sudo sealert -a /var/log/audit/audit.log
... If you want to fix the label: # /sbin/restorecon -v /var/www/html/index.html
```

A Calm SELinux Method

Step	Do this
1	Confirm: does it work in permissive mode? (setenforce 0, test, setenforce 1)
2	Read the denial: ausearch -m AVC -ts recent, or sealert
3	Wrong file label? semanage fcontext -a + restorecon -Rv
4	Feature switch? setsebool -P <boolean> on
5	Non-standard port? semanage port -a -t <type> -p tcp <port>
6	Test again in enforcing mode; never leave it permissive or disabled
Remember	After a root password reset: touch /.autorelabel (Lesson 6)

Summary and Homework

- SELinux = labels + policy; keep it Enforcing
- ls -Z, ps -Z: the TYPE is what matters
- Wrong label → semanage fcontext -a + restorecon -Rv
- Booleans → setsebool -P; ports → semanage port -a
- Denials → ausearch -m AVC, sealert, audit2why
- Homework: serve /srv/web with Apache on port 8888 — fix the label, port and firewall, in enforcing mode

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

Slides for this lesson: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity · @MyWebUniversity-Dari

Wahidullah Lutfy — Founder and Director of IT of MyWebUniversity, and CS teacher

Book: The Direct Path to Linux Ubuntu (Amazon · Barnes & Noble)

Learn it, then pass it on.