درس ۹ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

SELinux: حالت‌ها، context ها، boolean ها و عیب‌یابی

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس نهم چه یاد می‌گیرید

- چرا SELinux: کنترل دسترسی اجباری
- حالت‌ها: enforcing، permissive، disabled
- Context ها: user، role، type، level
- اصلاح context فایل‌ها: semanage fcontext و restorecon
- Boolean ها: کلیدهایی برای نیازهای عام
- پورت‌ها: semanage port
- عیب‌یابی منع‌های AVC: ausearch، sealert، audit2why

چرا SELinux؟

SELinux (MAC)	اجازه‌های عادی (DAC)	
یک policy مرکزی از Red Hat	مالک فایل	چه کسی تصمیم می‌گیرد
برچسب‌ها (type) روی پروسس‌ها و فایل‌ها	کاربر، گروه، rwx	بر اساس
او هم توسط policy محدود است	از همه چیز عبور می‌کند	root
مهاجم به type های محتوای وب محدود است	مهاجم همه دسترسی فایل apache را می‌گیرد	اگر وب سرور هک شود
Enforcing، targeted policy	همیشه روشن	پیش‌فرض در RHEL

حالت‌ها

```
[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
```

Context ها: برچسب روی همه چیز

```
[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
```

مشکل کلاسیک: فایل‌های جابجا شده

```
[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
```

مکان‌های سفارشی: 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
```

Boolean ها: کلیدهای policy

```
[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
```

پورت‌ها: 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
```

عیب‌یابی منع‌ها

```
[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
```

یک روش آرام برای SELinux

قدم	این کار را کنید
۱	تأیید: آیا در حالت permissive کار می‌کند؟ (setenforce 0، آزمایش، setenforce 1)
۲	منع را بخوانید: ausearch -m AVC -ts recent، یا sealert
۳	برچسب فایل اشتباه؟ semanage fcontext -a + restorecon -Rv
۴	کلید ویژگی؟ setsebool -P <boolean> on
۵	پورت غیرعادی؟ <semanage port -a -t <type> -p tcp <port
۶	دوباره در حالت enforcing آزمایش کنید؛ هرگز permissive یا disabled نگذارید
به یاد داشته باشید	بعد از تنظیم دوباره رمز root: touch /.autorelabel (درس ۶)

خلاصه و کارخانگی

- SELinux = برچسب‌ها + policy؛ آن را Enforcing نگه دارید
- ls -Z، ps -Z: TYPE مهم است
- برچسب اشتباه ← semanage fcontext -a + restorecon -Rv
- Boolean ← setsebool -P؛ پورت‌ها ← semanage port -a
- منع‌ها ← ausearch -m AVC، sealert، audit2why
- کارخانگی: /srv/web را با Apache روی پورت 8888 سرو کنید — برچسب، پورت و فایروال را در حالت enforcing اصلاح کنید

تشکر از شما! 🤲

ویدیوها و PDF های رایگان: www.MyWebUniversity.com

سلایدهای این درس: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity-Dari · @MyWebUniversity

وحیدالله لطفی – مؤسس و رئیس IT مای وب یونیورسیتی، و استاد علوم کامپیوتر

یاد بگیرید و به دیگران انتقال دهید