درس ۴ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

کاربران، گروه‌ها، اجازه‌ها، ACL ها و sudo

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس چهارم چه یاد می‌گیرید

- کاربران، گروه‌ها، UID ها و فایل‌های پشت آن‌ها
- ساختن و مدیریت کاربران و گروه‌ها
- رمزها و کهنه شدن رمز
- اجازه‌های فایل: read، write، execute؛ chmod و chown
- اجازه‌های خاص: sticky bit، setgid؛ umask
- ACL ها برای دسترسی دقیق
- sudo و گروه wheel

کاربران و گروه‌ها: اساسات

جزئیات	مورد
UID 0: هر کاری می‌تواند	root
UID 1 تا 999: سرویس‌هایی مانند apache یا sshd را اجرا می‌کنند	کاربران سیستم
UID 1000 به بالا: انسان‌ها	کاربران عادی
هر کاربر یکی دارد؛ فایل‌های نو این گروه را می‌گیرند	گروه اصلی
گروه‌های بیشتر، مانند wheel برای مدیران	گروه‌های اضافی
uid=1000(student) gid=1000(student) groups=...,10(wheel)	id student

فایل‌های پشت کاربران

فایل	چه دارد
/etc/passwd	name:x:UID:GID:comment:home:shell — همه می‌توانند بخوانند
/etc/shadow	hash رمزها و کهنه شدن — فقط root
/etc/group	group:x:GID:members
/etc/gshadow	رمز گروه‌ها و مدیران گروه — فقط root
/etc/login.defs	پیش‌فرض‌ها: محدوده UID، کهنه شدن رمز، ساختن خانه
/etc/skel	فایل‌هایی که در هر دایرکتوری خانگی نو کاپی می‌شوند

ساختن و مدیریت کاربران و گروه‌ها

```
[student@server1 ~]$ sudo groupadd -g 2000 developers
[student@server1 ~]$ sudo useradd -c 'Sara Ahmadi' -G developers sara
[student@server1 ~]$ sudo passwd sara
[student@server1 ~]$ sudo useradd -u 1500 -s /sbin/nologin svc-backup   # no login
[student@server1 ~]$ sudo usermod -aG wheel sara       # -a: append, keep old groups!
[student@server1 ~]$ sudo usermod -L sara ; sudo usermod -U sara   # lock / unlock
[student@server1 ~]$ sudo userdel -r olduser           # delete with home directory
[student@server1 ~]$ id sara ; getent group developers
```

رمزها و کهنه شدن رمز

```
[student@server1 ~]$ sudo chage -l sara
Last password change                    : Nov 20, 2026
Password expires                        : never
[student@server1 ~]$ sudo chage -M 90 -m 1 -W 7 sara     # max 90 days, warn 7 days before
[student@server1 ~]$ sudo chage -d 0 sara                 # must change at next login
[student@server1 ~]$ sudo chage -E 2027-06-30 contractor  # account expires
[student@server1 ~]$ grep ^PASS_ /etc/login.defs            # defaults for new users
[student@server1 ~]$ cat /etc/security/pwquality.conf       # minlen, complexity
```

اجازه‌های فایل

معنی	بخشی از ls -l
نوع، اجازه‌ها، مالک، گروه، نام	-rw-r----- 1 sara developers report.txt
مالک (u) / گروه (g) / دیگران (o)	rw- r-- ---
خواندن، نوشتن، اجرا — جمع کنید: rw- = 6	r = 4، w = 2، x = 1
r خواندن، w تغییر، x اجرا به عنوان برنامه	روی فایل‌ها
r فهرست، w ساختن/حذف فایل، x داخل شدن (cd)	روی دایرکتوری‌ها
اول مالک، بعد گروه، بعد دیگران	کدام برنده است؟

chmod و chown

```
[student@server1 ~]$ chmod 640 report.txt           # rw-r-----
[student@server1 ~]$ chmod u+x,g-w,o= script.sh     # symbolic form
[student@server1 ~]$ chmod -R g+rwX /srv/projects   # X: execute on directories only
[student@server1 ~]$ sudo chown sara:developers report.txt
[student@server1 ~]$ sudo chown -R :developers /srv/projects
[student@server1 ~]$ ls -l report.txt
-rw-r----- 1 sara developers 2048 Nov 20 10:00 report.txt
[student@server1 ~]$ stat -c '%A %a %U:%G %n' report.txt
```

اجازه‌های خاص و umask

اثر	تنظیم
برنامه به عنوان مالک خود اجرا می‌شود، مثلاً /usr/bin/passwd	setuid (4، u+s)
فایل‌های نو گروه دایرکتوری را می‌گیرند — عالی برای تیم‌ها	setgid روی دایرکتوری (2، g+s)
فقط مالک می‌تواند فایل‌های خود را حذف کند، مثلاً /tmp	sticky bit (1، o+t)
فولدر تیم: گروه شریک است، دیگران بیرون	chmod 2770 /srv/projects
از فایل‌های نو حق کم می‌کند: 644/755، 664/775، 600/700	umask 022 / 002 / 077
~/.bashrc برای یک کاربر؛ /etc/login.defs برای پیش‌فرض	تنظیم umask

ACL ها: دسترسی دقیق

```
[student@server1 ~]$ setfacl -m u:ahmad:rw report.txt       # one extra user
[student@server1 ~]$ setfacl -m g:auditors:r report.txt     # one extra group
[student@server1 ~]$ setfacl -R -m d:g:developers:rwX /srv/projects   # default ACL
[student@server1 ~]$ getfacl report.txt
# file: report.txt
user::rw-
user:ahmad:rw-
group::r--
group:auditors:r--
mask::rw-
[student@server1 ~]$ setfacl -x u:ahmad report.txt ; setfacl -b report.txt   # remove
```

sudo: حق مدیر به شکل امن

```
[student@server1 ~]$ sudo -l                    # what may I run?
[student@server1 ~]$ sudo -i                    # root shell (logged)
[student@server1 ~]$ sudo visudo -f /etc/sudoers.d/webteam
%webteam  ALL=(root)  /usr/bin/systemctl restart httpd, /usr/bin/systemctl status httpd
ahmad     ALL=(ALL)   ALL

# wheel group already has full sudo in /etc/sudoers:
%wheel    ALL=(ALL)   ALL
[student@server1 ~]$ sudo journalctl _COMM=sudo --since today   # who ran what
```

خلاصه و کارخانگی

- useradd، usermod -aG، passwd، chage، userdel -r
- rwx = 421؛ chmod 640، chmod g+s، chown user:group
- فولدرهای تیمی با setgid؛ umask حق فایل‌های نو را کنترل می‌کند
- setfacl/getfacl وقتی یک مالک و یک گروه کافی نیست
- sudo + wheel؛ کمترین امتیاز با /etc/sudoers.d
- کارخانگی: گروه developers، کاربران sara و ahmad، و فولدر تیمی setgid /srv/projects را بسازید

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