درس ۱۱ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

امنیت، آپدیت‌ها، زمان، بکاپ و ارتقا از 9 به 10

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس یازدهم چه یاد می‌گیرید

- یک چک‌لیست مستحکم‌سازی برای هر سرور
- Crypto policies سراسری و رمزنگاری post-quantum
- اسکن مطابقت با OpenSCAP؛ fapolicyd
- زمان دقیق با chrony
- مدیریت patch و Red Hat Lightspeed (Insights)
- بکاپ و بازیابی: tar، rsync، ReaR
- ارتقای درجا RHEL 9 ← 10 با Leapp

چک‌لیست مستحکم‌سازی

این کار را کنید	بخش
فقط آنچه لازم است نصب کنید (Minimal / Server)؛ باقی را حذف کنید	نرم‌افزار
root را قفل کنید؛ sudo + wheel؛ pwquality قوی؛ کاربران کهنه را حذف کنید	حساب‌ها
فقط کلید؛ PermitRootLogin no؛ AllowGroups (درس ۸)	SSH
zone پیش‌فرض firewalld فقط با سرویس‌های لازم (ss -tulpn)	شبکه
Enforcing، همیشه (درس ۹)	SELinux
آپدیت امنیتی هفتگی؛ جورنال دائمی؛ لاگ مرکزی	آپدیت‌ها و لاگ‌ها
LUKS برای لپ‌تاپ‌ها و دیتای حساس؛ /var/log جدا در صورت امکان	ذخیره‌سازی

Crypto policies سراسری

```
[student@server1 ~]$ update-crypto-policies --show
DEFAULT
[student@server1 ~]$ sudo update-crypto-policies --set FUTURE    # stricter
[student@server1 ~]$ sudo update-crypto-policies --set DEFAULT:NO-SHA1
[student@server1 ~]$ ls /usr/share/crypto-policies/policies/
DEFAULT.pol  FIPS.pol  FUTURE.pol  LEGACY.pol ...
# Applies to OpenSSL, GnuTLS, NSS, OpenSSH, Kerberos, Java ...
# RHEL 10: post-quantum algorithms (ML-KEM, ML-DSA) enabled in TLS and SSH
[student@server1 ~]$ sudo fips-mode-setup --check    # RHEL 9; RHEL 10: enable FIPS at install
```

اسکن مطابقت با OpenSCAP

```
[student@server1 ~]$ sudo dnf install -y openscap-scanner scap-security-guide
[student@server1 ~]$ oscap info /usr/share/xml/scap/ssg/content/ssg-rhel10-ds.xml | grep Id:
  Id: xccdf_org.ssgproject.content_profile_cis
  Id: xccdf_org.ssgproject.content_profile_stig
[student@server1 ~]$ sudo oscap xccdf eval --profile cis \
      --report /tmp/cis-report.html \
      /usr/share/xml/scap/ssg/content/ssg-rhel10-ds.xml
[student@server1 ~]$ firefox /tmp/cis-report.html        # pass / fail for each rule
# Remediate: --remediate, or generate an Ansible playbook with oscap xccdf generate fix
```

ابزارهای امنیتی بیشتر

چه می‌کند	ابزار
فقط به برنامه‌های مورد اعتماد اجازه اجرا می‌دهد (allow-listing)	fapolicyd
فایل‌های تغییر یافته را پیدا می‌کند: aide --init، بعد aide --check	AIDE
رویدادهای امنیتی را ثبت می‌کند: ausearch، aureport، قوانین audit	auditd
دستگاه‌های USB ناشناس را مسدود می‌کند	usbguard
تحلیل Red Hat: آسیب‌پذیری‌ها، هشدارها، خطرها	Lightspeed (Insights)
به دستیار AI اجازه می‌دهد دیتای سیستم را برای عیب‌یابی با دسترسی کنترل‌شده بخواند	MCP server for RHEL (10.3)

زمان دقیق با chrony

```
[student@server1 ~]$ timedatectl
               Local time: Fri 2026-11-20 10:15:02 PST
System clock synchronized: yes
              NTP service: active
[student@server1 ~]$ chronyc sources -v
^* time.cloudflare.com     3   6   377    35   +214us[ +301us] +/-   12ms
[student@server1 ~]$ sudo vim /etc/chrony.conf
server 10.0.0.1 iburst              # your own time source
pool 2.rhel.pool.ntp.org iburst
[student@server1 ~]$ sudo systemctl restart chronyd ; chronyc tracking
```

مدیریت patch

چگونه	روش
dnf updateinfo summary؛ سرویس آسیب‌پذیری Lightspeed	بدانید چه کم است
سرورهای آزمایشی را patch کنید، صبر کنید، بعد production	اول آزمایش
امنیتی هفتگی؛ آپدیت کامل ماهانه؛ پنجره‌های نگهداری	زمان‌بندی
dnf-automatic، Ansible، یا Red Hat Satellite	خودکارسازی
dnf needs-restarting -r؛ kernel live patching (kpatch) برای سرورهای حساس	ریبوت در صورت نیاز
dnf history undo؛ LVM snapshot یا VM قبل از تغییرات بزرگ	برگشت

بکاپ و بازیابی

```
# Files: tar with ACLs and SELinux labels
[student@server1 ~]$ sudo tar --xattrs --acls --selinux -czpf /backup/etc-$(date +%F).tgz /etc
[student@server1 ~]$ sudo tar --xattrs --acls --selinux -xzpf /backup/etc-2026-11-20.tgz -C /restore

# Copy to another server, only the changes:
[student@server1 ~]$ sudo rsync -aAXv --delete /srv/web/ backup@server2:/backup/web/

# Disaster recovery: Relax-and-Recover (ReaR) makes a bootable rescue image
[student@server1 ~]$ sudo dnf install -y rear ; sudo rear -v mkbackup
# Rule: a backup is only real after you have TESTED a restore
```

ارتقای درجا: RHEL 9.9 ← 10.3 با Leapp

```
[student@server2 ~]$ sudo dnf update -y && sudo reboot          # be on the latest 9.9
[student@server2 ~]$ sudo dnf install -y leapp-upgrade
[student@server2 ~]$ sudo leapp preupgrade --target 10.3        # report only, no changes
[student@server2 ~]$ sudo less /var/log/leapp/leapp-report.txt
Risk Factor: high (inhibitor)  ... fix every inhibitor, then run again
[student@server2 ~]$ sudo leapp upgrade --target 10.3
[student@server2 ~]$ sudo reboot                                # upgrade runs during boot
[student@server2 ~]$ cat /etc/redhat-release
Red Hat Enterprise Linux release 10.3 (Coughlan)
```

خلاصه و کارخانگی

- مستحکم‌سازی: نرم‌افزار کم، کلیدها، فایروال، SELinux، آپدیت‌ها
- update-crypto-policies؛ اسکن OpenSCAP در برابر CIS / STIG
- chrony برای زمان دقیق: chronyc sources، tracking
- Patch با پلان: آزمایش، زمان‌بندی، خودکارسازی، برگشت
- tar --acls --selinux، rsync -aAX، ReaR؛ بازیابی را آزمایش کنید
- کارخانگی: یک گزارش CIS OpenSCAP بگیرید؛ server2 را با Leapp از 9.9 به 10.3 ارتقا دهید (بعد از snapshot)

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