دوره کامل · ۱۲ درس

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

dnf، systemd، LVM، firewalld،
SELinux، Podman و Ansible

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



درس ۱ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

RHEL 9 و 10: نسخه‌ها، دوره پشتیبانی، اشتراک رایگان و لابراتوار

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس اول چه یاد می‌گیرید

- RHEL چیست و کجا کار می‌کند
- خانواده: Rocky، RHEL، CentOS Stream، Fedora و AlmaLinux
- RHEL 9 در برابر RHEL 10: چه تغییر کرد
- نسخه‌ها و دوره پشتیبانی ۱۰ ساله
- اشتراک رایگان Red Hat Developer
- نیازمندی‌های سخت‌افزار و لابراتوار ما: server1 و server2
- این دوره چگونه سازمان‌دهی شده است

RHEL چیست؟

جواب	موضوع
Red Hat، از سال ۲۰۱۹ بخشی از IBM	شرکت
اشتراک: آپدیت‌ها، اصلاحات امنیتی، تصدیق و پشتیبانی	پول برای چه
متن باز؛ از CentOS Stream ساخته می‌شود	کود منبع
سخت‌افزار فزیکی، VM ها، کانتینرها، edge، Google Cloud، Azure، AWS	کجا کار می‌کند
ARM 64، x86-64 بیتی، IBM Z، IBM Power	معماری‌ها
RHCSA و RHCE از معتبرترین سرتفیکیت‌های لینوکس هستند	سرتفیکیت‌ها

خانواده Red Hat

هزینه	نقش	توزیع
رایگان	Upstream: ویژگی‌های نو اول اینجا، نسخه نو هر ۶ ماه	Fedora
رایگان	نسخه کوچک بعدی RHEL، به صورت آشکار ساخته می‌شود	CentOS Stream
اشتراک	محصول سازمانی با پشتیبانی	RHEL
رایگان	بازسازی اجتماعی سازگار با RHEL	Rocky Linux
رایگان	بازسازی اجتماعی سازگار با RHEL	AlmaLinux
رایگان / پشتیبانی	توزیع سازگار با RHEL از Oracle	Oracle Linux

RHEL 9 در برابر RHEL 10

بخش	RHEL 9 (2022)	RHEL 10 (2025)
Kernel	5.14	6.12
سطح CPU در x86	x86-64-v2	x86-64-v3 (تقریباً CPU های ۲۰۱۳ به بعد)
دسکتاپ	GNOME روی Wayland یا Xorg	فقط GNOME روی Wayland؛ RDP برای دسکتاپ از راه دور
بسته‌ها	dnf 4 با module ها	dnf 4 بدون module؛ Application Streams
امنیت	SELinux، crypto policies	به علاوه رمزنگاری post-quantum و MCP server
روش‌های نو نصب	Image builder	Image mode (bootc) کاملاً پشتیبانی می‌شود

نسخه‌ها و دوره پشتیبانی

نسخه	آخرین نسخه کوچک	پایان پشتیبانی کامل	پایان نگهداری
RHEL 10	10.3 (۱۱ نوامبر ۲۰۲۶)	۳۱ می ۲۰۳۰	۳۱ می ۲۰۳۵
RHEL 9	9.9 (۱۱ نوامبر ۲۰۲۶)	۳۱ می ۲۰۲۷	۳۱ می ۲۰۳۲
RHEL 8	8.10 (آخرین)	در می ۲۰۲۴ پایان یافت	۳۱ می ۲۰۲۹
نسخه‌های کوچک	هر ۶ ماه	در دوره پشتیبانی کامل	بعد از آن فقط اصلاحات امنیتی

اشتراک رایگان Developer

جزئیات	مورد
developers.redhat.com — یک حساب رایگان Red Hat بسازید	کجا
RHEL برای توسعه و یادگیری، تا ۱۶ سیستم	چه می‌گیرید
ISO کامل (DVD) و boot ISO برای RHEL 10 و RHEL 9	دانلودها
دسترسی کامل به مخازن Red Hat بعد از ثبت	آپدیت‌ها
سرورهای تجاری واقعی — آن‌ها اشتراک پولی لازم دارند	نه برای
Rocky Linux یا AlmaLinux: رایگان و سازگار	جایگزین

نیازمندی‌های سخت‌افزار

مورد	حداقل	پیشنهاد برای لابراتوار
CPU	x86-64-v3 (RHEL 10) یا ARM 64	۲ vCPU برای هر VM
RAM	۲ GB (سرور، بدون GUI)	۴ GB برای server1، ۲ GB برای server2
دیسک	۱۰ GB	دیسک سیستم ۳۰ GB + دو دیسک اضافه ۵ GB
Firmware	UEFI یا BIOS	UEFI با Secure Boot
میزبان	هر PC یا Mac ۶۴ بیتی	۱۶ GB RAM روی میزبان
Hypervisor	KVM، VirtualBox، Hyper-V، VMware، UTM	هر کدام که دارید

لابراتوار ما برای این دوره

هدف	آدرس IP	سیستم عامل	ماشین
سرور اصلی؛ بیشتر درس‌ها	10.0.0.11/24	RHEL 10.3	server1
سرور دوم: NFS، SSH، درس ارتقا	10.0.0.12/24	RHEL 9.9	server2
Gateway 10.0.0.1، DNS 10.0.0.1	10.0.0.0/24	شبکه لابراتوار	شبکه
با student کار می‌کنیم و از sudo استفاده می‌کنیم	—	root + student	کاربران
ذخیره‌سازی و LVM در درس ۷	/dev/vdb، /dev/vdc	server1	دیسک‌های اضافه

اولین نگاه شما به RHEL

```
[student@server1 ~]$ cat /etc/redhat-release
Red Hat Enterprise Linux release 10.3 (Coughlan)
[student@server1 ~]$ uname -r
6.12.0-...el10.x86_64
[student@server1 ~]$ hostnamectl
[student@server1 ~]$ nproc ; free -h ; df -h /
[student@server1 ~]$ ld.so --help | grep supported     # x86-64-v3 (supported)?
```

این دوره چگونه سازمان‌دهی شده است

موضوعات	درس‌ها
نسخه‌ها و لابراتوار، نصب و Cockpit، ضروریات خط فرمان	۱–۳
کاربران و اجازه‌ها، نرم‌افزار با dnf، systemd، بوت و لاگ‌ها	۴–۶
ذخیره‌سازی و LVM، شبکه، firewalld و SSH	۷–۸
SELinux — یک درس کامل	۹
Podman، NFS، Apache؛ امنیت، آپدیت‌ها و ارتقا از 9 به 10	۱۰–۱۱
اسکریپت‌نویسی، image mode، Ansible، عیب‌یابی و RHCSA	۱۲

خلاصه و کارخانگی

- RHEL: لینوکس سازمانی با پشتیبانی؛ Fedora و CentOS Stream پیش از آن می‌آیند
- RHEL 10 برای سرورهای نو؛ RHEL 9 هنوز همه جا است
- دوره پشتیبانی ده ساله؛ نسخه‌های کوچک هر شش ماه
- اشتراک رایگان developer: تا ۱۶ سیستم
- کارخانگی: حساب Red Hat بسازید و ISO کامل RHEL 10 را دانلود کنید
- کارخانگی: VM های server1 و server2 را بسازید (هنوز نصب نکنید)

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

درس ۲ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

نصب RHEL، ثبت سیستم و کنسول ویب (Cockpit)

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس دوم چه یاد می‌گیرید

- فایل‌های ISO نصب و نصب‌کننده Anaconda
- قدم به قدم: زبان، دیسک‌ها، شبکه، کاربران، نرم‌افزار
- Server with GUI در برابر Server و Minimal
- ثبت سیستم با subscription-manager یا rhc
- کارهای اول: آپدیت‌ها، hostname، منطقه زمانی
- کنسول ویب: Cockpit روی پورت 9090
- Kickstart: نصب خودکار

رسانه‌های نصب

چه وقت استفاده کنید	اندازه	ISO
انتخاب عادی: همه چیز داخل است، بدون انترنت کار می‌کند	تقریباً ۸ تا ۱۲ GB	DVD (binary) ISO
کوچک؛ بسته‌ها بعد از ثبت از شبکه می‌آیند	تقریباً ۱ GB	Boot ISO
VM ها و instance های کلاود آماده	کوچک	Cloud images (qcow2، AMI)
نصب RHEL به شکل container image (درس ۱۲)	container image	Image mode (bootc)
ISO را با Fedora Media Writer یا dd بنویسید	—	USB

نصب‌کننده Anaconda

در لابراتوار چه انتخاب کنید	صفحه
English (United States)، یا زبان خودتان	زبان و کیبورد
دیسک ۳۰ GB، پارتیشن‌بندی خودکار (LVM)	Installation destination
کارت شبکه را فعال کنید؛ server1.lab.local hostname	شبکه و نام سیستم
منطقه زمانی شما؛ زمان شبکه روشن	زمان و تاریخ
Server (بدون GUI) برای server2؛ Server with GUI برای server1	انتخاب نرم‌افزار
قفل یا رمز قوی؛ بدون ورود root از راه SSH	حساب root
student با حق مدیر (گروه wheel)	ساختن کاربر

انتخاب نرم‌افزار

Base environment	چه می‌گیرید	بهترین برای
Server with GUI	دسکتاپ GNOME + ابزارهای سرور	یادگیری، کمپیوترهای مدیر
Server	خط فرمان + ابزارهای عادی سرور	بیشتر سرورهای واقعی
Minimal Install	کوچکترین سیستم کارا	میزبان کانتینر، امنیت، کلاود
Workstation	دسکتاپ برای کار روزانه	لپ‌تاپ‌های developer
Add-ons	گروه‌های بسته اضافه	بعداً با dnf group install اضافه کنید

ثبت سیستم

```
[student@server1 ~]$ sudo rhc connect -u <your-Red-Hat-login>
# or the classic tool:
[student@server1 ~]$ sudo subscription-manager register --username <your-Red-Hat-login>
[student@server1 ~]$ sudo subscription-manager status
[student@server1 ~]$ sudo dnf repolist
repo id                                    repo name
rhel-10-for-x86_64-appstream-rpms          Red Hat Enterprise Linux 10 ... AppStream
rhel-10-for-x86_64-baseos-rpms             Red Hat Enterprise Linux 10 ... BaseOS
```

کارهای اول بعد از نصب

```
[student@server1 ~]$ sudo dnf -y update            # install all updates
[student@server1 ~]$ sudo reboot                   # if the kernel was updated

[student@server1 ~]$ sudo hostnamectl set-hostname server1.lab.local
[student@server1 ~]$ timedatectl                   # time zone and NTP status
[student@server1 ~]$ sudo timedatectl set-timezone America/Los_Angeles
[student@server1 ~]$ ip -brief address             # check the IP address
[student@server1 ~]$ sudo systemctl enable --now cockpit.socket
```

کنسول وب: Cockpit

ویژگی	چه کاری می‌توانید انجام دهید
آدرس	https://server1.lab.local:9090 — با student وارد شوید
Overview	گراف‌های CPU، حافظه، دیسک و شبکه؛ آپدیت‌ها؛ ریبوت
لاگ‌ها و سرویس‌ها	خواندن journal؛ شروع، توقف و فعال‌سازی سرویس‌ها
ذخیره‌سازی و شبکه	دیسک‌ها، LVM، فایل سیستم‌ها؛ interface ها، فایروال
حساب‌ها و ترمینال	ساختن کاربران؛ یک ترمینال کامل در مرورگر
Add-on ها	cockpit-podman، cockpit-machines، cockpit-files

نصب Cockpit و add-on ها

```
[student@server2 ~]$ sudo dnf install -y cockpit cockpit-podman cockpit-files
[student@server2 ~]$ sudo systemctl enable --now cockpit.socket
[student@server2 ~]$ sudo firewall-cmd --add-service=cockpit --permanent
[student@server2 ~]$ sudo firewall-cmd --reload
[student@server2 ~]$ ss -tlnp | grep 9090
LISTEN 0  4096   *:9090   *:*
# From server1 Cockpit: Add new host > server2.lab.local
```

Kickstart: نصب خودکار

```
# /root/anaconda-ks.cfg is created on every installed system
lang en_US.UTF-8
keyboard us
timezone America/Los_Angeles --utc
network --bootproto=static --ip=10.0.0.13 --hostname=server3.lab.local
rootpw --lock
user --name=student --groups=wheel --password=<hash> --iscrypted
autopart --type=lvm
%packages
@^server-product-environment
%end
```

نصب RHEL 9 روی server2

تفاوت با RHEL 10	مورد
همان Anaconda؛ صفحه‌ها تقریباً یکسان	نصب‌کننده
روی CPU های قدیمی‌تر x86-64-v2 کار می‌کند	CPU
جلسه Xorg هنوز موجود است	دسکتاپ
VNC موجود است؛ RHEL 10 از RDP استفاده می‌کند	GUI از راه دور
همان فرمان‌ها: dnf، subscription-manager، rhc	ثبت و آپدیت
rhel-9-for-x86_64-baseos-rpms و appstream-rpms	مخازن

خلاصه و کارخانگی

- نصب از ISO کامل با Anaconda؛ پارتیشن‌بندی خودکار LVM
- student را به عنوان مدیر (wheel) بسازید؛ root را قفل کنید
- ثبت با rhc connect یا subscription-manager، بعد dnf update
- Cockpit: https://host:9090 برای مدیریت از مرورگر
- کارخانگی: RHEL 10 را روی server1 و RHEL 9 را روی server2 نصب کنید
- کارخانگی: هر دو را ثبت و آپدیت کنید، Cockpit را فعال کنید، anaconda-ks.cfg را بخوانید

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

درس ۳ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

ضروریات خط فرمان: فایل‌ها، راهنما، ویرایش و pipe ها

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس سوم چه یاد می‌گیرید

- شِل bash، prompt و ساختار فرمان
- ساختار فایل سیستم: /etc، /var، /home و غیره
- حرکت و مدیریت فایل‌ها و دایرکتوری‌ها
- گرفتن راهنما: --help، man، /usr/share/doc
- ویرایش فایل‌ها با vim و nano
- pipe، Redirection ها و grep
- پیدا کردن فایل‌ها، link ها و آرشیو با tar

شِل و prompt

معنی	بخش
کاربر، میزبان، دایرکتوری فعلی؛ $ = کاربر عادی	[student@server1 ~]$
# = root، مدیر؛ محتاط باشید	[root@server1 ~]#
ls -l /etc — فرمان، option، argument	command -options arguments
فرمان‌ها و نام فایل‌ها را کامل می‌کند	کلید Tab
تکرار و جستجوی فرمان‌های قبلی	کلید بالا، history، Ctrl+R
توقف فرمان / خروج / پاک کردن صفحه	Ctrl+C / Ctrl+D / clear

ساختار فایل سیستم

محتوا	دایرکتوری
ریشه همه چیز	/
فایل‌های تنظیمات سیستم	/etc
دایرکتوری خانگی کاربران؛ خانه root	/home، /root
دیتای متغیر: لاگ‌ها (/var/log)، وب سایت‌ها، دیتابیس‌ها	/var
برنامه‌ها و کتابخانه‌های نصب‌شده (/usr/bin، /usr/lib)	/usr
فایل‌های موقت، خودکار پاک می‌شوند	/tmp
فایل‌های کِرنِل و بوت؛ دستگاه‌ها؛ معلومات زنده سیستم	/boot، /dev، /proc، /run

حرکت و مدیریت فایل‌ها

```
[student@server1 ~]$ pwd                        # where am I?
/home/student
[student@server1 ~]$ ls -la /etc | less         # long list, hidden files, page by page
[student@server1 ~]$ cd /var/log ; cd ~ ; cd -   # go there, go home, go back
[student@server1 ~]$ mkdir -p projects/web/html
[student@server1 ~]$ touch notes.txt
[student@server1 ~]$ cp notes.txt projects/ ; cp -r projects backup
[student@server1 ~]$ mv notes.txt todo.txt       # rename or move
[student@server1 ~]$ rm todo.txt ; rm -r backup  # no recycle bin!
```

گرفتن راهنما

چه می‌دهد	فرمان
صفحه راهنما؛ q برای خروج، /word برای جستجو	man ls
جستجوی یک کلمه در عنوان صفحه‌های راهنما	man -k password
بخش ۵: فارمت فایل‌ها (بخش ۱ = فرمان‌ها، ۸ = مدیریت)	man 5 passwd
خلاصه کوتاه option ها	ls --help
مستندات اضافه و مثال‌ها	/usr/share/doc
رهنمودهای رسمی و رایگان RHEL برای هر نسخه	docs.redhat.com

ویرایش فایل‌ها با vim

عمل	کلیدها
باز کردن (یا ساختن) فایل در normal mode	vim file.txt
Insert mode برای تایپ / برگشت به normal mode	i / Esc
ذخیره / خروج / ذخیره و خروج / خروج بدون ذخیره	:w :q :wq :q!
حذف خط / کاپی خط / paste / undo	dd yy p u
جستجو به جلو / مورد بعدی	/text n
جایگزینی در همه جای فایل	:%s/old/new/g
ویرایشگر ساده‌تر: فرمان‌ها پایین صفحه نشان داده می‌شوند	nano file.txt

Redirection و pipe ها

```
[student@server1 ~]$ ls /etc > etc-list.txt          # stdout to a file (overwrite)
[student@server1 ~]$ date >> etc-list.txt            # append
[student@server1 ~]$ ls /nothing 2> errors.txt       # stderr to a file
[student@server1 ~]$ dnf list installed &> pkgs.txt  # both stdout and stderr
[student@server1 ~]$ ls /etc | wc -l                 # pipe: count the files
[student@server1 ~]$ ps aux | sort -k3 -nr | head -5 # top 5 CPU users
[student@server1 ~]$ cat /etc/passwd | cut -d: -f1 | sort
[student@server1 ~]$ echo 'hello' | tee copy.txt      # screen AND file
```

جستجوی متن با grep

```
[student@server1 ~]$ grep student /etc/passwd
student:x:1000:1000:student:/home/student:/bin/bash
[student@server1 ~]$ grep -i error /var/log/messages     # ignore case
[student@server1 ~]$ grep -r 'Listen' /etc/httpd/ 2>/dev/null
[student@server1 ~]$ grep -v '^#' /etc/ssh/sshd_config | grep -v '^$'
[student@server1 ~]$ grep -E 'fail(ed|ure)' /var/log/secure
[student@server1 ~]$ grep -c bash /etc/passwd              # count matching lines
```

پیدا کردن فایل‌ها و ساختن link

```
[student@server1 ~]$ find /etc -name '*.conf' -mtime -7      # changed in 7 days
[student@server1 ~]$ find / -user student -type f 2>/dev/null
[student@server1 ~]$ find /var/log -size +10M
[student@server1 ~]$ find /tmp -name '*.tmp' -delete
[student@server1 ~]$ locate sshd_config        # fast; needs: sudo dnf install plocate
[student@server1 ~]$ ln -s /var/log/messages mylog   # symbolic (soft) link
[student@server1 ~]$ ln notes.txt hardlink.txt       # hard link: same inode
[student@server1 ~]$ ls -li mylog hardlink.txt
```

آرشیو و فشرده‌سازی با tar

```
[student@server1 ~]$ tar -czvf etc-backup.tar.gz /etc        # create, gzip
[student@server1 ~]$ tar -cJf etc-backup.tar.xz /etc         # create, xz (smaller)
[student@server1 ~]$ tar -tzf etc-backup.tar.gz | head        # list contents
[student@server1 ~]$ tar -xzf etc-backup.tar.gz -C /tmp/restore
[student@server1 ~]$ gzip big.log ; gunzip big.log.gz
[student@server1 ~]$ zip -r site.zip projects/ ; unzip site.zip
[student@server1 ~]$ du -sh /var/log ; ls -lh etc-backup.*
```

خلاصه و کارخانگی

- Prompt: $ کاربر عادی، # root؛ Tab و history وقت را ذخیره می‌کنند
- /etc تنظیمات، /var دیتا و لاگ‌ها، /home کاربران، /usr برنامه‌ها
- man، man -k و --help: جواب‌ها همیشه روی سیستم هستند
- vim: i برای نوشتن، Esc، :wq برای ذخیره و خروج
- Pipe و redirection: | > >> 2> &>
- کارخانگی: vimtutor را تمرین کنید؛ همه فایل‌های conf. در /etc را پیدا کنید؛ از /etc با tar آرشیو 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

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

درس ۵ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

مدیریت نرم‌افزار با RPM، DNF، مخازن و Flatpak

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس پنجم چه یاد می‌گیرید

- بسته‌های RPM و مخازن: BaseOS و AppStream
- dnf: جستجو، نصب، آپدیت، حذف
- گروه‌های بسته و environment ها
- تاریخچه و undo
- Application Streams: نسخه‌های نوتر زبان‌ها و دیتابیس‌ها
- بررسی بسته‌ها با rpm
- اضافه کردن مخازن: EPEL و مخزن خودتان؛ Flatpak

بسته‌ها و مخازن

اصطلاح	معنی
بسته RPM	httpd-2.4.63-1.el10.x86_64.rpm — نام، نسخه، release، معماری
مخزن	مجموعه امضاشده بسته‌ها که dnf از آن دانلود می‌کند
BaseOS	سیستم عامل اصلی، در تمام عمر نسخه پشتیبانی می‌شود
AppStream	برنامه‌ها، زبان‌ها، دیتابیس‌ها و ابزارها
CodeReady Builder	بسته‌های اضافه developer (در صورت نیاز فعال کنید)
امضای GPG	ثابت می‌کند بسته واقعاً از Red Hat آمده است

جستجو، نصب و حذف

```
[student@server1 ~]$ dnf search nginx
[student@server1 ~]$ dnf info httpd
[student@server1 ~]$ dnf provides /usr/bin/dig       # which package has this file?
bind-utils-9.18...el10.x86_64 : Utilities for querying DNS name servers
[student@server1 ~]$ sudo dnf install -y httpd bind-utils
[student@server1 ~]$ sudo dnf remove nginx
[student@server1 ~]$ sudo dnf reinstall httpd
[student@server1 ~]$ dnf list installed | grep httpd
[student@server1 ~]$ sudo dnf install ./local-tool-1.0.rpm   # a downloaded file
```

آپدیت‌ها

```
[student@server1 ~]$ dnf check-update                    # what is waiting?
[student@server1 ~]$ sudo dnf update -y                  # update everything
[student@server1 ~]$ sudo dnf update --security          # security fixes only
[student@server1 ~]$ dnf updateinfo list --security      # advisories (RHSA)
[student@server1 ~]$ sudo dnf update openssl             # one package
[student@server1 ~]$ dnf needs-restarting -r              # is a reboot needed?
[student@server1 ~]$ sudo dnf install dnf-automatic
[student@server1 ~]$ sudo systemctl enable --now dnf-automatic.timer
```

گروه‌ها، تاریخچه و undo

```
[student@server1 ~]$ dnf group list
[student@server1 ~]$ dnf group info 'Development Tools'
[student@server1 ~]$ sudo dnf group install -y 'Development Tools'
[student@server1 ~]$ dnf history
ID | Command line              | Date and time    | Action(s) | Altered
 7 | group install Developmen.. | 2026-11-20 10:42 | Install   |   38
 6 | install -y httpd bind-u..  | 2026-11-20 10:30 | Install   |    9
[student@server1 ~]$ dnf history info 7
[student@server1 ~]$ sudo dnf history undo 7           # remove those 38 packages
```

Application Streams

مورد	RHEL 9	RHEL 10
ایده	چند نسخه از یک زبان یا دیتابیس	همان ایده
چگونه	Module ها: dnf module enable nodejs:22	بسته‌های نسخه‌دار، مثلاً nodejs24
مثال‌ها	module های postgresql، php، nodejs، ruby	python3.12، postgresql18، nodejs24
فهرست	dnf module list	dnf list --available 'postgresql*'
دوره پشتیبانی	هر stream تاریخ‌های پشتیبانی خود را دارد	صفحه Application Streams life cycle را ببینید

بررسی بسته‌ها با rpm

```
[student@server1 ~]$ rpm -qa | wc -l                    # how many packages?
[student@server1 ~]$ rpm -qi httpd                      # information
[student@server1 ~]$ rpm -ql httpd | head               # files in the package
[student@server1 ~]$ rpm -qc httpd                      # its configuration files
[student@server1 ~]$ rpm -qf /etc/ssh/sshd_config      # which package owns this file?
openssh-server-9.9p1-...el10.x86_64
[student@server1 ~]$ rpm -V openssh-server              # what changed since install?
S.5....T.  c /etc/ssh/sshd_config
[student@server1 ~]$ rpm -q --changelog openssl | head
```

مخازن: EPEL و مخزن خودتان

```
[student@server1 ~]$ dnf repolist --all
[student@server1 ~]$ sudo subscription-manager repos \
      --enable codeready-builder-for-rhel-10-x86_64-rpms
[student@server1 ~]$ sudo dnf install \
      https://dl.fedoraproject.org/pub/epel/epel-release-latest-10.noarch.rpm
[student@server1 ~]$ sudo dnf install htop

[student@server1 ~]$ sudo vim /etc/yum.repos.d/internal.repo
[internal]
name=Company packages
baseurl=http://10.0.0.11/repo/
gpgcheck=1
gpgkey=http://10.0.0.11/repo/RPM-GPG-KEY-internal
```

Flatpak و برنامه‌های دسکتاپ

```
[student@server1 ~]$ flatpak remotes
Name    Options
rhel    system,oci
[student@server1 ~]$ flatpak search firefox
[student@server1 ~]$ flatpak install rhel org.mozilla.firefox
[student@server1 ~]$ flatpak list --app
[student@server1 ~]$ flatpak update
# Optional, community apps:
[student@server1 ~]$ flatpak remote-add --if-not-exists flathub \
      https://dl.flathub.org/repo/flathub.flatpakrepo
```

خلاصه و کارخانگی

- BaseOS + AppStream؛ بسته‌ها RPM های امضاشده با GPG هستند
- dnf search، info، provides، install، remove، update
- dnf history undo تور ایمنی شما است
- rpm -qa، -qi، -ql، -qc، -qf، -V به سوالات جواب می‌دهند
- EPEL برای بسته‌های اضافه (بدون پشتیبانی)؛ Flatpak برای برنامه‌های دسکتاپ
- کارخانگی: httpd و Development Tools را نصب کنید، مالک /etc/ssh/sshd_config را پیدا کنید، نصب گروه را undo 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

درس ۶ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

systemd، بوت، لاگ‌ها، پروسس‌ها و زمان‌بندی

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس ششم چه یاد می‌گیرید

- unit های systemd و systemctl
- روند بوت: firmware، GRUB، کِرنِل، systemd، target ها
- بازیابی رمز گم‌شده root
- لاگ‌ها: journalctl و /var/log
- پروسس‌ها: ps، top، kill، nice
- پروفایل‌های کارایی با tuned
- زمان‌بندی: cron، at و تایمرهای systemd

systemd و unit ها

هدف	مثال	نوع unit
یک daemon (برنامه پس‌زمینه)	sshd.service	service
وقتی اتصال می‌رسد یک سرویس را شروع می‌کند	cockpit.socket	socket
گروهی از unit ها: یک حالت سیستم	multi-user.target	target
یک سرویس را طبق برنامه اجرا می‌کند	dnf-automatic.timer	timer
یک فایل سیستم وصل‌شده	home.mount	mount
تغییرات شما در /etc/systemd/system	/usr/lib/systemd/system	فایل‌های unit

مدیریت سرویس‌ها با systemctl

```
[student@server1 ~]$ systemctl status sshd
● sshd.service - OpenSSH server daemon
     Active: active (running) since Fri 2026-11-20 09:12:01 PST
[student@server1 ~]$ sudo systemctl start httpd ; sudo systemctl stop httpd
[student@server1 ~]$ sudo systemctl restart httpd ; sudo systemctl reload httpd
[student@server1 ~]$ sudo systemctl enable --now httpd     # start now and at boot
[student@server1 ~]$ systemctl is-enabled httpd ; systemctl is-active httpd
[student@server1 ~]$ systemctl list-units --type=service --state=failed
[student@server1 ~]$ sudo systemctl mask cups               # can never be started
```

تنظیمات خودتان: drop-in و فایل unit

```
[student@server1 ~]$ sudo systemctl edit httpd          # creates a drop-in override
[Service]
Restart=on-failure
RestartSec=5
[student@server1 ~]$ systemctl cat httpd                # unit + overrides

# /etc/systemd/system/hello.service — your own service
[Unit]
Description=Hello web app
After=network-online.target
[Service]
ExecStart=/usr/local/bin/hello --port 8080
User=svc-hello
[Install]
WantedBy=multi-user.target
```

روند بوت

قدم	چه اتفاق می‌افتد
۱. Firmware	UEFI یا BIOS سخت‌افزار را آزمایش می‌کند؛ Secure Boot امضاها را بررسی می‌کند
۲. Boot loader	GRUB 2 منو را نشان می‌دهد و کِرنِل و initramfs را بارگذاری می‌کند
۳. کِرنِل	شروع می‌شود، با initramfs فایل سیستم ریشه را پیدا می‌کند
۴. systemd	PID 1 تارگِت پیش‌فرض را می‌خواند و unit ها را موازی شروع می‌کند
۵. Target	multi-user.target (متنی) یا graphical.target (دسکتاپ)
فرمان‌ها	systemctl get-default / set-default؛ systemd-analyze blame

تنظیم دوباره رمز گم‌شده root

```
# 1. Reboot; in the GRUB menu press e on the kernel entry
# 2. At the end of the line starting with 'linux' add:   rd.break
# 3. Press Ctrl+X to boot into the initramfs shell
switch_root:/# mount -o remount,rw /sysroot
switch_root:/# chroot /sysroot
sh-5.2# passwd root
sh-5.2# touch /.autorelabel                # SELinux must relabel the files
sh-5.2# exit ; exit                        # the system relabels and reboots

# Protect GRUB in production:  sudo grub2-setpassword
```

خواندن لاگ‌ها با journalctl

```
[student@server1 ~]$ journalctl -u sshd --since '1 hour ago'
[student@server1 ~]$ journalctl -p err -b              # errors since this boot
[student@server1 ~]$ journalctl -f                     # follow live, like tail -f
[student@server1 ~]$ journalctl -b -1                  # the previous boot
[student@server1 ~]$ journalctl _UID=1000 -o verbose
[student@server1 ~]$ sudo mkdir -p /var/log/journal    # keep logs across reboots
[student@server1 ~]$ sudo less /var/log/messages ; sudo tail /var/log/secure
[student@server1 ~]$ logger 'backup finished'          # write your own message
```

پروسس‌ها

```
[student@server1 ~]$ ps aux --sort=-%mem | head -5
[student@server1 ~]$ ps -ef --forest | less          # parent/child tree
[student@server1 ~]$ pgrep -a httpd
[student@server1 ~]$ top                              # press 1, M, P, k, q
[student@server1 ~]$ kill 4321 ; kill -9 4321         # TERM (polite) / KILL (forced)
[student@server1 ~]$ pkill -u sara                    # all of sara's processes
[student@server1 ~]$ nice -n 10 tar -czf big.tgz /data ; sudo renice -n -5 -p 4321
[student@server1 ~]$ sleep 300 &  ;  jobs  ;  fg %1   # background jobs
```

پروفایل‌های کارایی با tuned

```
[student@server1 ~]$ tuned-adm active
Current active profile: virtual-guest
[student@server1 ~]$ tuned-adm list
balanced  powersave  throughput-performance  virtual-guest ...
[student@server1 ~]$ tuned-adm recommend
virtual-guest
[student@server1 ~]$ sudo tuned-adm profile throughput-performance
[student@server1 ~]$ uptime ; vmstat 2 5 ; free -h     # load and memory
```

زمان‌بندی: cron، at و تایمرها

```
[student@server1 ~]$ crontab -e                          # your personal jobs
# min hour day month weekday  command
30 2 * * *   /home/student/bin/backup.sh                # every day at 02:30
*/15 8-17 * * 1-5  /usr/local/bin/check-site            # every 15 min, office hours
[student@server1 ~]$ crontab -l ; sudo crontab -u sara -l
[student@server1 ~]$ echo 'systemctl restart httpd' | sudo at 23:00   # once
[student@server1 ~]$ atq
[student@server1 ~]$ systemctl list-timers               # systemd timers
```

خلاصه و کارخانگی

- systemctl enable --now، status، restart؛ override با systemctl edit
- بوت: GRUB 2 ← firmware ← کِرنِل ← target ← systemd
- تنظیم دوباره رمز root: rd.break، chroot، passwd، touch /.autorelabel
- journalctl -u، -p err، -b، -f؛ جورنال دائمی
- ps، top، kill، nice؛ tuned-adm profile؛ cron، at، تایمرها
- کارخانگی: رمز root را روی server2 دوباره تنظیم کنید؛ یک بکاپ روزانه tar از /etc زمان‌بندی 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

درس ۷ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

ذخیره‌سازی: پارتیشن‌ها، XFS، Swap، LVM و Stratis

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس هفتم چه یاد می‌گیرید

- دیسک‌ها، پارتیشن‌ها و نام دستگاه‌ها
- پارتیشن‌بندی با parted: GPT
- فایل سیستم‌ها: XFS و ext4؛ وصل کردن
- وصل دائمی در /etc/fstab با UUID
- LVM: physical volume، volume group، logical volume
- بزرگ کردن فایل سیستم در هنگام استفاده
- فضای swap؛ Stratis؛ رمزنگاری LUKS

دیسک‌های خود را پیدا کنید

```
[student@server1 ~]$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
vda           252:0    0   30G  0 disk
├─vda1        252:1    0  600M  0 part /boot/efi
├─vda2        252:2    0    1G  0 part /boot
└─vda3        252:3    0 28.4G  0 part
  ├─rhel-root 253:0    0 25.4G  0 lvm  /
  └─rhel-swap 253:1    0    3G  0 lvm  [SWAP]
vdb           252:16   0    5G  0 disk
vdc           252:32   0    5G  0 disk
[student@server1 ~]$ lsblk -f ; df -hT ; sudo blkid
```

پارتیشن‌بندی دیسک با parted

```
[student@server1 ~]$ sudo parted /dev/vdb mklabel gpt
[student@server1 ~]$ sudo parted /dev/vdb mkpart data xfs 1MiB 2GiB
[student@server1 ~]$ sudo parted /dev/vdb mkpart lvm1 2GiB 100%
[student@server1 ~]$ sudo parted /dev/vdb set 2 lvm on
[student@server1 ~]$ sudo parted /dev/vdb print
Number  Start   End     Size    File system  Name  Flags
 1      1049kB  2147MB  2146MB               data
 2      2147MB  5368MB  3221MB               lvm1  lvm
[student@server1 ~]$ sudo udevadm settle ; lsblk /dev/vdb
```

ساختن و وصل کردن فایل سیستم

```
[student@server1 ~]$ sudo mkfs.xfs -L data /dev/vdb1      # XFS: the RHEL default
[student@server1 ~]$ sudo mkdir /data
[student@server1 ~]$ sudo mount /dev/vdb1 /data
[student@server1 ~]$ df -h /data
Filesystem      Size  Used Avail Use% Mounted on
/dev/vdb1       2.0G   47M  1.9G   3% /data
[student@server1 ~]$ sudo umount /data
# ext4 is also supported:  sudo mkfs.ext4 /dev/vdX1
# XFS can grow but cannot shrink; ext4 can do both (offline)
```

وصل دائمی در /etc/fstab

```
[student@server1 ~]$ sudo blkid /dev/vdb1
/dev/vdb1: LABEL="data" UUID="5b2e7c1a-..." TYPE="xfs"
[student@server1 ~]$ sudo vim /etc/fstab
# device                                  mount  type  options   dump fsck
UUID=5b2e7c1a-...                         /data  xfs   defaults  0 0
[student@server1 ~]$ sudo systemctl daemon-reload
[student@server1 ~]$ sudo mount -a          # test: mounts everything in fstab
[student@server1 ~]$ findmnt /data
# A mistake here can stop the boot: ALWAYS test with mount -a
```

Logical Volume Manager :LVM

لایه	چیست	فرمان‌ها
Physical volume (PV)	یک دیسک یا پارتیشن که به LVM داده شده	pvcreate، pvs
Volume group (VG)	یک حوض فضا از یک یا چند PV	vgcreate، vgextend، vgs
Logical volume (LV)	یک «پارتیشن» بریده شده از حوض	lvcreate، lvextend، lvs
فایل سیستم	XFS یا ext4 روی LV	mkfs.xfs، xfs_growfs
چرا	بزرگ کردن آنلاین، اضافه کردن دیسک، snapshot	RHEL به طور پیش‌فرض روی LVM نصب می‌شود

ساختن LVM قدم به قدم

```
[student@server1 ~]$ sudo pvcreate /dev/vdb2 /dev/vdc
[student@server1 ~]$ sudo vgcreate vgdata /dev/vdb2 /dev/vdc
[student@server1 ~]$ sudo lvcreate -n lvweb -L 3G vgdata
[student@server1 ~]$ sudo lvcreate -n lvlogs -l 50%FREE vgdata
[student@server1 ~]$ sudo mkfs.xfs /dev/vgdata/lvweb
[student@server1 ~]$ sudo mkdir /srv/web
[student@server1 ~]$ echo '/dev/vgdata/lvweb /srv/web xfs defaults 0 0' | sudo tee -a /etc/fstab
[student@server1 ~]$ sudo systemctl daemon-reload ; sudo mount -a
[student@server1 ~]$ sudo pvs ; sudo vgs ; sudo lvs
```

بزرگ کردن فایل سیستم به شکل آنلاین

```
[student@server1 ~]$ df -h /srv/web
/dev/mapper/vgdata-lvweb  3.0G  2.8G  200M  94% /srv/web
[student@server1 ~]$ sudo lvextend -r -L +1G /dev/vgdata/lvweb    # -r grows the FS too
  Size of logical volume vgdata/lvweb changed from 3.00 GiB to 4.00 GiB.
[student@server1 ~]$ df -h /srv/web
/dev/mapper/vgdata-lvweb  4.0G  2.8G  1.2G  70% /srv/web

# Pool full? Add a disk first:
[student@server1 ~]$ sudo vgextend vgdata /dev/vdd
# Without -r:  sudo xfs_growfs /srv/web   (ext4: sudo resize2fs /dev/vgdata/lvweb)
```

فضای swap

```
[student@server1 ~]$ swapon --show ; free -h
[student@server1 ~]$ sudo lvcreate -n lvswap -L 1G vgdata
[student@server1 ~]$ sudo mkswap /dev/vgdata/lvswap
[student@server1 ~]$ echo '/dev/vgdata/lvswap none swap defaults 0 0' | sudo tee -a /etc/fstab
[student@server1 ~]$ sudo systemctl daemon-reload ; sudo swapon -a
[student@server1 ~]$ swapon --show
NAME       TYPE      SIZE USED PRIO
/dev/dm-1  partition   3G   0B   -2
/dev/dm-4  partition   1G   0B   -3
```

Stratis و رمزنگاری LUKS

ابزار	چه می‌کند	مثال
Stratis	ذخیره‌سازی حوضی روی XFS: thin provisioning، snapshot	stratis pool create pool1 /dev/vdd
Stratis FS	فایل سیستم‌ها داخل حوض خودکار بزرگ می‌شوند	stratis fs create pool1 docs
وصل Stratis	fstab به x-systemd.requires=stratisd.service نیاز دارد	see man stratis; mount -a to test
LUKS	یک پارتیشن یا LV کامل را رمزنگاری می‌کند	cryptsetup luksFormat /dev/vdb1
باز کردن LUKS	باز کنید، بعد mkfs و mount روی دستگاه mapper	cryptsetup open /dev/vdb1 secret
در بوت	/etc/crypttab، یا Clevis با TPM 2.0 / Tang	لپ‌تاپ‌ها: در هنگام نصب رمزنگاری کنید

خلاصه و کارخانگی

- lsblk، blkid، df -hT دیسک‌ها، UUID ها و فضا را نشان می‌دهند
- parted mklabel gpt / mkpart؛ mkfs.xfs؛ mount
- fstab با UUID؛ همیشه با mount -a آزمایش کنید
- LVM: lvcreate ← vgcreate ← pvcreate؛ lvextend -r آنلاین بزرگ می‌کند
- mkswap + swapon؛ حوض‌های Stratis؛ رمزنگاری LUKS
- کارخانگی: vgdata را از vdb2 و vdc بسازید، lvweb را بسازید، در /srv/web وصل کنید، بعد ۱ GB بزرگ 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

درس ۸ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

شبکه، firewalld و SSH امن

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس هشتم چه یاد می‌گیرید

- اساسات شبکه: interface ها، IP، gateway، DNS
- بررسی شبکه: ip، ss، ping، dig
- NetworkManager با nmcli: IP ثابت، DNS، hostname
- تبدیل نام: /etc/hosts و resolv.conf
- firewalld: zone ها، سرویس‌ها و پورت‌ها
- SSH: کلیدها، تنظیمات امن، کاپی فایل‌ها
- عیب‌یابی قدم به قدم

بررسی شبکه

```
[student@server1 ~]$ ip -br addr
lo        UNKNOWN  127.0.0.1/8 ::1/128
enp1s0    UP       10.0.0.11/24 fe80::5054:ff:fe12:3456/64
[student@server1 ~]$ ip route                    # default via 10.0.0.1
[student@server1 ~]$ ping -c 3 10.0.0.1          # gateway reachable?
[student@server1 ~]$ dig +short redhat.com        # DNS working?
[student@server1 ~]$ ss -tulpn                   # listening ports + programs
[student@server1 ~]$ tracepath redhat.com
[student@server1 ~]$ curl -I https://www.mywebuniversity.com
```

مفاهیم NetworkManager

اصطلاح	معنی
Device	یک کارت شبکه، مثلاً enp1s0
Connection (profile)	تنظیمات یک device: IP، gateway، DNS، اتصال خودکار
فایل‌ها	/etc/NetworkManager/system-connections/*.nmconnection
ابزارها	nmcli (خط فرمان)، nmtui (منوی متنی)، Cockpit، GNOME
RHEL 9 و 10	فارمت keyfile؛ فایل‌های قدیمی ifcfg در RHEL 10 دیگر استفاده نمی‌شوند
قانون	در حالی که NetworkManager کار می‌کند ویرایش نکنید — از nmcli استفاده کنید

IP ثابت با nmcli

```
[student@server1 ~]$ nmcli device status
[student@server1 ~]$ nmcli connection show
NAME    UUID        TYPE      DEVICE
enp1s0  9c2e...     ethernet  enp1s0
[student@server1 ~]$ sudo nmcli con mod enp1s0 ipv4.method manual \
      ipv4.addresses 10.0.0.11/24 ipv4.gateway 10.0.0.1 \
      ipv4.dns '10.0.0.1 1.1.1.1' ipv4.dns-search lab.local
[student@server1 ~]$ sudo nmcli con up enp1s0
[student@server1 ~]$ sudo nmcli con add con-name lab2 type ethernet ifname enp2s0 \
      ipv4.method manual ipv4.addresses 192.168.50.11/24
[student@server1 ~]$ sudo hostnamectl set-hostname server1.lab.local
```

تبدیل نام

```
[student@server1 ~]$ cat /etc/hosts
127.0.0.1   localhost
10.0.0.11   server1.lab.local server1
10.0.0.12   server2.lab.local server2
[student@server1 ~]$ cat /etc/resolv.conf      # written by NetworkManager
search lab.local
nameserver 10.0.0.1
[student@server1 ~]$ grep ^hosts /etc/nsswitch.conf
hosts:      files dns myhostname
[student@server1 ~]$ getent hosts server2      # uses the same order as programs
```

firewalld: zone ها، سرویس‌ها، پورت‌ها

مفهوم	معنی
Zone	یک سطح اعتماد برای شبکه؛ public پیش‌فرض است
Service	مجموعه نام‌دار پورت‌ها، مثلاً ssh = 22/tcp ،http = 80/tcp
Port	یک پورت/پروتوکول، مثلاً tcp/8080
Runtime در برابر permanent	Runtime با reload از بین می‌رود؛ --permanent ذخیره می‌شود
Rich rules	اجازه یا منع بر اساس آدرس منبع، لاگ، محدودیت
Backend	nftables در RHEL 9 و 10

استفاده از firewall-cmd

```
[student@server1 ~]$ sudo firewall-cmd --state ; sudo firewall-cmd --get-active-zones
[student@server1 ~]$ sudo firewall-cmd --list-all
public (active)
  interfaces: enp1s0
  services: cockpit dhcpv6-client ssh
[student@server1 ~]$ sudo firewall-cmd --permanent --add-service={http,https}
[student@server1 ~]$ sudo firewall-cmd --permanent --add-port=8080/tcp
[student@server1 ~]$ sudo firewall-cmd --permanent --remove-service=dhcpv6-client
[student@server1 ~]$ sudo firewall-cmd --permanent --add-rich-rule=\
      'rule family=ipv4 source address=10.0.0.0/24 service name=mysql accept'
[student@server1 ~]$ sudo firewall-cmd --reload ; sudo firewall-cmd --list-services
```

کلیدهای SSH

```
[student@server1 ~]$ ssh-keygen -t ed25519 -C 'student@server1'
Your public key has been saved in /home/student/.ssh/id_ed25519.pub
[student@server1 ~]$ ssh-copy-id student@server2
[student@server1 ~]$ ssh student@server2              # no password now
[student@server1 ~]$ ssh server2 'uptime; df -h /'    # run a remote command
[student@server1 ~]$ scp report.txt server2:/tmp/
[student@server1 ~]$ rsync -avz projects/ server2:projects/
[student@server1 ~]$ sftp server2
```

یک سرور SSH امن

```
[student@server2 ~]$ sudo vim /etc/ssh/sshd_config.d/50-security.conf
PermitRootLogin no
PasswordAuthentication no          # keys only (test your key first!)
MaxAuthTries 3
AllowGroups wheel sshusers
[student@server2 ~]$ sudo sshd -t                    # test the syntax
[student@server2 ~]$ sudo systemctl reload sshd

# A different port needs SELinux and firewall changes (Lesson 9):
[student@server2 ~]$ sudo semanage port -a -t ssh_port_t -p tcp 2222
```

عیب‌یابی شبکه

قدم	بررسی	فرمان
۱	آیا لینک بالا و آدرس درست است؟	ip -br addr; nmcli device status
۲	آیا به gateway می‌رسم؟	ping -c3 10.0.0.1; ip route
۳	آیا DNS کار می‌کند؟	dig redhat.com; getent hosts server2
۴	آیا سرویس گوش می‌دهد؟	ss -tlnp | grep :80; systemctl status httpd
۵	آیا فایروال باز است؟	firewall-cmd --list-all
۶	آیا SELinux جلوی آن را می‌گیرد؟	ausearch -m AVC -ts recent (درس ۹)
۷	لاگ‌ها چه می‌گویند؟	journalctl -u NetworkManager -u httpd

خلاصه و کارخانگی

- ip، ss، ping، dig، getent: قبل از تغییر نگاه کنید
- nmcli con mod … ipv4.method manual؛ nmcli con up
- DNS ← /etc/hosts (ترتیب در nsswitch.conf)
- firewall-cmd --permanent --add-service، بعد --reload
- ssh-keygen، ssh-copy-id؛ PermitRootLogin no
- کارخانگی: IP ثابت روی هر دو سرور، باز کردن http روی server1، SSH فقط با کلید به server2

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

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

درس ۱۰ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

سرویس‌ها: Apache، NFS، autofs و کانتینرهای Podman

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس دهم چه یاد می‌گیرید

- Apache (httpd): نصب، تنظیم، آزمایش
- Virtual host ها و HTTPS با mod_ssl
- سرور NFS روی server2؛ کلاینت NFS روی server1
- autofs: وصل در صورت نیاز
- Podman: کانتینرهای rootless، image ها، volume ها
- اجرای کانتینرها به عنوان سرویس systemd با Quadlet
- دیتابیس‌ها از AppStream: MariaDB و PostgreSQL

وب سرور Apache

```
[student@server1 ~]$ sudo dnf install -y httpd
[student@server1 ~]$ sudo systemctl enable --now httpd
[student@server1 ~]$ sudo firewall-cmd --permanent --add-service={http,https}
[student@server1 ~]$ sudo firewall-cmd --reload
[student@server1 ~]$ echo '<h1>Welcome to MyWebUniversity lab</h1>' | \
      sudo tee /var/www/html/index.html
[student@server1 ~]$ curl http://server1.lab.local
<h1>Welcome to MyWebUniversity lab</h1>
# Config: /etc/httpd/conf/httpd.conf  +  /etc/httpd/conf.d/*.conf
# Logs:   /var/log/httpd/access_log, error_log
[student@server1 ~]$ sudo apachectl configtest      # Syntax OK
```

ها Virtual host

```
# /etc/httpd/conf.d/courses.conf
<VirtualHost *:80>
    ServerName courses.lab.local
    DocumentRoot /srv/web/courses
    ErrorLog /var/log/httpd/courses-error.log
    CustomLog /var/log/httpd/courses-access.log combined
</VirtualHost>
<Directory /srv/web/courses>
    Require all granted
</Directory>
[student@server1 ~]$ sudo mkdir -p /srv/web/courses ; sudo restorecon -Rv /srv/web
[student@server1 ~]$ sudo apachectl configtest && sudo systemctl reload httpd
```

HTTPS با mod_ssl

```
[student@server1 ~]$ sudo dnf install -y mod_ssl
# Lab: a self-signed certificate (production: Let's Encrypt or your CA)
[student@server1 ~]$ sudo openssl req -x509 -newkey rsa:3072 -nodes -days 365 \
      -keyout /etc/pki/tls/private/courses.key -out /etc/pki/tls/certs/courses.crt \
      -subj '/CN=courses.lab.local'
<VirtualHost *:443>
    ServerName courses.lab.local
    DocumentRoot /srv/web/courses
    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/courses.crt
    SSLCertificateKeyFile /etc/pki/tls/private/courses.key
</VirtualHost>
[student@server1 ~]$ curl -k https://courses.lab.local
```

سرور NFS روی server2

```
[student@server2 ~]$ sudo dnf install -y nfs-utils
[student@server2 ~]$ sudo mkdir -p /exports/shared ; sudo chmod 2775 /exports/shared
[student@server2 ~]$ sudo vim /etc/exports
/exports/shared   10.0.0.0/24(rw,sync,root_squash)
[student@server2 ~]$ sudo systemctl enable --now nfs-server
[student@server2 ~]$ sudo exportfs -rav
exporting 10.0.0.0/24:/exports/shared
[student@server2 ~]$ sudo firewall-cmd --permanent --add-service={nfs,rpc-bind,mountd}
[student@server2 ~]$ sudo firewall-cmd --reload
```

کلاینت NFS و autofs روی server1

```
[student@server1 ~]$ showmount -e server2
/exports/shared 10.0.0.0/24
[student@server1 ~]$ sudo mkdir /mnt/shared
[student@server1 ~]$ sudo mount -t nfs server2:/exports/shared /mnt/shared
# Permanent (fstab):  server2:/exports/shared  /mnt/shared  nfs  defaults,_netdev  0 0

[student@server1 ~]$ sudo dnf install -y autofs
[student@server1 ~]$ echo '/nfs  /etc/auto.nfs' | sudo tee /etc/auto.master.d/nfs.autofs
[student@server1 ~]$ echo 'shared  -rw,sync  server2:/exports/shared' | sudo tee /etc/auto.nfs
[student@server1 ~]$ sudo systemctl enable --now autofs
[student@server1 ~]$ ls /nfs/shared        # mounted on first access
```

Podman: کانتینرها روی RHEL

موضوع	جزئیات
چیست	کانتینرهای OCI را اجرا می‌کند؛ فرمان‌های سازگار با Docker
بدون daemon	هیچ daemon پس‌زمینه ندارد؛ هر کانتینر یک پروسس عادی است
Rootless	کاربران عادی کانتینرها را امن اجرا می‌کنند
Image ها	image های UBI از registry.redhat.io (رایگان برای توزیع)، docker.io، quay.io
ابزارها	buildah، podman (ساختن)، skopeo (کاپی، بررسی)
امنیت	SELinux هر کانتینر را برچسب می‌زند؛ :Z روی volume ها

اجرای کانتینرها

```
[student@server1 ~]$ sudo dnf install -y container-tools
[student@server1 ~]$ podman search --limit 3 ubi10
[student@server1 ~]$ podman pull registry.access.redhat.com/ubi10/ubi
[student@server1 ~]$ podman run -it --rm ubi10/ubi cat /etc/redhat-release
[student@server1 ~]$ mkdir -p ~/site ; echo 'Hello from a container' > ~/site/index.html
[student@server1 ~]$ podman run -d --name web -p 8080:8080 \
      -v ~/site:/var/www/html:Z registry.access.redhat.com/ubi10/httpd-24
[student@server1 ~]$ podman ps ; curl http://localhost:8080
[student@server1 ~]$ podman logs web ; podman exec -it web bash
[student@server1 ~]$ podman stop web ; podman rm web ; podman images
```

کانتینرها به عنوان سرویس: Quadlet

```
[student@server1 ~]$ mkdir -p ~/.config/containers/systemd
[student@server1 ~]$ vim ~/.config/containers/systemd/web.container
[Container]
Image=registry.access.redhat.com/ubi10/httpd-24
PublishPort=8080:8080
Volume=%h/site:/var/www/html:Z
[Install]
WantedBy=default.target
[student@server1 ~]$ systemctl --user daemon-reload
[student@server1 ~]$ systemctl --user start web
[student@server1 ~]$ sudo loginctl enable-linger student     # run without a login
```

دیتابیس‌ها از AppStream

دیتابیس	نصب و شروع	یادداشت
MariaDB	dnf install mariadb-server; systemctl enable --now mariadb	mariadb-secure-installation را اجرا کنید
MySQL	dnf install mysql-server; systemctl enable --now mysqld	MySQL 8.4 LTS
PostgreSQL	dnf install postgresql-server; postgresql-setup --initdb	نسخه‌های نوتر مانند postgresql18
فایروال	firewall-cmd --add-service=mysql / postgresql	فقط برای سرورهای برنامه باز کنید
SELinux	پورت‌ها و مسیرهای پیش‌فرض از قبل برچسب دارند	دایرکتوری دیتای سفارشی؟ semanage fcontext
کانتینرها	podman run … rhel10/postgresql-16	سریع برای توسعه

خلاصه و کارخانگی

- httpd + virtual host ها در conf.d؛ apachectl configtest؛ mod_ssl برای HTTPS
- NFS: /exportfs -rav + etc/exports؛ فایروال nfs، rpc-bind، mountd
- کلاینت: mount -t nfs، fstab با _netdev، یا autofs در صورت نیاز
- Podman: rootless، volume با :Z، image های UBI؛ Quadlet برای سرویس‌ها
- دیتابیس‌ها از AppStream؛ پورت‌ها را با احتیاط باز کنید
- کارخانگی: courses.lab.local با HTTPS روی server1؛ اشتراک NFS از server2 با autofs؛ یک کانتینر ویب با Quadlet

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

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

درس ۱۲ از ۱۲

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

اسکریپت‌نویسی، Image، Ansible، Mode، عیب‌یابی و RHCSA

دوره کامل · RHEL 10.3 & 9.9 (Nov 2026)



در درس دوازدهم چه یاد می‌گیرید

- اسکریپت‌نویسی bash: متغیرها، شرط‌ها، حلقه‌ها، exit code ها
- یک اسکریپت واقعی: گزارش سلامت سرور
- Ansible: inventory، فرمان‌های ad hoc، playbook ها
- RHEL system roles
- Image mode (bootc): RHEL به شکل container image
- یک روش عیب‌یابی از بوت تا برنامه
- امتحان‌های RHCSA و RHCE، و قدم بعدی

اساسات اسکریپت‌نویسی bash

```
#!/bin/bash
# /usr/local/bin/adduser-batch.sh — create users from a file
set -euo pipefail
file=${1:?usage: $0 users.txt}
if [[ ! -r $file ]]; then
    echo "Cannot read $file" >&2 ; exit 1
fi
while read -r user group; do
    if id "$user" &>/dev/null; then
        echo "skip: $user exists"
    else
        useradd -G "$group" "$user" && echo "added: $user ($group)"
    fi
done < "$file"
```

اجزای اسکریپت

جزء	مثال
متغیرها	name=web01 ; echo "Host: $name" ; today=$(date +%F)
آرگومِنت‌ها	$1 $2 … ; $# count ; $@ all ; $0 script name
Exit code ها	$? — 0 = موفق؛ هر چیز دیگر = ناکام
آزمایش‌ها	[[-f file]] [[-d dir]] [[$a == $b]] ((n > 5))
حلقه‌ها	for h in server1 server2; do ssh $h uptime; done
Function ها	log() { echo "$(date +%T) $*"; }
بررسی اسکریپت‌ها	bash -n script.sh ; shellcheck script.sh (EPEL)

یک اسکریپت واقعی: گزارش سلامت سرور

```
#!/bin/bash
# /usr/local/bin/health.sh — run daily from cron or a systemd timer
echo "== $(hostname) $(date '+%F %T') =="
echo "Uptime: $(uptime -p)"
echo "Load:   $(cut -d' ' -f1-3 /proc/loadavg)"
df -h --output=target,pcent -x tmpfs | awk 'NR>1 && $2+0 > 80 {print "DISK WARNING:", $0}'
free -m | awk '/Mem/ {printf "Memory used: %d%%\n", $3*100/$2}'
systemctl --failed --no-legend | sed 's/^/FAILED: /'
echo "SELinux: $(getenforce)   Updates waiting: $(dnf -q check-update | grep -c .)"
journalctl -p err --since yesterday --no-pager | tail -5
```

Ansible: inventory و فرمان‌های ad hoc

```
[student@server1 ~]$ sudo dnf install -y ansible-core rhel-system-roles
[student@server1 ~]$ mkdir ~/ansible && cd ~/ansible
[student@server1 ansible]$ cat inventory
[web]
server1.lab.local
[files]
server2.lab.local
[student@server1 ansible]$ cat ansible.cfg
[defaults]
inventory = ./inventory
[privilege_escalation]
become = true
[student@server1 ansible]$ ansible all -m ping
[student@server1 ansible]$ ansible files -m dnf -a 'name=htop state=present'
```

یک playbook

```
# web.yml
- name: Configure web servers
  hosts: web
  tasks:
    - name: Install Apache
      ansible.builtin.dnf: { name: httpd, state: latest }
    - name: Home page
      ansible.builtin.copy:
        content: "Managed by Ansible on {{ inventory_hostname }}\n"
        dest: /var/www/html/index.html
    - name: Start and enable
      ansible.builtin.service: { name: httpd, state: started, enabled: true }
    - name: Open firewall
      ansible.posix.firewalld: { service: http, permanent: true, immediate: true, state: enabled }
[student@server1 ansible]$ ansible-playbook web.yml
```

RHEL System Roles

Role	چه را تنظیم می‌کند
rhel-system-roles.timesync	منابع زمان chrony
rhel-system-roles.firewall	zone ها، سرویس‌ها و پورت‌های firewalld
rhel-system-roles.selinux	حالت‌ها، boolean ها، context فایل، پورت‌ها
rhel-system-roles.storage	پارتیشن‌ها، LVM، فایل سیستم‌ها، وصل‌ها
rhel-system-roles.network	اتصال‌های NetworkManager
rhel-system-roles.podman	کانتینرها و unit های Quadlet
مستندات و مثال‌ها	/usr/share/doc/rhel-system-roles/

Image mode: RHEL به شکل container image

```
# Containerfile
FROM registry.redhat.io/rhel10/rhel-bootc:10.3
RUN dnf -y install httpd && systemctl enable httpd
COPY index.html /var/www/html/

[student@server1 ~]$ podman build -t registry.lab.local/web-os:1.0 .
[student@server1 ~]$ podman push registry.lab.local/web-os:1.0
# Install: bootc-image-builder makes an ISO, qcow2 or cloud image from it
# On a running image-mode host:
[root@web01 ~]# bootc status
[root@web01 ~]# bootc upgrade      # pull the new image, applied at next reboot
[root@web01 ~]# bootc rollback     # go back to the previous image
```

یک روش عیب‌یابی

لایه	بپرسید	ابزارها
بوت	بوت می‌شود؟ کدام target؟	GRUB menu, rd.break, journalctl -b -1
ذخیره‌سازی	دیسک پر؟ خط بد در fstab؟	df -h, lsblk, mount -a, emergency mode
شبکه	آدرس، gateway، DNS؟	ip، ping، dig، nmcli (قدم‌های درس ۸)
سرویس	در حال اجرا؟ فعال؟ خطا؟	systemctl status, journalctl -u
امنیت	فایروال؟ SELinux؟ اجازه‌ها؟	firewall-cmd, ausearch -m AVC, ls -lZ
منابع	CPU، حافظه، I/O؟	top, free, vmstat, iostat (sysstat)
تغییر	اخیراً چه تغییر کرد؟	dnf history, journalctl, git log of configs

RHCSA، RHCE و قدم‌های بعدی

جزئیات	مورد
امتحان عملی: کارهای واقعی روی سیستم‌های زنده؛ این دوره موضوعات آن را پوشش می‌دهد	RHCSA (EX200)
خودکارسازی با Ansible؛ RHCSA لازم است	RHCE (EX294)
هر کارخانگی را دو بار انجام دهید؛ وقت بگیرید؛ فقط از man استفاده کنید	تمرین
نسخه و اهداف فعلی امتحان در redhat.com	قبل از ثبت‌نام بررسی کنید
Red Hat Developer، docs.redhat.com، ویدیوها و PDF های ما	یادگیری رایگان
Rocky Linux 9/10، خانواده Fedora، Debian/Ubuntu در MyWebUniversity	دوره‌های بعدی

خلاصه دوره

- درس‌های ۱–۳: نسخه‌ها و لابراتوار، نصب و Cockpit، خط فرمان
- درس‌های ۴–۶: کاربران و اجازه‌ها، dnf، systemd، بوت و لاگ‌ها
- درس‌های ۷–۹: ذخیره‌سازی و LVM، شبکه و firewalld، SELinux
- درس‌های ۱۰–۱۱: Apache، NFS، Podman؛ امنیت، بکاپ، ارتقا از 9 به 10
- درس ۱۲: اسکریپت‌نویسی، Ansible، image mode، عیب‌یابی، RHCSA
- پروژه نهایی: server1 را از صفر با یک Ansible playbook دوباره 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