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