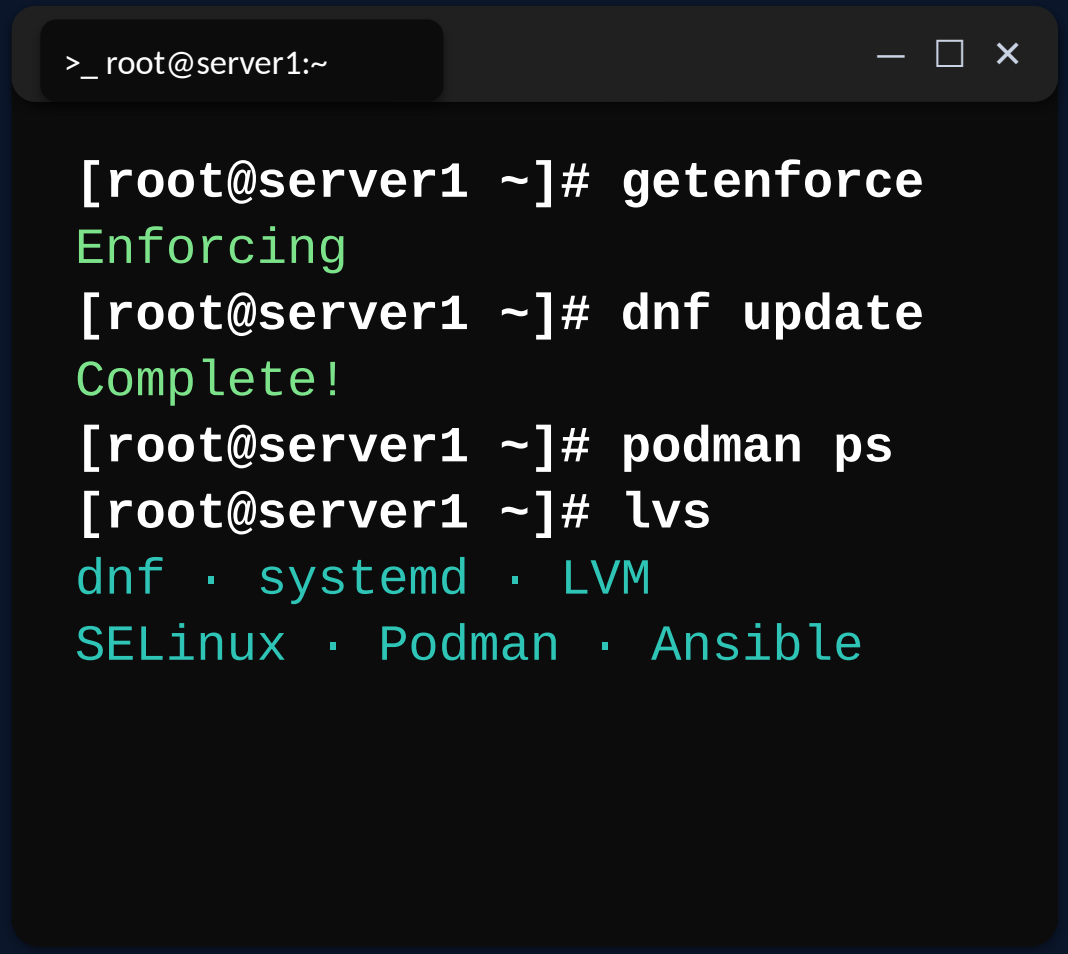


LESSON 11 OF 12

Red Hat Enterprise Linux

RHEL 9 & 10 · Admin · SELinux

Security, Updates, Time, Backup & Upgrading 9 to 10

Full Course · RHEL 10.3 & 9.9 (Nov 2026)

What You Will Learn in Lesson 11

- A hardening checklist for every server
- System-wide crypto policies and post-quantum crypto
- Compliance scanning with OpenSCAP; fapolicyd
- Accurate time with chrony
- Patch management and Red Hat Lightspeed (Insights)
- Backup and restore: tar, rsync, ReaR
- In-place upgrade RHEL 9 → 10 with Leapp

Hardening Checklist

Area	Do this
Software	Install only what you need (Minimal / Server); remove the rest
Accounts	Lock root; sudo + wheel; strong pwquality; remove old users
SSH	Keys only; PermitRootLogin no; AllowGroups (Lesson 8)
Network	firewalld default zone with only needed services (ss -tulpn)
SELinux	Enforcing, always (Lesson 9)
Updates and logs	Security updates weekly; persistent journal; central logging
Storage	LUKS for laptops and sensitive data; separate /var/log if possible

System-Wide Crypto Policies

```
[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
```

Compliance Scanning with 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
```

More Security Tools

Tool	What it does
fapolicyd	Allows only trusted programs to run (application allow-listing)
AIDE	Detects changed files: aide --init, then aide --check
auditd	Records security events: ausearch, aureport, audit rules
usbguard	Blocks unknown USB devices
Lightspeed (Insights)	Red Hat's analysis: vulnerabilities, advisories, risks
MCP server for RHEL (10.3)	Lets an AI assistant read system data for diagnostics, with controlled access

Accurate Time with 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
```

Patch Management

Practice	How
Know what is missing	dnf updateinfo summary; Lightspeed vulnerability service
Test first	Patch test servers, wait, then production
Schedule	Security weekly; full updates monthly; maintenance windows
Automate	dnf-automatic, Ansible, or Red Hat Satellite
Reboot when needed	dnf needs-restarting -r; kernel live patching (kpatch) for critical servers
Roll back	dnf history undo; LVM or VM snapshots before big changes

Backup and Restore

```
# 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
```

In-Place Upgrade: RHEL 9.9 → 10.3 with 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)
```

Summary and Homework

- Hardening: minimal software, keys, firewall, SELinux, updates
- update-crypto-policies; OpenSCAP scans against CIS / STIG
- chrony for accurate time: chronyc sources, tracking
- Patch with a plan: test, schedule, automate, roll back
- tar --acls --selinux, rsync -aAX, ReaR; test your restores
- Homework: run an OpenSCAP CIS report; upgrade server2 from 9.9 to 10.3 with Leapp (after a snapshot)

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

Slides for this lesson: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity · @MyWebUniversity-Dari

Wahidullah Lutfy — Founder and Director of IT of MyWebUniversity, and CS teacher

Book: The Direct Path to Linux Ubuntu (Amazon · Barnes & Noble)

Learn it, then pass it on.