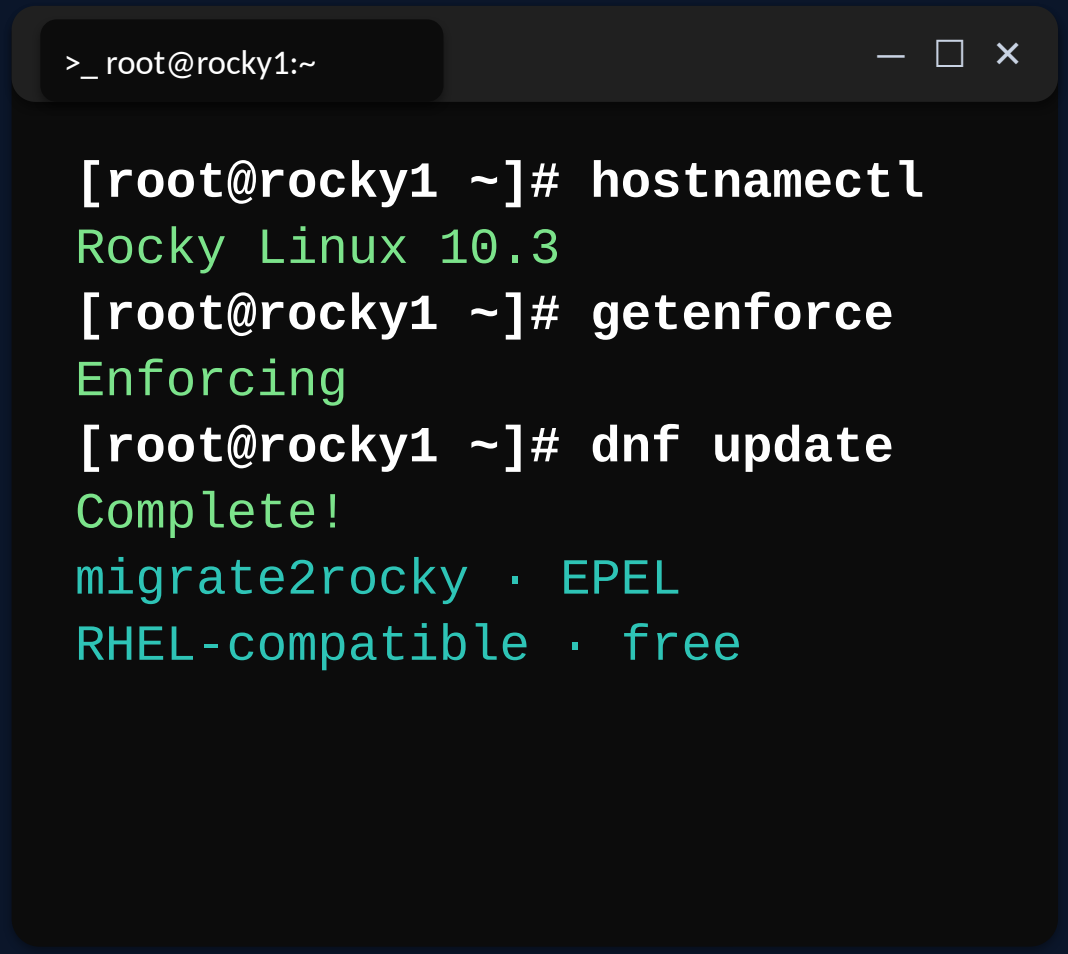


LESSON 4 OF 12

Rocky Linux 9 & 10

Install · Migrate · Differences

Updates, Errata & Security on Rocky Linux

Full Course · Rocky Linux 10.3 & 9.9 (Nov 2026)

What You Will Learn in Lesson 4

- How security fixes flow: RHEL → Rocky
- Rocky errata (RLSA, RLBA, RLEA) and dnf updateinfo
- Checking a CVE on your system
- Automatic updates with dnf-automatic
- Kernel updates, reboots and rollback
- Hardening Rocky: SELinux, firewalld, crypto policies, OpenSCAP
- Watching your servers without a subscription

How Security Fixes Reach Rocky

Step	What happens
1	A vulnerability (CVE) is found and fixed upstream
2	Red Hat releases an advisory (RHSA) and updated RHEL packages
3	The fixed sources appear publicly (CentOS Stream and other public sources)
4	Rocky rebuilds, tests and signs the packages
5	Rocky publishes an advisory (RLSA) and the packages reach mirrors
Typical delay	Usually hours to a few days; urgent fixes are prioritized

Rocky Errata

Type	Meaning	Example
RLSA	Rocky Linux Security Advisory	RLSA-2026:xxxx openssl
RLBA	Bug fix advisory	RLBA-2026:xxxx systemd
RLEA	Enhancement advisory	RLEA-2026:xxxx podman
Severity	Critical, Important, Moderate, Low	Patch Critical and Important first
Where	errata.rockylinux.org; also inside dnf	Search by CVE or package

Errata with dnf updateinfo

```
[student@rocky1 ~]$ dnf updateinfo summary
Updates Information Summary: available
    3 Security notice(s)
        1 Important Security notice(s)
        2 Moderate Security notice(s)
    5 Bugfix notice(s)
[student@rocky1 ~]$ dnf updateinfo list --security
[student@rocky1 ~]$ dnf updateinfo info RLSA-2026:xxxx
[student@rocky1 ~]$ sudo dnf upgrade --security                # security fixes only
[student@rocky1 ~]$ sudo dnf upgrade --advisory=RLSA-2026:xxxx # one advisory
[student@rocky1 ~]$ sudo dnf upgrade --sec-severity=Critical
```

Is This CVE Fixed on My Server?

```
[student@rocky1 ~]$ dnf updateinfo list --cve CVE-2026-xxxxx      # waiting?
[student@rocky1 ~]$ dnf updateinfo list --installed --cve CVE-2026-xxxxx   # already fixed?
[student@rocky1 ~]$ rpm -q --changelog openssl | grep -i CVE-2026 | head
[student@rocky1 ~]$ rpm -q openssl kernel
[student@rocky1 ~]$ uname -r                # the RUNNING kernel may be older!
[student@rocky1 ~]$ sudo dnf needs-restarting -r
Core libraries or services have been updated since boot-up:
  * kernel
Reboot is required to fully utilize these updates.
```

Automatic Updates with dnf-automatic

```
[student@rocky1 ~]$ sudo dnf install -y dnf-automatic
[student@rocky1 ~]$ sudo vim /etc/dnf/automatic.conf
[commands]
upgrade_type = security          # or default (all updates)
apply_updates = yes
reboot = when-needed             # check: man dnf-automatic
[emitters]
emit_via = motd                  # or email, command_email
[student@rocky1 ~]$ sudo systemctl enable --now dnf-automatic.timer
[student@rocky1 ~]$ systemctl list-timers dnf-automatic*
```

Kernel Updates, Reboots and Rollback

Task	How
Keep old kernels	installonly_limit=3 in /etc/dnf/dnf.conf (default)
Boot an older kernel	Choose it in the GRUB menu if the new one fails
Make it the default	sudo grubby --set-default /boot/vmlinuz-<version>
See kernels	sudo grubby --info=ALL | grep ^kernel
Live patching	Not provided by Rocky; commercial options exist (e.g. from CIQ)
Undo packages	dnf history undo <id>; snapshots before big changes

Hardening Rocky with Free Tools

```
[student@rocky1 ~]$ getenforce                          # Enforcing — keep it!
[student@rocky1 ~]$ sudo firewall-cmd --list-all
[student@rocky1 ~]$ update-crypto-policies --show       # DEFAULT
[student@rocky1 ~]$ sudo dnf install -y openscap-scanner scap-security-guide
[student@rocky1 ~]$ ls /usr/share/xml/scap/ssg/content/ | grep -i -E 'rl|rocky|rhel'
[student@rocky1 ~]$ sudo oscap xccdf eval --profile cis --report /tmp/cis.html \
      /usr/share/xml/scap/ssg/content/<datastream-for-your-version>.xml
[student@rocky1 ~]$ sudo dnf install -y fail2ban aide ; sudo systemctl enable --now fail2ban
```

Watching Servers Without a Subscription

Need	Free option
Updates waiting	dnf updateinfo summary via Ansible or a cron report
Health and metrics	Cockpit, PCP, Prometheus node_exporter + Grafana
Logs	Central rsyslog or journald remote; Loki or OpenSearch
Vulnerability scanning	OpenSCAP; open source scanners such as Trivy for images
Inventory and patching	Foreman/Katello (Lesson 11), Ansible
Commercial	CIQ and others offer support and management for Rocky

Summary and Homework

- Fixes flow RHEL → public sources → Rocky rebuild → RLSA
- dnf updateinfo summary / list --security / --cve
- dnf upgrade --security; dnf-automatic for automation
- Reboot for kernel fixes: needs-restarting -r; grubby for rollback
- Free hardening: SELinux, firewalld, crypto policies, OpenSCAP, fail2ban
- Homework: report waiting security advisories on rocky1; enable dnf-automatic for security updates

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.