Services, Boot & Logs (Core)

Linux Commands Course · Section 11

What Is systemd?

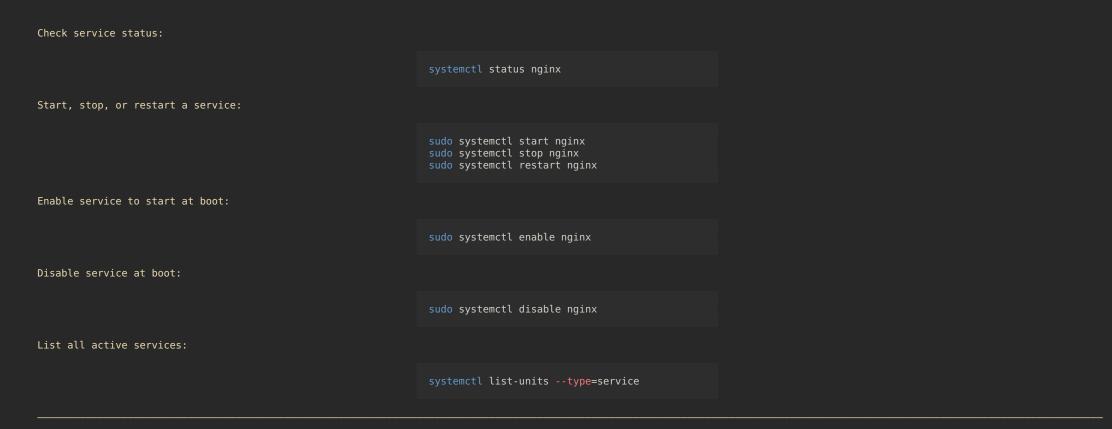
systemd is the default init system on most modern Linux distributions.

It manages:

- Service startup and shutdownBoot targets (runlevels)System logging (via journalctl)Time and clock synchronization

All of this is unified under the systemctl command.

Managing Services — systemctl



Inspecting All Units

A "unit" can be a service, device, socket, or timer.		
List failed units:		
	systemctlfailed	
List all (loaded) units:		
	systemctl list-units	

Viewing Boot Targets

A target defines which services and environment are active - like traditional runlevels.

Show the current target:

systemctl get-default

Common targets:

graphical.target - GUI mode
multi-user text mode
rescue.target - multi-user text mode
rescue.target - maintenance mode

Switch (temporarily) to another target:

sudo systemctl isolate multi-user.target

sudo systemctl set-default graphical.target

sudo systemctl set-default graphical.target

System Time Management — timedatectl

Display current date, time, and time zone:		
	timedatectl	
Set the system time zone:		
	sudo timedatectl set-timezone Europe/Baku	
Enable NTP (Network Time Protocol) synchronization:		
	sudo timedatectl set-ntp true	
This ensures automatic time syncing with internet servers.		

Service Logs — journalctl

journalctl reads logs from the systemd journal — a binary log database maintained by systemd-journald. Show all logs: Show logs for a specific service: View logs since the last boot: Filter by time: Follow live logs (like tail -f):

Filtering by Priority

Classic Log Files - /var/log

Older and non-systemd logs still live under /var/log.

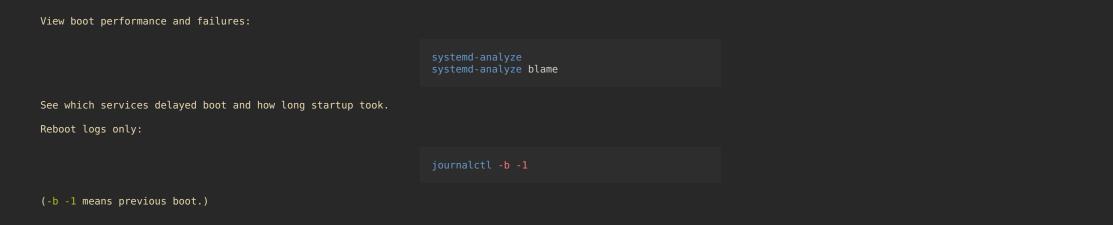
Common log files:

File	Description
<pre>/var/log/syslog /var/log/messages /var/log/auth.log /var/log/dmesg /var/log/nginx/ /var/log/secure</pre>	General system activity (Debian/Ubuntu) General system log (RHEL/Fedora) Authentication and sudo logs Kernel messages during boot Web server logs Security messages (RHEL-based)

Inspect with standard tools:

sudo less /var/log/syslog
sudo tail -f /var/log/auth.log

Boot Diagnostics



Combining Tools

Practical example — check a web server status, restart it, and read its logs:

sudo systemctl status nginx
sudo systemctl restart nginx
journalctl -u nginx --since today

You'll often use systemctl and journalctl together when troubleshooting.

Recap

- Services: manage with systemctl start/stop/restart/status
 Boot control: systemctl get-default, isolate, set-default
 Time management: timedatectl
 Logs: use journalctl and /var/log/ for full visibility

Together, these tools give total control over system services and events.