Services, Boot & Logs (Core)

Linux Commands Course · Section 11

Goal

Learn how to manage system services, control boot behavior, and inspect logs using modern systemd tools.

You'll understand how Linux starts, how services run, and where to find diagnostic information.

What Is systemd?

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

It manages:

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

All of this is unified under the systematl command.

Managing Services — systemctl

Check service status:		
	systemctl status nginx	
Start, stop, or restart a service:		
	<pre>sudo systemctl start nginx sudo systemctl stop nginx sudo systemctl restart nginx</pre>	
Enable service to start at boot:		
	sudo systemctl enable nginx	
Disable service at boot:		
	sudo systemctl disable nginx	
List all active services:		
	systemctl list-unitstype=service	

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.target — multi-user text mode
rescue.target — multi-user text mode
sudo systemctl isolate multi-user.target

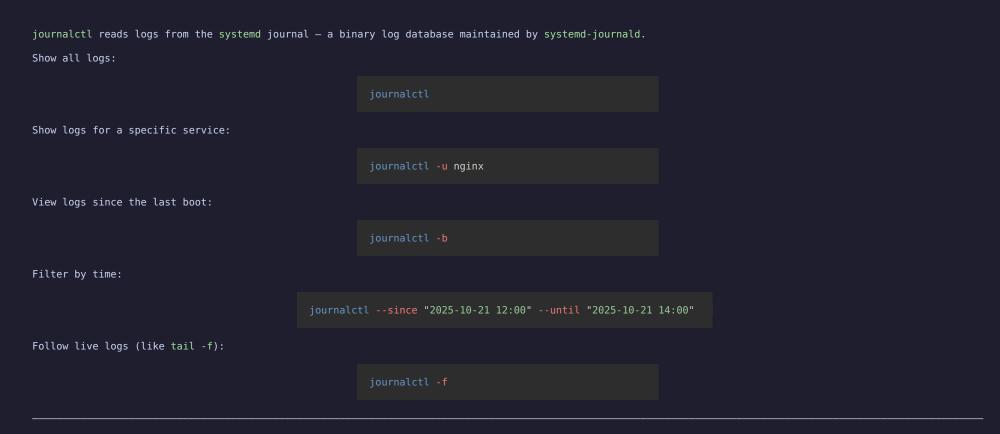
Set the default boot target permanently:

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 serve	ers.	

Service Logs — journalctl



Filtering by Priority

Show only errors:		
	journalctl -p err	
Show warnings and higher:		
	journalctl -p warning	
Priority levels range from 0 (emerg) to 7 (debug).		

Classic Log Files - /var/log

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

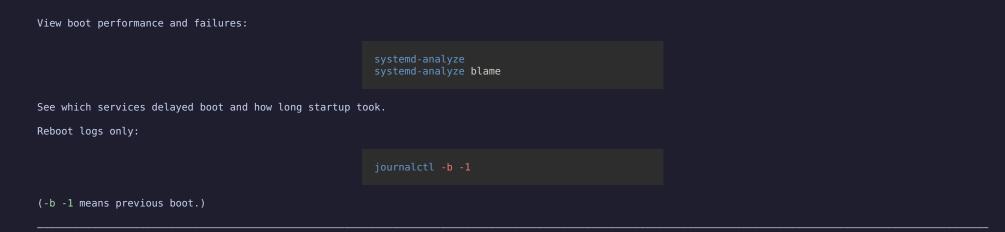
Common log files:

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.

Practice

- Check which target your system boots into.
 Restart the SSH or networking service.
 Enable automatic NTP time sync with timedatectl.
 View all logs since last boot.
 Display only authentication errors from the system journal.
 Examine /var/log/syslog for today's entries.

Next Up

Networking (Core) — exploring interfaces, routes, and connectivity tools.