Services, Boot & Logs (Core)

Linux Commands Course · Section 11

IDSchool

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 `systemctl` command.

Managing Services — systemctl

Check service status:

```
systemctl status nginx
```

Start, stop, or restart a service:

```
sudo systemctl start nginx
sudo systemctl stop nginx
sudo systemctl restart nginx
```

Enable service to start at boot:

```
sudo systemctl enable nginx
```

Disable service at boot:

Inspecting All Units

A “unit” can be a service, device, socket, or timer.

List failed units:

```
systemctl --failed
```

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 — maintenance mode

Switch (temporarily) to another target:

```
sudo systemctl isolate multi-user.target
```

Set the default boot target permanently:

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:

```
journalctl
```

Show logs for a specific service:

```
journalctl -u nginx
```

View logs since the last boot:

```
journalctl -b
```

Filter by time:

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

Inspect with standard tools:

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

Boot Diagnostics

View boot performance and failures:

```
systemd-analyze
systemd-analyze blame
```

See which services delayed boot and how long startup took.

Reboot logs only:

```
journalctl -b -1
```

(`-b -1` means previous boot.)

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.