Logování (Logging)

Logování je systematický zápis informací o aktivitě systému do textových souborů (logů) nebo specializovaných databází. Dobře nastavené logování umožňuje zpětně zjistit, co se v systému stalo, kdy se to stalo a proč k tomu došlo.

1. Úrovně logování (Log Levels)

Aby bylo možné v obrovském množství dat filtrovat, používá se standardizovaná hierarchie důležitosti. Většina systémů (včetně Linuxu) používá standard **Syslog**:

Úroveň	Název	Význam
0	**EMERGENCY**	Systém je nepoužitelný (panika).
1	**ALERT**	Je nutná okamžitá akce.
2	**CRITICAL**	Kritický stav (např. selhání HW).
3	**ERROR**	Došlo k chybě, ale systém běží dál.
4	**WARNING**	Varování, které může v budoucnu vést k chybě.
5	**NOTICE**	Normální, ale významná událost.
6	**INFO**	Běžná informativní zpráva o aktivitě.
7	**DEBUG**	Detailní výpisy pro vývojáře (při hledání chyb).

2. Kam se v Linuxu ukládají logy?

Většina systémových logů se nachází v adresáři **/var/log/**.

- **/var/log/syslog** (nebo **messages**): Hlavní systémový log.
- **/var/log/auth.log**: Záznamy o přihlášení a bezpečnosti.
- **/var/log/apache2/** (nebo **nginx/**): Logy webového serveru.
- **/var/log/dmesg**: Zprávy z jádra systému (kernelu) po startu.

3. Práce s logy v příkazové řádce

K analýze logů se nejčastěji používají nástroje, které jsme již probrali:

- **tail -f /var/log/syslog**: Sleduje log v reálném čase (nové řádky se okamžitě vypisují).
- **grep „ERROR“ /var/log/myapp.log**: Vyfiltruje pouze chybové hlášky.
- **journalctl -u nginx**: Moderní způsob prohlížení logů v systémech se *systemd*.

4. Správa logů (Log Rotation)

Logy mohou velmi rychle narůst a zaplnit celý disk. Proto existuje nástroj **logrotate**, který:

```
1. Staré logy zkomprimuje (např. do .gz).
2. Po určité době (např. 30 dní) je smaže.
3. Přejmenuje aktuální log a založí nový.
```

5. Moderní centralizované logování

U velkých cloudových aplikací (běžících na stovkách serverů) není možné procházet logy ručně. Používají se tzv. **Log Management** platformy:

- **ELK Stack:** (Elasticsearch, Logstash, Kibana) – standard pro vyhledávání a vizualizaci logů.
- **Grafana Loki:** Moderní a úsporný systém pro logy v Kubernetes.
- **Splunk:** Komerční nástroj pro hloubkovou analýzu strojových dat.

> **Důležité pravidlo:** Nikdy nelogujte citlivá data! Do logů nepatří hesla, čísla platebních karet ani osobní údaje (GDPR). V případě úniku dat by se logy staly zlatým dolem pro útočníky.

Zpět na Rozcestník