ELK Stack (Elastic Stack)

ELK Stack je zkratka pro spojení tří open-source projektů vyvíjených společností Elastic: **Elasticsearch**, **Logstash** a **Kibana**. Společně tvoří ucelenou platformu, která dokáže pojmout miliony záznamů z různých zdrojů a bleskově v nich vyhledávat.

V novějších verzích se k trojici přidal čtvrtý člen – **Beats**, proto se dnes častěji používá název **Elastic Stack**.

Komponenty stacku a jejich role

Proces zpracování dat připomíná výrobní linku:

1. Beats (Sběr dat)

Lehcí agenti (odesílatelé), kteří se instalují přímo na koncová zařízení nebo servery. Jejich úkolem je pouze sbírat data a posílat ich dál.

- **Filebeat:** Sleduje soubory s logy (např. `/var/log/syslog`).
- **Metricbeat:** Sbírá systémové metriky (využití CPU, RAM).

2. Logstash (Zpracování a transformace)

Nástroj pro úpravu dat. Data z různých zdrojů (často nesourodá) zde projdou filtry, které je vyčistí a sjednotí.

- Dokáže například z řádku textu vytáhnout IP adresu, uživatelské jméno a pomocí filtru Grok je rozdělit do políček.

3. Elasticsearch (Ukládání a vyhledávání)

Srdce celého systému. Jde o distribuovaný vyhledávací engine. Data ukládá ve formátu JSON do tzv. indexů. Díky své architektuře dokáže prohledávat terabajty dat v řádu milisekund.

4. Kibana (Vizualizace)

Webové grafické rozhraní. V Kibaně si uživatelé klikají na grafy, vytvářejí mapy a dashboardy. Slouží k tomu, aby data z Elasticsearch byla čitelná pro člověka.

Architektura a tok dat

Typický tok dat vypadá takto: **[Zdroj/Server]** –(Beats)–> **[Logstash]** –(JSON)–> **[Elasticsearch]** ←→ **[Kibana]**

V moderních a jednodušších nasazeních mohou Beats posílat data přímo do Elasticsearch, pokud není vyžadována složitá transformace v Logstashi.

Hlavní využití v praxi

- **Log Management:** Centrální místo pro logy ze všech firemních serverů, routerů a aplikací.
- **Monitoring infrastruktury:** Sledování zdraví systémů v reálném čase (např. upozornění při zaplnění disku).
- **Security (SIEM):** Hledání bezpečnostních incidentů (např. detekce útoku typu Brute Force analýzou logů z firewallu).
- **Full-text search:** Vyhledávač uvnitř e-shopů nebo dokumentací.

Klíčové výhody

- **Škálovatelnost:** Systém můžete začít na jednom serveru a postupně ho rozšířit na stovky uzlů.
- **Real-time:** Data jsou dostupná k analýze téměř okamžitě po jejich vygenerování (latence v řádu sekund).
- **Flexibilita:** Stack si poradí s jakýmkoliv formátem dat (strukturovaným i nestrukturovaným).

> **Tip pro správce:** Elasticsearch je velmi náročný na operační paměť (RAM). Pro plynulý chod produkčního ELK Stacku je kritické správně nastavit velikost JVM heapu.

— **Viz také:** Grok, SIEM, Cloud Monitoring, JSON