

**PROJEKT Č. 4**

**Sběr, ukládání a vizualizace logů, hrozeb a HW statistik**

B0B32KTI - Komunikační technologie pro IoT

Jan Tonner, Petr Procházka, Petr Kučera

22. 11. 2022 | ČVUT Praha

# Obsah

[**Abstrakt**](#_e3arxjr4tpx9) **3**

[Cíl projektu](#_ffyidc1i3avt) 3

[Závěr projektu](#_21ommofpuhq) 3

[**Průběh projektu**](#_pounl62rsaes) **4**

[Naplánování spolupráce](#_ihtt9dvsprcn) 4

[Průběh práce](#_fwj3b5xbwrpq) 5

[Rešerše](#_neh9eca8r9o) 5

[Uvedení do problematiky](#_vnjmpn7vtfo2) 5

[Přehled nástrojů a služeb](#_dwe6dkprv3tp) 5

[Elastic Stack](#_j2pvsy3fu3ae) 5

[Beats](#_5quxbul3ew70) 5

[Logstash](#_ib1ir7wcgqi3) 5

[Elasticsearch](#_wyv5ku8yrp1s) 5

[Kibana](#_rrun55hkvlgy) 5

[Microsoft](#_uh0uebeygicy) 5

[Power BI](#_q76kxaddmkkv) 5

[Azure Monitor](#_1aobttrkz42c) 6

[TIG Stack](#_8zoxs5abj27n) 6

[Grafana](#_wn6rijpccjww) 6

[InfluxDB](#_dye7a96wz2xo) 6

[Telegraf](#_ilh18snkyc5n) 6

[Měření](#_u6cwt57hhytd) 7

[Popis měřené infrastruktury](#_9icv7y56664d) 7

[Výsledný Dashboard](#_zdjc2mxn4akl) 7

[Závěr práce](#_sixylvnazj5r) 9

[Zhodnocení měření](#_f7nojchrb7e2) 9

[Zhodnocení spolupráce](#_nd9vvo5axb0o) 9

[**Zdroje**](#_yazzxhksboyh) **10**

[Literatura a reference](#_iqwscoldhmy) 10

# Abstrakt

## Cíl projektu

Cílem čtvrtého projektu je nastudovat možnosti sbírání, ukládání a vizualizace dat v *open-source* prostředí.

## Závěr projektu

Byly analyzovány nástroje pro sběr, posílání, ukládání a zobrazení dat a systémových logů. Byly vytvořeny dashboardy s vizualizací požadovaných měřených parametrů. Dílčí problémy byly identifikovány a odstraněny, zejména restartem sondy.

# Průběh projektu

## Naplánování spolupráce

Na tomto projektu budeme spolupracovat během úterků po obědě v pauze mezi předměty. Prvně si detailně prostudujeme zadání, abychom se vyvarovali chybám z předchozích projektů, (např. nepozorné prostudování požadavků na projekt před začátkem samotné práce). Následně se každý z nás zaměří na danou oblast (Jan T. - konfigurace sondy a logování dat, Petr K. - tvorba rešerše a logování dat, Petr P. - konfigurace sondy a logování dat) tak, abychom zefektivnili spolupráci. V závěru vše společně zhodnotíme.

## Průběh práce

### Rešerše

#### Uvedení do problematiky

V dnešní době velikého množství zařízení a jejich variability je vhodné mít nástroj, který umožní sbírat data ze zařízení, orientovat se v nich a na jejich základě vyhodnocovat závěry, které vedou ke konkrétním akcím.

#### Přehled nástrojů a služeb

Příkladem jsou 2 *open-source* řešení (Elastic Stack a TIG Stack) a jedno komerční od firmy Microsoft.

##### Elastic Stack

###### Beats

Beats je *open-source* nástroj pro přenesení dat z agenta na lokálním serveru do Elasticsearch.[[1]](#footnote-0)

###### Logstash

Logstash je *open-source* nástroj pro sbírání dat z různých zdrojů a posílání dat do cílové destinace.[[2]](#footnote-1)

###### Elasticsearch

Elasticsearch je distribuovaný fulltextový vyhledávací engine vycházející z *Apache Lucene*. Poskytuje REST APIs s fysokou dostupností a škálovatelností. Je vyvíjený v *Javě*. [[3]](#footnote-2)Elasticsearch je hlavním komponentem tzv. Elastic Stacku, který obsahuje *open-source* nástroje sloužící k ukládání, analýze a vizualizace.[[4]](#footnote-3)

###### Kibana

Kibana je *open-source* frontendová aplikace poskytující vyhledávání a vizualizace dat indexovaných v Elasticsearch.[[5]](#footnote-4)

##### Microsoft

###### Power BI

Nástroj od společnosti Microsoft sloužící k analýze dat s primárním zaměřením na business intelligence.[[6]](#footnote-5)

###### Azure Monitor

Nástroj od společnosti Microsoft sloužící k měření, monitorování a vyvození akcí na základě dat z daných zařízení. Existuje jak cloudová tak on-premise verze.[[7]](#footnote-6)

##### TIG Stack

TIG Stack je pojem označující **T**elegraf, **I**nfluxDB a **G**rafanu.[[8]](#footnote-7)

###### Grafana

Grafana je *open-source* služba pro vizualizaci a monitorování. Podporuje Graphite, Elasticsearch, Prometheus, influxdb a spoustu dalších databází.

Má spoustu distribucí závislých na platformě, která ji provozuje: AWS CloudWatch, kubernetes, Postgre, Splunk atd.

###### InfluxDB

InfluxDB je *open-source* databáze s časovou značkou naprogramovaná v jazyce Go. Je optimalizovana pro rychlost, vysokou dostupnost paměti a používá se k monitorování dat na základě timestamp (časové značky). Je používaná v monitorování DevOps procesů, logování dat, metrik aplikací a real-time analýze.

###### Telegraf

Telegraf je agent pro sbírání, procesování, agregaci a zapisování metrik.

#### 

### Měření

#### Popis měřené infrastruktury

Byl zvolen Elastic Stack, který vizualizuje v Kibaně. Tu máme za povinnost dle zadání využít.

Logovací systém jsme konfigurovali podle dokumentace[[9]](#footnote-8):

* **Beats** - monitorování systémových služeb a zapisování dat do databáze *Elasticsearch,*
* **Elasticsearch** - ukládání dat a indexace dat,
* **Kibana** - vizualizace dat.



### 

#### Výsledný Dashboard

Po zprovoznění infrastruktury byl připraven Dashboard s požadovanými parametry.









## Závěr práce

### Zhodnocení měření

Během konfigurace byly řešeny dílčí problémy.

Prvně se nám nepodařilo připojit do Elasticu. Chybu jsme konzultovali s vyučujícím, který nám ji pomohl rozklíčovat. Jednalo se o chybný stav Elasticu. Služba byla v chybovém stavu, nicméně dle stavu byla stále funkční. Cvičící provedl restart a tím jsme chybu vyřešili.

Druhou chybou bylo to, že se nám nepodařilo připojit z koncentrátoru na sondu. Problém jsme řešili tím, že jsme požádali vyučujícího restart sondy a připojení proběhlo v pořádku.

Během měření jsme si uvědomili chybu, kterou jsme udělali při plánování pořadí práce na úkolech. Pokud bychom prvně realizovali tento projekt, mohli bychom ho využít i v jiných úkolech při měření vytíženosti systémových funkcí sondy.

### Zhodnocení spolupráce

Se spoluprací jsme spokojeni. Rozdělení rolí a zodpovědností se osvědčilo. Práce ve studovně nám vyhovovala více než při online hovoru. Rozhodně tak budeme také pokračovat při dalších projektech.

# Zdroje

## Literatura a reference

Dokumentace k Softwarovému Fraimeworku Metasploit: <https://docs.metasploit.com/>

Navo na praci s Metasploit: <https://nooblinux.com/metasploit-tutorial/>

Instalace Metasploit Framework: <https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/>

Přehlad zabuovaných nástrojů v Kali Linux: <https://www.kali.org/docs/tools/>

3 Penetrační test. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2022-10-28]. Dostupné z: <https://cs.wikipedia.org/wiki/Penetra%C4%8Dn%C3%AD_test>

1. <https://www.elastic.co/guide/en/beats/libbeat/current/beats-reference.html> [↑](#footnote-ref-0)
2. <https://aws.amazon.com/what-is/elk-stack/> [↑](#footnote-ref-1)
3. <https://cs.wikipedia.org/wiki/Elasticsearch> [↑](#footnote-ref-2)
4. <https://www.elastic.co/what-is/elasticsearch> [↑](#footnote-ref-3)
5. <https://www.elastic.co/what-is/kibana> [↑](#footnote-ref-4)
6. <https://powerbi.microsoft.com/cs-cz/> [↑](#footnote-ref-5)
7. <https://learn.microsoft.com/en-us/azure/azure-monitor/overview> [↑](#footnote-ref-6)
8. <https://medium.com/@hoanglc/tig-stack-powerful-monitoring-tool-822521dce102> [↑](#footnote-ref-7)
9. <https://www.elastic.co/guide/en/beats/metricbeat/current/command-line-options.html> [↑](#footnote-ref-8)