

**PROJEKT Č. 5**

**Monitoring a reporting negativních událostí**

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

[Měřené scénáře](#_m8uebdplsq6y) 5

[Nadměrné využití CPU delší dobu](#_wbdclbodvvtw) 5

[Technický popis rutiny](#_xtrhciinlklb) 5

[Plná paměť](#_ag4g1omychuh) 5

[Technický popis rutiny](#_4cz8pdtkh2m0) 5

[Opakující se bezpečnostní hrozby nebo hrozby s vysokým skórem](#_kc777whsqq3z) 5

[Technický popis rutiny](#_x8mtame49tch) 6

[Závěr práce](#_ql38xvv9gut3) 7

[Zhodnocení měření](#_f7nojchrb7e2) 7

[Zhodnocení spolupráce](#_nd9vvo5axb0o) 7

[**Zdroje**](#_yazzxhksboyh) **8**

[Literatura a reference](#_iqwscoldhmy) 8

# Abstrakt

## Cíl projektu

Cílem pátého projektu je nastudovat a realizovat problematiku výstrah a jejich následného zprocesování.

## Závěr projektu

Seznámili jsme se s problematikou notifikací a alertů, které je vhodné použít při sledování dat z IoT sondy.

# Průběh projektu

## Naplánování spolupráce

Na tomto projektu budeme spolupracovat během volného cvičení, případně v úterní 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 kibany, Petr K. - tvorba rešerše a vhodné sledované scénáře, Petr P. - konfigurace sondy a kibany) 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, které nás mohou upozornit na kritické stavy, nutné zásahy administrátora či bezpečnostní ohrožení.

K dané problematice lze využít nástroje, kterým jsme se detailně věnovali v minulé laboratorní úloze (např. Elastic Stack, TIG Stack, Azure Monitor, …).

#### Měřené scénáře

Než se pustím do konkrétního nastavení Kibany, je nutné si specifikovat pro jaké parametry a při jakých scénářích chceme definovat alerty. Zvolili jsme tyto scénáře:

##### Nadměrné využití CPU delší dobu

Pokud na sondě poběží proces, který po delší dobu bude vytěžovat CPU sondy, chceme upozornit administrátora. Může se jednat o systémovou nebo bezpečnostní chybu, nebo může daný stav indikovat nutnost horizontálně nebo vertikálně škálovat.

###### Technický popis rutiny

Pokud na sondě bude CPU na sondě vytíženo po dobu 30svytíženost CPU rovna nebo vyšší 98% upozorní administrátora emailovou notifikací.

##### Plná paměť

V případě zaplněnosti paměti mohou na sondě selhávat nejen kritické obslužné rutiny. Proto je nutné uvolnit paměť o nepodstatná nebo redundantní data či vertikálně škálovat paměť sondy. V tomto případě je opět nutné uvědomit administrátora nebo pomocí hooku spustit rutinní skript, který paměť vyčistí.

###### Technický popis rutiny

Pokud bude paměť sondy zaplněná více než 95%, upozorní administrátora emailovou notifikací.

##### Opakující se bezpečnostní hrozby nebo hrozby s vysokým skórem

V případě opakujících se bezpečnostních hrozeb je třeba situaci okamžitě řešit. Může se jednat např. o DDoS útok, který se v podstatě nedá moc efektivně řešit jinak, než že se zvětší propustnost nebo se provoz přesměruje jinam. Nebo se také může jednat o typ útoků, které jsou vyhodnoceny jako obzvlášť kritické či často opakované. V takovém případě je nutné situaci řešit. I v takovém případě je vhodné informovat administrátora.

###### Technický popis rutiny

Pokud sonda zpozoruje útok s vysokým bezpečnostním skórem, zaznamená útok, který se často opakuje nebo zaznamená změnu trendu bude informovat administrátora emailovou notifikací.

## Závěr práce

### Zhodnocení měření

Během konfigurace byly řešeny dílčí problémy. Příkladem může být např. to, že se při spuštění Elasticsearch sonda přestala odpovídat. Kontaktovali jsme cvičícího a prosili o reset sondy. Nakonec jsme chybu opravili tak, že jsme na sondě odstranili přebytečná data a sondu se nám povedlo spustit v pořádku.

### 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

<https://www.elastic.co/guide/en/observability/current/metrics-threshold-alert.html>