Projekt č. 4

SBĚR, UKLÁDÁNÍ A VIZUALIZACE LOGŮ, HROZEB a HW STATISTIK

B0B32KTI- Komunikační technologie pro IoT

Ing. Bc. Marek Neruda, Ph.D., Ing. Tomáš Straka

Datum: 9 / 2022

1. Zadání projektu

Studenti si vytvoří řešerši na téma “sběr, ukládání a vizualizace dat v open-source prostředí”, např. článek[1] nebo článek[2]. Dále si nastudují, jak je řešen centrální sběr logů na sondě (lokální řešení), ukládání do DB a následné zobrazení nasbíraných dat za účelem jejich reprezentace v human readable podobě. Následně návrhnou, vytvoří a otestují řešení, které bude do Elasticsearch DB umístěné na sondě sbírat metriky z HW a to především tyto:

- cpu # CPU usage
- load # CPU load averages
- memory # Memory usage
- network # Network IO
- process # Per process metrics
- process_summary # Process summary
- uptime # System Uptime
- socket_summary # Socket summary
- core # Per CPU core usage
- diskio # Disk IO

Studenti si zvolí na základě rešerše a znalosti o aktuálním SW na sondě nejvhodnější řešení tak, aby byla zajištěna minimální HW zátěž (load) navíc (tj. např. nástroj, který již na sondě existuje, nebo je ze stejné série nástrojů, které na sondě existují). Studenti tak mohou nainstalovat v rámci tohoto projektu potřebný SW na jejich sondu. Zároveň je požadovaná jednoduchá implementace nástroje s minimem programování, nejlépe žádným programováním. Zároveň studenti volí četnost odečítání dat dle svých nejlepších úsudků, které ve výstupním protokolu vysvětlí (např. vzorek využití CPU 1/hodina nedává smysl a 1/vteřina vykazuje zbytečnou zátěž navíc).

Dále je požadována vizualizace těchto sbíraných metrik v prostředí Kibana, které je součástí sondy SonIoT. Vizualizace bude v podobě jednoho dashboardu, který bude centrálně zobrazovat tyto metriky, aby jejich grafická reprezentace dávala smysl. Tento projekt lze aplikovat pouze na jeden režim sondy, tzn. studenti si zvolí IDS nebo IPS režim.

Studenti do protokolu zanesou veškeré poznatky, implementace a výsledky, které je vedly k úspěšné realizaci projektu v jasné a přehledné formě s patřičnými náležitostmi (za využití standardního formátování dokumentu včetně číslování) a to především:

- 1. strana: logo, název protokolu, jména osob, datum, místo, stručný závěr protokolu
- 2. a další strany: cíl projektu, měřené parametry, tabulkové stavy jednotlivých komponent, případně grafy se správně označenými osami
- přesný postup realizace (dle postupu zvládne realizaci i jiná osoba)
- literární zdroje a SW nástroje, které byly využity pro realizaci
- pokud byla provedena vlastní invence, tak zadokumentovat postup

[1] https://medium.com/@hoanglc/tig-stack-powerful-monitoring-tool-822521dce102
[2] https://logz.io/learn/complete-guide-elk-stack/#intro

- práce v týmu: rozdělení rolí, rozdělení zodpovědností, návrh časového plánu projektu, vybrané způsoby komunikace
- zhodnocení: dosaženého plánu včetně časové alokace, plnění zodpovědností, plnění rolí, způsoby komunikace
- závěrečné zhodnocení výsledků testu obsahující dosažené hodnoty a statistické zhodnocení měřených hodnot, zhodnocení práce v týmu

Studenti zároveň navrhnou v závěru protokolu možné způsoby optimalizace na základě zjištěných poznatků, tj. např. odstranění nepotřebného SW a jiné.

2. Doporučení k projektu

Projekt je navržen tak, aby se studenti seznámili s open-source nástroji pro sběr, uchovávání a vizualizaci dat pro krátkodobé a dlouhodobé účely. Vyzkouší si nejen práci v operačním systému Ubuntu, ale také s grafickým prostředím pro analýzu a vizualizaci dat. Studenti na projektu pracují v laboratoři, nebo v domácím prostředí, ale vždy dbají na pravidla bezpečnosti a bezpečného užití HW a nevyužijí sondu k nekalé či trestné činnosti. Projekt je vypracováván s vědomím, že výsledky budou krom výstupního protokolu prezentovány na konci semestru před cvičícími.

Doporučené otázky, které by si studenti měli klást jsou především tyto:

- Jaké nástroje či příkazy, které jsou standardní součástí distribuce Ubuntu Server 20.04 LTS můžu využít k získání odpovědí?
- Potřebuji na sondu instalovat další SW? Pokud ano, nevyužívá příliš HW zdrojů?
- Pokud vyžaduji pro testování více koncových stanic, nestačila by virtualizace, např. s využitím open-source nástroje VirtualBox[3]?
- Je námi vytvořený protokol reprodukovatelný jiným týmem?

[3] https://www.virtualbox.org/