

Distribuovaný repositář digitálních forenzních dat

Bc. Martin Josefík

Vysoké učení technické v Brně, Fakulta informačních technologií
Božetěchova 1/2. 602 00 Brno - Královo Pole
xjosef00@fit.vutbr.cz



19. ledna 2018

Teoretická část - Seznámení se s

- Formáty digitálních forenzních dat
- Existujícími systémy pro jejich uložení
- Distribuovanými databázemi

Praktická část

- Navržení distribuovaného úložiště
- Zvolení vhodných technologií
- Implementace
- Testy použití a výkonu
- Vyhodnocení

Forenzní analýza digitálních dat

- Cíl, průběh, vlastnosti
- Formáty digitálních forenzních dat
- Existující systémy (AFF4)

Úložiště pro strukturovaná a nestrukturovaná data

- Big data
- Distribuované databáze
- Strukturovaná a nestrukturovaná data

Požadavky

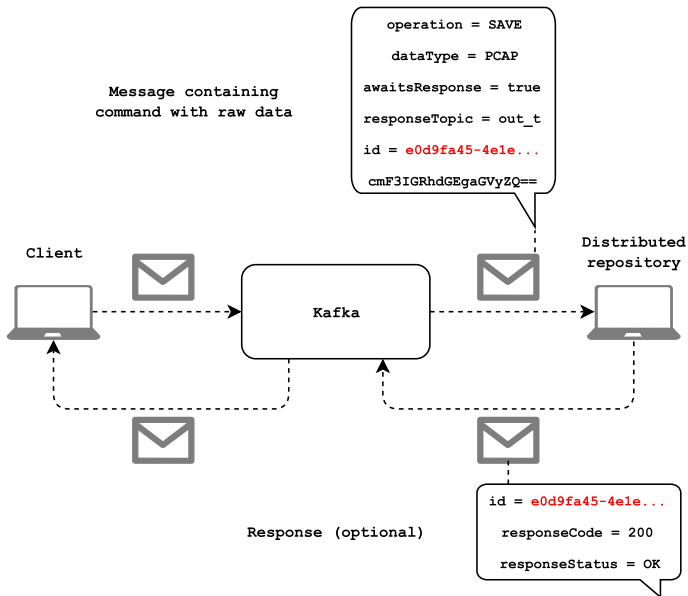
- Distribuované úložiště
- Rozsáhlá digitální forenzní data
- Optimální přístup k datům
- Rozšiřitelnost pro nové druhy dat

Technologie

- Kafka
- NoSQL databáze - Cassandra, MongoDB
- HDFS

Ovládání systému

- Zasílání zpráv - příkazů



Zpracování zpráv

- Přiřazení akce k příkazu
- Akce zapouzdřuje všechny potřebné operace
- Obsluha úložišť

Metadata

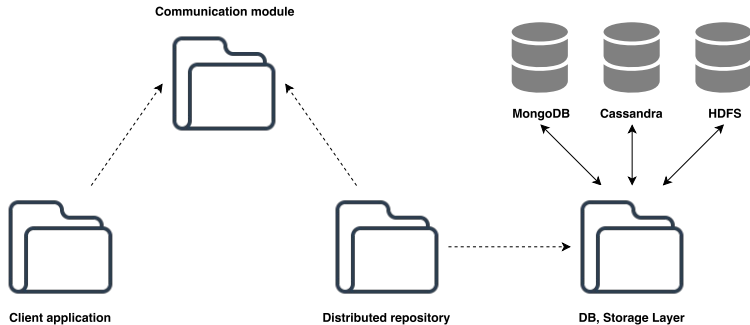
- Registr dat
- Předzpracování dat
- Optimální přístup k datům
- Dynamičnost metadat

Strukturovaná data

- Lze rozdělit na části, segmenty, bloky
- Před uložením serializována
- NoSQL databáze

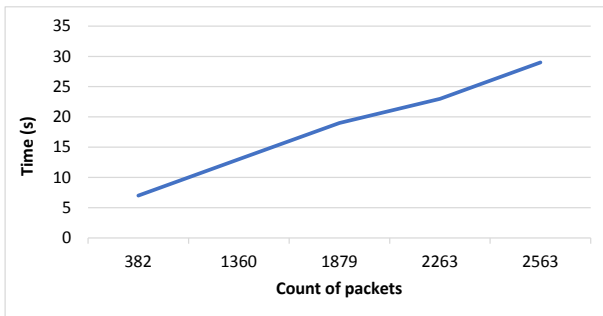
Nestrukturovaná data

- Logy, multimédia, ...
- Rozdělení a serializace dat brzdí výkon
- Distribuovaný souborový systém (HDFS)



Implementace ověřující

- Základní aspekty návrhu
- Konfiguraci technologií
- Komunikaci s klientem
- Výkon



Implementace a vyhodnocení

- Rozšíření prototypu
- Podsystem metadat
- Optimální přístup k datům
- Vyhodnocení z hlediska výkonu

Děkuji za pozornost.