Ingestor metadat z network flow do Apache Kafka

Adam Masaryk (xmasar15)
Lukáš Šišmiš (xsismi01)
Matúš Švancár (xsvanc06) • 10.12.2020

Architektúra

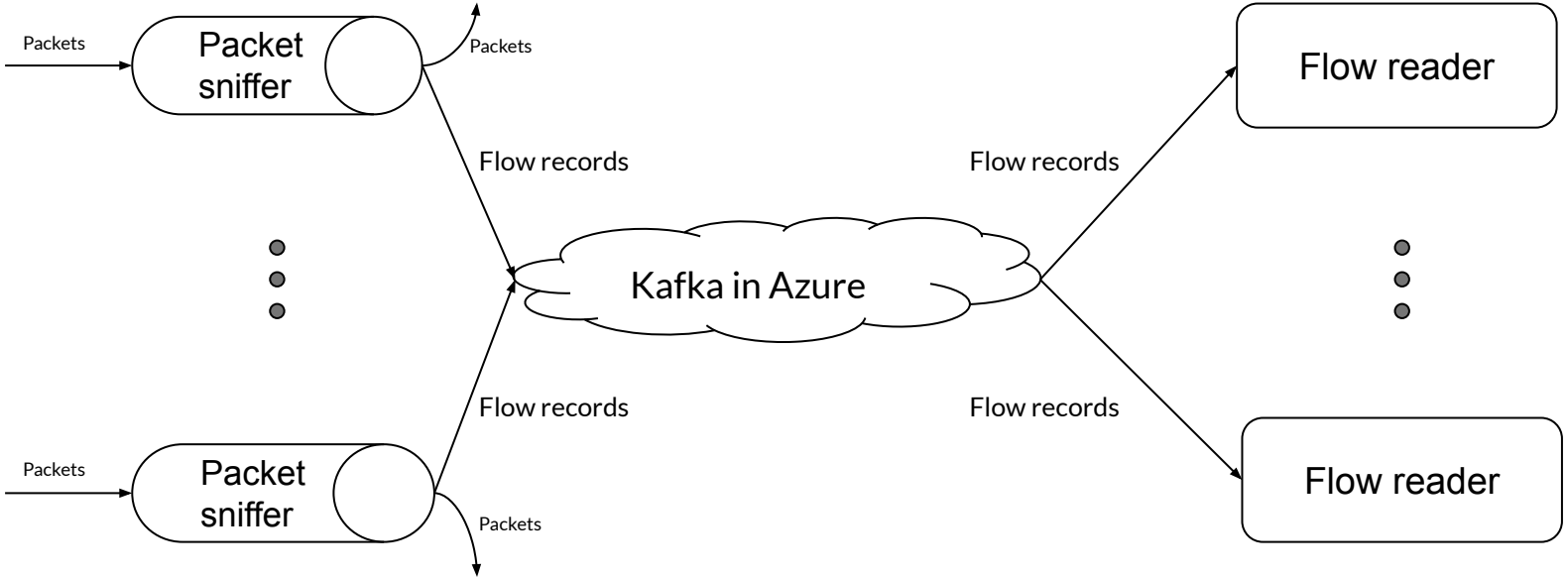
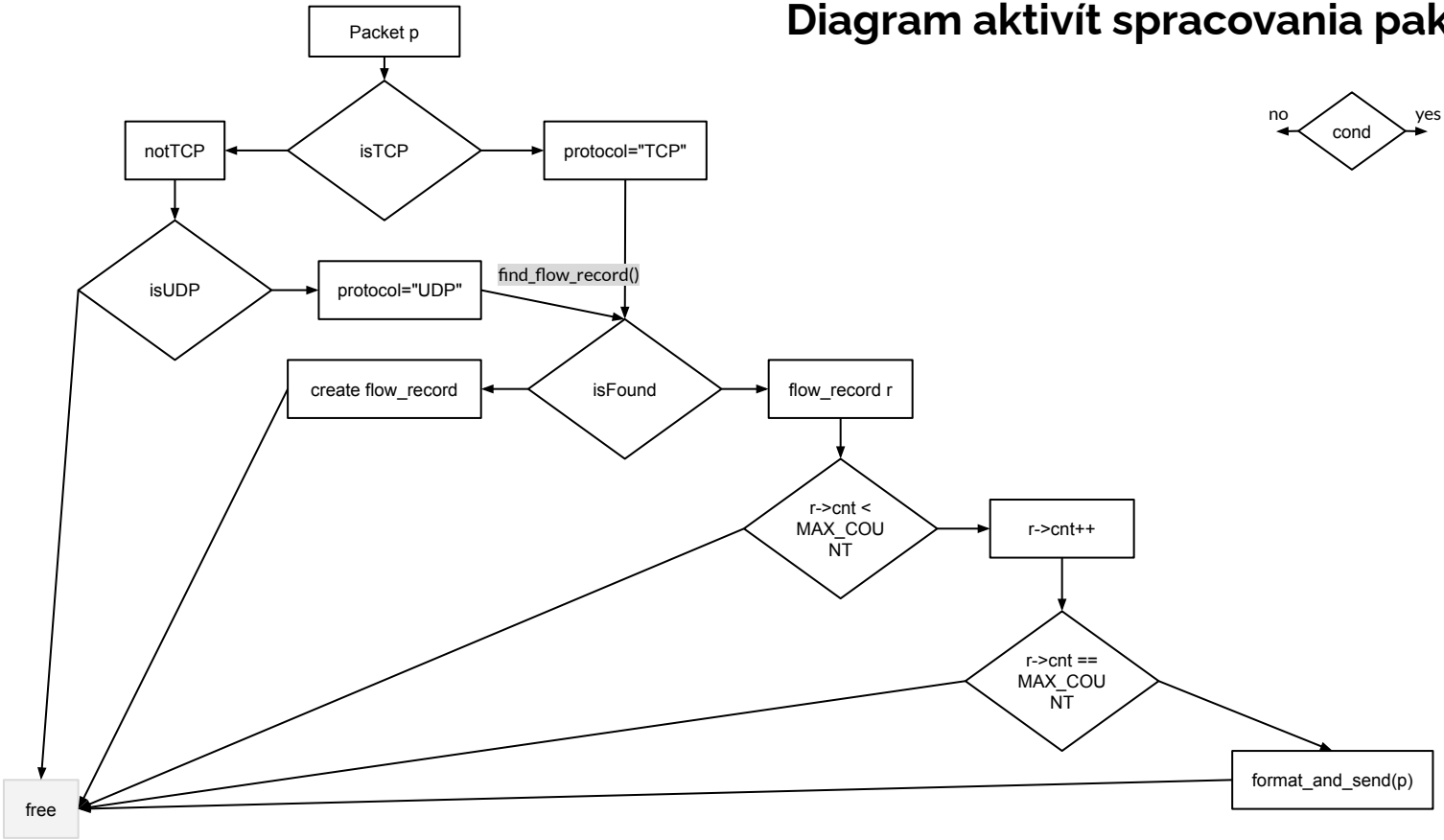


Diagram aktivít spracovania paketu



flow_record linked list

```
typedef struct packet {
    uint32_t src_addr;
    uint32_t dst_addr;
    uint16_t src_port;
    uint16_t dst_port;
    char protocol[4];
} packet_t;
```

```
typedef struct flow_record_entry {
    time_t time;
    ssize_t payload_size;
    struct flow_record_entry *next;
} flow_record_entry_t;
```

```
typedef struct flow_record {
    packet_t packet;
    flow_record_entry_t *record;
    unsigned int record_count;
    struct flow_record *next;
} flow_record_t;
```

```
typedef struct flow_record {
    packet_t packet;
    flow_record_entry_t *record;
    unsigned int record_count;
    struct flow_record *next;
} flow_record_t;
```

```
flow_record_t *list
```

Rozdelenie práce

Adam

- Príjem paketov, kontrola ich správnosti a ich nahrávanie do štruktúr
- flow_record table

Lukáš

- Nastavenie cloudového prístupu
- Nastavenie a sprevádzkovanie Kafky
- run-script.sh

Matúš

- flow_record kolektor a odosielanie na Kafku