UNIVERSITÀ DI PISA

Dipartimento di Informatica

Gestione di Rete

sFlow to Influx

Luca Pippi

Corso A

Matricola 533706

Introduzione

Il progetto ha lo scopo di realizzare un tool per la raccolta dei dati statistici dei counter samples di sFlow e memorizzarli direttamente su di un database per serie temporali, nel caso specifico in Influx.

Gli agent sFlow inviano i counter samples divisi per interfaccia e contengono i seguenti contatori:

- Indice di interfaccia (`ifIndex`)
- Tipo di interfaccia (`ifType`)
- Velocità dell'interfaccia (`ifSpeed`)
- Direzione di comunicazione (`ifDirection`)
- Stato operativo interfaccia (`ifStatus`)
- Bytes in ingresso (`ifInOctects`)
- Pacchetti unicast, multicast e broadcast in ingresso (`ifInUcastPkts,ifInMulticastcastPkts,ifInBroadcastPkts`)
- Errori e pacchetti scartati in ingresso (`ifInDiscards,ifInErrors`)
- Protocolli sconosciuti in ingresso (`ifInUnknownProtos`)
- Bytes in uscita (`ifOutOctects`)
- Pacchetti unicast, multicast e broadcast in uscita (`ifOutUcastPkts,ifOutMulticastcastPkts,ifOutBroadcastPkts`)
- Errori e pacchetti scartati in uscita (`ifOutDiscards,ifOutErrors`)
- Stato "promiscuous mode" (`ifPromiscuousMode`)

Il tool ignorerà i packet samples inviati dagli agent e prenderà in considerazione i soli contatori utili per le statistiche.

Prerequisiti

Per l'utilizzo del tool è necessario aver installato:

- InfluxDB (`https://www.influxdata.com/`)
- sflowtool (`https://github.com/sflow/sflowtool`)

È necessario inoltre un agent sFlow (`https://sflow.org/developers/tools.php`), che ho allegato al tool e verrà compilato assieme al tool per i test.

Implementazione

Il tool `sflowtoinflux` sfrutta `sflowtool` per raccogliere i dati dagli agent e poi li elabora per creare delle query corrette da inviare al database InfluxDB.

Per il corretto funzionamento di `sflowtoinflux` è necessario modificare il file di configurazione `conf.ini` con il percorso di installazione di `sflowtool` sulla propria macchina, l'indirizzo del database che si vuole utilizzare e la porta sul quale gli agent stanno comunicando.
`sflowtool` viene utilizzato in modo da raccogliere solamente i dati dei counter samples e non tutto il contenuto dei pacchetti sFlow dopodiché il tool identifica dall'ouput di `sflowtool` quali sono l'agent, l'interfaccia ed il timestamp del counter sample ricevuto e crea una query di inserimento per ogni contatore.

Formato file configurazione

Il file di configurazione conf.ini deve avere il seguente formato:

```
DATABASE=http://<indirizzo_database>:<porta_database>/
ORG=<nome_organizzazione_influx>
BUCKET=<bucket_influx>
TOKEN=<token_autorizazzione_influx>
PATH=<posizione_sflowtool>
PORT=<porta_di_ascolto>
```

È necessario mantenere questo ordine preciso dei tag per la corretta lettura del file.

Compilazione e test

Per la compilazione di `sflowtoinflux` sarà sufficiente utilizzare il comando `make`.
Per eseguire dei test si può utilizzare il comando `sudo make test`, che decomprimerà, compilerà il programma agent e ne lancerà in esecuzione un'istanza sull'interfaccia attualmente attiva della propria macchina, che avrà anche la funzione di collector in quanto infine verrà eseguito sflowtoinflux.

Per eseguire individualmente un agent è sufficiente utilizzare il comando:

```
sudo sflsp -d <interfaccia> -P -s <sampling_rate>
                                    -A <indirizzo_agent>
                                        -C <indirizzo_collector>
                                            -c <porta_collector>
```

Per arrestare tutti gli agent a fine test ho incluso uno script `killall.sh`.

Analisi con Influx Dashboards

Il tool serve solamente a memorizzare i dati su un database a serie temporale, ma non crea nessun report statistico della rete né ne valuta le prestazioni.
Per utilizzare i dati memorizzati a fini statistici è necessario il supporto di InfluxDB che permette di manipolare i dati delle timeseries al suo interno e creare grafici prestazionali quasi in tempo reale e raccoglierli in delle tabelle grafiche, chiamate Dashboards.

Per dare un esempio ho creato una semplice dashboard per visualizzare alcuni dati memorizzati tramite `sflowtoinflux`; la dashboard ha 5 panel che mostrano l'andamento nel tempo di:

- Utilizzo banda totale: percentuale di occupazione della banda totale per ogni interfaccia di un agent.
- Utilizzo banda input: percentuale di banda utilizzata per traffico in ingresso per ogni interfaccia.
- Utilizzo banda output: percentuale di banda utilizzata per traffico in uscita per ogni interfaccia.
- Numero di pacchetti input: numero di pacchetti in ingresso su ogni interfaccia in un dato istante.
- Numero di pacchetti output: numero di pacchetti in uscita su ogni interfaccia in un dato istante.
- Volume traffico input: volume di traffico in ingresso espresso in bytes.
- Volume traffico output: volume di traffico in uscita espresso in bytes.
- Velocità media di trasferimento: velocità media di trasferimento in un intervallo di 10 secondi, espressa in bits al secondo.

La visualizzazione è divisa per Agent ed è possibile cambiare Agent visualizzato semplicemente selezionandolo da una variabile della dashboard.

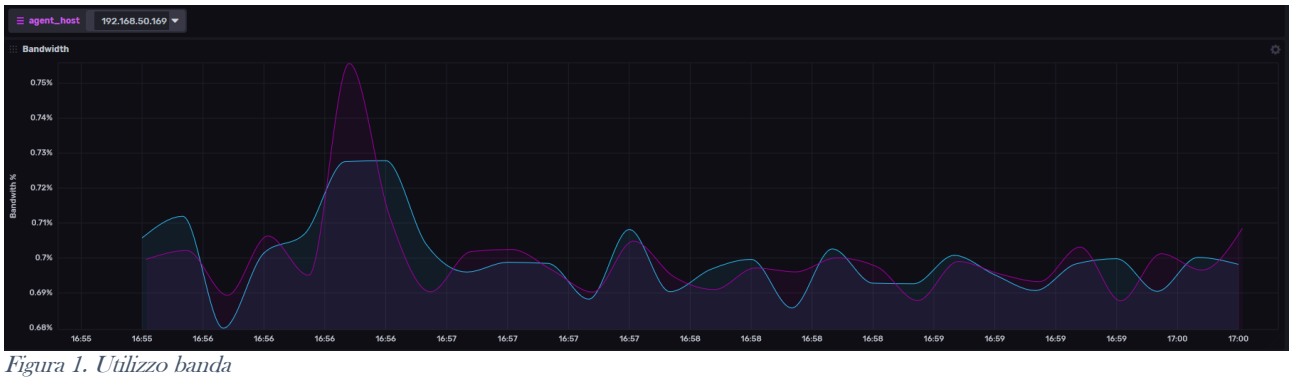

Figura 1. Utilizzo banda

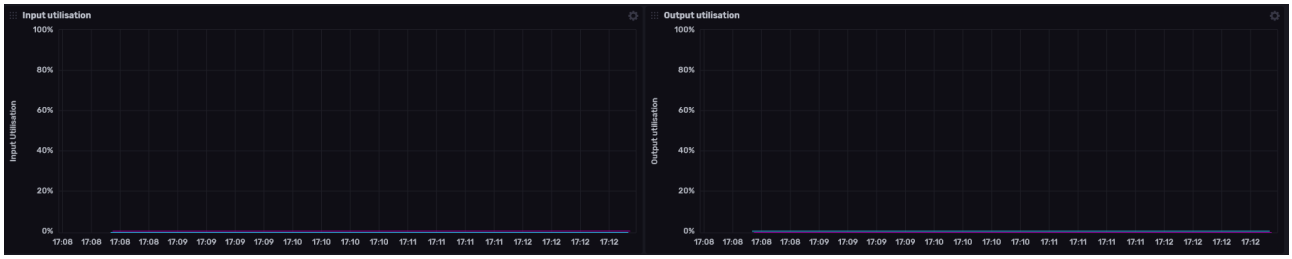

Figura 2. Utilizzo banda input (sinistra) ed output (destra)

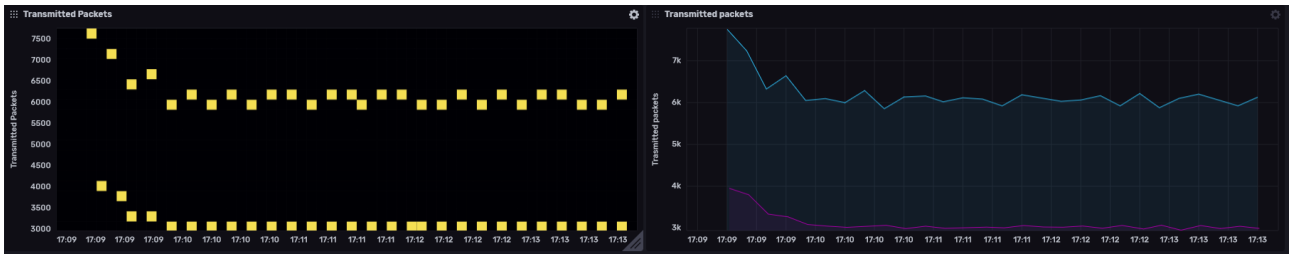

Figura 3. Pacchetti in output

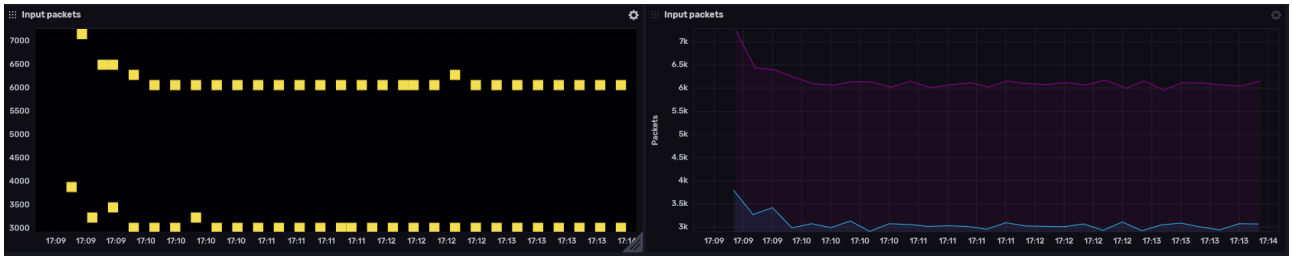

Figura 4. Pacchetti in input

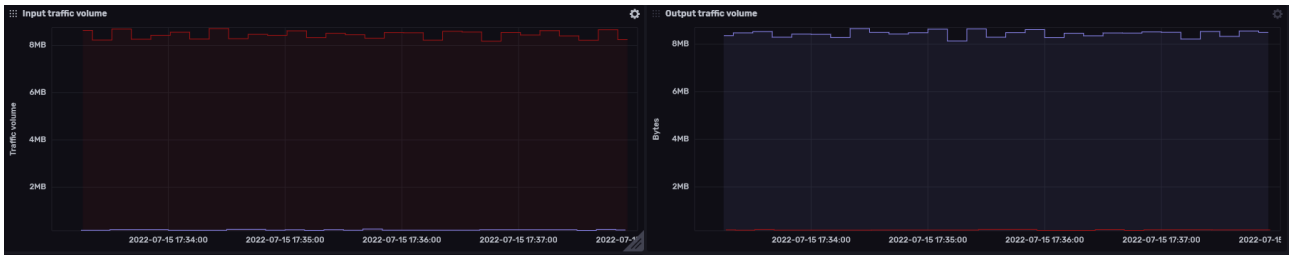

Figura 5. Volumi di traffico in ingresso (sinistra) ed in uscita (destra)

Figura 6. Velocità media