Università degli Studi di Pisa

FACOLTÀ DI INFORMATICA
Corso di Laurea in Informatica Triennale

Progetto di Gestione di Reti

Dashboard di aiuto per l'esposizione di un servizio

Candidati:
Angelo Gorini
Matricola 481404

Marco Ceragioli
Matricola 277008

Anno Accademico 2015-2016

Indice

1 Introduzione

Il progetto consiste nella implentazione di una dashboard di supporto per un server che vuole esporre un nuovo servizio. Per quanto riguarda la parte hardware della macchina il compito di collezionare le metriche è affidato a Collectd, le metriche vengono poi raccolta da Logstash, il quale permette di centralizzare metriche da più macchine direttamente su Elasticsearch. Per quanto riguarda la parte delle metriche di rete il compito di collezionare è affidato a Ntopng, il quale permette di inoltrare direttamente le misurazioni a Elasticsearch. La rappresentazione grafica è affidara a Kibana che è connessa direttamente ad Elasticsearch. I tool utilizzati nel progetto sono quindi:

1. Collectd
2. Logstash
3. Elasticsearch
4. Ntopng
5. Kibana

2 Misurazione delle metriche hardware

La misurazione delle metriche hardware avviene attraverso Collectd, il quale invia tramite UDP le misurazioni a Logstash (nel nostro caso per comodità i due programmi sono in esecuzione sullo stessa macchina), i file di log, immagazzinati in Logstash, vengono poi inviati a Kibana tramite Elastichsearch da cui Kibana preleva i dati che verrano mostrati nella dashboard.

Figura 1: Architettura complessiva dei tool per la misurazione delle metriche hardware.

2.1 Collectd

Collectd è un software che raccoglie periodicamente statistiche sulle performance del sistema e le salva in speciali file RRD. Le statistiche sono quindi consultabili attraverso un'interfaccia web fornita da Kibana come illustrato nella Figura 1. Attraverso questo tool abbiamo scelto di misurare le seguenti metriche:

1. CPU
2. RAM
3. Hard-Disk
4. Processi e Thread

2.1.1 Installazione

Per installare Collectd su Debian/Ubuntu è sufficiente digitare il seguente comando da bash:

```
sudo apt-get install collectd collectd-utils
```

2.1.2 Configurazione

Per configurare Collectd al fine di collezionare le metriche hardware da noi scelte è necessario modificare il file `/etc/collectd/collectd.conf` includendo i plugin corrispondenti come segue:

```
Hostname "Gateway"
FQDNLookup false
LoadPlugin cpu
LoadPlugin df
LoadPlugin disk
LoadPlugin irq
LoadPlugin load
LoadPlugin users
LoadPlugin swap
LoadPlugin memory
LoadPlugin uptime
LoadPlugin processes
LoadPlugin ethstat
LoadPlugin syslog

<Plugin syslog>
  LogLevel info
</Plugin>
```

```
19
20 LoadPlugin network
21
22 <Plugin network>
23   Server "127.0.0.1" "25826"
24 </Plugin>
25
26 LoadPlugin ping
27 <Plugin "ping">
28   Host "8.8.4.4"
29 </Plugin>
30
31 <Include "/etc/collectd/collectd.conf.d">
32         Filter ".conf"
33 </Include>
```

2.2 Logstash

Logstash è un collezionatore open source di dati real-time la cui peculiarità è quella di unire misurazioni ricevute da più fonti e di aggregarle in modo tale che possano essere mandate ad una destinazione a nostra scelta (nel nostro caso Elasticsearch).

2.2.1 Installazione

Per installare Logstash è sufficiente scaricare dal sito https://elastic.co/downloads/logstash l'ultima versione stabile.

2.2.2 Configurazione

Per la configurazione di Logstash è necessario modificare il file `etc/logstash/conf.d/logstash.conf`, in modo da settare come input Logstash e come output Elasticsearch, come segue:

```
1 input{
2   udp{
3     port => 25826
4     buffer_size => 1452
5     codec => collectd()
6     }
7   }
8 output{
9   elasticsearch{
10    template_overwrite => true
11    }
12  }
```

2.3 Elasticsearch

Elasticsearch è un motore di ricerca open source le cui informazioni sono gestite come documenti JSON, il suo ruolo nel nostro progetto è quello di ponte tra Logstash e Kibana dove i dat vengono poi reppresentati graficamente.

2.3.1 Installazione

Per installare Elasticsearch è sufficiente scaricare dal sito https://elastic.co/downloads/elasticsearch l'ultima versione stabile.

2.3.2 Configurazione

Elasticsearch non necessita di configurazione in quanto si interfaccia direttamente con Kibana.

2.4 Kibana

Kibana è una piattaforma di visualizzazione dei dati open source che permette di interagire con i dati stessi attraverso grafici che possono essere combinati per creare delle dashboard, come quella in figura 2, che aiutano il gestore della rete a comprendere comportamenti e prestazioni delle macchine che compongono la suddetta rete.

2.4.1 Installazione

Per installare Kibana è sufficiente scaricare dal sito https://elastic.co/downloads/kibana l'ultima versione stabile.

2.4.2 Configurazione

Per configurare Kibana al fine di ricevere le misurazione da Collectd è sufficiente accedere a Kibana all'indirizzo http://localhost:5601, andare su Setting > Indices > Configure an index pattern e aggiungere la stringa `logstash-*`.

2.4.3 Dashboard

3 Misurazione delle metriche di rete

La misurazione delle metriche di rete avviene attraverso Ntopng, il quale invia tramite UDP le misurazioni a Elasticsearch (nel nostro caso per comodità i due programmi sono in esecuzione sullo stessa macchina), le misurazione

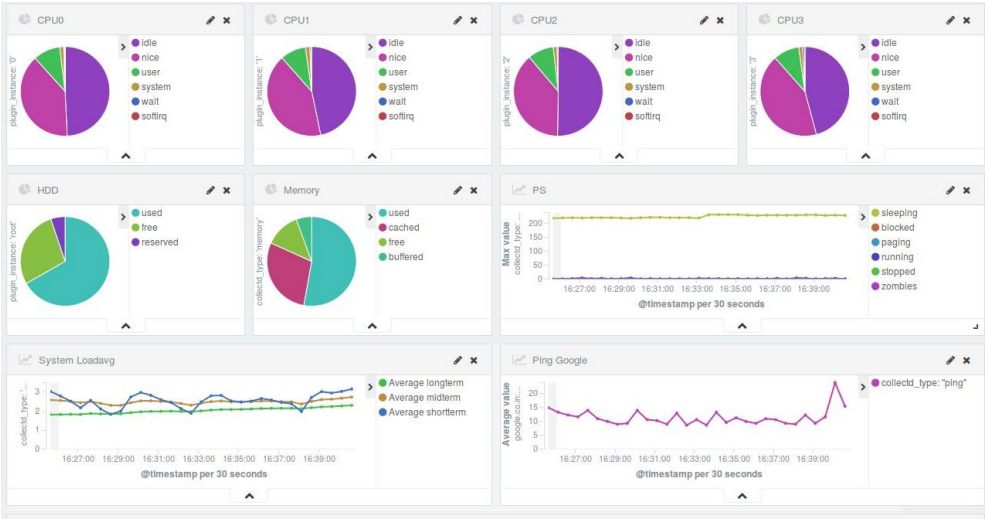

Figura 2: Dashboard misurazioni metriche hardware.

vengono poi rappresentate su Kibana tramite Elastichsearch da cui Kibana preleva i dati che verrano mostrati nella dashboard.

3.1 Ntopng

Ntopng è una sonda per il traffico di una rete che mostra l'utilizzo che si fa della rete stessa. Per accedere all'interfaccia di ntopng è sufficiente accedere alla pagina all'indirizzo http://localhost:3000 dopo averlo avviato da riga di comando. Attraverso questo tool abbiamo scelto di misurare le seguenti metriche:

1. Servizi più usati sulla macchina
2. Media dei pacchetti al secondo
3. Bytes in/out al secondo

3.1.1 Installazione

Per installare Ntopng su Debian/Ubuntu è sufficiente digitare il seguente comando da bash:

```
git clone https://github.com/ntop/ntopng.git
cd ntopng
./autogen.sh
./configure
make
make install
```

3.1.2 Configurazione

Per configurare Ntopng al fine di inviare le metriche di rete a Elasticsearch è sufficiente digitare da bash il comando:

```
sudo ntopng -F 'es;ntopng;ntopng-%Y.%m.%d;http://localhost:9200/_bulk;'
```

3.2 Kibana

3.2.1 Configurazione

Per configurare Kibana al fine di ricevere le misurazione da Collectd è sufficiente accedere a Kibana all'indirizzo http://localhost:5601, andare su Setting > Indices > Configure an index pattern e aggiungere la stringa `ntopng-*`.

3.2.2 Dashboard

Figura 3: Grafici misurazioni delle metriche di rete. Rispettivamente il primo misura in/out bytes al minuto e media pacchetti in/out al minuto.

4 Esempio di utilizzo della Dashboard

È stata utilizzata questa Dashboard per misurare l'impatto di un piccolo social network (implementato per il progetto di Laboratorio di Reti), volevamo

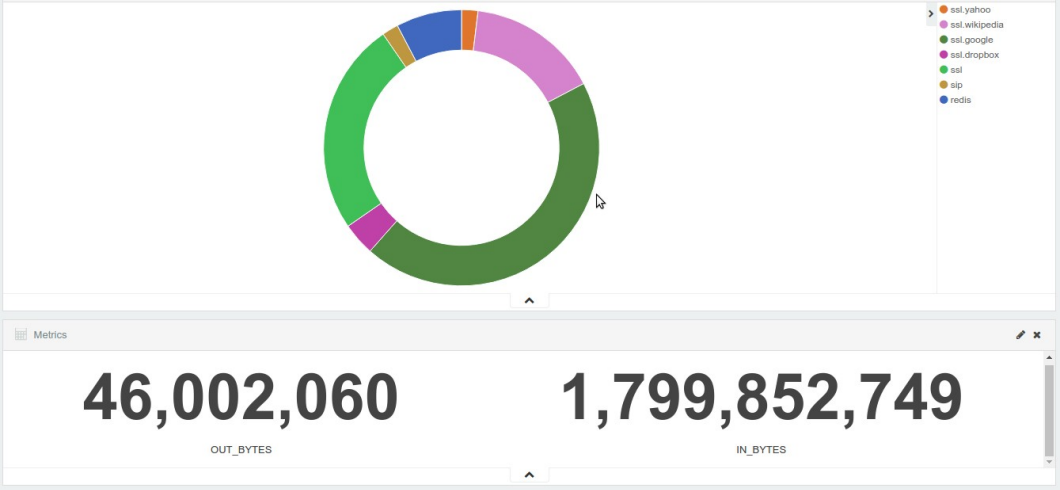

Figura 4: Grafici misurazioni delle metriche di rete. Rispettivamente il primo misura attraverso una pie chart i servizi più utilizzati sulla macchina e il secondo i bytes totali in input e output.

sapere la mole di dati scambiati sulla rete oltre all'incidenza sulle prestazioni della macchina. Abbiamo misurato il numero di tentativi di accesso al servizio di login, utile per riconoscere un tentivo di accedere al servizio da un utente con credenziali fasulle in caso di attacco brute force. Abbiamo misurato inoltre l'impatto del servizio sulla macchina, in particolare: l'utilizzo di CPU e RAM e Hard Disk sia per controllare possibili malfunzionamenti per testare sia l'efficienza, sia possibili attacchi, sia se le risorse assegnate al servizio sono sufficienti, per lo stesso motivo abbiamo misurato anche lo stato dei processi e la media del tempo di attesa per la schedulazione, importanti per controllare il grado di occupazione della CPU. Inoltre mostriamo il grafico che rappresenta il RTT del ping al server DNS di Google per testare la connesione internet della macchina su cui è in esecuzione del servizio.

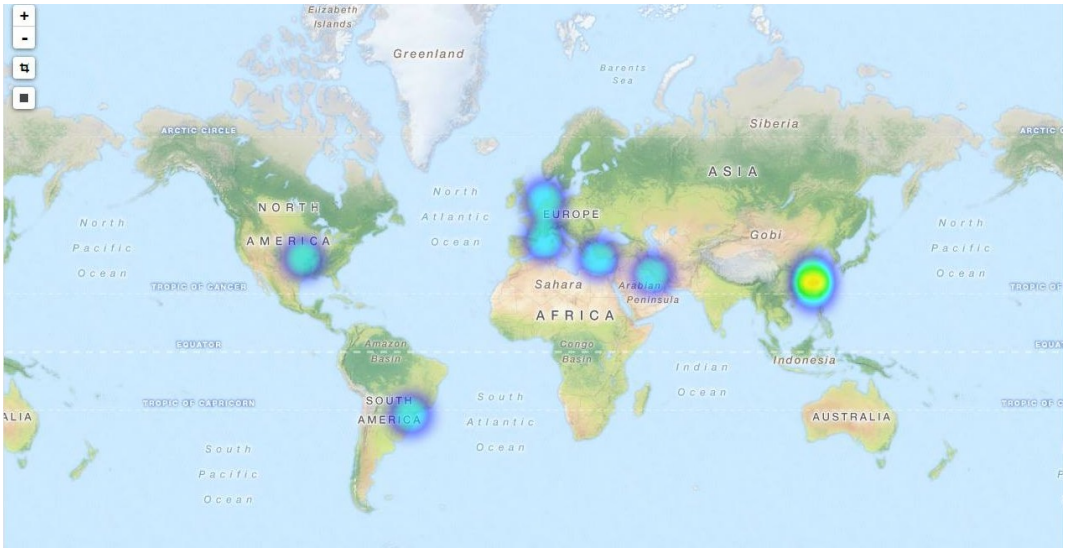

Figura 5: Heatmap di utilizzo del servizio.

Figura 6: Grafico del numero di accessi al login del servizio.