Monitoring with Elasticsearch, Kibana and Logstash

Teamleden:
- Tibo De Clercq
- Bjorn Vandebergen

Gebruikt materiaal:

AWS EC2 instantie 2t.xl (16GB ram) met ubuntu 20.0

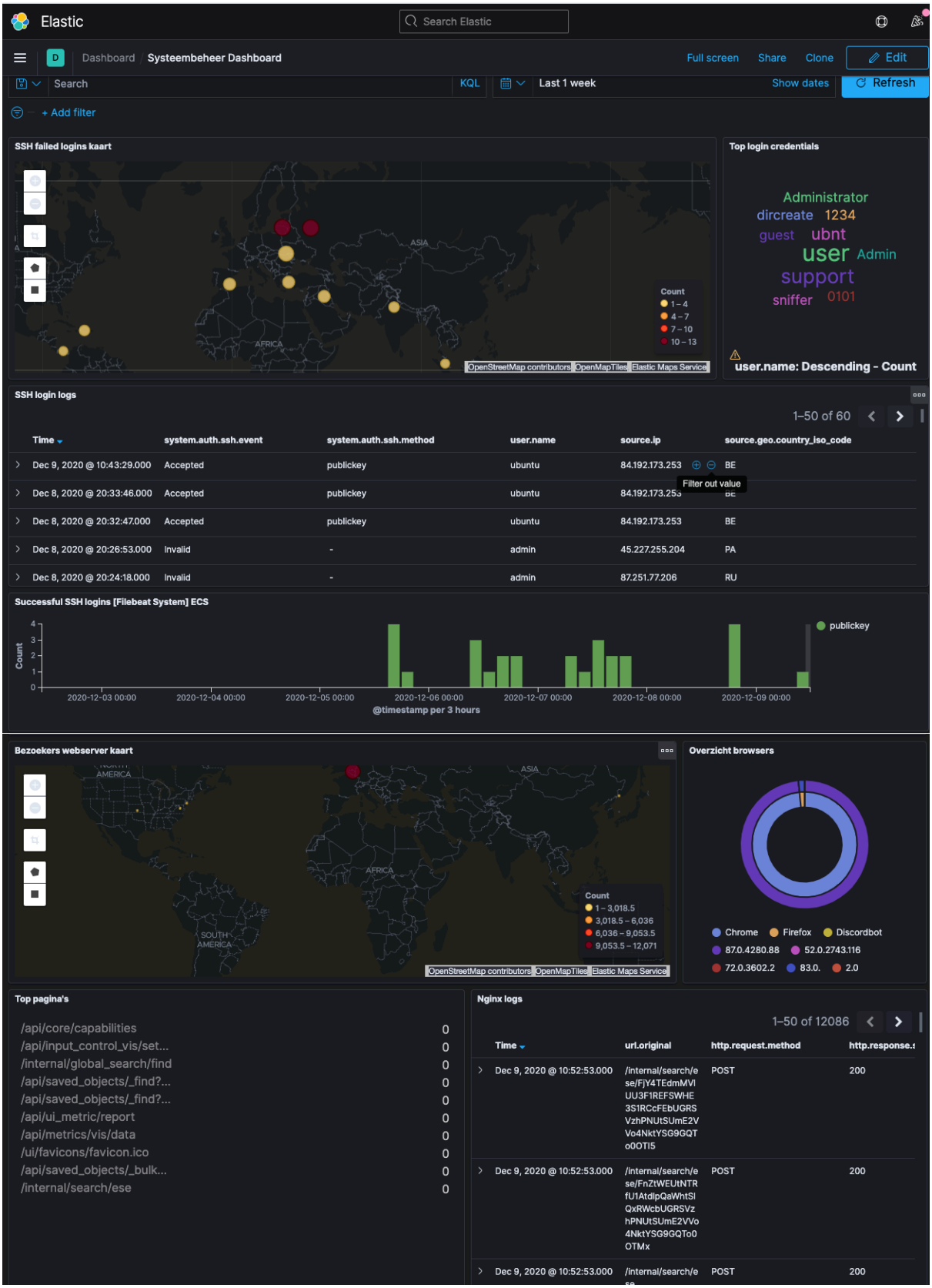
Visualiseren van SSH en Nginx logs

We hebben de volgende tutorial gevolgd voor het opzetten van onze ELK stack: https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-20-04

Deze handleiding zet de volledige omgeving op: Elasticsearch, Kibana dashboard, Logstash en Filebeat. Naast deze tutorial hebben we de filebeat module System en Nginx aangezet. We hebben gekozen om een Nginx webserver te draaien i.p.v. een Apache2 webserver.

Vervolgens hebben we met deze data in Kibana een dashboard gemaakt van de SSH en Nginx logs.

Dashboard: Systeembeheer SSH en Nginx



Visualiseren van Netflow data

Voor het 2de deel van de opdracht hebben we geprobeerd om netflow data door te sturen naar het dashboard. Het is ons niet gelukt om de data te visualiseren in het kibana dashboard. Maar we hebben het volgende geprobeerd:

We hebben gebruik gemaakt van Nprobe:

```
apt-get install software-properties-common wgetadd-apt-repository
universewget https://packages.ntop.org/apt-stable/20.04/all/apt-
ntop-stable.debapt install ./apt-ntop-stable.deb
```

Vervolgens hebben we gebruikt van Elastiflow v4.0.1
https://github.com/robcowart/elastiflow/releases/tag/v4.0.1
We hebben gekozen voor Elastiflow omdat deze verschillende network flow data ondersteund (Netflow v5/v9, sFlow en IPFIX flow types). Daarnaast komt Elastiflow met een aantal verschillende Logstash filters en Kibana dashboards.
Het enige nadeel aan dit Elasitflow is dat Elastiflow een hoge systeemvereiste heeft (CPU en werkgeheugen).

We hebben de installatie instructies gevolgd zoals beschreven staat in de installatiehandleiding van de release (versie 4.0.1). We hebben bewust niet gekozen om de master branch gebruikt. Omdat er misschien kleine verschillen kunnen zijn tussen een release en de master branch.
https://github.com/robcowart/elastiflow/blob/master/INSTALL.md
Vervolgens hebben we geprobeerd om met nprobe data te sturen:

```
nprobe -T %SAMPLING_INTERVAL %IN_BYTES %IN_PKTS %IPV4_SRC_ADDR
%IPV4_DST_ADDR %IPV4_NEXT_HOP %IPV6_SRC_ADDR %IPV6_DST_ADDR %IPV6_NEXT_HOP
%L4_SRC_PORT %L4_DST_PORT %SRC_VLAN %DOT1Q_SRC_VLAN %SRC_TOS %TCP_FLAGS
%PROTOCOL %IP_PROTOCOL_VERSION %DIRECTION %FLOW_START_MILLISECONDS
%FLOW_END_MILLISECONDS %INPUT_SNMP %OUTPUT_SNMP %IN_SRC_MAC %OUT_DST_MAC
%ICMP_TYPE %BIFLOW_DIRECTION %L7_PROTO_NAME" --tcp "0.0.0.0:2055" -b 1 -i
any --json-labels -t 60
```

Poort 4739 is de TCP poort waarop elastiflow luistert voor netflow data (zie handleiding).

Helaas verscheen deze data niet in ons Kibana dashboard. Wanneer we naar de logs van Logstash keken, zagen we het volgende:

```
Dec 07 12:56:20 ip-10-0-0-41 logstash[2358]: [2020-12-07T12:56:20,137][WARN
][logstash.codecs.netflow
][elastiflow][6cdbbc24fc25ddb786714c77ddf2ff692d2c8c38bc72834ce7d08da78acf4
303] Ignoring Netflow version v2683

Dec 07 12:56:20 ip-10-0-0-41 logstash[2358]: [2020-12-07T12:56:20,137][WARN
][logstash.codecs.netflow
][elastiflow][e05f3254de6bd67a513a705bf17a338b50ed37230f6a5299a9c256d6402a4
371] Can't (yet) decode flowset id 257 from source id 17, because no
template to decode it with has been received. This message will usually go
away after 1 minute.
```

```
Dec 07 12:56:20 ip-10-0-0-41 logstash[2358]: [2020-12-07T12:56:20,138][WARN
][logstash.codecs.netflow
][elastiflow][e05f3254de6bd67a513a705bf17a338b50ed37230f6a5299a9c256d6402a4
371] Can't (yet) decode flowset id 258 from source id 17, because no
template to decode it with has been received. This message will usually go
away after 1 minute.
```

Daarna hebben we geprobeerd om de netflow data te verzenden met een andere nprob template.

```
nprobe -T "%IPV4_SRC_ADDR %L4_SRC_PORT %IPV4_DST_ADDR %L4_DST_PORT
%PROTOCOL %IN_BYTES %OUT_BYTES %FIRST_SWITCHED %LAST_SWITCHED %IN_PKTS
%OUT_PKTS %IP_PROTOCOL_VERSION %APPLICATION_ID %L7_PROTO_NAME %ICMP_TYPE
%SRC_IP_COUNTRY %DST_IP_COUNTRY %APPL_LATENCY_MS" --tcp "0.0.0.0:2055" -b 1
-i any --json-labels -t 60
```

Ook bij het veranderen van de template, verscheen onze data niet in het kibana dashboard.

Als laatste hebben we onze nprob daemon geconfigueerd zoals Rob Cowart aanbeveeld in de installatie handleiding:
https://gist.github.com/robcowart/afd538026db29ee96dd9c495efb52ea6

Ook dit werkte helaas niet.