

Labra 1

Palveluiden automatisointi

Markus Häkkinen
Ville Pulkkinen
Mikael Romanov

Harjoitustyö
Tammikuu 2018
Tieto- ja viestintätekniikan koulutusohjelma
Tekniikan ala

Sisältö

1	Johdanto	2
2	Palvelut.....	3
2.1	NtopNG	3
2.2	nProbe	4
2.3	Elasticsearch	5
3	Palveluiden asennus.....	7
3.1	Ntopng	8
3.2	Elasticsearch	11
4	Komennot	14
4.1	Ntopng	14
4.2	Elasticsearch	15
5	Muutoskenaario	17
5.1	IP-osoitteen tai portin muuttaminen	17

1 Johdanto

Palveluiden automatisoinnin kurssilla ensimmäisessä laboratorioharjoituksessa piti suunnitella palvelu, joka automatisoidaan eri tekniikoita käyttäen. Lisäksi kaikki palvelut pitää paketoida ns. ”kontteihin” (eräänlainen helposti siirrettävä virtuaalikone) tulevissa harjoituksissa. Otimme tavoitteeksi ottaa käyttöön NtopNG-palvelun, joka on verkkoliikenteen taltiointiin ja analysointiin tarkoitettu ohjelmistopaketti. Toinen käyttämämme palvelu on Elasticsearch tiedon tallennus- ja hakukonemoottori. Elasticsearchin tarkoitus on säilöä NtopNG:n saama verkkoliikenne myöhempää analysointia ja tarkistelua varten.

2 Palvelut

Palvelun valinnassa oli tiettyjä vaatimuksia joiden mukaan ne tuli valita. Palvelun komponenttien pitää olla ilmaisia, muokattavissa sekä niiden tulee toimia Linux käyttöjärjestelmän päällä. Lisäksi palveluiden kontittaminen pitää olla mahdollista. Kontit tulevat olemaan Docker-kontteja. Tämä aiheutti hieman rajoitteita alkuperäiseen suunnitelmaan. Alkuperäinen suunnitelma oli automatisoida IDS/verkkoolyysaattori-järjestelmä ja tallentaa sen data erilliselle tietokannalle, mutta verkkoliikenteen haistelu tapahtuu käyttämällä ”promiscuous”-tilassa (verkkokortti vastaanottaa kaiken tulevan liikenteen, ei pelkästään sille suunnattua liikennettä) olevaa L2-verkkokorttia. Kontin verkkorajapinnat taas ovat L3-rajapintoja, eli kontin sisällöllä on käytettävissä vain IP-rajapinta, joten kontti ei itse kykene tekemään verkkoliikenteen haistelua.

Tästä huolimatta työ onnistuu, sillä NtopNG tukee etäpalvelimella tehtävää verkkoliikenteen haistelua nProbe nimisellä sovelluksella. Tällöin kontissa oleva NtopNG vain vastaanottaa nProben lähettämää tiivistelmää verkkoliikenteestä ja NtopNG:n vastuulle jää analysoida data, sekä taltioida se Elasticsearch järjestelmään.

2.1 NtopNG

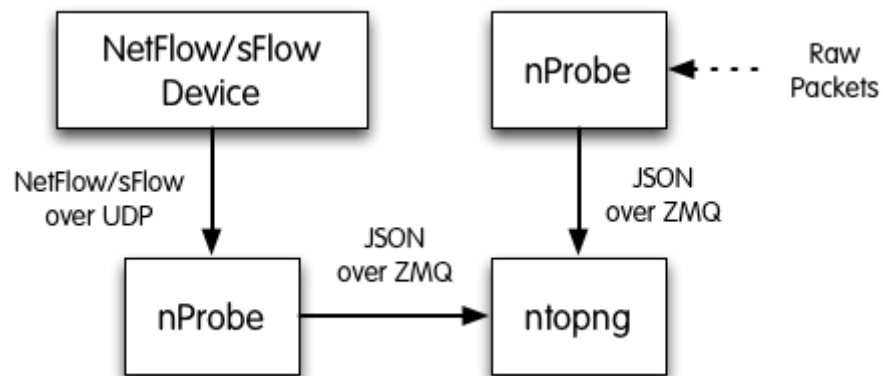
NtopNG on libPcap-kirjastoon perustuva verkkoliikenteen valvontaan ja analysointiin tarkoitettu ohjelmisto. NtopNG perusversio on ilmainen ja avoimen lähdekoodin, mutta ohjelmistosta on tarjolla myös kaupalliset versiot. Kaupallisissa versioissa on mm. enemmän lisäosia liikenteen analysointiin, sekä tuotetuki. NtopNG voidaan asentaa mihin tahansa Linux alustaan. Ntopng:ssä on HTTPS-pohjainen web-käyttöliittymä. NtopNG:llä voidaan analysoida verkkoliikennettä eri kriteerien perusteella, kuten IP-osoitteiden, VLANeiden, AS-alueiden tai protokollan mukaan. NtopNG tukee datan vientiä mm. MySQL ja Elasticsearch tietokantoihin.

NtopNG suorittaa verkkoliikenteen haistelun joko itse suoraan L2-tasolla verkkokortista, tai vastaanottaa nProbe-palvelimelta verkkoliikenteen tiivistelmää. Tiivistelmä nProbelta tulee JSON-muodossa ZMQ-protokollalla. Tiivistelmä verkkoliikenteestä sisältää mm. lähde ja kohde IP-osoitteet, lähde- ja kohdeportit,

protokollan, VLAN-tunnukset, hyötykuorman koon. Kaikki ns. otsikkotiedot (header), mutta ei varsinaista datapaketin sisältöä.

NtopNG säilöo vastaanotetun datan tietokantamoottoriin, joka meidän tapauksessa on Elasticsearch. Tästä datasta NtopNG luo analyysiä verkkoliikenteestä. Graafisessa käyttöliittymässä NtopNG esittää mm. mitkä laitteet (lähde-IP ja kohde-IP) luovat liikennettä kuinka paljon, millä protokollalla. NtopNG siis näyttää mitä verkossa tapahtuu ja mistä verkkoliikenne koostuu. NtopNG:n kyky analysoida dataa on kohtalaisen kehittynyt, sillä voi helposti esittää mikä verkkoliikennettä juuri nyt käyttää, sekä historiaa pitemmältä aikajaksolta. Dataa voi myös analysoida protokolla ja laitekohtaisesti.

2.2 nProbe



Kuvio 1 NtopNG ja nProbe järjestelmän datankeruu

nProbe on NtopNG:n tekijöiltä erillinen ohjelmisto datan etäkeruuta varten. nProbe asennetaan yleensä erilliselle palvelimelle, jossa nProbe haistelee verkkoliikennettä suoraan L2-tasolla verkkokortista. nProbe kerää aiemmin mainitun tiivistelmän verkkoliikenteestä ja lähettää sen JSON-muodossa ZMQ-protokollaa käyttäen NtopNG-analysoitsijalle. Konsepti on siinä, että analyysiä (ja taltiointia) tekevä palvelin voi olla omansa ja varsinainen verkkoliikenteen kaappaus ja haistelu voidaan ulkoistaa eri palvelimelle. Myöskin näitä haistelevia nProbe-palvelimia voi olla useita,

eri puolilla isoakin verkkoa. Näin saadaan kuorma jaettua tehokkaasti, sekä verkkoliikenne-analyysi monesta eri pisteestä.

nProbe tukee myös NetFlow ja sFlow datankeruuta. NtopNG ei itse tue sitä, vaan tällaisen datan keräämiseen vaaditaan nProbe. NetFlow ja sFlow ovat kytkinten/reitittimien käyttämä protokolla, jolla läpikulkevasta verkkoliikenteestä kerätään tiivistelmä (aiemmin mainitut headerit) ja kerrotaan keräävälle palvelimelle. Näin verkkoympäristön ylläpitäjä saa jonkinnäköistä kuvaa siitä, mitä läpikulkeva verkkoliikenne on. Tästä datasta voidaan tehdä analyysiä niin vikatilanteissa, kuin mahdollisissa hyökkäystilanteissa.

Huom! nProbe on maksullinen komponentti, joten sitä ei sisällytetä tähän harjoitukseen. nProbe on testiympäristössämme käytössä toiminnallisuuden varmistamiseksi, mutta varsinaiseen kontitusharjoitukseen sitä ei sisällytetä.

2.3 Elasticsearch

Elasticsearch perustuu Apache Lucenen hakukoneeseen, se on yleisen datan tallennus- ja hakukonejärjestelmä. Elasticsearch tarjoaa reaaliaikaista hakua HTTP rajapinnan avulla JSON-formaatissa. Elasticsearch on nimensä mukaisesti elastinen, sillä sitä voidaan laajentaa erittäin helposti. Elasticsearch toimii erittäin helposti miten isoissa ympäristöissä tahansa, sillä se tukee clusterointia (datan ja datankäsittelyn, sekä tallentamisen jakamista useille koneille) ja järjestelmä osaa pilkkoa varsinaisen datan useammille koneille, sekä suorittaa haut datasta useilta koneilta. Elasticsearch ympäristöä voidaan laajentaa helposti jälkeenpäin, esimerkiksi jos kuormitus kasvaa liian suureksi, clusteria voidaan laajentaa hyvin pienellä vaivalla.

Elasticsearch ei ole varsinainen tietokantamoottori, vaan vapaamuotoisen datan säilömis- ja hakemisjärjestelmä. Elasticsearchissa ei määritellä tiukasti tietokantoja tai datan tyyppiä, vaan järjestelmään voi ajaa hyvinkin vapaamuotoista dataa. Järjestelmästä pystyy myös hakemaan dataa erittäin kehittyneillä suodattimilla ja rajauksilla. Elasticsearch sopii parhaiten tilanteeseen, kun tarvitaan korkeaa suorituskykyä ja käytetty data on erittäin epäsäännöllistä ja monimuotoista.

Elasticsearchissa on myös valmiiksi datan replikointiin, eli varmuuskopiointiin, erinomaiset valmiudet. Voit ilman erillistä replikointijärjestelmää määrittää, mitkä koneet toimivat vain varmuuskopiointia varten. Elasticsearch osaa myös automaattisesti palauttaa dataa replikoista, varsinaisen clusterin käyttöön.

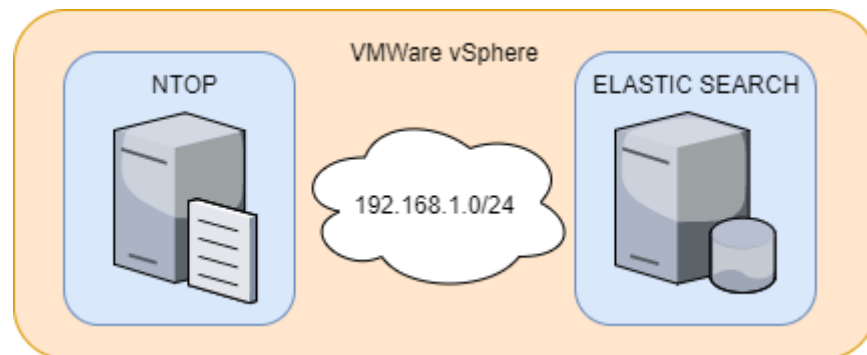
Elasticsearch on avoimen lähdekoodin tuotos, täten myös siis ilmainen.

Käyttämässämme ympäristössä emme käytä Elasticsearchia cluster-tilassa, vaan yksi ainoa kone tuottaa koko palvelun.

Elasticsearchissa koneiden tyypit voivat olla joko *"client"*, *"master"* tai *"data"*. Client-koneet tarjoavat HTTP-rajapinnan, josta ulkopuoliset palvelut voivat taltioda tai hakea dataa. Master-koneet taas toimivat clusterin valvojina, nämä määrittelevät miten data pirstaloidaan eri datasäilöihin, kuka replikoi (varmuuskopioi) ja miten, sekä seuraa clusterin toimintaa ja kuntoa. Data-koneet taas säilövät dataa, nämä ovat vain orjia jotka tallentavat datan. Meidän ympäristössä on vain yksi Elasticsearch kone, joka toimii niin data, client ja master tilassa. Täten yksi ainoa kone tuottaa HTTP-rajapinnan, säilöö datan ja valvoo/hallitsee omaa toimintaansa.

3 Palveluiden asennus

Molemmat palvelut asennetaan Debian 9 jakeluiden päälle. Ympäristö asennetaan kahdelle virtuaalikoneelle VMware vSphere-ympäristössä. VMwaressa hypervisorina on ESXi 6.5U1 ja hallintana vCenter 6.5. Ympäristö toimii lähtökohtana harjoituksen luomisessa, eli tässä pystytämme palvelut virtuaalikoneisiin ja testaamme palveluiden toiminnan, ennen kuin palveluita ryhdytään kontittamaan.



Kuvio 2 Ympäristö

Molemmat virtuaalikoneet päivitetään ensiksi ajan tasalle, ennen kuin uusia paketteja aletaan asentamaan. Tällä varmistamme, että koneissa on kaikki ajantasaiset tietoturvapäivitykset, jotta koneet olisivat turvallisia ja luotettavia. Koneiden päivitys tapahtuu yksinkertaisesti komennolla *"sudo apt-get update && sudo apt-get -y upgrade"* (Kuvio 3), jolloin kone päivittää ensimmäisenä pakettilistat, jonka jälkeen päivitetään paketit kysymättä mitään. Parametri -y tarkoittaa, että vastataan kaikkiin kyselyihin "yes", jolloin paketit päivittyvät laakista ilman erillisiä kyselyitä.

```
rooki@ntopng:~$ sudo apt-get update && sudo apt-get upgrade -y
Hit:1 http://fi.archive.ubuntu.com/ubuntu artful InRelease
Hit:2 http://fi.archive.ubuntu.com/ubuntu artful-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu artful-security InRelease
Hit:4 http://fi.archive.ubuntu.com/ubuntu artful-backports InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  linux-generic linux-headers-generic linux-image-generic
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
rooki@ntopng:~$
```

Kuvio 3 Perusjärjestelmän päivitys

Koska ympäristömme toimii VMware ympäristössä, niin koneisiin asennetaan paketti `open-vm-tools`, jotka parantavat virtuaalikoneen suorituskykyä, sekä helpottaa järjestelmien hallintaa vSphere-ympäristössä. VM-tools raportoi VMCI-hallintakanavaa pitkin hypervisorille mm. laitteen IP-osoitteen, sekä virtualisoidun raudan tilan, kuten muistinkäytön. Ohjelmisto myös nollaa vapautuneen muistin ja raportoi vapautuneen muistin alueen hypervisorille, jolloin virtualisointia suorittava hypervisor tietää mikä alue fyysisestä muistista on vapaana ja käytettävissä muille virtuaalikoneille. Open-vm-tools paketin asennus tapahtuu komennolla *"sudo apt-get -y install open-vm-tools"* (Kuvio 3).

```
rooki@ntopng:~$ sudo apt-get -y install open-vm-tools
[sudo] password for rooki:
Reading package lists... Done
Building dependency tree
Reading state information... Done
open-vm-tools is already the newest version (2:10.1.10-3).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
rooki@ntopng:~$
```

Kuvio 4 open-vm-tools asennus

3.1 Ntopng

Ntopng voidaan asentaa joko esikäännettyistä binääreistä, lähdekoodeista tai paketinhallinnasta. Debianissa oletus pakettienhallintatyökalu on apt. Debianiin täytyy ensiksi lisätä Ntop:in pakettilähde, jolloin apt tietää mistä paketit pitää asentaa. Tämä suoritetaan komennoilla

- *wget http://apt-stable.ntop.org/stretch/all/apt-ntop-stable.deb*
- *sudo dpkg -i apt-ntop-stable.deb*

Ensiksi ladataan ntop-projektin deb-paketti, jossa on apt-pakettienhallinnalle uudet lähdeosoitteet, sekä GPG-avain pakettilähteille. Tämänjälkeen deb-paketti asennetaan pääkäyttäjän oikeuksilla järjestelmään

Tämän jälkeen päivitetään pakettienhallinta ja asennetaan NtopNG komennoilla

- *sudo apt-get update && sudo apt-get install pfring ntopng ntopng-data*

Ntopng:n konfiguraatitiedostot löytyvät `/etc/ntopng` kansion alta. Varsinainen asetustiedosto on kansioista löytyvä `ntopng.conf`. Oletus konfiguraatio kuuntelee TCP

porttia 3000 hallintaa varten. Ntop tunnistaa automaattisesti parhaan kuunneltavat rajapinnan, jos sitä ei ole erikseen määritetty. NtopNG:n konfiguraation muokataan muutamia arvoja, jotta NtopNG alkaa lähettämään dataa Elasticsearchin datasäilöön, sekä kuuntelemaan nProbea. Muokataan siis tiedostoa */etc/ntopng/ntopng.conf*. Lisätään sinne seuraavat rivit (jos parametri on jo olemassa, eli parametri löytyy, eikä sitä ole kommentoitu pois #-etumerkillä, niin muokataan parametri listan mukaiseksi).

- *-e=*
- *-i=tcp://172.16.81.24:5556*
- *-w=3000*
- *-m=172.16.81.0/24*
- *-F=es;flows;ntopng-%Y.%m.%d;http://172.16.81.20:9200/_bulk;*
- *--no-promisc=""*

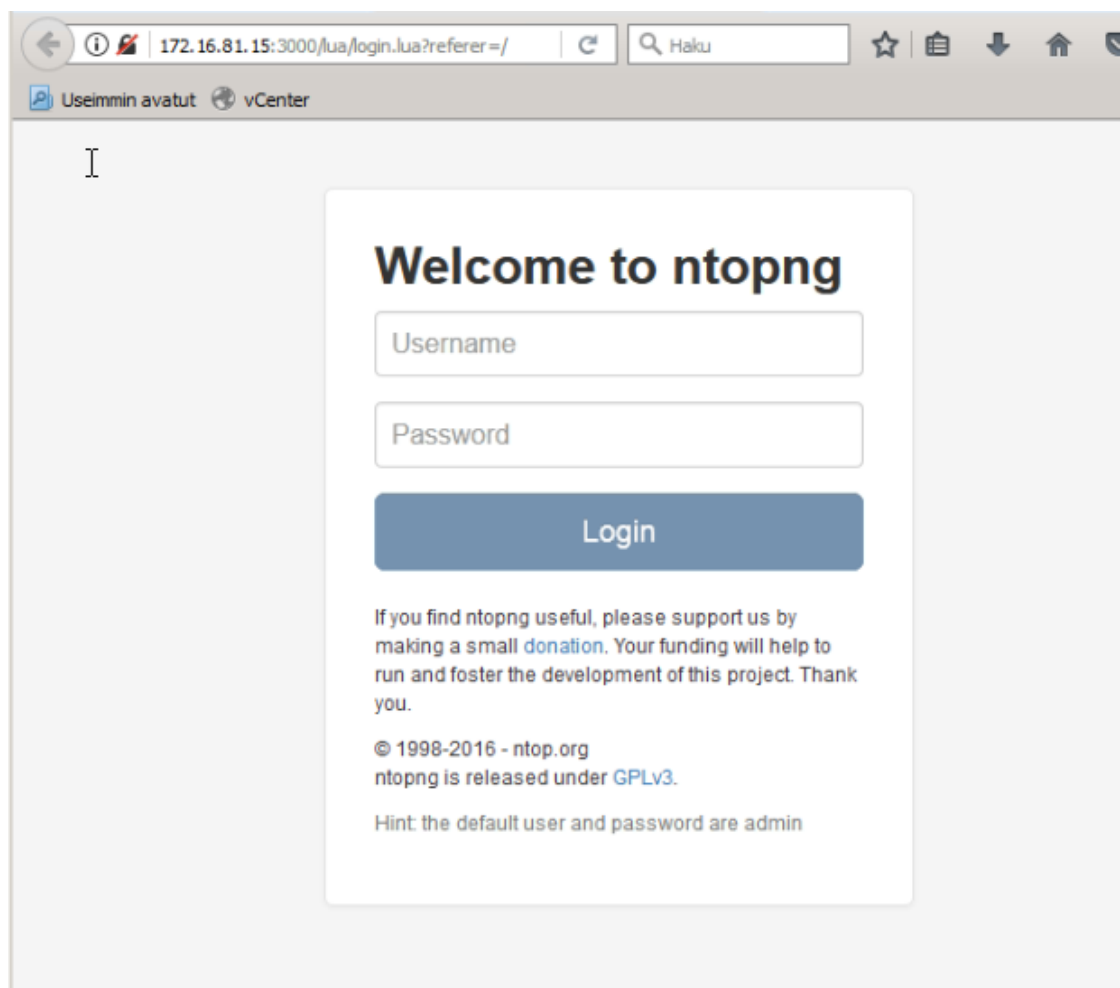
Konfiguraatiossa täytyy olla tarkkana, että yksittäisetkin parametrit (ilman attribuuttia) päättyvät = merkkiin. Parametri *-e* käskii NtopNG:n käynnistyvän palvelutilassa, jolloin SystemD huolehtii järjestelmän toiminnasta. Ilman kyseistä parametria palvelu toimisi vain aktiivisessa terminaalissa. Parametrillä *"-i=tcp://172.16.81.24:5556"* käsketään, että NtopNG kerää analysoitavan liikenteen palvelimelta 172.16.81.24 portista 5556/TCP. Kyseinen palvelin on nProbe-palvelin, joka tekee varsinaisen liikenteen haistelun. Parametri *"-w=3000"* määrää NtopNG:n web-hallinnan toimimaan portissa 3000/TCP. Parametrillä *"-m=172.16.81.0/24"* määritellään NtopNG:lle niinsanottu lähiverkko, jolla NtopNG tietää mikä verkkoliikenne on esimerkiksi sen luomaa ja mikä verkko luokitellaan lähiverkoksi. Tämä vaikuttaa lähinnä verkkoliikenteen analysointiin ja sen kuvaamiseen ylläpitäjälle.

Parametrillä *"-F=es;flows;ntopng-%Y.%m.%d;http://172.16.81.20:9200/_bulk;"* määrätään NtopNG tallentamaan liikennedatan Elasticsearch-tallennusmoottoriin (parametri *"es;"*), tietokantaan tyypiltään *"flows"*, tietokantaan nimeltään *"ntopng-%Y.%m.%d"* (joista %Y korvataan nelinumeroisella vuosiluvulla, %m korvataan kaksinumeroisella kuukauden numerolla, sekä %d korvataan kaksinumeroisella päivän numerolla). Tallennusmoottorin osoite on *"http://172.16.81.20:9200"* ja

”/_bulk” määrittelee, että Elasticsearchiin tallennetaan data POST-menetelmällä, jolloin voidaan tallentaa isompi määrä dataa kerralla. Viimeinen parametri ”;” on tyhjä. Puolipisteen jälkeen voisi olla käyttäjätunnus ja salasana Elasticsearch tietokantaan, mutta tätä meillä ei ole käytössä.

Viimeinen parametri on ”—no-promisc=” jolla määrätään, ettei NtopNG muuta verkkokorttejansa *promiscuous*-tilaan, eli NtopNG ei yritä itse haistella verkkoliikennettä.

NtopNG käynnistään komennolla ”systemctl restart ntopng.service”.



Kuvio 5 NtopNG käynnissä

3.2 Elasticsearch

Elasticsearch pohjautuu Javaan, joten se tarvitsee toimiakseen Java 8 tai uudemman asennettuna palvelinkoneeseen. Voimme asentaa Javan pakettienhallinnasta komennolla lisäämällä Javan pakettilähteen komennoilla (root-oikeuksilla):

- `echo "deb http://ppa.launchpad.net/webupd8team/java/ubuntu xenial main" >> /etc/apt/sources.list.d/webupd8team-java.list`
- `apt-key adv --keyserver http://keyserver.ubuntu.com:80 --recv-keys EEA14886`

Pakettilähteiden lisäämisen jälkeen pystymme asentaa Elasticsearchin vaatiman Java version komennolla:

- `apt-get update && apt-get install oracle-java8-installer`

Asennetun Javan version voi tarkistaa komennolla `"java -version"`.

```
rooki@elasticsearch:~$ java -version
openjdk version "1.8.0_151"
OpenJDK Runtime Environment (build 1.8.0_151-8u151-b12-0ubuntu0.17.10.2-b12)
OpenJDK 64-Bit Server VM (build 25.151-b12, mixed mode)
rooki@elasticsearch:~$
```

Kuvio 6 Java-version tarkistus

Elasticsearch paketin asentamiseen on useita eri vaihtoehtoja. Kaikista helpoin tapa on asentaa se pakettihallinnasta lisäämällä Elasticsearchin pakettilähteen:

- `apt-get install apt-transport-https`
- `echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" >> /etc/apt/sources.list.d/elastic-6.x.list`
- `wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -`
- `apt-get update && apt-get install elasticsearch`

Pakettilähteiden lisäämisessä on huomioitava ensimmäinen komento, eli `"apt-transport-https"`-paketin asennus. Elasticin pakettilähteet ovat HTTPS-protokollan takana, eikä APT osaa ilman kyseistä pakettia asentaa pakettilähteestä paketteja.

Elasticsearch ei automaattisesti käynnisty asennuksen jälkeen. Elasticsearch määritellään käynnistymään järjestelmän käynnistyessä komennolla `"sudo systemctl enable elasticsearch.service"`.

Jotta Elasticsearch voidaan käynnistää, meidän pitää säätää kyseisen palvelun asetuksia. Nämä asetukset löytyvät `/etc/elasticsearch/elasticsearch.conf` tiedostosta. Muokattavat asetukset arvoineen ovat seuraavat:

- `cluster.name: NtopNG-ELASTIC`
- `node.name: srv-elastic`
- `network.host: 172.16.81.20`
- `http.cors.enabled: true`
- `http.cors.allow-origin: "*"`
- `http.cors.allow-methods: OPTIONS, HEAD, GET, POST, PUT, DELETE`
- `http.cors.allow-headers: "X-Requested-With, Content-Type, Content-Length, X-User"`

Asetukset tarkoittavat seuraavaa, "*cluster.name*" arvo määrittelee Elasticsearch-clusterin nimen. "*node.name*" määrittelee tämän Elasticsearch koneen nimen. Asetukset ovat erityisen kriittisiä jos Elasticsearchia käytetään monen koneen clusterissa, mutta yhden koneen tapauksessa nimet eivät ole niin merkitseviä. "*network-host*" määrittelee, missä rajapinnassa Elasticsearch toimii. Jos koneen IP-osoite vaihtuu, tämä täytyy vaihtaa sopivaksi! Asetus "*http.cors.enabled*" määrittelee, sallitaanko Cross-Origin-Resource-Sharing, eli sallitaanko muista domaineista/IP-osoitteista tulevat pyynnöt järjestelmään. Asetus "*http.cors.allow-origin*" kertoo, mistä tulevat pyynnöt Elasticsearch-moottorille sallitaan. Asennus ja testausvaiheessa käytetään tähteä (*wildcard*), jolla sallitaan kyselyt kaikkialta. Tämä on tietoturva-uhka oikeassa ympäristössä, mutta asennus- ja testausvaiheessa pyyntöjen salliminen kaikkialta helpottaa testausta. Lopuilla CORS-asetuksilla määritellään, mitä pyyntöjä muualta sallitaan. Ainoa asetus mihin tarvitsee jälkeenpäin koskea, on "*http.cors.allow-origin*", jolla rajataan kuka voi pyyntöjä tehdä. Toinen vaihtoehto tehdä tämä tietoturvallisesti, on rajata IPtables-palomuurilla kuka voi Elasticsearch-palveluun yhdistää.

Toinen asetustiedosto mitä pitää muokata, on Elasticsearchin käynnistysparametri-tiedosto, joka löytyy sijainnista `/etc/default/elasticsearch`. Muokataan tiedostoon seuraavat parametrit:

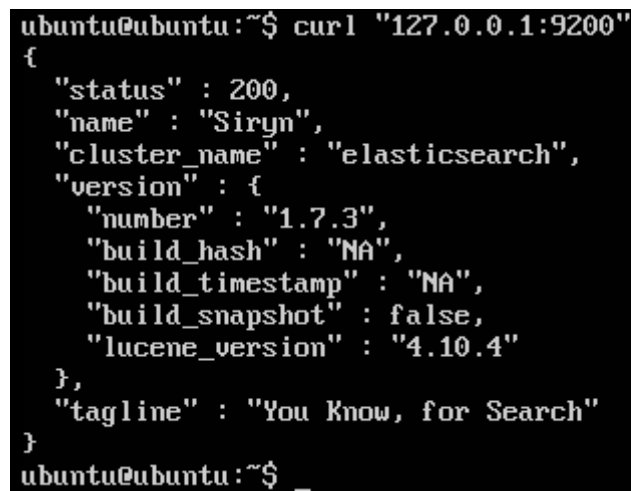
```
ES_HOME=/usr/share/elasticsearch
```

```
RESTART_ON_UPGRADE=true
```

Parametrit määrittelevät Elasticsearchin kotihakemiston, sekä jälkimmäinen parametri käskii Elasticsearch-palvelua käynnistymään uudelleen päivitysten yhteydessä.

Tiedostojen muokkaamisen jälkeen uudelleenkäynnistetään palvelu komennolla *"systemctl restart elasticsearch.service"*.

Elasticsearch käynnistäminen tapahtuu komennolla *"systemctl start elasticsearch"*. Tietokannan toimivuus voidaan testata komennolla *"curl '127.0.0.1:9200'"* joka tekee HTTP-pyyntöä Elasticsearch palvelimelle porttiin 9200 ja palauttaa sieltä JSON vastauksen joka tulostuu ruudulle.

A terminal window with a black background and white text. The prompt is 'ubuntu@ubuntu:~\$'. The command 'curl "127.0.0.1:9200"' is entered. The output is a JSON object: {'status': 200, 'name': 'Siryn', 'cluster_name': 'elasticsearch', 'version': {'number': '1.7.3', 'build_hash': 'NA', 'build_timestamp': 'NA', 'build_snapshot': false, 'lucene_version': '4.10.4'}, 'tagline': 'You Know, for Search'}. The prompt returns to 'ubuntu@ubuntu:~\$' followed by a cursor.

```
ubuntu@ubuntu:~$ curl "127.0.0.1:9200"
{
  "status" : 200,
  "name" : "Siryn",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.7.3",
    "build_hash" : "NA",
    "build_timestamp" : "NA",
    "build_snapshot" : false,
    "lucene_version" : "4.10.4"
  },
  "tagline" : "You Know, for Search"
}
ubuntu@ubuntu:~$ _
```

Kuvio 7 Onnistunut pyyntö Elasticsearch palvelulle

4 Komennot

Palveluiden automatisointia varten jokainen syötettävä komento palvelun asentamista varten on otettava ylös, jotta ne voidaan myöhemmin syöttää automaattisesti eikä mikään paketti tai asetus jää muuttumaan.

4.1 Ntopng

Tässä kappaleessa on kerrottu palveluiden asentamiseen vaadittavat komentoketjut. Komennot suoritetaan pääkäyttäjän oikeuksilla.

1. *apt-get update && apt-get -y upgrade*
2. *apt-get -y install open-vm-tools openssh-server*
3. *wget http://apt-stable.ntop.org/stretch/all/apt-ntop-stable.deb*
4. *dpkg -i apt-ntop-stable.deb*
5. *apt-get install pfring ntopng ntopng-data*

Palvelun asentamisen jälkeen muokataan konfiguraatiota seuraavasti. Huom, tässä oletetaan palvelimen 172.16.81.24 olevan nProbe-palvelin, sekä palvelimen 172.16.81.20 olevan Elasticsearch palvelin.

1. *echo "-e=" >> /etc/ntopng/ntopng.conf*
1. *echo "-i=tcp://172.16.81.24:5556" >> /etc/ntopng/ntopng.conf*
2. *echo "-w=3000" >> /etc/ntopng/ntopng.conf*
3. *echo "-m=172.16.81.0/24" >> /etc/ntopng/ntopng.conf*
4. *echo "-F=es;flows;ntopng-%Y.%m.%d;http://172.16.81.20:9200/_bulk;" >> /etc/ntopng/ntopng.conf*
5. *echo "--no-promisc=" >> /etc/ntopng/ntopng.conf*

Viimeiseksi palvelu pitää vain käynnistää komennolla
"systemctl restart ntopng.service"

4.2 Elasticsearch

Elasticsearchin asennukseen liittyvät komennot ovat listattuna alla.

1. *apt-get update && apt-get -y upgrade*
2. *apt-get -y install open-vm-tools openssh-server*
3. *echo "deb http://ppa.launchpad.net/webupd8team/java/ubuntu xenial main"*
>> /etc/apt/sources.list.d/webupd8team-java.list
4. *apt-key adv --keyserver http://keyserver.ubuntu.com:80 --recv -keys*
EEA14886
5. *apt-get update && apt-get -y install oracle-java8-installer*
6. *apt-get -y install apt-transport-https*
7. *echo "deb <https://artifacts.elastic.co/packages/6.x/apt> stable main" >>*
/etc/apt/sources.list.d/elastic-6.x.list
8. *apt-get update && apt-get -y install elasticsearch*

Elasticsearchin asetukset ovat listattuna alla. Tässä oletetaan Elasticsearch palvelun kuuntelevan pyyntöjä osoitteessa "172.16.81.20".

1. *echo "cluster.name: NtopNG-ELASTIC" >> /etc/elasticsearch/elasticsearch.yml*
2. *echo "node.name: srv-elastic" >> /etc/elasticsearch/elasticsearch.yml*
3. *echo "network.host: 172.16.81.20" >> /etc/elasticsearch/elasticsearch.yml*
4. *echo "http.cors.enabled: true" >> /etc/elasticsearch/elasticsearch.yml*
5. *echo "http.cors.allow-origin: \"*\":" >> /etc/elasticsearch/elasticsearch.yml*
6. *echo "http.cors.allow-methods: OPTIONS, HEAD, GET, POST, PUT, DELETE" >>*
/etc/elasticsearch/elasticsearch.yml
7. *echo "http.cors.allow-headers: \"X-Requested-With, Content-Type, Content-*
Length, X-User\"" >> /etc/elasticsearch/elasticsearch.yml

Tämän jälkeen lisätään vielä käynnistymisasetukset.

1. *echo "ES_HOME=/usr/share/elasticsearch" >> /etc/default/elasticsearch*
2. *echo "RESTART_ON_UPGRADE=true" >> /etc/default/elasticsearch*

Lopuksi uudelleenkäynnistetään palvelu komennolla *"systemctl restart elasticsearch.service"*. Kaikki komennot suoritetaan pääkäyttäjän oikeuksilla.

Komennoissa on käyttökohteesta riippuen tarkistettava IP-osoitteet. Elasticsearch käsketään kuuntelemaan yksittäisessä IP-osoitteessa parametrilla *"network.host:"*, jolloin IP-osoitteen täytyy olla koneen (tai kontin) osoite, johon Elasticsearchille tulevat kyselyt lähetetään. Yhtä lailla NtopNG:n asetuksissa parametrin *"-m="* täytyy olla NtopNG:n lähiverkko/IP-avaruus, jonka pyyntöjä ei käsitellä. Samoin parametri *"-F="* täytyy sisältää Elasticsearch-tallennusjärjestelmän IP-osoitteen, sekä parametri *"-i="* täytyy osoittaa nProbe liikenteenkeruujärjestelmään.

5 Muutosskenaario

Palvelussamme yleisiä muutoksia voivat olla tietokantapalvelimen muuttaminen toiseen IP-osoitteeseen, portin muuttaminen tai tietokannan siirtäminen kokonaan toiselle koneelle.

5.1 IP-osoitteen tai portin muuttaminen

Jos elasticsearch ip-osoite tai portti muuttuu niin palvelimeen ei tarvitse kuin muuttaa network.host osoite. Koska ntopng siirtää kaiken datan elasticsearchille on ntopng palvelu pysäytettävä ja muokattava sen konfiguraatioon uuden elasticsearchin IP-osoite ja portti.

1. *systemctl stop ntopng.service*
2. *systemctl stop elasticsearch.service*
3. *NANO /etc/ntopng/ntopng.conf*
4. *-F=es;flows;ntopng-%Y.%m.%d;http://uusi_ip_osoite:uusiportti/_bulk;*
5. *NANO /etc/elasticsearch/elasticsearch.yml*
6. *network.host: uusi_ip_osoite*
7. *http.port: uusiportti*
8. *systemctl restart elasticsearch.service*
9. *systemctl restart elasticsearch.servivce*