Ville Suominen

LOKITIEDOSTOJEN HALLINTAA
- GRAYLOG

Tietotekniikan koulutusohjelma

2018

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

LOKITIEDOSTOJEN HALLINTAA - GRAYLOG

Suominen, Ville
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Toukokuu 2018
Ohjaaja: Aromaa, Juha DI
Sivumäärä: 29

Asiasanat: lokitiedostot, UNIX, verkkoliikenne, tietoverkot, verkonhallinta

---

Tässä opinnäytetyössä selvitettiin avoimeen lähdekoodiin perustuvan lokitiedostojen hallintajärjestelmän perustamista virtuaalipalvelimelle ja tutkittiin kyseisen sovelluksen tarjoamia vaihtoehtoja ja mahdollisuuksia käyttöliittymien sekä verkkoliikenteen lokitiedostojen valvontaan. Sovelluksella pystytään pitämään tarkkaa lokia liikenteestä, tämän sisällöstä ja tyypistä sekä näiden tietojen pohjalta priorisoida ja tehostaa verkon toimintaa ja turvallisuutta.

Käytetty sovellus on UNIX-pohjainen Graylog, joka perustettiin Satakunnan ammattikorkeakoulun omalle virtuaalikonepalvelimelle hyödyntäen käyttöliittymää Ubuntu. Graylog on vain yksi monista vaihtoehdoista avoimeen lähdekoodiin perustuvien sovellusten saralla, mutta Graylog valittiin tämän suosion vuoksi. Tällä opinnäytetyöllä haetaan käyttöarvoa seurantasovelluksille yleisesti ja tutkitaan saatuja tuloksia niiden käyttöarvon valossa.

LOGFILE MANAGEMENT - GRAYLOG

Suominen, Ville
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information Technology
May 2018
Supervisor: Aromaa, Juha MSc.
Number of pages: 29

Keywords: logfiles, UNIX, network traffic, information networks, network management

---

The purpose of this thesis was to find out how to setup and manage an open source logfile management software on a virtual server and note the practicalities and opportunities offered for network surveillance by the software. This management application allows the user to keep detailed logs about traffic in the network, the contents of it and the types of data included within for more prioritized, optimized and secure networking.

The application used in this thesis is the UNIX based Graylog, which was installed on the Satakunta University of Applied Sciences own virtual machine server using Ubuntu as its base. It is to be noted that Graylog is only one of the many available open source alternatives for monitoring networks and was chosen for its general popularity. This thesis is focused on the value offered by using a monitoring software and the possibility to gain more value with the results and data achieved with it.

SISÄLLYS

LYHENTEET

ARP	Address Resolution Protocol
FTP	File Transfer Protocol
GELF	Graylog Extended Log Format
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
OVA	Open Virtual Appliance
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

1 JOHDANTO

Lokitiedostot ovat tietoliikenteen kuten käyttöliittymien ja ohjelmistojen kirjanpitoa, jotka tallentavat tietoa siitä, miten niitä on käytetty, mahdollisista virhesanomista ja ohjelmistokohtaisista valinnoista, joita käyttäjä on kohdannut.

Lokitiedostojen käytöllä voidaan ehkäistä väärinkäyttöä, määrittää ongelmien lähteet, havaita järjestelmien heikkouksia sekä parantaa suorituskykyä ja turvallisuutta. Pilvipalvelujen suosion kasvaessa myös verkkorikollisuus on kehittynyt ja yleistynyt, suuren mittakaavan tietomurrot ja rikokset vaativat entistä kehittyneemmän lokitiedostojen valvontaratkaisun.

Tässä opinnäytetyössä selvitetään, onko avoimeen lähdekoodiin perustuva sovellus Graylog mahdollisesti sopiva ratkaisu Satakunnan ammattikorkeakoulun lokitiedostojen valvontatarpeeseen.

Resursseina toimivat Satakunnan ammattikorkeakoulun oma virtuaalikonepalvelin Bokxi. Palvelimeen asennettiin yksi virtuaalikone käyttöliittymällä Ubuntu Linux ja kaksi virtuaalikonetta käyttöliittymillä Windows 7.

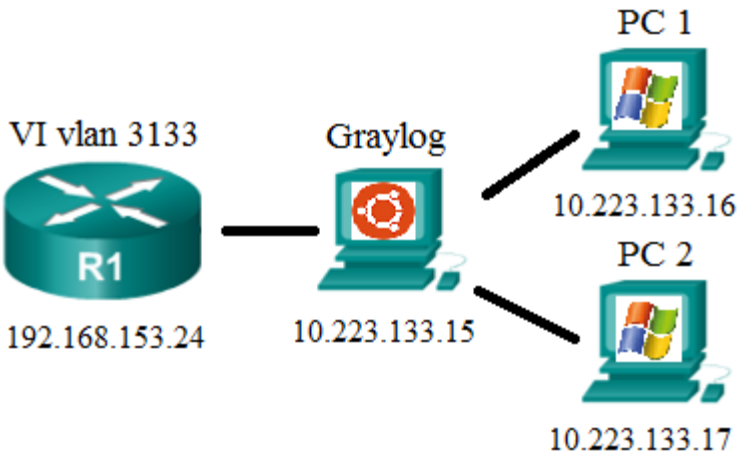
2 GRAYLOG

2.1 Yleistä

Graylog on UNIX-pohjainen avoimeen lähdekoodiin perustuva lokitiedostojen hallinta ja analysointityökalu. Sen pohjana toimivat ohjelmointikieli Java sekä apuohjelmat Elasticsearch ja MongoDB, jotka mahdollistavat yksinkertaisen ja kauniin käyttöliittymän keskitettyyn lokitiedostojen hallintaan ja analysointiin. Graylog käyttää Elasticsearch hakukonetta lokitiedostojen etsimiseen ja varastointiin, MongoDB varastoi metadataa sekä konfiguraatioita. Graylog kerää, indexoi ja analysoi lokitiedostoja eri lähteistä ja näyttää niiden sisällön verkkokäyttöliittymässä. Graylog on käyttäjäystävällinen ja valmis yritystason käyttöön ilman muutoksia.

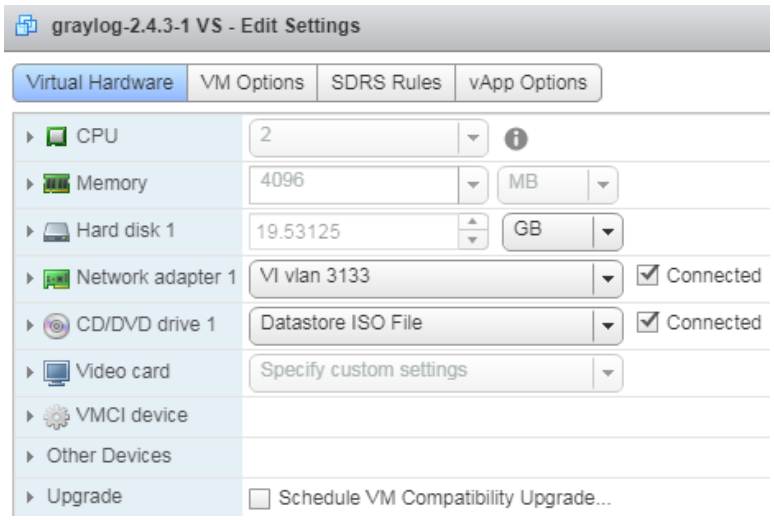
2.2 Käyttöönotto

Graylog voidaan asentaa monella eri tavalla. Tässä työssä pohjana käytettiin Samkin omaa virtuaalikonepalvelin Bokxia, kuvan 1 mukaisesti.



Kuva 1. Virtuaalinen Graylog-ympäristö.

Helpoin tapa asentaa Graylog on käyttää valmista OVA-imagea, joka löytyy Graylogin sivulta. OVA voidaan avata esimerkiksi VMware- tai Virtualbox:illa.



Kuva 2. Virtuaalisen Graylog koneen asetukset VMware:ssa.

Käyttöjärjestelmänä toimii Ubuntu Linux (64-bit). Peruskonfiguraatio jolla luodaan käyttäjä sekä asetetaan aikavyöhyke, on seuraava:

```
sudo graylog-ctl set-email-config <smtp server> [--port=<smtp port> --
user=<username> --password=<password>]
sudo graylog-ctl set-admin-password <password>
sudo graylog-ctl set-timezone <zone acronym>
sudo graylog-ctl reconfigure
```

Käyttäessä WMware:a hostina tarvitaan vielä WMware toolsit, jotka saadaan komennolla:

```
sudo apt-get install -y open-vm-tools
```

Kun kaikki on valmista, voidaan käynnistää virtuaalikone, josta saadaan seuraava näkymä:

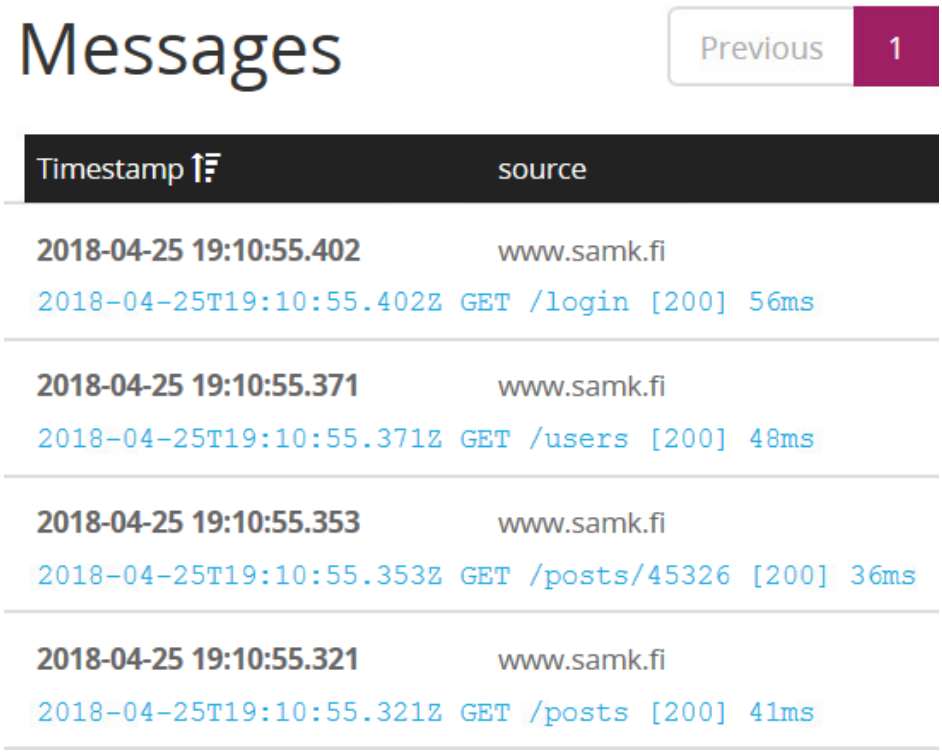
(Kuva 3. Graylog-server käyttövalmiina.)

Graylog on nyt käyttövalmis tunnuksilla admin/admin.

3 VIESTINTÄ

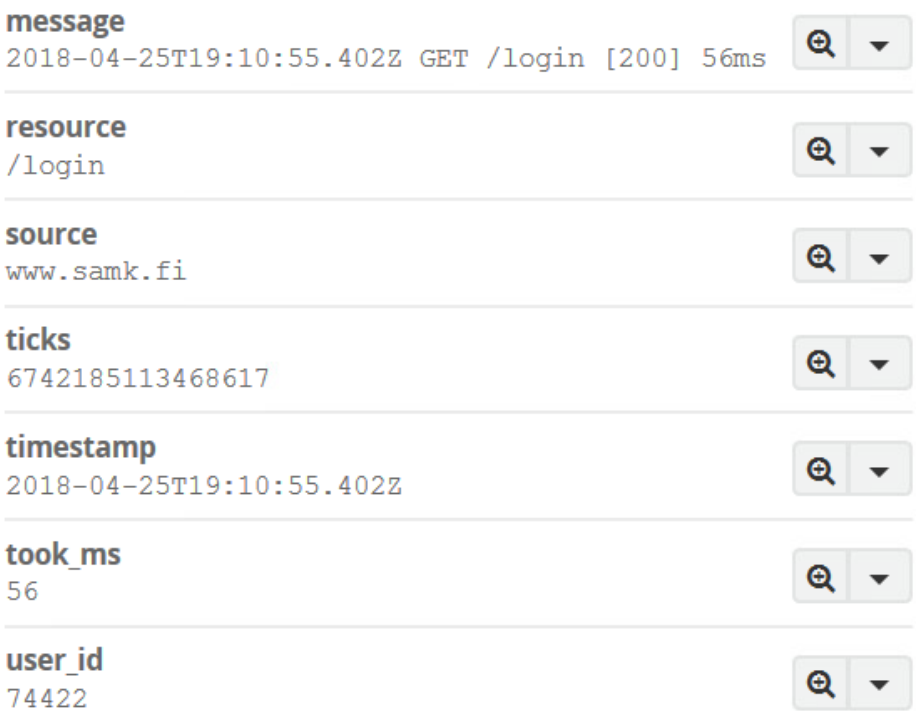
3.1 Lokitiedostot

Lokitiedosto on tiedosto, joka pitää tapahtumien, prosessien, viestien ja viestinnän rekisterin eri kommunikoivien ohjelmistosovellusten ja käyttöjärjestelmän välillä. Lokitiedostot ovat läsnä suoritettavassa ohjelmistossa, käyttöjärjestelmissä ja ohjelmissa, joiden avulla kaikki viestit ja prosessitiedot tallennetaan. Jokainen suoritettava tiedosto tuottaa lokitiedoston, jossa kaikki toiminnot on merkitty.



Kuva 4. Loki-viestejä Graylog-sovelluksessa lähteestä www.samk.fi.

Yleisimmin käytetty loki-standardi on syslog, joka on lyhennetty sanoista "system log". Ohjelmistoilla on oma ennalta määritetty lokitiedosto, eikä se useimmiten näy yleisessä järjestelmän lokissa tai käyttöjärjestelmän tapahtumalokissa. Syslog tuottaa automaattisesti aikaleimaisen dokumentaation järjestelmän prosessien suorituksesta ja tilasta, kuten Internet Engineering Task Force (IETF) RFC 5424: ssa määritellään. Lokitiedostojen lokiviestit voidaan tallentaa ja analysoida myöhemmin myös sen jälkeen, kun ohjelma on suljettu.



Kuva 5. Loki-viestin /login yksityiskohtia Graylog-sovelluksessa.

Sovellus sisältää yleensä koodin kirjoittamaan erilaisia tapahtumatietoja sovelluslokitiedostoon. Lokitiedosto voi paljastaa viestivirtaongelmia ja sovellusongelmia. Se voi myös sisältää tietoja käytetyistä käyttäjä- ja järjestelmätoimista. Kirjattuihin tapahtumiin kuuluu:

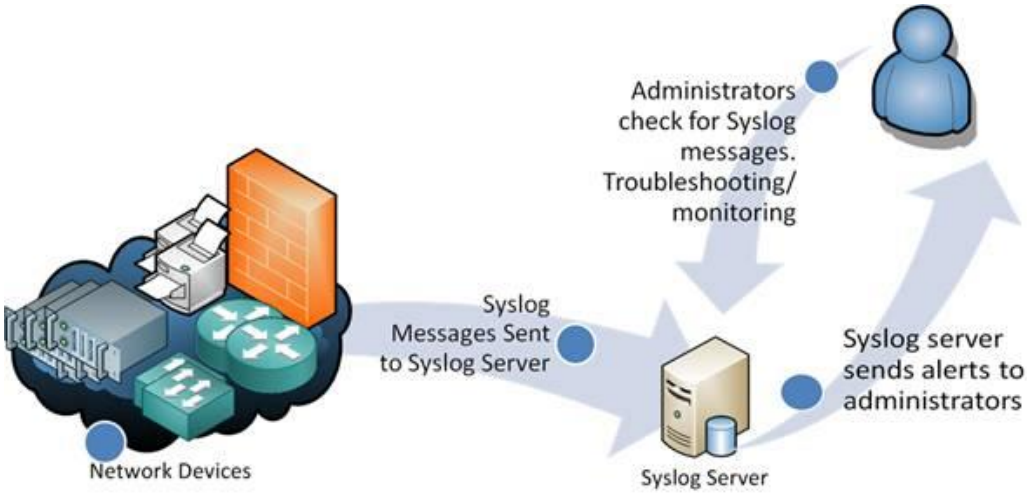
- Varoitukset alhaisesta levytilasta
- Toimenpide, joka on suoritettu
- Kaikki merkittävät ongelmat - jotka tunnetaan virhetilanteena - estävät sovelluksen käynnistämisen
- Menestystarkastus, joka ilmaisee tietoturvatapahtuman, kuten onnistuneen kirjautumisen
- Vikatarkistus ilmoittaa tapahtumat, kuten kirjautumisvian

Event log eli tapahtumaloki on perusresurssi, joka auttaa tarjoamaan tietoa verkkoliikenteestä, käyttötavoista ja muista olosuhteista kuten esimerkiksi se voi kaapata kaikki kirjautumiset verkkoon sekä tilien lukkiutumiset, epäonnistuneet salasanasyötöt jne. Se voi myös tallentaa erilaisia sovelluskohtaisia tapahtumia, kuten sovellusvirheitä, sulkemisia tai muita niihin liittyviä tapahtumia. Tapahtumaloki tallentaa nämä tiedot

tietoturva-alan ammattilaisille tai automaattisiin turvajärjestelmiin, jotta verkonvalvojat voivat hallita erilaisia näkökohtia, kuten turvallisuutta, suorituskykyä ja avoimuutta. [1.]

3.1.1 Syslog

Syslog on tapa, jolla verkkolaitteet lähettävät tapahtumaviestejä lokiin, joka tunnetaan tavallisesti Syslog-palvelimena. Syslog-protokollaa tukee laaja valikoima laitteita ja sitä voidaan käyttää erilaisten tapahtumien kirjaamiseen. Esimerkiksi reititin voi lähettää viestejä käyttäjistä, jotka kirjautuvat konsoli-istuntoihin, kun taas verkkopalvelin voi kirjata käyttöoikeuksien puuttumisesta johtuvia virhesanomia. Lyhyesti sanottuna Syslog lähettää viestejä keskeiseen paikkaan, kun tiettyjä tapahtumia laukaistaan.



Kuva 6. Syslog-serverin rooli syslog-viestiketjussa. [2.]

Useimmat verkkolaitteet, kuten reitittimet ja kytkimet, voivat lähettää Syslog-viestejä. Useimmat palomuurit, jotkut tulostimet ja jopa web-palvelimet, kuten Apache mahdollistavat myös Syslog-tietojen tuottamisen. Windows-pohjaiset palvelimet eivät tue Syslogia luonnollisesti, mutta useat kolmannen osapuolen työkalut helpottavat Windows Event Login tai IIS-tietojen keräämistä ja toimittavat sen Syslog-palvelimelle.

Syslog-viestit sisältävät yleensä tietoja, joiden avulla voidaan tunnistaa perustiedot siitä, missä, milloin ja miksi loki lähetettiin: IP-osoite, aikaleima ja todellinen lokiviesti. Viestit ovat usein ihmisen luettavassa muodossa, mutta ei aina.

Syslog käyttää konseptia nimeltä "facility" jolla tunnistetaan viestin lähde millä tahansa laitteella. Esimerkiksi "0" - olisi ydinviesti, ja "11" - olisi FTP-viesti. Tämä on peräisin Syslogin UNIX-juurista. Useimmat Cisco-verkkolaitteet käyttävät "Local6" tai "Local7" -palvelukoodeja.

Syslog-viesteillä on myös vakavuusaste kenttä. Vakavuusaste osoittaa kuinka tärkeä viesti on. "0": n vakavuus on hätätilanne, "1" on hälytys, joka tarvitsee välitöntä toimintaa ja asteikko jatkuu aina "6" ja "7" - informaatio- ja vianmääritysviestejä varten. [3.]

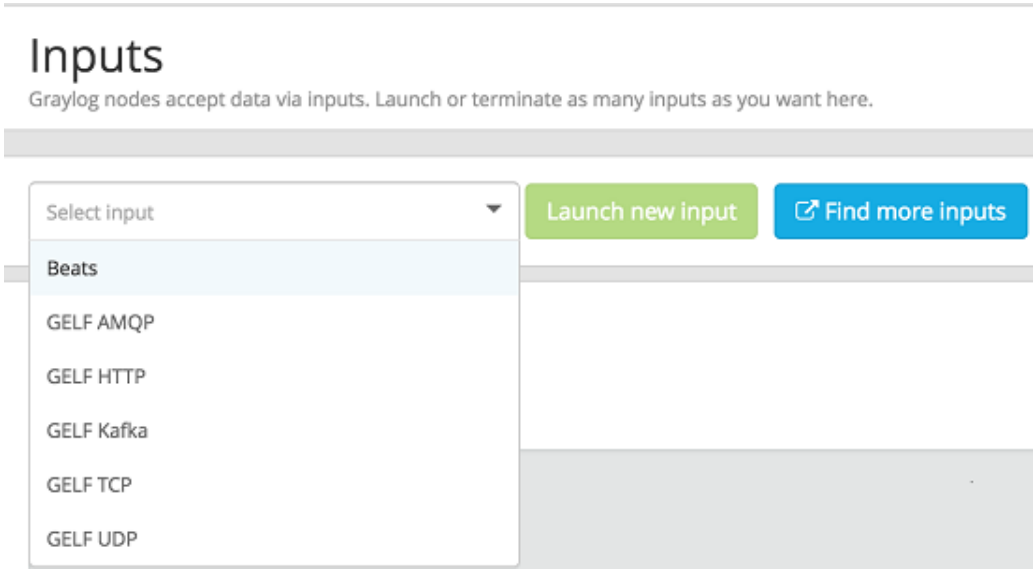
Syslog Severity Level

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

Kuva 7. Syslog-viestien vakavuusasteet 0-7.

3.1.2 GELF

Graylog Extended Log Format lyhyenä GELF on lokiformaatti, joka on suunniteltu välttämään syslogissa ilmeneviä ongelmia ja puutteita. Suurimpia syslogin puutteita joita haluttiin parantaa ovat sen rajattu 1024 tavun pituus, data tyyppien rajallinen määrittely, erilaisten syslog murteiden liiallinen määrä sekä lokitiedostojen kompressoinnin puuttuminen.



Kuva 8. GELF sisääntulot Graylog sovelluksessa.

Syslog on hyvä formaatti koneiden ja verkkolaitteiden järjestelmä viestien hallintaan. GELF on erittäin hyvä valinta sovellusten lokitiedostojen ylläpitoon. Kaikki poikkeukset voidaan lähettää lokiviesteinä Graylogiin, eikä tarvitse välittää aikakatkaisuista tai verkkoyhteys ongelmista koska GELF viestit voidaan lähettää UDP:n kautta.

UDP eli User Datagram Protocol datagrammit ovat yleensä rajattuja 8192 tavuun. Yhteen datagrammiin mahtuu paljon kompressoitua informaatiota mutta joskus halutaan lähettää vielä enemmän. Tämän vuoksi Graylog tukee paloiteltua GELF: iä.

Paloiteltuja viestejä voidaan määrittää antamalla GELF-viesteille tavuylätunniste, joka sisältää viestitunnuksen sekä jaksonumeron, joiden avulla viesti voidaan koota myöhemmin uudelleen.

Suurin osa GELF kirjastoista tukee paloiteltuja viestejä läpinäkyvästi ja havaitsee jos viesti on liian suuri eikä sitä voida lähettää yhdessä datagrammissa.

Esimerkki GELF viesti:

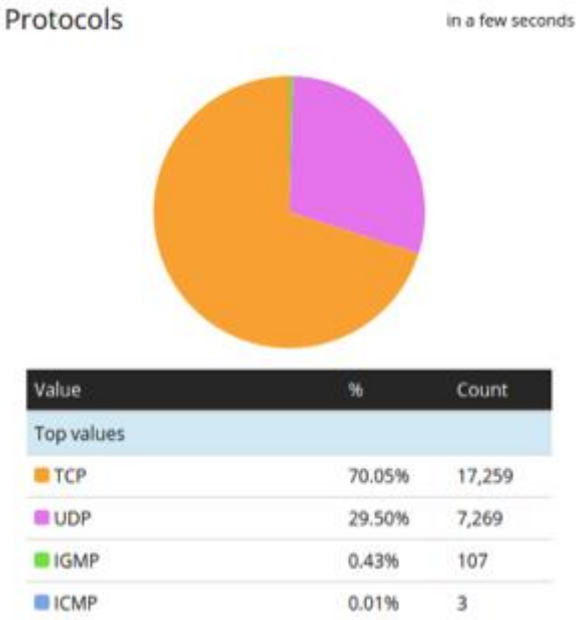
```
{
`short_message´ : `Something went wrong´,
`host´ : `www.samk.fi´.
`severity´ : 2,
`facility´ : `some subsystem´,
`full_message´ : `Stacktrace and stuff´,
`file´ : `some_controller.rb´,
`line´ : 8,
`_from_load_balancer´ : `lb-3´,
`_user_id´ : 9001,
`_http_response_code´ : 500
}
```

Myös TCP eli Transmission Control Protocol ratkaisisi tämän viestien kokoon liittyvän ongelman mutta sen käyttö toisi mukanaan muita ongelmia kuten hitaat yhteydet, aikakatkaisut sekä muita ikäviä verkkoon liittyviä ongelmia. UDP voi mahdollisesti hukata viestin, kun taas TCP voi kaataa koko ohjelmiston, jos sitä ei ole suunniteltu huolella. Mutta molemmilla on käyttötarkoituksensa. TCP on järkevä ratkaisu, kun puhutaan erittäin suurista viesti määristä. Monet GELF kirjastot tukevat molempia TCP:tä ja UDP:tä kulkuväylänä, jotkut myös jopa HTTP:tä. [4.]

3.2 Verkkoprotokollat

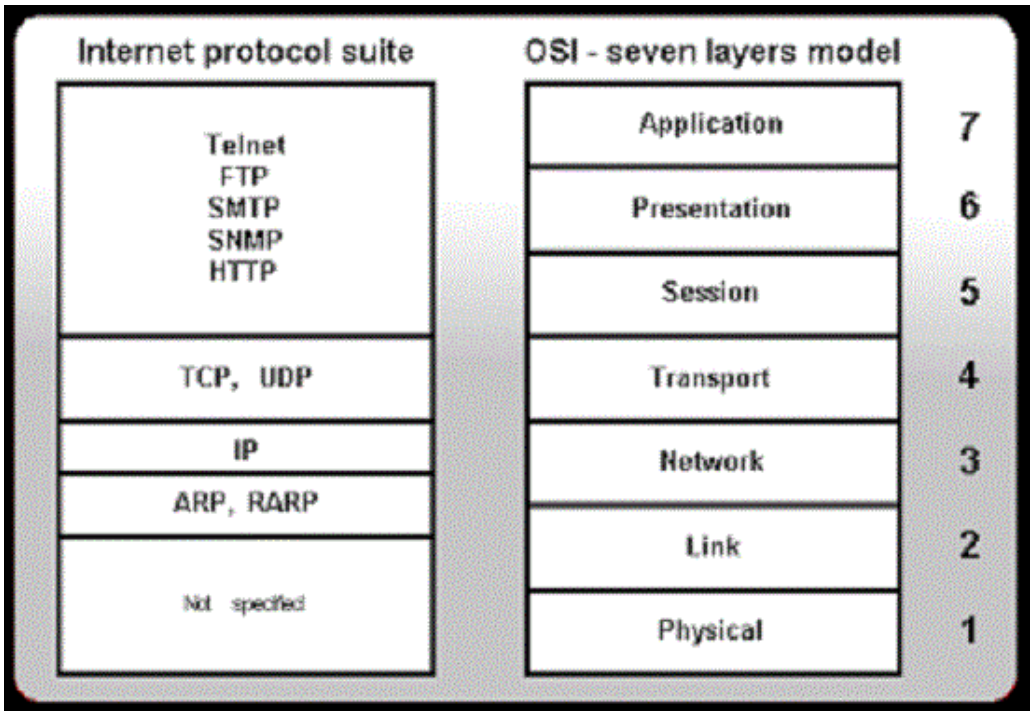
Verkkoprotokolla määrittää säännöt ja yleissopimukset verkkolaitteiden väliselle viestinnälle. Nämä protokollat sisältävät mekanismeja laitteille, joilla tunnistetaan ja tehdään yhteyksiä toisiinsa, sekä muotoilusääntöjä, jotka määrittävät, miten tiedot pakataan lähetettyihin ja vastaanotettuihin viesteihin. Jotkin protokollat tukevat myös viestien tunnistamista ja tietojen pakkaamista, jotka on suunniteltu luotettavaan ja/tai suorituskykyiseen verkkoviestintään.

Modernit protokollat tietokoneverkossa käyttävät yleensä pakettikytkentätekniikoita viestien lähettämiseen ja vastaanottamiseen pakettien muodossa - viestejä, jotka on jaettu osioihin, jotka kerätään ja kootaan uudelleen määränpäähänsä. Satoja erilaisia tietokoneverkkoprotokollia on kehitetty eri tarkoituksiin ja ympäristöihin.



Kuva 9. Verkkoprotokollat järjestyksessä käyttömäärän perusteella Graylogissa.

Internet Protocol -perhe sisältää joukon niihin liittyviä (ja useimmin käytettyjä verkkoprotokollia.) Internet-protokollan (IP) lisäksi korkeamman tason protokollat, kuten TCP, UDP, HTTP ja FTP, integroivat IP: hen lisäominaisuuksien tarjoamiseksi. Yleensä IP-perheen korkeamman tason protokollat toimivat läheisemmin sovellusten kuten Web-selainten kanssa, kun taas alemman tason protokollat, kuten ARP ja ICMP, toimivat vuorovaikutuksessa verkkolaitteiden ja muun tietokonelaitteiston kanssa. [5.]



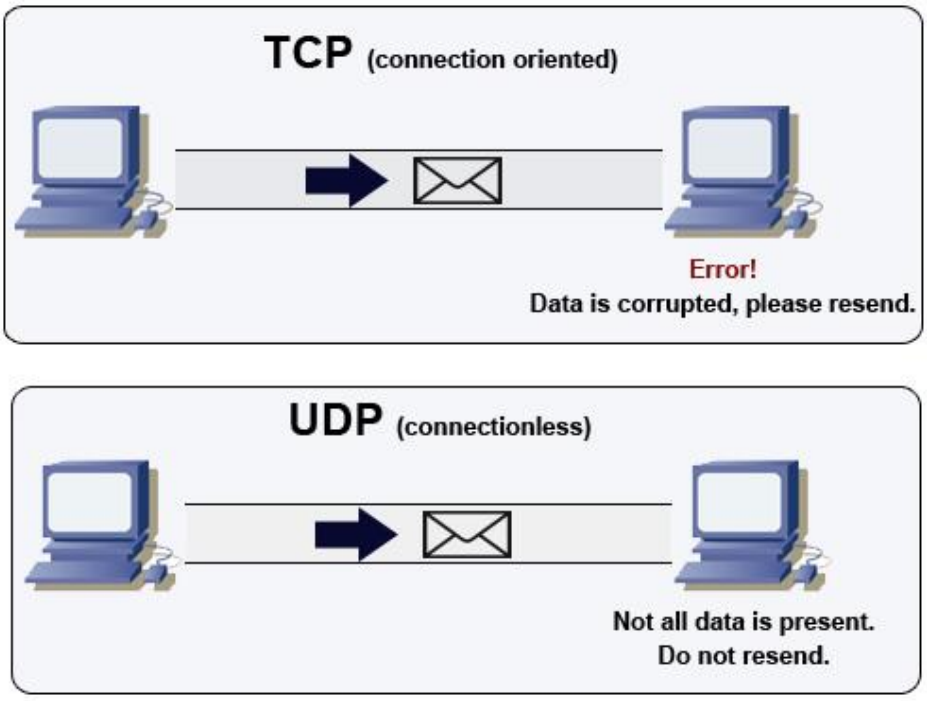
Kuva 10. Verkkoprotokollat järjestyksessä OSI-mallin mukaan. [6.]

3.2.1 UDP

User Datagram Protocol (UDP) otettiin käyttöön vuonna 1980 ja on yksi vanhimmista olemassa olevista verkkoprotokollista. Se on yksinkertainen OSI-mallin kuljetusprotokolla asiakas ja palvelinverkkosovelluksiin. UDP perustuu Internet Protocol (IP) -perheeseen ja on TCP: n tärkein vaihtoehto.

UDP: n lyhyt selitys voisi olla, että se on epäluotettava protokolla. Vaikka tämä on osittain totta, koska tiedonsiirroissa ei ole virhetarkistuksia tai korjauksia, on myös totta, että tälle protokollalle on käyttötarpeita joihin muut protokollat eivät voi vastata.

UDP: tä (jota kutsutaan joskus UDP / IP: ksi) käytetään usein videoneuvotteluissa tai tietokonepeleissä, jotka vaativat nimenomaan reaaliaikaista suorituskykyä. Suorituskyvyn maksimoimiseksi protokolla mahdollistaa yksittäisten pakettien pudottamisen (ilman uusintoja) ja UDP-pakettien vastaanottamisen eri järjestyksessä kuin lähetettiin, sovelluksen määrittelemällä tavalla.

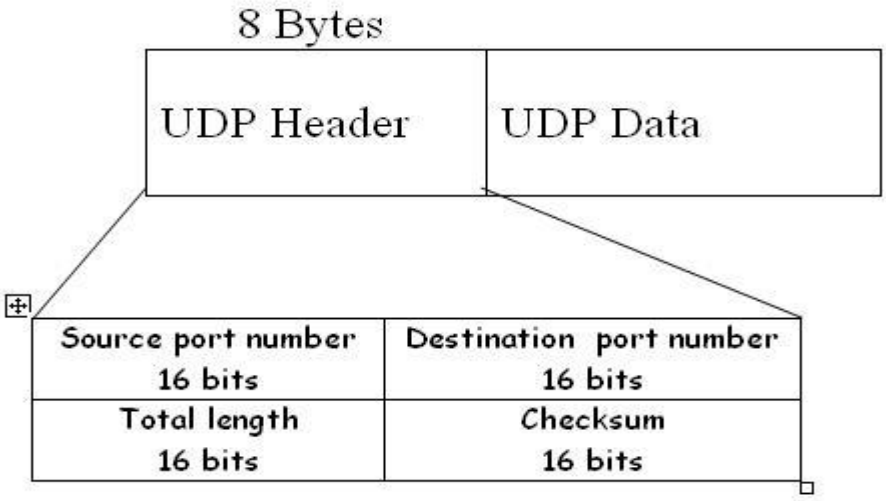


Kuva 11. TCP:n ja UDP:n oleellinen ero. [7.]

Tämä lähetystapa mahdollistaa vähemmän datan ylivuotoa ja viivästyksiä, koska paketit lähetetään joka tapauksessa ja ilman virhetarkistuksia. Tämän vuoksi UDP vaatii vähemmän kaistanleveyttä kuin TCP.

UDP-liikenne toimii ns. Datagrammien kautta, ja jokainen datagrammi koostuu yhdestä sanomayksiköstä. Otsikko (header) tallennetaan ensimmäisiin kahdeksaan tavuun, mutta loppuosa on se, mikä pitää sisällään todellisen viestin. Jokainen seuraavaksi lueteltu osa UDP datagrammin otsikkoa vastaa kahta tavua:

- Lähtöportin numero
- Kohdeportin numero
- Datagrammikoko
- Tarkistussumma



Kuva 12. UDP-datagrammin otsikon koostumus. [8.]

UDP-datagrammin koko on otsikon ja datan osissa olevien tavujen kokonaismäärä. Datagrammien koko vaihtelee käyttöympäristön mukaan, mutta korkeintaan 65535 tavua.

UDP-tarkistussummat suojaavat viestitietoja väärentämiseltä. Tarkistussumma-arvo edustaa datagrammin sisältyvän datan koodausta, kun se on laskettu ensin lähettäjän ja myöhemmin vastaanottajan toimesta. Jos yksittäinen datagrammi vioittuu tai korruptoituu lähetyksen aikana, UDP-protokolla havaitsee muutoksen tarkistussummassa. [9.]

3.2.2 TCP

TCP (Transmission Control Protocol) on tärkeä verkkoprotokolla, jota käytetään tiedonsiirtoon verkon kautta. TCP toimii yhdessä IP-protokollan (Internet Protocol) kanssa ja kaksikko tunnetaan nimellä TCP/IP.

TCP: n tehtävänä on hallita tietojen siirtoa niin, että se on luotettava. Luotettavassa tiedonsiirrossa seuraavat vaatimukset täyttyvät:

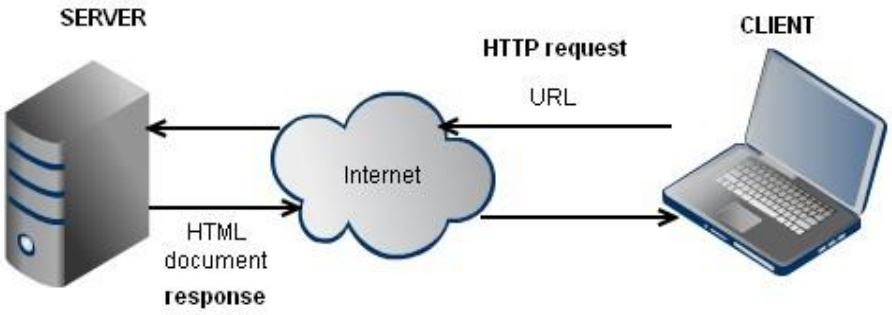
- Kaikki paketit saapuvat kohteeseen, eli mikään paketti ei katoa.
- Ei ole sellaista viivettä, joka vaikuttaisi datan laatuun.
- Kaikki datapaketit kootaan uudelleen järjestyksessä.

TCP merkitsee paketit siten, että ne on numeroitu. Se myös varmistaa, että niillä on määräaika päästä kohteeseen (joka on kestoltaan useita satoja millisekunteja kutsuttu aikakatkaisu). Jokaisesta vastaanotetusta paketista lähettävälle laitteelle ilmoitetaan lähettämällä kuittaus paketti. Jos aikarajan jälkeen ei vastaanoteta kuittausta, lähde lähettää toisen kopion, luultavasti puuttuvasta tai viivästyneestä paketista.

Tilauksen ulkopuolisia paketteja ei myöskään tunneta. Tällä tavoin kaikki paketit on aina koottu järjestykseen ennalta määritetyn ja hyväksyttävän viiveen sisällä. [10.]

3.2.3 HTTP

Hypertext Transfer Protocol (HTTP) on protokolla hypermedia-asiakirjojen, kuten HTML:n lähettämiseen. Se on suunniteltu kommunikoimaan verkkoselainten ja web-palvelimien välillä, mutta sitä voidaan käyttää myös muihin tarkoituksiin. HTTP seuraa klassista client-server mallia, sovellus avaa yhteyden pyynnön tekemiseen ja odottaa, kunnes se saa vastauksen.



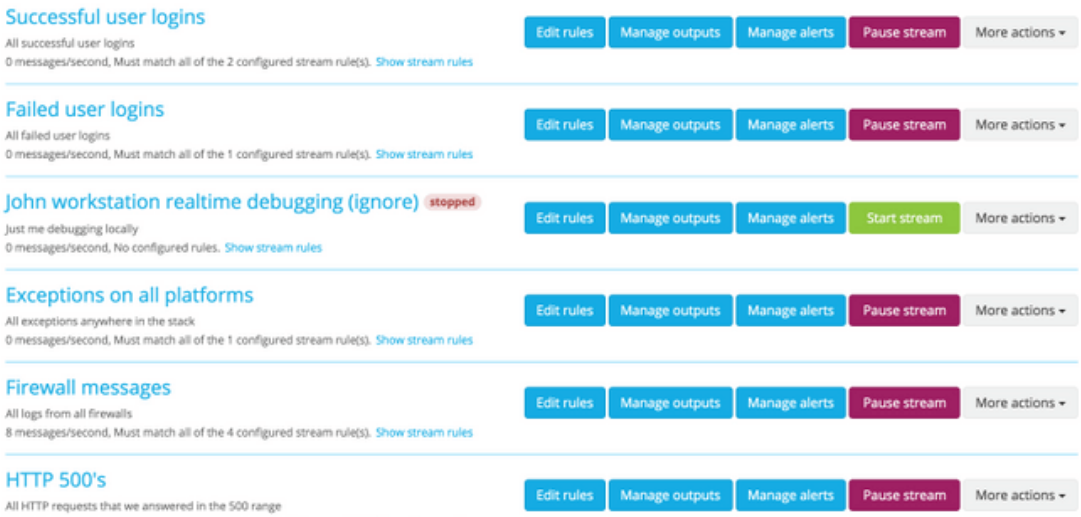
Kuva 13. HTTP-liikenne käyttäjän ja palvelimen välillä. [11.]

HTTP on stateless protokolla, eli palvelin ei pidä mitään dataa (tilaa) kahden pyynnön välillä. Vaikka se perustuu usein TCP / IP-kerrokseen, sitä voidaan käyttää millä tahansa luotettavalla siirtokerroksella; eli protokollaa, joka ei kadota viestejä äänettömästi, kuten UDP. [12.]

4 KÄYTTÖ

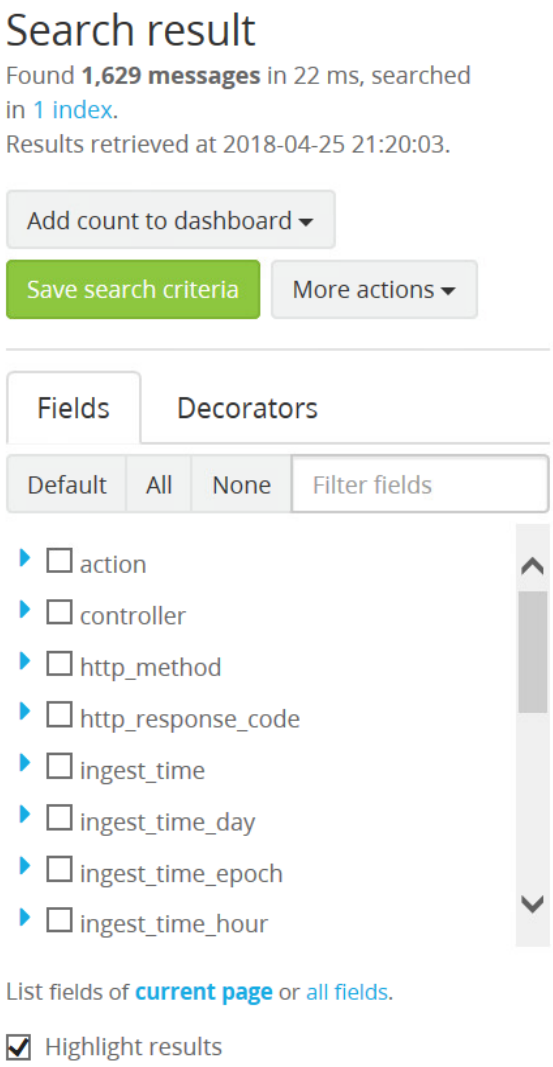
4.1 Käyttötavat

Graylog mahdollistaa lokitiedostojen helpon parsimisen ja hallitsemisen mistä tahansa tietolähteestä. Se on myös yhteensopiva kolmannen-osapuolen tiedonkeräämis- ohjelmien kuten beats, fluentd ja nxlog:in kanssa. Verkko-käyttöliittymän työkalut tarjoavat helpon tavan viestien varastointiin, mustalistaukseen ja muokkaukseen reaaliajassa, kun ne saapuvat Graylogiin.



Kuva 14. Esimerkki viestivirtoja Graylog sovelluksessa.

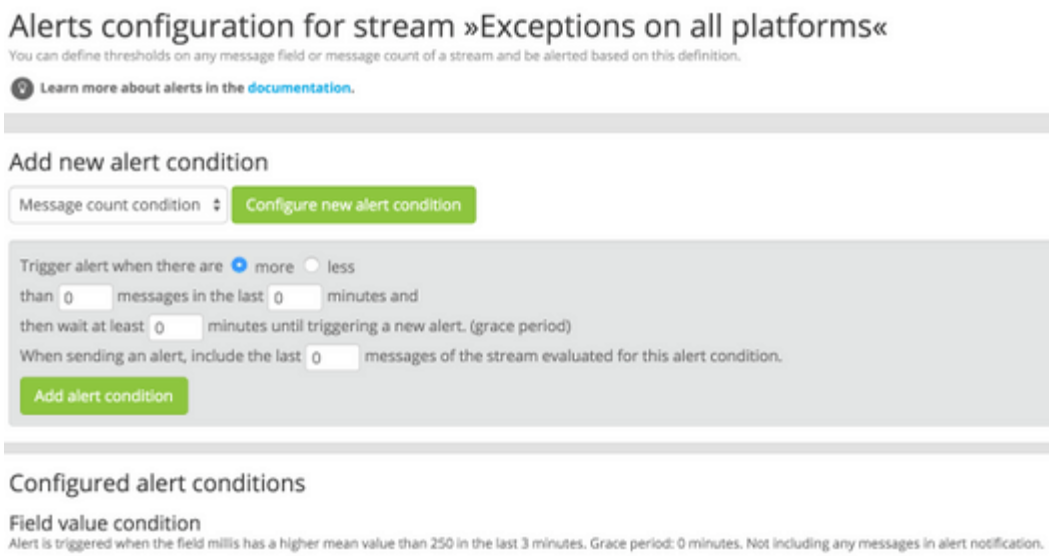
Monipuolinen hakutyökalu helpottaa lokitiedostojen hakemista massan joukosta tarkkojen ja yksinkertaisten hakusyntaksien avulla. Suosikkihakukyselyt voi myös tallentaa.



Kuva 15. Graylog sovelluksen hakutyökalu.

Luomalla erilaisia ”dashboardeja” voi helposti visualisoida ja seurata tapahtumia yhdestä keskisestä sijainnista. Tarjolla on kenttätilastoja, nopeita arvoja ja kaavioita tietojen tarkempaan analysointiin suoraan hakutulossivulta.

Graylog antaa käyttäjän luoda erilaisia hälytyksiä ja ilmoituksia, kun jotain tärkeää tapahtuu, esimerkiksi epäonnistuneita kirjautumisyrityksiä, poikkeuksia tai suorituskyvyn heikkenemistä.



Kuva 16. Graylog sovelluksen työkalu hälytysten luomiseen.

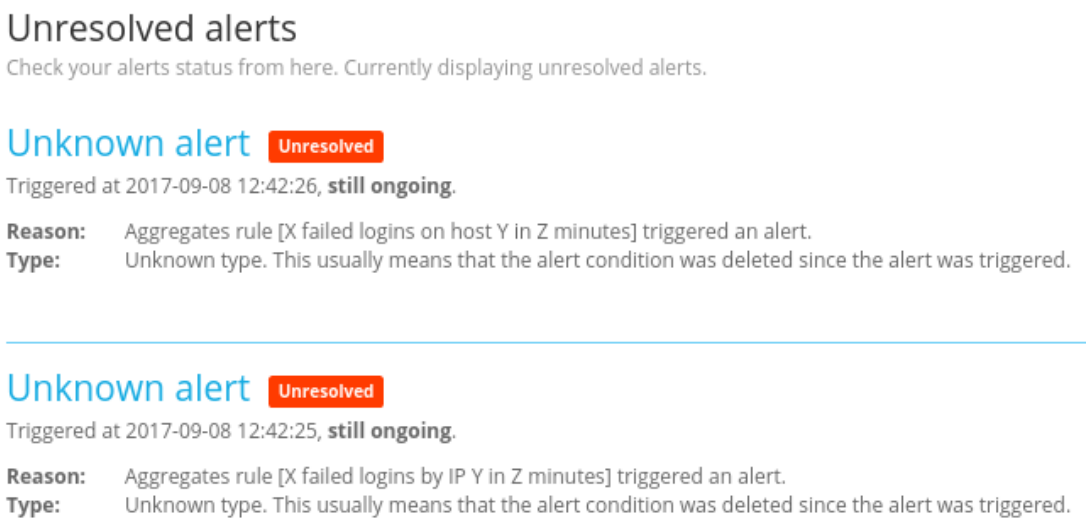
4.2 Hälytykset

Hälytykset perustuvat aina viestivirtoihin. Graylogilla voi määrittää häiriöitä aiheuttavat ehdot. Esimerkiksi aina, kun viestivirran poikkeukset sisältävät yli 50 viestiä minuutissa tai kun keskimääräinen poikkeama aika on liian korkea.

Graylog-hälytykset ovat säännöllisiä hakuja, jotka voivat aiheuttaa joitain ilmoituksia, kun määritelty ehto täyttyy. Hälytyksillä on kaksi mahdollista tilaa:

Ratkaisematon
Hälytyksillä on ratkaisematon tila, kun määritelty ehto täyttyy. Uudet hälytykset näkyvät tässä tilassa. Ne näyttävät myös viestivirtaan liittyvät ilmoitukset. Tässä tilassa olevat hälytykset vaativat yleensä toimia käyttäjältä.

Ratkaistu
Graylog ratkaisee automaattisesti hälytykset, kun niiden hälytysolosuhteet eivät enää täyty. Tämä on hälytyksen lopullinen tila, koska Graylog luo uuden hälytyksen, jos hälytystila täyttyy uudelleen tulevaisuudessa. Kun hälytys on ratkaistu, Graylog soveltaa hälytystilanteessa määritettyä odotusaikaa, ennen kuin luo uuden hälytyksen tähän hälytystilaan.



Kuva 17. Ratkaisemattomia hälytyksiä Graylog sovelluksessa.

4.3 Turvallisuus

Graylog on alusta asti rakennettu lokien hallintajärjestelmä nopeaan interaktiiviseen lokien-analysointiin, jonka avulla voidaan tallentaa lokeja kaikista palvelimista, sovelluksista ja verkkolaitteista. Kehittyneillä näkymillä ja hallintapaneeleilla on valmiiksi määritetyt liitännät, jotka parantavat tilannetietoisuutta ja auttavat vastaamaan tapahtumiin.

Siirtyminen digitaaliseen liiketoimintaan vie organisaatiot tuottamaan, käyttämään ja tallentamaan paljon tietoa. Se myös kiihdyttää tiedon saannin tarvetta eli se muuttuu nopeammin kuin koskaan ennen. Enemmän tietoa voi tuoda enemmän yksityiskohtia asiakkaista, markkinoista ja mahdollisuuksista. Mutta enemmän dataa voi olla myös ongelma.

Perinteiset lähestymistavat riskien hallitsemiseksi kaiken tämän datan ympärillä ovat olleet sen seuranta erityisesti tarkastelemalla niitä lokitiedostoja, jota kaikki tietojenkäsittelyjärjestelmät luovat. Pitämällä silmällä lokeja voidaan helposti ja nopeasti havaita mahdolliset tietomurrot ennen kuin mitään todellista vahinkoa syntyy.

Lokitiedostot ovat edelleen turvallisuuden hallinnan parhaiden käytäntöjen ytimessä. Lokitiedostoihin sisältyvät tiedot voivat näyttää, kuka tekee mitä ja milloin ja missä he tekevät sen. Mutta ennen kuin voidaan saada hyvä käsitys siitä, mitä tapahtuu koko IT-ympäristössä, on saatava kaikki tapahtumatiedot yhteen helposti hallittavaan paikkaan.

Vaikka mikään yksittäinen tietoturvateknologia ei voi ratkaista kaikkia ongelmia, lokitiedostojen keskeinen rooli turvallisuus- ja riskienhallintatyökaluna on vielä tänä päivänäkin yhtä tärkeä kuin vuosikymmen sitten. [13.]

5 YHTEENVETO

Työn tavoitteena oli luoda virtuaalinen ympäristö, joka mahdollistaa Graylog-järjestelmän tutkimisen ja sen tarjoamien mahdollisuuksien kokeilemisen. Järjestelmän piti toimia kuten normaali lokitiedostojen valvonta ohjelmisto, joten se piti yhdistää verkkoon. Tällä järjestelmällä oli tarkoitus pystyä pitämään yksityiskohtaista lokia liikenteestä, tämän sisällöstä ja tyypistä sekä mahdollisesti tehostaa verkon toimintaa ja turvallisuutta. Bokxi osoittautui erittäin käteväksi ja helpoksi tavaksi luoda tämä virtuaaliympäristö.

Aikaa olisin voinut säästää työssäni käyttämällä heti alusta alkaen valmista OVA-tiedostoa Graylogin sivuilta. Aloitin Linux-palvelimen kokoamista tyhjästä, CentOS käyttöjärjestelmälle ilman merkittävää aikaisempaa kokemusta Linux-käyttöjärjestelmistä. Tämä osoittautui haastavaksi mutta tärkeäksi oppimisvaiheeksi, joka laajensi näkökantaani, tietoani sekä taitojani Linux-käyttöjärjestelmistä.

Työssäni tutkin Graylogin soveltuvuutta Satakunnan ammattikorkeakoulun lokitiedostojen valvontatarpeisiin. Mielestäni Graylog on erinomainen sovellus keskitettyyn lokitiedostojen hallintaan ja analysointiin, sen yksinkertaisen ja käyttäjäystävällisen käyttöliittymän takia. Olen myös sitä mieltä, että verkon selkeyttäminen ja turvallisuuden parantaminen on mahdollista Graylogin laajojen työkalujen avulla.

LÄHTEET

[1] Techopedia. Viitattu 20.3.2018. https://www.techopedia.com/definition/5445/log-file

[2] Aaron Leskiw. Viitattu 6.5.2018. www.networkmanagementsoftware.com/what-is-syslog/

[3] Aaron Leskiw. Viitattu 10.4.2018. https://www.networkmanagementsoft-ware.com/what-is-syslog/

[4] Graylog. Viitattu 20.3.2018. http://docs.graylog.org/en/2.4/pages/gelf.html

[5] Bradley Mitchell. Viitattu 21.3.2018. https://www.lifewire.com/definition-of-pro-tocol-network-817949

[6] Rohit Verma. Viitattu 6.5.2018. http://techietechieblog.blogspot.fi/2012/03/inter-net-protocols.html

[7] Viitattu 7.5.2018. http://cs-pages.blogspot.fi/2011/10/compare-and-contrast-ad-vantages-and.html

[8] Viitattu 7.5.2018

https://en.wikibooks.org/wiki/Communication_Net-

works/TCP_and_UDP_Protocols/UDP

[9] Bradley Mitchell. Viitattu 21.3.2018. https://www.lifewire.com/user-datagram-protocol-817976

[10] Nadeem Unuth. Viitattu 24.3.2018. https://www.lifewire.com/tcp-transmission-control-protocol-3426736

[11] dsandesari. Viitattu 8.5.2018. https://github.com/dsandesari/http

[12] usatyal. Viitattu 9.4.2018. https://developer.mozilla.org/fi/docs/Web/HTTP

[13] Alyssa Fox. Viitattu 24.4.2018. https://www.graylog.org/post/the-data-explo-sion-and-its-effect-on-security