SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

SYSLOG-PALVELIN VERKON VALVOMISEN TUKENA

TEKIJÄ/T: Noora Heikkinen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Noora Heikkinen	
Työn nimi Syslog-palvelin verkon valvomisen tukena	
Päiväys 4.9.2014	Sivumäärä/Liitteet 32/2
Ohjaaja(t) tietohallintopäällikkö Matti Kuosmanen, lehtori Veijo Pitkänen	
Toimeksiantaja/Yhteistyökumppani(t) Savonia-ammattikorkeakoulu	

Tiivistelmä

Työ tehtiin Savonia-ammattikorkeakoulun Tietohallinnolle ja työn aiheena oli syslog-palvelin verkon valvomisen apuna. Syslog on tärkeä verkon hallinta työkalu, jota Savonian verkkoon ei vielä ole saatu pystytettyä.

Aihe oli tekijälle tuntematon, joten työ oli aloitettava tutustumalla huolellisesti syslogin toimintaan ja käyttöön. Teoriaosuudessa käydään läpi syslogin toiminta malli, viestien rakenne ja syslogin turvallisuus ja huonot puolet.

Testausvaiheessa oli valittava työkalut, joilla palvelimen ja koko syslog-systeemin saisi toimivaksi. Palvelimeksi valikoitui rsyslog, tietokannaksi MySQL ja Adiscon LogAnalyzer analysointia ja raportointia varten. Huomioon otettiin myös vaihtoehtoisia työkaluja, vaikka niiden testaamiseen ei aikaa riittänyt.
Ongelmat saatiin karsittua hyvin pois jo labratesteissä, joiden yhteydessä palvelimen käyttö tuli tutuksi. Tämän ansiosta oikeassa verkkoympäristössä testaaminen onnistui ilman suurempia ongelmia.

Avainsanat
syslog, verkonhallinta, palvelin

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Noora Heikkinen			
Title of Thesis Syslog Server Assisted Network Monitoring			
Date	September 4, 2014	Pages/Appendices	32/2
Supervisor(s) Mr. Matti Kuosmanen, Chief Information Officer Mr. Veijo Pitkänen, Lecturer			
Client Organisation /Partners Savonia University of Applied Sciences			

Abstract

This Thesis was made for Savonia University of Applied Sciences. The subject of this work was syslogserver assisted network monitoring. Syslog is a very useful tool for monitoring networks and there has not been a successful installation of a syslog server in Savonias netwok.

This work had to be started with getting to know the theory of syslog since the subject was unknown to the author. In this work the theory section includes the intended uses of syslog, its negatives and its security, how syslog messages are compiled and the functions of syslog.

In addition to telling about the tools that were used in making a functioning syslog system, there is also a section about alternative tools. The chosen server was rsyslog, MySQL was chosen for the database and for analyzing and reporting Adiscon LogAnalyzer. These chosen tools worked satisfyingly.

The testing in a real network environment worked almost without problems. The problems came when installing parts of the system, but they were successfully resolved before moving on to a real network.

Keywords
syslog, server, network administration

SISÄLTÖ

TERMIT JA LYHENTEET

MySQL	MySQL on relaatiotietokantaohjelmisto.
C	C on järjestelmä- ja sovellusohjelmointiin sopiva ohjelmointikieli.
C++	C-kieleen perustuva ohjelmointikieli.
LAMP	LAMP (Linux, Apache, MySQL, Perl/PHP/Python) on ohjelmistokokonaisuus, joista sen nimi koostuu. Yhdessä niistä voi muodostaa WWW-palvelimen.
Open Source	Ohjelman lähdekoodi on vapaasti käytettävissä.
TLS	TLS (Transport Layer Security) on protokolla, jolla voidaan kommunikoida verkossa turvallisesti.
TCP	TCP (Transmission Control Protocol) on protokolla, jolla voidaan kuljettaa tietoa verkossa niin että se on luotettavaa, virheetöntä ja oikeassa järjestyksessä.
UDP	UDP (User Datagram Protocol) on TCPn kaltainen protokolla. UDP kuljettaa tietoa verkossa, mutta se ei huolehdi tiedon perille pääsystä, sen virheettömyydestä tai järjestyksestä.
Cisco	Amerikkalainen yhtiö, joka valmistaa tietoverkko laitteita.
IETF	IETF (Internet Engineering Task Force) on avoin Internet standardien kehittäjä.
FQDN	FQDN (Fully Qualified Domain Name) verkkotunnus, joka määrittää tarkasti missä kohtaa Domain Name Systemiä tunnus on.
HTML	HTML (Hyper Text Markup Language) on tietokone kieli, jolla koodataan nettisivuja.
PDF	PDF (Portable Document Format) on tiedostomuoto, joka ei ole riippuvainen ohjelmasta, käyttöjärjestelmästä tai laitteistosta.
GNU GPL	GNU GPL (General Public License) on yleisesti käytetty vapaiden ohjelmistojen julkaisemislisenssi. Se antaa luvan käyttää, tutkia, jakaa ja muuttaa ohjelmaa vapaasti.
PostgreSQL	Tietokannanhallintajärjestelmä.

1 JOHDANTO

Tämä työ sai alkunsa Savonia-ammattikorkeakoulun tarpeesta saada toimiva syslog-palvelin. Toimiva syslog-systeemi on nykypäivänä tärkeä työkalu verkon ylläpitoon. Palvelinta oli yritetty pystyttää aikaisemminkin, mutta työ oli silloin jäänyt kesken. Työn teko oli aloitettava kokonaan alusta. Aihe oli myös tuntematon, joten ensimmäisenä vaiheena oli teorian opiskelu.

Työn tekemisessä oli melko vapaat kädet. Rajoitteeksi tuli vain, että käytettävien ohjelmien täytyy olla ilmaisia. Sen sijaan alustan, palvelimen ja muut systeemin osat oli tekijän päätettävissä.

Työssä kerrotaan esittelyjen jälkeen tarkasti syslogin toiminnasta. Sen käyttötarkoituksesta ja historiasta, viestin osista ja sen toiminnasta verkossa. Toiminta-osassa esitellään syslogin huonoja puolia ja käydään läpi sen turvallisuutta. Viestin osat kappaleessa käydään tarkasti läpi, mistä syslog-viesti koostuu. Toiminnasta käydään läpi syslogin kerrokset ja koko syslog-systeemin toiminta.

Työn tekemisestä kertovassa osassa on työkaluista ja niille harkituista vaihtoehdoista. Valitut työkalut toimivat tyydyttävästi, mutta vaihtoehtoja täytyi kuitenkin harkita. Kaikki valitut ja vaihtoehtoiset ohjelmat ovat alun perin sovitun mukaan ilmaisia.

Lopuksi on raportti testaamisesta ja palvelimen ja muiden systeemin osien pystyttämisestä. Asennus on raportoitu mahdollisimman tarkasti. Ajatuksena oli, että asennuksia pystyisi toistamaan helposti raportin pohjalta. Syslogin turvallisuuteen liittyvä tärkeä osa eli salaus jäi testauksesta pois.

2 SAVONIA

Savonia-ammattikorkeakoulu toimii Pohjois-Savon alueella ja yksiköitä sillä on Kuopion lisäksi Iisalmessa ja Varkaudessa. Opiskelija määrä on yli 6000 ja henkilökunnan määrä on yli 600. Savonian osaamisalueet ovat teknologia, ympäristö, hyvinvointi ja liiketoiminta.

Toimintaansa Savonia tarvitsee suuren ja hyvin toimivan tietoverkon. Reitittiminä on Juniperin-reitittimet, joita on kaksi. Palomuureina on kaksi Checkpoint-palomuuria. Reunakytkimiä on 35 kappaletta. Näiden lisäksi kaikilla kampuksilla on yhteensä 211 kytkintä ja yhteensä 111 WLAN-tukiasemaa.

Kytkimet ja tukiasemat ovat Cisco-merkkisiä. Kytkimet ovat 2960-sarjan X-, S- ja G-tyyppisiä. Osa niistä on stackattuja eli monta kytkintä toimii yhtenä kytkimenä, jolloin saadaan lisää portteja. Tukiasemat ovat Ciscon 1300-sarjaa.

3 SYSLOG

Syslogia alettiin kehittää jo 1980-luvulla Eric Allmanin toimesta. Syslog syntyi alun perin vain apuvälineeksi Sendmail projektiin, mutta kun se huomattiin hyödylliseksi muuallakin, sen käyttö alkoi levitä. Nykyään IETF on standardisoinut sen. (Wikipedia Syslog 2014.)

Syslog on client/server-protokolla. Tämä protokolla onkin nykyajan tietoverkkojen yksi keskeisimmistä malleista. Sen perimmäinen idea on, että asiakaslaite lähettää pyynnön palvelimelle. Palvelin täyttää pyynnön eli esimerkiksi etsii tietoja, joita on pyydetty ja lähettää ne sitten asiakaslaitteelle, jolta pyyntö alun perin tuli. Syslog palvelimen tapauksessa verkkolaitteita on asennettu lähettämään tietoja palvelimelle. Palvelin ottaa tiedot vastaan, laittaa ne tietokantaan ja tarpeen vaatiessa laatii raportin ja ilmoituksen verkon hallinnoijalle. Voisi myös sanoa, että syslog on standardi, joka yhdistää verkon hallintaan tarvittavia ohjelmia. Eli ohjelman, joka luo viestit, tietokannan, johon tiedot tallennetaan ja ohjelman, joka analysoi ja raportoi niistä. (TechTarget 2008.)

Syslog on yhteenkäyvä monien laitteiden ja käyttöjärjestelmien kanssa, vaikka se on standardi lokien hallinta malli Unix-systeemille. Esimerkiksi Windows-laitteet eivät oletuksena ole kykeneviä syslog viestien luontiin ja lähettämiseen. Kolmannet osapuolet ovat kuitenkin kehittäneet sovelluksia, joilla myös Windows-laitteet saadaan käyttämään syslogia. Verkkolaitteissa kyky syslog viestien lähettämiseen oletuksena on nykyään jo yleistä. Varsinkin monet kytkimet ja reitittimet osaavat luoda ja lähettää syslog viestejä. Myös jotkin palvelimet, palomuurit ja tulostimet osaavat tämän. (Leskiw, A. 2014.)

3.1 Syslogin käyttötarkoitus

Syslog-palvelin on työkalu verkon ylläpitoon. Tarkemmin sanoen se auttaa verkkolaitteiden lokitietojen ylläpidossa. Sillä voidaan integroida lokitietoa monista systeemeistä yhteen paikkaan. Näitä tietoja on paljon helpompi käyttää hyväksi kun ne ovat yhdessä paikassa. Tietoja voidaan käyttää reaaliajassa tai myöhemmin. Syslogin ansiosta verkonylläpitäjä voi myös ennustaa missä paikoissa verkossa voi ilmetä ongelmia tulevaisuudessa.

Nykyajan verkoissa kulkee niin suuri määrä viestejä, ettei verkonylläpitäjällä ole mitään mahdollisuuksia lukea niistä jokaista. Tässä syslog siis tulee avuksi, mutta sekään ei osaa tehdä asioita automaattisesti. On siis hyvä miettiä, kuinka ohjaa palvelimen keräämään viestejä ja milloin ja mistä asioista haluaa sen raportoivan. Tässä on myös mietittävä millaista tietokantaa, hallintatyökalua ja event manageria palvelin käyttää.

Tietokantojen avulla voidaan esimerkiksi pitää silmällä viallisia osoittajia ja suorituskyvyn alenemista, kuten tuulettimien ja virtalähteiden vajaatoimintaa. Reitittimet voivat lähettää tiedon muutetusta asennuksesta tai liitäntöjen tilojen muutoksista.

Palvelin on myös hyödyksi jos verkkolaite sammuu tai menee rikki, sen tiedot ovat tallessa palvelimella ja vikaa voidaan mahdollisesti tutkia.

Palvelin auttaa myös tietoturvaan. Jos joku pääsee murtautumaan verkkolaitteeseen, hänen on helppo pyyhkiä jälkensä laitteesta. Jos murtoon viittavasta toiminnasta on kuitenkin lähtenyt viesti syslog palvelimelle, jälkien sieltä pyyhkiminen on vaikeampaa. Näistä jäljistä voidaan hyötyä. Niitä

voidaan käyttää tietoturvan parantamiseen, mutta myös murrosta aiheituneiden vahinkojen korjaamiseen. (Cisco Press 2005.)

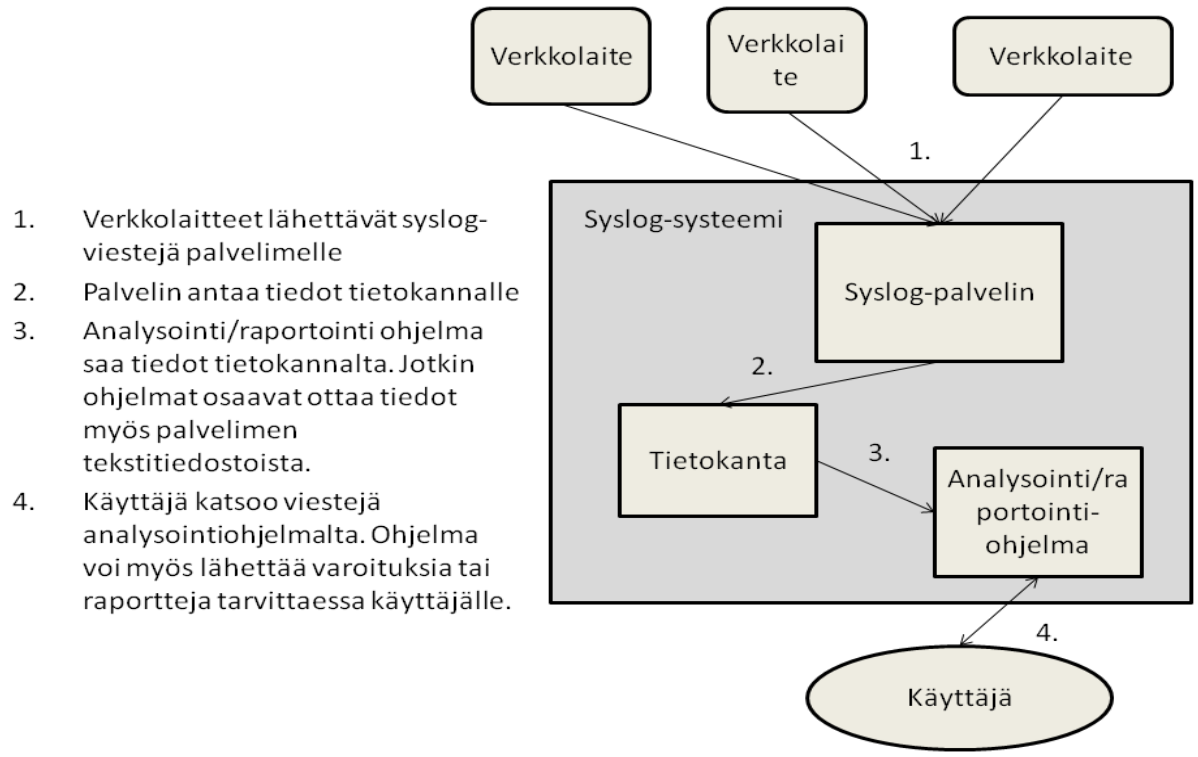
3.2 Syslogin toiminta

Syslog-tekniikalla voidaan laittaa laite lähettämään viestejä valituista tapahtumista palvelimelle. Tällaisia tapahtumia voi esimerkiksi olla kirjautumiset laitteelle tai virheilmoitukset tai laitteen kaatuminen. Syslog-systeemillä näitä viestejä lähetetään vain silloin, kun määrätty tapahtuma tapahtuu. Toisin kuin jotkin muut systeeminvalvonta ja hallinta työkalut, syslog ei lähetä mitään kyselyjä toisille laitteille.(Leskiw, A. 2014.)

Syslog lähettäjä laite lähettää pienen viestin, tämän paketin koko on alle 1 KB. Syslog vastaanottaja on yleensä nimeltään ”syslogd”, ”Syslog daemon” tai ”syslog server”. Viestit ovat yleensä UDP:nä ja käyttävät tällöin porttia 514. UDP-viestit eivät lähetä varmistusta vastanotosta eli niiden perille pääsy ei ole taattua. Riippuen laitteesta ne saattavat joskus lähettää tiedot TCP:nä, jolloin viestin vastaanotosta tulee ilmoitus takaisin laitteelle. (Cisco Systems 2011.)

Syslog lähettäjä siis lähettää viestejä vastaanottajalle, vaikkei se tiedä ovatko edelliset viestit päässeet perille. Lähettäjä saattaa myös lähettää viestejä vaikka niille ei olisi vastaanottajaa. Tällaiset viestit usein vain katoavat verkkoon. (Cisco Systems 2011.)

Syslog-komponentteihin kuuluu myös kuuntelija eli prosessi, joka kerää lähetettyjä tietoja. Näitä tietoja varten palvelimella täytyy olla tietokanta. Ja jotta kerättyä tietoa pystyisi käyttämään ja että palvelin lähettäisi tarvittaessa hälytyksen ylläpitäjälle, tarvitaan hallinta- ja suodatusohjelma(Kuva 1).



Kuva 1 Yksinkertainen kuvaus syslog-systeemin toiminnasta

3.2.1 Syslogin huonot puolet

Kuten kaikessa myös syslogissa on huonoja puolia. Syslog ei ole kovinkaan yhtenäinen systeemi. Protokolla ei määrittele missä muodossa viestien täytyy olla ja jokaisella kehittäjällä on oma tapansa muodostaa viesti. Koska viestit ovat yleensä UDP:nä, niiden perille pääsy ei ole varmaa. Viestit voivat tippua pois esimerkiksi ruuhkaisen verkon takia tai ne voidaan siepata ja hävittää. Viestien alkuperä voi myös olla epämääräinen, koska syslog ei käytä autentikointia. Tästä seuraavia ongelmia voi olla esimerkiksi väärin konfiguroitu laite, joka lähettää viestejä toisen laitteen nimissä. Tai se voi olla etu verkkoon murtautujille. Tämä hyökkääjä voi lähettää virheellisiä viestejä, joilla voidaan harhauttaa verkon valvojaa, kun toiseen kohtaan verkkoa murtaudutaan.
Kaikesta huolimatta syslogin huonoja puolia pidetään kuitenkin melko vähäisinä. (Leskiw, A. 2014; Wikipedia Syslog 2014.)

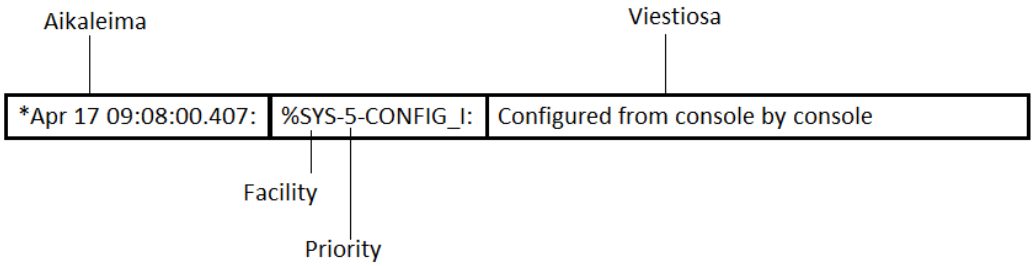
3.2.2 Syslog turvallisuus

Viestit tulisi pitää aina mahdollisimman lyhyinä ja tärkein sisältö tulisi aina olla mahdollisimman alussa viestiä. Tämä siitä syystä, että viestin koon ylittäessä tietyn rajan transport receiver saattaa lyhentää tai hävittää viestin. Tässä on riskinä viestien katoaminen ja verkkoon hyökkääjä voi tätä hyväksi käyttämällä piilottaa loki tietoa.
Hyökkääjä voi myös käyttää hyväkseen sitä, ettei syslog pysty havaitsemaan uudelleen lähetettyjä viestejä. Toisin sanoen hyökkääjä voi lähettää muokattuja viestejä, jotka vaikuttavat tulevan joltakin laitteelta. Tällä voidaan antaa valheellinen kuva verkon toiminnasta.
Syslog-viestien määrä verkossa voi olla valtava, joten on hyvä ottaa huomioon, voiko tämä aiheuttaa tukoksia. Tämä voi tulla ongelmaksi varsinkin jos viestien kuljetukseen käytetään UDP:tä, koska se ei kontrolloi viestien määrää millään tavalla. Systeemissä tulisi olla jokin sovellus, joka osaa tukoksen tapahtuessa jakaa viestit tärkeyden mukaan ja päättää mitä millekin viestille tehdään.
Hyökkääjät voivat myös käyttää Denial Of Service-hyökkäystä eli lähettävät viestejä niin paljon että niiden käsittely systeemi menee tukkoon ja mitään viestejä ei enää pystytä käsittelemään.
Väärät asennukset ovat myös yksi suuri riskitekijä. Tämä voi aiheuttaa ongelmia, kuten vääriin paikkoihin meneviä viestejä ja viestit voivat jäädä matkalle kiertämään kehää. Standardissa on kerrottu esimerkistä, jossa viestit jäivät kulkemaan kahden relayn väliä. Tämä oli seurausta siitä, että ylläpitäjä oli laittanut relayt lähettämään tietyllä severityllä olevia viestejä toisilleen. Ne eivät siis osanneet laittaa näitä viestejä eteenpäin kenellekään muulle. (RFC 5424 2009.)

3.3 Syslog viestin rakenne

Viestissä on tietenkin perustiedot mistä, milloin ja miksi. Nämä ovat muodossa ip-osoite, aikaleima ja viesti. Viesti voi olla teksti muodossa, mutta se voi olla myös jossain muussa muodossa. Viestissä näkyy laite ja ohjelma, jolta se on tullut eli facility-koodi. Ja vakavuusaste eli severity-koodi (Kuva 2).

Syslog viestissä on kolme osaa PRI (priority) eli tärkeys, HEADER eli ylätunniste ja MSG (message) eli itse viesti. Unixin syslog-viesti on siis muodossa: <PRI> HEADER MESSAGE. (Cisco Systems 2011; Wikipedia Syslog 2014.)



Kuva 2 Syslog-viesti näkyy tässä muodossa palvelimella. Se ei kuitenkaan välttämättä vastaa sitä, millaisena viesti kulkee.

3.3.1 Priority

Priority-kentässä on 8 bitin luku hakasulkeissa, joka kertoo viestin tärkeyden. Priority alkaa aina ”<” merkin jälkeen ja päättyy ”>” merkkiin. Lukuja on nollasta 191:een. Tähän lukuun sisältyy facility eli laite ja severity eli kuinka vakavaa se on. Kolme vähiten merkitsevää bittiä kertovat vakavuuden. Vakavuusasteita on siis kahdeksan erilaista. Loput viisi bittiä kertovat lähettäjän. Nämä arvot on päättänyt ja muodostanut lähettävä laite. Priorityn voi myös joissakin tapauksissa määrittää itse. Tässä tapauksessa 191 suurempia lukuja voi käyttää, mutta niiden käyttäminen on riskialtista ja seuraukset voivat olla arvaamattomia. Tärkeysarvon lasku tapahtuu siten, että ensin kerrotaan facility kahdeksalla ja sitten lisätään severityn numeerinen arvo. Näitä lukuja voidaan käyttää tapahtuma suodattimien teossa. Vakavuusasteen tärkeimmät viestit ovat ”0” eli hätätila. Nämä luvut jatkuvat aina ”6” ja ”7” asti. Kuusi on tiedotusviesti ja seitsemän on vain debug-viesteille eli konsolin vianmääritystä varten. Taulukossa 1 on esitelty severity-tasot ja niiden merkitykset.

Taulukko 1 Severity tasot (Cisco Press.)

Luku	Severity	Selitys
0	Emergency (hätätila)	Tämä viesti tulee kun systeemiä ei voi enää käyttää.
1	Alert (hälytys)	Hälytys vakavasta virhetilasta.
2	Critical (kriittinen)	Kiireelliset virhetilanteet, joihin on reagoitava heti.
3	Error (virhe)	Viestit tulevat virhetiloista, jotka eivät ole kiireellisiä. Vaatii usein jatkotoimia.
4	Warning (varoitus)	Viestit varoittavat mahdollisesti tulevista ongelmista. Nämä viestit vaativat jatkotoimia.
5	Notice (huomautus)	Näitä viestejä tulee erikoisten tapahtumien takia, eivät kuitenkaan tarvitse jatkotoimia.
6	Informational (tiedotus)	Nämä viestit ovat tiedonkeräystä ja raportointia varten. Niiden takia ei tarvitse ryhtyä toimiin.
7	Debug (virheiden etsintä)	Nämä viestit ovat kehittäjiä varten. Niitä käytetään ohjelman virheiden etsinnässä.

Myös facility-arvot ovat kokonaislukuina. Niitä käytetään siis kertomaan mistä viesti on tullut. Lähteitä voivat olla esimerkiksi käyttöjärjestelmä, prosessi tai sovellus. Tämä systeemi on alun perin tehty unixille, joten tasojen nimetkin ovat sen mukaan. Facility-arvot näkyvät taulukossa 2.
Unix ei käytä 16 - 23 tasoja, ne ovat verkkolaitteita varten. Esimerkiksi Cisco-reitittimet käyttävät local6 tai local7. (Cisco Systems 2011; Wikipedia Syslog 2014.)

Taulukko 2 Facility (Cisco Press 2005.)

Luku	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons
4	Security/authorization messages
5	Messages generated internally by syslogd
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon
10	Security/authorization messages
11	FTP daemon
12	NTP subsystem
13	Log audit
14	Log alert
15	Clock daemon
16	Local use 0 (local0)
17	Local use 1 (local1)
18	Local use 2 (local2)
19	Local use 3 (local3)
20	Local use 4 (local4)
21	Local use 5 (local5)
22	Local use 6 (local6)
23	Local use 7 (local7)

3.3.2 Header

Ylätunniste sisältää timestampin eli aikaleiman, hostnamen eli verkonnimen tai ip-osoitteen. Aikaleimassa näkyy milloin lähettäjä on luonut viestin, aika näkyy lähettäjän paikallisena aikana. Aikaleima ei enää nykyään ole kovin tärkeä, koska syslog-palvelin itse leimaa ajan ja ip-osoitteen paketteihin niiden saapuessa. Verkonnimi kentässä on verkonnimi tai ip-osoite. Laitteissa joissa on monia liitäntöjä, kuten reitittimet ja palomuurit, käytetään sen liitännän ip-osoitetta, josta viesti lähetetään. Standardin mukaan hostnamen sisältö pitäisi olla FQDN. Jos tämä ei ole mahdollista sisältö voi olla myös muissa muodoissa. Muodot on laitettu järjestykseen sen mukaan, kuinka tarkka ja luotettava muoto on. Järjestys on FQDN, staattinen ip-osoite, hostname, dynaaminen ip-osoite ja NILVALUE. Eli jos FQDN ei ole mahdollinen, seuraavaksi paras vaihtoehto on staattinen ip-osoite. Jos sitäkään ei ole käytetään hostnamea ja niin edelleen. (Cisco Systems 2011; RFC 5424 2009; Wikipedia Syslog 2014.)

3.3.3 Viestiosa

Viestiosa jakautuu kahteen kenttään. TAG-kentässä on viestin lähettäneen ohjelman tai prosessin nimi. CONTENT-kentässä on itse viesti vapaassa muodossa, viestin muoto riippuu kehittäjästä.

3.4 Syslog viestien tallennus ja raportointi, suodatus

Syslog tallentaa viestejä itse vain tekstitiedostoon. Se voidaan kuitenkin ohjata viemään viestit erilliseen tietokantaan. Tietokanta voi olla esimerkiksi MySQL.
Raportoinnista ja analysoinnista syslog ei huolehdi vaan niille tarvitaan erillinen ohjelma. Syslogin voi asentaa tekemään jonkinlaista suodatusta. Se toimii kuitenkin vain enimmäkseen niin, että voit määrittää mitä viestejä palvelin lähettää tai on lähettämättä tietokannalle. Suodatuskin on parempi hoitaa analysointi ohjelmalla.

3.5 Syslogin kerrokset

Syslog koostuu kolmesta kerroksesta. Sisältökerros huolehtii viestin sisällöstä. Sovelluskerros on vastuussa lähettävässä päässä viestin luomisesta ja sen reitin etsimisestä ja vastaanottavassa päässä viestin tulkitsemisesta ja säilömisestä. Kuljetuskerros vain huolehtii viestin lähettämisestä ja vastaanottamisesta.
Sovellus- ja kuljetuskerroksilla tapahtuu erilaisia toimintoja. Sovelluskerroksella ovat toiminnot originator, collector ja relay. Kuljetuskerroksella ovat toiminnot transport sender ja -receiver. Originator on se joka luo viestit. Collector kerää viestit. Relay ottaa viestit vastaan ja lähettää ne eteenpäin, joko seuraavalle relaylle tai collectorille. Transport sender ja -receiver lähettävät ja vastaanottavat viestejä.
Syslog-standardi ei määrittele kuljetuskerroksen protokollaa. Se kuitenkin määrittää, ettei kuljetusprotokolla saa muuttaa viestin sisältöä. Jos muuttaminen on kuitenkin välttämätöntä, se saa olla

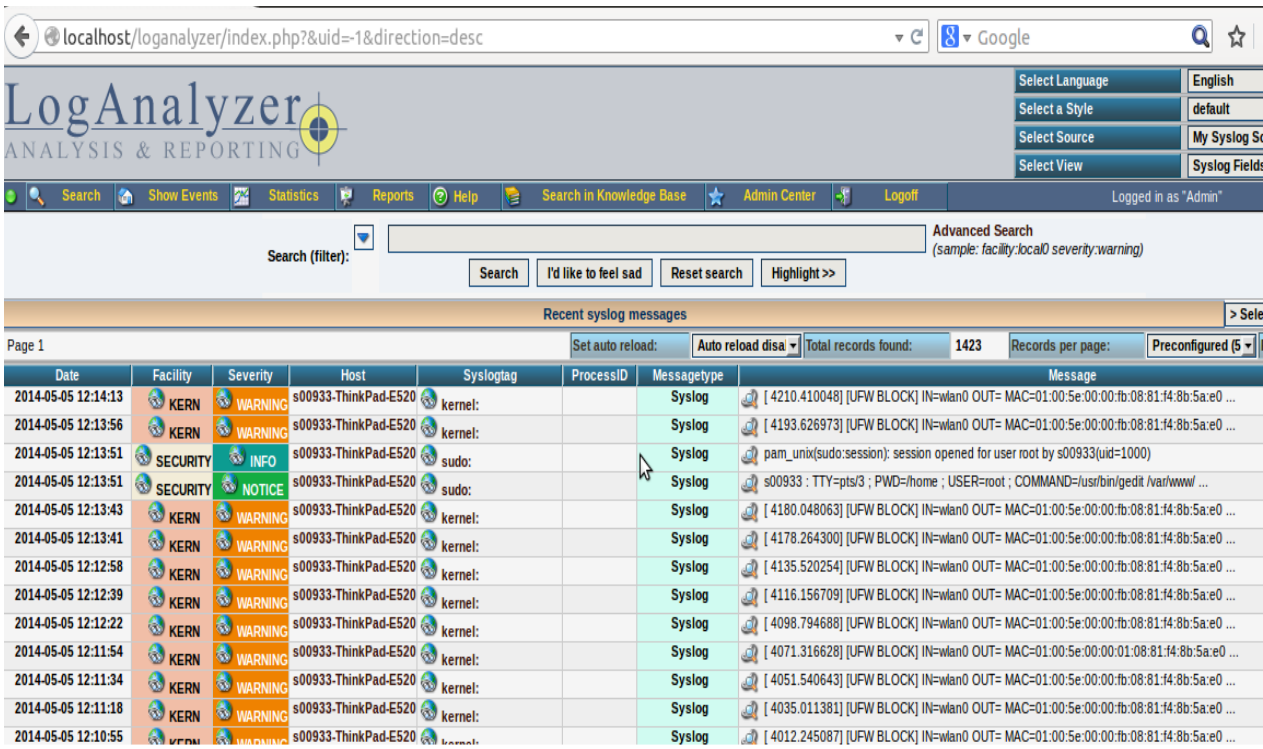
vain viestin kuljetuksen ajaksi. Viesti täytyy muuttaa takaisin juuri samanlaiseksi kuin se oli sitä luodessa, kun se saapuu relaylle tai collectorille. Tässä ei kuitenkaan oteta huomioon virheistä johtuvia muutoksia. (RFC 5424 2009.)

4 KÄYTETYT TYÖKALUT

4.1 Rsyslog

Rsyslog on Open Source-työkalu lokien hallintaan, joka korvaa syslogd:n. Sen kehittämisen aloitti Rainer Gerhards ja tarkoituksena oli luoda kilpailija syslog-ng:lle, jotta käyttäjillä olisi vaihtoehtoja. Se noudattaa BSD-protokollaa, joka on määritelty RFC 3164. Syslogien perustoimintojen lisäksi rsyslogissa on monia lisäyksiä, jotka keskittyvät turvallisuuden ja luotettavan kuljetuksen parantamiseen. Sillä voi suodattaa viestejä sisällön perusteella, se tukee TCP-kuljetusta, joka tekee viestien kuljetuksesta varmempaa. Sen aikaleimat ovat tarkempia ja se tukee MySQL:ää ja PostgreSQL:ää.(Rsyslog 2014; Wikipedia Rsyslog 2014.)

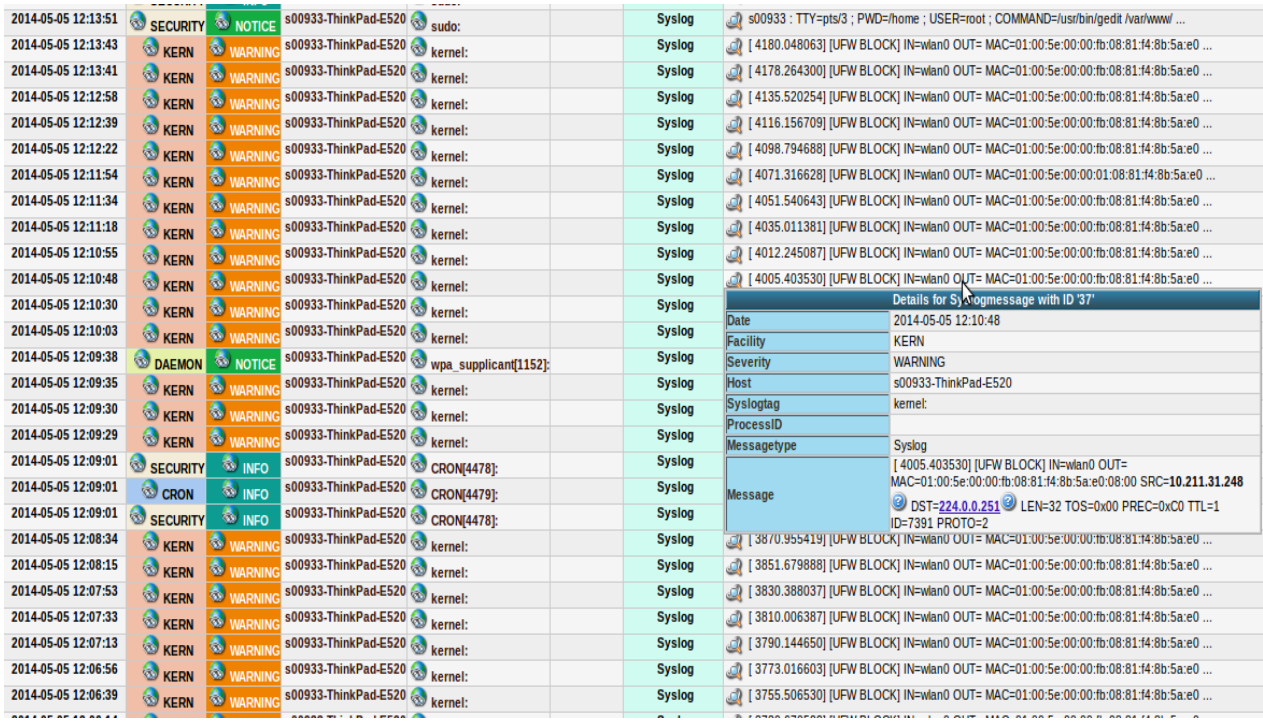
4.2 Adiscon LogAnalyzer



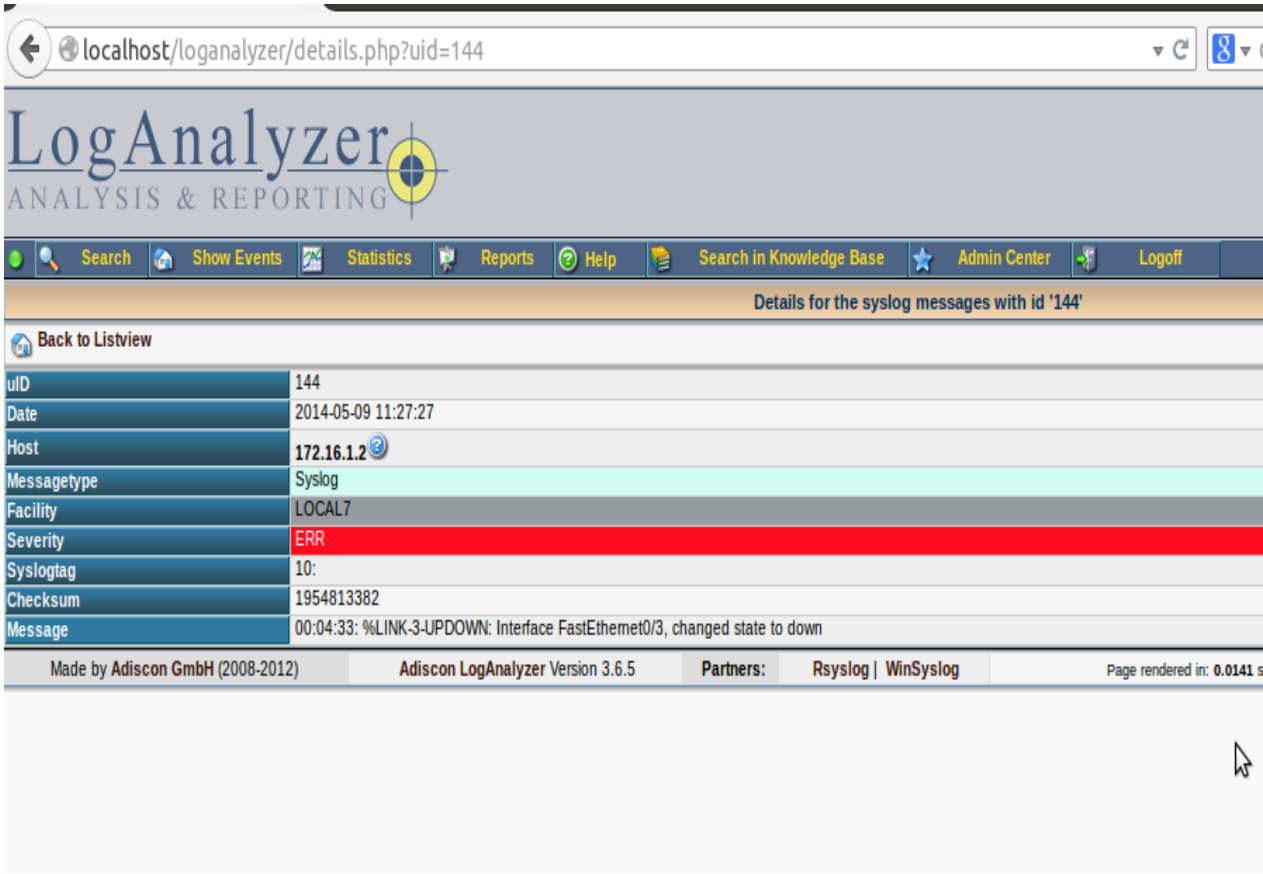
Kuva 3 LogAnalyzer näyttää tietokannassa olevat viestit. Ohjelmalla voi valita, minkä arvon mukaan viestit suodatetaan.

Adiscon LogAnalyzer on lokien analysointityökalu. LogAnalyzer on ilmainen, Open Source-sovellus. Ohjelma on kirjoitettu php:llä ja toimii hyvin Linux- ja Windows-alustoilla. Sillä voi etsiä haluamiaan tietoja lokien tietokannasta ja analysoida ja katsastaa lokeja. Se pystyy keräämään tiedot tietokannasta tai tekstitiedostosta (Kuva 3).
Analyzerilla voi tarkastella viestejä, viestejä voi katsoa tarkemmin viemällä hiiren viestin päälle (Kuva 4) tai klikkaamalla viestiä, jolloin avautuu uusi ikkuna (Kuva 5). Lisäksi viesteistä voi tehdä haluamiaan käyriä tai taulukkoja. Ohjelmalla saa myös tehtyä raportteja tietokannassa olevista viesteistä. Raportit voi tehdä html- tai pdf-muodoissa ja tiedot niihin saa itse määrittää (Kuvat 6-8).
LogAnalyzerilla on sama kehittäjä kuin rsyslogilla, joten sen pitäisi toimia helposti oikein rsyslogin kanssa.

Päätin jättää analysointi ohjelmien testaamisen tähän ohjelmaan. Se on selkeä ja melko yksiselitteinen käyttää. Se myös vaikutti olevan riittävä verkon tarpeisiin.



Kuva 4 Viemällä hiiri viestiosan päälle saa näkyviin tarkempia tietoja



Kuva 5 Valitsemalla viestin pääsee kuvan mukaiseen näkymään

4.3 MySQL

MySQL on yksi maailman suosituimmista relaatiotietokantaohjelmistoista. Se on ilmainen vapaalla GNU GPL-lisensillä, mutta siitä on myös kaupallisenlisenssin versio. Sen kehittäminen alkoi vuonna 1995 ja nykyään kehittämisestä vastaa Oracle. Sitä käyttävät monet suuret verkkosivut, kuten Google, YouTube ja Facebook.

MySQL toimii monilla alustoilla, Linux ja Windows mukaan lukien. Lisäksi se toimii myös pilvialustoilla. Sen kirjoittamiseen käytetään kieliä C ja C++. MySQL:ä käytettään varsinkin verkko sovellusten tietokantana. Se on hyvin toimiva vaihtoehto kun tarvitaan monipuolinen, ilmainen Open Source-tietokannan hallintatyökalu.

MySQL on yksi osa LAMP:ia. LAMP on ilmaisohjelmista koostuva pino ratkaisu. Vaikka LAMP on ilmainen ratkaisu, se kuitenkin toimii myös suuren tietomäärän kanssa.

5 VAIHTOEHTOISET TYÖKALUT

5.1 Syslog-ng

Syslog-ng on rsyslogin tapaan syslog-protokollan mukainen Open Source-ohjelma. Nykyään sitä kehittää BalaBit-ohjelmistoyritys, joka on erikoistunut tietotekniikka turvallisuuteen. Syslog-ng noudattaa BSD-protokollaa, joka on määritelty RFC 3164:ssä. Uudemmat versiot tukevat myös RFC 5424:n mukaista protokollaa.

Perus syslog-protokollan lisäksi syslog-ng:ssä on paljon lisäyksiä. Sillä pystyy esimerkiksi lähettämään viestejä paikallisille sovelluksille ja tekemään lokimerkinnät suoraan tietokantaan. Hallitsemaan viestien virtaa ja luokittelemaan sisään tulevia viestejä. Siinä on myös tarkennettu aikaleima, mahdollisuus tarkastella viestin kulkemaa reittiä, varmempi kuljetus TCP-kuljetuksen ansiosta ja TLS-salaus.

Syslog-ng on yhteensopiva monen alustan kanssa ja löytyy joillekin peräti oletuksena. Lopuille se on pakettina, joka korvaa standardin syslogd:n.

Toisin kuin rsyslog, syslog-ng löytyy ilmaisen Open Source-version lisäksi maksullisena Premium Edition-versiona. Tämä versio on patentoitu ja siinä on enemmän liitännäisiä kuin ilmaisversiossa. Balabit kehittää nykyään myös syslog-ng Store Boxia. Se on lokipalvelin sovellus, jossa on ominaisuuksina lokien keräys, lokien eteenpäin vienti, lokien merkkaus ja luokittelu. (BalaBit 2014; Wikipedia Syslog-ng 2014.)

Päädyin kuitenkin vain käyttämään rsyslogia, koska se toimi moitteettomasti. On kuitenkin vaikea sanoa toimisiko syslog-ng paremmin, kun palvelimen täyttyy toimia melko suuren yrityksen verkossa.

5.2 LOGalyze

Ilmainen lokien analysointi ja raportointi ohjelma. Olisin mielelläni testannut tätäkin ohjelmaa, mutta sen asentaminen tuntui ongelmalliselta. Sain Adisconin LogAnalyzerin toimimaan aikaisemmin ja aikaa oli vähän joten luovutin LOGalyzen asentamisen suhteen. Ohjelma kuitenkin vaikuttaa hyvältä vaihtoehdolta.

7 TESTAUS

7.1 Palvelimen valinta

Palvelimeksi haluttiin ilmainen versio. Palvelin sai olla Linux- tai Windows-pohjainen, mutta muuten rajoituksia ei ollut. Savonian verkkoon oli aikaisemmin yritetty pystyttää syslog-palvelinta. Työ oli kuitenkin jäänyt kesken. Silloin palvelimena oli käytetty Linux-pohjaista ja komentoliittymällä. Päädyin siihen tulokseen, että tälläkin kertaa samanlainen ratkaisu olisi paras vaihtoehto.
Alustaksi palvelimelle tuli kannettava, johon asennettiin Ubuntu 12.04 LTS desktop. Ensimmäiseksi otin kokeiluun rsyslog-palvelimen, siitä syystä, että se löytyy ubuntusta valmiina pakettina.

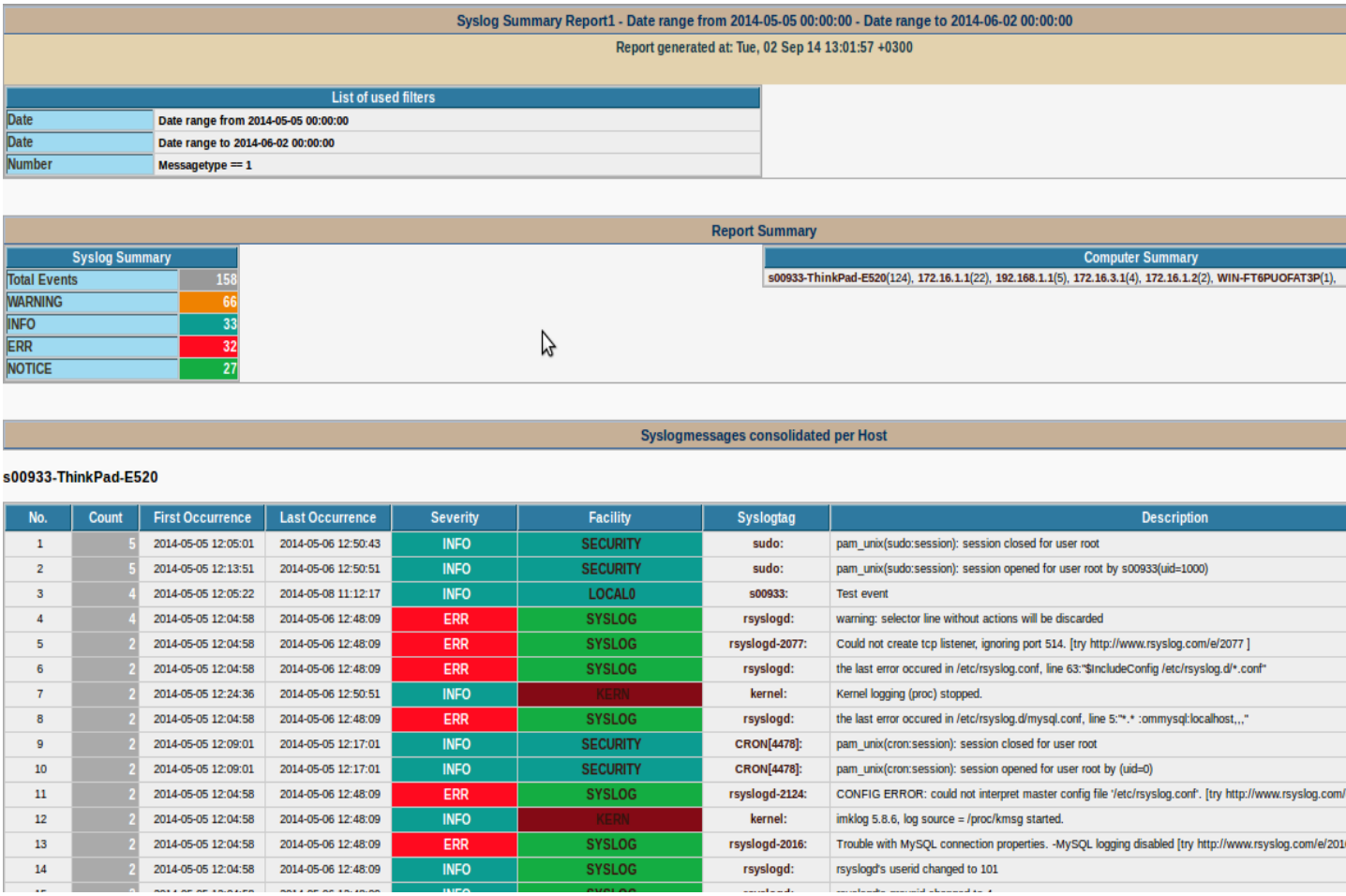
7.1.1 Rsyslog testaus laboratoriossa

Ensimmäisessä testissä oli mukana vain yksi reititin, joka oli asennettu lähettämään syslog-viestejä. Yritys ei heti onnistunut. Oli vaikea selvittää kummassa päässä ongelma oli. Eikö reititin lähettänyt-kään viestejä vai eikö palvelin osannut ottaa niitä vastaan. Ping onnistui kumpaankin suuntaan, joten yhteydessä ei ollut ongelmia. Palvelin kuitenkin osasi ottaa vietejä vastaan koneelta, jolle se oli asennettu, joten palvelinkin vaikutti toimivan.
Vika löytyi palomuurista, joka ei päästänyt läpi viestejä. Palomuuri oli ohjattava päästämään läpi porttia 514 käyttävät viestit.
Suurimpana ongelmana tässä vaiheessa oli tietokanta. Tietokannaksi valitsin mysql:llän. Viestit eivät aluksi suostuneet menemään millään tietokantaan. Internetistä löytyi monia erilaisia ohjeita ongelman ratkaisemiseksi. Ohjeissa oli yleensä eroja vain yksityiskohdissa. Koetin monen eri ohjeen avulla muuttaa rsyslogin konfiguraatiotiedostoa. Tein myös MySQL:n asennuksen uudestaan, siltä varalta että ongelma olisikin siellä. Epäilin kuitenkin jo tässä vaiheessa, että ongelmana oli, etteivät rsyslog ja MySql vielä osanneet kommunikoida keskenään. En kuitenkaan saanut asennettua niiden kommunikointi työkalua netistä löytämieni ohjeiden avulla. Tästä syystä luulin, että työkalua olisi jo tullut rsyslogin asennuksen mukana. Siksi keskityin löytämään ongelmaa muulta.
Löysin lopulta syslog-viestien avulla ongelmakohdan. Kuten olin alussa epäillyt rsyslogin ja MySql:n väliltä puuttui työkalu. Huomasin syslog-viesteistä, ettei rsyslog osannut lukea omaa konfiguraatiotiedostoaan. Viesteissä näkyi, että tämä johtui siitä, ettei rsyslogilla ollut ommysql.so nimistä tiedostoa. Tämä tiedosto on plugin, jonka avulla Rsyslog osaa viedä viestit MySql-tietokantaan. Löysin netistä tiedon, että tiedosto kuuluu rsyslog-mysql-nimiseen pakettiin. Olin aikaisemmin yrittänyt asentaa tätä pakettia ohjeiden avulla. Silloin ubuntu väitti, ettei pakettia löydy. Tajusin nyt itse koittaa komentoa ”sudo apt-get install rsyslog-mysql”, jolla pakettin sai vihdoinkin asennettua. Tämän jälkeen palvelin osasi lähettää viestit tietokantaan.
Seuraavaksi keskityin siihen mitä viestejä palvelin lähettää tietokantaan. Tuntui järkevimmältä ja helpommalta neuvoa palvelinta lähettämään tietyllä facility-koodilla tulevat viestit tietokantaan. Tässä vaiheessa on kuitenkin vaikea sanoa toimiiko tämä ratkaisu, kun palvelin laitetaan oikeaan verkoon ja sille tulee viestejä suurelta määrältä verkkolaitteita.

7.1.2 Testaus verkossa

Testaus aloitettiin varovaisesti vain yhdellä kytkimellä. Kun nähtiin, että kytkin osasi lähettää viestit palvelimelle siirryttiin useampaan kytkimeen. Seuraavaksi kytkimiä lisättiin jo useita. Näistä yksi ei suostunut ottamaan syslog käskyjä vastaan, eikä myöskään lähettänyt viestejä palvelimelle. Syy tähän ei selvinnyt.

Testauksessa kokeiltiin myös pakottaa kytkimet lähettämään verkkoturvallisuuteen liittyviä viestejä. Lopuksi lisäsin vielä syslog-viestien analysointityökalun. Testasimme vielä sen kanssa palvelinta. Ne toimivat heti hyvin yhdessä.



Syslog Summary Report1 - Date range from 2014-05-05 00:00:00 - Date range to 2014-06-02 00:00:00

Report generated at: Tue, 02 Sep 14 13:01:57 +0300

List of used filters

Date	Date range from 2014-05-05 00:00:00
Date	Date range to 2014-06-02 00:00:00
Number	Messagetype == 1

Report Summary

Syslog Summary	
Total Events	158
WARNING	66
INFO	33
ERR	32
NOTICE	27

Computer Summary

s00933-ThinkPad-E520(124), 172.16.1.1(22), 192.168.1.1(5), 172.16.3.1(4), 172.16.1.2(2), WIN-FT6PUOFAT3P(1),

Syslogmessages consolidated per Host

s00933-ThinkPad-E520

No.	Count	First Occurrence	Last Occurrence	Severity	Facility	Syslogtag	Description
1	5	2014-05-05 12:05:01	2014-05-06 12:50:43	INFO	SECURITY	sudo:	pam_unix(sudo:session): session closed for user root
2	5	2014-05-05 12:13:51	2014-05-06 12:50:51	INFO	SECURITY	sudo:	pam_unix(sudo:session): session opened for user root by s00933(uid=1000)
3	4	2014-05-05 12:05:22	2014-05-08 11:12:17	INFO	LOCAL0	s00933:	Test event
4	4	2014-05-05 12:04:58	2014-05-06 12:48:09	ERR	SYSLOG	rsyslogd:	warning: selector line without actions will be discarded
5	2	2014-05-05 12:04:58	2014-05-06 12:48:09	ERR	SYSLOG	rsyslogd-2077:	Could not create tcp listener, ignoring port 514. [try http://www.rsyslog.com/e/2077]
6	2	2014-05-05 12:04:58	2014-05-06 12:48:09	ERR	SYSLOG	rsyslogd:	the last error occured in /etc/rsyslog.conf, line 63:"$IncludeConfig /etc/rsyslog.d/*.conf"
7	2	2014-05-05 12:24:36	2014-05-06 12:50:51	INFO	KERN	kernel:	Kernel logging (proc) stopped.
8	2	2014-05-05 12:04:58	2014-05-06 12:48:09	ERR	SYSLOG	rsyslogd:	the last error occured in /etc/rsyslog.d/mysql.conf, line 5:"*.* :ommysql:localhost,,,"
9	2	2014-05-05 12:09:01	2014-05-05 12:17:01	INFO	SECURITY	CRON[4478]:	pam_unix(cron:session): session closed for user root
10	2	2014-05-05 12:09:01	2014-05-05 12:17:01	INFO	SECURITY	CRON[4478]:	pam_unix(cron:session): session opened for user root by (uid=0)
11	2	2014-05-05 12:04:58	2014-05-06 12:48:09	ERR	SYSLOG	rsyslogd-2124:	CONFIG ERROR: could not interpret master config file '/etc/rsyslog.conf'. [try http://www.rsyslog.com/
12	2	2014-05-05 12:04:58	2014-05-06 12:48:09	INFO	KERN	kernel:	imklog 5.8.6, log source = /proc/kmsg started.
13	2	2014-05-05 12:04:58	2014-05-06 12:48:09	ERR	SYSLOG	rsyslogd-2016:	Trouble with MySQL connection properties. -MySQL logging disabled [try http://www.rsyslog.com/e/201
14	2	2014-05-05 12:04:58	2014-05-06 12:48:09	INFO	SYSLOG	rsyslogd:	rsyslogd's userid changed to 101

Kuva 6 Syslog-viesteistä tehty raportti html-muodossa

List of used filters	
Date	**Date range from 2014-05-05 00:00:00**
Date	**Date range to 2014-06-02 00:00:00**
Number	**Messagetype == 1**

Report Summary

Syslog Summary	
Total Events	158
WARNING	66
INFO	33
ERR	32
NOTICE	27

Computer Summary
s00933-ThinkPad-E520(124), 172.16.1.1(22), 192.168.1.1(5), 172.16.3.1(4), 172.16.1.2(2), WIN-FT6PUOFAT3P(1),

Kuva 7 Syslog-viesteistä tehty raportti pdf-muodossa

No.	Count	First Occurrence	Last Occurrence	Severity	Facility	Syslogtag
1	5	2014-05-05 12:05:01	2014-05-06 12:50:43	INFO	SECURITY	sudo:
	Description		pam_unix(sudo:session): session closed for user root			
2	5	2014-05-05 12:13:51	2014-05-06 12:50:51	INFO	SECURITY	sudo:
	Description		pam_unix(sudo:session): session opened for user root by s00933(uid=1000)			
3	4	2014-05-05 12:05:22	2014-05-08 11:12:17	INFO	LOCAL0	s00933:
	Description		Test event			
4	4	2014-05-05 12:04:58	2014-05-06 12:48:09	ERR	SYSLOG	rsyslogd:
	Description		warning: selector line without actions will be discarded			

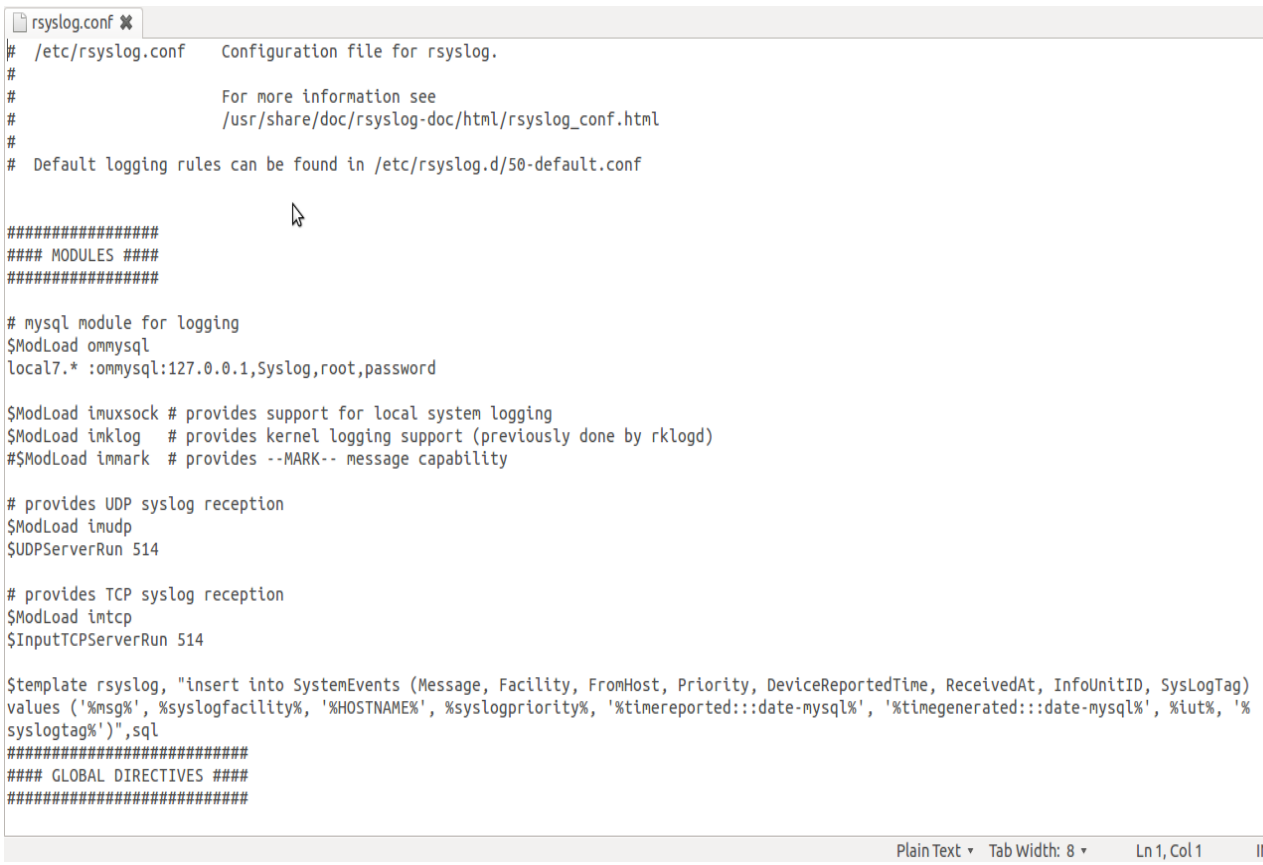
Kuva 8 Edellisen kuvan raportin osa, jossa näkyy viestit

8 PALVELIMEN PYSTYTYS

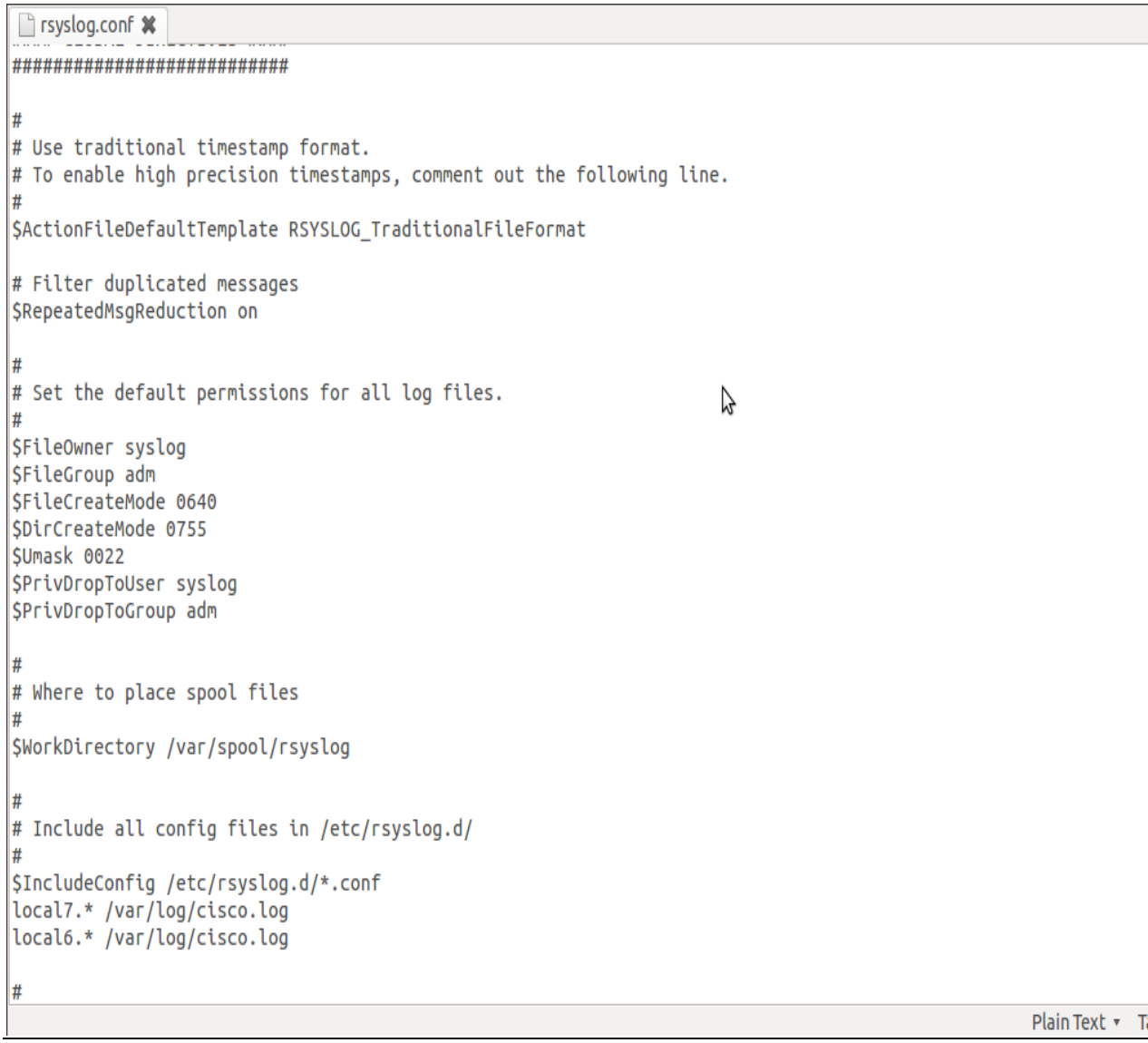
8.1 Palvelin, kytkimet

Palvelin pystytettiin linux-pohjalle. Se asennettiin paketista, joka tuli ubuntussa valmiina. Asennukseen käytettiin komentoa ”sudo apt-get install rsyslog”. Lisäksi latasin verkosta uusimmat päivitykset palvelimeen.

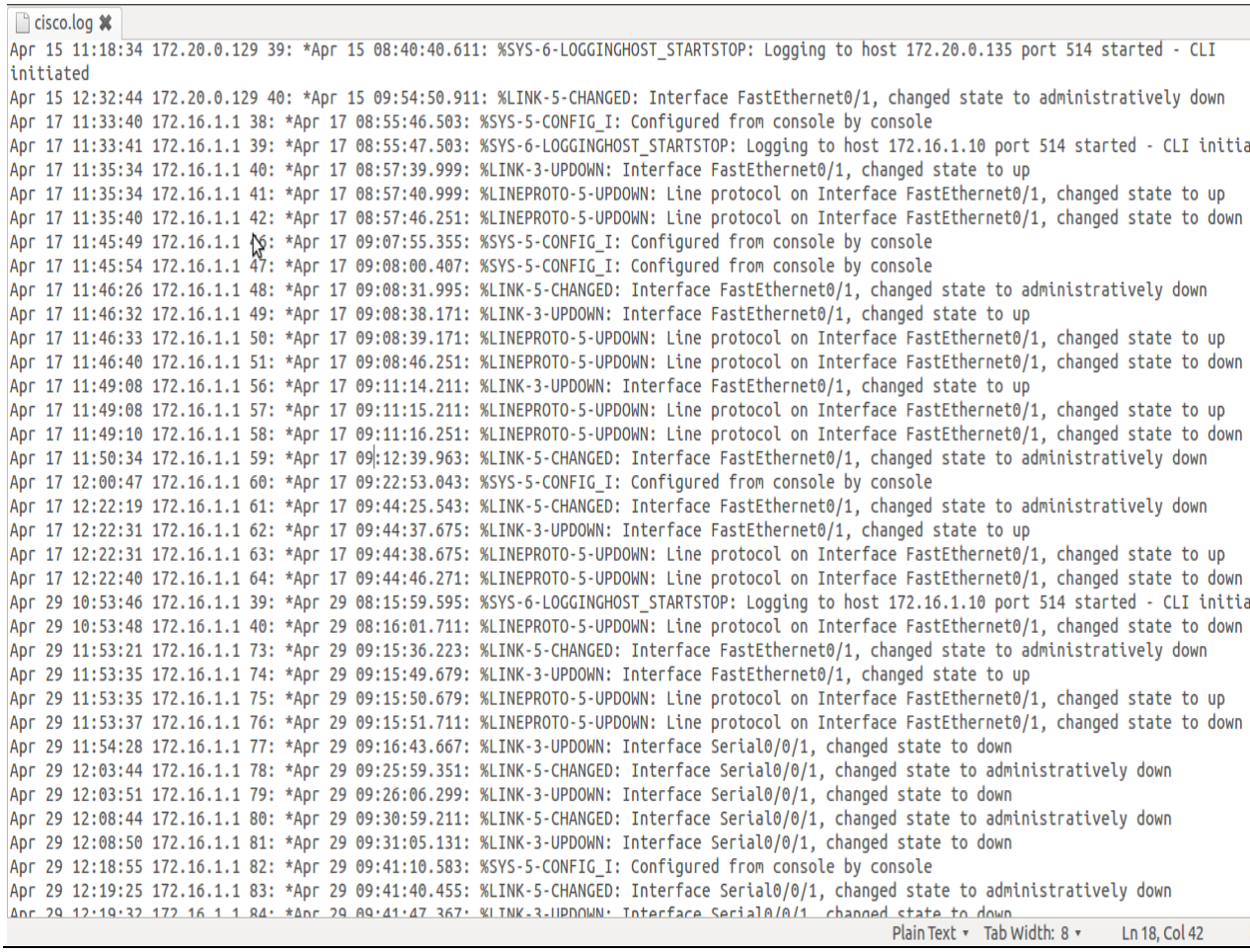
Palvelin tarvitsi vielä säätämistä toimiakseen oikein. Muutoksia täytyi tehdä rsyslog.conf-tiedostoon, joka on rsyslogd:n pääkonfigurointi tiedosto. Tämä tiedosto määrittää säännöt, joiden mukaan palvelin käsittelee viestejä. Tässä tiedostossa on rivit ”$ModLoad imudp”, ”$UDPServerRun 514”, ”$ModLoad imtcp” ja ”$InputTCPServerRun 514”. Näistä riveistä täytyi poistaa #-merkki, että ne tulivat voimaan. ModLoad imudp ja imtcp mahdollistavat viestien vastaanoton udp:n ja tcp:n kautta. ”ServerRun 514”-komennot ohjaavat palvelimen kuuntelemaan porttia 514. Tähän tiedostoon lisätään myös tieto viestien säilytyspaikasta. Kyseessä oleva config-tiedosto muutoksineen on esitetty kuvassa 9.



Kuva 9 Rsyslog-tiedoston yläosa



Kuva 10 Rsyslog-tiedoston alaosa



Kuva 11 Palvelimelle tulleet viestit tekstitiedostossa

Laitoin aluksi viestit menemään tekstitiedostoon. Rivi, jonka lisäsin conf-tiedostoon, on ”*.* /var/log/syslog.log” eli kaikki syslog-tiedostot menevät log-kansion syslog-tiedostoon. Muutin rivin kuitenkin myöhemmin muotoon ”local7.* /var/log/cisco.log” eli local7-facilityllä tulevat viestit menvät cisco.log tiedostoon (Kuva 10). Tämä johtui siitä, että kannettava tietokone jolla palvelin oli lähetti viestejä palvelimelle suuria määriä. Kun testasin palvelinta verkkolaitteilla, näiden viestien tarkastelu kannettavan koneen viestien seasta olisi ollut hankalaa. Käytin local7-facility koodia, koska suurin osa verkkolaitteista käyttää sitä.

Kytkinten asennus lähettämään syslog-viestejä on yksinkertainen. Käskyllä ”logging on” kytkin saadaan lähettämään viestejä. Kytkimelle annetaan palvelimen ip-osoite käskyllä ”logging 0.0.0.0”. Lopuksi kannattaa vielä antaa käsky, jolla määritetään minkä tasoisia viestejä kytkin lähettää. Tähän käytetään käskyä ”logging trap informational”, jossa viimeisen sanan kohdalle tulee severity-tason nimi. Kytkimen pitäisi tämän jälkeen lähettää viestejä. Samat käskyt toimivat myös reitittimille.

Testasin palvelimen toimintaa, yhdistämällä siihen verkkolaitteita. Kun palvelin sai laitteilta viestejä ja selvästi toimi oikein, aloin suunnitella tietokannan yhdistämistä palvelimeen.

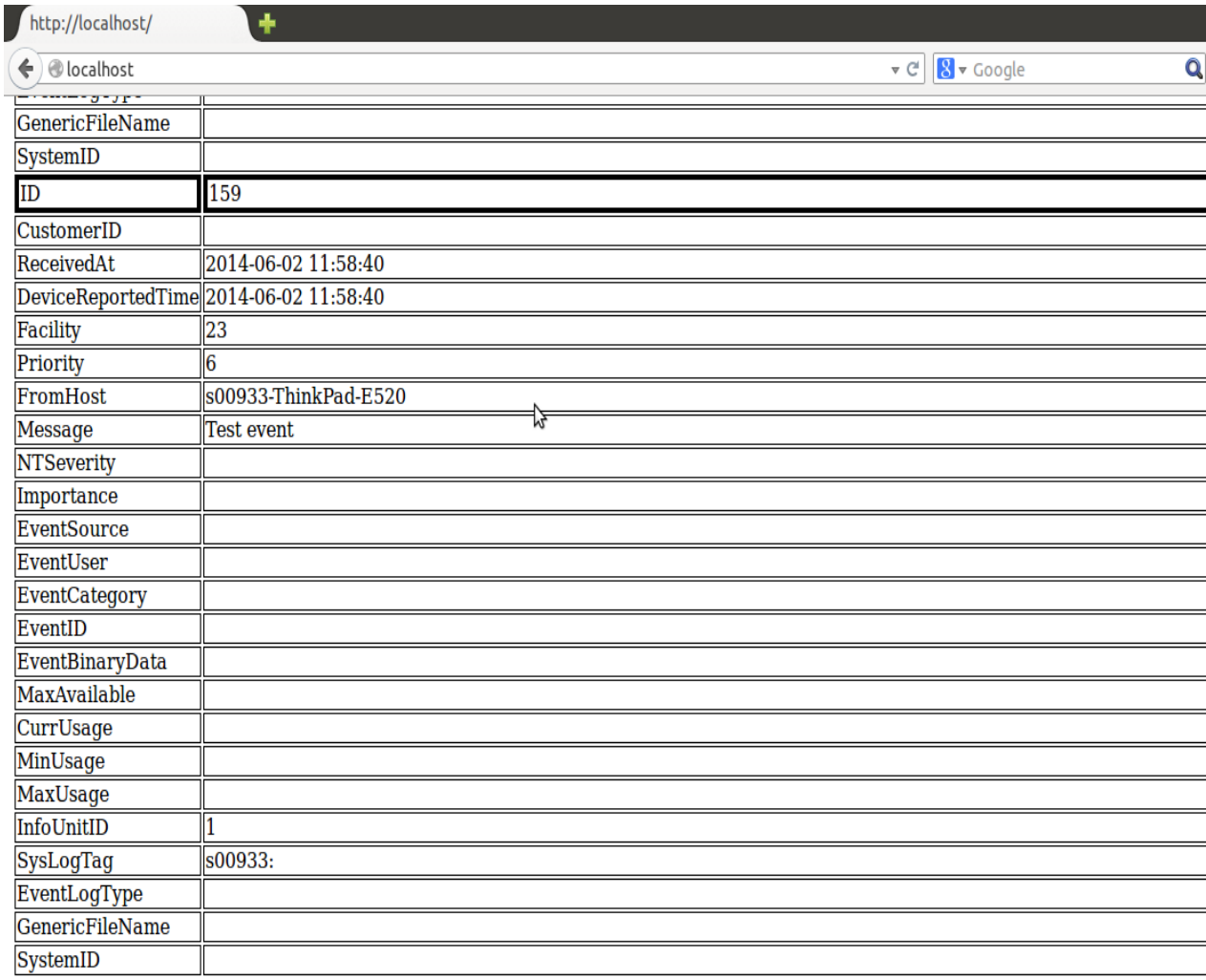
Tietokannaksi valitsin MySQL:n. Kun se oli asennettu, rsyslog.conf tiedostoon täytyi taas tehdä lisäyksiä. Toimiakseen oikein palvelin täytyi neuvoa käyttämään MySQL-liitännäistä. Tein tämän käskyllä ”$ModLoad ommysql”, joka on paras laittaa ensimmäiseksi MySQL:n liittyväksi komennoksi. Lisäsin myös rivin ”local7.* :ommysql:127.0.0.1,Syslog,root,password”. Ensimmäinen osa määrittää millai-

set viestit tietokantaan menevät. Halusin tietokantaan menevän vain verkkolaitteiden viestit, joten käytin taas suodattamiseen facility koodia local7. Seuraavaksi on moduulinnimi ja tietokantapalvelimen osoite. Koska tietokanta oli tässä tapauksessa samalla koneella kuin syslog-palvelin, käytin ”localhostia” vastaavaa osoitetta. Kolme viimeistä kohtaa ovat tietokannan nimi, tietokannan käyttäjän nimi ja salasana.

Lisäsin vielä rivin, joka kertoi millaista templatea tietokannan pitäisi käyttää. Monien ohjeiden mukaan se ei kuitenkaan ole välttämättä tarpeellinen.

Tämän jälkeen tarvitsin jonkin tavan tarkastella tietokannassa olevia tietoja, koska niiden tarkastelu tekstitiedostosta on hyvin epäkäytännöllistä (Kuva 11). Se onnistui pienellä ohjelmoinnilla, jonka ansiosta pystyin katsomaan tietokannan sisältöä taulukko muodossa selaimella (Kuva 12). Se oli kuitenkin hyvä ratkaisu vain niin pitkään kuin viestien määrä oli pieni. Kun siirrytään oikeassa verkossa testaamiseen, olisi oltava jokin kunnollinen ratkaisu viestien tarkasteluun. Viestien analysointiohjelman käyttö oli alun perinkin ollut tarkoituksena.

Viestien tarkasteluun ja analysointiin valikoitui ohjelma Adiscon LogAnalyzer. Paketin sai ohjelman kotisivuilta, joilta löytyi myös ohjeet asennukseen ja käyttöön. Jouduin kuitenkin käyttämään lisäksi muualta verkosta löytämiäni ohjeita, jotka olivat selkokielisemmät.



GenericFileName	
SystemID	
ID	159
CustomerID	
ReceivedAt	2014-06-02 11:58:40
DeviceReportedTime	2014-06-02 11:58:40
Facility	23
Priority	6
FromHost	s00933-ThinkPad-E520
Message	Test event
NTSeverity	
Importance	
EventSource	
EventUser	
EventCategory	
EventID	
EventBinaryData	
MaxAvailable	
CurrUsage	
MinUsage	
MaxUsage	
InfoUnitID	1
SysLogTag	s00933:
EventLogType	
GenericFileName	
SystemID	

Kuva 12 Itseohjelmoitu selaimella toimiva taulukko

8.2 Salaus

Syslog-viestien salaukselle ei riittänyt aikaa. Salaus on kuitenkin ensiarvoisen tärkeää syslog-systeemissä, varsinkin kun kyseessä on yritys. Koska syslog on teksti-pohjainen, sen viestien lukeminen on helppoa, ellei salaus ole kunnossa.

Rsyslogin kehittäjä suosittelee käyttämään TLS kuljetusta syslog-viestien salaukseen. TLS:n ansiosta client-server sovellus voi lähettää viestejä verkossa ja niitä ei pysty peukaloimaan tai salakuuntelemaan.

TLS ei toimi UDP:llä, koska se vaatii luotettavan kuljetuksen. Kaikkien viestien tulisi siis liikkua TCP:nä.

Ensimmäinen vaihe on sertifikaattien hankinta niin palvelimelle kuin client-laitteellekin. Sertifikaatit kannattaa luoda itse, koska silloin ne ovat turvallisimmat. Palvelimelle täytyy myös kertoa missä sertifikaatit ovat. Eli palvelimen conf-tiedostoon kirjoitetaan tiedot siitä mistä sertifikaatit löytyvät. Tämä tehdään kirjoittamalla sinne polku sertifikaatien kansioon.

Client päähän tarvitaan vain yksi sertifikaatti, joka on CA sertifikaatti.

9 YHTEENVETO

Aihe oli minulle melkein täysin tuntematon, jouduin siis opettelemaan kaiken alusta lähtien. Aloitin opiskelemalla syslogin toimintaa.

Minulle tuli hieman yllätyksenä se, kuinka käytetty systeemi syslog on ja myös sen käytännöllisyys. Syslog on standardoitu ja se toimii nykyajan hyvin käytetyllä client/server-mallilla. Sen käytettävyyteen vaikuttaa sen yhteenkäyvyys monien eri laitteiden ja käyttöjärjestelmien kanssa. Syslogin suosiosta kertoo jotain myös, että se on jo nykyään oletus toimintona useimmissa verkkolaitteissa. Syslogilla on myös huonot puolensa. Tulin kuitenkin siihen tulokseen, etteivät sen ongelmat ole kovinkaan suuria. Yleinenkin mielipide vaikuttaa pitävän syslogin ongelmia vähäisinä. Tässä työssä luetellut ongelmat ovat mielestäni suurimmaksi osaksi korjattavissa. Ne voi saada vähäisiksi tai kokonaan poistettua. Syslogin voi siis saada melkein ongelmattomaksi hyvällä suunnittelulla ja asennuksella.

Työn alussa minulle muodostui ajatus siitä, että testaisin useampaa palvelinta ja samalla myös useampaa työkalua muihin systeemiin osiin. Olin varma, että en heti löytäisi parhaiten toimivia ohjelmia. Ajan puutteen vuoksi hylkäsin idean. Toisaalta olin tyytyväinen ensimmäiseksi valittujen työkalujen toimintaan, joten asia ei jäänyt pahasti vaivaamaan. Halusin kuitenkin esitellä työssä vaihtoehtoisia työkaluja.

Työn keskeisin osa oli tietysti itse palvelin. Palvelimen testauksen jääminen vain yhteen versioon olikin ainoa osa, joka jäi todella harmittamaan. Rsyslog kuitenkin vaikutti toimivan hyvin, ainakin pienessä mittakaavassa. Rsyslogin lisäksi olisin testannut toista tunnettua palvelinta syslog-ng:tä. Yleisen keskustelun perusteella en kuitenkaan pystynyt tekemään minkäänlaista johtopäätöstä siitä kumpi olisi parempi tai sopivampi palvelin. Saattaa kuitenkin olla, että ng:lle löytyy parempi tuki. Johtuen siitä, että siitä on olemassa myös kaupallinen versio.

Ensimmäiset testaukset laboratoriossa sujuivat hitaasti. Olin tekemässä syslog-palvelimen pystyttämistä ensimmäistä kertaa. Jouduin siksi lukemaan samalla ohjeita ja ratkaisemaan ongelmia koko ajan. Ensimmäinen ongelma oli palomuuri, joka esti viestien kulun. Paljon suurempi ongelma oli, kuinka saada palvelimen ja tietokannan välinen yhteys toimimaan. Sain lopulta päättelemällä ratkaistua ongelman. Ainoa ratkaisematon ongelma oli, että jotkut kytkin-mallit eivät suostuneet lähettämään syslog-viestejä. Kykimet ottivat käskyt vastaan, mutta niiltä ei tullut viestejä palvelimelle. En löytänyt mistään ohjeita näille kytkimille, joten lopulta oli pakko luovuttaa asian suhteen.

Verkossa testaamisessa ei ongelmia oikeastaan tullut. Ainoastaan yksi kytkin ei suostunut lähettämään syslog-viestejä.

Palvelimen ja systeemin muiden osien asennus sujui suhteellisen hyvin. Ohjeita löytyi yleensä hyvin, johtuen varmaankin siitä, että syslog on hyvin käytetty. Ohjeissa oli kuitenkin aina eroja yksityiskohdissa, joten ohjeita piti yhdistellä ja löytää toimivin ratkaisu. Ainoa osuus, johon ei löytynyt toimivia ohjeita oli edellä mainittu palvelimen ja tietokannan välinen yhteys.

Testauksesta pois jäi valitettavasti todella tärkeä osuus, salaus. Viestien salaus on oltava kunnossa, muuten verkkossa liikkuva tieto voi päätyä vääriin käsiin. Syslogissa ei ole automaattisesti mitään salausta, vaan viestit liikkuvat tekstimuodossa, jolloin niitä voi lukea kuka tahansa. Viestien on kuljettava TCP:nä ja palvelimelle ja verkkolaitteille on laitettava sertifikaatteja. Ratkaisuja on varmasti

muitakin. Tämä oli kuitenkin rsyslogin kehittäjän ehdottama ratkaisu, joten olisin varmaankin testannut sitä ensimmäisenä jos aikaa olisi ollut enemmän.

Olen melko tyytyväinen työhön, kuitenkin minua jäi harmittamaan se, että muista asioista johtuvat ongelmat tulivat häiritsemään työtä. Siitä johtuen jouduin tekemään paljon asioita kiireellä ja ne eivät saaneet huomiota niin paljon kuin olisi tarvinnut. Työstä jäi myös puuttumaan osuuksia, jotka olisivat olleet tärkeitä.

Olen kuitenkin yllättynyt siitä, kuinka hyvin asiat loppujen lopuksi sujuivat. Vastaan tulleet ongelmat sai suurimmaksi osaksi ratkaistua ja tuloksena oli toimiva systeemi.

LÄHTEET JA TUOTETUT AINEISTOT

BalaBit 2014. *The Foundation of Log Management* [verkkosivu]. BalaBit IT Security [Viitattu 16.6.2014]. Saatavissa:

http://www.balabit.com/network-security/syslog-ng/

Broughton, J. 2011. *Creating a Centralized Syslog Server* [verkkojulkaisu]. Linux Journal [Viitattu 2.3.2014]. Saatavissa:

http://www.linuxjournal.com/content/creating-centralized-syslog-server

Cisco Systems 2011. *Building Scalable Syslog Management Solutions* [verkkodokumentti]. Cisco Systems [Viitattu 5.3.2014]. Saatavissa:

http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-557812.html

Cisco Press 2005. *An Overview of the Syslog Protocol* [verkkojulkaisu]. Cisco Press [24.3.2014]. Saatavissa: http://www.ciscopress.com/articles/article.asp?p=426638

Leskiw, A. 2014. *Understanding Syslog: Servers, Messages & Security* [verkkojulkaisu]. Network Management Software [Viitattu 10.3.2014]. Saatavissa: http://www.networkmanagementsoftware.com/what-is-syslog

RFC 5424 2009. *The Syslog Protocol*. Internet Engineering Task Force (IETF). [Viitattu 27.2.2014]. Saatavissa:

http://tools.ietf.org/html/rfc5424

Rsyslog 2014. *RSyslog – Documentation* [verkkodokumentti]. Rsyslog [Viitattu 7.4.2014]. Saatavissa: http://www.rsyslog.com/doc/

SolarWinds 2012. *Kiwi Syslog Server* [verkkodokumentti]. SolarWinds [Viitattu 24.3.2014]. Saatavissa: http://www.kiwisyslog.com/help/syslog/index.html?

TechTarget 2008. *client/server* [verkkosivu]. TechTarget [Viitattu 14.3.2014]. Saatavissa: http://searchnetworking.techtarget.com/definition/client-server

WIKIPEDIA. LAMP [verkkojulkaisu]. [Viitattu 18.6.2014]. Saatavissa:

http://en.wikipedia.org/wiki/LAMP_%28software_bundle%29

WIKIPEDIA. MySQL [verkkojulkaisu]. [Viitattu 18.6.2014]. Saatavissa:

http://en.wikipedia.org/wiki/MySQL

WIKIPEDIA. Rsyslog [verkkojulkaisu]. [Viitattu 7.4.2014]. Saatavissa: http://en.wikipedia.org/wiki/Rsyslog

WIKIPEDIA. Syslog [verkkojulkaisu]. [Viitattu 27.2.2014]. Saatavissa: http://en.wikipedia.org/wiki/Syslog

WIKIPEDIA. Syslog-ng [verkkojulkaisu]. [Viitattu 7.4.2014]. Saatavissa: http://en.wikipedia.org/wiki/Syslog-ng

LIITE 1: RSYLOG.CONF-TIEDOSTON SISÄLTÖ

```
#  /etc/rsyslog.conf Configuration file for rsyslog.
#
#                               For more information see
#                               /usr/share/doc/rsyslog-
doc/html/rsyslog_conf.html
#
#  Default logging rules can be found in /etc/rsyslog.d/50-
default.conf


#################
#### MODULES ####
#################

# mysql module for logging
$ModLoad ommysql
local7.* :ommysql:127.0.0.1,Syslog,root,password

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support (previously done
by rklogd)
#$ModLoad immark  # provides --MARK-- message capability

# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514

$template rsyslog, "insert into SystemEvents (Message, Facility,
FromHost, Priority, DeviceReportedTime, ReceivedAt, InfoUnitID,
SysLogTag)
values ('%msg%', %syslogfacility%, '%HOSTNAME%', %syslogpriority%,
'%timereported:::date-mysql%', '%timegenerated:::date-mysql%', %iut%,
'%syslogtag%')",sql
###########################
#### GLOBAL DIRECTIVES ####
```

```
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup adm

#
# Where to place spool files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
local7.* /var/log/cisco.log
local6.* /var/log/cisco.log

#
```

LIITE 2: SELAIN-TAULUKON KOODI

Kuvan 12 taulukon koodaus.

```
<!DOCTYPE html>
<html><body><h1>SELECT * FROM SystemEvents</h1>

<table>
<?php
          $con = mysql_connect("localhost", "root", "password");
          mysql_select_db("Syslog", $con);

          $res = mysql_query("SELECT * FROM SystemEvents", $con);
          while($row = mysql_fetch_assoc($res))
          {
                    foreach($row as $key => $val)
                    {
                              echo "<tr><td style='border: " . ($key ==
'ID'?"4px":"1px") . " solid;'>$key</td><td style='border: " . ($key ==
'ID'?"4px":"1px") . " solid;'>$val</td></tr>";
                    }
          }
?>
</table>
</body></html>
```