Haaga-Helia
ammattikorkeakoulu Oy

Yhdistyksen verkkosivuston julkaisualustan päivittäminen

Ari Hartikainen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2017

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Ari Hartikainen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Yhdistyksen verkkosivuston julkaisualustan päivittäminen.

Sivu- ja liitesivumäärä
25 + 36

Opinnäytetyön tavoitteena on yhdistyksen verkkosivuston julkaisualustan päivittäminen.

Toiminnallinen työ, jossa toteutetaan pienen yhdistyksen http-palvelimen hankinta ja käyttöönotto. Työhön liittyy palvelimen toimintakuntoon saattaminen, sekä sähköposti- ja Wordpress palvelimen käyttöönotto.

Teoriaosuus esittelee tekniikan ja ohjelmistojen sopivuutta tähän produktiin, työhön liittyvät ohjelmistot sekä tietoturvaan liittyviä asioita käsitellään syvällisemmin.

Toiminnallinen osuus sisältää palvelimen käytännön suorittamista, sekä ohjeistusta miksi tai miten tietyt vaiheet on määritelty.

Opinnäytetyön tavoitteena on luoda uusi palvelin ja dokumentoida sen eri vaiheet. Dokumentoinnin osalta palvelimen uudelleen asennus on toistettavissa ohjeita seuraamalla. Lisäksi toteutetaan ohjeet palvelun käyttäjille, joiden avulla palvelua voidaan käyttää turvallisesti ja tehokkaasti.

Asiasanat
http-palvelin, wordpress, apache, linux

Sisällys

Keskeiset termit ja käsitteet 1

Johdanto 4

1 Tavoitteet 5

2 Palvelimen merkitys Skaalalle 6

2.1 Palvelimen, käyttöjärjestelmän ja ohjelmistojen valinta 6

2.2 Palvelimen rakenne 7

3 Tietoturva 8

3.1 Tietoturvan osa-alueet. 8

3.2 Linux 10

4 Toiminnallinen osuus / Palvelimen asennus 11

4.1 VPS 11

4.2 Ubuntu 12

4.3 Verkkotunnus 13

4.4 Palvelimen määrittely ja käyttöönotto 13

4.4.1 Asennetaan määrittelyssä tarvittavat ohjelmat 15

4.5 Verkkotunnus Nimipalvelu / DNS määrittely 16

4.5.1 Palvelimen hosts tiedoston ja aikavyöhykkeen määrittely 17

4.6 SSL Let’s Encrypt-sertifikaatin asennus 17

4.6.1 SSL-sertifikaatin automaattinen päivittäminen. 18

4.6.2 Apache Http Server 18

4.6.3 SSL ja Apache2 19

4.7 MySQL 19

4.8 Postfix 20

4.9 Dovecot 20

4.10 Wordpress 21

4.10.1 Wordfence plugin 21

4.10.2 Aktivoidaan Permalinks 22

4.10.3 Turvalliset päivitykset Wordpressiin ja SALT:n lisäys 22

4.10.4 Wordpress backup 22

4.10.5 Lokitiedostot 23

5 Pohdinta 24

Lähteet 26

Liitteet 29

Liite 1. Käyttöjärjestelmän ensimmäiset määritykset 29

Liite 2. Nimipalvelu DNS määritykset 31

Liite 3. Let’s Encrypt SSL-sertifikaatin käyttöönotto 34

Liite 4. MySQL asennus ja määrittely 39

Liite 5. Postfix:n määrittely 42

Liite 6. Dovecot:n määrittely 47
Liite 7. Wordpress asennus ja määrittely 52
Liite 8. Käyttäjän Opas 60

Keskeiset termit ja käsitteet

A tietue	Palvelimen IP-osoite johon domain ohjataan, arvo on aina IP-osoite.
Apache	Avoimeen lähdekoodiin perustuva HTTP-palvelinohjelma. Apache on Apache Software Foundation (ASF) lisensoima vapaa ohjelmisto. Maailman http-palvelimista 50,6% on toteutettu Apachella. (W3Techs 2017.)
APT	Advanced Package Tool, Ubuntussa toimiva paketinhallintatyökalu
BYOD	Bring your own device, käytäntö, jossa työntekijä käyttää omaa laitettaan työtä tehdessään.
CNAME	Tietue, joka liitetään domainnimeen, esim www.oopperskaala.fi → oopperaskaala.fi
Cron	Ubuntussa toimiva ajastuspalvelu, jolla voidaan ajastaa tietty toiminto tapahtumaan tietyllä ajalla.
DNS	Domain Name System, nimipalvelujärjestelmä, joka muuttaa verkkotunnuksia IP-osoitteiksi.
Document root	Hakemisto missä on Apache HTTP-palvelimen talletetut tiedostot.
Domain	Verkkotunnus, esim. oopperaskaala.fi
Dovecot	Avoimen lähdekoodin IMAP ja POP3 sähköpostipalvelin.
FQDN	Fully qualified domain name, käytössä olevan koneen tarkka nimi, esim. www.oopperaskaala.fi.
FTP	File Transfer Protocol, tiedonsiirtoon käytettävä protokolla, heikkoutena ettei sisällä salausta.
GNU	GNU's Not Unix, projekti, jonka tavoitteena on kehittää täysin vapaa käyttöjärjestelmä. "GNU is Not Unix". GNU on projekti, jonka tarkoitus on tarjota täysin ilmaisia ohjelmia ja käyttöjärjestelmiä. (GNU 2014.) GNU projekti sai alkunsa 1984, kun Richard M. Stallman aloitti projektin tavoitteenaan kehittää UNIX-käyttöjärjestelmä, joka olisi vapaasti levitettävissä. (Negus 2012, 11.) Unix-tyylisen käyttöjärjestelmän kehittäminen vaatii useita erillisiä ohjelmia, mikä johti vuonna 1985 Free Software Foundation perustamiseen, jonka päätarkoituksena oli kerätä rahoitusta GNU kehitykselle. (GNU 2014.)

GPL	General Public License, vapaiden ohjelmien julkaisemiseen tarkoitettu lisenssi.
IMAP, IMAPS	Internet Message Access Protocol, sähköpostien lukemiseen tarkoitettu protokolla.
Latenssi	Aika, jossa tietoliikennepaketti kulkee lähettäjältä vastaanottajalle ja takaisin. Voidaan mitata esim. ping-komennolla.
Linux	Linux-ydintä käyttävä käyttöjärjestelmä. Linuxin ensimmäinen julkinen versio julkaistiin 1991. Linus Torvalds julkaisi Mimix-versionsa, josta myöhemmin kehittyi Linux. Linux oli tarkoitettu vain 386 prosessoreille, mikä tarkoitti, että Unix-tyylistä käyttöjärjestelmää voitiin käyttää kotikoneissa. Järjestelmän tärkein osa ydin oli saatavilla ja se oli lisensoitu GPL lisenssin alle. (Negus 2012, 13-14.)
Linux-jakelut	Linux-jakelut (distributions) perustavat yleiseen ytimeen (kernel) mutta muut ohjelmistot vaihtelevat jakelun mukaan. (Nemeth, Snyder, Hein & Whaley 2010, 9.)
LTS	Long Term Support, Ubuntun käyttämä termi jola tarkoitetaan pidennettyä, kolmen vuoden tukea.
MySQL	Avoimen lähdekoodin relaatiotietokantaohjelmisto.
MX	MX-tietue määrittää domainin sähköpostipalvelimen.
OpenSSL	Avoimen lähdekoodin SSL ja TLS toteutus.
PHP	Avoimen lähdekoodin ohjelmointikieli, jota käytetään web-sivujen luonnissa.
Postfix	Avoimen lähdekoodin sähköpostin välitysohjelmisto.
Root	Ubuntun pääkäyttäjä.
SSH	Secure Shell, salattuun tietoliikenteeseen tarkoitettu protokolla. SSH mahdollistaa etäyhteyden palvelimelle. SSH avulla voidaan luoda autentikoitu yhteys palvelimen ja käyttäjän välille. Yhteys on turvallinen ja sen avulla voidaan käyttää ja siirtää tiedostoja järjestelmien välillä. SSH korvaa vanhemman Telnet-protokollan. (Vacca, 2009, 73-74.)
SSL	Secure Sockets Layer, Katso TLS.
sudo	Ohjelma, jolla voidaan suorittaa komentoja toisen käyttäjän oikeuksilla.
TLS	Transport Layer Security, aiemmin tunnettu nimellä SSL. Salausprotokolla, jolla suojataan internet yli toimiva tietoliikenne.
Ubuntu	Ubuntu käyttöjärjestelmä perustuu Linux-ytimeen. Ubuntua sponsoroi Canonical Software. Ensimmäinen Ubuntu versio

	tehtiin 2004. Ubuntu perustuu Debian-jakeluun, joka on yksi luotetuimmista jakeluista. (Helmke, 2015, 39.)
UFW	Uncomplicated Firewall, Ubuntun palomuurin hallinta ohjelma.
Unix	Laitteisto riippumaton käyttöjärjestelmä. Linux perustuu Unix käyttöjärjestelmään. Unix-käyttöjärjestelmän ensimmäiset piirteet olivat 1965 aloitetussa MULTICS-käyttöjärjestelmässä. MULTICS:n projekti hiipui 1969 isojen toimijoiden jätettyä projektin. Dennis Ritchie ja Ken Thompson jatkoivat käyttöjärjestelmän kehittämistä ja vuonna 1970 valmistuva versio sai nimen UNICS ja myöhemmin nimi taipui UNIX muotoon. UNIX sai nykyisen muotonsa 1973 ja se tuki useita käyttäjiä sekä laitteistoriippumattomuutta. (Kuutti 2007, 5.) UNIX-käyttöjärjestelmän kehitys suunnattiin avoimeen suuntaan, AT&T, joka oli yksi MULTICS projektin alkuperäisistä jäsenistä, pyrki kaupallistamaan UNIX-käyttöjärjestelmää mutta yhteisön tuoma avoimuus ja jatkokehittäminen jatkoivat kasvuaan. (Negus 2012, 7-8.)
VPS	Virtual Private Server, virtuaalipalvelin.
Wordpress	Wordpress on suosittu avoimen lähdekoodin ohjelmisto, jolla voidaan toteuttaa näyttäviä http-sivustoja. Alustana Wordpress on avoin, kevyt ja nopea sisällönhallintajärjestelmä. Alun perin Wordpress oli suunniteltu blogeja varten mutta nykyisin se toimii kokonaisena sisällönhallintajärjestelmänä. (Wordpress.org)

Johdanto

Opinnäytetyön aiheena on tuottaa Ooppera Skaala ry:n uusi palvelin. Tällä hetkellä Skaalan käytössä oleva palvelin ei toimi toivotulla tavalla. Nykyinen palvelu on ostettu ulkoiselta toimittajalta, mutta tarpeet eivät kohtaa palvelun vaatimia tavoitteita. Webhotellina ostettu palvelu ei mahdollista ongelmanratkaisua muuten, kuin ostamalla lisää palveluita toimittajalta, eräänlainen toimittajariippuvuus. Erityisesti ongelmaksi on muodostunut Wordpressiin kohdistunut jatkuva ”häkkeröinti”. Vika sinänsä ei ole palveluntarjoajassa, mutta heidän automatiikka sulkee sivuston, jos haittakoodia löydetään. Sivustoa ei pääse käyttämään tai korjaamaan, ennen kuin on soittanut ja toimittanut korjaustoimenpiteet toimittajalle. Tästä on seurannut ”oravanpyörä” vikatilanteissa, mikä taas on johtanut siihen, että vikatilanteissa websivusto on ollut poissa käytössä useita päiviä.

Omalla palvelimella voidaan toteuttaa halutut toimenpiteet itsenäisesti. Palvelimen avulla tuotetaan Skaalan websivusto sekä sähköpostipalvelut. Websivusto toimii tärkeänä osana Skaalaan markkinointia ja tiedotusta yhdessä sosiaalisen median kanssa. Samoin sähköposti on olennainen osa yhdistyksen toimintaa esim. sähköpostilistojen muodossa. Nykyinen webhotelli tarjoaa palvelimen perusominaisuudet, mutta myös puutteita löytyy, kuten SSH mahdollisuuden käyttäminen.

Uuden palvelimen hankinnan ohella muodostetaan pohja Skaalan IT-strategialle, jolla pyritään luomaan kestävä pohja Skaalan IT-toiminnoille, sekä varmistamaan IT:n toiminallisuus ja kehitys jatkossa.

Nykyinen palvelin on ostettu Suomesta, mikä on mahdollistanut tuen suomeksi mutta tuki on pääsääntöisesti tehtävä puhelimella, mikä taas on ollut erikseen maksullista. Uusi palvelin hankitaan todennäköisesti Euroopasta. Uudella palvelimella on tikettipohjainen tukipalvelu, mikä mahdollistaa ilmaisen tuen tai tuen maksullisuuden kyselyn. Uusi palvelin on huomattavasti tehokkaampi nykyiseen verrattuna, silti palvelun hinta on selkeästi edullisempi nykyiseen verrattuna. Palvelimia testattiin etukäteen muutamasta Euroopan maasta, vaikka testatut palvelimet olivat hinnaltaan ja kapasiteetiltaan kevyimmästä päästä, todettiin että palvelimien tehot ovat riittävät yhdistyksen tarkoitukseen. Valittu palvelin ylitti tehovaatimukset selvästi ja 2 viikon testiajanjaksolla ei huomattu yhtäkään virhettä palvelimen toiminnassa.

1 Tavoitteet

Opinnäytetyö on toiminnallinen ja tarkoituksena on tuottaa tietoturvallinen web-palvelinympäristö, joka sisältää Wordpress sisällöntuotanto järjestelmän ja Postfix sähköpostipalvelimen.

Tutkimuskysymykset:

Miten asennetaan tietoturvallinen webpalvelin sähköposti- ja webominaisuuksilla?
Mitä ohjelmia tarvitaan web- ja sähköpostipalvelimen luotettavaan toimintaan?
Voidaanko pienen yhdistyksen web- ja sähköpostipalvelin toteuttaa open source ohjelmilla?

Opinnäytetyön tuloksena syntyy internetissä toimiva sähköposti- ja webpalvelin. Opinnäytetyö tuottaa pienelle organisaatiolle dokumentaation, jonka avulla voidaan asentaa sekä ylläpitää tietoturvallista palvelinympäristöä.

Vanhasta palvelimesta ei siirretä mitään tietoa uudelle palvelimelle. Vanhan palvelimen Wordpress ohjelmisto on ”häkkeröity” useaan kertaa, eikä mahdollisia haittaohjelmia ole pystytty paikantamaan. Tämän takia uudelle palvelimelle ei siirretä tietoja vanhalta palvelimelta, vain muutamia tarvittavia tiedostoja, sekä muutama ostettu lisäohjelma asennetaan myös uuteen palvelimeen.
Sähköpostien osalta päädyttiin siirtämään vanhan palvelimen tarvittavat sähköpostit käyttäjien omille tietokoneille. Käyttäjät ohjeistettiin tekemään paikallinen arkisto omalle tietokoneelleen, ja sen varmistaminen esim. ulkoiselle usb-levylle.

2 Palvelimen merkitys Skaalalle

Palvelimen on tarkoitus tuottaa www-sivusto ja sähköpostipalvelut, sekä mahdollisuus muihin palveluihin tulee huomioida tulevaisuutta varten. Www-sivut ovat yhdistyksen tärkein informaatiokanava sosiaalisen median ohella. Toiminallisella työllä haetaan riippumattomuutta palveluntarjoajaan, sekä mahdollisuutta ylläpitää palveluja itsenäisesti, etenkin tietoturva ja dokumentointi huomioiden. Kysymyksessä on pieni yhdistys, joten kulujen on pysyttävä pienenä. Kulujen minimoiseksi palvelut toteutetaan avoimen lähdekoodin ohjelmistoilla ja Linux-käyttöjärjestelmällä. Myös tietoturvan kannalta avoin lähdekoodi ja Linux ovat hyvä lähtökohta järjestelmälle.

Käyttöjärjestelmänä toimii Ubuntu ja sisällönhallintajärjestelmänä Wordpress. Dokumentaatio ja strategian suunnittelu mahdollistavat palvelimen uudelleen asennuksen sekä sijoittamisen toisen palveluntarjoajan palvelimelle muutaman tunnin viiveellä. Palvelimen yksinkertainen rakenne, sekä varmistusten palauttaminen mahdollistavat tämän.

2.1 Palvelimen, käyttöjärjestelmän ja ohjelmistojen valinta

Toimeksiantajalta on tullut muutama edellytys, joita toimeksiannossa noudatetaan.

1. Wordpress, ohjelma jota yhdistyksen työntekijät ovat tottuneet käyttämään. Wordpress on hyvä valinta, eikä sen takia tarvita erillistä koulutusta http-sivujen tekijöille. Yhdistyksellä on muutama ostettu plugin, joita voidaan myös käyttää uudessa palvelimessa.

2. Ylläpito, palvelimen ylläpidon tulisi olla mahdollisimman helppoa. Palvelinta ylläpidetään yhdistyksen tekijöiden toimesta, joten kaikki aika, joka käytetään ylläpitoon, on pois muusta tekemisestä.

3. Kustannus, palvelin ei suoranaisesti tuota rahaa vaan on osa markkinointia. Tällä hetkellä palvelimen kulut ovat n. 100e vuosi, mikä on hyväksytty kuluerä.

Palvelimeksi hankitaan VPS palvelin Euroopasta. Hinta vaikuttaa huomattavasti valintaan, palvelimen kapasiteetti on huomattavasti tehokkaampi kuin vastaavalla hinnalla Suomesta saatavilla olevissa palveluissa. Palvelimia testattiin Suomesta (nykyinen palvelin), Ruotsista, Liettuasta ja Hollannista. Testaus suoritettiin asentamalla tarvittavat ohjelmat palvelimelle ja toteamalla palvelut toimiviksi. Tarkkaa statistiikkaa ei hankittu, lähinnä tarkistettiin, että verkon nopeus ja vasteajat ovat toimivia, prosessori sekä muistin käyttö riittävää.

Ruotsista ja Liettuasta palvelimet saatiin testien ajaksi käyttöön ”rahat takaisin” periaatteella, jota käytimme hyväksi Ruotsin kohdalla. Hollannista ostimme palvelimen yhdeksi kuukaudeksi hintaan 5 US$. Testit haluttiin suorittaa, jotta edes pieni varmuus VPS toiminnasta saataisiin. Testien perusteella Liettuan palvelin oli selkeä valinta kaikilla toivotuilla kriteereillä. Lopullinen palvelin päätettiin hankkia Liettuasta, perusteluina hinta, teho, kapasiteetti ja maantieteellinen läheisyys. Yleisesti kaikki testatut palvelimet toimivat erinomaisesti ja olisivat teknisesti hyvin toimivia valintoja http-palvelimeksi.

Käyttöjärjestelmäksi valittiin Linux. Http-palvelimena Linux on selkeä vaihtoehto jo kustannussyistä. Linux on toimiva pohja kaikille yhdistyksen tarvittaville ohjelmistoille, samoin Linuxin maine toimivana http-palvelimena on huomioitu.

2.2 Palvelimen rakenne

Palvelimen käyttöönotto vaatii VPS palvelimen hankinnan, domain/DNS määrittelyn sekä käyttäjärjestelmän asennuksen. Palvelimen asentaminen tehdään kolmessa osassa.

Palvelin otetaan käyttöön kolmessa vaiheessa.

- Palvelimen hankinta ja luonti, domain/dns määrittely. Käyttöjärjestelmän asennus.
- Palvelimen ohjelmistojen riippuvuudet, MySQL, PHP ja SSL.
- Palvelimen ohjelmistot, Apache, Postfix, Dovecot ja Wordpress.

Ensimmäisessä osassa valmistellaan itse palvelin ja sen käyttöjärjestelmä Ubuntu, sekä nimipalveluun liittyvät asiat. Tässä vaiheessa luodaan käyttäjät ja määritellään SSH-palvelut tehokkaampaa etäkäyttöä varten.
Toisessa osassa asennetaan palvelimen vaatimat riippuvuudet, MySQL, PHP ja SSL. Samalla varmistetaan, että päivitykset ovat ajan tasalla ja valmistaudutaan asentamaan ohjelmistot.
Kolmannessa vaiheessa asennetaan ja viimeistellään palvelin, asentamalla Postfix, Dovecot, Wordpress sekä viimeistellään asetukset.

3 Tietoturva

Tietoturva on olennainen osa tietoteknistä ympäristöä, koska produkti sisältää ainoastaan yhden palvelimen käydään läpi tietoturvaa, joka läheisesti koskee tätä tuotantoa. Tietoturva on erittäin laaja-alainen käsite ja produktin ollessa hyvin pienimuotoinen, käsitellään tietoturvaa osilta jotka koskettavat produktia eniten. Yhdistyksen IT-infraan ei ole suunnitteilla uusia palvelimia tai muita laitteita, joten suunnitellaan yhdistykselle tämän hetken kattava tietoturva ohjeistus.

Tietoturvan kohdalla keskitytään neljään kohtaan.

- Kenellä on pääsy palvelimelle ja kuinka sitä valvotaan.
- Sähköposti ja sen eheys.
- Wordpress ja sen tietoturva.
- Käyttäjien opastaminen.

Palvelimelle pystyvät kirjautumaan kolmella eri tunnuksella, root ja asennuksen aikana tehty ”adminx” tunnus sekä myöhemmin tehtävällä tunnuksella wp-user. Palvelimelle kirjautuminen tapahtuu joko VPS toimittajan web-hallinnan kautta tai SSH yhteyttä käyttäen. Root tunnus ei pysty kirjautumaan SSH kautta (kirjautuminen estetään asennus vaiheessa), eikä adminx/wp-user pysty kirjautumaan web-hallinnan kautta. Kirjautumisia valvotaan palvelimen tuottamien lokien tiedoista. Koska tunnuksia on vain kolme, on niiden seuraaminen helppoa sekä mahdollisten väärinkäytösten havaitseminen nopeaa.
Sähköposti kirjautuminen tapahtuu sähköposti-osoitteella, kirjautuminen tapahtuu MySQL tietokannan kautta eikä sähköpostitunnuksilla pysty kirjautumaan palvelimelle. Sähköpostin salasana ei ole käyttäjän vaihdettavissa, vaan salasanan voi ainoastaan vaihtaa pääkäyttäjä. Sähköpostin käytöstä on erillinen ohjeistus käyttäjille.
Tietoturvan kannalta Wordpress on haasteellinen, sillä Wordpress on suosittu ohjelmisto ja sitä vastaan on paljon erilaisia haitakkeita olemassa, myös päivityksiä tulee usein, mitkä ovat suositeltavaa asentaa heti niiden ilmestyessä. Lisäosien turvallisuus on tarkistettava ennen niiden käyttöä sekä asennettava ainoastaan turvallisia lisäosia.
Käyttäjille tehdään oma ohjeistus palvelimen käytöstä, joka sisältää kirjautumisen palvelimelle, sähköpostiin sekä yleisiä ohjeita.

3.1 Tietoturvan osa-alueet.

Tietoturva on perinteisesti jaettu kahdeksaan osa-alueeseen seuraavasti:

Hallinnollinen tietoturva
Henkilöstötietoturva
Fyysinen tietoturva
Tietoliikennetietoturva
Laitteistotietoturva
Ohjelmistotietoturva
Tietoaineistoturvallisuus
Käyttöturvallisuus
(Andreasson, 2013, 52.)

Laitteistotietoturva ja henkilöstötietoturva käsitellään tarkemmin, koska ne liittyvät ensisijaisesti produktiin. Yhdistyksen palvelin on sijoitettu palveluntarjoajan tiloihin, fyysisen tietoturvan kannalta ei yhdistyksellä ole erillistä sopimusta eikä muitakaan täsmällisiä tietoja, miten palvelin on suojattu fyysisesti (palveluntarjoajan www-sivuilla on yleisesti esittely tietoturvasta, esim. kulunhallinta, varavoima jne.).

Laitteistoturvallisuus käsittää laitteistoon liittyvää turvallisuutta. Laitteisto voi olla esim. tietokone, älypuhelin, tulostin, modeemi. Myös ylläpito ja tuki, kuuluvat laitteistotietoturvan piiriin. (Andreasson, 2013, 65.)

Yhdistyksellä ei ole omia laitteita eikä ohjelmistoja, vaan käyttäjät käyttävät omia laitteita (BYOD).
Omien laitteiden käyttö on otettava huomioon tietoturvassa. Omien laitteiden tukeminen on hankalaa, koska niitä ei ole vakioitu, vaan laitteet voivat sisältää mitä tahansa käyttäjien käyttämiä sovelluksia. Vikatilanteissa ongelmien ratkominen mutkistuu ja selvitystyö hankaloituu, koska ei ole tarkkoja tietoja käytettävistä laitteista tai sovelluksista.
Yhdistyksen järjestelmiin liittyvien laitteiden tietoturvakomponenttien tulisi olla määritelty, mutta se vaatii, että yhdistyksellä on määritelty ja hallittu tietoturvastrategia. Tietojen omistajuus voi olla ongelma omien laitteiden kanssa, miten erotella henkilökohtaiset- ja työtiedot. (Andreasson, 2013, 66-67.)

Yhdistyksellä ei ole tietoteknisiä henkilöitä töissä, joten ohjeistuksesi määriteltiin, että käyttäjien on pidettävä laitteensa päivitettynä. Samoin omat tiedostot ja sovellukset ovat pidettävä päivitettyinä, sekä yleisesti käyttäjien on huolehdittava omien laitteiden tietoturvasta. Omat tiedostot tulisi eritellä työtiedostoista ja mahdollisuuksien mukaan varmistettava työtiedostot säännöllisesti.

Tietoturvastrategian on syytä mainita asioita ja vastuita mitkä jäävät käyttäjän hallittaviksi, esim.

- Selvittää mitä IT-osasto voi ja ei voi tehdä käyttäjän laitteelle.
- Hyväksyttää käyttäjällä yhdistyksen menettelytavat.
- Kouluttaa käyttäjät laitteiden käyttöä varten.
- Mahdollistaa laitteiden ja tietojen tietoturvallinen käyttö.
- Kertoa miten käyttäjä voi käyttää laitteitta vastuullisesti. (O'Hanley, 2013, 136.)

3.2 Linux

Ubuntu on yleisesti tietoturvallinen järjestelmä, mutta se vaatii jatkuvaa ylläpitoa. Tietoturvan näkökulmasta määriteltiin seuraavat toimenpiteet suoritettavaksi.

Käyttöjärjestelmän ja sen sisältämien ohjelmistojen tietoturva määriteltiin seuraavasti:

- Ubuntu ja ohjelmistot päivitetään vähintään kerran viikossa (apt-get).
- SSL-sertifikaatti päivitetään kerran kuukaudessa.
- Salasanojen päivittämiseen ei määritelty rajoituksia. Salasanat luo pääkäyttäjä, jolta voi tarvittaessa pyytää salasanan vaihtoa. Nykyiset salasanat ovat riittävän turvallisia.
- Palomuurin toiminta tarkistetaan lokeista kerran viikossa.
- Lokien läpikäynti kerran viikossa.
- Varmistus luodaan kerran viikossa (Wordpress ja MySQL). Palveluntarjoaja varmistaa kaikki tiedot päivittäin.
- Satunnaiset testit kuten SSL-sertifikaatin toiminta tai porttien avoimuus tarkistetaan satunnaisesti.

Päivitystä varten luodaan tarkistuslista, jota seuraamalla voidaan essldetä päivitysten tekemistä.

4 Toiminnallinen osuus / Palvelimen asennus

4.1 VPS

Virtuaalipalvelin hankittiin Time4vps palveluntarjoajalta Liettuasta. Time4vps valittiin koska se oli edullinen mutta täytti silti myös muut kriteerit. Kriteereinä seuraavat vaatimukset:

- maantieteellinen läheisyys, Eurooppa minimi vaatimus.
- verkon nopeus ja yleinen toimivuus.
- palvelimen teho ja suorituskyky.
- palvelimen tehokas etähallinta.
- palvelimen ominaisuuksien muokattavuus.
- palvelimen hinta.

Maantieteellisellä läheisyydellä haettiin mahdollisimman pientä latenssia palvelimen ja käyttäjien välille. Lähes kaikki palvelimen käyttäjät ovat Suomesta, joten latenssin on oltava pieni, etenkin Suomeen tapahtuvassa liikenteessä.
Verkon nopeudella ja yleisellä toimivuudella haettiin yleisesti verkon toimivuutta. Verkon jatkuva toimivuus ilman katkoja tai pätkimistä oli tärkeä kriteeri. Verkon nopeus ei ollut suuri tekijä, sillä palvelimen www-sivusto ei ole erityisen raskas eikä se vaadi kaistanleveyttä. Etukäteen arvioitiin, että 10Mbps kaistalla palvelin toimisi luotettavasti, vaikka palvelimella olisi useita käyttäjiä. Palvelimen verkkoyhteys on toteutettu 400Mbps yhteydellä, mikä ylittää reilusti minimikriteerin.
Time4vps palvelin on myös riittävän tehokas ajamaan useita http-sivustoja samaan aikaan. Nykyinen http-sivusto ei rasita palvelinta, samoin muistikäyttö on n. 15% tasolla.
Etähallinta voidaan suorittaa tehokkaasti SSH-yhteyden avulla tai hallintapaneelista selaimen avulla. Etähallintaan ei ole mitään rajoituksia, hallintaa voidaan käyttää omilla työkaluilla.
Palvelimen ominaisuuksia voidaan muuttaa hallintapaneelin kautta. Esimerkiksi voidaan lisätä levytilaa tai muistia palvelimeen, joka saadaan käyttöön heti.

Palvelinta myös testattiin n. kahden viikon ajan, jolloin totesimme palvelimen vastaavan luvattua palvelua. Samoin tuki toimi kuten luvattu, kahden viikon testaus on varsin lyhyt aika, mutta Skaalan tapauksessa ei ole kyse kriittisestä palvelusta, joten totesimme palvelun olevan riittävä. Palvelinten vertailussa ei käytetty erinäisiä testiohjelmia, vaan tarvittavat palvelut asennettiin palvelimille ja asennuksen yhteydessä todettiin asennusten sekä palveluiden toimivuus. Kaikki testatut palvelimet täyttivät yhdistyksen ohjelmien toiminnan kannalta tarvittavat vaatimukset, valittu palvelin ylitti vaatimukset sekä tarjosi muutaman

yksityiskohdan, mitä taas ei ollut muilla toimittajilla. Valittu palvelu oli selkeästi paras edellä mainituilla kriteereillä.

Valitun palvelimen tietoja:

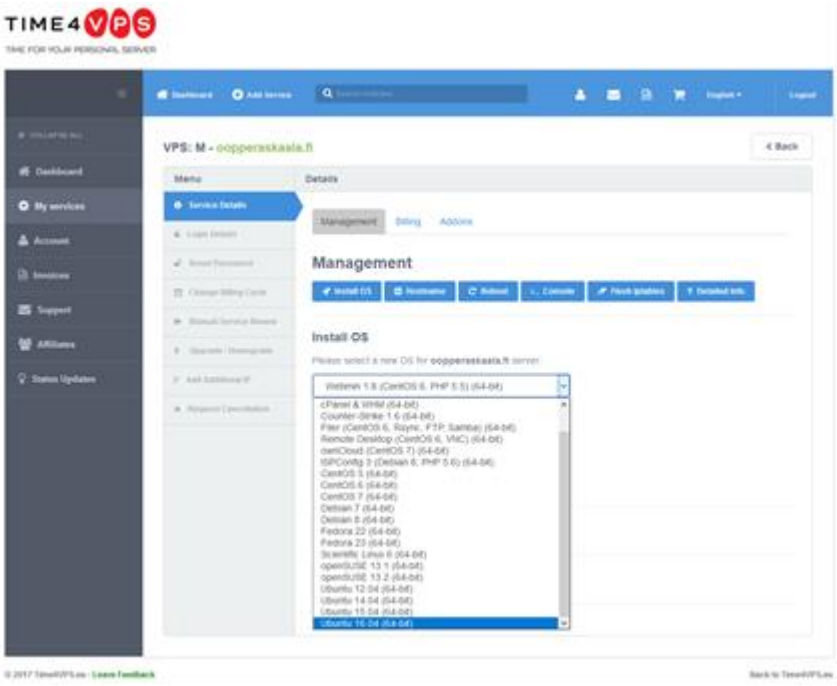
Käyttöjärjestelmä:	Ubuntu 16.04 64bit
Prosessori:	2x 2.40 GHz (4.80GHz taattu)
Muisti:	2048 MB ram + 1024 MB swap
Kiintolevy:	80 GB RAID
Verkon nopeus:	400 Mbps
Siirto/kk	2 TB

Palvelimen tehot ovat hivenen ylimitoitettu nykyiseen tarpeeseen, mutta näin mahdollistetaan mahdolliset uudet palvelut ilman lisäkuluja tulevaisuudessa.

Käyttöjärjestelmänä on Linux Ubuntu 16.04 64bit LTS. Palveluntarjoajalla on valmiina esiasennusta varten useita levykuvia, joista valinta on Ubuntu LTS versio.
Palvelimelle asennetaan uusin Wordpress (4.72), ennen Wordpressin asennusta asennetaan muut vaadittavat sovellukset. Sähköposti palvelimeksi on valittu Postfix/Dovecot yhdistelmä. Http-palvelimeksi Apache2. Postfix ja Wordpress käyttävät MySQL tietokantaa. Wordpress vaatii myös PHP toimiakseen.

4.2 Ubuntu

Ubuntussa yhdistyy Debianin luotettavuus sekä Ubuntun yleisyys ja hyvä yhteisön tuki. Ubuntu tukee kaikkia ohjelmia, joita käytämme palvelimella ja testit tehtiin Ubuntulla, eikä ongelmia ilmennyt. Palvelin asennetaan palveluntarjoajan web-hallinnan kautta. Kuva 1.



Kuva 1. VPS toimittajan web-hallinta, asennettavan käyttöjärjestelmän valinta ikkuna

Alasvetovalikosta valitaan haluttu käyttöjärjestelmä ja asennus on valmis muutaman minuutin päästä. Asennuksen jälkeen web-hallintaan tule näkyviin salasana, jolla palvelinta voi alkaa käyttää, joko web-hallinnan kautta luodulla etäyhteydellä tai SSH:n kautta.

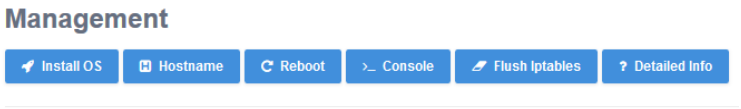
4.3 Verkkotunnus

Ooppera Skaala ry omistaa oopperaskaala.fi verkkotunnuksen, joka tullaan liittämään uuteen palvelimeen. Nimipalvelu (DNS), joka muuttaa verkkotunnuksen IP-osoitteeksi on ostettu webhotelli.fi palveluntarjoajalta. Nimipalvelut määritellään webhotelli.fi web-hallinnassa heti, kun uuden palvelimen IP-osoite on selvillä. Verkkotunnus on oleellinen osa palvelinta, sähköposti vaatii FQDN toimiakseen, samoin SSL käyttö ilman verkkotunnusta olisi tarpeetonta.
Verkkotunnus on rekisteröity vanhalle palveluntarjoajalle. Sopimus vanhan palveluntarjoajan kanssa loppuu loppuvuodesta 2017. Verkkotunnus täytyy siirtää toiselle välittäjälle, ennen sopimuksen loppumista. Muutosta ei kuitenkaan tehty tässä yhteydessä, mutta se on tehtävä, sillä vanhalla palveluntarjoajalla ei ole sopivaa palvelua, millä voisimme jatkaa uuden palvelimen kanssa. Osa määrityksistä on mahdollista tehdä vain vanhan palveluntarjoajan IP-osoitteisiin, mikä taas ei tue uuden palvelimen toimintaa.

4.4 Palvelimen määrittely ja käyttöönotto

Kun palvelin on asennettu, määritellään palvelimen asetuksia. Tarkat ohjeet määrityksistä on dokumentoitu seitsemään liitteeseen, jotka ovat osa tätä raporttia. Liitteet sisältävät lyhyen ohjeen ja itse komennot, miten tietty määritys tulee tehdä.

Ensimmäinen kirjautuminen tehdään web-hallinnan kautta ”Console” kohdasta. Kuva 2.



Kuva 2. Web-hallinnan valikko

Selaimeen avautuu palvelimen terminaali, johon kirjaudutaan root tunnuksella ja asennuksen jälkeen saadulla salasanalla.

Pääkäyttäjänä (root) ei ole suositeltavaa käyttää palvelinta, turvallisuussyistä rootin kirjautuminen estetään SSH-palvelimelle. Pääkäyttäjän tunnusta voidaan käyttää tarvittaessa, mutta se edellyttää, että käyttäjä on liitetty sudoers ryhmään. Pääkäyttäjän tilillä ei silti-kään ole suositeltavaa antaa komentoja, vaan käyttää sudo komentoa, jos pääkäyttäjän oikeuksia tarvitaan.
Käyttäjät, jotka ovat sudoers ryhmässä, voivat suorittaa komentoja toisen käyttäjän oikeuksilla, yleensä tätä käytetään, kun tarvitaan pääkäyttäjän oikeuksia esim. päivityksien asentamiseen.
Palvelimelle tehdään ensiksi käyttäjä, jota käytetään palvelimen ylläpidossa sekä määrittelyssä (tämä käyttäjä lisätään sudoers ryhmään). Koska tällä käyttäjällä on oikeus käyttää pääkäyttäjän oikeuksia, nimetään tunnus tyyliin, oikean etunimen ensimmäinen kirjain ja 2 ensimmäistä kirjainta sukunimestä = aha.

Uuden käyttäjän lisäämiseen käytetään adduser komentoa, joka on Ubuntussa oletuksena asennettuna. Adduser komento on komentoriviltä suoritettava käyttäjien lisäämiseen tarkoitettu komento. Uudelle käyttäjälle on tärkeää antaa riittävän turvallinen salasana samalla kun uusi käyttäjä luodaan. Käyttäjän luontia varten tarvitaan root-käyttäjän oikeudet, uusi käyttäjä lisätään sudoers ryhmään, minkä jälkeen voidaan käyttää muuta kuin root-käyttäjää. (Nemeth, Snyder, Hein & Whaley 2010,188-189.)

LIITE 1. sisältää tarkemmat määritykset.

Asennuksen ensimmäisessä vaiheessa määritellään:

- Uusi käyttäjä ja lisätään uusi käyttäjä ”sudoers” ryhmään.
- Asennetaan tekstieditori (nano).
- Palomuurin hallintaohjelmisto (ufw).
- Päivitetään järjestelmä (apt).

- Asennetaan SSH-palvelin (openssh-server).

Toimenpiteet suoritetaan web-konsolista root-tunnuksella. Asennus järjestyksellä ei ole sinänsä väliä, kunhan lopputuloksena on:

- Teksti-editori, jolla voidaan editoida tekstitiedostoja.
- SSH-palvelin on päällä ja oikea portti on avattu, jolla SSH-palvelimelle pääsy sallitaan.
- Etäyhteys SSH-palvelimeen on estetty root-tunnukselta.
- Palvelimelle luotu uusi käyttäjä, jolla on oikeudet ”sudo” komennon suorittamiseen.
- Päivitykset on tehty tai tehdään seuraavaksi.

4.4.1 Asennetaan määrittelyssä tarvittavat ohjelmat

Asennetaan nano tekstieditori, jolla voidaan tehdä loput ohjeessa olevat määritykset. Huom. mikä tahansa tekstieditori käy, nano on pieni ja helppokäyttöinen.

UFW (Uncomplicated Firewall) on palomuurin hallintaohjelma, joka tarjoaa perusominaisuudet palomuurin hallintaan käyttäjäystävällisellä tavalla. UFW on oletuksena asennettu Ubuntuun, mutta se ei ole käynnistetty. (Ubuntu.com. 2017.)
Käynnistetään UFW ja määritellään tarvittavat asetukset. Erityisesti SSH-palvelimen portin avaaminen on huomioitava.

APT komennolla voidaan asentaa, poistaa tai päivittää ohjelmistoja Ubuntussa. APT komento toimii SSH yhteyden yli, mikä mahdollistaa järjestelmien hallinnan etäyhteyden päässä oleviin palvelimiin. (Ubuntu.com. 2017.)
Palvelimen päivitys tehdään kolmella, terminaalissa annetulla komennolla.

- apt-get update, jolla päivitetään pakettilista. Tämä komento on hyvä ajaa aina kun, palvelimelle kirjaudutaan ja etenkin ennen kuin paketteja asennetaan tai päivitetään. Komento päivittää uusimmat, saatavilla olevat paketit.
- apt-get upgrade, järjestelmään asennetut paketit päivitetään. Komennolla päivitetään uusimmat paketit, jotka ovat pakettilistalla. Jos edellistä komentoa ”apt-get update” ei ole ajettu, ei myöskään ole tietoa uusista paketeista.
- apt-get upgrade, suoritetaan järjestelmän päivitys. Komennolla päivitetään järjestelmä, siten että myös tarvittaessa vanhempia paketteja poistetaan ja päivitetään samalla. (Ubuntu.com. 2017.)
-

OpenSSH Server, palvelimen avulla voidaan muodostaa etäyhteys ja siirtää tiedostoja turvallisesti internetissä olevien koneiden välillä.

Kirjaudutaan palvelimelle SSH-yhteyden avulla. Ei käytetä root tunnusta vaan luomaamme aha tunnusta.
SSH-palvelin toimii oletuksena portissa 22, avasimme edellisessä kohdassa portin 22 palomuurista (UFW allow ssh). Samalla avasimme portin 22222, jota tulemme käyttämään oletus SSH-palvelimen porttina. Yksinkertainen syy on, että porttiin 22 tulee iso määrä yhteyksiä tuntemattomista osoitteista. Portin vaihto, sekä root tunnuksen käytön estäminen lisää tietoturvaa.
Huom. Tarkista ennen portin vaihtamista, että uusi portti on avoinna (sudo ufw status), jos portti 22222 ei ole listalla, lisää se (sudo ufw allow 22222).

4.5 Verkkotunnus Nimipalvelu / DNS määrittely

Nimipalvelujärjestelmä (DNS), jonka tarkoituksena on muuttaa IP-osoitteet helpommin muistettaviksi nimiksi. Palvelimella on oltava täysi domain nimi (FQDN), joka tässä tapauksessa on oopperaskaala.fi. (Ubuntu.com. 2017.)

Nimipalvelu on olennainen osa sähköposti- ja web-palvelimen toimintaa. Yhdistyksellä on käytössä oopperaskaala.fi osoite, jonka DNS hallinta on tällä hetkellä webhotelli.fi palvelussa. DNS määritykset tehdään webhotellin hallintapaneelissa selaimen kautta.

Lisätään A tietue oopperaskaala.fi johon liitetään palvelimen IP-osoite. Lisätään CNAME tietue www.oopperaskaala.fi, joka viitataan oopperaskaala.fi osoitteeseen. Lisätään CNAME tietue mx.oopperskaala.fi joka viitataan oopperaskaala.fi osoitteeseen.
Lisäksi määritellään MX tietue mx.oopperaskaala.fi sähköpostipalvelimen osoitteeksi. (Ubuntu.com. 2017.)

Muutokset tehdään seuraavasti:

oopperaskaala.fi.	900	IN	A	194.135.92.151
localhost.oopperaskaala.fi.	900	IN	A	127.0.0.1
mx.oopperaskaala.fi.	900	IN	CNAME	oopperaskaala.fi
www.oopperaskaala.fi.	900	IN	CNAME	oopperaskaala.fi

Sähköpostin MX asetus:

0 mx.oopperaskaala.fi

LIITE 2. sisältää tarkemmat määritykset.

4.5.1 Palvelimen hosts tiedoston ja aikavyöhykkeen määrittely

Ubuntun hosts tiedostolla määritellään palvelimen IP-osoite sekä isäntänimi. Hosts tiedosto pitää sisällään yksinkertaisimmillaan palvelimen IP-osoitteen ja domain nimen. (Ubuntu.com. 2017.)
Määritellään /etc/hosts-tiedoston tiedot vastaamaan DNS asetuksia:

127.0.1.1 oopperaskaala.localdomain oopperaskaala
127.0.0.1 localhost
194.135.92.151 oopperaskaala.fi www.oopperaskaala.fi mx.oopperaskaala.fi

Hosts tiedoston tietojen tulee vastata nimipalveluun annettujen tietojen kanssa. Hosts tiedoilla on

Palvelimen aikavyöhyke on CET, muutetaan se näyttämään Suomen aikaa ja asennetaan NTP (NetworkTimeProtocol), joka synkronisoi kellon oikeaan aikaa tarvittaessa. Postfix sähköpostipalvelin tarvitsee oikean ajan toimiakseen. Samoin lokien tarkistelu on helpompaa, kun aikaleimat perustuvat oikeaan aikaan.

4.6 SSL Let’s Encrypt-sertifikaatin asennus

SSL mahdollistaa turvallisen yhteyden käyttäjän selaimen ja http-palvelimen välille. SSL salaa yhteyden käyttäjän ja palvelimen välillä. Yhdistyksen web-palvelut eivät välttämättä vaadi salattua yhteyttä, mutta sertifikaatti luo luottamuksen asiakkaan toiminnalle. Lets Encrypt on ilmainen palvelu, mutta myös maksullisia sertifikaatin tarjoajia on runsaasti tarjolla. (Let’s Encrypt 2017.)

Let’s Encrypt:n ominaisuuksia ovat vapaa käyttö, eli kuka tahansa joka omistaa verkkotunnuksen voi hankkia SSL-sertifikaatin ilman kustannuksia ja automaattinen sertifikaatin päivittäminen turvallisesti. Avoimuus, tiedot virhetilanteista ja haavoittuvuuksista ovat yhteisön saatavilla ja tutkittavissa.
(Let’s Encrypt 2017.)

HTTP-palvelin toimii oletuksena portissa 80 ja käytössä on http-protokolla. SSL:n käyttöönotto vaatii, että portti 443 on auki ja myöhemmässä vaiheessa muutamme http-palvelimen oletusprotokollaksi HTTPS. Let’s Encrypt tarjoaa myös TLS varmenteen, jota käytämme sähköpostipalvelimen kanssa. Seuraavaksi asennamme Let’s Encrypt ohjelman GIT versionhallinnasta sekä haemme sertifikaatit.

LIITE 3. sisältää tarkemmat määritykset.

4.6.1 SSL-sertifikaatin automaattinen päivittäminen.

Let’s Encrypt-sertifikaatit ovat voimassa 90 päivää. Sertifikaatti voidaan päivittää koska tahansa, joten seuraavaksi luomme automatiikan, joka päivittää sertifikaatin 30 päivän välein. Samalla päivitämme Let’s Encrypt clientin päivittymään kerran viikossa. (Let’s Encrypt 2017.)

Clientin päivitys kerran viikossa antaa korjauksille aikaa, jos jokin vika havaitaan. Samoin 30 päivän päivitysrutiini antaa aikaa reagoida, jos päivitys jostain syystä ei onnistu itse sertifikaatin kohdalla. Kummatkin croniin lisättävät ajot lähettävät root:lle sähköpostin lokien kera. SSL on olennainen osa järjestelmää, kun http-palvelin on ohjattu näyttämään sivut https muodossa. SSL-sertifikaatin toimimattomuus antaisi jokaiselle sivun lataukselle virheilmoituksen sertifikaatin toimimattomuudesta.

Päivitys ei toimi, mikäli portti 443 on käytössä. SSL käyttää oletuksena porttia 443, joka on myös http-palvelimen käytössä. Tästä seurauksena päivitys ei toimi, ellei http-palvelinta pysäytetä. Ajastus muistuttaa 30 päivän välein, ettei päivitys onnistu, joten automatiikka jätetään päällä. SSL päivitys tehdään käsin, kunnes sovelluksen automatiikka on korjattu.

4.6.2 Apache Http Server

Apache http-palvelin tulee toimimaan Wordpressin alustana tuotettaessa web-sivuja. Apache on avoimen lähdekoodin http-palvelin, joka toimii olennaisena osana produktia. Apachen yhteensopivuus MySQL:n ja PHP:n kanssa sekä Apachen hyvä yhteisön tuki perustelevat sen valintaa http-palvelimeksi. (Ubuntu.com. 2017.)

Oletuksena Apachen sivut ovat palvelimella /var/www/html hakemistossa. Koska palvelimelle on tarkoitus tehdä myöhemmin useita virtuaalipalvelimia, muutetaan yhdistyksen ”document root” /var/www/”yhdistys”/public_html/ hakemistoon. Tämä mahdollistaa uusien virtuaalipalvelimien helpon hakemistokäytännön (/var/www/*domainnimi*/).
Samalla muutetaan hakemiston oikeuksia sekä tehdään esimerkkisivu, jolla testataan web-palvelimen toimivuus.
Viimeistellään virtuaalipalvelimen määritykset, lisätään testisivu ja conf tiedostot. (DigitalOcean 2016.)

4.6.3 SSL ja Apache2

Palvelimelle on hankittu SSL-sertifikaatti, sekä http-palvelin on asennettuna, määritellään apache käyttämään suojattua SSL-yhteyttä.
Palvelimelle on jo tehty Let's Encrypt-sertifikaatit, käytämme niitä. Käsitellään seuraavia tiedostoja:
/etc/apache2/conf-available/ssl-params.conf
/etc/apache2/sites-available/default-ssl.conf

- Luodaan ja muutetaan oikeuksia dhparams.pem sertifikaatille.
- Määritellään ssl-params.conf
- Käynnistetään tarvittavat apache moduulit
- Määritellään default-ssl.conf.
- Määritellään http-palvelin käyttämään Https-protokollaa. (DigitalOcean 2016.)

4.7 MySQL

MySQL on suosittu tietokannan hallintajärjestelmä, jolla voidaan luoda tietokantoja ja ylläpitää niitä. MySQL on avointa lähdekoodia ja sen perus versio (Community Edition) on ilmainen, Oracle omistaa MySQL:n ja siitä on myös tarjolla kaupallisia versioita. (MySQL 2017.)

LIITE 4. sisältää tarkemmat määritykset.

Suoraan käyttöjärjestelmään tehdyillä tunnuksilla ei voida käyttää sähköpostin palveluja. Sähköpostiin kirjaudutaan tunnuksilla, jotka haetaan tietokannasta. Tietokantaan lisätään osoitteet, joita käytetään sähköpostin toimittamiseen. Lisäksi luodaan seuraavat taulut:

- virtual_domains, johon lisätään oopperaskaala.fi domainit.
- virtual_users, johon lisätään salasanat ja sähköpostiosoitteet.
    - Esim. etunimi.sukunimi@oopperaskaala.fi tai admin@oopperaskaala.fi
- virtual_aliases, johon lisätään sähköpostialiakset.
    - Esim. laskutus@oopperaskaala.fi -> admin@oopperaskaala.fi
    - info@oopperaskaala.fi -> admin@oopperaskaala.fi

Virtual_aliases määrittelee sähköpostiosoitteen, joka liitetään jo olemassa olevaan osoitteeseen, esim. olemassa oleva matti.meikalainen@oopperaskaala.com on talouspäällikön osoite ja halutaan, että laskutus@oopperaskaala.fi postit menevät suoraan matin osoitteeseen, lisätään laskutus@oopperaskaala.fi osoittamaan matin osoitteeseen virtual_aliases tauluun.

4.8 Postfix

Postfix on suosittu sähköposti-palvelin ohjelma, joka on nopea, helppokäyttöinen ja turvallinen. (Postfix 2017.)

Asennuksessa käytetään virtuaalikäyttäjiä ja virtuaaliverkkotunnusta. Tämä tarkoittaa, että sähköpostitunnukset sekä verkkotunnus haetaan MySQL kannasta. Sähköpostit lähetetään ja luetaan MySQL:n tehdyillä tunnuksilla, heikkoutena tässä kohtaa on, ettei käyttäjät pysty vaihtamaan salasanojaan itsenäisesti, vaan he joutuvat pyytämään uuden salasanan pääkäyttäjältä. Toisaalta eduksi voidaan laskea, että pääkäyttäjä tekee salasanoista riittävän monimutkaisia ja turvallisia, sekä salasanat pystytään kryptaamaan MySQL tietokantaan.
Määritellään Postfix ja tehdään muutokset, joiden jälkeen saadaan yhteys MySQL tietokantaan.

LIITE 5. sisältää tarkemmat määritykset.

Postfix asennuksessa konfiguroidaan kahta Postfix:n määrittely tiedostoa:

- /etc/postfix/main.cf
- /etc/postfix/master.cf

Sekä luodaan neljä uutta tiedostoa, joilla otetaan yhteys MySQL tietokantaan.

- /etc/postfix/mysql-virtual-mailbox-domains.cf
- /etc/postfix/mysql-virtual-mailbox-maps.cf
- /etc/postfix/mysql-virtual-alias-maps.cf
- /etc/postfix/mysql-virtual-email2email.cf (DigitalOcean 2016.)

4.9 Dovecot

Dovecot on avoimen lähdekoodin IMAP/POP3 palvelin. Dovecot mahdollistaa sähköpostien lukemisen IMAP protokollan avulla. Let’s Encrypt-sertifikaatin avulla luodaan turvallinen ja salattu yhteys käyttäjän ja palvelimen välille IMAPS protokollan avulla. (Ubuntu.com. 2017.)

LIITE 6. sisältää tarkemmat määritykset.

Dovecotin asennuksen aikana editoimme 7 tiedostoa:

- /etc/dovecot/dovecot.conf

- /etc/dovecot/conf.d/10-mail.conf
- /etc/dovecot/conf.d/10-auth.conf
- /etc/dovecot/conf.d/auth-sql.conf.ext
- /etc/dovecot/dovecot-sql.conf.ext
- /etc/dovecot/conf.d/10-master.conf
- /etc/dovecot/conf.d/10-ssl.conf

Määritellään Dovecot käyttämään ainoastaan IPv4 protokollaa, koska palvelun tarjoajalla ei ole mahdollisuutta käyttää IPv6 protokollaa, poistetaan se käytöstä. Määritellään Dovecotin muita asetuksia, lisätään vmail-käyttäjä ja ryhmä, määritellään Dovecot käyttämään MySQL tietokantaa ja aktivoidaan SSL. (DigitalOcean 2016.)

4.10 Wordpress

Wordpress on suosittu avoimen lähdekoodin ohjelmisto, jolla voidaan toteuttaa näyttäviä http-sivustoja. Alustana Wordpress on avoin, kevyt ja nopea sisällönhallintajärjestelmä. Alun perin Wordpress oli suunniteltu blogeja varten, mutta nykyisin se toimii kokonaisena sisällönhallintajärjestelmänä. (Wordpress 2017.)

LIITE 7. sisältää tarkemmat määritykset.

Toimiakseen Wordpress vaatii http-palvelimen, PHP:n ja tietokannan. Palvelimeen on jo asennettuna Apache sekä MySQL. Asennetaan PHP ja määritellään MySQL, minkä jälkeen asennetaan Wordpress. Wordpress määrittely tiedosto on wp-config.php, johon lisätään MySQL:n tehdyt tietokannan nimi, käyttäjän nimi ja salasana. Asennuksen valmistuttua Wordpress viimeistellään selaimella osoitteessa oopperaskaala.fi.

4.10.1 Wordfence plugin

Wordfence on turvallisuus lisäosa, joka sisältää useita toiminta, jolla voidaan turvata Wordpressin toiminta. Wordfencen maksuton versio sisältää seuraavia ominaisuuksia:

- Ohjelmallisen palomuurin
- Useita tapoja blokata mahdollisia tunkeutujia
- Haittaohjelmien skannerin
- Käyttäjien seurantaa
- Valvoa levytilaa (Wordfence 2017.)

Palvelimella ei ole FTP-palvelinta eikä lisäosia voida asentaa suoraan Wordpressiin selaimen avulla. Wordfencen asennus tehdään kopioimalla Wordfence tiedostot wp-content/plugins/ hakemistoon.

Kun asennus on tehty, siirry selaimella Wordpressiin ja aktivoi Wordfence.

4.10.2 Aktivoidaan Permalinks

Permalinks tarkoittaa pysyvää osoitetta, jossa URL ei muutu, osoite saadaan myös näkymään helposti ymmärrettävänä. Muutetaan linkin perusmuoto (http://example.com/?p=N) näyttämään tältä (http://example.com/2012/post-name/)
(Wordpress 2017.)

Permalinks saadaan käyttöön editoimalla seuraavia tiedostoja:

- /var/www/oopperaskaala/public_html/.htaccess
- /etc/apache2/sites-available/oopperaskaala.conf

Lisäksi otetaan käyttöön Apachen mod_rewrite moduuli ja viimeistellään permalinksin käyttöönotto selaimella.

4.10.3 Turvalliset päivitykset Wordpressiin ja SALT:n lisäys

Oletuksena Wordpress päivitykset ja ohjelmistojen lataukset tapahtuvat FTP:n kautta. FTP on turvaton protokolla, minkä seurauksena haluamme tehdä siirrot SSH:n avulla. Päivityksiä varten lisätään järjestelmään uusi käyttäjä. Käyttäjälle luodaan SSH avaimet, joiden avulla määritellään turvallinen tiedonsiirto. (DigitalOcean 2016.)

SALT, Security Keys lisää tietoturvaa lisäämällä sattumanvaraisia elementtejä käytössä oleviin salasanoihin. SALT:n käyttö ei ole pakollista mutta suositeltavaa, avaimia voi luoda itse tai ne voi generoida Wordpressin API.n avulla. Avaimia voi myös muuttaa koska vain, muutoksen jälkeen käyttäjien on kirjauduttava uudestaan järjestelmään. (Wordpress 2017.)

Avainten lisääminen tehdään wp-config.php tiedostoon.

4.10.4 Wordpress backup

Wordpress ei sisällä minkäänlaista varmistus ohjelmaa, varmistukseen on kuitenkin saatavilla useita lisäosia tai ohjelmia joilla varmistuksen voi tehdä. (Wordpress 2017.)

Varmistuksen voi myös tehdä suoraan komentoriviltä. Tehdään skripti, jolla varmistusten teko on helppoa ja nopeaa. Varmistus otetaan Wordpress tiedostoista ja Wordpressiin liittyvistä tietokannoista.
(OrbitingWeb 2017.)

Varmistus tehdään wordpress/ hakemistosta kokonaisuudessa, sekä tietokannoista jotka liittyvät Wordpressiin. Tiedot pakataan ja siirretään toiselle palvelimelle. Varmistusta ei ole automatisoitu, vaan se tehdään satunnaisesti toistaiseksi. Palveluntarjoaja varmistaa koko palvelimen tiedot päivä- ja viikkotasolla, mikä on riittävä varmistustapa. Wordpressin varmistuksella haetaan tapaa, jolla voidaan palauttaa yksittäistä tietoa nopeasti. Omista varmistuksista voidaan myös palauttaa tietoa itsenäisesti, ilman että palveluntarjoajan tarvitsee tehdä toimenpiteitä.

4.10.5 Lokitiedostot

Ubuntu tallentaa oletuksena tietoja tapahtumista lokitiedostoihin. Tapahtumia saattaa tulla paljon, jopa satoja rivejä muutamassa minuutissa. Lokien analysointi on aikaa vievää, mutta niiden säännöllinen tarkkailu ja analysointi ovat perusta tietoturvalliselle ympäristölle.
Ubuntun lokit löytyvät /var/log/ hakemistosta. Tärkein on syslog, tällä komennolla voit lukea syslogin 50 viimeistä riviä -> sudo tail -50 /var/log/syslog

Toinen kätevä komento näyttää syslogin viimeiset rivit ja päivittää rivit reaaliajassa, erittäin hyödyllinen esim. testatessa jotakin samaan aikaan.
sudo tail -f /var/log/syslog

Mail.log, mail.err ovat sähköpostin lokeja. Auth.log kirjautumiseen liittyviä tietoja ja apache2 hakemisto sisältää http-palvelimen lokeja.

5 Pohdinta

Produktia suunnitellessa oli useita vaihtoehtoja toteutukselle. Www-sivuston ja sähköpostin toteuttamiselle oli monia eri vaihtoehtoja tarjolla. Google ja Microsoft tarjoavat palveluitaan, jotka sopivat myös pienille organisaatioille, kohtuullisilla kustannuksilla. Useita muita tuottajia oli myös tarjolla, joilta olisi saanut Wordpress ja sähköpostipalvelut avaimet käteen-periaatteella. Lopullinen päätös toteuttaa oma vuokrapalvelin oli kuitenkin se, että on mahdollisuus tuottaa kaikki halutut palvelut itse. Kaikissa tapauksissa oli rajoituksia, mutta omassa virtuaalipalvelimessa niitä oli vähiten, ja ominaisuuksiin voitiin vaikuttaa ostohetkellä.
Toinen päätökseen vaikuttava asia, oli tuen saaminen. Avaimet käteen ostettuna tuen saaminen on yleisesti liitetty palvelun hintaan. Edullisimmat palvelut eivät sisällä tukea tai tuki on erikseen maksullista. Samoin tuen vasteaikaa ei ole määritelty, tai se on määritelty päivissä. Tästä pääteltiin, että yksinkertaiset ongelmat on helpompi ratkaista itse, eikä niistä tässä tapauksessa kannata maksaa ylimääräistä. Yhdistyksen työntekijät eivät ole kovinkaan tietoteknisiä henkilöitä, joten heidän ja palveluntarjoajan tuen välillä ei aina puhuttu samaa kieltä. Kommunikaatio oli vähäistä eikä aina ymmärretty mistä asioista puhuttiin, mikä taas johti hitaaseen ongelmanratkaisuun.

Palvelimentarjoajan valinta oli myös helppo tehdä. Kaikki testatut palvelimet olivat toimivia, joten valinta osui parhaaseen tuotteeseen. Testauksesta oli huomattava hyöty työtä tehdessä. Kaikki palvelut asennettiin jokaiselle palvelimelle, mikä toi esille dokumentaatiossa olevat puutteet, jotka pystyttiin korjaamaan dokumentaation seuraavaan versioon. Samalla uudet versiot esim. PHP7 ja sen vaatimat riippuvuudet saatiin dokumentoitua ja testattua toimivaksi.

Kokonaisuutena avoimen lähdekoodin ohjelmat sopivat erittäin hyvin työn vaatimaan käyttöön. Pienellä kustannuksella (n. 35e/vuosi), saadaan palvelin ja .fi domain käyttöön. Kaikki ohjelmistot ovat avointa lähdekoodia eikä niiden käyttäminen vaadi lisenssi tai muita maksuja. Neljän kuukauden ajanjakson jälkeen, palvelin toimii moitteettomasti minimaalisella ylläpidolla.
Eniten aikaa kului sopivien ohjelmistojen löytämiseen ja yleisesti suunnitteluun, miten palvelimen tulisi toimia. Etenkin testausvaiheessa, ohjelmistojen asennus ja määrittely veivät aikaa. Ohjeita löytyi kattavasti, mutta luotettavan ja ajan tasalla olevan dokumentaation löytäminen oli työlästä sekä aikaa vievää. Ohjeet eivät yleisesti päivity samaan aikaan ohjelmistojen ja niiden riippuvuuksien päivittyessä. Esimerkiksi Wordpress löytyy hyvin helposti useita hyviä ohjeita PHP5 version käyttöön, mutta Wordpress ja PHP7 versioon ohjeita ei juurikaan löytynyt palvelimen asennusvaiheessa.

Palvelin on toiminut erittäin hyvin, jopa odotettua paremmin neljän kuukauden ajan. Wordpress sivusto on rakennettu uudelleen, eikä sivustolla ole juuri nyt tuotantojen välissä suurta liikennettä eikä kävijäkuormaa. Seuraavan tuotannon tullessa, sivut päivitetään ja käyttäjämäärät nousevat huomattavasti nykyisestä. Http-palvelin ja sähköposti palvelin toimivat käyttäen hyvin vähän palvelimen resursseja, eikä muitakaan ongelmia ole havaittu. Ainoa katkos oli palveluntarjoajan toimesta, kun palvelimien päivitys suoritettiin. Katkoksesta tuli ilmoitus etukäteen ja se tehtiin aamuyöstä, mikä ei häirinnyt palvelimen toimintaa.

Tällä hetkellä produkti on mielestäni saavuttanut tavoitteensa, palvelin toimii suunnitellulla tavalla, ylläpidon tarve on minimaalista, arvioidut kustannukset ovat pitäneet, palveluntarjoaja on toiminut luotettavasti eikä ongelmia ole ilmaantunut ja asiakas on tyytyväinen produktiin.

Lähteet

Andreasson, Ari & Koivisto, Juha. 2013. Tietoturvaa toteuttamassa. Helsinki. Tietosanoma Oy.

DigitalOcean 2016. Create the ssl certificate. Luettavissa: https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-16-04#step-1-create-the-ssl-certificate. Luettu 8.3.2017.

DigitalOcean 2016. Configure postfix. Luettavissa: https://www.digitalocean.com/community/tutorials/how-to-configure-a-mail-server-using-postfix-dovecot-mysql-and-spamassassin#step-3-configure-postfix. Luettu 8.3.2017.

DigitalOcean 2016. How to set up apache virtual hosts. Luettavissa: https://www.digitalocean.com/community/tutorials/how-to-set-up-apache-virtual-hosts-on-ubuntu-16-04. Luettu 8.3.2017.

DigitalOcean 2016. Configure dovecot. Luettavissa: https://www.digitalocean.com/community/tutorials/how-to-configure-a-mail-server-using-postfix-dovecot-mysql-and-spamassassin#-step-4-configure-dovecot. Luettu 8.3.2017.

DigitalOcean 2016. Set up secure updates with ssh. Luettavissa: https://www.digitalocean.com/community/tutorials/how-to-configure-secure-updates-and-installations-in-wordpress-on-ubuntu#set-up-secure-updates-with-ssh. Luettu 8.3.2017

GNU. 2017. GNU operating system. Luettavissa: https://www.gnu.org/gnu/about-gnu.html. Luettu: 8.3.2017.

GNU. 2017. Overview of the GNU system. Luettavissa: https://www.gnu.org/gnu/gnu-history.html. Luettu: 8.3.2017.

Helmke, Matthew. 2015. Ubuntu Unleashed, 2015 edition. Indianapolis. Pearson Education, Inc.

Kuutti, Wille & Rantala, Ari. 2007. Linux. Jyväskylä. WSOY.

Let’s Encrypt 2017. How it works. Luettavissa: https://letsencrypt.org/how-it-works/. Luettu 8.3.2017.

Let’s Encrypt 2017. Why 90 days. Luettavissa: https://letsencrypt.org/2015/11/09/why-90-days.html. Luettu 8.3.2017.

MySQL 2017. MySQL Community Edition. Luettavissa: https://www.mysql.com/products/community/. Luettu: 8.3.2017.

Negus, Christopher. 2015. Linux Bible, 9th edition. Indianapolis. John Wiley & Sons, Inc.

Nemeth, Evi & Snyder, Garth & Hein, Trent R. & Whaley, Ben. 2010. Boston. Pearson Education, Inc.

O'Hanley, Richard & Tiller, James S. 2014. Information Security Management Handbook., sixth edition. Boca Raton, Florida. CRC Press.

OrbitingWeb 2017. Auto BackUp WordPress Files Using a Simple Bash Script. Luettavissa: http://orbitingweb.com/blog/automatically-backup-wordpress-database/. Luettu 8.3.2017.

Postfix 2017. Postfix home page. Luettavissa: http://www.postfix.org/. Luettu: 8.3.2017.

Ubuntu.com. 2017. Firewall. Luettavissa: https://help.ubuntu.com/lts/serverguide/firewall.html. Luettu: 8.3.2017.

Ubuntu.com. 2017. Apt. Luettavissa: https://help.ubuntu.com/lts/serverguide/apt.html. Luettu: 8.3.2017.

Ubuntu.com. 2017. AptGet. Luettavissa: https://help.ubuntu.com/community/AptGet/Howto. Luettu: 8.3.2017.

Ubuntu.com. 2017. Dns. Luettavissa: https://help.ubuntu.com/lts/serverguide/dns.html. Luettu: 8.3.2017.

Ubuntu.com. 2017. Dns-references. Luettavissa: https://help.ubuntu.com/lts/serverguide/dns-references.html. Luettu: 8.3.2017.

Ubuntu.com. 2017. Hosts. Luettavissa: http://manpages.ubuntu.com/manpages/trusty/man5/hosts.5.html. Luettu: 8.3.2017.

Ubuntu.com. 2017. Httpd. Luettavissa: https://help.ubuntu.com/lts/serverguide/httpd.html. Luettu: 8.3.2017.

Ubuntu.com. 2017. Dovecot. Luettavissa: https://help.ubuntu.com/community/Dovecot. Luettu: 8.3.2017.

Vacca, 2009. Computer and Information Security Handbook. Burlington, MA. Morgan Kaufmann.

W3Techs 2017. Web Servers. Luettavissa: https://w3techs.com/technologies/overview/web_server/all. Luettu 8.3.2017.

Wordfence 2017. Features. Luettavissa: https://www.wordfence.com/#features. Luettu: 8.3.2017.

Wordpress 2017. Wordpress Features. Luettavissa: https://codex.wordpress.org/WordPress_Features. Luettu: 6.3.2017.

Wordpress 2017. Using Permalinks. Luettavissa: https://codex.wordpress.org/Using_Permalinks. Luettu: 6.3.2017.

Wordpress 2017. Security Keys. Luettavissa: https://codex.wordpress.org/Editing_wp-config.php#Security_Keys, Luettu: 8.3.2017.

Wordpress 2017. Backing Up Your WordPress Site. Luettavissa: https://codex.wordpress.org/WordPress_Backups#Backing_Up_Your_WordPress_Site. Luettu: 8.3.2017.

Liitteet

Liite 1. Käyttöjärjestelmän ensimmäiset määritykset

Lisätään käyttäjä:

```
# adduser aha
```

Anna käyttäjälle salasana ja muut tarvittavat tiedot (eivät pakollisia mutta kokonimi olisi hyvä tallentaa).

Lisätään käyttäjä sudoers ryhmään.

```
# usermod -aG sudo aha
```

Nano asennus:

```
# sudo apt-get install nano -y
```

UFW palomuuri hallinnan asennus ja määrittely.

```
# ufw status
# ufw enable
# ufw disable
```

SSH portin voi avata komennolla:

```
# ufw allow ssh
# sudo ufw allow 22/tcp
```

Molemmat ylläolevista komennoista avaavat SSH portin 22, turvallisuus syistä SSH-palvelimen portti muutetaan porttiin 22222, jonka avaamme firewallista komennolla:

```
# sudo ufw allow 22222/tcp
```

Asennetaan järjestelmän päivitykset.

```
# sudo apt get update
```

```
# sudo apt-get upgrade
# sudo apt-get dist-upgrade
```

Kaikki kolme komentoa voi suorittaa myös kerralla (autoremove poistaa vanhentuneet paketit) ->

```
# sudo -- sh -c 'apt-get update; apt-get upgrade -y; apt-get dist-upgrade -y; apt-get autoremove -y'
```

Asennetaan ja määritellään SSH-palvelin.

Editoidaan SSH-palvelimen ominaisuuksia:

```
$ sudo nano /etc/ssh/sshd_config
```

Huom. tarkista että olet editoimassa sshd_config tiedostoa, samassa hakemistossa on ssh_config (ssh ilman D kirjainta, joka taas määrittelee ssh clientin ominaisuuksia)!

Muutetaan Port asetusta:

```
# What ports, IPs and protocols we listen for
Port 22222
```

Estetään root tunnuksen kirjautuminen ssh-palvelimeen:

```
# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
```

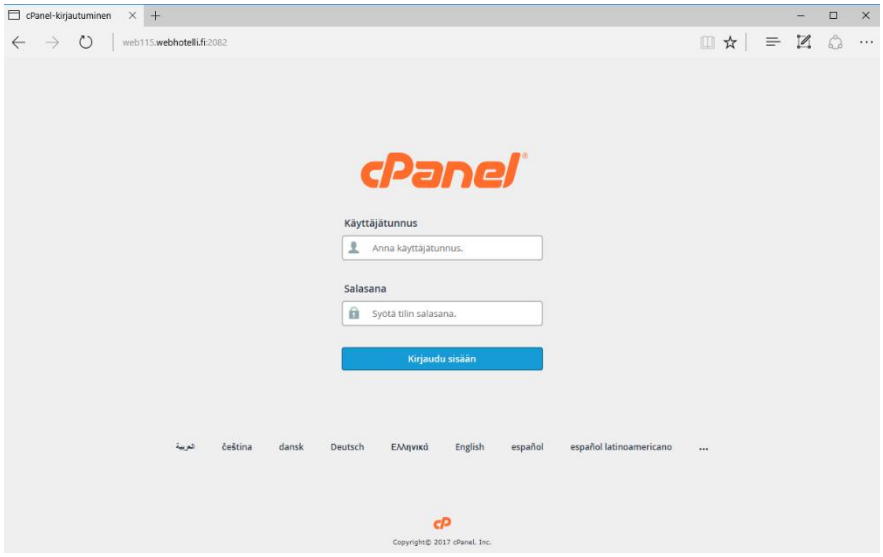
Uusien asetuksien voimaan tulo vaatii sshd uudelleen käynnistämisen

```
$ sudo service sshd restart
```

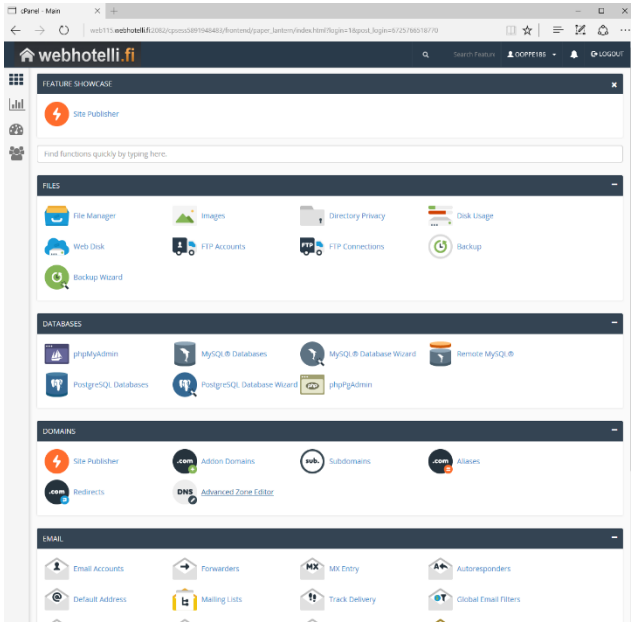
Liite 2. Nimipalvelu DNS määritykset

Nimipalvelu DNS

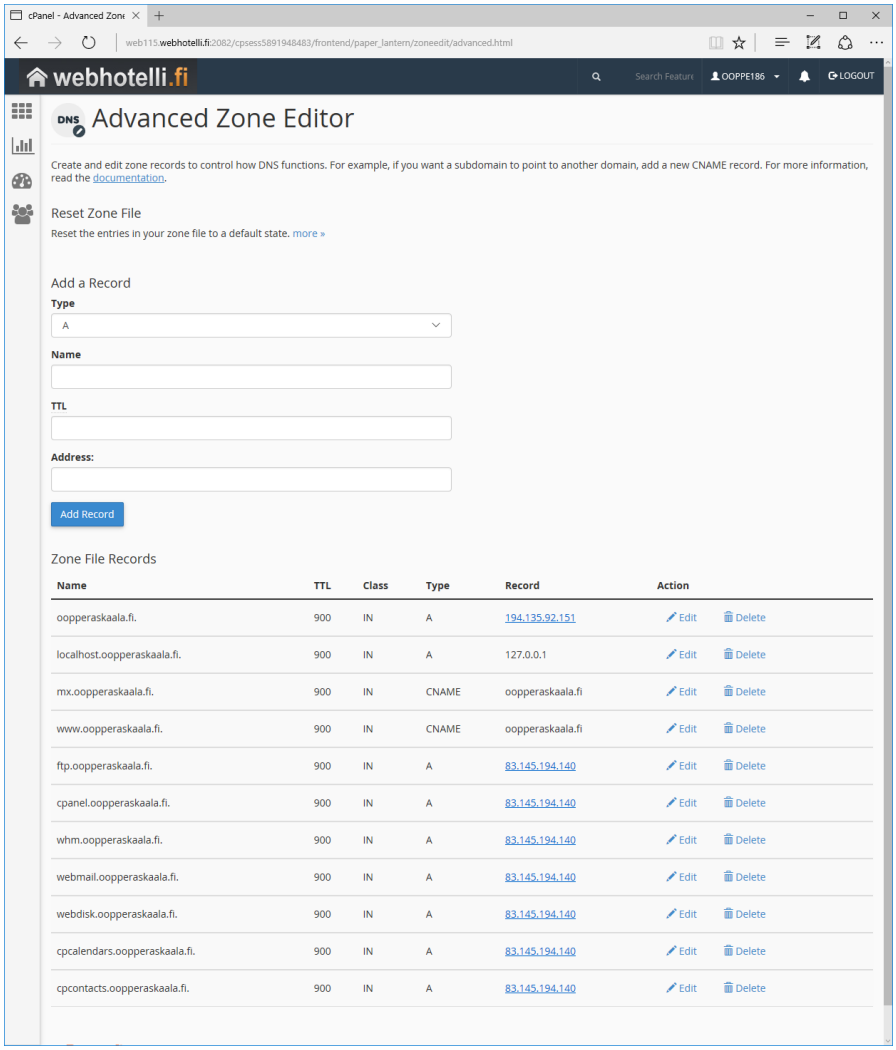
Nimipalvelu toimii webhotellin cPanelin kautta. Avaa selaimella http://web115.webhotelli.fi/cpanel tai http://web115.webhotelli.fi:2082



Anna tunnus ja salasana, avaa Domains kohdasta Advanced Zone Editor,



Odota hetki ja sivun alalaitaan avautuu nykyiset asetukset.

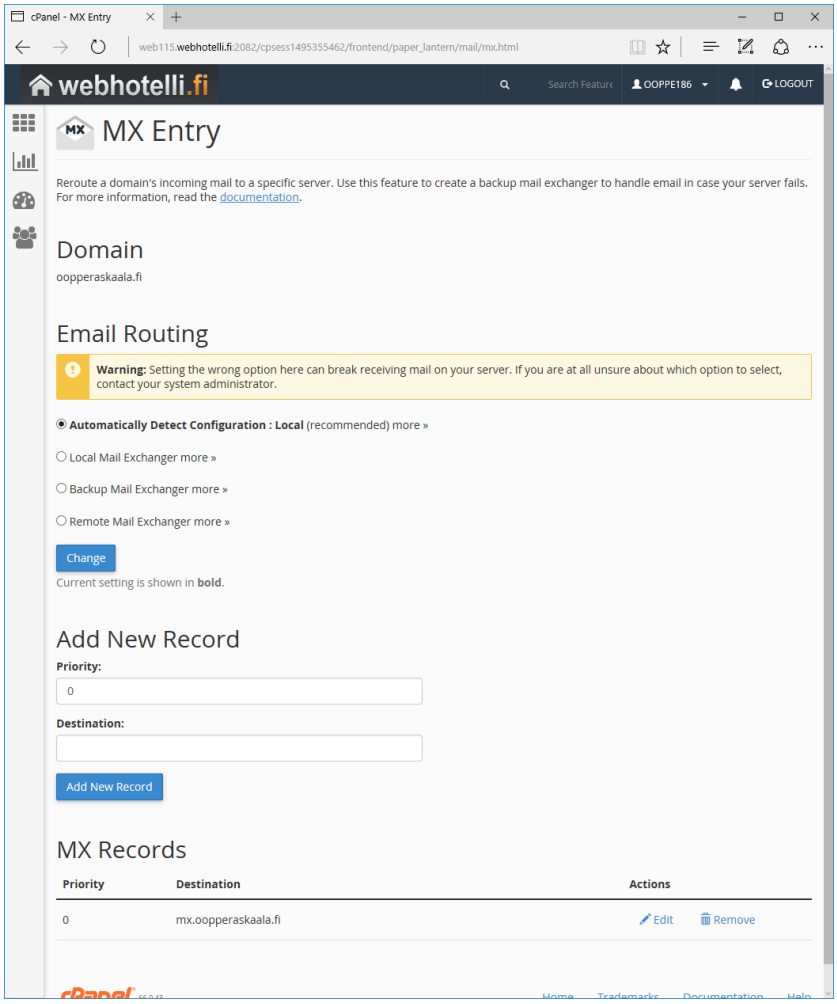


Huom: 83.145. alkuinen osoite on webhotelli.fi osoite (osoittaa webhotelli.fi:n omalle palvelimelle, nämä eivät toimi nykyisen VPS:n palvelimen kanssa), vaikka osan määrityksistä poistaa, ne tulevat takaisin automaattisesti. Tarvittavat asetukset ovat:

oopperaskaala.fi.	900	IN	A	194.135.92.151
localhost.oopperaskaala.fi.	900	IN	A	127.0.0.1
mx.oopperaskaala.fi.	900	IN	CNAME	oopperaskaala.fi
www.oopperaskaala.fi.	900	IN	CNAME	oopperaskaala.fi

Sähköpostiin liittyvät asetukset cPanelin pääsivulta, EMAIL – MX Entry sivun alalaidasta:

0 mx.oopperaskaala.fi



Muutoksien voimaantulo saattaa kestää jopa 24 tuntia, mikä tulee ottaa huomioon, kun muutoksia suunnitellaan. Seuraavaksi muokkaamme palvelimen asetuksia (palvelimelle saa yhteyden IP-osoitteella, jos nimipalvelu ei toimi).

Palvelimen hosts tiedoston muokkaaminen:

Seuraavat tietueet lisätään omaan palvelimeen, /etc/hosts tiedostoon.

```
$ sudo nano /etc/hosts
```

lisää rivit:

```
127.0.1.1 oopperaskaala.localdomain oopperaskaala
127.0.0.1 localhost
194.135.92.151 oopperaskaala.fi www.oopperaskaala.fi mx.oopperaskaala.fi
```

Huom. Jos palvelin asennetaan uudestaan, anna oopperaskaala.fi VPS hallintapaneeliin host kohtaan, muuten palvelimen nimeksi tulee automaattisesti VPS :n tarjoama domain nimi.

Aikavyöhyke ja NTP.
Määritellään palvelin käyttämään suomen aikavyöhykettä:

Komennolla timedatectl saadaan lista valittavista aikavyöhykkeistä.

```
$ timedatectl list-timezones
```

Valitaan Europe/Helsinki, seuraavaksi määritellään Helsinki oletus aikavyöhykkeeksi.

```
$ sudo timedatectl set-timezone Europe/Helsinki
```

Tarkistetaan muutos:

```
$ timedatectl
```

Asennetaan NTP (Network Time Protocol), jonka avulla palvelimen aika synkronisoidaan internetin aikapalvelimelta.

```
$ sudo apt-get update

$ sudo apt-get install ntp
```

Liite 3. Let’s Encrypt SSL-sertifikaatin käyttöönotto

SSL Lets Encrypt-sertifikaatin asennus.

Varmista että portti 443 on avoinna!

```
$ sudo ufw status
```

Jos portti ei ole avoinna ->$ sudo ufw allow 443

Asennetaan git versiohallintaohjelma ja Lets Encrypt SSL-sertifikaatti.

```
$ sudo apt-get install git
$ sudo git clone https://github.com/letsencrypt/letsencrypt
/opt/letsencrypt
```

Luodaan sertifikaatti oopperaskaala.fi, www.oopperaskaala.fi ja mx.oopperaskaala.fi osoitteille.

```
$ cd /opt/letsencrypt
$ sudo -H ./letsencrypt-auto certonly --standalone -d oopperaskaala.fi -d www.oopperaskaala.fi -d mx.oopperaskaala.fi
```

Tarkistetaan että sertifikaatit on saatu:

`$ sudo ls /etc/letsencrypt/live/oopperaskaala.fi` <- täällä pitäisi olla 4 .pem tiedostoa.
`$ sudo stat /etc/letsencrypt/live/oopperaskaala.fi/fullchain.pem` <- näyttää certin tilan.

SSL-sertifikaatin automaattinen päivittäminen.

Päivitetään sertifikaatit:

```
$ cd /opt/letsencrypt
$ sudo -H ./letsencrypt-auto certonly --standalone --renew-by-default -d oopperaskaala.fi -d www.oopperaskaala.fi -d mx.oopperaskaala.fi
```

Lisätään Let’s Encrypt sertifikaatin päivitys croniin, päivitys tapahtuu kerran kuukaudessa:

```
$ sudo echo '@monthly root /opt/letsencrypt/letsencrypt-auto certonly --quiet --standalone --renew-by-default -d oopperaskaala.fi -d www.oopperaskaala.fi -d mx.oopperaskaala.fi >> /var/log/letsencrypt/letsencrypt-auto-update.log' | sudo tee --append /etc/crontab
```

Lisätään Let’s Encrypt clientin päivitys croniin, päivitys tapahtuu kerran viikossa:

```
$ sudo echo '@weekly root cd /opt/letsencrypt && git pull >> /var/log/letsencrypt/letsencrypt-auto-update.log' | sudo tee --append /etc/crontab
```

Apachen asennus:

Asennetaan apache web-palvelin.

```
$ sudo apt-get install apache2
```

Testaa toimiiko www.oopperaskaala.fi selaimella, jos näkyviin tulee oletus www-sivu niin jatka ohjeen mukaisesti. Poista nykyinen oletussivu /var/www/html/ kansiosta.

Web-palvelimen tiedostot ovat oletuksena /var/www/html hakemistossa. Koska palvelimelle on mahdollisesti tulossa muitakin web-sivustoja, tehdään skaalalle oma ”document root” http-palvelimelle.

Lisätään virtuaalinen palvelin oopperaskaala, luodaan hakemisto tiedostoille ja annetaan oikeuksia:

```
$ sudo mkdir -p /var/www/oopperaskaala/public_html
$ sudo chown -R $USER:$USER /var/www/oopperaskaala/public_html
$ sudo chmod -R 755 /var/www
```

Palvelimen toimintaa voi testata luomalla esimerkkisivun:

```
$ nano /var/www/oopperaskaala/public_html/index.html
```

```
<html>
 <head>
 <title>Welcome to Skaala!</title>
 </head>
 <body>
 <h1>Success! Skaala virtual host is working!</h1>
 </body>
</html>
```

Määritellään apachen conf tiedostoja, kopiodaan oletus. conf -> oopperaskkala.conf.

```
$ sudo cp /etc/apache2/sites-available/000-default.conf
/etc/apache2/sites-available/oopperaskaala.conf
```

Editoidaan oopperaskaala.conf tiedostoon seuraavat rivit:

```
$ sudo nano /etc/apache2/sites-available/oopperaskaala.conf

<VirtualHost *:80>

 ServerAdmin admin@oopperaskaala.fi
 ServerName oopperaskaala.fi
 ServerAlias www.oopperaskaala.fi
 DocumentRoot /var/www/oopperaskaala/public_html

 ErrorLog ${APACHE_LOG_DIR}/error.log
 CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

Aktivoidaan uusi määrittely ja käynnistetään web-palvelin uudelleen:

```
$ sudo a2ensite oopperaskaala.conf
$ sudo service apache2 restart
```

HUOM. http-palvelin toimii portissa 80, SSL/HTTPS/443 yhdistetään palvelimeen myöhemmin tässä liitteessä.

HUOM2. Poista tarpeettomat index.html tiedostot (/var/www/html/index.html) tietoturvasyistä.

SSL ja Apache

Luodaan OpenSSL avulla itse allekirjoitettu sertifikaatti:

```
$ openssl dhparam -out /etc/ssl/private/dhparams.pem 2048
```

Muutetaan pem tiedoston oikeuksia:

```
$ chmod 600 /etc/ssl/private/dhparams.pem
```

Huom! /etc/ssl/private/dhparams.pem liitetään ssl-params.conf seuraavassa vaiheessa!

Luodaan tiedosto /etc/apache2/conf-available/ssl-params.conf ja editoidaan sitä. Huomaa viimeisen rivin polku ”`/etc/ssl/private/dhparams.pem`” täsmää edellisessä kohdassa tehtyyn tiedostoon.

```
$ sudo nano /etc/apache2/conf-available/ssl-params.conf

SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLProtocol All -SSLv2 -SSLv3
SSLHonorCipherOrder On
Header always set Strict-Transport-Security "max-age=63072000; include-
Subdomains"
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
# Requires Apache >= 2.4
SSLCompression off
SSLSessionTickets Off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"
SSLOpenSSLConfCmd DHParameters "/etc/ssl/private/dhparams.pem"
```

Käynnistetään tarvittavat moduulit:

```
$ sudo a2enmod deflate expires headers rewrite ssl
$ sudo a2ensite default-ssl
```

Määritellään default-ssl.conf, huomaa kahden viimeisen rivin polkujen on osoitettava Let’sEncrypt SSL tiedostoihin.

```
$ sudo nano /etc/apache2/sites-available/default-ssl.conf
```

Lisää seuraavat rivit:

```
<VirtualHost *:443>

    ServerAdmin admin@oopperaskaala.fi
    ServerName oopperaskaala.fi
    ServerAlias www.oopperaskaala.fi
    DocumentRoot /var/www/oopperaskaala/public_html

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
    SSLEngine ON
    SSLCertificateFile
/etc/letsencrypt/live/oopperaskaala.fi/fullchain.pem
    SSLCertificateKeyFile
/etc/letsencrypt/live/oopperaskaala.fi/privkey.pem
</VirtualHost>
```

Määritellään oopperaskaala.fi käyttämään porttia 443 (https):

```
$ sudo nano /etc/apache2/sites-available/oopperaskaala.conf
```

Lisää seuraava rivi tiedoston loppuun:

```
Redirect "/" "https://oopperaskaala.fi/"
```

Aktivoidaan ssl_params mod ja käynnistetään apache uudestaan:

```
$ sudo a2enconf ssl-params
$ sudo service apache2 restart
```

Liite 4. MySQL asennus ja määrittely

Asennetaan MySQL ja käynnistetään “mysql_secure_installation”:

```
$ sudo apt-get update
$ sudo apt-get install mysql-server
$ sudo mysql_secure_installation
```

Luodaan sähköpostin tarvitsema käyttäjä ja tietokanta.
Huom. osassa komentoja tarvitaan root käyttäjän oikeuksia (sudo ei riitä)!

Luodaan taulu ”maildb”:

```
# mysqladmin -p create maildb
```

Kirjaudutaan tietokantaan ja luodaan käyttäjä sähköpostin autentikointia varten:

```
# mysql -p maildb
```

```
GRANT SELECT ON maildb.* TO 'mailuser'@'127.0.0.1' IDENTIFIED BY 'Sala-
sana1';
FLUSH PRIVILEGES;
```

Siirrytään maildb tauluun.

```
use maildb;
```

Tehdään virtual_domains taulu:

```
CREATE TABLE `virtual_domains` (
  `id` int(11) NOT NULL auto_increment,
  `name` varchar(50) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Tehdään virtual_users taulu:

```
CREATE TABLE `virtual_users` (
  `id` int(11) NOT NULL auto_increment,
  `domain_id` int(11) NOT NULL,
  `password` varchar(106) NOT NULL,
  `email` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `email` (`email`),
  FOREIGN KEY (domain_id) REFERENCES virtual_domains(id) ON DELETE CAS-
CADE
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Tehdään virtual_aliases taulu:

```
CREATE TABLE `virtual_aliases` (
  `id` int(11) NOT NULL auto_increment,
  `domain_id` int(11) NOT NULL,
  `source` varchar(100) NOT NULL,
  `destination` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
```

```
  FOREIGN KEY (domain_id) REFERENCES virtual_domains(id) ON DELETE CAS-
CADE
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Lisätään virtual_domains tauluun domainit:

```
INSERT INTO `maildb`.`virtual_domains`
  (`id` ,`name`)
VALUES
  ('1', 'oopperaskaala.fi'),
  ('2', 'mx.oopperaskaala.fi'),
  ('3', 'oopperaskaala');
```

Lisätään virtual_users tauluun salasanat ja sähköpostiosoitteet:

```
INSERT INTO `maildb`.`virtual_users`
  (`id`, `domain_id`, `password` , `email`)
VALUES
  ('1', '1', ENCRYPT('6Uu!h8"qfdhO56', CONCAT('$6$',
SUBSTRING(SHA(RAND()), -16))), 'aha@oopperaskaala.fi'),
  ('2', '1', ENCRYPT('salasana', CONCAT('$6$', SUBSTRING(SHA(RAND()), -
16))), 'kari@oopperaskaala.fi'),
  ('3', '1', ENCRYPT('salasana', CONCAT('$6$', SUBSTRING(SHA(RAND()), -
16))), 'etu.suku@oopperaskaala.fi'),
  ('4', '1', ENCRYPT('salasana', CONCAT('$6$', SUBSTRING(SHA(RAND()), -
16))), 'nimi.nimi@oopperaskaala.fi'),
  ('5', '1', ENCRYPT('salasana', CONCAT('$6$', SUBSTRING(SHA(RAND()), -
16))), 'toimisto@oopperaskaala.fi'),
  ('6', '1', ENCRYPT('salasana', CONCAT('$6$', SUBSTRING(SHA(RAND()), -
16))), 'admin@oopperaskaala.fi'),
  ('7', '1', ENCRYPT('salasana', CONCAT('$6$', SUBSTRING(SHA(RAND()), -
16))), 'bob@oopperaskaala.fi'),
  ('8', '1', ENCRYPT('salasana', CONCAT('$6$', SUBSTRING(SHA(RAND()), -
16))), 'info@oopperaskaala.fi');
```

Lisätään virtual_values tauluun mahdolliset sähköpostialiakset:

```
INSERT INTO `maildb`.`virtual_aliases`
```

```
  (`id`, `domain_id`, `source`, `destination`)
VALUES
  ('1', '1', 'root@oopperaskaala.fi', 'admin@oopperaskaala.fi'),
  ('2', '1', 'webmaster@oopperaskaala.fi', 'admin@oopperaskaala.fi'),
  ('3', '1', 'abuse@oopperaskaala.fi', 'admin@oopperaskaala.fi');
```

Tarkistetaan että tiedot ovat oikein tauluissa:

```
SELECT * FROM maildb.virtual_domains;
SELECT * FROM maildb.virtual_users;
SELECT * FROM maildb.virtual_aliases;
```

Liite 5. Postfix:n määrittely

Sähköpostin käyttämät oletusportit ovat 110, 143, 465, 587, 993 ja 995. Portit joita tullaan käyttämään asennuksen valmistuttua, ovat 587 ja 993. Asennuksen aikana saatetaan tarvita myös muita portteja, lähinnä asennuksen edistymisen ja toimivuuden testaamista varten.

Asennetaan Postfix, ja Dovecot

```
$ sudo apt-get install postfix postfix-mysql dovecot-core dovecot-imapd
dovecot-pop3d dovecot-lmtpd dovecot-mysql
```

Postfix asennuksen aikana valitaan ”General type of mail configuration:
Internet Site
System mail name:
oopperaskaala.fi

Määritellään Postfix, kopioidaan alkuperäinen määrittely tiedosto turvaan:

```
$ sudo cp /etc/postfix/main.cf /etc/postfix/main.cf.orig
```

Editoidaan main.cf tiedostoa (tarkista etenkin että **lihavoidut** tekstit ovat oikein!):

```
$ sudo nano /etc/postfix/main.cf

# TLS parameters
#smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
#smtpd_use_tls=yes
#smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
#smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
smtpd_tls_cert_file=/etc/letsencrypt/live/oopperaskaala.fi/fullchain.pem
smtpd_tls_key_file=/etc/letsencrypt/live/oopperaskaala.fi/privkey.pem
smtpd_use_tls=yes
smtpd_tls_auth_only = yes

#Enabling SMTP for authenticated users, and handing off authentication
to Dovecot
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes

smtpd_recipient_restrictions =
        permit_sasl_authenticated,
        permit_mynetworks,
        reject_unauth_destination

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package
for
# information on enabling SSL in the smtp client.

# smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated
defer_unauth_destination
myhostname = oopperaskaala.localdomain
myorigin = /etc/mailname
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
```

```
#mydestination = $myhostname, localdomain, localhost, local-
host.localdomain, localhost
#mydestination = localhost
relayhost =
# mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mynetworks = 127.0.0.0/8
#mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = ipv4

#Handing off local delivery to Dovecot's LMTP, and telling it where to
store mail
virtual_transport = lmtp:unix:private/dovecot-lmtp

#Virtual domains, users, and aliases
virtual_mailbox_domains = mysql:/etc/postfix/mysql-virtual-mailbox-
domains.cf
virtual_mailbox_maps = mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
virtual_alias_maps = mysql:/etc/postfix/mysql-virtual-alias-maps.cf,
        mysql:/etc/postfix/mysql-virtual-email2email.cf
```

SSL osassa tehdyt sertit löytyvät täältä ->

```
ssl_cert = </etc/letsencrypt/live/oopperaskaala.fi/fullchain.pem
ssl_key = </etc/letsencrypt/live/oopperaskaala.fi/privkey.pem
```

Seuraavaksi editoidaan neljää tiedostoa jotka sisältävät tarvittavat tiedot MySQL varten. Ensimmäisenä editoidaan `/etc/postfix/mysql-virtual-mailbox-domains.cf`:

```
$ sudo nano /etc/postfix/mysql-virtual-mailbox-domains.cf

user = mailuser
password = Salasana1
hosts = 127.0.0.1
dbname = maildb
```

```
query = SELECT 1 FROM virtual_domains WHERE name='%s'
```

Seuraavaksi editoidaan /etc/postfix/mysql-virtual-mailbox-maps.cf:

```
$ sudo nano /etc/postfix/mysql-virtual-mailbox-maps.cf
```

```
user = mailuser
password = Salasana1
hosts = 127.0.0.1
dbname = maildb
query = SELECT 1 FROM virtual_users WHERE email='%s'
```

Seuraavaksi editoidaan /etc/postfix/mysql-virtual-alias-maps.cf:

```
$ sudo nano /etc/postfix/mysql-virtual-alias-maps.cf
```

```
user = mailuser
password = Salasana1
hosts = 127.0.0.1
dbname = maildb
query = SELECT destination FROM virtual_aliases WHERE source='%s'
```

Seuraavaksi editoidaan /etc/postfix/mysql-virtual-email2email.cf:

```
$ sudo nano /etc/postfix/mysql-virtual-email2email.cf
```

```
user = mailuser
password = Salasana1
hosts = 127.0.0.1
dbname = maildb
query = SELECT email FROM virtual_users WHERE email='%s'
```

Käynnistetään Postfix uudelleen ja tarkistetaan että tehdyt asetukset toimivat:

```
$ sudo service postfix restart
```

Kaikki allaolevat komennot palattavat “1” jos konfiguraatiot ovat oikein:

```
$ postmap -q oopperaskaala.fi mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf
$ postmap -q aha@oopperaskaala.fi mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
$ postmap -q root@oopperaskaala.fi mysql:/etc/postfix/mysql-virtual-alias-maps.cf
```

Seuraavaksi aktivoidaan portti 587 portti TLS yhteyttä varten, ensiksi kopioidaan alkuperäinen määrittely tiedosto turvaan:

```
$ sudo cp /etc/postfix/master.cf /etc/postfix/master.cf.orig
```

Editoidaan master.cf seuraavasti:

```
smtp      inet  n       -       y       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
#tlsproxy  unix  -       -       y       -       0       tlsproxy
submission inet n       -       y       -       -       smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
  -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
smtps     inet  n       -       y       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
```

```
  -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
```

Muutetaan Postfix:n oikeuksia ja käynnistetään Postfix uudelleen:

```
$ sudo chmod -R o-rwx /etc/postfix
$ sudo service postfix restart
```

Liite 6. Dovecot:n määrittely

Kopiodaan alkuperäiset määrittely tiedostot turvaan:

```
$ sudo cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf.orig
$ sudo cp /etc/dovecot/conf.d/10-mail.conf /etc/dovecot/conf.d/10-
mail.conf.orig
$ sudo cp /etc/dovecot/conf.d/10-auth.conf /etc/dovecot/conf.d/10-
auth.conf.orig
$ sudo cp /etc/dovecot/dovecot-sql.conf.ext /etc/dovecot/dovecot-
sql.conf.ext.orig
$ sudo cp /etc/dovecot/conf.d/10-master.conf /etc/dovecot/conf.d/10-
master.conf.orig
$ sudo cp /etc/dovecot/conf.d/10-ssl.conf /etc/dovecot/conf.d/10-
ssl.conf.orig
```

Editoidaan dovecot.conf tiedostoa:

```
$ sudo nano /etc/dovecot/dovecot.conf
```

Lisätään tarvittavat protokollat käyttöön (imap lmpt pop3). Poistetaan IPV6 käytöstä (listen = *). Tarkista että nämä rivit löytyvät:

```
!include_try /usr/share/dovecot/protocols.d/*.protocol
```

```
protocols = imap pop3 lmtp

listen = *
```

Editoidaan 10-mail.conf tiedostoa, määritellään vhostin asetuksia:

```
$ sudo nano /etc/dovecot/conf.d/10-mail.conf

mail_location = maildir:/var/mail/vhosts/%d/%n
mail_privileged_group = mail
```

Tarkistetaan oikeuksia, luodaan hakemisto, joka vastaa MySQL:n luotua nimeä:

```
$ sudo ls -ld /var/mail
$ sudo mkdir -p /var/mail/vhosts/oopperaskaala.fi
```

Luodaan vmail käyttäjä, jolle annetaan id 5000 ja muutetaan hakemiston oikeuksia:

```
$ sudo groupadd -g 5000 vmail
$ sudo useradd -g vmail -u 5000 vmail -d /var/mail
$ sudo chown -R vmail:vmail /var/mail
```

Editoidaan 10-auth.conf tiedostoa, muokataan tiedostoa seuraavasti:

```
$ sudo nano /etc/dovecot/conf.d/10-auth.conf

disable_plaintext_auth = yes
auth_mechanisms = plain login
#!include auth-system.conf.ext
!include auth-sql.conf.ext
```

Editoidaan auth-sql.conf.ext tiedostoa. Määritellään vhost ja sql asetuksia seuraavasti:

```
$ sudo nano /etc/dovecot/conf.d/auth-sql.conf.ext

passdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
```

```
}
userdb {
  driver = static
  args = uid=vmail gid=vmail home=/var/mail/vhosts/%d/%n
   }
```

Editoidaan dovecot-sql.conf.ext tiedostoa. Määritellään tiedostoa seuraavasti:

```
$ sudo nano /etc/dovecot/dovecot-sql.conf.ext

driver = mysql
connect = host=127.0.0.1 dbname=maildb user=mailuser pass-word=salasana1
default_pass_scheme = SHA512-CRYPT
password_query = SELECT email as user, password FROM virtual_users WHERE
email='%u';
```

Muutetaan hakemistojen ja käyttäjien oikeuksia:

```
$ sudo chown -R vmail:dovecot /etc/dovecot
$ sudo chmod -R o-rwx /etc/dovecot
```

Editoidaan 10-master.conf tiedostoa seuraavasti:

```
$ sudo nano /etc/dovecot/conf.d/10-master.conf

service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
    mode = 0600
    user = postfix
    group = postfix
  }

service auth {
  # auth_socket_path points to this userdb socket by default. It's typi-
cally
  # used by dovecot-lda, doveadm, possibly imap process, etc. Its de-
fault
```

```
  # permissions make it readable only by root, but you may need to relax
these
  # permissions. Users that have access to this socket are able to get a
list
  # of all usernames and get results of everyone's userdb lookups.
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }

  unix_listener auth-userdb {
    mode = 0600
    user = vmail
    #group =
  }

  # Postfix smtp-auth
  #unix_listener /var/spool/postfix/private/auth {
  #  mode = 0666
  #}

  # Auth process is run as this user.
  user = dovecot
}
```

Editoidaan 10-ssl.conf tiedostoa. Aktivoidaan SSL ja käytetään aikaisemmin tehtyjä sertifikaatteja:

```
$ sudo nano /etc/dovecot/conf.d/10-ssl.conf

ssl = required
ssl_cert = </etc/letsencrypt/live/oopperaskaala.fi/fullchain.pem
ssl_key = </etc/letsencrypt/live/oopperaskaala.fi/privkey.pem
```

Käynnistetään Dovecot uudelleen:

```
$ sudo service dovecot restart
```

Jos Postfix herjaa ettei ole oikeuksia main.cf tiedostoon:

```
$ chmod 644 /etc/postfix/main.cf; chmod 755 /usr/sbin/sendmail
```

Liite 7. Wordpress asennus ja määrittely

Asennetaan PHP:

```
$ sudo apt-get install libapache2-mod-php7.0 php7.0-mysql php7.0-curl
php7.0-json php7.0 php7.0-cli installphp7.0-gd
```

Mysql wordpress määritykset, lisätään tietokanta (skaaladb) ja käyttäjä (skaala):

```
$ mysql -u root -p

CREATE DATABASE skaaladb;
create user 'skaala'@'localhost' identified by 'Gfjfkjghk579ghjj';
GRANT ALL PRIVILEGES ON skaaladb.* TO skaala@localhost;
```

Salasanan vaihto Mysql:ssä, kirjaudu sisään mysql roottina:

```
SET PASSWORD FOR 'skaala'@'localhost' = PASSWORD('Gfjfkjghk579ghjj');
```

Wordpressin asennus, kopiointi ja määrittely:

```
$ cd ~
$ wget http://wordpress.org/latest.tar.gz
$ tar xzvf latest.tar.gz
$ cd ~/wordpress
$ cp wp-config-sample.php wp-config.php
```

Editoidaan wp-config.php tiedostoa seuraavasti:

```
$ nano wp-config.php

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'skaaladb');

/** MySQL database username */
define('DB_USER', 'skaala');

/** MySQL database password */
```

```
define('DB_PASSWORD', 'Gfjfkjghk579ghjj');
```

Kopioidaan Wordpress tiedostot web-palvelimen hakemistoon, muutetaan oikeuksia ja luodaan uploads hakemisto:

```
$ sudo rsync -avP ~/wordpress/ /var/www/oopperaskaala/public_html/
$ cd /var/www/oopperaskaala/public_html/
$ sudo rm index.html
$ sudo chown -R aha:www-data * (aha = käyttäjätunnuksesi!).
$ mkdir /var/www/oopperaskaala/public_html/wp-content/uploads
$ sudo chown -R :www-data /var/www/oopperaskaala/public_html/wp-content/uploads
```

Siirry selaimella -> oopperaskaala.fi ja viimeistele wordpress-asennus.

Wordfence plugin

Lataa uusin versio Wordfence pluginista, linkki löytyy wordpress.org, etsi lisäosa ”wordfence”:

```
$ cd ~
$ wget https://downloads.wordpress.org/plugin/wordfence.6.3.2.zip
$ unzip wordfence.6.2.9.zip
$ sudo rsync -avP ~/wordfence /var/www/oopperaskaala/public_html/wp-content/plugins/
```

Käynnistetään Wordfence selaimesta:

```
Wordpress Dashboard - Plugins - Installed plugins - Valitse Wordfence Security ja aktivoi.
```

Lisäksi blokataan xmlrpc.php tulleet hyökkäykset:

```
Wordfence -Options -Other options - Immediately block IPs that access these URLs: - Lisää /xmlrpc.php
```

Permalink

Editoidaan .htaccess sekä oopperaskaala.conf tiedostoa.
Lisää /var/www/oopperaskaala/public_html/.htaccess tiedostoon seuraavat rivit:

```
$ nano /var/www/oopperaskaala/public_html/.htaccess

<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
```

Lisää /etc/apache2/sites-available/oopperaskaala.conf tiedostoon seuraavat rivit:

```
$ nano /etc/apache2/sites-available/oopperaskaala.conf

        <Directory />
Options FollowSymLinks
AllowOverride All
</Directory>

<Directory /var/www/oopperaskaala/public_html/>

#Options Indexes FollowSymLinks MultiViews
#AllowOverride All
#Require all granted

Options Indexes FollowSymLinks MultiViews
        AllowOverride All
        Order allow,deny
        allow from all

</Directory>
```

Käynnistetään mod_rewrite apache2 palvelimella.

```
$ sudo sudo a2enmod rewrite
```

Käynnistä apache2 uudestaan:

```
$ sudo service apache2 restart
```

Siirry selaimella wordpressiin ja aktivoi permalinks:

```
Wordpress – Settings – Permalinks – Post name, valitse Post name.
```

```
Turvalliset päivitykset Wordpressiin
```

Tehdään uusi käyttäjä, annetaan oikeuksia ja lisätään SSH avaimet käyttäjälle.

```
$ sudo adduser wp-user
$ sudo cd /var/www/oopperaskaala/public_html
$ sudo chown -R wp-user:wp-user /var/www/oopperaskaala/public_html
```

Kirjaudutaan järjestelmään wp-user tunnuksella ja luodaan SSH avaimet:

```
$ sudo su - wp-user
$ ssh-keygen -t rsa -b 4096
```

Ohjelman kysyessä tallenna avaimet /home/wp-user/wp_rsa
Passphrase jätetään tyhjäksi.
Poistutaan wp-user tililtä:

```
$ exit
```

Muutetaan uudelleen oikeuksia, www-data saa oikeudet avaimiin.

```
$ sudo chown wp-user:www-data /home/wp-user/wp_rsa*
$ sudo chmod 0640 /home/wp-user/wp_rsa*
```

Luodaan /home/wp-user/.ssh ja annetaan oikeuksia:

```
$ sudo mkdir /home/wp-user/.ssh
$ sudo chown wp-user:wp-user /home/wp-user/.ssh/
```

```
$ sudo chmod 0700 /home/wp-user/.ssh/
```

Kopioidaan julkinen avain ja määritellään oikeuksia:

```
$ sudo cp /home/wp-user/wp_rsa.pub /home/wp-user/.ssh/authorized_keys
$ sudo chown wp-user:wp-user /home/wp-user/.ssh/authorized_keys
$ sudo chmod 0644 /home/wp-user/.ssh/authorized_keys
```

Muutetaan avaimien asetuksia niin että vain palvelimelta voidaan ottaa yhteys wordpressiin. Editoidaan /home/wp-user/.ssh/authorized_keys tiedostoa, heti ensimmäisellä riville lisätään ensimmäiseksi from="127.0.0.1":

```
$ sudo nano /home/wp-user/.ssh/authorized_keys
```

Rivi näyttää tältä:

```
from="127.0.0.1" ssh-rsa AAA…..
```

Määritellään Wordpress käyttämään luotuja avaimia.

Asennetaan tarvittavat paketit:

```
$ sudo apt-get install php7.0-dev libssh2-1-dev php-ssh2
```

Editoidaan /var/www/oopperaskaala/public_html/wp-config.php tiedostoa:

```
$ sudo nano /var/www/oopperaskaala/public_html/wp-config.php
```

Lisätään rivit:

```
/** Bypass FTP */
define('FS_METHOD', 'direct');

define('FTP_PUBKEY','/home/wp-user/wp_rsa.pub');
define('FTP_PRIKEY','/home/wp-user/wp_rsa');
define('FTP_USER','wp-user');
define('FTP_PASS','');
define('FTP_HOST','127.0.0.1:22222);
```

Käynnistetään apache uudelleen:

```
$ sudo service apache2 restart
```

Huom. Jos muutosten jälkeen on ongelmia, voi kokeilla oikeuksien muuttamista!

Tiedostot:

```
$ find /var/www/oopperaskaala -type f -exec chmod 664 {} \;
```

Hakemistot:

```
$ find /var/www/oopperaskaala -type d -exec chmod 775 {} \;
```

Ryhmä: huom. wp-user on lisätty certin kanssa wp-config.php... Samoin www-data on lisätty wp-user ryhmään!

```
$ chgrp -R wp-user /var/www/oopperaskaala/
```

SALT:n lisäys.

Editoidaan wp-config-php tiedostoa lisäämällä SALT avaimet:
(avaimet saa generoitua -> $ curl -s https://api.wordpress.org/secret-key/1.1/salt/, kopioi avaimet määrittely tiedostoon).

```
define('AUTH_KEY',         'saltkey1 tähän');
define('SECURE_AUTH_KEY',  'saltkey2 tähän'');
define('LOGGED_IN_KEY',    'saltkey3 tähän'');
define('NONCE_KEY',        'saltkey4 tähän'');
define('AUTH_SALT',        'saltkey5 tähän'');
define('SECURE_AUTH_SALT', 'saltkey6 tähän'');
define('LOGGED_IN_SALT',   'saltkey7 tähän'');
define('NONCE_SALT',       'saltkey8 tähän'');
```

Wordpress backup.

Tehdään kotihakemistoon wp_backup hakemisto ja määritellään sinne wp_backup.sh tiedosto seuraavasti:

```
$ cd
```

$ mkdir wp_backup
$ cd wp_backup
$ nano wp_backup.sh

Ja lisää allaoleva teksti, muuta tarvittaessa databasename, username ja password sekä tarkista että hakemistot ovat oikein:

```
#!/bin/bash

# your backups will use these filenames.
db_backup_name="wp-db-backup-"`date "+%Y-%m-%d"`".sql.gz"
wpfiles_backup_name="wp-files-backup-"`date "+%Y-%m-%d"`".tar.gz"

## 1: database connection info. You can get these details from your wp-config file.
db_name="skaaladb"
db_username="skaala"
db_password="Gfjfkjghk579ghjj"

## 2: Path to your WordPress Upload and Theme directories. Replace /home/username/ with path to your home directory.
wp_upload_folder="/var/www/oopperaskaala/public_html/wp-content/uploads"
wp_theme_folder="/var/www/oopperaskaala/public_html/wp-content/themes"

## 3: Path to your backup folder. Replace /home/username/ with path to your home directory.
backup_folder_path="/home/aha/wp_backup"

# backup MYSQL database, gzip it and send to backup folder.
mysqldump --opt -u$db_username -p$db_password $db_name | gzip > $back-up_folder_path/$db_backup_name

# create a tarball of the wordpress files, gzip it and send to backup folder.
tar -czf $backup_folder_path/$wpfiles_backup_name $wp_upload_folder $wp_theme_folder
```

```
# delete all but 5 recent wordpress database back-ups (files having
.sql.gz extension) in backup folder.
find $backup_folder_path -maxdepth 1 -name "*.sql.gz" -type f | xargs -x
ls -t | awk 'NR>5' | xargs -L1 rm

# delete all but 5 recent wordpress files back-ups (files having .tar.gz
extension) in backup folder.
find $backup_folder_path -maxdepth 1 -name "*.tar.gz" -type f | xargs -x
ls -t | awk 'NR>5' | xargs -L1 rm
```

Liite 8. Käyttäjän Opas

3/30/2017

Käyttäjän Opas

Sähköpostin asetukset ja etäyhteyden muodostaminen

Ari Hartikainen

Käyttäjän Opas

Sähköpostitilin käyttö

Ooppera Skaala ry:n sähköpostin lukemiseen ja lähettämiseen liittyvät määritykset.

Sähköpostiin kirjaudutaan seuraavilla tiedoilla:

Tunnus: matti.meikalainen@oopperaskaala.fi (oma sähköpostiosoitteesi)

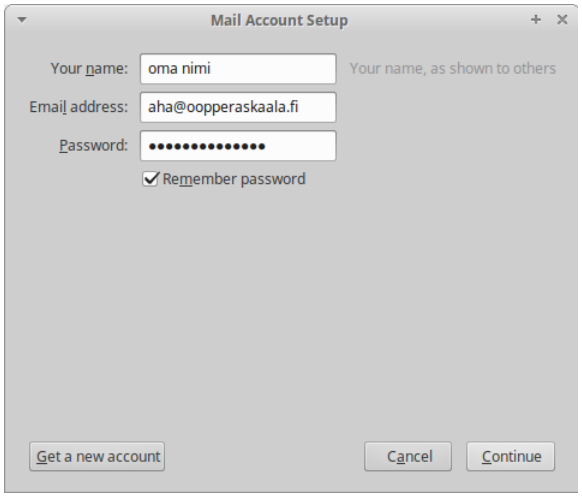
Salasana: Salasanan saat toimistolta.

Saapuva posti: IMAP, mx.oopperaskaala.fi, 993 (Portti), SSL/TLS (SSL), Normaali salasana (Todennus).

Lähtevä posti: SMTP, mx.oopperaskaala.fi, 587 (Portti), STARTTLS (SSL), Normaali salasana (Todennus).

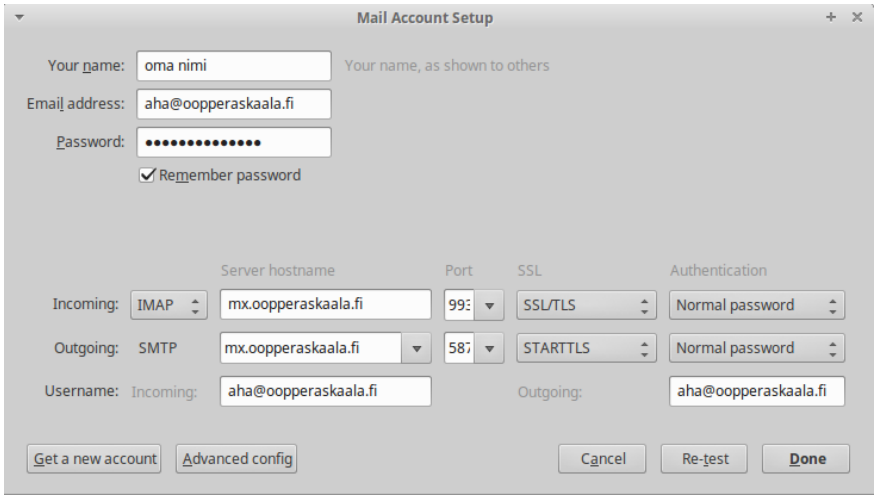
Mozilla Thunderbird

1. Avaa Thunderbird ja valitse ”uusi sähköpostitili”



Kirjoita Oma Nimesi (näkyy vastaanottajalla lähettäjän nimenä), sähköpostiosoitteesi ja salasanasi. Jatka valitsemalla ”Continue”.

2. Seuraavaksi valitse ”Manual config” (ilmestyy alariviin, kun painoit edellisessä kohdassa ”Continue”).



Lisää/muuta seuraavat kohdat:

Incoming: IMAP, mx.oopperaskaala.fi (Server hostname), 993 (Port), SSL/TLS (SSL), Normal password (Authentication).

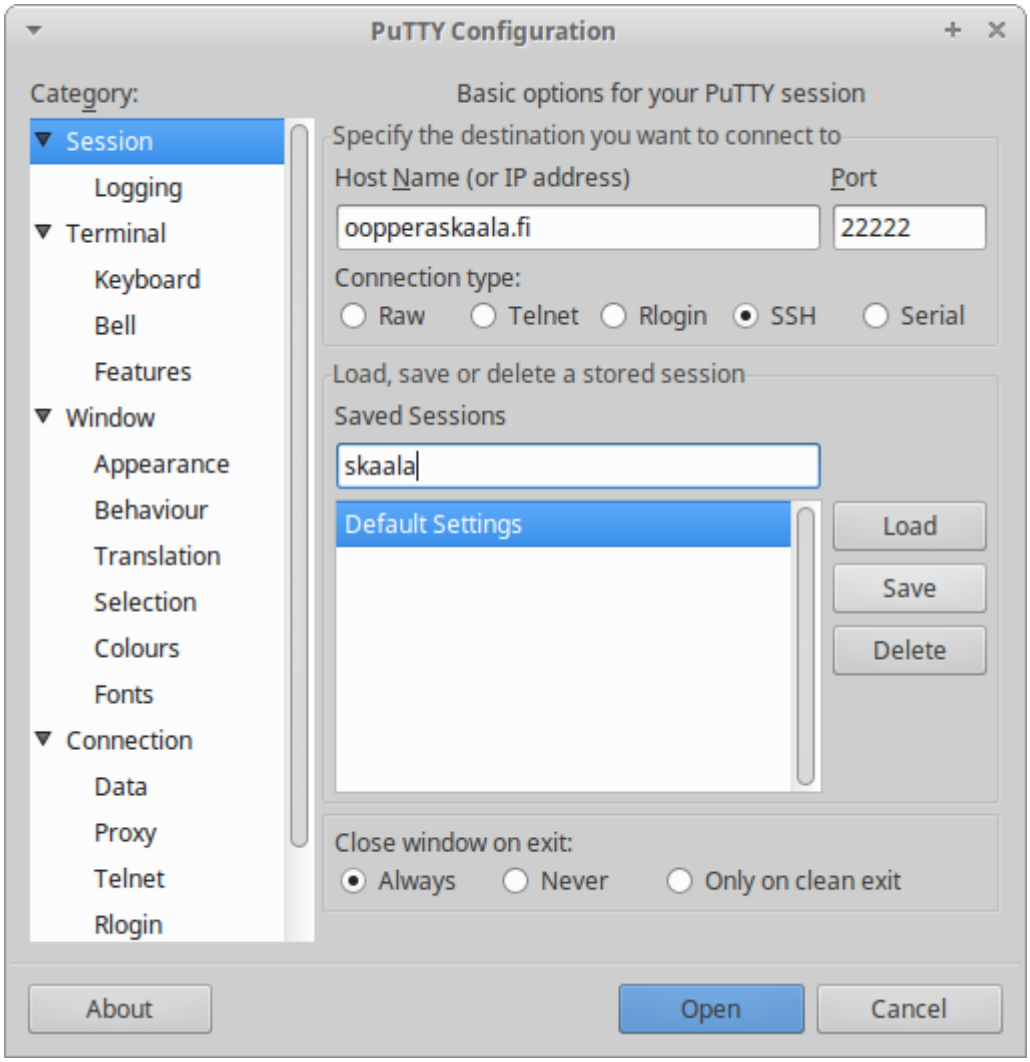
Outgoing: SMTP, mx.oopperaskaala.fi (Server hostname), 587 (Port), STARTTLS (SSL), Normal password (Authentication).

Username: sähköpostiosoitteesi (Incoming/Outgoing).

Tunnuksen ja salasanan saat toimistolta.

Yhteyden muodostamiseen käytetään Putty ohjelmaa. Puttyn voit ladata täältä http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Avaa Putty



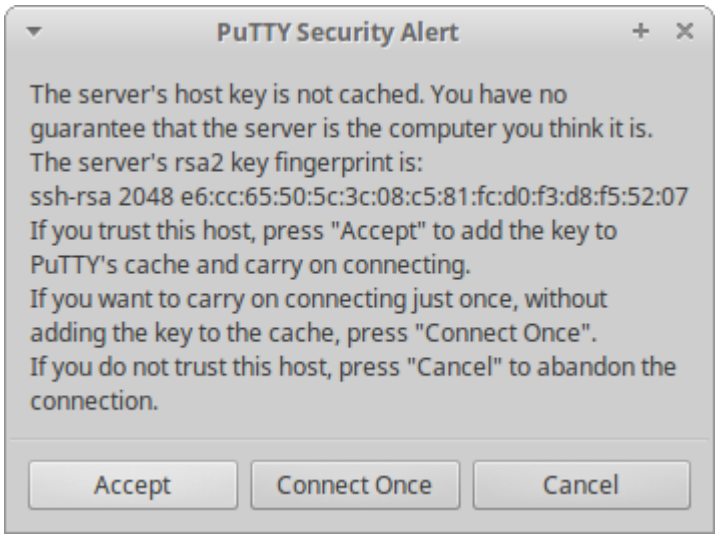
Määrittele Host name kohtaan: oopperaskaala.fi

Port kohtaan: 22222

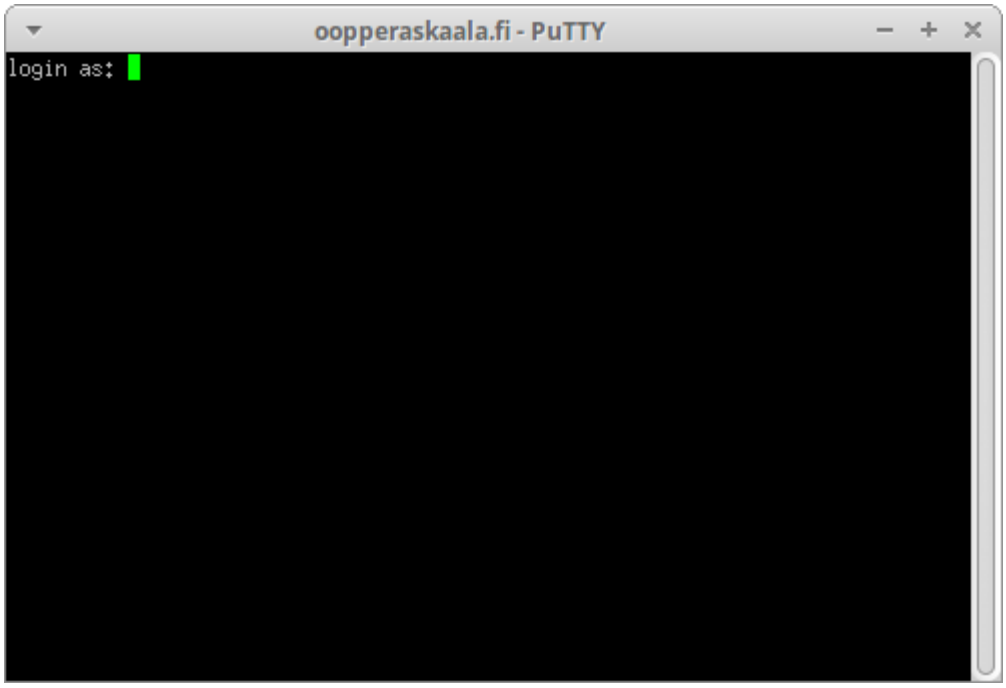
Tallenna asetukset, Saved Sessions kohtaan anna tallennukselle nimi: skaala

Paina Save nappia. Seuraavalla kerralla saat tarvittavat asetuksen käyttöön valitsemalla listasta ”skaala” ja ”Load”.

Seuraavaksi valitse ”Open”



Hyväksy yhteys (tämä ikkuna tulee vain ensimmäisellä yhteyskerralla).



Anna tunnuksesi ja salasanasi.