VERKKOPALVELIMEN TIETOTURVALLINEN KÄYTTÖÖNOTTO KOTIKÄYTTÖÖN

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus, Hämeenlinnan korkeakoulukeskus
syksy, 2021

Otto Wasenius

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus Tiivistelmä

Hämeenlinnan korkeakoulukeskus

Tekijä Otto Wasenius Vuosi 2021

Työn nimi Verkkopalvelimen tietoturvallinen käyttöönotto kotikäyttöön

Ohjaajat Erkki Laine

TIIVISTELMÄ

Työn tavoitteena oli suunnitella ja ottaa käyttöön toimiva verkkopalvelin, millä julkaista verkkosivut ja jakaa tiedostoja vain tietyille käyttäjille. Työ tehtiin omaan kotiin ja sen tarkoituksena oli toimia henkilökohtaisena verkkopalvelimena, mutta ratkaisua voi käyttää mahdollisesti myös yritysratkaisuissa.

Opinnäytetyössä tutkitaan ja vertaillaan verkkopalvelinohjelmia ja niiden ominaisuuksia ja tämän vertailun avulla päätetään mitä ohjelmaa käytetään kodin verkkopalvelimessa. Työssä tutkittiin myös käyttöjärjestelmiä ja niiden sopivuutta palvelinkäyttöön. Aineisto kertyi lukemalla artikkeleja, palstoja ja dokumentaatioita ja tekemällä itse asennuksia, testejä ja konfiguraatioita, mitkä johtivat toimiviin ratkaisuihin.

Käytännön osuudessa palvelimelle asennettiin Ubuntu-käyttöjärjestelmä ja palvelinohjelmistoksi valittiin Caddy sen luvatun helppokäyttöisyyden vuoksi ja koska siitä ei ole vielä paljoa dokumentaatiota, joten se on hyvä ohjelma tutkia. Palvelimen ja ohjelmistojen asennusten yhteydessä tehtiin jatkuvasti tietoturvaa edistäviä ja palvelimen jatkuvuutta edistäviä konfiguraatioita.

Työn lopputuloksena saatiin käyttöön toimiva ja turvallinen Caddy-verkkopalvelin, jolla pystyttiin jakamaan verkkosivuja ja tiedostoja paikalliseen ja julkiseen verkkoon käyttäen omaa domain-osoitetta ja käyttäjää.

Avainsanat Verkkopalvelin, Caddy, Tietoturva, Windows, Linux, Wordpress, Nextcloud

Sivut 49 sivua ja liitteitä 1 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Hämeenlinna University Centre

Abstract

Author Otto Wasenius
Year 2021
Subject Secure deployment of a web server for home use
Supervisors Erkki Laine

ABSTRACT

The purpose of the thesis was to install and configure a web server for home use. The server was intended to serve websites and files with access only to authenticated users. The work was done for home use and the server is intended to work as a personal server, but it can possibly be implemented on small enterprise solutions as well.

In the work different software and operating systems and their compatibility with server use is researched. The research is used to decide which software to use. Research material was produced by reading articles, columns, and documentations and by doing installations, tests and configurations that lead to working solutions.

The practical part of the work consisted of Ubuntu and Caddy software installation. Caddy was chosen for its easy installation and unfamiliarity, which meant it was possible to learn something new about server installations. Added to that configurations and installations were done that proved beneficial to the security of the server. The work focuses on making the server future-proof by configuring backups, updates, and other useful features.

The result of the work was a working web server that could be used for website and file sharing. The server is secure and accessible only by authenticated users. The server is accessible by the authenticated users from local network and public network using our domain.

Keywords Web server, Caddy, Security, Windows, Linux, Wordpress, Nextcloud
Pages 49 pages and appendices 1 pages

Sanasto

Active Directory	Windows-toimialueen hakemisto- ja käyttäjäpalvelu
Apt	Komento mihin lisäämällä esim. update voidaan suorittaa ohjelmien päivityksiä, asennuksia ja poistoja
BIOS	Ohjelma mikä lataa käyttöjärjestelmän ja käynnistää sen
DirectX	Kokoelma ohjelmointirajapintoja, jotka hoitavat multimedia toiminnot
Domain	Verkkotunnus
Gb	Gigatavu
GHz	Gigahertsi
GPT	Osointi kiintolevylle
HTML	HyperText Markup Language, verkkosivujen määrittelykieli
http	Hypertekstin siirtoprotokolla mitä selaimet käyttävät tiedonsiirtoon
https	Hypertekstin turvallinen siirtoprotokolla. http ja tls yhdistelmä
HDD	Kiintolevy
IIS	Palvelinohjelmisto Windows-laitteisiin
Kernel	Käyttöjärjestelmän ydin mikä hallitsee kaikkea järjestelmässä
Localhost	Osoitteen oma osoite, eli 127.0.0.1
Mt	Megatavu
Partitio	Kiintolevyn osiointi
Proxy	Välityspalvelin
Root	Juurihakemisto tai pääkäyttäjä
Reverse proxy	Välimies palvelimen ja asiakkaan välillä. Voi piilottaa palvelimen ja parantaa sen resurssienkäyttöä.
Repositorio	Kokoelma metadataa tiedostoille tai kansioille
Samba	Ohjelma millä voi tehdä tiedoston jaon Linux ja Windows-järjestelmien välillä
Sovellusarja	Kokoelma työprosesseja
SSH	Secure Shell, salattu tietoliikenne protokolla
TLS	Protokolla mikä suojaa internet yhteydet tehty IP-osoitella

UEFI	BIOS korvaava ohjelma mikä toimii käyttöjärjestelmän ja firmwaren välissä
VPS	Virtuaalinenpalvelin
WDDM	Videoajuri arkkitehtuuri näytönohjaimille
WWW	World wide web
IP	Protokolla mikä huolehtii IP-tietoliikennepakettien toimittamisesta

Sisällys

Kuvat, ohjelmakoodit ja taulukot

Liitteet

1 Johdanto

Itselleni esiintyi tarve verkkopalvelimelle, jolla voin jakaa tiedostoja ja verkkosivuja kotiverkkoon ja ulkoverkkoon. Työ käsittelee myös tietoturvaa, että mahdolliset tietomurrot voidaan välttää tulevaisuudessa. Omassa käytössäni on paljon eri laitteita, joiden välillä haluan jakaa tiedostoja kuten pelejä, videoita ja musiikkia helposti. Tässä helpottaisi verkkosivut mihin voisin suoraan siirtää tiedostoja ja ladata niitä tarpeen mukaan.

Palvelin luodaan käyttämällä omasta kodista löytyvää ylimääräistä tietokonetta ja koska budjetti ei ole suuri, ainut päivitys koneeseen on tallennuskapasiteetin osto. Tietokone on asennettu valmiiksi ja sen tehot riittävät kotikäyttöön. Vastaavanlaisia palvelimia voi nähdä myös yrityksien käytössä, joten työstä on hyötyä myös työelämässä.

Jotta palvelimesta saataisiin toimiva ja käyttökelpoinen, pitää vastata seuraaviin tutkimuskysymyksiin:

1. Miten ohjelmat IIS, Caddy, Apache Server ja NGINX eroavat toisistaan?
2. Linux- vai Windows-käyttöjärjestelmä verkkopalvelimelle?
3. Kuinka luoda toimiva ja turvallinen verkkopalvelin?
4. Miten varmistaa verkkopalvelimen koventaminen, päivitykset, varmuuskopiointi ja palautus?

Tietoturvan huomioonotto tässä työssä oli tärkeää, johtuen palvelimen sisältämistä tiedostoista. Tiedostopalvelimelle on tarkoituksena tallentaa suuria määriä dataa, mistä osa saattaa sisältää henkilökohtaista tietoa. Täydellistä tietoturvallisuutta on mahdotonta saavuttaa, mutta tavoitteena on suojautua yleisimmiltä uhilta verkossa.

Tietoturvan lisäksi on tärkeää, että palvelimen palvelut ovat helppoja käyttää ja hyödyllisiä, että tarve muiden tarjoamille palveluille vähenee. Tämän saavuttaminen on vaikeata, mutta ei mahdotonta. Palvelimen käyttötarkoitus on hyvä varmistaa ennen asennusta. Mikäli palvelimen käyttötarkoitus muuttuu asennuksen jälkeen, voi se johtaa erilaisiin ongelmiin. Esimerkiksi ohjelmien yhteensopivuus käytössä olevan käyttöjärjestelmän kanssa on erittäin

tärkeä ottaa huomioon palvelinta suunnitellessa. Palvelimen käyttötarkoituksen muuttuminen voi kyllä tapahtua, mikäli käyttäjien tarve muuttuu, jolloin on suositeltavaa suunnitella uudestaan palvelimen asennus, käyttöönotto ja konfiguraatio. Työssä käytettävä palvelinohjelmisto valittiin muiden ohjelmien vertailun jälkeen. Vaikka käytetty vaihtoehto ei olekkaan suosituin, on se silti erittäin sopiva vaihtoehto kyseiseen käyttötarkoitukseen.

Tämä työ on erittäin käytännönläheinen, mikä voi poiketa perinteisestä opinnäytetyöstä. Käytönnönosuudessa asioita käydään läpi hieman ohjemaisesti, mutta tämä on tarkoituksella, mikäli lukija haluaa tehdä samanlaisia asennuksia. Teoriaosuus kattaa tarvittavat taustatiedot liittyen käytettäviin palvelinohjelmiin ja niiden ominaisuuksiin. Tietoturva osuus työssä on vain pintaraapaisu mitä oikeasti tietoturvalla tarkoitetaan, mutta työssä käydään tarvittavat suojaustoimenpiteet läpi, että varmistetaan riittävän turvallinen palvelinympäristö.

2 Verkkopalvelimen käyttöjärjestelmät

Palvelimen käyttöjärjestelmän valinta on tärkeää, joten työssä tutkitaan kahta mahdollista käyttöjärjestelmää Windows ja Linux. Kotikäytössä valinnanvaraa on rajoitetummin johtuen budjetista ja koska Mac-laitteita ei ole, ei niitä voi käyttää työssä. Windows-käyttöjärjestelmistä käytetään ainoastaan Windows 10 -käyttöjärjestelmää. Linux-käyttöjärjestelmistä voidaan valita melkein minkä tahansa työlle sopiva järjestelmä.

Windows 10 Home edition on Microsoftin tuottama helppokäyttöinen ja suosittu käyttöjärjestelmä. Siinä on valmiina tietoturvaominaisuuksia kuten antivirus, palomuuri ja verkkosuojauksia. Käyttöjärjestelmään tulee jatkuvasti päivityksiä ja sen tuki jatkuu vuoteen 2025 asti. Windows 10 -käyttöjärjestelmä vaatii palvelimelta 1GHz tai nopeamman prosessorin, vähintään 1GB muistia, vähintään 32GB tallennuskapasiteetin, DirectX9 tai myöhemmän yhteensopivan näytönohjaimen WDDM 1.0 ajurilla, näytön vähintään 800x600 tarkkuudella ja verkkoyhteyden päivitysten suorittamiseksi. Windows 10 -käyttöjärjestelmällä on paljon ominaisuuksia mitkä helpottavat normaalia käyttöä. Se sisältää paljon helppokäyttötoimintoja, työkaluja kouluun ja muuta. (Microsoft Corporation, 2021)

Windows 10 -käyttöjärjestelmästä löytyy valmiiksi Internet Information Services (IIS) -palvelinohjelma. IIS-palveluun kuuluva WWW-palvelu hallitsee HTTP ylläpidon ja asetukset, prosessin hallinnan ja suorituskyvyn seurannan. IIS 7 ja myöhemmissä versioissa Windows Process Activation Service (WAS) hallitsee sovellussarjoja ja työprosesseja. (Templin;Moore;Schonning;& Patel, 2007)

Tämän lisäksi on saatavilla myös aiemmin mainitut Caddy-, Apache Server- ja NGINX-ohjelmat. Myös muita ohjelmia kuten Lighttpd ja OpenLiteSpeed on käytettävissä, mutta näitä ei käsitellä tässä työssä.

Toinen vaihtoehto Ubuntu 20.04 on suosittu Linux-jakelu, mikä toimii hyvin normaalissa käytössä ja palvelin käytössä. Asennuksen yhteydessä voi valita asennuksen tyypiksi minimaalisen tai normaalin, mikä vaikuttaa mitä ohjelmia asennuksen mukana tulee. Käyttöjärjestelmän tuen päättymistä ei ole ilmoitettu vielä (Wood, 2021).

Ubuntu minimivaatimukset palvelimelta on vähintään 1023 Mt muisti, 7 GB tallennuskapasiteettia, näyttö vähintään 1023x768 tarkkuudella ja USB portti tai DVD asema. Suositellut vaatimukset laitteistolle on 8192 Mt muistia, 64 GB tallennuskapasiteettia, näyttö vähintään 1280x720 tarkkuudella ja USB portti tai DVD asema. (wiki.Ubuntu-fi.org, 2021)

Ubuntu on ilmainen, helppokäyttöinen, suomenkielinen ja turvallinen käyttöjärjestelmä. Sen mukana tulee paljon ohjelmia tekstinkäsittelyyn, laskentaan, selaamiseen, viestintään ja muuhun. Ubuntu-käyttöjärjestelmästä on ladattavissa monta eri versiota eri käyttötarpeisiin. Esimerkiksi versio ilman työpöytää on ladattavissa Ubuntun sivuilta. (Ubuntu-fi.org, 2021)

Ubuntu-käyttöjärjestelmään saa asennettua useita eri palvelinohjelmia. Caddy, NGINX ja Apache Server toimivat myös Linux Ubuntu -käyttöjärjestelmässä. Myös muita ohjelmia kuten Lighttpd, OpenLiteSpeed, Hiawatha jne. on käytettävissä, mutta näitä ei käsitellä tässä työssä.

3 Verkkopalvelinohjelmistojen vertailu ja valinta

Työssä käydään läpi neljä eri palvelinohjelmistoa ja niiden hyötyjä, haittoja ja ominaisuuksia. Käsiteltäviksi ohjelmiksi valittiin IIS, Caddy-, Apache Server- ja NGINX-ohjelmat. Ohjelmista löytyy laajasti mielipiteitä, joten työssä tutkitaan monia näkökulmia, että löydetään mahdollisimman tarkat kuvaukset ohjelmista.

IIS on Windows 10 -käyttöjärjestelmästä löytyvä Microsoftin valmistama palvelinohjelma. Sen käyttöön löytyy laajat ohjeet Microsoftin omilta sivuilta. IIS-palvelulla voidaan ylläpitää verkkopalveluja, kuten FTP-palvelin, applikaatio tai verkkosivut. Se ajetaan Microsoftin .NET alustalla Windows-käyttöjärjestelmissä. (Vuollet, 2018). Seuraavaksi verrataan IIS-palvelinohjelmiston hyötyjä ja haittoja (Taulukko 1).

Taulukko 1 IIS-palvelinohjelmiston hyödyt ja haitat

Hyödyt	Haitat
Graafinen käyttöliittymä auttaa uusia käyttäjiä ja sillä on hyvä integraatio suorituskyvyn seurannan kanssa (Hilton, 2021)	Palvelin ei ole kestävä ja saattaa vaatia uudelleenkäynnistyksen palautuakseen (Hilton, 2021).
IIS käyttää vähemmän CPU tehoa kuin Apache (Janjic, 2017)	IIS-palvelinta voi hallita vain graafisella käyttöliittymällä, mikä tekee palvelimen hallinnasta isomman työn, kun ei ole mahdollista muokata asetuksia yhdellä konfiguraatiotiedostolla (Hilton, 2021).
IIS voi hallita useampi pyyntöjä sekunnissa kuin Apache (Janjic, 2017).	Huonompi suoritusteho verrattuna muihin palvelinohjelmistoihin kuten Nginx ja Apache (Dhangar, 2019).
Helppo asennus ja käyttöönotto (Brown, 2020).	Koska ohjelmalla ei ole avoin lähdekoodi, voi se olla suurempi tietoturvariski (Dhangar, 2019).
Tietoturva päivitykset tulevat käyttöjärjestelmän päivitysten mukana (Brown, 2020).	Epämääräiset lokitiedostot saattavat hidastaa vianetsintää (Dhangar, 2019).
Active Directory integrointi mahdollistaa nopean yhden kirjautumisen ilman salasanaa (Brown, 2020).	Tietoturva voi olla vaikeaa, jos haluaa käyttää kolmannen osapuolen todennusta (Kochtan, 2019).

Vianetsintä on helppoa johtuen palvelimen pitämistä lokitiedostoista (Dhangar, 2019).	
Koska Microsoft IIS on yleisessä käytössä löytää sen käyttöön helposti apua (Kochtan, 2019).	
Paras suoritusteho Microsoftin työkalujen ja palvelujen kanssa (Dhangar, 2019).	

Caddy on tehokas, avoimen lähdekoodin verkkopalvelin missä on valmiiksi saatavilla HTTPS. Caddy on kirjoitettu Go-ohjelmointikielellä. Caddy kuvaillaan yksinkertaiseksi, tietoturvalliseksi ja helppokäyttöiseksi. Se hakee ja päivittää TLS-sertifikaatit automaattisesti. Sitä voi käyttää staattisena verkkosivuna ja käänteisenä välityspalvelimena (Caddyserver.com, 2021). Vertaamalla hyötyjä ja haittoja huomataan, että ohjelmassa on joitain ongelmia, mutta paljon hyviäkin puolia kuten automaattinen TLS asennus ja päivitys (Taulukko 2).

Taulukko 2 Caddy-palvelinohjelmiston hyödyt ja haitat

Hyödyt	**Haitat**
Automaattinen TLS asennus ja päivitys (caddyserver.com, 2021).	Heikko suorituskyky (Buranasanti, 2019).
Caddy on yksinkertainen (Buranasanti, 2019).	Dokumentaatio voi olla hankala lukea ja mallitiedostot eivät välttämättä toimi normaali käyttötapauksissa (Salter, 2020).
Avoin lähdekoodi (caddyserver.com, 2021).	Konflikteja versioiden 1 ja 2 konfiguraatioiden välillä (Salter, 2020).
Sallii myös omat sertifikaatit (caddyserver.com, 2021).	Helppo eksyä Caddy v1 ohjeisiin, kun etsii ohjeita Caddy v2:seen (Salter, 2020).
Skaalattavissa (caddyserver.com, 2021).	
Tyylikäs tiedostojen ja kansioiden selain (caddyserver.com, 2021).	
Toimii Windows, Mac, Linux järjestelmillä (Buranasanti, 2019).	
Helppo asentaa ja päivittää (Salter, 2020).	
Voidaan siirtää eri Linux-jakelujen välillä ilman konflikteja (Salter, 2020).	

Apache http-palvelin on avoimen lähdekoodin palvelin, mikä toimii moderneilla käyttöjärjestelmillä kuten UNIX ja Windows. Sen tavoitteena on olla turvallinen, tehokas ja

laaja palvelin mikä tarjoaa http-palveluja nykyaikaisilla standardeilla (httpd.apache.org, 2021). Apache http-palvelimella voi ylläpitää staattisia sivuja. Apache on yhteensopiva IPv6 kanssa ja tukee myös HTTP/2 protokollaa. Apache http-palvelinta käyttää suositut yritykset kuten eBay, Adobe, PayPal, Linkedin ja Facebook (Fahim, 2020). Apache http-palvelimella on paljon hyötyjä, mutta myös huomattavia ongelmia (Taulukko 3). Kuitenkin ohjelma on erittäin toimiva ja hyvä vaihtoehto moniin palvelin ratkaisuihin.

Taulukko 3 Apache Http Server-palvelinohjelmiston hyödyt ja haitat

Hyödyt	Haitat
Avoin lähdekoodi (httpd.apache.org, 2021).	Mahdollisuus muokata koodia saattaa aiheuttaa tietoturvaongelmia (Fahim, 2020).
Mahdollisuus lisätä moduuleja ja palveluja (Fahim, 2020).	Mahdollisuus muokata koodia saattaa aiheuttaa vikoja ja ongelmia (Fahim, 2020).
Luotettava (Fahim, 2020).	Jatkuva päivitys on tarpeen ja pitää tehdä tietyn ajan välein (Fahim, 2020).
Hyvä suorituskyky (Fahim, 2020).	Suorituskyky ongelmia sivuilla, joilla on paljon vierailijoita (Fahim, 2020).
Voidaan käyttää kaikilla käyttöjärjestelmillä (Fahim, 2020).	
Yhteisö on aktiivinen ja päivittää ohjelmistoa (Fahim, 2020).	
Hyödyllinen ja kattava dokumentaatio (Fahim, 2020).	

NGINX on ilmainen ja avoimen lähdekoodin http-palvelin hyvällä suorituskyvyllä ja käänteisellä välityspalvelimella. Se on tunnettu sen suorituskyvystä, yksinkertaisesta konfiguraatiosta ja matalasta resurssien käytöstä (Nginx.com, 2021). NGINX-palvelinohjelmistosta löytyy paljon hyötyjä ja vähän haittoja (Taulukko 4).

Taulukko 4 NGINX-palvelinohjelmiston hyödyt ja haitat

Hyödyt	Haitat
Kevyt ja käyttää vähän muistia kuin Apache (Keycdn.com, 2018).	Pienempi tuki yhteisöltä kuin Apachella (Keycdn.com, 2018).

Kestää yli 10 tuhatta yhdenaikaista yhteyttä pienellä muistin kulutuksella (Keycdn.com, 2018).	Vähemmän moduuleja (Keycdn.com, 2018).
Parempi skaalautuvuus verrattuna Apacheen (Keycdn.com, 2018).	
Suositeltu sivuille, jotka käyttävät VPS (Keycdn.com, 2018).	
Kuormituksen tasapainotus (Kinsta.com, 2021).	

Nyt kun on tutkittu ohjelmien ominaisuuksia, hyötyjä ja haittoja, voidaan valita mikä ohjelma otetaan käyttöön kotipalvelimelle. Yleisin valinta olisi todennäköisesti Apache tai NGINX johtuen niiden nopeudesta, suosiosta ja luotettavuudesta, mutta vähemmän tunnettu Caddy -ohjelma vaikuttaa myös lupaavalta vertailun perusteella. IIS-ohjelmaa voitaisiin käyttää, mikäli käyttöjärjestelmänä olisi Windows 10.

Jos palvelin olisi julkisessa käytössä suurella kävijämäärällä, olisi paras vaihtoehto NGINX johtuen sen tehokkaasta kuormituksenhallinnasta, mutta kyseistä palvelinta käyttää rajoitettu määrä ihmisiä. Koska palvelin tulee kotikäyttöön, on Caddy täysin hyvä valinta johtuen sen helposta asennuksesta ja automaattisesta HTTPS-konfiguraatiosta.

4 Palvelimen tietoturva ja jatkuvuus

Koska palvelimeen on tarkoitus päästä käsiksi sisäverkon lisäksi myös ulkoverkosta, on tärkeää ottaa huomioon tietoturva käyttöönoton yhteydessä ja sen jälkeen. Myös sisäverkon tietoturva pitää varmistaa. Yksi tietoturvariski on se, että ulkopuolinen käyttäjä pääsee varastamaan tai tuhoamaan tietoa palvelimelta, mikäli sitä ei ole huolella suojattu. Palvelinta asentaessa pitää siis varmistaa, että vain tietyt käyttäjät pääsevät käsiksi palvelimen sisältöön ja konfiguraatioon ja että kyseiset käyttäjät ovat suojattu vahvalla salasanalla. Myös fyysinen suojaus on tärkeää, eli palvelin pitää asettaa turvalliseen paikkaan, missä se on suojassa vahingoilta ja muilta ihmisiltä. Tietoturvassa otetaan huomioon muutama eri osa-alue. Näistä tärkeimpiä ovat käyttäjät, palomuuri, sisäverkko, koventaminen ja laitteet. (Taulukko 5)

Taulukko 5 Verkkopalvelimen tietoturvan osa-alueet

Aihe	Tavoite
Käyttäjät	Varmistetaan, että käyttäjillä on vahvat salasanat.
Palomuuri	Avataan vain tarvittavat portit ja vain luotettaville IP-osoitteille.
Virustorjunta	Mikäli käytössä olisi Windows 10 -käyttöjärjestelmä, voitaisiin asentaa esimerkiksi Norton Antivirus, vaikka Windows 10 -käyttöjärjestelmän oma antivirus onkin yleensä riittävä. Ubuntu -käyttöjärjestelmässä ei yleensä ole tarvetta antivirukselle. Paras tapa välttää viruksia on käyttää järkeä verkossa.
Ohjelmistot	Varmistetaan käytettävien ohjelmien päivitykset, luotettavuus ja tietoturva.
Laitteet	Estetään pääsy fyysisiin laitteisiin ulkopuolisilta.
Sisäverkko	Varmistetaan että sisäverkon langattomat yhteydet ovat suojattuja. Estetään ulkopuolisten pääsy sisäverkkoon.
Ulkoverkko	Estetään ulkoverkosta pääsy palvelimeen, ilman luotettavaa IP-osoitetta ja tunnuksia.
Varmuuskopiointi	Varmistetaan, että sähkökatkokset, tulipalot tai vastaavat tapahtumat eivät tuhoa kaikkea dataa tekemällä

	varmuuskopioita tärkeistä tiedostoista. Myös varmuuskopiot on suojattava ulkopuolisilta.
Koventaminen	Poistetaan turhat palvelut, muutetaan oletusportteja, poistetaan esimerkkitunnukset, vaihdetaan oletussalasanat, muokataan heikkoja oletusarvoja, poistetaan turhat protokollat käytöstä (Malmberg, 2017).

Tietoturvalla tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista (blogs.helsinki.fi, 2021). Jokaisella olisi hyvä olla nämä periaatteet hallinnassa, mikäli aikomuksena on tehdä palveluja henkilökohtaiseen tai julkiseen käyttöön. Erityisesti julkisilla palvelimilla on tärkeää ottaa huomioon tietoturvan eri periaatteet:

- **Luottamuksellisuus** - Varmistetaan, että tiedot ovat saatavilla vain oikeutetuille käyttäjille (Kyberturvallisuuskeskus.fi, 2020).
- **Eheys** - Palvelimessa olevaa tietoa ei voi muuttaa muut kuin siihen oikeutetut (Kyberturvallisuuskeskus.fi, 2020). Palvelimella olevat tiedot eivät muutu tai tuhoutu hallitsemattomasti (juhanit.wordpress.com, 2013).
- **Käytettävyys** - Tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä (Kyberturvallisuuskeskus.fi, 2020).
- **Todentaminen** - Tämä tarkoittaa käyttäjän tai järjestelmän luotettavaa tunnistettavuutta. Siinä käytetään esim. muutettavia avaintunnuksia, salasanoja ja sertifikaatteja. (blogs.helsinki.fi, 2021)

4.1 Verkon topologia

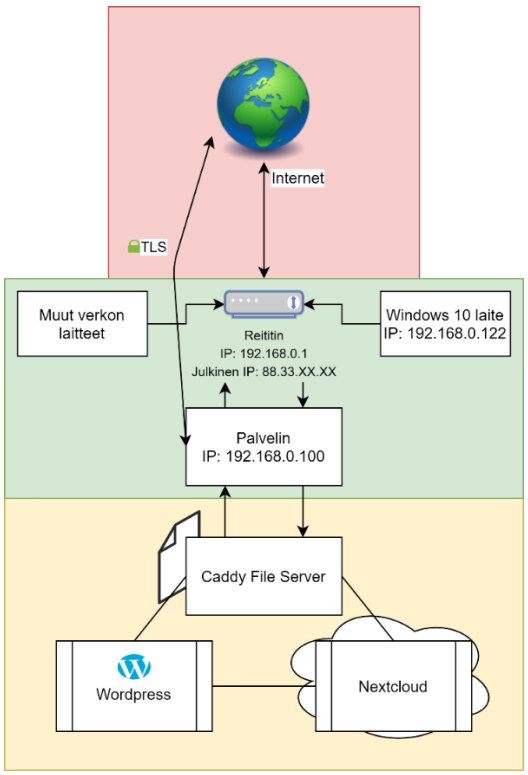
Kun halutaan varmistaa verkon turvallisuus, on hyvä suunnitella sen topologia. Suunnitellaan mikä laite tai palvelu yhdistää mihin laitteeseen tai palveluun. Kotiverkossa on useita laitteita, mitkä yhdistävät reitittimen kautta ulkoverkkoon ja sisäverkkoon. Esimerkiksi Windows 10-laite yhdistää verkossa reitittimen kautta verkkoon ja sitä kautta kommunikoi muiden laitteiden ja palveluiden kanssa sisä- ja ulkoverkossa. Jokaiselle laitteelle on hyvä miettiä omat tietoturvatarpeet. Windows-laitteissa on hyvä olla päällä antivirus ja palomuuri ja Linux-laitteissa palomuuri. Yleisesti kaikki laitteet verkossa yhdistävät reitittimen kautta verkkoon. Tämän vuoksi myös reitittimen konfiguraatio on otettava huomioon.

Palvelin puolella pyörii useita palveluja. Näistä tärkein tässä työssä on Caddy. Caddy ylläpitää tiedostopalvelinta ja jakaa verkkosivut sisä- ja ulkoverkkoon, kun se on asennettu ja konfiguroitu oikein. Caddy-palveluun asennettavia Nextcloud- ja Wordpress-palveluita käytetään verkkosivujen ylläpitoon ja pilvitallennustilan käyttöön. Wordpress ylläpitää ja julkaisee sivuja Caddy-palvelimessa ja Nextcloud ylläpitää tiedostojen tallennustilaa pilveen. Wordpress ja Nextcloud eivät kuitenkaan kommunikoi keskenään, muuta kuin linkeillä mistä pääsee sivuilta toiselle.

Palvelin julkaisee sivuja suojatulla HTTPS-yhteydellä minkä se luo automaattisesti sivujen asennuksen yhteydessä. Normaalisti sivuihin päästään käsiksi käyttämällä palvelimen IP-osoitetta, mutta konfiguraatiossa ohjataan omistettu domain niin, että päästään verkkosivuihin ja palveluun käsiksi käyttämällä oma-domain.fi osoitetta ilman tarvetta IP-osoitteelle.

Verkon topologia itsessään on yksinkertainen. Palvelut toimivat itsenäisesti ja yhdessä ja laitteet kommunikoivat reitittimen kautta keskenään tai ulkoverkon kautta palvelimen kanssa (Kaava 1). Palvelimessa on asennettuna UFW-palomuuri, mikä hallitsee, mikä portti on auki. Windows-laitteissa on asennettuna palomuuri sekä antivirus.

Kaava 1 Verkkotopologia



4.2 Palvelimen jatkuvuus

Verkkopalvelimen jatkuvuudella tarkoitetaan sen tulevaisuuden toimivuuden varmistamista. Tavoitteena on varmistaa, että tulevaisuudessa ei esiinny ongelmia mitkä estävät palvelimen toimivuuden. Työssä käydään läpi verkkopalvelimen päivitykset, varmuuskopiointi, palautuminen ja koventaminen. Nämä ovat myös tärkeä osa tietoturvaa.

Palvelimen päivitykset voidaan automatisoida tarvittaessa, niin että manuaalinen päivittäminen ei ole jatkuvasti tarpeellista, eikä tärkeät tietoturva päivitykset unohdu. Käytettävien ohjelmien, käyttöjärjestelmän ja palvelinohjelmiston päivitykset ovat tärkeä varmistaa, ettei käytössä ole vanhentuneet versiot.

Varmuuskopiointi on tärkeää, mikäli tapahtuu jotain odottamatonta, kuten tulipalo, hakkerointi tai käyttäjän aiheuttamia vikoja. Varmuuskopiot on hyvä tehdä ulkoiselle asemalle tai esimerkiksi pilveen. Varmuuskopiot on hyvä ajoittaa tasaisen ajan välein, riippuen miten usein palvelimelle tulee muutoksia. Esimerkiksi kerran viikossa on yleensä hyvä aika varmuuskopioida palvelimella missä muutoksia tapahtuu vain vähän viikon aikana.

Palautuminen tehdään, kun halutaan palata palvelimen aiempaan versioon. Yleensä näin tehdään, kun on tapahtunut virhe järjestelmässä tai konfiguraatiossa, mistä palautuminen manuaalisesti on mahdotonta tai liian monimutkaista. Jotta palautuminen voidaan tehdä, tarvitaan toimiva varmuuskopio järjestelmästä ja tiedostoista.

Koventamisessa poistetaan turhat palvelut, muutetaan oletusportteja, poistetaan esimerkkitunnukset, vaihdetaan oletussalasanat, muokataan heikkoja oletusarvoja ja poistetaan turhat protokollat käytöstä (Malmberg, 2017). Tämä edistää myös tietoturvaa huomattavasti ja vaikeuttaa mahdollisten hyökkääjien työtä.

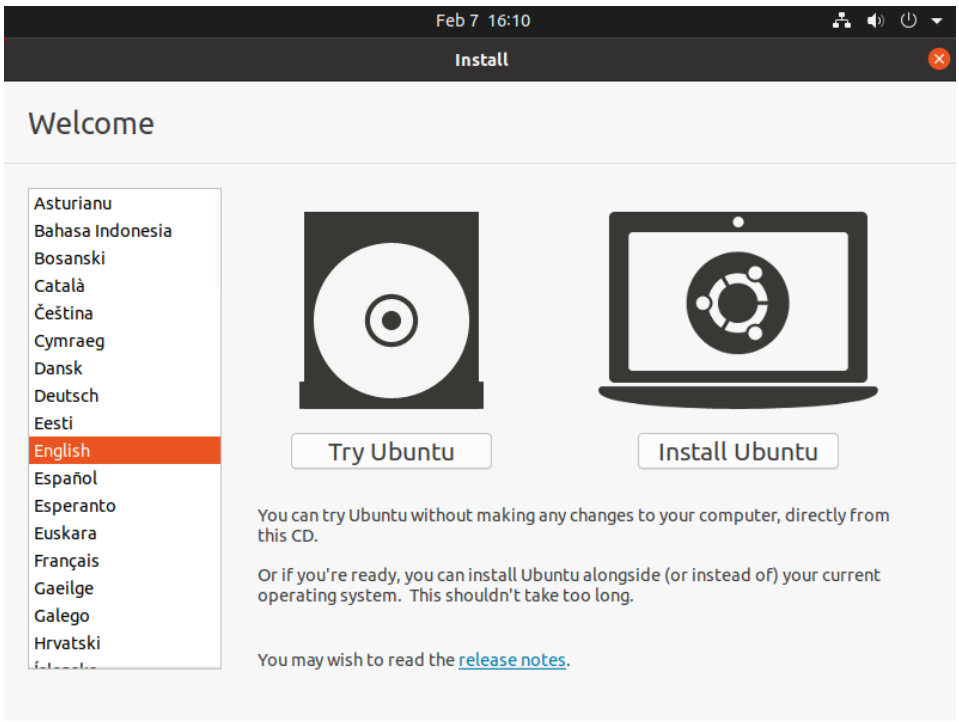
5 Verkkopalvelimen käyttöjärjestelmän asennus

Tässä osassa asennetaan käyttöjärjestelmä palvelimelle. Tämä vaihe on yksi helpoimmista tehtävistä työssä ja varsin suoralinjainen, vaikka tiettyihin asioihin pitää kiinnittää huomiota.

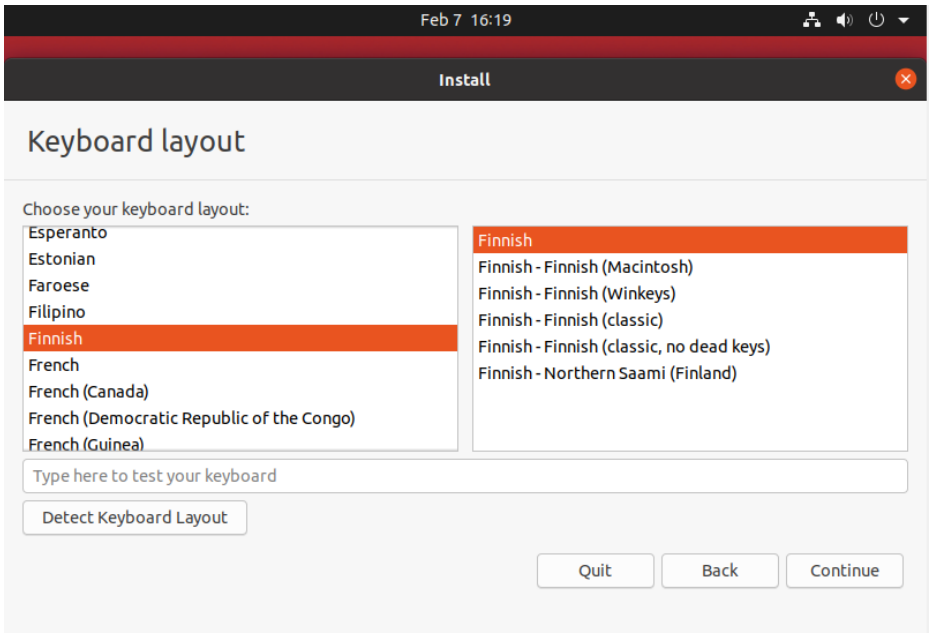
Aloitetaan Ubuntu-käyttöjärjestelmän asennuksella. Asennukset käydään läpi vaihe vaiheelta. Ubuntu-käyttöjärjestelmästä on saatavilla myös työpöydätön versio, mikä on hyvä palvelinkäytössä. Tässä työssä palvelin otetaan kotikäyttöön, joten asennetaan työpöytäversio, että laitetta voi käyttää myös normaalina tietokoneena tarvittaessa. Asennus tapahtuu USB tikulta. Tietokone käynnistetään USB tikulta löytyvään asennusohjelmaan ja Ubuntu-käyttöjärjestelmän asennus voidaan aloittaa.

Asennus alkaa valitsemalla kielen ja valitsemalla **Install Ubuntu** (Kuva 1), jonka jälkeen valitaan näppäimistön kieli ja painetaan Continue (Kuva 2).

Kuva 1 Ubuntu asennus - Aloitus

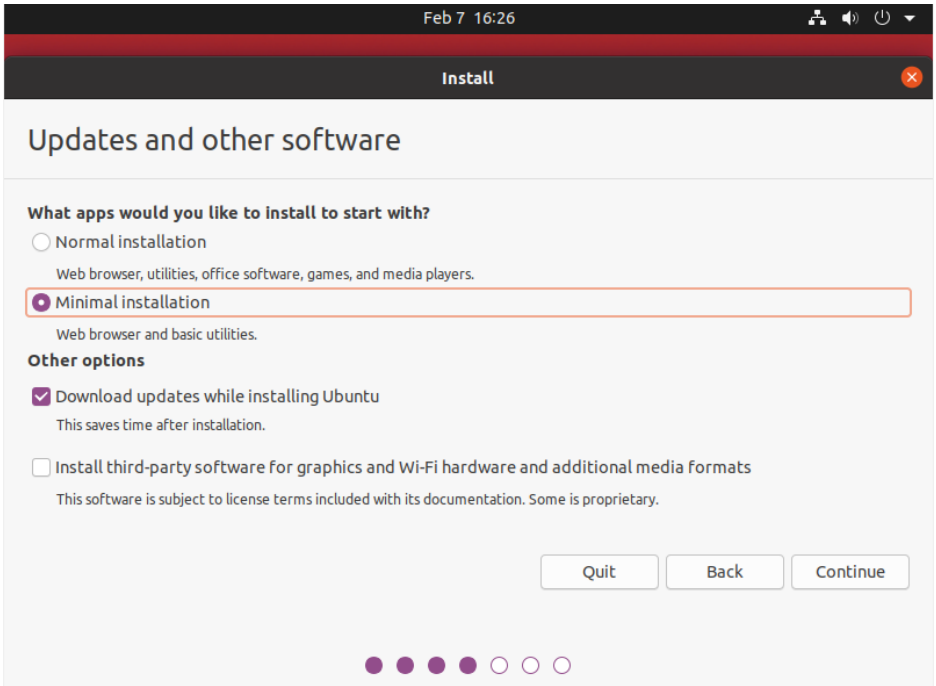


Kuva 2 Ubuntu asennus - Näppäimistön kieli



Kun näppäimistön kieli on valittu, siirrytään valitsemaan asennustyyppi ja muita asetuksia. Tässä kohtaa valitaan **Minimal Installation** ja **Download updates while installing Ubuntu** minkä jälkeen painetaan **Continue** (Kuva 3).

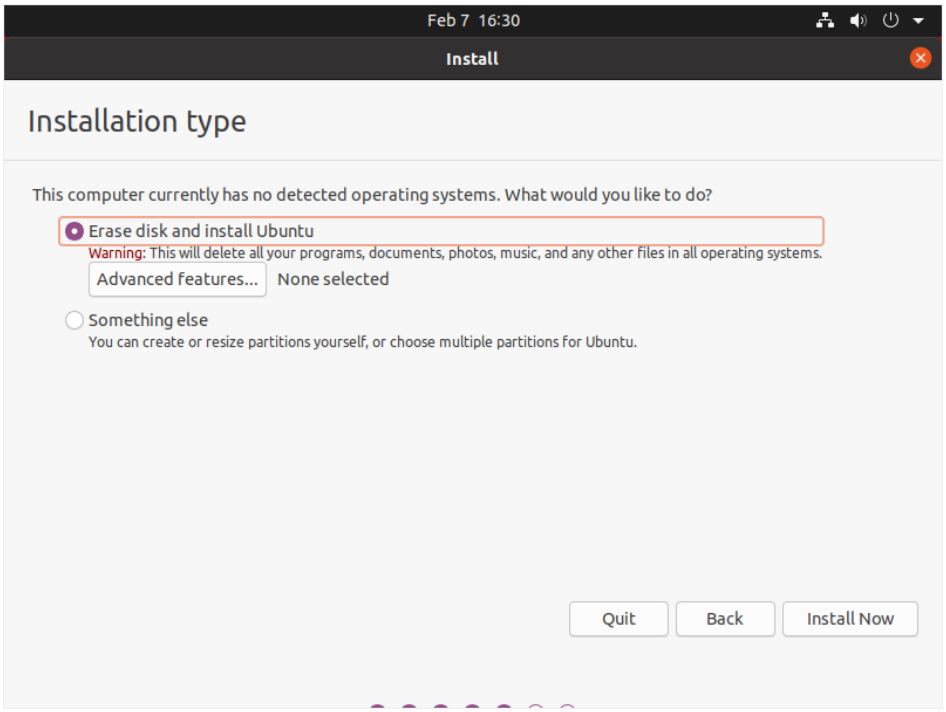
Kuva 3 Ubuntu asennus - Minimaalinen asennus ja päivitykset valinta



Seuraavassa kohdassa valinta saattaa muuttua riippuen millaiseen laitteeseen käyttöjärjestelmä asennetaan. Koska työssä käytetyn laitteen tallennustila on tyhjä, voidaan

valita **Erase disk and install Ubuntu** minkä jälkeen painetaan **Install Now** (Kuva 4). Tämän jälkeen saattaa tulla vahvistuskysymys missä valitaan **Continue.** Mikäli halutaan tehdä kiintolevyn partitiointi itse, voidaan tässä kohtaa hypätä kohtaan 5.1.

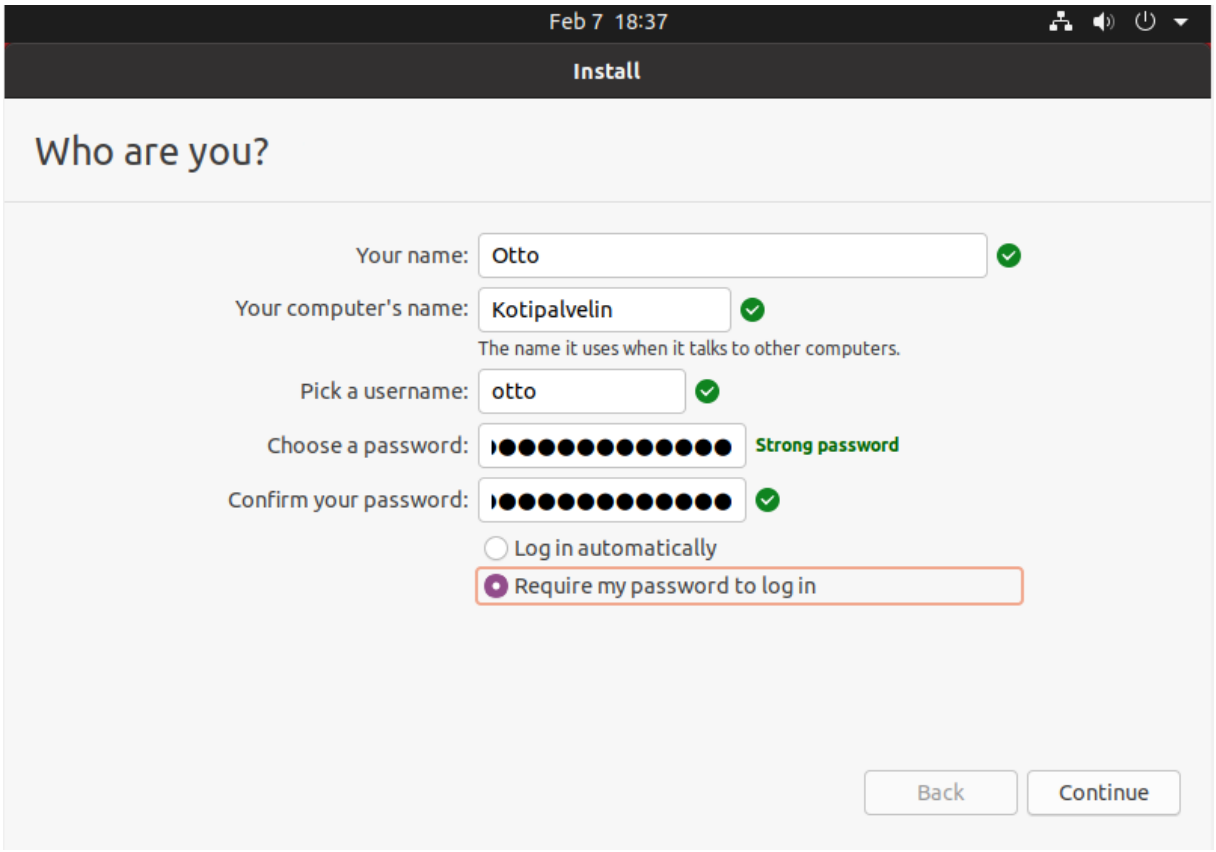
Kuva 4 Ubuntu asennus - Asennuksen tyyli valinta



Seuraavat vaiheet ovat yksinkertaisia ja riippuvaisia käyttäjästä. Tässä vaiheessa valitaan sijainti ja painetaan **Continue.**

Nyt tehdään käyttäjä. Annetaan nimi, tietokoneen nimi, käyttäjänimi ja mahdollisimman vahva salasana. Valitaan myös **Require my password to login** ja painetaan **Continue** (Kuva 5).

Kuva 5 Ubuntu asennus - Käyttäjän luonti



Nyt järjestelmän asennus alkaa. Tämä vaihe kestää hetken. Asennuksen jälkeen tietokone käynnistetään uudestaan painamalla **Restart Now.** Kun tietokone käynnistyy uudestaan, voidaan irrottaa USB-tikku tietokoneesta.

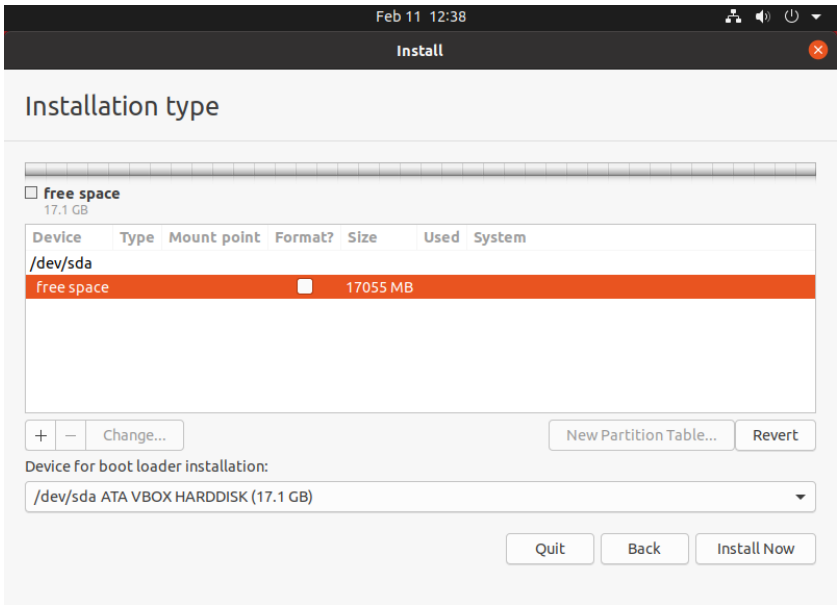
5.1 Kiintolevyn partitionti asennuksen yhteydessä

Mikäli halutaan tehdä itse kiintolevyn partitiointi, se kannattaa tehdä käyttöjärjestelmän asennuksen yhteydessä. Koska palvelimelle on jo tehty partitiointi, tämä käydään läpi virtuaalikoneella, joten se poikkeaa hieman tehdystä asennuksesta.

Aiemmin tehdyssä Ubuntu -käyttöjärjestelmän asennuksessa poiketaan kuva 5 vaiheessa ja valitaan **Something Else** ja **Continue** (Kuva 4).

Tässä vaiheessa, jos ei ole **free space** vaihtoehtoa, pitää valita **New Partition Table…** ja vahvistuksessa valita **Continue.** Tämän jälkeen ruudulla näkyy vapaa tila minkä valitsemalla ja klikkaamalla **+** voidaan luoda uusi partitio (Kuva 6).

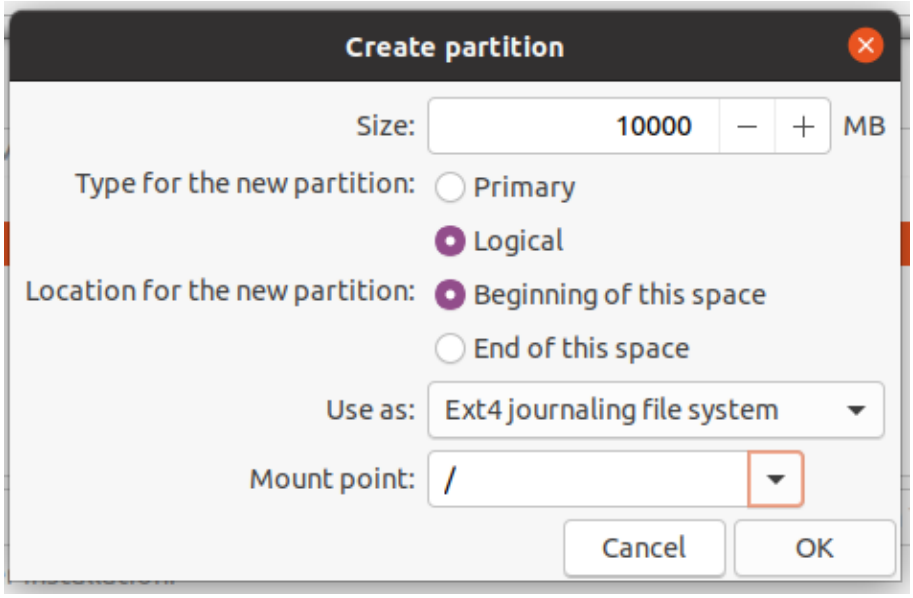
Kuva 6 Ubuntu asennus - Partitiointi



Ensimmäinen partitio mikä tehdään, on root (

Kuva 7). Tämän partition suositeltu koko on vähintään 15 GB. On hyvä muistaa, että root partition täyttyessä järjestelmää ei voi käyttää. (help.ubuntu.com, *DiskSpace*, 2017)

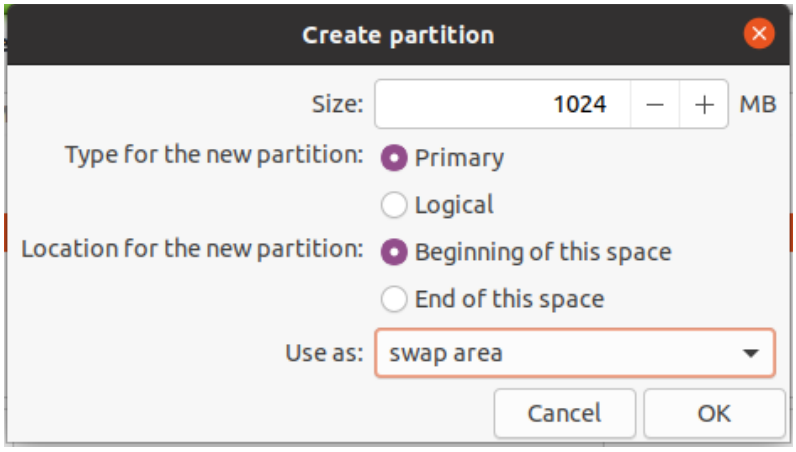
Kuva 7 Ubuntu asennus - Root partitio



Seuraavaksi tehdään **swap** partition (

Kuva 8). Tämä partitio varmistaa, että muistin loppuessa kesken, järjestelmä ei kaadu. Swap partition suositeltu tila on sama kuin muistin määrä. Esim. jos muistia on 8 GB, suositellaan swap partition kooksi 8 GB. (Imes, 2017)

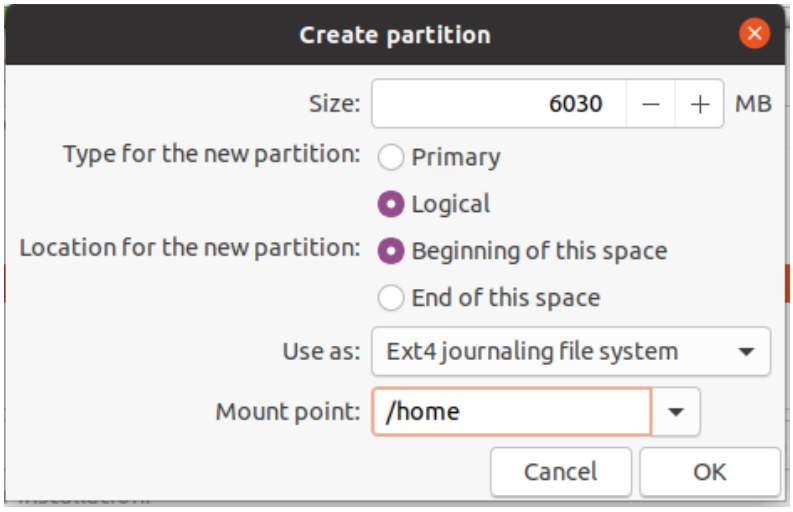
Kuva 8 Ubuntu asennus - Swap partitio



Tehdään myös erillinen **home** partitio, että on mahdollista tarvittaessa päivittää tai vaihtaa Linux-jakelua ilman, että menetetään tiedostoja. (

Kuva 9)

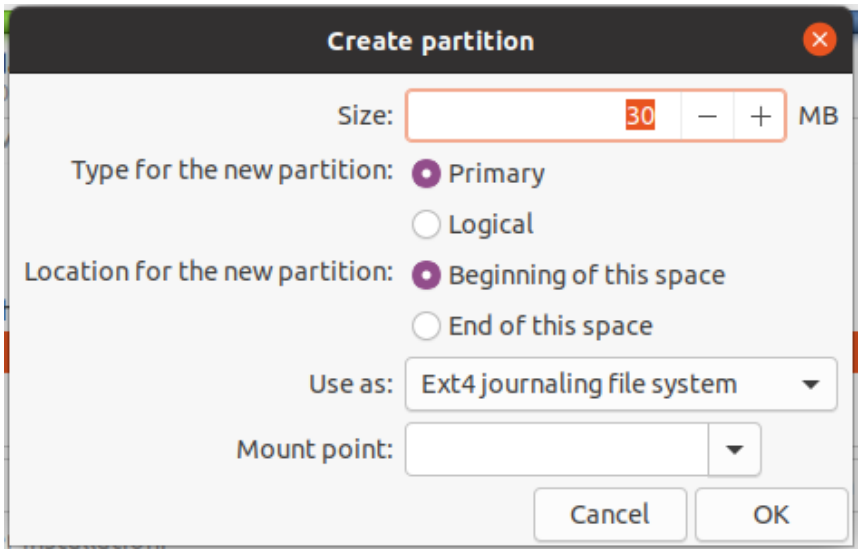
Kuva 9 Ubuntu asennus - Home partitio



Mikäli käytössä on GPT levy, pitää tehdä vielä erillinen EFI tai BIOS-boot partitio, riippuen onko BIOS UEFI vai Legacy muodossa. (Imes, 2017) Koska työssä käytettävässä laitteessa on GPT-levy ja BIOS on EFI muodossa, joudutaan tehdä vielä EFI partitio. (

Kuva 10).

Kuva 10 Ubuntu asennus - EFI partitio



Kun partitiointi on valmis, voidaan valita **Install Now** ja **Continue** niin asennus voi jatkua. Loppu asennus käy samalla tavalla kuin kohdan Kuva 4 jälkeen. Järjestelmän käynnistyttyä suositellaan ajamaan päivitys komennot (Komento 1).

Komento 1 Päivitys komennot

```
sudo apt update
sudo apt upgrade
```

5.2 HDD-levyn käyttöönotto

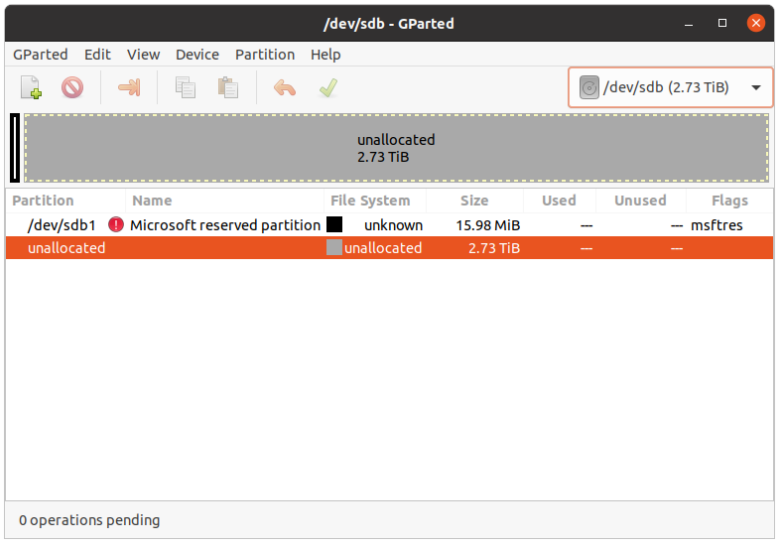
Palvelimessa on asennettuna 3Tt kovalevy, minkä on tarkoitus toimia päätallennustilana. HDD ei näy automaattisesti, joten se pitää ottaa käyttöön manuaalisesti. Levynhallinta voidaan tehdä helposti käyttämällä Gparted työkalua, mikä toimii hyvin graafisella käyttöliittymällä. Gparted-ohjelman voi asentaa helposti apt install -komennolla (Komento 2).

Komento 2 Gparted asennus -komento

```
sudo apt install Gparted
```

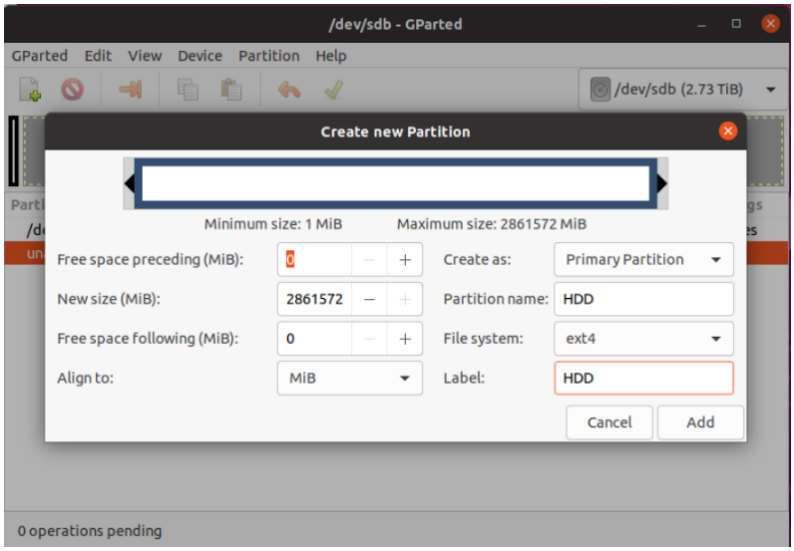
Kun gparted on asennettu, käynnistetään se. Kun Gparted on auki, voidaan oikeasta ylänurkasta valita haluttu HDD-levy ja tehdä sille uusi partitio.

Kuva 11 Gparted näkymä



Uusi partitio voidaan tehdä klikkaamalla oikealla tyhjästä tilasta missä lukee **unallocated** ja valitsemalla **New**. Nyt aukeaa uusi ikkuna missä voidaan valita osion koko ja nimi (Kuva 12).

Kuva 12 Gparted uusi partitio



Painamalla **Add** voidaan jatkaa asennusta. Mitään muutoksia ei vielä tapahdu ennen kuin painetaan vihreää hyväksy merkkiä (Kuva 13) ja **Apply**. Nyt HDD-levy on käytettävissä.

Kuva 13 Gparted hyväksy muutokset

6 UFW-palomuuri

UFW nimensä mukaisesi (Uncomplicated Firewall) on yksinkertainen käyttää. Yksinkertaisilla komennoilla voi hallita minkä tyyppisiä yhteyksiä palomuurin läpi pääsee tai ei pääse. Se on valmiiksi asennettu Ubuntu-käyttöjärjestelmiin, mutta jos sitä ei jostain syystä ole, se on helppo asentaa apt install -komennolla (Komento 3). UFW-palomuuri kytketään päälle yksinkertaisella komennolla (Komento 4).

Komento 3 UFW asennus -komento

```
sudo apt install ufw
```

Komento 4 UFW päälle -komento

```
sudo ufw enable
```

Tässä vaiheessa on hyvä asettaa tietyt portit auki, että SSH-, http- ja https-palvelut toimivat tulevaisuudessa (Komento 5).

Komento 5 SSH-, HTTP- ja HTTPS-portit auki

```
sudo ufw allow 22
sudo ufw allow 80
sudo ufw allow 443
```

Jatkossa portteja avataan asennusten yhteydessä, näin ei avata turhaan portteja ja jätetä palvelinta haavoittuvaiseksi. Portteja voi säätää oman tarpeen mukaan, jos tietää mitä portteja haluaa käyttää. On mahdollista käyttää UFW-palomuuria kaiken liikenteen estämiseen tarvittaessa ja avata portteja ainoastaan tarpeen mukaan. Vaikka UFW-palomuuri saattaa olla valmiina joissakin Linux-jakeluissa, on mahdollista että se ei ole päällä automaattisesti, vaan pitää aktivoida erikseen (Komento 4).

7 Etähallinta, jaot ja niiden tietoturvallisuus

Mikäli ei haluta hallita palvelinta itse laitteelta, voidaan varmistaa, että siihen pääsee turvallisesti yhdistämään SSH- tai VNC-yhteydellä ja tiedostojen siirto onnistuu Samban avulla.

SSH-yhteyden muodostaminen palvelimelle on helppoa. Yksinkertaisesti pitää asentaa openssh-server ja sallia se palomuurissa. Koska työn tavoitteena on tehdä palvelimesta mahdollisimman turvallinen käyttää, täytyy tehdä jatkotoimia tietoturvan varmistamiseksi. SSH-yhteys normaalisti käyttää tunnistautumista käyttäjällä ja salasanalla, mutta tämä ei ole aina turvallisin vaihtoehto, mikäli käyttäjän salasana on heikko (Jethva, 2015) tai mikäli käyttäjän salasana on varastettu.

Ensin tehdään normaali SSH-asennus ja päivitetään sen turvallisuutta tekemällä muutoksia sen konfiguraatioon. Aloitetaan tekemällä päivitykset ja asentamalla openssh-server (Komento 6). Tämän jälkeen sallitaan SSH-yhteydet palomuurista (Komento 7).

Komento 6 Open-ssh -asennus

```
sudo apt update
sudo apt install openssh-server
```

Komento 7 SSH salliminen palomuurista

```
sudo ufw allow ssh
```

Tässä vaiheessa SSH-yhteys palvelimelle on mahdollista tehdä toiselta Linux-laitteelta tai Windows-laitteelta käyttämällä palvelimen IP-osoitetta ja omaa käyttäjätunnusta. Työssä halutaan myös varmistaa, että SSH-yhteys on mahdollisimman turvallinen, joten tehdään vielä muutaman jatkotoimenpide SSH-palvelimen tietoturvan varmistamiseksi. Tässä käytetään Hitesh Jethvan kirjoittamaa ohjetta (Jethva, 2015), mikä käy hyvin läpi tarvittavat vaiheet SSH-yhteyden turvaamiseen. Ohjeiden avulla saadaan SSH-yhteys muodostettua turvallisesti käyttämällä SSH-avainta käyttäjän sijaan ja muita tietoturva parannuksia. Aloitetaan tekemällä varmuuskopio SSH-konfiguraatiotiedostosta, mikäli muutoksissa esiintyy ongelmia (Komento 8).

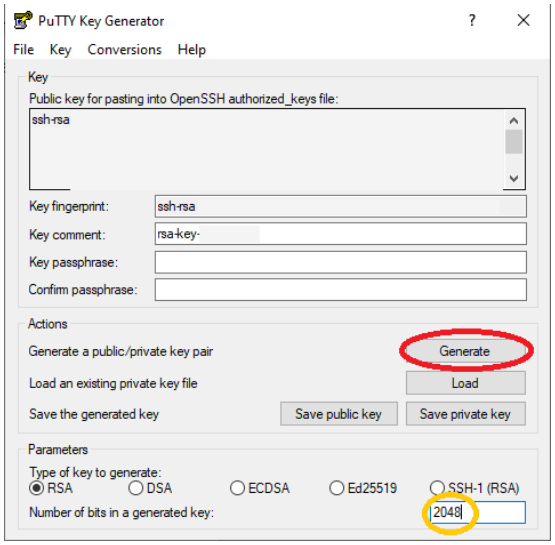
Komento 8 SSH-konfiguraatio varmuuskopio

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
```

Koska client laite on Windows 10, missä käytetään Putty (putty.org) -ohjelmaa SSH-yhteyden luomiseen Ubuntu-palvelimeen, pitää vielä tehdä Windows-laitteelle SSH-avain. Putty-ohjelman lisäksi tarvitaan PuTTYgen-ohjelma, mikä luo SSH-avaimen (Devenport, 2014). PuTTYgen asentuu yleensä samalla Putty-ohjelman kanssa. Sen löytää painamalla **Windows** painiketta ja hakemalla **Puttygen**.

Uusi public ja private SSH-avain voidaan tehdä painamalla Actions kohdasta **Generate.** Varmistetaan myös, että bittien määrä on vähintään 2048. Kohtaan **Key passphrase** kirjoitetaan myös salasana, että avainta ei voi käyttää, jos se varastetaan (Kuva 14). Tässä vaiheessa ohjelma pyytää hiiren liikutusta satunnaisen avaimen luomiseen.

Kuva 14 Puttygen SSH-avaimen luonti



Kun avain on luotu, valitaan Actions kohdasta **Save private key.** Avain tallennetaan nimellä **id_rsa.ppk** työpöydälle tai suojattuun kansioon. Yläpuolella Key kohdassa olevasta laatikosta voidaan kopioida Public avain (Kuva 14). Tämä avain pitää kopioida palvelimelle **authorized_keys** tiedostoon (Komento 9).

Jotta public avain voidaan siirtää, pitää ensin ottaa yhteys palvelimeen käyttämällä normaalia Putty SSH kirjautumista käyttäjällä. Tämä käy helposti avaamalla Putty-ohjelman, kirjoittamalla IP-osoitteen Host Name kohtaan ja valitsemalla Open. Komentokehotteeseen

kirjoitetaan käyttäjätunnus ja muodostetaan yhteys. Nyt voidaan kopioida tehty Public Key-avain palvelimelle authorized_keys tiedostoon (Komento 9).

Komento 9 SSH Public Key sallituksi avaimeksi lisääminen

```
sudo nano ~/.ssh/authorized_keys
```

Varmistetaan myös, että tiedoston käyttöoikeudet ovat turvalliset (Komento 10). Myös oikeudet ja sshd_config tiedosto pitää muokata, että ei tule ongelmia (Forkbeard, 2013).

Komento 10 authorized_keys tiedoston ja ssh kansion käyttöoikeudet kuntoon

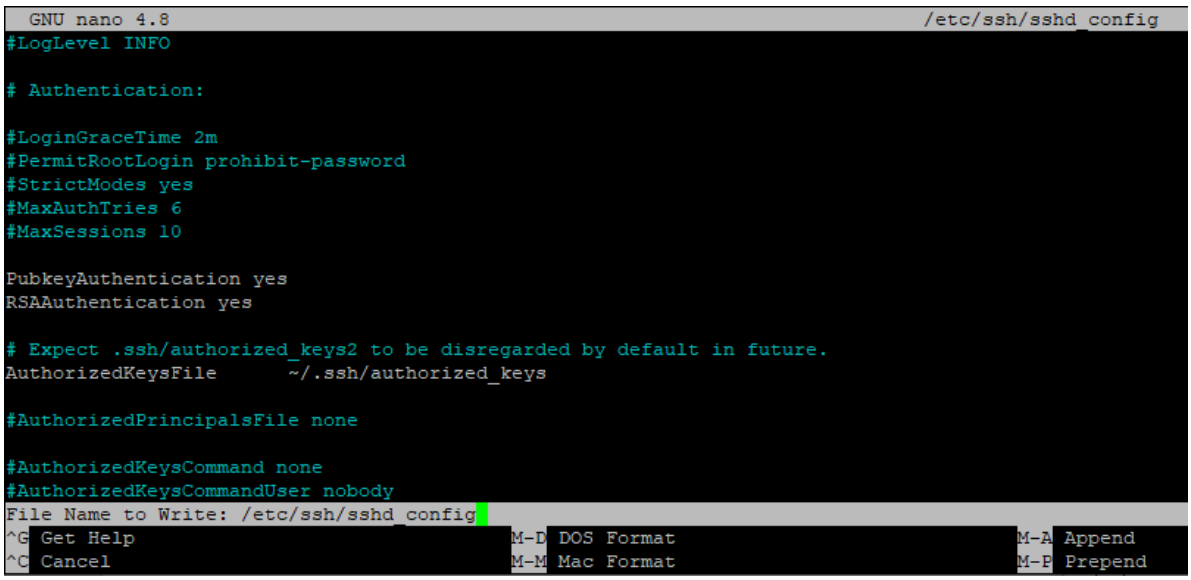
```
sudo chmod 600 ~/.ssh/authorized_keys
sudo chmod 700 ~/.ssh/
sudo chown <käyttäjä>:<käyttäjä> ~/.ssh -R
```

Pitää myös varmistaa, että /etc/ssh/sshd_config tiedostossa on asetettu AuthorizedKeysFile oikeaan polkuun ja että PubkeyAuthentication on päällä (Kuva 15). Tiedostoon pääsee sudo nano -komennolla (Komento 11).

Komento 11 sudo nano tekstinkäsittely -komento sshd_config tiedostoon

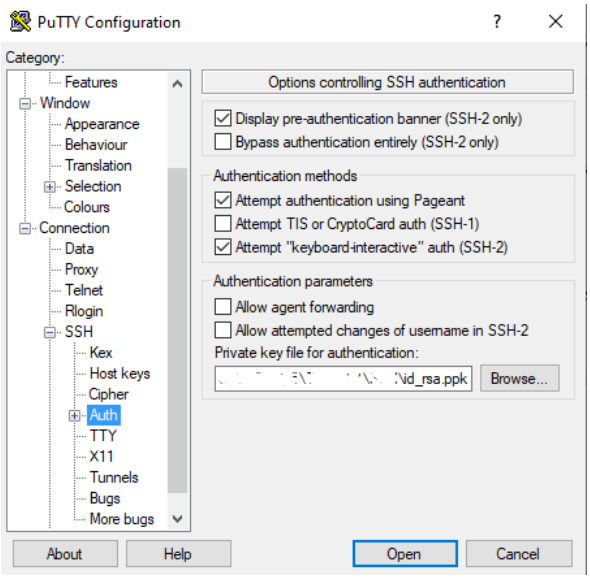
```
sudo nano /etc/ssh/sshd_config
```

Kuva 15 sshd_config tiedoston asetukset

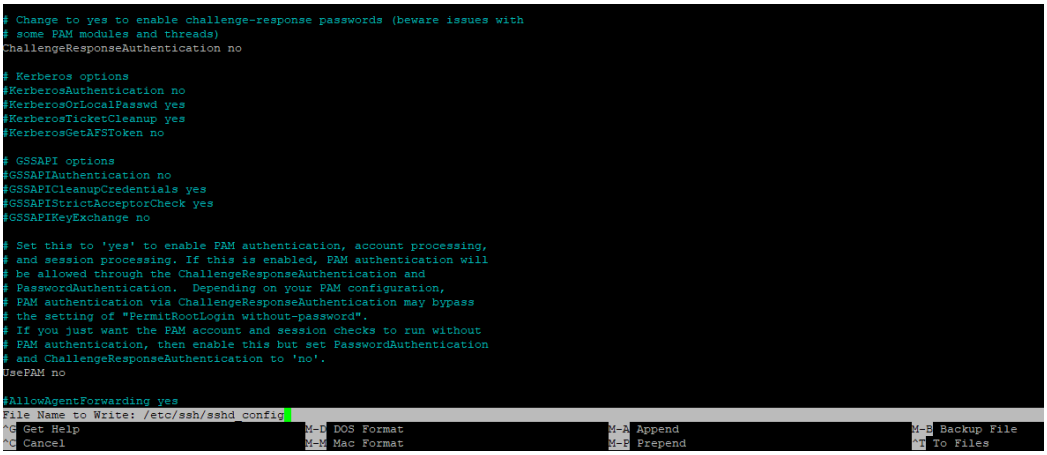


Tämän jälkeen suljetaan yhteys ja siirrytään PuTTYn asetuksiin Connection>SSH>Auth kohtaan missä valitaan tehty private avain (Kuva 16). Seuraavaksi painetaan Open. Koska private avaimelle asetettiin salasana, palvelin kysyy sitä yhdistäessä. Mikäli yhteys ei vielä toimi, otetaan PAM pois käytöstä (Kuva 17).

Kuva 16 PuTTY SSH private avain käyttöönotto



Kuva 17 PAM pois päältä sshd_config tiedostossa



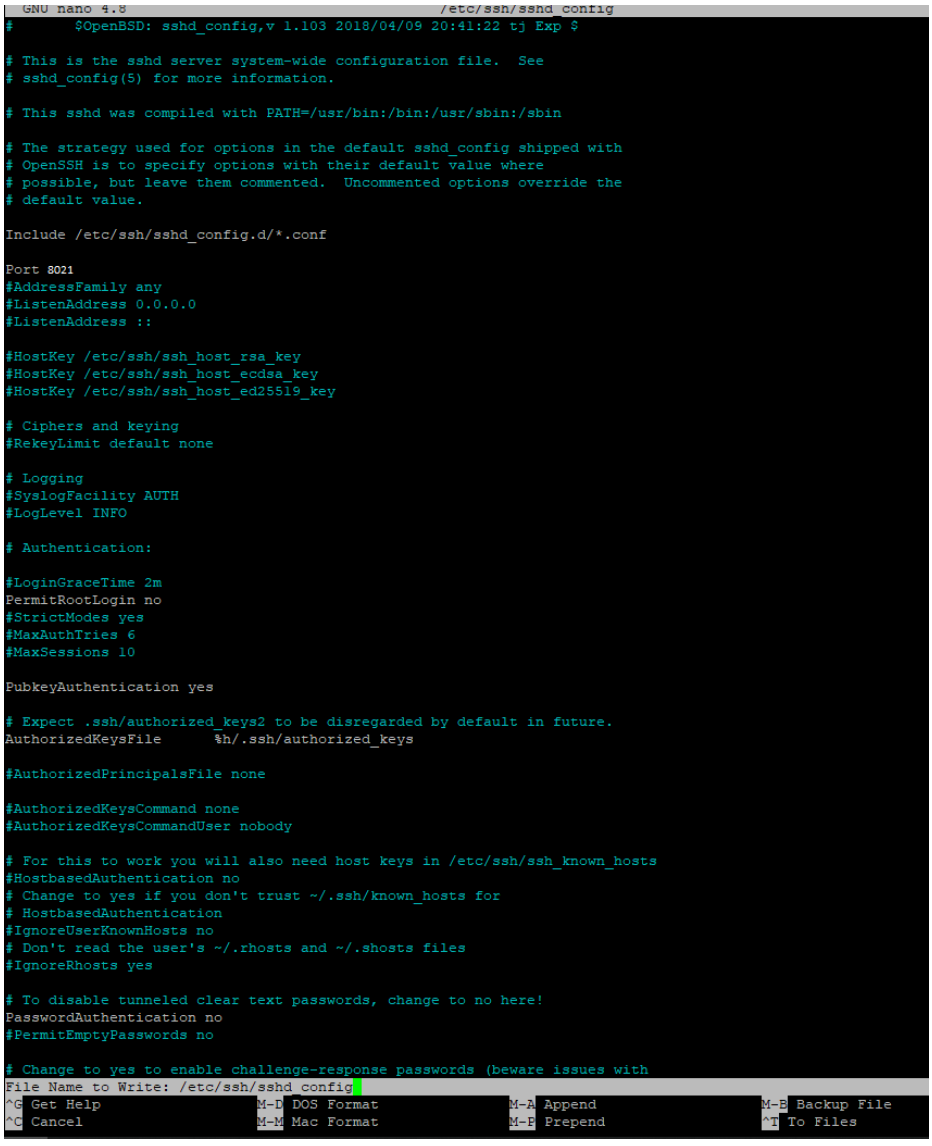
Seuraavaksi muokataan sshd_config tiedostoa lisää (Komento 11). Aloitetaan muuttamalla oletus portin 22:sta numeroon 1024 ja 32,767 välillä. Tämä löytyy tiedoston alusta **#Port 22** ja se pitää muuttaa aktiiviseksi poistamalla kommentti merkki alusta (Kuva 18). Valittu portti avataan UFW:n asetuksissa (Komento 12).

Komento 12 Ufw sallimaan yhteys IP-osoitteesta SSH porttiin

```
sudo ufw allow from 192.168.0.56 to any port 22
```

Tämän jälkeen asetetaan **PermitRootLogin** kielletyksi eli **no** (Kuva 18).Viimeisimmän kirjautumisyrityksen voi piilottaa asettamalla **PrintLastLog no.** Myös **PasswordAuthentication** voidaan ottaa pois päältä, kun SSH-avaimet on saatu toimimaan (Kuva 18).

Kuva 18 sshd_config tietoturvalliset asetukset



Kun asetukset ovat valmiit, voidaan tallentaa tiedoston painamalla **Ctrl+O** ja poistua tiedostosta painamalla **Ctrl+X.** Seuraavaksi käynnistetään SSH-palvelun uudestaan, että asetukset päivittyvät (Komento 13).

Komento 13 SSH uudelleenkäynnistys

```
sudo service ssh restart
```

Kun SSH on asennettu ja turvattu, asennetaan seuraavaksi Samba. Ohjeet Samban asennukseen löytyy tecmint.com sivuilta Aaron Kilin kirjoittamasta artikkelista (Kili, 2017). Tässä työssä tehdään näiden ohjeiden mukaan samban asennus ja käyttäjät. Käytetään ohjeista löytyvää turvallista tiedostonjako vaihtoehtoa mihin tehdään pieniä muutoksia, mitkä korjaavat vikoja ohjeissa. Asennus alkaa yksinkertaisesti Samban latauksella ja asennuksella (Komento 14).

Komento 14 Samba asennus -komennot

```
sudo apt update
sudo apt install samba samba-common python-dnspython
```

Tässä vaiheessa on hyvä myös tehdä varmuuskopio samban konfiguraatiotiedostosta (Komento 15).

Komento 15 Samba konfiguraation varmuuskopio

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
```

Nyt tehdään ryhmää ja lisätään siihen käyttäjät, joille halutaan antaa oikeudet käyttää jaettua kansiota ja lisätään myös salasanat samban käyttäjille (Komento 16). Tämä varmistaa, että vain halutut henkilöt voivat jakaa tiedostoja. **<käyttäjä>** kohtaan laitetaan käyttäjänimi **ilman < > merkkejä**. Tämän jälkeen tehdään kansio samban jaolle (Komento 17).

Komento 16 Komento ryhmän lisäämiselle ja salasanan asettamiselle käyttäjille

```
sudo addgroup smbgrp
sudo usermod <käyttäjä> -aG smbgrp
sudo smbpasswd -a <käyttäjä>
```

Komento 17 Samba kansion luonti -komento **ilman < > merkkejä**

```
mkdir /home/<käyttäjä>/sambashare
```

Muokataan tehdyn kansion käyttöoikeudet sopiviksi seuraavalla komennolla (Komento 18). Tällä asetuksella vain kansion omistaja ja ryhmän jäsenet pääsevät siihen käsiksi. Sitten muokataan samban konfiguraatiotiedostoa, että se jakaa tehdyn kansion (Komento 19).

Komento 18 Samba-jaon kansion käyttöoikeudet -komento

```
sudo chmod -R 0770 /home/<käyttäjä>/sambashare
sudo chown -R root:smbgrp /home/<käyttäjä>/sambashare
```

Komento 19 Komento samban konfiguraatiotiedoston muokkaamiselle

```
sudo nano /etc/samba/smb.conf
```

Muokataan **global** -asetuksia missä varmistetaan, että laitteen nimenä näkyy Ubuntu ja tunnistautumiseen käytetään käyttäjää (Komento 20).

Komento 20 Samba global konfiguraatio

```
[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will
part of
      workgroup = WORKGROUP
      netbios name = ubuntu
      security = user
```

Loppuun lisätään seuraava teksti (Komento 21). Kohta **<käyttäjä>** muutetaan omaksi käyttäjäksi **ilman < > merkkejä.**

Komento 21 Samban konfiguraatiotiedostoon lisättävä tekstinpätkä

```
[sambashare]
    comment = Turvallinen kansion jako
    path = /home/<käyttäjä>/sambashare
    valid users = @smbgrp
    read only = no
    public = no
    writable = yes
    browsable = yes
```

Tiedosto tallennetaan painamalla **Ctrl + O** ja tiedostosta poistutaan painamalla **Ctrl + X.**

Koska käytössä on UFW-palomuuri, pitää avata tietyt portit verkon koneille mitä käytetään tiedoston jaossa (Kili, 2017). Se tapahtuu **sudo ufw allow** -komennolla (Komento 22). Mikäli ylempi vaihtoehto ei toimi, voidaan käyttää myös alempaa yksinkertaisempaa komentoa.

Komento 22 Komento millä saa UFW-palomuurin portit auki Sambaa varten

```
sudo ufw allow proto udp to any port 137 from 192.168.1.0/24
sudo ufw allow proto udp to any port 138 from 192.168.1.0/24
```

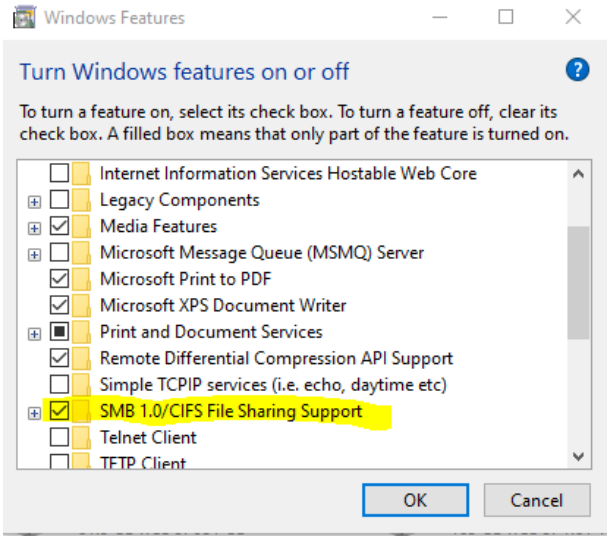
```
sudo ufw allow proto tcp to any port 139 from 192.168.1.0/24
sudo ufw allow proto tcp to any port 445 from 192.168.1.0/24
```

ja/tai

```
sudo ufw allow samba
```

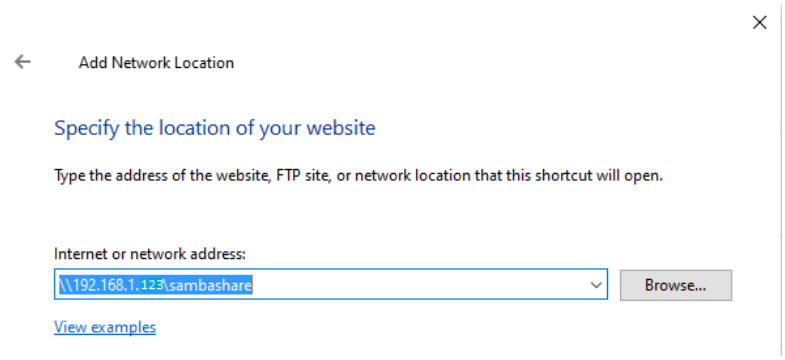
Nyt on mahdollista yhdistää jaettuun kansioon käyttäjän tunnuksilla. Mikäli halutaan yhdistää Windows 10 -käyttöjärjestelmästä, pitää ensin varmistaa, että **Turn Windows Features on or off** kohdassa **SMB 1.0** on päällä (Kuva 19).

Kuva 19 Samba asennus - Windows SMB 1.0 päälle



Jotta kohteet saadaan näkyviin Windowsin puolella, pitää ne ensin lisätä klikkaamalla resurssienhallinnassa hiiren oikealla **This PC** ja valitsemalla **Add a network location**. Painetaan **next,** kunnes kysytään IP-osoitetta kohteelle. Tähän kohtaan laitetaan Ubuntu-laitteen IP-osoite ja loppuun jaon nimi (Kuva 20)

Kuva 20 Samba asennus - Network Location



Seuraavaksi jako nimetään ja painetaan **Next** ja **Finish.** Nyt pystytään helposti jakaa tiedostoja suojatusti käyttäjällä Ubuntu-laitteen ja Windows-laitteiden välillä.

8 Caddy-palvelinohjelmiston asennus

Palvelimelle asennetaan Caddy-ohjelma, mikä ylläpitää verkkopalveluja ja tiedostoja. Koska Caddyn asennus vaatii curl -komennon käytön, pitää se ensin asentaa (Komento 23).

Komento 23 Curl asennus

```
sudo apt install curl
```

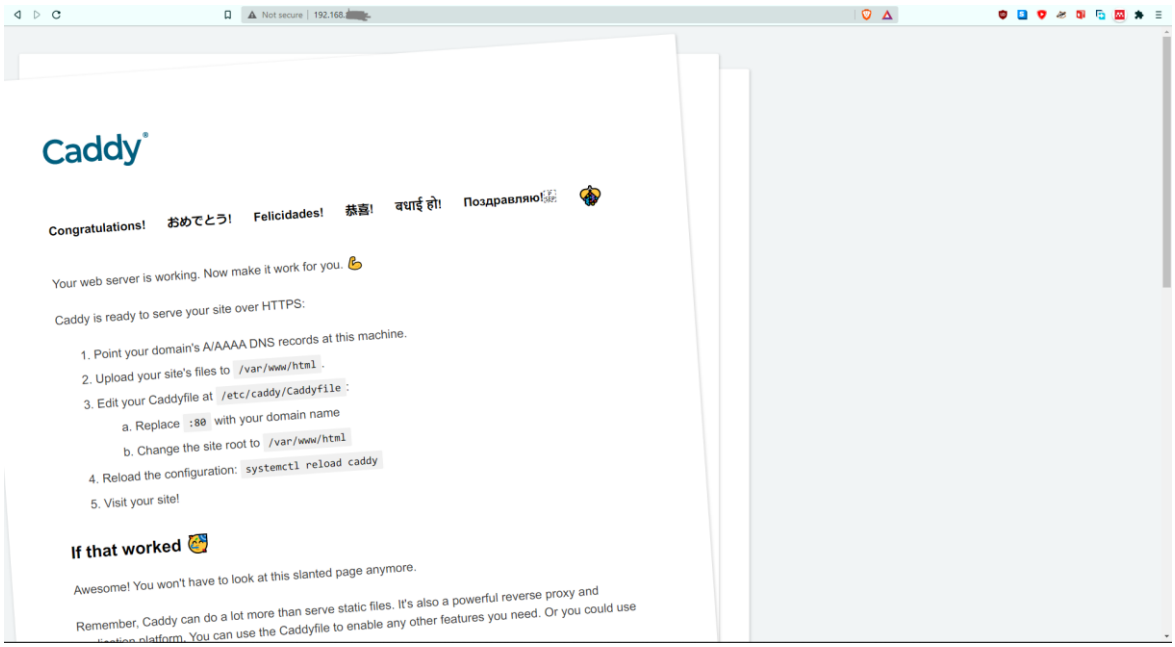
Tästä eteenpäin seurataan Caddy -sivustolta löytyvän dokumentaation ohjeistusta (caddyserver.com, 2021), millä saadaan palvelin toimivaksi. Asennus on varsin yksinkertainen. Asennus aloitetaan lisäämällä tarvittavat repositoriot, päivittämällä ja asentamalla caddyn (Komento 24).

Komento 24 Caddy asennus -komennot

```
sudo apt install -y debian-keyring debian-archive-keyring apt-
transport-https
curl -1sLf 'https://dl.cloudsmith.io/public/caddy/stable/gpg.key' |
sudo apt-key add -
curl -1sLf
'https://dl.cloudsmith.io/public/caddy/stable/debian.deb.txt' | sudo
tee -a /etc/apt/sources.list.d/caddy-stable.list
sudo apt update
sudo apt install caddy
```

Seuraavaksi ohjeistetaan tekemään ryhmä ja käyttäjä nimellä caddy, mutta asennus vaikuttaa tekevän sen automaattisesti, joten tämä kohta voidaan ohittaa. Siirrytään selaimeen ja laitetaan osoitekenttään palvelimen IP-osoite missä nähdään, että Caddy on asennettu (Kuva 21).

Kuva 21 Caddy asennettu



Huomataan, että sivulla näkyy uudet ohjeet, mitkä opastavat hieman mitä pitää tehdä seuraavaksi. Koska työssä halutaan käyttää omaa domain-osoitetta, eikä IP-osoitetta, siirrytään ostamaan oma domain nimi esim. **domainhotelli.fi** -sivustolta. Domainille valitaan sopiva nimi, tehdään tilaus ja siirrytään palvelun **cpanel** -hallintaan. Täältä etsitään **DNS-asetukset** ja valitaan **Hallinta**. Hallinta kohdassa poistetaan ylimääräiset tyyppi A- ja tyyppi AAAA-tietueet ja lisätään uudet tietueet, mitkä osoittavat palvelimen julkiseen Ipv4- ja Ipv6-osoitteeseen. Tyyppi A-tietueeseen merkitään Ipv4-osoite ja tyyppi AAAA-tietueeseen Ipv6-osoite (Kuva 22). Nämä IP-osoitteet löytyvät hakemalla googlesta **my ip**.

Kuva 22 DNS-tietue esimerkki

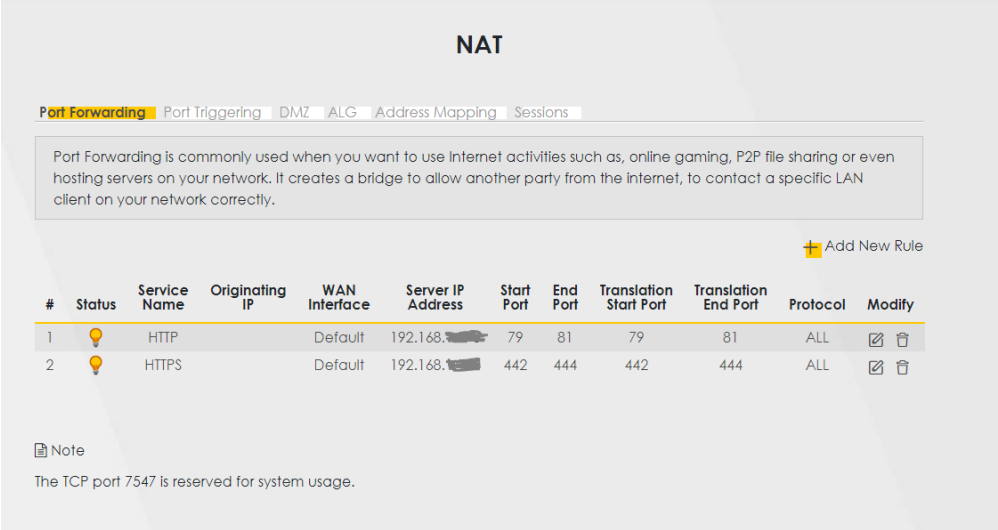
Tämän lisäksi varmistetaan, että reitittimen portit ovat ohjattu palvelimelle. Reitittimen IP-osoitteen löytää avaamalla komentokehotteen käyttämällä Windows hakua ja kirjoittamalla seuraavan komennon (Komento 25).

Komento 25 IP-osoite tiedot komentokehotteella

```
ipconfig
```

Default Gateway on reitittimen IP-osoite. Reitittimen asetuksiin pääsee käsiksi laittamalla Default Gateway osoitteen selaimen osoitekenttään. Jokaisen reitittimen valmistaja käyttää erilaista käyttöliittymää, joten porttien ohjaus (port forwarding) voi olla erilaista muille. Zyxel reitittimessä porttien ohjaus löytyy **Network Setting > NAT > Port Forwarding.** Täältä ohjataan http- ja https -portit palvelimelle (Kuva 23).

Kuva 23 Porttien ohjaus palvelimelle (Port Forwarding)



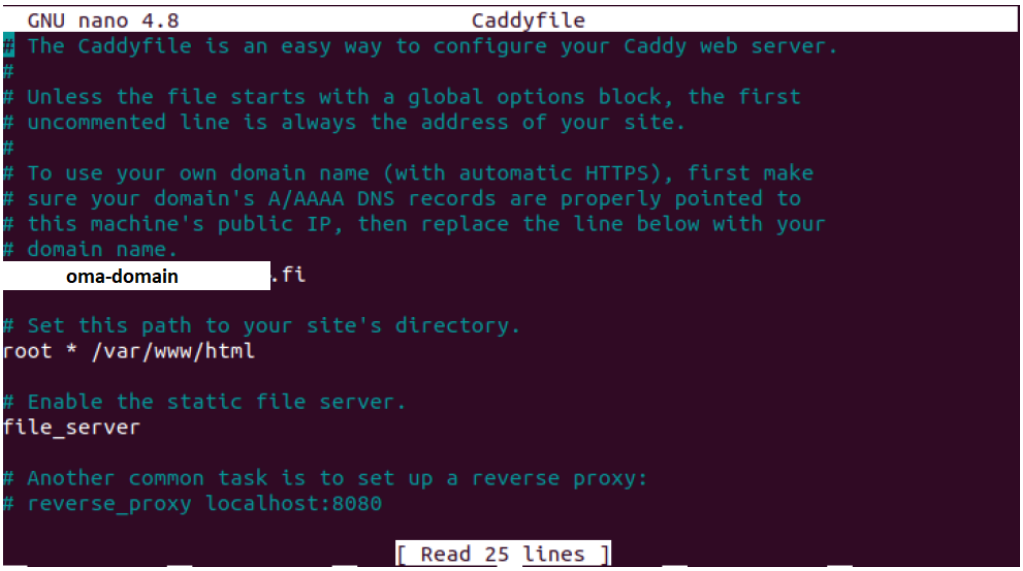
Seuraavaksi muokataan palvelimella löytyvää Caddyfile-tiedostoa. Tästä tiedostosta tehdään myös varmuuskopion. (Komento 26)

Komento 26 Caddyfile varmuuskopio ja muokkauskomento

```
cd /etc/caddy
cp Caddyfile Caddyfile.bak
sudo nano Caddyfile
```

Tässä tiedostossa korvataan :80 omalla domain osoitteella ja muutetaan sivujen hakemisto /var/www/html kansioksi (Kuva 24).

Kuva 24 Caddyfile



/var/www/html kansiota ei ole valmiiksi luotu, joten se pitää tehdä (Komento 27).

Komento 27 Tee html kansio

```
mkdir -p /var/www/html
```

Seuraavaksi päivitetään Caddy ja käynnistetään se (Komento 28).

Komento 28 Caddy reload ja käynnistys

```
systemctl reload caddy
caddy start
```

Mikäli käynnistäessä tulee virheilmoitus missä mainitaan, että portteja ei voi käyttää, voi se tarkoittaa, että caddy käyttäjällä ei ole oikeuksia kuunnella pienempiä portteja. Ongelman saa korjattua seuraavalla komennolla (Komento 29), (Keith, 2020).

Komento 29 Salli Caddyn kuunnella pienempiä portteja

```
sudo setcap CAP_NET_BIND_SERVICE=+eip $(which caddy)
```

Nyt sivuihin pääsee käsiksi verkosta käyttämällä tehtyä domain-osoitetta. Kuten aiemmin mainittu, Caddy luo automaattisesti TLS-sertifikaatit.

Kun halutaan tehdä normaalit HTML verkkosivustot, tehdään ne Caddyfile-tiedostoon merkattuun kansioon, eli /var/www/html.

9 Wordpress-sisällönhallintaohjelmisto

Mikäli halutaan tehdä Wordpress -sivustot, asennetaan PHP, MariaDB ja Wordpress. Navjot Singh on kirjoittanut hyvät ohjeet, miten asentaa ja konfiguroida PHP ja MariaDB Caddy-verkkopalvelimen kanssa (Singh, 2020). Koska Wordpressin käyttöön Caddy 2 kanssa ei löydy paljoa ohjeistusta, voi sen käytössä esiintyä ongelmia, minkä ratkomiseen kuluu aikaa. Työssä on kuitenkin saatu Wordpress toimimaan palvelimella.

Aloitetaan PHP-asennuksella (Komento 30). Kun asennus on suoritettu, voidaan siirtyä asentamaan MariaDB (Komento 31). Kun MariaDB on asennettu, voidaan tehdä sen konfiguraatio (Komento 32).

Komento 30 PHP-asennus

```
sudo add-apt-repository ppa:ondrej/php

sudo apt install php-cli php-fpm php-mysql
php --version
```

Komento 31 Maria DB -asennus

```
sudo apt-key adv --fetch-keys
'https://mariadb.org/mariadb_release_signing_key.asc'

sudo add-apt-repository 'deb [arch=amd64]
http://mirror.lstn.net/mariadb/repo/10.4/ubuntu focal main'

sudo apt install mariadb-server

mysql –version

sudo systemctl enable mariadb
```

Komento 32 MariaDB konfiguraatio

```
 sudo mysql_secure_installation
```

Konfiguraatiossa on monta osaa. Ensimmäisenä kysytään root salasanaa, mitä ei ole vielä asetettu, joten se jätetään tyhjäksi. Laitetaan unix_socket autentikaatio päälle sen turvallisuuden vuoksi. Ohitetaan root salasanan vaihto suosituksen mukaisesti. Poistetaan anonyymit käyttäjät, että anonyymeillä käyttäjillä ei ole pääsyä tietokantoihin. Kielletään root kirjautuminen etänä. Poistetaan myös testi tietokanta, mikä on automaattiesti luotu. Ja viimeisenä päivitetään oikeustaulukot. Nyt konfiguraatio on valmis ja on mahdollista kirjautua SQL shelliin (Komento 33).

Komento 33 Mysql shell -käynnistys

```
sudo mysql
```

Seuraavaksi tehdään tietokanta ja käyttäjä tietokantaan WordPressille. Annetaan myös käyttäjälle kaikki oikeudet tietokantaan. (Komento 34)

Komento 34 Uusi tietokanta ja käyttäjä

```
CREATE DATABASE wordpresskanta;
CREATE USER 'käyttäjä' IDENTIFIED BY 'salasana';
GRANT ALL PRIVILEGES ON wordpresskanta.* TO 'käyttäjä';
exit
```

Seuraavaksi tehdään Caddy:lle log kansio, mihin ohjelma voi tallentaa lokitiedostot. Annetaan myös caddy käyttäjälle oikeudet kansioon (Komento 35).

Komento 35 Log kansio ja sen oikeudet caddylle

```
sudo mkdir /var/log/caddy
sudo chown -R caddy:caddy /var/log/caddy
```

Sitten lisätään seuraava tekstinpätkä Caddyfile nimiseen tiedostoon, missä <oma-domain> on aiemmin tehty domain (Komento 26)

```
log {
        output file /var/log/<oma-domain>.access.log {
                roll_size 3MiB
                roll_keep 5
                roll_keep_for 64h
        }
}
```

Samalla otetaan php_fastcgi pois kommenteista, poistamalla siitä ensimmäisen # merkin ja vaihtamalla php-version asennettuun php versioon, eli rivi päättyy **php8.0-fpm.sock** (Kuva 24). Seuraavaksi konfiguroidaan PHP, muokkaamalla www.conf-tiedostoa (Komento 36).

Komento 36 PHP -konfiguraatiotiedoston muokkaus

```
sudo nano /etc/php/8.0/fpm/pool.d/www.conf
```

Tästä tiedostosta etsitään ja vaihdetaan kaikki www-data kohdat nimeksi caddy, minkä jälkeen tiedosto tallennetaan ja PHP-prosessi käynnistetään uudestaan (Komento 37).

Komento 37 PHP uudelleenkäynnistys

```
sudo systemctl restart php8.0-fpm
```

Nyt MariaDB ja PHP 8.0 on asennettu ja konfiguroitu sopivaksi caddy:n kanssa. Nyt voidaan siirtyä Wordpressin -asennukseen. Wordpress voidaan ladata wordpress.org sivuilta. Ladataan .tar.gz paketoitu versio ja puretaan se /var/www/html kansioon (Komento 38).

Komento 38 Siirretään Wordpress-tiedosto html kansioon ja puretaan se ja poistetaan pakattu tiedosto

```
sudo mv ~/Downloads/wordpress-5.6.2.tar.gz /var/www/html
cd /var/www/html
sudo tar -xvf wordpress-5.6.2.tar.gz
sudo rm wordpress-5.6.2.tar.gz
```

Seuraavaksi käynnistetään Caddy-palvelu. Käynnistäessä normaalisti ilman sudoa, palvelu ilmoittaa, että ei ole oikeuksia muuttaa lokitiedostoa. Tämä on korjattu seuraavassa komennossa käynnistämällä Caddy-palvelu käyttämällä sudo caddy -komentoa (Komento 39).

Komento 39 Caddy -käynnistys caddy käyttäjänä

```
sudo caddy start
```

Nyt päästään Wordpressiin menemällä selaimella osoitteeseen omadomain.fi/wordpress. Wordpressin asennukseen tarvitaan aiemmin tehty mysql-tietokannan nimi, käyttäjä ja salasana. Database Host kohtaan jätetään localhost. Table Prefix kohtaan vaihdetaan oma teksti, että se ei ole oletusasetuksena.

Ennen kuin jatketaan, annetaan caddy käyttäjälle omistajuus html kansioon ja sen sisältöön (Komento 40).

Komento 40 Caddy ryhmälle ja käyttäjälle omistajuus www-kansioon ja sisältöön

```
sudo chown -R caddy:caddy /var/www
```

Nyt voidaan jatkaa ja jos asetukset on laitettu oikein, ilmoittaa wordpress, että asennus voidaan aloittaa. Asennuksen aloitetaan valitsemalla **Run the installation.**

Asennus on jokaiselle henkilökohtainen ja helppo. Tehdään käyttäjä ja annetaan sivulle nimi. Koska kyseessä on sivusto tarkoitettu henkilökohtaiseen käyttöön, otetaan **Search engine visibility** pois päältä. Kun nämä on laitettu, valitaan **Install WordPress**. Wordpressin voi nyt kirjautua oma-domain.fi/wp-login osoitteesta.

Nyt kun verkkosivut ovat toimivat, voidaan siirtyä asentamaan Wordpress-lisäosia ja tekemään sivustot, minkä kautta voidaan siirtää tiedostoja palvelimelle ja ladata tiedostoja palvelimelta. Tärkeä osa työtä on tietoturva, joten asennetaan Wordpress-lisäosia ja tehdään muutoksia asetuksiin, mitkä parantavat sivujen turvallisuutta. Lisäosat löydetään menemällä oma-domain.fi/wordpress/wp-admin, kirjautumalla sisään ja valitsemalla valikosta **Plugins** ja plugins sivulta **Add New.** Asennetaan seuraavat lisäosat (Taulukko 6).

Taulukko 6 Wordpress-lisäosat

Lisäosa	Käyttö
Classic Editor	Sallii klassisen tyylisen Wordpress editorin
UpdraftPlus	Varmuuskopioi Wordpress sivut joko paikallisesti tai pilveen. Voidaan myös ajoittaa.
All in one WP security	Auttaa edistämään Wordpress tietoturvaa. Ilmoittaa haavoittuvuuksista ja automaattisesti korjaa niitä tai neuvoo miten korjata ne manuaalisesti. Tärkeimmät asetukset: • Admin käyttäjän nimen vaihto • Kirjautumisyritysten määrä • Tiedostojen käyttöoikeudet • Palomuuri • Kirjautumisen sivun muutos • Tiedostojen listaus pois päältä • Tiedostojen skannaus
Password Protected	Lisäosaa voidaan käyttää sivujen suojaamiseen salasanalla.

Kun lisäosat on asennettu, pitää niiden asetukset muokata. Lisäosat ovat yksinkertaiset käyttää. Kun tarkastellaan lisäosien asetuksia, huomataan, että niistä löytyy ohjeet mitä asetukset tekevät. Näiden ohjeiden perusteella voidaan kytkeä päälle asetuksia kuten kirjautumisosoitteen muuttaminen, kirjautumisyritysten määrä, varmuuskopiointi jne.

Halutessa voidaan tehdä Wordpress-sivut itse tai valmiista teemasta ja julkaista siihen videoita ja muita tiedostoja.

10 Nextcloud-tiedostopalvelu

Nextcloud-palvelua käytetään, kun halutaan pelkkä tallennustila käyttöön. Tänne lähetetään tiedostoja, mitä voidaan ladata muille laitteille. Nextcloud toimii pilvitallennustilana ja se asennetaan palvelimelle samalla idealla kuin Caddy. Asennukseen löytyy ohjeet Nextcloudin omilta sivuilta (Nextcloud, 2021), mutta työssä tehdään niihin muutoksia koska ohjeet ovat alun perin tarkoitettu Apache-palvelimille. HDD-kiinnitykseen löytyy hyvä ohjeistus askubuntu palstoilta (Cainikovs, 2012). Asennetaan ensin tarvitut PHP-paketit ajamalla seuraavat komennot (Komento 41).

Komento 41 PHP-pakettien asennus

```
sudo apt update
sudo apt install php8.0-gd php8.0-mysql php8.0-curl php8.0-mbstring
php8.0-intl
sudo apt install php8.0-gmp php8.0-bcmath php-imagick php8.0-xml
php8.0-zip
```

Seuraavaksi avataan mysql ja tehdään uusi tietokanta nextcloud (Komento 42). Tässä käytetään aiemmin tehtyä käyttäjää (Komento 34).

Komento 42 Nextcloud-tietokannan luonti ja käyttöoikeudet

```
sudo mysql
CREATE DATABASE IF NOT EXISTS nextcloud CHARACTER SET utf8mb4 COLLATE
utf8mb4_general_ci;
GRANT ALL PRIVILEGES ON nextcloud.* TO ‘käyttäjä’;
FLUSH PRIVILEGES;
exit
```

Seuraavaksi ladataan Nextcloud-sivustolta palvelinversio ohjelmasta valitsemalla **Download for server** ja lataamalla tar.gz paketin ja sen MD5-tiedoston (Nextcloud, 2021). Siirrytään kansioon mihin tiedostot latautuivat cd /home/käyttäjä/downloads tai vastaava ja varmistetaan tiedoston MD5 (Komento 43). Version numero 21.0.0 voi muuttua tulevaisuudessa.

Komento 43 Nextcloud-tiedoston MD5 sum

```
md5sum -c nextcloud-21.0.0.tar.bz2.md5 < nextcloud-21.0.0.tar.bz2
```

Kun tiedosto on varmennettu, se voidaan purkaa, siirtää kovalevylle ja antaa sen omistajuus caddy käyttäjälle (Komento 44).

Komento 44 Pura Nextcloud-tiedosto, kopioi se html kansioon ja annetaan omistajuus caddy käyttäjälle

```
sudo tar -xjf nextcloud-21.0.0.tar.bz2
sudo cp nextcloud /var/www/html
sudo chown -R caddy:caddy /var/www/html/nextcloud
```

Nyt Nextcloud-palveluun päästään menemällä selaimella **oma-domain.fi/nextcloud**.

Seuraavaksi tehdään HDD-levyn kiinnitys kohteeseen /HDD ja sinne kansion data. (Komento 48). Muokataan ensin /etc/fstab-tiedostoa (Komento 45) lisäämällä sinne tehdyn partition tiedot (Komento 46) tiedoston loppuun (Komento 47).

Komento 45 Muokkaa fstab-tiedostoa

```
sudo nano /etc/fstab
```

Komento 46 Hae levyjen tiedot

```
sudo fdisk -l
```

Komento 47 Fstab-tiedoston loppuun lisättävä teksti

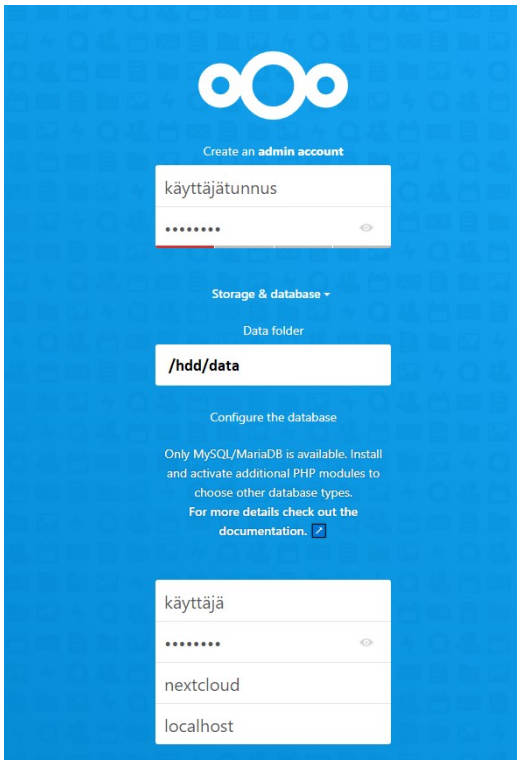
```
/dev/sdb2 /hdd ext4 defaults 0 0
```

Komento 48 Nextcloud data kansio luonti, oikeudet ja HDD-levyn kiinnitys

```
sudo mkdir /hdd
sudo mkdir /hdd/data
sudo chmod -R 0770 /hdd/data
sudo chown -R caddy:caddy /hdd/data
sudo mount /hdd
```

Seuraava vaihe on selaimella **oma-domain.fi/nextcloud** osoitteessa admin tunnusten luominen, Nextcloud-tiedostojen sijainnin valinta tallennuksille ja tehdyn tietokannan valinta. (Kuva 25).

Kuva 25 Nextcloud käyttäjä, tallennus kohde ja tietokanta valinta



Kun asennus on valmis, käytettävissä on pilvipalvelu mihin pääsee käsiksi jopa ulkoverkosta ja koska data kansioksi on asetettu tehty HDD-kiinnitys, on käytettävissä yli 2Tt tallennuskapasiteettia.

Mikäli tämä tapa ei toimi ja palvelu näyttää eri määrän tallennuskapasiteettia, voidaan käyttää External storages -lisäosaa valitsemalla oikealta ylhäältä **oma kuvake > apps > Disabled apps** ja laittamalla External storages aktiiviseksi. Tämän jälkeen kirjaudutaan ulos ja takaisin sisään ja siirrytään **oma kuvake > settings > External storages** ja lisätään halutun kovalevyn polun tänne. Valitaan myös oikealta käyttäjä, jolle halutaan antaa oikeudet tallennustilaan.

Kytketään myös päälle tiedostojen suojaus AES 256 -avaimilla. Moduulin kytketään päälle valitsemalla oikealta ylhäältä **oma kuvake > apps > Disabled apps** ja valitsemalla **enable** Default encryption module kohdan oikealta puolelta. Seuraavaksi kirjaudutaan ulos ja takaisin sisään ja siirrytään **oma kuvake > settings > Administration - Security** ja laitetaan **Enable server-side encryption** päälle.

11 Palvelimen varmuuskopiointi ja päivitykset

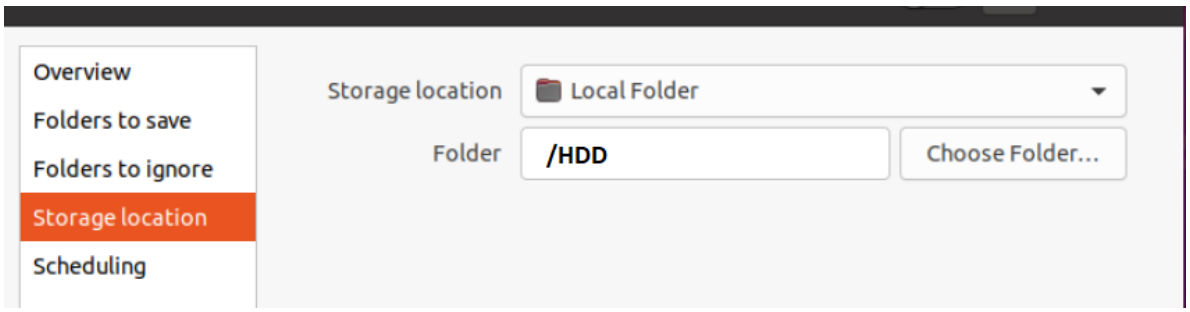
Palvelimen varmuuskopiointiin käytetään tässä työssä Deja Dup nimistä ohjelmaa. Se on suosittu työkalu ja toimii hyvin tiedostojen varmuuskopioinnissa. Deja Dup -ohjelmalla saa myös ajoitettua varmuuskopiot. Ohjelman voi asentaa helposti apt install -komennolla (Komento 49).

Komento 49 Deja Dup asennus

```
sudo apt-get install deja-dup
```

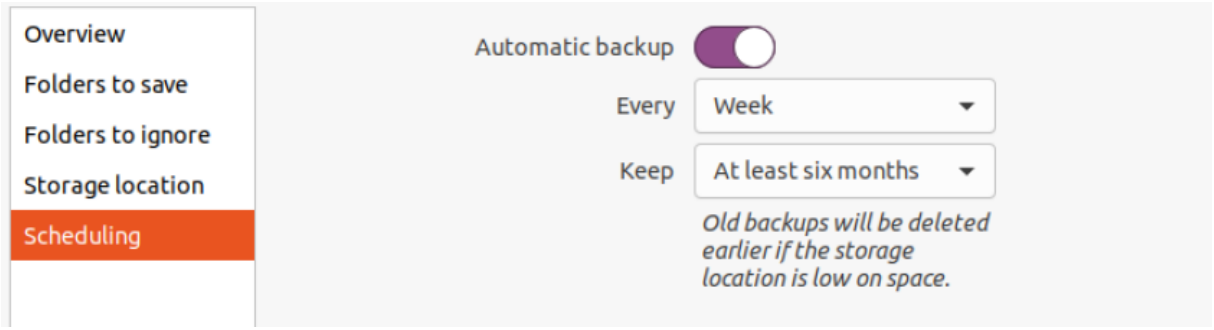
Kun työkalu on asentunut, se voidaan avata hakemalla ja valitsemalla **Backup**. Nyt voidaan valita **Folders to save** kohdasta mitä halutaan varmuuskopioida. Valitaan **/home** kansio, **/var/www** kansio ja **/etc/caddy** kansio. **Folders to ignore** kohtaan valitaan vain **Trash**. **Storage location** kohdasta valitaan mihin varmuuskopio tallennetaan (Kuva 26). Varmuuskopion voi tehdä minne vaan, mutta on suositeltua käyttää erillistä kovalevyä, usb tikkua tai vastaavaa palvelimesta erillistä tallennustilaa. Näin varmistetaan, että varmuuskopio ei tuhoudu, mikäli palvelimelle tapahtuu jotain. Käytetään tehtyä /HDD-kiinnitystä, koska käytettävissä ei ole muuta vaihtoehtoa tällä hetkellä.

Kuva 26 Varmuuskopio sijainti



Kun kohde on valittu, voidaan siirtyä **Scheduling** valikkoon mistä valitaan, kuinka usein varmuuskopio tehdään. Valitaan viikoittainen varmuuskopiointi ja säilytetään tiedostoja enintään 6kk (Kuva 27).

Kuva 27 Automaattinen varmuuskopio ajoitus



Kun asetukset ovat valmiit, siirrytään **Overview** välilehteen ja valitaan **Backup now**. Ohjelma kysyy, halutaanko suojata varmuuskopiota salasanalla, niin että palautus onnistuu vain sillä salasanalla. Jos salasana hukkuu, ei palautus enää onnistu. Koska halutaan, että varmuuskopio on suojattu, sille asetetaan vahva salasana ja painetaan **Forward**. Tämä aloittaa varmuuskopioinnin missä kestää hetki johtuen varmuuskopion koosta. Mikäli työ halutaan pysäyttää, voidaan valita **Resume later**. Jos varmuuskopioidessa esiintyy ongelmia käyttöoikeuksien kanssa, voidaan sulkea Deja dup-ohjelma, siirtyä terminaaliin ja käynnistää varmuuskopio sitä kautta (Komento 50).

Komento 50 Deja dup varmuuskopio -komento

```
sudo deja-dup --backup
```

Työssä halutaan myös varmistaa, että mahdolliset tietoturvapäivitykset eivät unohdu, joten palvelimelle tehdään automaattiset päivitys konfiguraatiot. Tähän löytyy ohjeet libre-software sivustoilta (Eva, 2018).

Automaattiset päivitykset konfigurointi voidaan tehdä muokkaamalla tiedostoa 50unattended-upgrades (Komento 51).

Komento 51 Muokkaa tiedostoa 50unattended-upgrades

```
sudo nano /etc/apt/apt.conf.d/50unattended-upgrades
```

Tästä tiedostosta otetaan kommenttimerkit // pois seuraavista kohdista ja muokataan tarvittaessa tekstiä.

```
"${distro_id}:${distro_codename}-updates";
Unattended-Upgrade::Remove-Unused-Kernel-Packages "true";
```

```
Unattended-Upgrade::Remove-Unused-Dependencies "true";
Unattended-Upgrade::Automatic-Reboot "true";
Unattended-Upgrade::Automatic-Reboot-Time "02:30";
```

Tämä varmistaa, että palvelin päivittää automaattisesti, poistaa vanhentuneet ja käyttämättömät kernel-paketit ja käynnistää uudestaan tarvittaessa.

Automaattiset päivitykset saa päälle, muokkaamalla tiedostoa 20auto-upgrades (Komento 52).

Komento 52 Tiedoston 20auto-upgrades muokkaus -komento

```
sudo nano /etc/apt/apt.conf.d/20auto-upgrades
```

Todennäköisesti Caddy on lisännyt asennuksen yhteydessä hieman päivitysten automaatiota. Tiedostossa pitää olla seuraavat linjat.

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "7";
APT::Periodic::Unattended-Upgrade "1";
```

Nyt automaattiset päivitykset on konfiguroitu ja kytketty päälle. Toinen vaihtoehto automaattisille päivityksille on tehdä uusi Cron-job, jolla voidaan ajoittaa muitakin komentoja. Tätä menetelmää ei tarvita tässä työssä.

12 Yhteenveto

Työssä tutustuttiin palvelimen käyttöönottomahdollisuuksiin kotona. Työssä pääsin kokeilemaan uudenlaista Caddy-palvelinohjelmistoa. Tätä vertaisin muihin palvelinohjelmistoihin ja pystyin todeta, että Caddy-ohjelmalla on hyvät mahdollisuudet toimia yleisessä käytössä. Huomasin sen olevan helposti opittava, yksinkertainen ja toimiva. Ongelmana esiintyi vain dokumentaation ja käyttökokemusten puutteellisuus. Tällä hetkellä ohjelmat kuten Apache, IIS ja NGINX ovat pitkällä johdossa palvelinohjelmistojen suosiossa, mutta Caddy-ohjelma vaikuttaa lupaavalta kilpailijalta erityisesti sen helppokäyttöisyyden vuoksi. Caddy on hyvä erityisesti sen automaattisen TLS-asennuksen vuoksi, ja sen käyttöä saattaa nähdä jatkossa palvelinratkaisuissa enemmän ja enemmän.

Käyttöjärjestelmää valittaessa ei päätös ollut helppo. Molemmat Windows-, ja Linux-käyttöjärjestelmät olivat hyviä vaihtoehtoja, molemmat omilla hyödyillään ja haitoillaan. Pystyin kuitenkin valitsemaan Linux-pohjaisen käyttöjärjestelmän, sillä koin sen olevan käytännöllisempi kyseiseen tarpeeseen, johtuen sen vakaudesta, tietoturvasta ja joustavuudesta.

Palvelinta luodessa, otin huomioon mahdolliset tietoturva-aukot ja paikkailin niitä tarpeen mukaan. Maksimi tietoturvaa en pystynyt saavuttamaan, sillä se vaatisi kaiken ulkoisen verkkoliikenteen estämisen palvelimelle, mikä estäisi pääsyni julkisesta verkosta kyseiseen palvelimeen. Tähän löytyi kuitenkin pieniä helpotuksia, asettamalla vahvoja salasanoja ja pakottamalla tiettyjä sääntöjä kirjautumiseen. Palvelimen turhat tunnukset ja oletusportit muutettiin tai poistettiin tarvittaessa. Palvelimen jatkuvuuden varmistin automatisoimalla varmuuskopiot ja päivitykset. Ongelmien tullessa palvelimen tiedostot voidaan palauttaa varmuuskopiosta käyttämällä samaa työkalua, kuin millä varmuuskopiot tehtiin.

Työssä opin tutkimaan, vertaamaan ja käyttämään omaa osaamistani palvelimen käyttöönotossa. Suunnittelu oli tärkeä osa työtä ja se mahdollisti työn edistymisen ilman suurempia muutoksia. Työssä tuli paljon ongelmia vastaan, mitä ratkomalla opin paljon vianetsinnästä ja ongelmanratkaisusta, kun dokumentaatiota ja ohjeita vioista ei löytynyt helpolla.

Lähteet

blogs.helsinki.fi. (2021). *Tietoturvan periaatteet*. Noudettu osoitteesta https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-1-tietoturvan-ja-tietosuojan-perusteet/tietoturvan-edellytykset/

Brown, K. (2020). *Microsoft IIS reviews.* Noudettu osoitteesta https://www.trustradius.com/reviews/microsoft-iis-2020-09-10-16-29-37

Buranasanti, P. P. (2019). *Caddy web server.* Noudettu osoitteesta https://www.iiwnz.com/caddy/

caddyserver.com. (2021). Noudettu osoitteesta https://caddyserver.com/docs

Caddyserver.com. (2021). *The Ultimate Server.* Noudettu osoitteesta https://caddyserver.com/

Cainikovs, A. (2012). *How do I add an additional hard drive?* Noudettu osoitteesta https://askubuntu.com/questions/125257/how-do-i-add-an-additional-hard-drive

Devenport, E. (2014). *Use SSH Keys With PuTTY On Windows*. Noudettu osoitteesta https://devops.ionos.com/tutorials/use-ssh-keys-with-putty-on-windows/

Dhangar, R. (2019). *Microsoft IIS reviews.* Noudettu osoitteesta https://www.trustradius.com/reviews/microsoft-iis-2019-03-12-08-21-19

Eva, J. (2018). *How to set up automatic updates on Ubuntu Server 18.04 or 20.04*. Noudettu osoitteesta https://libre-software.net/ubuntu-automatic-updates/

Fahim, F. (2020). *What is Apache Web Server? (Pros and Cons of Apache)*. Noudettu osoitteesta https://serverguy.com/servers/what-is-apache-web-server/

Forkbeard. (2013). *Trying to do ssh authentication with key files: server refused our key*. Noudettu osoitteesta https://askubuntu.com/questions/306798/trying-to-do-ssh-authentication-with-key-files-server-refused-our-key?answertab=votes#tab-top

Hilton, P. (2021). *Pros and cons of using IIS.* Noudettu osoitteesta https://hilton.org.uk/iis-asp-perlscript-ado

httpd.apache.org. (2021). *Apache HTTP Server Project*. Noudettu osoitteesta https://httpd.apache.org/

Imes, C. (2017). *DiskSpace.* Noudettu osoitteesta https://help.ubuntu.com/community/DiskSpace

Janjic, V. (2017). *Performance Comparison: Apache vs. IIS.* Noudettu osoitteesta https://www.devx.com/webdev/performance-comparison-apache-vs.-iis.html

Jethva, H. (2015). *Secure The SSH Server On Ubuntu.* Noudettu osoitteesta https://devops.ionos.com/tutorials/secure-the-ssh-server-on-ubuntu/

juhanit.wordpress.com. (2013). *Tietoturvan kolme kovaa: Luottamuksellisuus, eheys ja saatavuus.* Noudettu osoitteesta https://juhanit.wordpress.com/2013/08/25/tietoturvallisuuden-kolme-kovaa-luottamuksellisuus-eheys-ja-saatavuus/

Keith. (2020). *Caddy "listen tcp :443: bind: permission denied"*. Noudettu osoitteesta https://serverfault.com/questions/807883/caddy-listen-tcp-443-bind-permission-denied

Keycdn.com. (2018). *Nginx vs Apache.* Noudettu osoitteesta https://www.keycdn.com/support/nginx-vs-apache

Kili, A. (2017). *How to Install Samba on Ubuntu for File Sharing on Windows*. Noudettu osoitteesta https://www.tecmint.com/install-samba-on-ubuntu-for-file-sharing-on-windows/

Kinsta.com. (2021). *What Is Nginx? A Basic Look at What It Is and How It Works.* Noudettu osoitteesta https://kinsta.com/knowledgebase/what-is-nginx/

Kochtan, K. (2019). *Microsoft IIS reviews.* Noudettu osoitteesta https://www.trustradius.com/reviews/microsoft-iis-2019-08-19-11-34-23

Kyberturvallisuuskeskus.fi. (2020). *Tietoturva.* Noudettu osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Malmberg, T. (2017). Noudettu osoitteesta https://www.mintsecurity.fi/tietojarjestelmien-kovennukset/

Microsoft Corporation. (2021). *System requirements for installing Windows 10*. Noudettu osoitteesta https://www.microsoft.com/en-us/windows/windows-10-specifications

Microsoft Corporation. (2021). *Windows 10 Home and Pro Lifecycle*. Noudettu osoitteesta https://docs.microsoft.com/en-us/lifecycle/products/windows-10-home-and-pro

Microsoft Corporation. (2021). *Windows 10:n käyttäminen.* Noudettu osoitteesta https://www.microsoft.com/fi-fi/windows/features?activetab=feature-pivot:primaryr6

Nextcloud. (2021). *Install Nextcloud*. Noudettu osoitteesta https://nextcloud.com/install/#

Nextcloud. (2021). *Nextcloud Example installation on Ubuntu 20.04 LTS*. Noudettu osoitteesta

https://docs.nextcloud.com/server/20/admin_manual/installation/example_ubuntu.html

Nginx.com. (2021). *Welcome to NGINX Wiki.* Noudettu osoitteesta https://www.nginx.com/resources/wiki/

Salter, J. (2020). *Caddy offers TLS, HTTPS, and more in one dependency-free Go Web server.* Noudettu osoitteesta https://arstechnica.com/gadgets/2020/05/caddy-offers-tls-https-and-more-in-one-dependency-free-go-web-server/

Singh, N. (2020). *How to Install and Configure Caddy Web Server with PHP and MariaDB on Ubuntu 20.04*. Noudettu osoitteesta https://www.howtoforge.com/tutorial/ubuntu-caddy-web-server-installation/

Templin, R.;Moore, S.;Schonning, N.;& Patel, S. (2007). *Introduction to IIS Architectures.* Noudettu osoitteesta https://docs.microsoft.com/en-us/iis/get-started/introduction-to-iis/introduction-to-iis-architecture

Ubuntu.com. (2021). *Install and Configure Samba.* Noudettu osoitteesta https://ubuntu.com/tutorials/install-and-configure-samba#1-overview

Ubuntu-fi.org. (2021). *Lataa Ubuntu*. Noudettu osoitteesta https://www.ubuntu-fi.org/lataa-ubuntu/

Ubuntu-fi.org. (2021). *Tapaa Ubuntu.* Noudettu osoitteesta https://www.ubuntu-fi.org

Vuollet, P. (2018). *What is IIS.* Noudettu osoitteesta https://stackify.com/iis-web-server/

wiki.Ubuntu-fi.org. (2021). *Laitteistovaatimukset.* Noudettu osoitteesta https://wiki.ubuntu-fi.org/Laitteistovaatimukset

Wood, G. (2021). *Ubuntu Releases*. Noudettu osoitteesta https://wiki.ubuntu.com/Releases

Liite 1: Aineistonhallintasuunnitelma

Miten aineistoa kerätään

Aineistoa kerätään lukemalla artikkeleja ja tekstejä mitä löydetään netistä. Aineistoa kerätään myös tekemällä itse asennuksia, testauksia ja vianselvityksiä.

Miten aineistoa käytetään

Aineistoa tutkitaan ja käsitellään tarpeen mukaan ja siitä kirjataan aiheelliset osat. Esimerkiksi hyödylliset löydökset asennuksissa ja vianselvityksissä on kirjattava ylös, että opinnäytetyötä lukeva voi selvittää mahdollisia ongelmia mitä voi esiintyä työn asennuksissa ja konfiguraatioissa.

Miten aineistoa säilytetään ja arkistoidaan

Aineisto säilytetään oman kodin päätietokoneella ja se varmuuskopioidaan saman tietokoneen erilliselle kovalevylle. Varmuuskopioita tehdään jatkuvasti aineiston kertyessä joka kerta kun aineistoon tulee muutoksia.

Arkaluontoisen ja luottamuksellisen tiedon keräämistä vältetään. Mahdolliset yksityiset IP-osoitteet ja salasanat sensuroidaan ja sensuroimattomat tiedot poistetaan heti.

Päätietokone mille aineisto tallennettu, on suojattu palomuurilla ja antivirus-ohjelmalla.

Miten aineistoa jatko käytetään ja tuhotaan

Aineiston tarve päättyy, kun työ on valmis, joten ne voidaan tuhota. Niitä säilytetään kuitenkin vähintään 1 vuosi työn valmistuttua.