

VIRTUAALINEN PILVIPALVELU AVOIMEN LÄHDEKODIN OHJELMISTOILLA

Ryynänen Ari

Opinnäytetyö
Tekniikan koulutusohjelma (Rovaniemi)
Tieto- ja viestintätekniikan koulutusohjelma
Insinööri (AMK)

2017

Tekniikan koulutusohjelma
(Rovaniemi)
Tieto- ja viestintätekniikan
koulutusohjelma
Insinööri (AMK)

Tekijä	Ari Ryyänen	Vuosi	2017
Ohjaaja	Tauno Tepsa		
Työn nimi	Virtuaalinen pilvipalvelu avoimen lähdekoodin ohjelmistoilla		
Sivumäärä	39		

Erilaiset etäpalvelut ja –tallennukset ovat kasvattaneet suosiotaan niin yksityishenkilöiden kuin yritysten käytössä. Esimerkiksi Google, Microsoft ja Apple tarjoavat omia versioitaan omille käyttöjärjestelmilleen ja myös riippumattomat toimijat ovat tuottaneet vastaavia ympäristöjä, osa suuremmalla, osa pienemmällä valikoimalla ominaisuuksia. Esille on myös noussut yksityisyydensuoja ja tietoturva, koska moni suuri toimija on Yhdysvaltalainen ja siellä tietosuoja on erittäin heikko verrattuna Euroopan Unionin ja etenkin Suomen vastaavaan. Tässä opinnäytetyössä kuvataan täysin omassa hallinnassa olevan palvelinympäristön luominen.

Tässä opinnäytetyössä kuvataan sellaisen kotikäyttöön ja pienyritykseen soveltuvan palvelinympäristön pystyttäminen, joka mahdollistaa useampien erilaisten palvelimien ylläpidon. Opinnäytetyössä keskitytään pilvipalvelimen asentamiseen ja käyttöönottoon, sisältäen tiedostojen, osoitetietojen ja kalenterin käytön eri päätelaitteilla.

Erilaisia palvelintyyppäjä on lukuisia, kuten kuvagalleriat, tietokannat, WWW-sivustot ja foorumit, mutta opinnäytetyö käsittelee vain yhtä osa-aluetta. Asennettava virtuaalipalvelinympäristö mahdollistaa kuitenkin melkein minkä tahansa palvelimen lisäämisen pelkästään virtuaalipalvelimen asentamalla.

Avainsanat NextCloud, virtualisointi, pilvipalvelut

Technology, Communication and
Transport
Degree Programme in Information
and Communication Technology
Bachelor of Engineering

Author	Ari Ryyänen	Year	2017
Supervisor	Tauno Tepsa		
Subject of thesis	Virtual Cloud Service Using Open Source Software		
Number of pages	39		

During the last years, different kinds of cloud services and storage options have become more popular for both personal and business use. Google, Microsoft and Apple are providing their own versions for their own operating systems, but also third-party providers are offering their own solutions, with a variety of components and service. Privacy and security have become more and more important during the development. This is mainly because several significant providers are from the USA, where the laws about privacy and security are quite different compared to the European Union and especially to Finland. The objective of this thesis was to show how to build a server environment that is totally in the owner's control.

This thesis described how to build a server environment for personal or SOHO use, allowing to run and control several various kinds of servers. In this thesis, it was concentrated on installing and deploying a cloud server, including the use of files, an address book and a calendar with several types of end devices.

There are many kinds of servers available, such as picture galleries, databases, WWW servers and chat forums, but in this thesis, only one of them was concentrated on. However, virtual server environment allows to install almost any kind of server software by only adding a new virtual server.

Key words NextCloud, virtualization, cloud services

SISÄLLYS

1	JOHDANTO	6
2	KÄYTETTÄVÄT JÄRJESTELMÄT	7
2.1	Virtualisointipalvelin	7
2.2	Pilvipalvelut	7
2.3	Laitteisto	8
3	VIRTUALISOINTIPALVELIMEN ASENNUS	9
3.1	Käyttöjärjestelmän asennus	9
3.1.1	Proxmox VE lisenssi	9
3.1.2	Sijainti ja aikavyöhyke	11
3.1.3	Pääkäyttäjän tiedot	11
3.1.4	Verkon määrittely	12
3.1.5	Asennuksen päättäminen	13
3.2	Kirjautuminen järjestelmään	13
4	VIRTUAALIKONEIDEN HALLINTA	16
4.1	Uuden virtuaalikoneen lisääminen	16
4.1.1	Aloituskäyttö	16
4.1.2	Levytila ja asennusmedian valinta	17
4.1.3	Virtuaalikoneen luominen ja käynnistyslevyn valinta	18
4.1.4	Suorittimet ja keskusmuisti	21
4.1.5	Verkon määrittely	23
4.1.6	Tarkistus ja hyväksyntä	25
4.2	Käyttöjärjestelmän asennus	27
4.2.1	Virtuaalikoneen käynnistäminen	27
4.2.2	Käyttäjätunnukset ja oikeudet	28
4.2.3	Ohjelmiston päivitys	30
5	NEXTCLOUDIN ASENTAMINEN	31
6	LISÄPALVELUT	34
6.1	Nimipalvelu	34
6.2	SSL-sertifikaatti	35
7	TYÖPÖYTÄ- JA MATKAPUHELINSOVELLUKSEN ASENTAMINEN	36

7.1	Työpöytäsovellukset	36
7.2	Matkapuhelinsovellukset.....	36
7.3	Selainkäyttöliittymä	37
8	POHDINTA.....	38
	LÄHTEET.....	39

1 JOHDANTO

Nykyaikana matkapuhelinten, tablettitietokoneiden ja kannettavien tietokoneiden käyttö on lisääntynyt huomattavasti johtaen valtavaan määrään sekä kuvallista että sanallista informaatiota, johon halutaan päästä käsiksi ajasta ja paikasta riippumatta. Tähän tarpeeseen ovat heränneet suuret palveluntarjoajat kuten Microsoft, Google ja Dropbox, jotka tarjoavat joko ilmaiseksi tai korvausta vastaan tallennustilaa niin kuville, muille tiedostoille, yhteystiedoille ja kalenterimerkinnöille. Nämä palvelut ovat kansainvälisten suuryritysten hallinnoimia ja niihin liittyy myös huonoja puolia, suurimpina tietoturvaongelmat ja mainokset. Tarjolla on koti- ja yrityskäyttöön ratkaisuja, jotka voi asentaa täysin omassa hallinnassa oleviin ympäristöihin.

Tämä opinnäytetyö käsittelee yhtä vaihtoehtoa tietojen tallentamiseen ja hallintaan omassa ympäristössä. Tässä opinnäytetyössä näytetään, miten rakennetaan oma palvelinympäristö, johon voidaan asentaa yksinkertaisesti myös muita palveluita, esimerkiksi media- ja WWW-palvelimet. Käytettävät ohjelmistot ovat avoimen lähdekoodin lisenssin alaisia ja ilmaisia käytössä.

Opinnäytetyössä käytettävät menetelmät vaativat perusteiden hallintaa pääasiassa Linux-käyttöjärjestelmästä ja sen komentotulkista sekä englannin kielen taitoa. Esimerkkilaitteisto on itse suunniteltu ja rakennettu tätä tarkoitusta varten, mutta järjestelmän voi rakentaa melkein mihin tahansa sopivaan laitteistoon. Itse pilvipalvelun voi asentaa myös ilman virtualisointia, mikäli ei ole tarvetta muille palveluille ja käytettävissä on oma tietokone sitä varten.

2 KÄYTETTÄVÄT JÄRJESTELMÄT

2.1 Virtualisointipalvelin

Virtualisoinnilla tarkoitetaan lyhyesti ilmaistuna tekniikkaa, jolla voidaan tilanteesta riippuen joko yhdistää suurempia kokonaisuuksia näkymään yhtenä yksikönä tai jakaa yhden laitteen useampaan osaan. Yleensä tällä tarkoitetaan tietokoneen resurssien jakoa useampaan osaan joista jokainen ajaa omaa versiotaan käyttöjärjestelmästä (What is virtualization 2017.)

Tähän opinnäytetyöhön valittiin käytettäväksi virtualisointipalvelimeksi Proxmox VE-palvelinohjelmisto (Server virtualization management with Proxmox VE 2017). Proxmox VE tukee kahta virtualisoinnin tyyppiä, KVM ja LXC. Erona näillä on virtualisoinnin aste. KVM on täysin virtualisoitu, jolloin asennettu käyttöjärjestelmä kuvittelee toimivansa sille kokonaan varatussa tietokoneessa, mahdollistaen useita eri käyttöjärjestelmävaihtoehtoja, kuten Microsoft Windows, Linux ja BSD:n eri versiot (KVM contributors 2017). LXC on tarkoitettu Linux-käyttöjärjestelmän suorittamiseen ja virtualisoi ainoastaan osan järjestelmästä käyttäen hyväkseen allansa toimivan käyttöjärjestelmän palveluita API-rajapinnan kautta (LXC 2017).

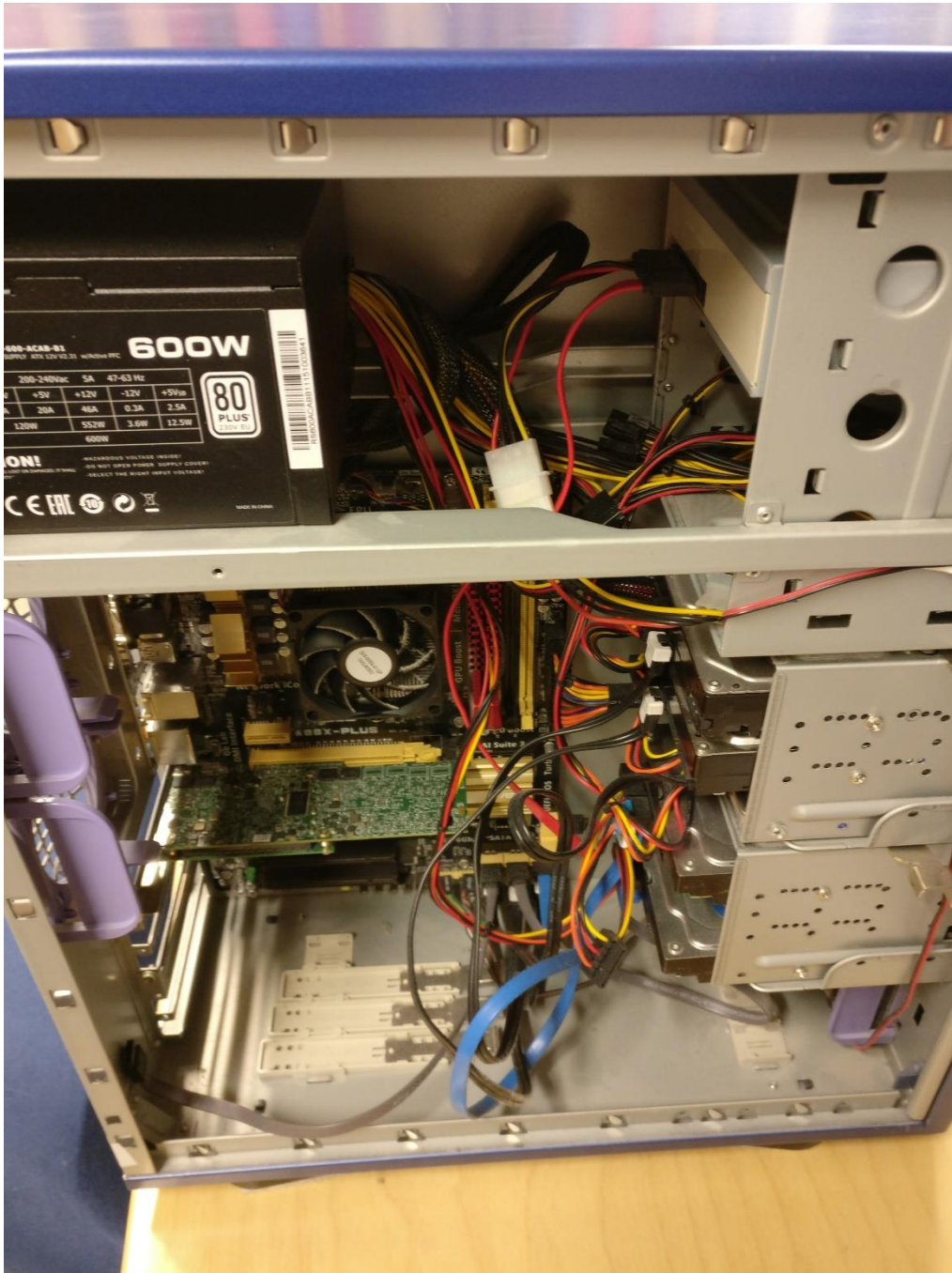
2.2 Pilvipalvelut

Pilvipalveluita on monia erilaisia, yksinkertaisesta tiedostopalvelimesta hyvinkin monimutkaisiin järjestelmiin. Periaatteessa mitä tahansa tietoa voidaan tallentaa pilveen, mutta tässä opinnäytetyössä keskitytään tiedostojen, kalenterin ja yhteystietojen tallentamiseen ja jakamiseen.

Käytettäväksi pilvipalvelinohjelmistoksi valikoitui Nextcloud, joka on ilmainen täysin avoimen lähdekoodin aktiivisesti kehittyvä projekti. Nextcloud tarjoaa muun muassa tiedostojen, yhteystietojen ja kalenterin jakamisen, mutta se sisältää myös monia muita ominaisuuksia, joita tässä opinnäytetyössä ei käsitellä (Nextcloud 2017.)

2.3 Laitteisto

Opinnäytetyössä käytettävä tietokone on itse kasattu peruskomponenteista (Kuvio 1). Laitteistossa on haettu edullista vaihtoehtoa kohtuullisen tehokkaaseen virtualisointiin kykenevään PC-standardien mukaista kokoonpanoa. Laitteiston rakentamiseen tämä opinnäytetyö ei keskity.

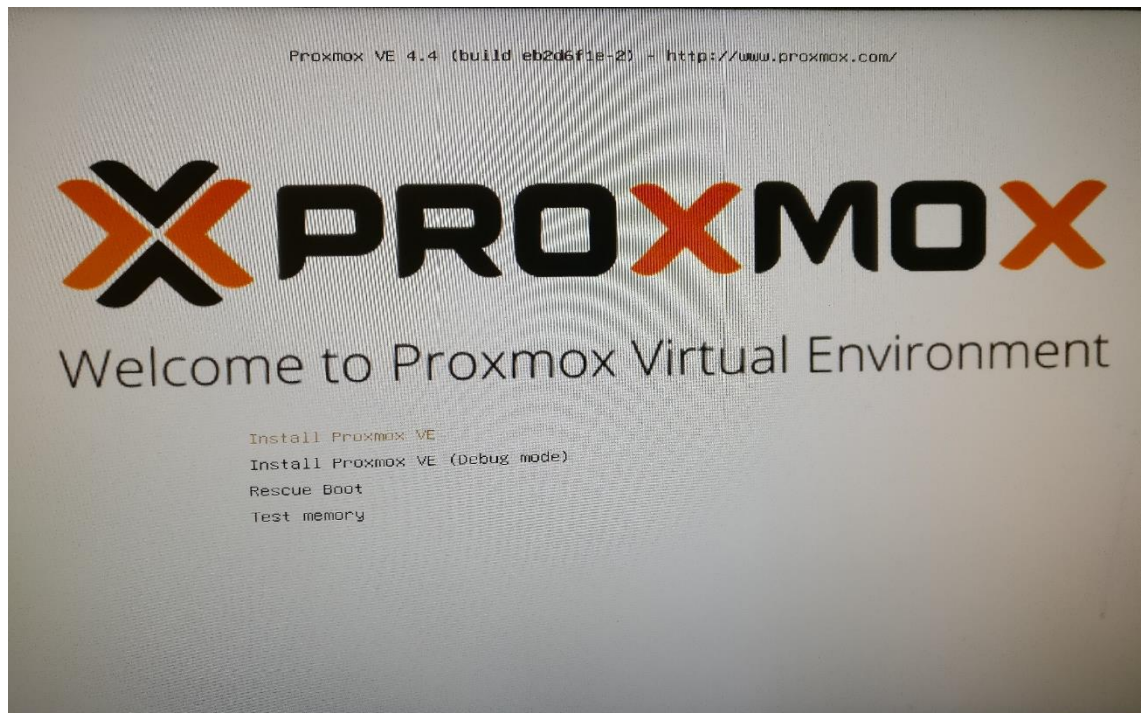


Kuvio 1. Palvelimen sisäkuva

3 VIRTUALISOINTIPALVELIMEN ASENNUS

3.1 Käyttöjärjestelmän asennus

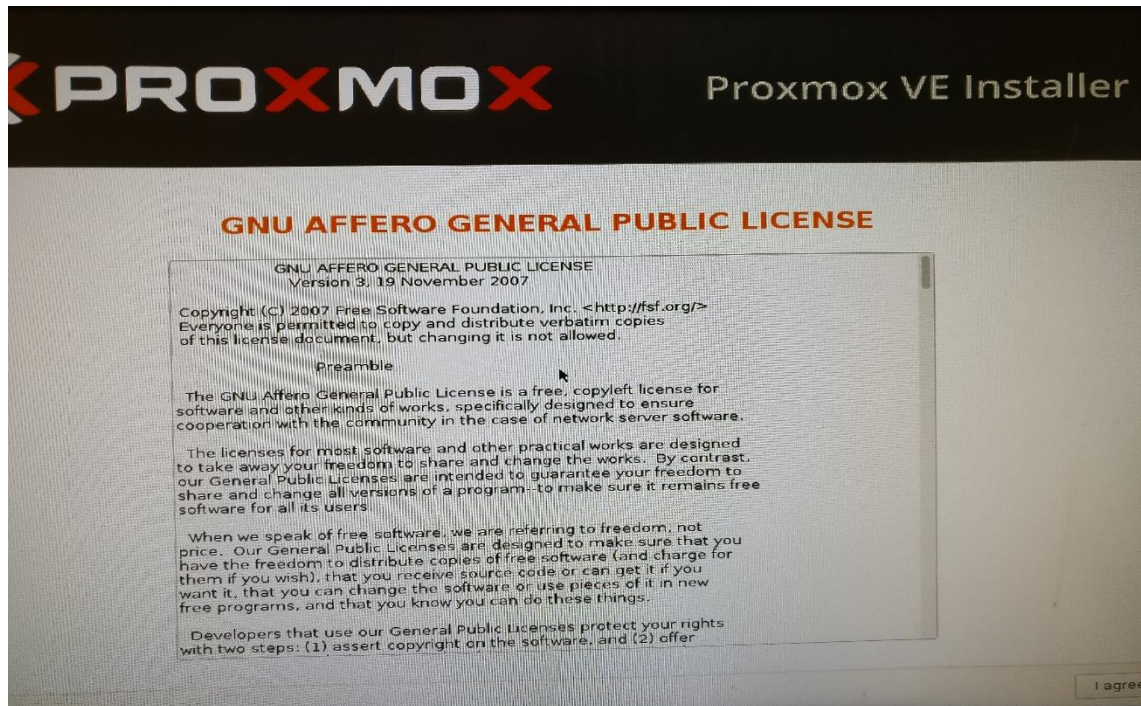
Asennus aloitetaan valmistelemalla USB-muistitikku, joka sisältää Proxmox VE-palvelinohjelmiston. Muistitikku kytketään tietokoneeseen ja kone käynnistetään siltä (Kuvio 2). Valikosta valitaan ensimmäinen kohta, "Install Proxmox VE", painamalla Enter.



Kuvio 2. Proxmox VE asennuksen käynnistysnäky

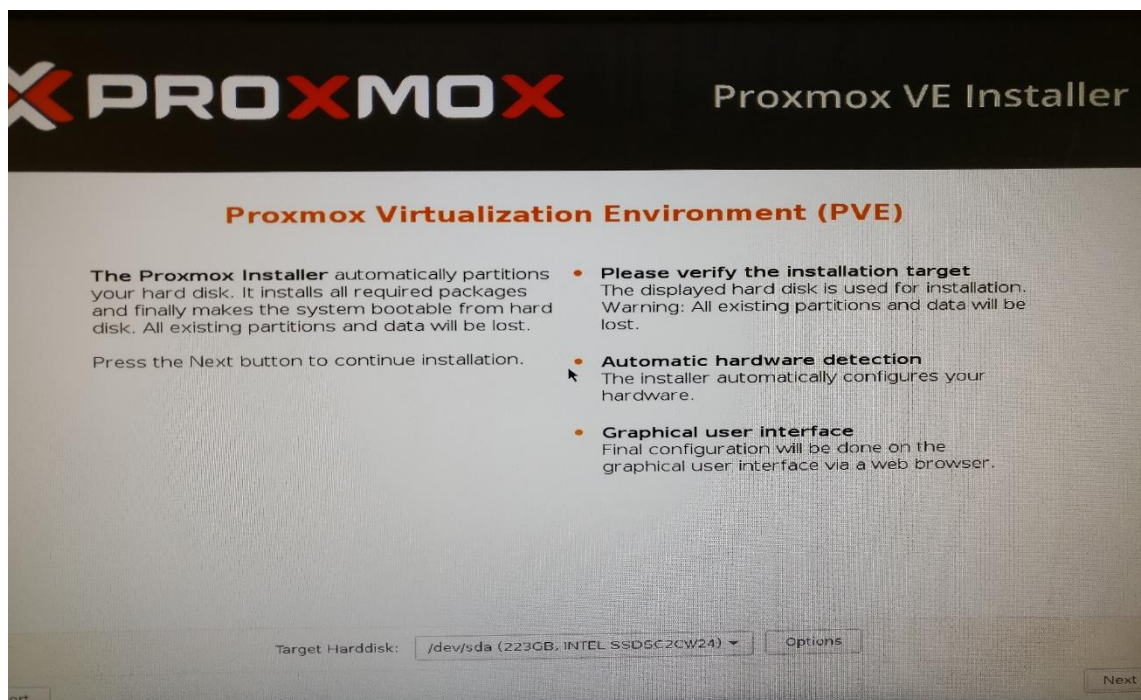
3.1.1 Proxmox VE lisenssi

Asennusohjelmiston lataaminen kestää hetken, minkä jälkeen ensimmäisenä tulee hyväksyttäväksi ohjelmiston lisenssi (Kuvio 3). Lisenssi hyväksytään painamalla oikeassa alakulmassa sijaitsevaa "I agree"-painonappia.



Kuvio 3. GNU Affero General Public License

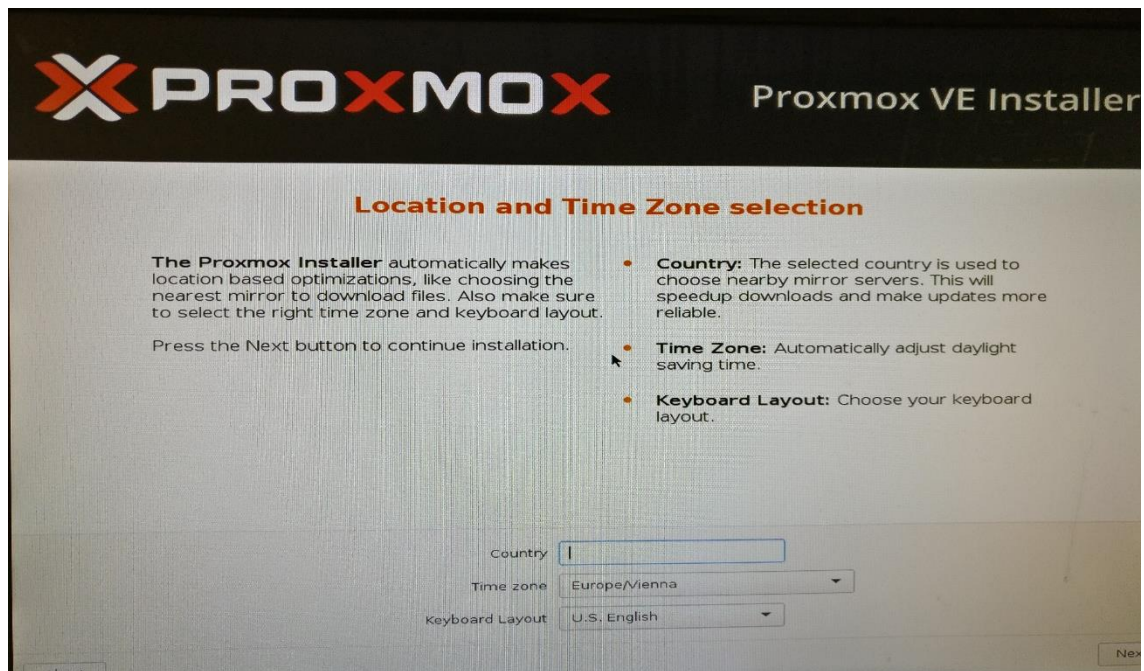
Tämän jälkeen ohjelmisto ehdottaa automaattisesti asennuskohteeksi tietokoneen ensimmäistä kiintolevyä ja kertoo, miten asennus jatkuu (Kuvio 4). Tässä opinnäytetyössä ei tarkastella lisävalintoja, koska niiden muuttaminen vaatii syvempää tietämystä Linux-käyttöjärjestelmästä ja tavasta käsitellä kiintolevyjä.



Kuvio 4. Levyn valinta

3.1.2 Sijainti ja aikavyöhyke

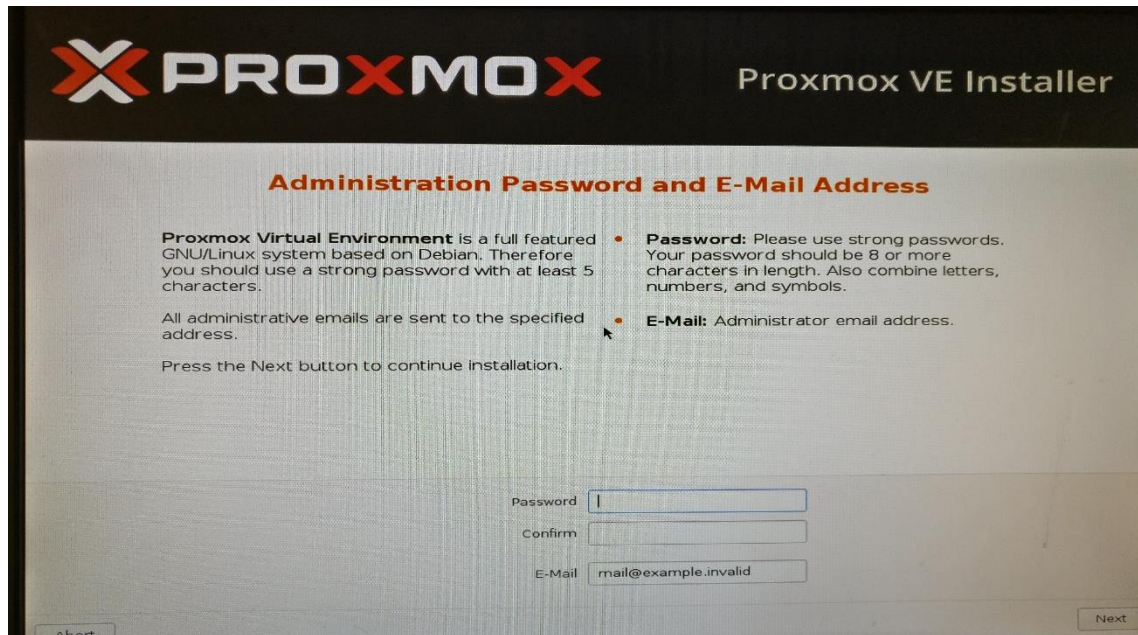
Seuraavana vuorossa on sijainnin ja aikavyöhykkeen määrittely (Kuvio 5). Tässä opinnäytetyössä käytetään suomalaisia asetuksia, joten maaksi syötetään Finland, minkä jälkeen asennusohjelmisto asettaa sekä aikavyöhykkeen että näppäimistöasettelun automaattisesti suomalaiseksi.



Kuvio 5. Sijainti ja aikavyöhyke

3.1.3 Pääkäyttäjän tiedot

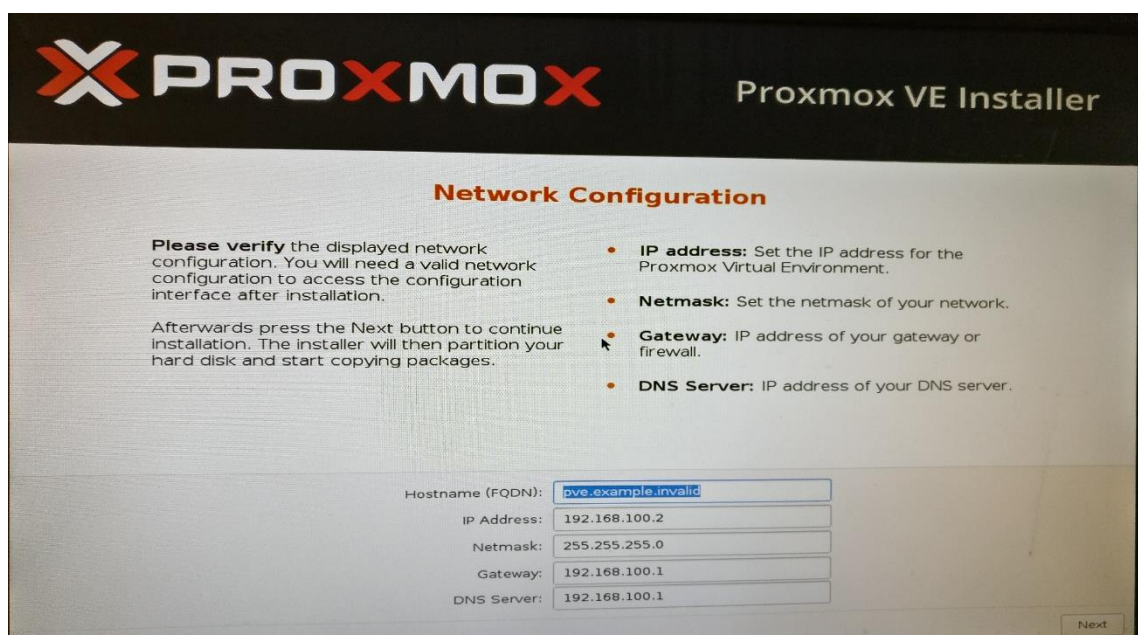
Sijaintiasetusten jälkeen asennusohjelmisto pyytää syöttämään pääkäyttäjän salasanan sekä sähköpostiosoitteen, jonne kaikki järjestelmän ylläpitoon liittyvät sähköpostit voidaan lähettää (Kuvio 6). Salasanan tulisi olla vähintään kahdeksan merkkiä pitkä, sisältäen kirjaimia, numeroita ja erikoismerkkejä.



Kuvio 6. Pääkäyttäjän salasana

3.1.4 Verkon määrittäminen

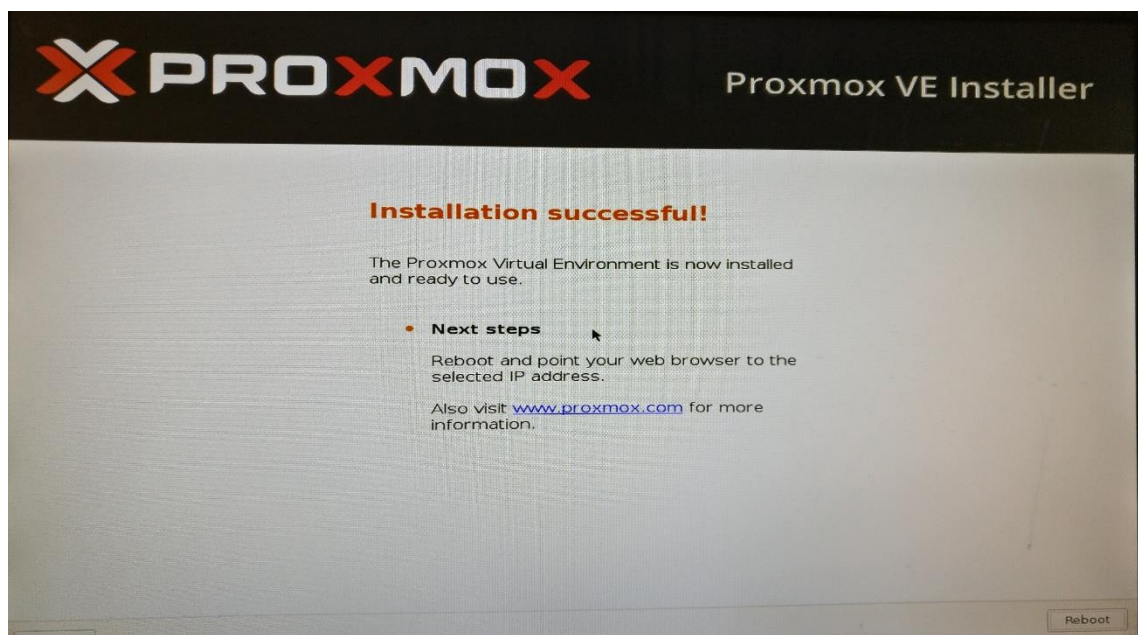
Verkon määrittämisen oletusarvoiset osoitetiedot eivät välttämättä sovi käytössä olevaan verkkoon, joten niiden kanssa tulee olla tarkkana (Kuvio 7). Tiedot voi muuttaa myös asennuksen jälkeen, mutta on yksinkertaisempaa laittaa ne heti oikein. On myös tärkeä tarkistaa "Hostname", eli virtualisointipalvelimen verkkonimi.



Kuvio 7. Verkoasetukset

3.1.5 Asennuksen päättäminen

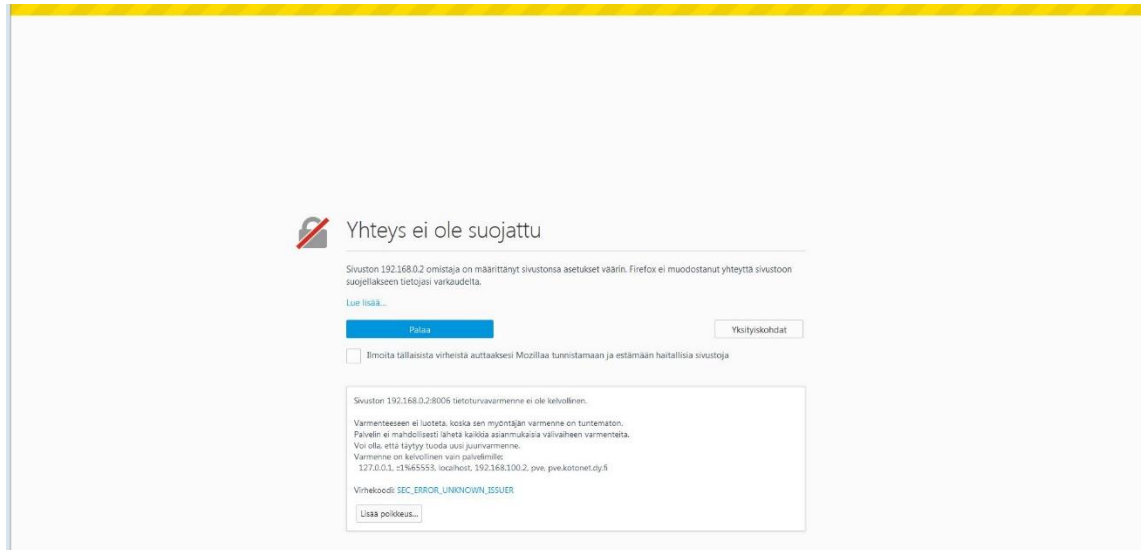
Verkkoasetusten hyväksymisen jälkeen asennusohjelmisto suorittaa järjestelmän varsinaisen asennuksen kiintolevyille. Asennuksen aikana näytöllä näkyy tietoja ja mainoksia Proxmoxin tarjoamista vaihtoehtoista sekä hallintaan että ylläpitoon. Kun asennus on suoritettu, asennusohjelmisto pyytää käynnistämään tietokoneen uudestaan ja kirjautumaan toiselta tietokoneelta aiemmin annettuun IP-osoitteeseen (Kuvio 8).



Kuvio 8. Uudelleenkäynnistys

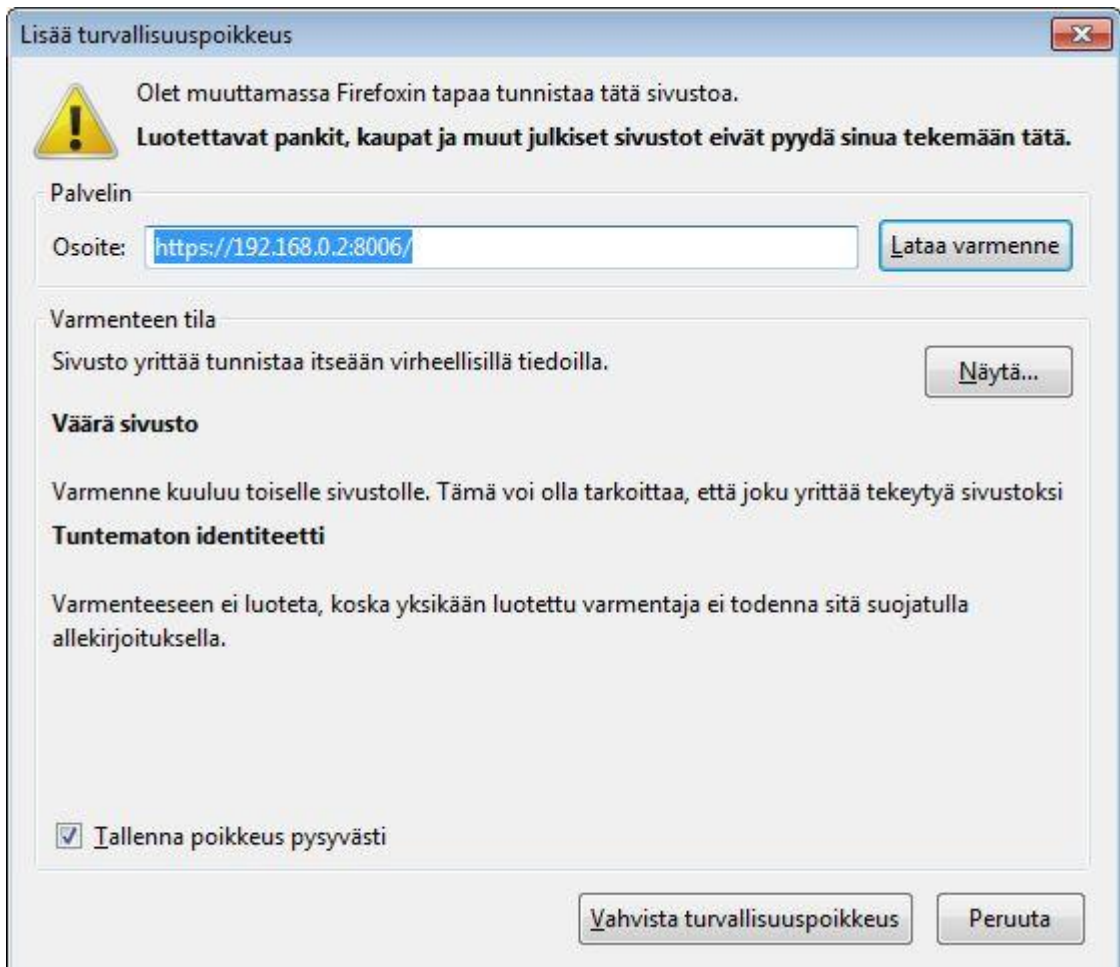
3.2 Kirjautuminen järjestelmään

Proxmox VE-järjestelmää hallitaan WWW-selaimella, esimerkiksi Mozilla Firefox tai Google Chrome. Selaimen osoiteriville syötetään osoitteeksi `https://192.168.100.2:8006`. IP-osoite korvataan asennuksen aikana syötetyllä osoitteella. Osoitteen perässä oleva `:8006` määrittelee portin, jota yhteys käyttää. Mikäli käytössä on palomuri, on siihen tehtävä aukko, jos järjestelmää halutaan ylläpitää sisäverkon ulkopuolelta. Koska varmennetta ei ole vielä käytössä, selain antaa varoituksen suojaamattomasta yhteydestä (Kuvio 9).



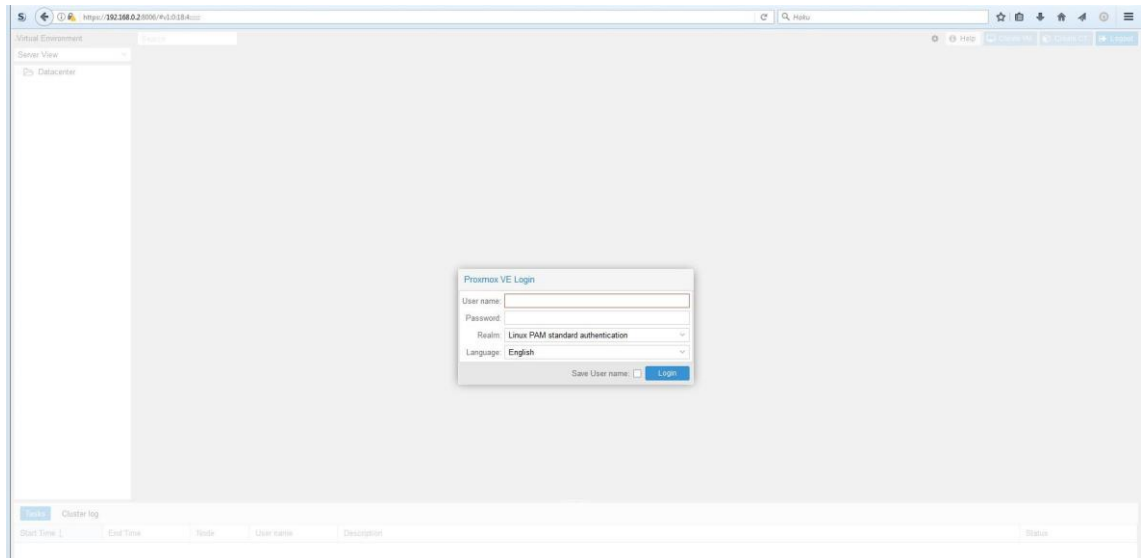
Kuvio 9. Varoitus suojaamattomasta yhteydestä

Valitsemalla ”Yksityiskohdat”, päästään lisäämään turvallisuuspoikkeus (Kuvio 10), jotta voidaan kirjautua sisälle. Myöhemmässä vaiheessa asennettava SSL-sertifikaatti mahdollistaa järjestelmän käytön ilman varoituksia.



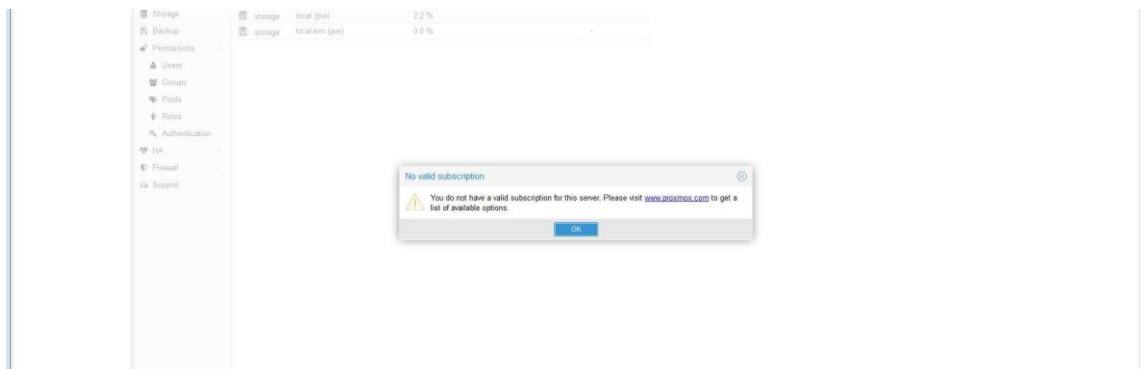
Kuvio 10. Turvallisuuspoikkeuksen lisääminen

Tässä vaiheessa on suositeltavaa tarkistaa palvelimen osoite. Valitsemalla ”Vahvista turvallisuuspoikkeus”, selain jatkaa kirjautumissivulle (Kuvio 11). Oletuskäyttäjätunnuksena on root ja salasanana asennuksen aikana syötetty salasana. Mikäli halutaan selaimen muistavan käyttäjätunnus tulevaisuudessa, voidaan laittaa rasti kohtaan ”Save User name”. Lopuksi valitaan ”Login”.



Kuvio 11. Sisäänkirjautuminen

Proxmox VE:lle on saatavilla maksullinen tukipalvelu, mutta peruskäytössä se ei ole välttämätön. Tukipalvelu mahdollistaa mm. automaattiset päivitykset järjestelmään, puhelintuen ja tämän ilmoituksen poistamisen kirjautumisen yhteydestä (Kuvio 12).



Kuvio 12. Ilmoitus maksullisen tukipalvelun puuttumisesta

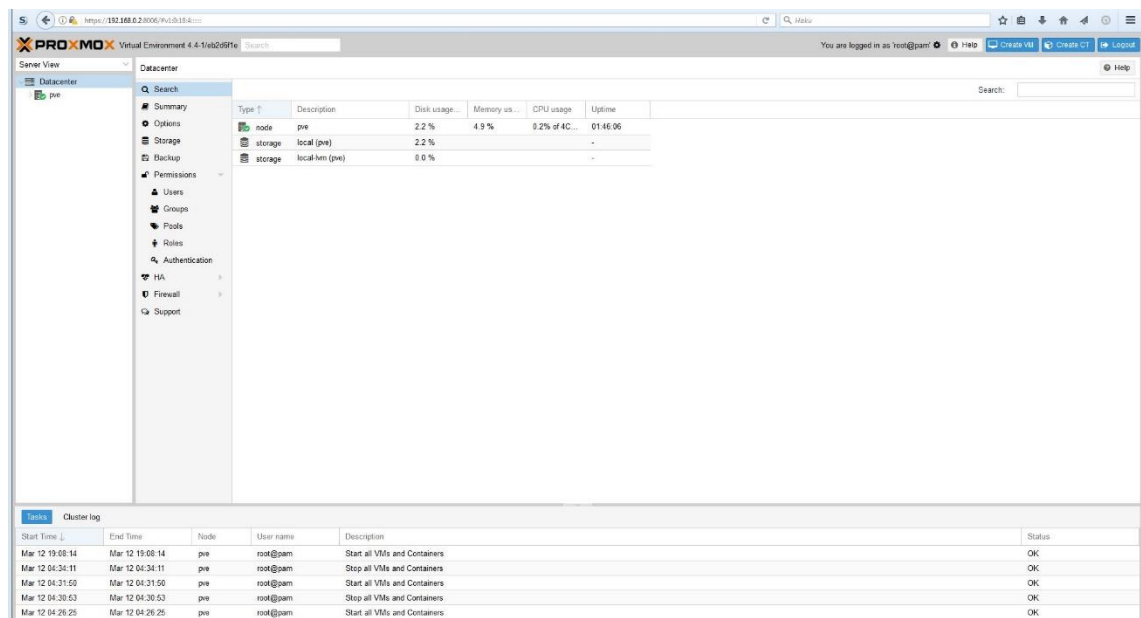
4 VIRTUAALIKONEIDEN HALLINTA

4.1 Uuden virtuaalikoneen lisääminen

Proxmox VE mahdollistaa valmiiden virtuaalikonepohjien käytön, mutta tällä hetkellä Nextcloudista ei valitettavasti ole sellaista saatavilla, joten asennus joudutaan suorittamaan useassa vaiheessa, joista ensimmäinen on virtuaalikoneen käyttöjärjestelmän asennus. Käyttöjärjestelmäksi valittiin Ubuntu 16.10 standard-jakelu johtuen sen hyvästä ohjelmistotuesta.

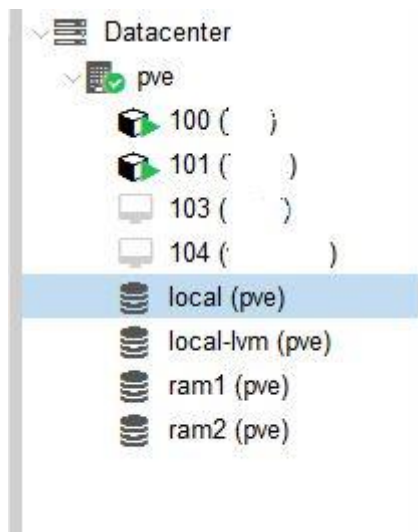
4.1.1 Aloitusnäky

Aloitusnäky (Kuvio 13) on oletusarvoinen näkymä sisäänkirjautumisen jälkeen. Tämän näkymän kautta pystytään hallitsemaan palvelimen resursseja ja virtuaalikoneita. Tätä kautta voidaan myös luoda laajempia kokonaisuuksia eli klustereita, joiden avulla yhdistetään useampia fyysisiä palvelimia esimerkiksi vi-kasietoisuuden varmistamiseksi.



Kuvio 13. Aloitusnäky

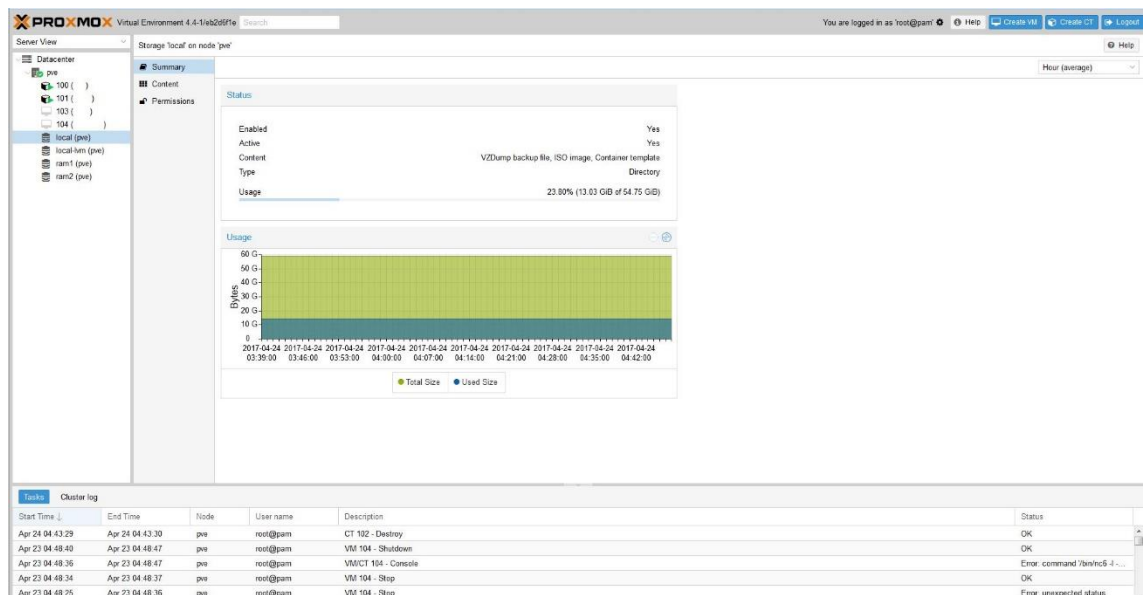
Klusterointi rajattiin opinnäytetyön ulkopuolelle, lisätietoa aiheesta löytyy Proxmox VE:n kotisivuilta. Opinnäytetyössä keskitytään pelkästään pve-nodeen eli käytössä olevaan palvelimeen ja sen käyttämään tallennustilaan (Kuvio 14).



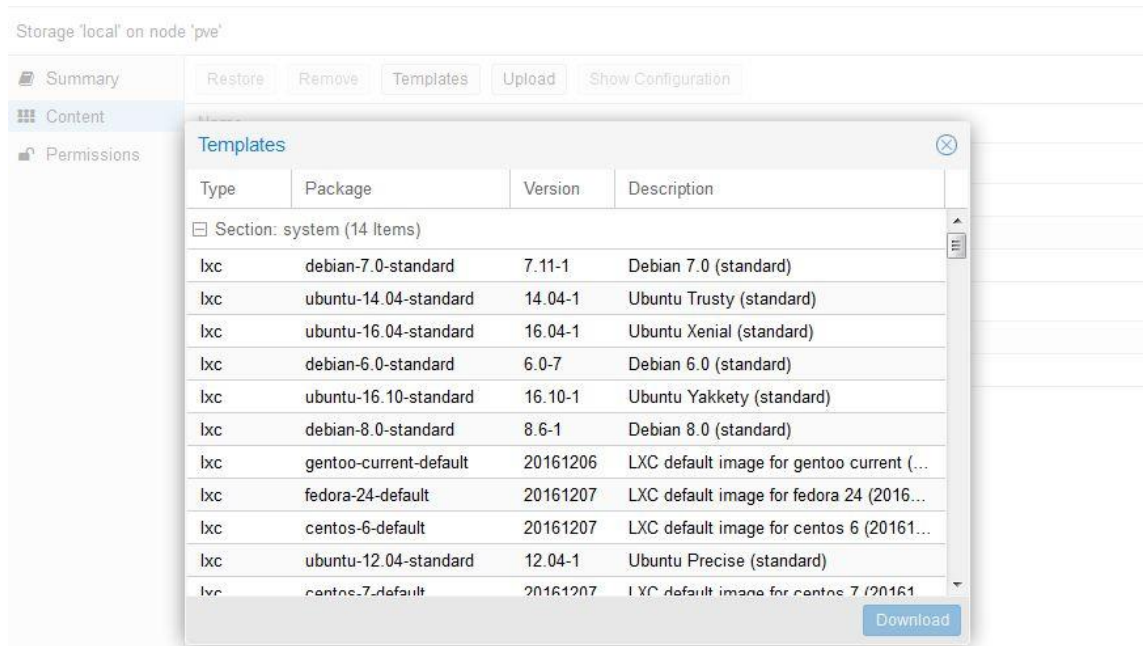
Kuvio 14. Palvelinlistaus

4.1.2 Levytila ja asennusmedian valinta

Ennen tallennustilan valintaa tarkistetaan käytettävissä oleva levytila. Tällä kertaa asennus suoritetaan palvelimen päälevylle, jossa on käytössä tarvittava määrä tyhjää tilaa (Kuvio 15). Ennen asentamista tarvitaan myös asennusmedian, jonka voi ladata joko netistä tai koneelta jolla ollaan yhteydessä palvelimeen. Koska Proxmox VE tukee valittua käyttöjärjestelmää suoraan, voi tarvittavan levykuvan ladata suoraan palvelimelle. Siirrytään valikossa kohtaan "Content" ja sieltä valitaan "Templates", jolloin saadaan esille lista palvelimen tukevista levykuvista (Kuvio 16).



Kuvio 15. Palvelimen levytila



Kuvio 16. Tuetut levykuvat

Listasta valitaan ”ubuntu-16.04-standard_16.04-1_amd64.tar.gz” ja klikataan linkkiä ”Download”. Palvelin lataa itsellensä levykuvan netistä, käytettävä aika riippuu palvelimen nettiyhteyden nopeudesta.

4.1.3 Virtuaalikoneen luominen ja käynnistyslevyn valinta

Levykuvan lataamisen jälkeen valitaan oikealta ylhäältä ”Create CT”-linkki, jolla käynnistetään LXC-asennus. Ensimmäisenä määritellään perustiedot (Kuvio 17), joista tärkeimpiä ovat palvelimen nimi (”Hostname”) ja pääkäyttäjän salasana (”Password”). Salasana annetaan kahteen kertaan, jotta kirjoitusvirheiden mahdollisuus olisi pienempi.

Create: LXC Container

General Template Root Disk CPU Memory Network DNS Confirm

Node: pve Resource Pool:

VM ID: 102 Password:

Hostname: nextcloud Confirm password:

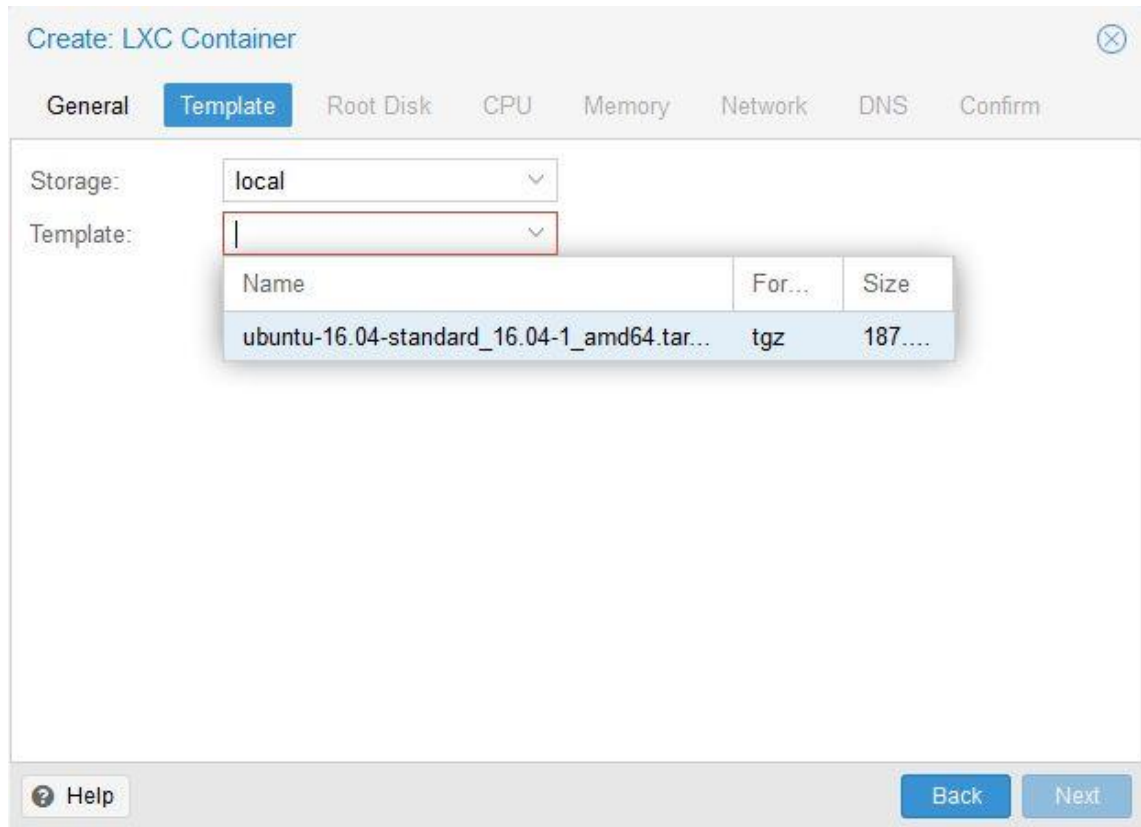
Unprivileged container: SSH public key:

Load SSH Key File

Help Back Next

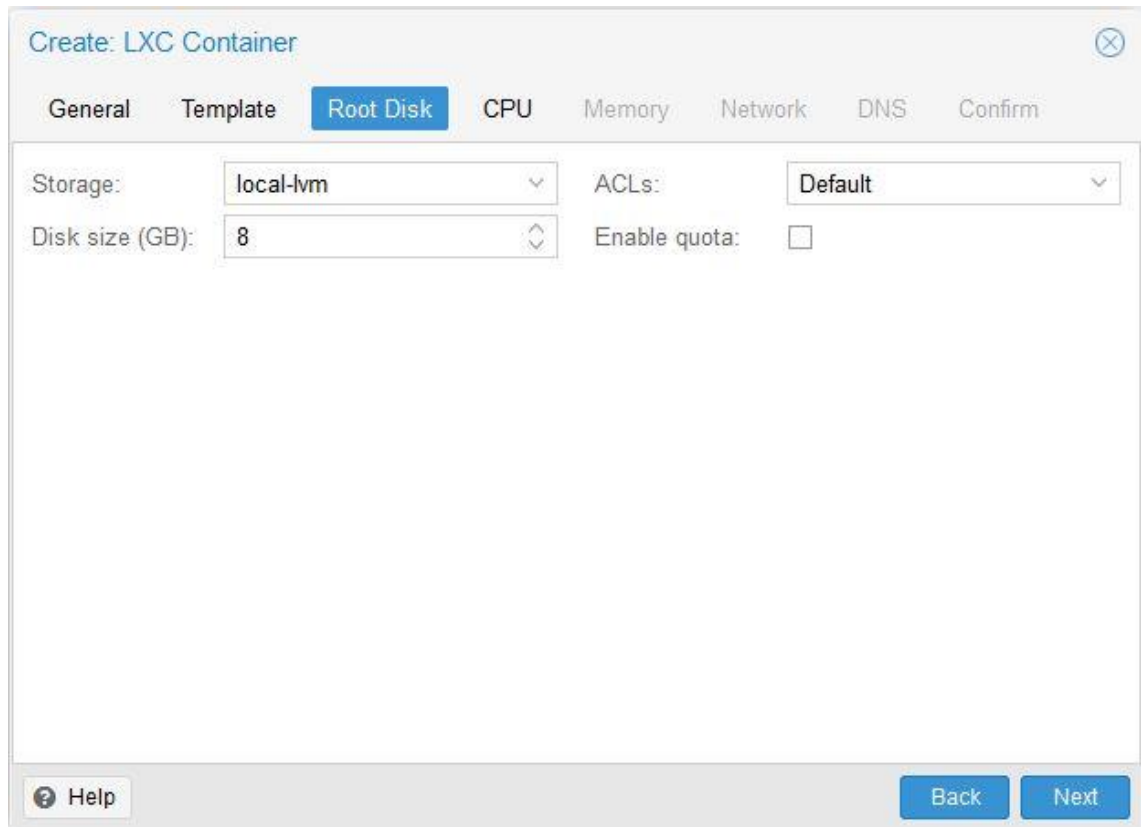
Kuvio 17. LXC asennuksen perustiedot

Perustietojen jälkeen valitaan asennuksessa käytettävä levykuva (Kuvio 18). Koska levykuvia voidaan ladata eri levyjärjestelmiin, tässä on mahdollisuus vaihtaa myös levyjärjestelmää.



Kuvio 18. LXC asennuksen levykuvan valinta

Käyttöjärjestelmälevy on tärkein resurssi (Kuvio 19). Tässä on mahdollista jälleen valita käytettävä levyjärjestelmä, käyttöoikeudet (ACL, Access Control Lists) ja järjestelmälevyn koko. Kahdeksan gigatavua on alkuvaiheessa riittävä, käytettävissä olevan levytilan mukaan määrää voi kasvattaa haluamukseen, mutta käytettävä järjestelmä mahtuu hyvin oletuskokoonkin.



The image shows a window titled "Create: LXC Container" with a close button in the top right corner. Below the title bar are several tabs: "General", "Template", "Root Disk" (which is selected and highlighted in blue), "CPU", "Memory", "Network", "DNS", and "Confirm". The "Root Disk" tab contains the following settings:

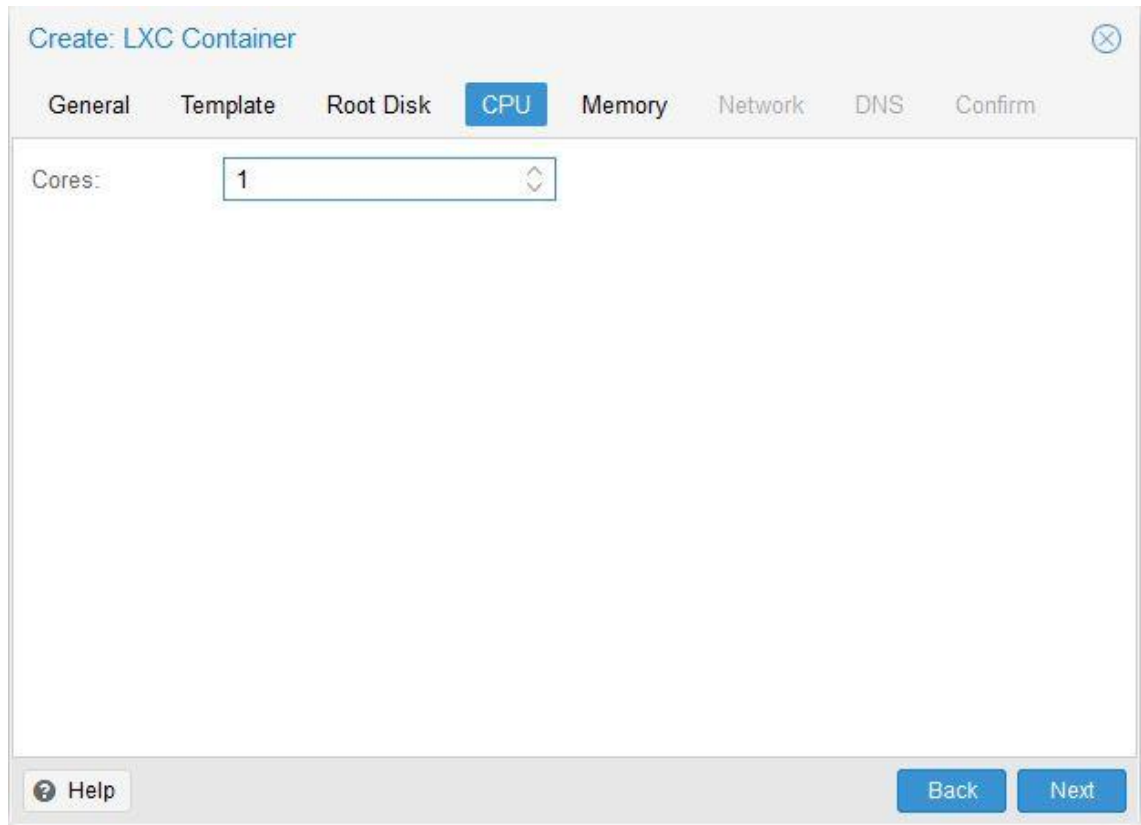
- Storage: local-lvm (dropdown menu)
- ACLs: Default (dropdown menu)
- Disk size (GB): 8 (spin button)
- Enable quota:

At the bottom left, there is a "Help" button with a question mark icon. At the bottom right, there are "Back" and "Next" buttons.

Kuvio 19. LXC asennuksen järjestelmälevyn asetukset

4.1.4 Suorittimet ja keskusmuisti

Suorittimien määrä on verrannollinen käyttäjien ja liikuteltavan datan määrään (Kuvio 20). Pitää myös huomioida fyysisen palvelimen ominaisuudet, etenkin jos asennetaan muitakin virtuaalikoneita. Yhden käyttäjän tarpeisiin yksi suoritinydin on riittävä. Suoritinydinten määrää voi muuttaa myöhemmässä vaiheessa tarpeen mukaan.



Kuvio 20. LXC asennuksen prosessorin asetukset

Yleisellä tasolla voidaan todeta, että käytössä oleva keskusmuisti vaikuttaa eniten koneen nopeuteen (Kuvio 21). Pitää ottaa kuitenkin huomioon palvelimen fyysinen muisti ja sitä käyttävien virtuaalikoneiden määrä. Opinnäytetyön tarkoitukseen riittää tässä vaiheessa 1024 megatavua ja heittovaihtomuistiksi (swap) 512 megatavua. Näitä arvoja on mahdollista muuttaa myöhemmin tarpeen mukaan.

The image shows a window titled "Create: LXC Container" with a close button in the top right corner. Below the title bar is a navigation bar with tabs: "General", "Template", "Root Disk", "CPU", "Memory" (which is highlighted in blue), "Network", "DNS", and "Confirm". The main area contains two input fields: "Memory (MB):" with the value "1024" and "Swap (MB):" with the value "512". At the bottom left is a "Help" button with a question mark icon. At the bottom right are "Back" and "Next" buttons.

Kuvio 21. LXC asennuksen muistin määrittely

4.1.5 Verkon määrittely

Verkko on tärkeä palvelimen saatavuuden vuoksi, joten tähän kohtaan kannattaa paneutua hieman (Kuvio 22). Normaalisissa pienverkossa oletusarvot kelpaavat muissa kohdissa, mutta IPv4-osion kanssa pitää olla tarkkana. Kohdassa "IPv4/CIDR" määritetään sekä virtuaalikoneen oma IP-osoite, että lähiverkon peite. Näiden avulla pystytään sekä saavuttamaan palvelin, että ohjaamaan ulkoverkkoon menevät pyynnöt oikeaan osoitteeseen (Classless Inter-Domain Routing 2017). Mikäli lähiverkossa on käytössä DHCP antamassa tietokoneille automaattisesti IP-osoitteet, on valittava virtuaalipalvelimelle osoite DHCP:n käyttämän alueen ulkopuolelta, ettei verkkoon tule päällekkäisiä osoitteita. IP-osoitteen jälkeen tuleva "/24" määrittelee lähiverkon käyttämän verkon peittomaskin, jolla selvitetään, kuuluuko osoite lähiverkkoon vai ulkoverkkoon. Esimerkissä on käytössä normaalit oletusarvot kotikäytössä, käytettävät asetukset voi tarkistaa verkon ylläpitäjältä tai toisesta tietokoneesta. "/24" vastaa netmask-arvoa "255.255.255.0"

Create: LXC Container ✕

General Template Root Disk CPU Memory **Network** DNS Confirm

Name (i.e. eth0): IPv4: Static DHCP

MAC address: IPv4/CIDR:

Bridge: Gateway (IPv4):

VLAN Tag: IPv6: Static DHCP SLAAC

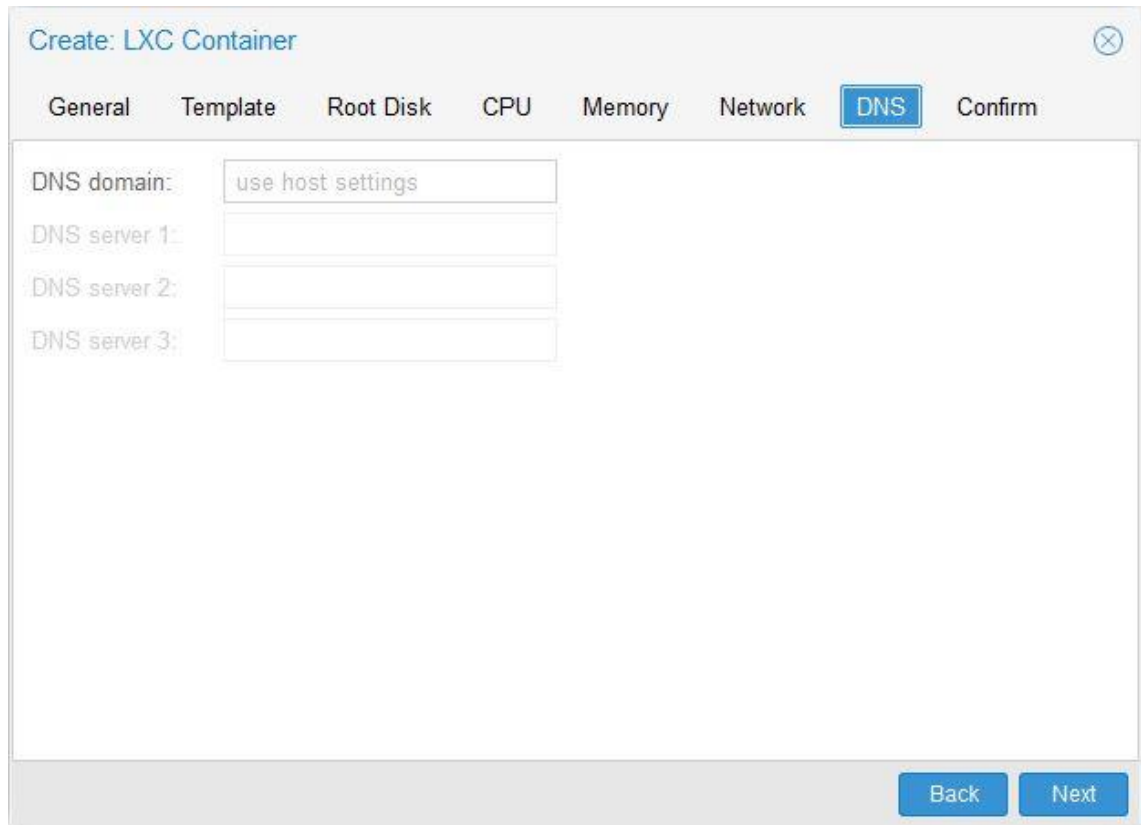
Rate limit (MB/s): IPv6/CIDR:

Firewall: Gateway (IPv6):

Kuvio 22. LXC asennuksen verkkomäärittelyt

Toinen tärkeä arvo on "Gateway", joka kertoo järjestelmälle ulkoverkkoon kohdistuvien yhteyksien reitittimen osoitteen. Tämä yleensä on palomuurin/modeemin osoite.

DNS-asetus (Kuvio 23) otetaan oletuksena automaattisesti asetuksista, joten mikäli ei halua käyttää jotain erikoisempaa palvelua, kuten Googlen nimipalvelua (8.8.8.8), tähän asetukseen ei tarvitse koskea.



Create: LXC Container

General Template Root Disk CPU Memory Network **DNS** Confirm

DNS domain: use host settings

DNS server 1:

DNS server 2:

DNS server 3:

Back Next

Kuvio 23. LXC asennuksen nimipalvelun määrittely

4.1.6 Tarkistus ja hyväksyntä

Kun perusasetukset on saatu kohdalleen, tarkistetaan vielä yhteenveto (Kuvio 24) ja hyväksytään kokoonpano. Painamalla "Finish" aloitetaan virtuaalikoneen luominen.

Create: LXC Container ✕

General Template Root Disk CPU Memory Network **DNS** **Confirm**

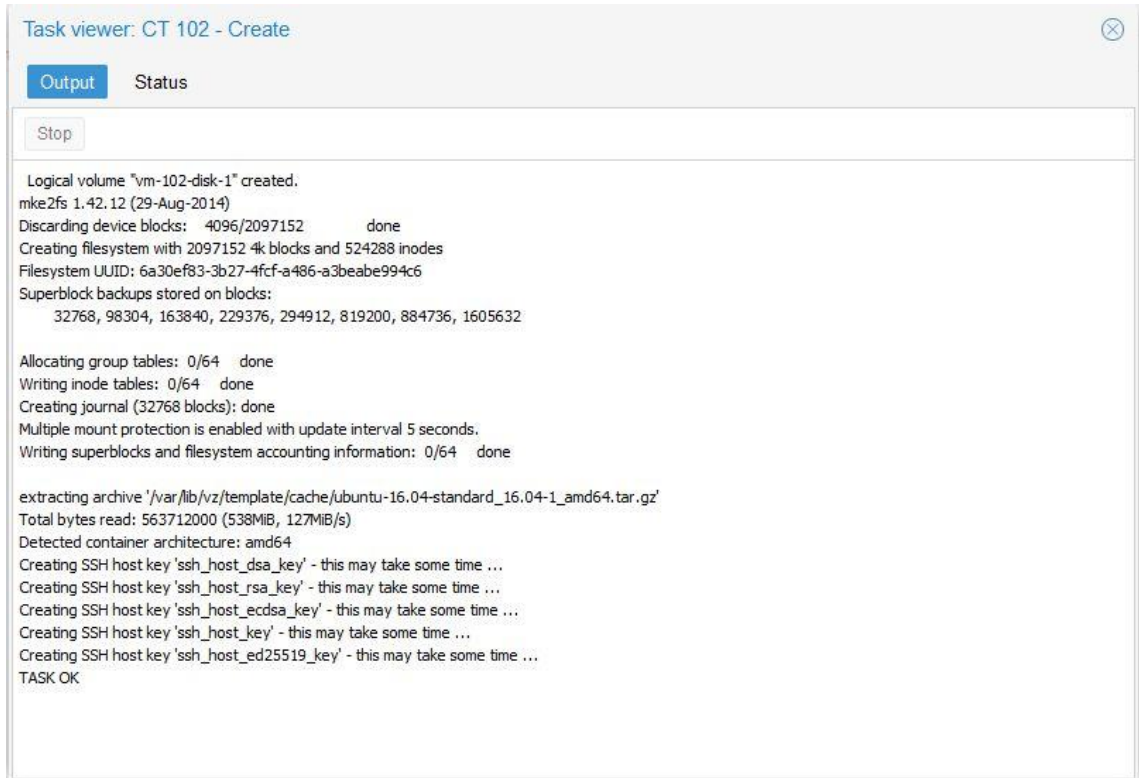
Settings

Key ↑	Value
cores	1
hostname	nextcloud
memory	1024
net0	bridge=vibr0,name=eth0,ip=192.168.0.99/24,gw=192.168.0.1
nodename	pve
ostemplate	local:vztmpl/ubuntu-16.04-standard_16.04-1_amd64.tar.gz
rootfs	local-lvm:8
swap	512
vmid	102

Back **Finish**

Kuvio 24. LXC asennuksen yhteenveto ja hyväksyntä

Virtuaalikoneen luomisessa menee hetki, lähinnä riippuen levytilan käytöstä. Loki (Kuvio 25) kannattaa lukea läpi, jotta mahdolliset ongelmatilanteet tulevat huomi-
oitua. Muussa tapauksessa ikkunan voi sulkea oikean yläkulman rastista.



```

Task viewer: CT 102 - Create

Output Status

Stop

Logical volume "vm-102-disk-1" created.
mke2fs 1.42.12 (29-Aug-2014)
Discarding device blocks: 4096/2097152 done
Creating filesystem with 2097152 4k blocks and 524288 inodes
Filesystem UUID: 6a30ef83-3b27-4fcf-a486-a3beabe994c6
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: 0/64 done
Writing inode tables: 0/64 done
Creating journal (32768 blocks): done
Multiple mount protection is enabled with update interval 5 seconds.
Writing superblocks and filesystem accounting information: 0/64 done

extracting archive '/var/lib/vz/template/cache/ubuntu-16.04-standard_16.04-1_amd64.tar.gz'
Total bytes read: 563712000 (538MiB, 127MiB/s)
Detected container architecture: amd64
Creating SSH host key 'ssh_host_dsa_key' - this may take some time ...
Creating SSH host key 'ssh_host_rsa_key' - this may take some time ...
Creating SSH host key 'ssh_host_ecdsa_key' - this may take some time ...
Creating SSH host key 'ssh_host_key' - this may take some time ...
Creating SSH host key 'ssh_host_ed25519_key' - this may take some time ...
TASK OK

```

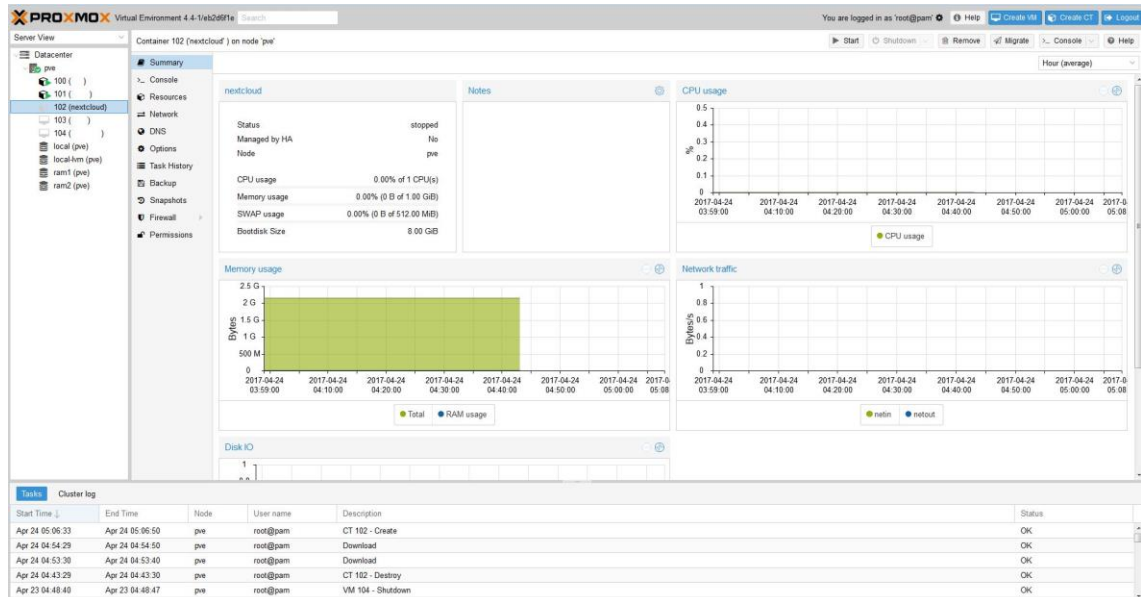
Kuvio 25. LXC asennuksen valmistuminen

4.2 Käyttöjärjestelmän asennus

Tähän mennessä on luotu virtuaalikone ja tehty siihen käyttöjärjestelmän perusasennus. Jakelupaketin julkaisemisen jälkeen on kuitenkin usein tullut päivityksiä sekä toiminnallisuuteen että tietoturvaan. Koska palvelinkäytössä olevalla koneella ei kannata suorittaa mitään tarpeettomia koneen resursseja käyttäviä ohjelmistoja, emme asenna graafista käyttöliittymää vaan käytämme komentoriviä. Komentojen kanssa tulee olla tarkkana, koska virheitä voi olla vaikea jäljittää, jos ei ole tottunut Linux-käyttäjä eikä komentorivi ole entuudestaan tuttu.

4.2.1 Virtuaalikoneen käynnistäminen

Virtuaalikone käynnistetään valitsemalla yläriviltä oikealta "Start" (Kuvio 26). Vasemmasta reunasta valitaan ">_ Console", jolla päästään käsiksi konsoliin. Kirjautuminen tapahtuu käyttäjätunnuksella "root" ja aiemmin asennuksessa annettulla salasanalla. Kirjautumisen jälkeen päästään virtuaalikoneen komentoriville (Kuvio 27).



Kuvio 26. LXC virtuaalikoneen yhteenveto asennuksen jälkeen

```

Connected to tty 1
Type <Ctrl+a q> to exit the console, <Ctrl+a Ctrl+a> to enter Ctrl+a itself

Ubuntu 16.04 LTS nextcloud pts/0
nextcloud login: root
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.35-1-pve x86_64)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@nextcloud:~#

```

Kuvio 27. Virtuaalikoneen konsoliyhteys

4.2.2 Käyttäjätunnukset ja oikeudet

Koska pääkäyttäjällä (root) on koneeseen kaikki oikeudet ilman kyselyitä, on tietoturvan vuoksi ensimmäinen tehtävä luoda peruskäyttäjä, jolla on oikeudet suorittaa komentoja pääkäyttäjän oikeuksilla (Linux Users and Groups 2017). Tätä varten suoritetaan komento **adduser clouduser** joka luo tunnuksen **clouduser** (Kuvio 28). Komento pyytää käyttäjälle salasanan joka annetaan kahdesti, sekä

muita perustietoja kuten käyttäjän nimen ja puhelinnumeron, jotka voi jättää tyhjäksi.

```

root@nextcloud:~# adduser clouduser
Adding user `clouduser' ...
Adding new group `clouduser' (1000) ...
Adding new user `clouduser' (1000) with group `clouduser' ...
Creating home directory `/home/clouduser' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for clouduser
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
root@nextcloud:~#

```

Kuvio 28. adduser-komento

Jotta pääkäyttäjän oikeuksilla voitaisiin suorittaa komentoja, lisätään käyttäjätunnus sudoers-listaan komennolla **visudo** (Kuvio 29) (Linux Users and Groups 2017). Ubuntu käyttää oletuksen **nano**-editoria, jossa poistuminen tapahtuu CTRL-X-näppäinyhdistelmällä, jonka jälkeen editori kysyy, tallennetaanko ja mihin tiedostoon.

```

GNU nano 2.5.3      File: /etc/sudoers.tmp      Modified
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
clouduser ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL
# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "#include" directives:
#include_dir /etc/sudoers.d
^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text      ^J Justify      ^C Cur Pos
^X Exit          ^R Read File    ^_ Replace      ^U Uncut Text   ^I To Spell     ^_ Go To Line

```

Kuvio 29. visudo-komento

Tallennuksen jälkeen on suositeltavaa vaihtaa käyttäjätunnusta, eli kirjaudutaan pääkäyttäjän tunnukselta pois komennolla **logout** ja sen jälkeen kirjaudutaan sisälle juuri luodulla tunnuksella ja salasanalla. Pääkäyttäjän oikeuksia vaativien

komentojen eteen annetaan komento **sudo**, jonka jälkeen järjestelmä kysyy käyttäjän salasanaa varmistaakseen, ettei kukaan asiaton ole käyttämässä yhteyttä.

4.2.3 Ohjelmiston päivitys

Varmistaaksemme tietoturvan tason ja että käytössä on tuoreimmat versiot järjestelmäohjelmista, käytetään komentoja **sudo apt-get update**, joka hakee viimeisimmät päivitystiedot, sekä **sudo apt-get upgrade**, joka suorittaa varsinaisen päivityksen. Järjestelmä ilmoittaa päivitettävien pakettien määrän, mahdollisen tarvittavan levytilan ja kysyy varmistuksen päivityksen suorittamiseen. Riippuen nettiyhteyden nopeudesta, päivitykseen menee muutama minuutti. Tämän jälkeen virtuaalikoneen käyttöjärjestelmä on ajan tasalla.

5 NEXTCLOUDIN ASENTAMINEN

Nextcloud vaatii tiettyjä perusohjelmia toimiakseen, tärkeimpänä LAMP-paketti (What is LAMP (Linux, Apache, MySQL, PHP)? - Definition from WhatIs.com 2008). Linux on jo asennettu, tarvitaan vielä Apache-sivupalvelin, MariaDB-tietokantapalvelin sekä PHP-skriptikielen tuki. Tässä vaiheessa on hyvä tutustua Nextcloudin palvelimen ylläpitäjän käsikirjaan ainakin pääpiirteittäin (Nextcloud 11 Server Administration Manual 2016). Käsikirjasta löytyy selkeät ohjeet Ubuntu 16.04-jakelua varten, sekä tarkemmat järjestelmävaatimukset (Manual Installation on Linux – Nextcloud 11 Server Administration manual 2016). Tämä käsikirja kannattaa pitää muistissa tulevaisuuden varalta, mikäli aikoo viritellä ja laajentaa asennusta.

Koska käsikirja käy asennuksen yksityiskohtaisesti läpi, tässä opinnäytetyössä ei paneuduta komentojen vaikutuksiin tarkemmin, käydään vain läpi komennot suoritussjärjestyksessä. Ainoa muutos ohjeisiin on itse Nextcloudin ohjelmistopakettin lataus, jossa käytetään komentorivipohjaista metodia, sekä tiedoston tarkistussumman laskemisen poisjättäminen. Tarkistussumman voi halutessaan laskea käsikirjassa olevan ohjeen avulla. Huomioitavaa on, että ladattu tiedosto on nimeltään `latest.tar.bz2`, joka on viimeisin julkaistu versio, joten versionumeroinnista ei tarvitse huolehtia (Kuvio 30).

```
sudo apt-get install apache2 mariadb-server libapache2-mod-php7.0
sudo apt-get install php7.0-gd php7.0-json php7.0-mysql php7.0-curl php7.0-mbstring
sudo apt-get install php7.0-intl php7.0-mcrypt php-imagick php7.0-xml php7.0-zip
wget https://download.nextcloud.com/server/releases/latest.tar.bz2
tar -xjf latest.tar.bz2
sudo cp -r nextcloud /var/www
```

Kuvio 30. Nextcloudin asennus komentoriviltä

Seuraavana luodaan Apachelle säännöt joiden perusteella se löytää Nextcloudin. Tätä varten luodaan uusi tiedosto komennolla **sudo nano /etc/apache2/sites-available/nextcloud.conf** ja syötetään sinne käsikirjassa olevat rivit. Mikäli Nextcloudi on asennettu johonkin muuhun hakemistoon, muokataan rivejä sen mukaan (Kuvio 31).

```

GNU nano 2.5.3      File: /etc/apache2/sites-available/nextcloud.conf
Alias /nextcloud "/var/www/nextcloud/"
<Directory /var/www/nextcloud/>
  Options +FollowSymLinks
  AllowOverride All
  <IfModule mod_dav.c>
    Dav off
  </IfModule>
  SetEnv HOME /var/www/nextcloud
  SetEnv HTTP_HOME /var/www/nextcloud
</Directory>

[ Read 11 lines ]
G Get Help      O Write Out    W Where Is     K Cut Text     J Justify      C Cur Pos
X Exit          R Read File    _ Replace      U Uncut Text   T To Spell    _ Go To Line

```

Kuvio 31. Apachen asetukset

Tämän jälkeen linkitetään luotu tiedosto Apachen käynnistettäviin sivustoihin ja aktivoidaan erinäisiä tarpeellisia Apachen moduleja (Kuvio 32).

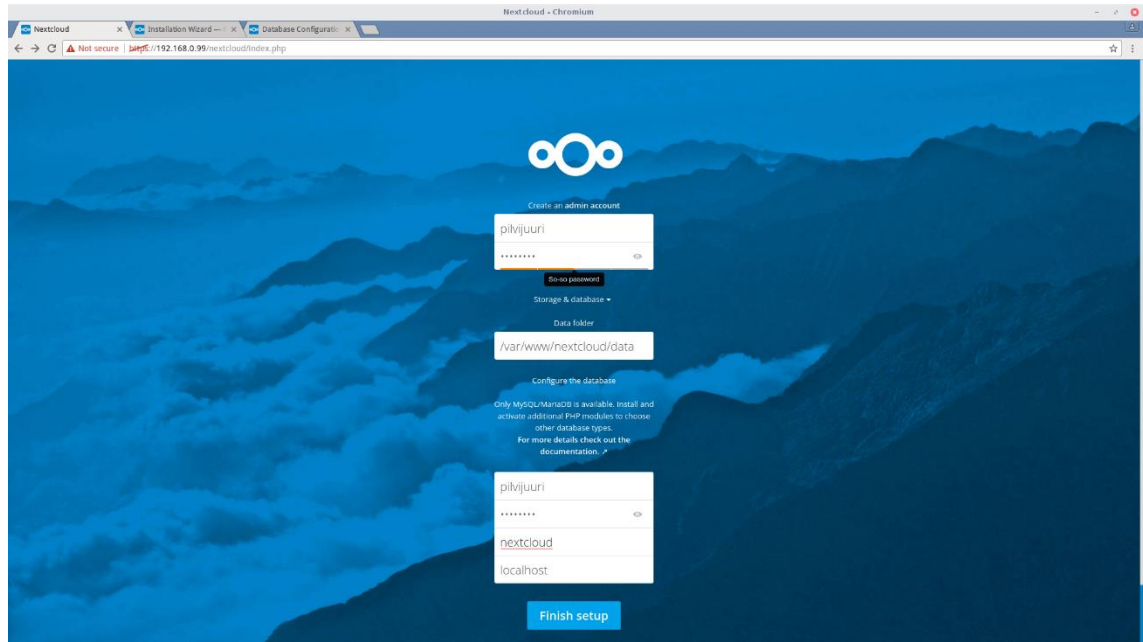
```

sudo ln -s /etc/apache2/sites-available/nextcloud.conf /etc/apache2/sites-enabled/nextcloud.conf
sudo a2enmod rewrite
sudo a2enmod headers
sudo a2enmod env
sudo a2enmod dir
sudo a2enmod mime
sudo service apache2 restart
sudo a2enmod ssl
sudo a2ensite default-ssl
sudo service apache2 reload

```

Kuvio 32. Apachen moduulit

MySQL-tietokanta vaatii myös oman käyttäjätunnuksensa ja tietokannan, jota käytetään Nextcloudissa (Kuvio 33). Käsikirjasta löytyy selkeät ohjeet ja taustatiedot, samoin kuin tuetut tietokantapalvelimet (Database Configuration – Nextcloud 11 Server Administration manual 2016). Tässä opinnäytetyössä käytetään MariaDB-tietokantapalvelinta, joka on yhteensopiva MySQL-palvelimen kanssa.



Kuvio 33. Käyttäjätunnusten luonti

6 LISÄPALVELUT

6.1 Nimipalvelu

Internetin yksi hyödyllisimmistä palveluista on nimipalvelu (DNS, Domain Name Service), joka mahdollistaa selkokielisemmän osoitteen tietokoneille. Ilman tätä palvelua jouduttaisiin käyttämään numeropohjaisia osoitteita, kuten 173.194.222.94 sen sijaan että kirjoitetaan selaimen google.fi. DNS-palvelua tarjoaa moni taho, ja kuten sertifikaattien kanssa, suurin osa on maksullisia. Tähän opinnäytetyöhön on valittu suomalainen DY.fi-palvelu (DY.fi 2017), joka tarjoaa suomalaisille IP-osoitteille ilmaisen DNS-palvelun. Mikäli käytössä on ulkomailla sijaitseva palvelin, joudutaan käyttämään jotain toista palveluntarjoajaa.

DY.fi-palvelu vaatii rekisteröinnin käyttäen sähköpostiosoitetta ja salasanaa. Palveluun voi rekisteröidä viisi domainia loppupääteillä dy.fi tai tunk.org. Muidenkin domainien käyttö on mahdollista, mutta ne pitää rekisteröidä domain-päätteen omistavan organisaation kautta ja sitten ilmoittaa DY.fi-palveluun. Kannattaa myös huomata, että oletusarvoisesti palvelun domainit ovat julkisia, joten mikäli osoitetta ei tahdota ulkopuolisten saataville liian helposti, kannattaa ottaa rasti pois ruudusta nimeä varatessa. Myös kiinteän IP-osoitteen ja sähköpostin ohjauksen käyttö on mahdollista.

DY.fi-osoitteet vanhenevat seitsemän päivän kuluttua, joten ne pitää uusia ennen ajan täyttymistä. Käyttämättömänä olleet osoitteet poistetaan tietokannasta 30 päivän jälkeen ja 60 päivän jälkeen käyttäjätunnus poistetaan. Lisätietoja palvelun **FAQ**-sivulla. Käsien uusiminen on aina oma vaivansa, vaikkakin melko nopeaa, mutta se täytyy suorittaa samasta liittymästä, jonka IP-osoite on palvelimen osoite, joten reissun päältä päivitys ei onnistu. Tätä varten on olemassa asiakasohjelmia jotka suorittavat päivityksen automaattisesti haluttuna aikana. Lisätietoja DY.fi-sivuston kohdasta **päivitysohjelmat**.

6.2 SSL-sertifikaatti

Verkkopohjaisissa palveluissa tietoturvallisuuden kannalta tärkeä asia on vasta puolen tunnistaminen luotettavaksi. Tätä tarkoitusta varten on kehitetty ssl-sertifikaatit (Verisign, Inc 2016), joita on useita eri tyyppisiä. Sertifikaatti myös mahdollistaa salatun turvallisen yhteyden muodostamisen asiakaskoneen ja palvelimen välille. Tämä on tärkeää, kun käsitellään arkaluontoisia ja/tai henkilökohtaisia tietoja. Sertifikaatteja myöntävät useat eri tahot, joista suurin osa perii maksun. Tähän opinnäytetyöhön valittiin ilmainen palveluntarjoaja Let's Encrypt (Let's Encrypt 2017) ja Single Domain Validation-tason sertifikaatti.

Let's Encrypt suosittelee käytettäväksi Certbot ACME-asiakasohjelmaa (Certbot 2017). Certbot ohjaa kädestä pitäen sertifikaatin luomisen, kun pääsivulla valitaan käytettävä ohjelmisto (Apache) ja käyttöjärjestelmä (Ubuntu 16.04 xenial). Certbot kysyy ensimmäistä kertaa ajettaessa sähköpostiosoitteen mahdollisia ilmoituksia varten, lupaa liittyä EFF-organisaation sähköpostilistalle sekä sivuston osoitetta. Asennus kysyy, halutaanko käyttää sekä salaamatonta että salattua yhteyttä vai ohjataanko kaikki palvelimelle tulevat pyynnöt salattuun yhteyteen. Koska Nextcloud käsittelee henkilökohtaisia tietoja, ei ole järkevää antaa mahdollisuutta salaamattomaan yhteyteen. Hyväksymisen jälkeen asennusohjelma luo sertifikaatin ja ottaa sen käyttöön. Ohjelma myös antaa linkin, jonka kautta voi tarkistaa sertifikaatin toimivuuden.

7 TYÖPÖYTÄ- JA MATKAPUHELINSOVELLUKSEN ASENTAMINEN

7.1 Työpöytäsovellukset

Nextcloudilla on asiakasohjelmat tietokonekäyttöä varten niin Windowsille, Macille kuin Linuxille. Ohjelma mahdollistaa tietojen synkronoinnin palvelimen ja tietokoneen välillä lähes reaaliajassa, nettiyhteyden nopeudesta riippuen. Asiakasohjelman voi ladata Nextcloudin kotisivuilta.

Ohjelman asennus on hyvin yksinkertaista, asennusohjelmalle syötetään palvelimen osoite ja käyttäjätunnus salasanoineen, synkronoidaanko kaikki palvelimen tiedostot vai vain osa, sekä mitä paikallista hakemistoa käytetään synkronointiin. Tämän jälkeen voidaan halutessa ottaa yhteys palvelimeen selaimella tai avata paikallinen kansio. On otettava huomioon, että ensimmäisellä kerralla tai jos edellisestä synkronoinnista on kulunut pidemmän aikaa ja palvelimelle on tallennettu suurempia määriä tietoja, synkronointi kestää oman aikansa.

7.2 Matkapuhelinsovellukset

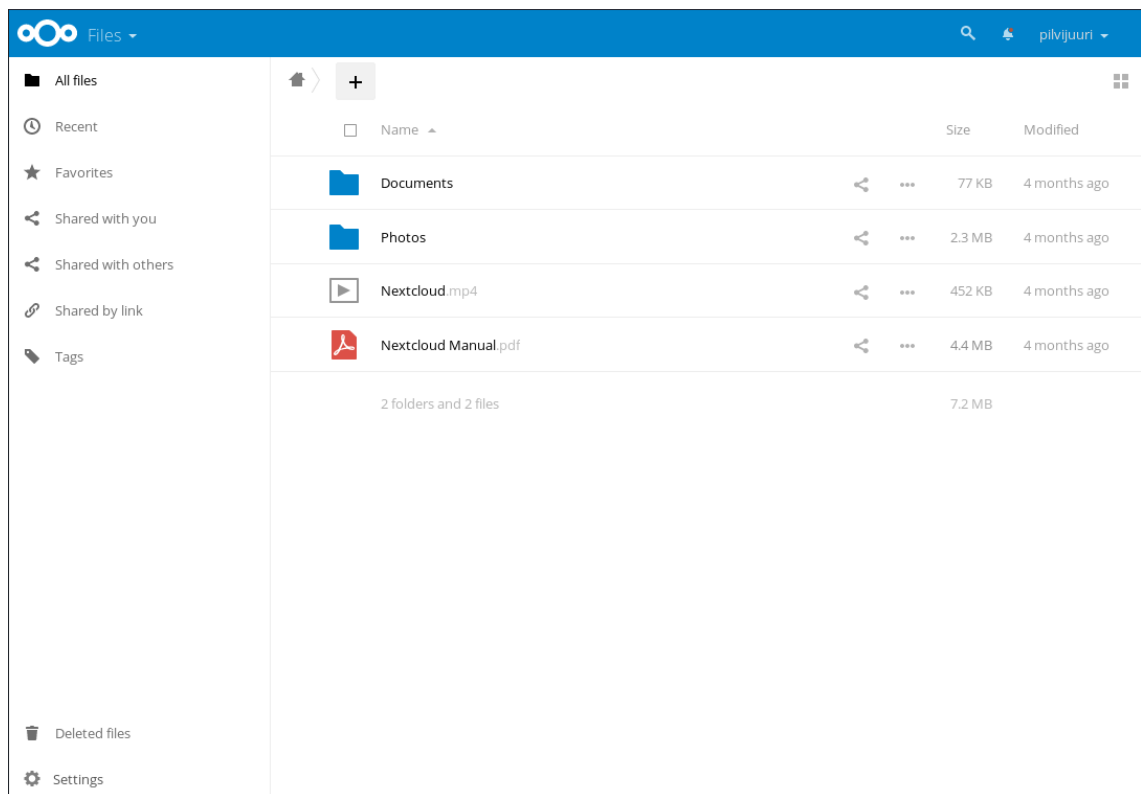
Nextcloudin matkapuhelinsovellus löytyy tällä hetkellä Androidille ja iPhoneille. Sovellus on helpon asentaa kirjautumalla puhelimella omalle palvelimelle, jolloin palvelin ehdottaa sovelluksen asentamista ja näyttää suorat linkit sovelluskaupoihin. Perussovellus mahdollistaa tiedostojen synkronoinnin, mutta mikäli halutaan synkronoida kalenteri ja yhteystiedot Android-puhelimessa, tarvitsemme apuohjelman nimeltä DAVdroid, joka mahdollistaa CalDAV- ja CardDAV-protokollien käytön. iPhone tukee molempia tekniikoita valmiiksi. Opinnäytetyön kirjoittamisen hetkellä Android-versiossa on virhe, joka estää kalenterin käytön. Korjaus on työn alla ja ominaisuuden saa käyttöön käyttämällä Developer-versiota, jonka voi ladata Nextcloudin kehittäjä sivustolta osoitteesta **<https://download.nextcloud.com/android/dev/latest.apk>**.

7.3 Selainkäyttöliittymä

Monipuolisin tapa käyttää Nextcloudia on sen tarjoama selainkäyttöliittymä (Kuvio 34). Sen kautta voidaan hallita tietoja ja käyttäjiä sekä asentaa lisäominaisuuksia. Kirjautuminen tapahtuu käyttötarkoituksesta riippuen joko käyttäjän omalla tunnuksella tai ylläpitotarkoituksessa pääkäyttäjän (root) tunnuksilla. On suositeltavaa olla käyttämättä samaa tunnusta sekä ylläpitoon että normaaliin käyttöön tietoturvariskin vuoksi.

Selainkäyttöliittymään pääse käsiksi käyttämällä määriteltyä julkista osoitetta ja asennuskansiota, esimerkiksi <https://pilvipalvelin.dy.fi/nextcloud>. On huomioitavaa, että kun käytössä on SSL-suojattu sivusto, joudutaan käyttämään URL-muotoa https.

Sisäänkirjautumisen jälkeen esille tulee pilvipalvelimen pääsivu, joka näyttää palvelimella olevat tiedostot (Kuvio 34). Oletusarvoisesti kaikilla käyttäjillä on pieni esittelyvideo ja Nextcloudin käyttöohje.



Kuvio 34. Selainkäyttöliittymä

8 POHDINTA

Tässä opinnäytetyössä keskityttiin asentamaan Nextcloud-pilvipalvelujärjestelmä tietokoneeseen, jossa ajetaan virtualisoinnin mahdollistavaa käyttöjärjestelmää. Koska ohjelmistotekniikka kehittyy suurella nopeudella, on todennäköistä, että käytetyt ohjelmistot ovat päivittyneet uudempiin versioihin. Kehittäjät lisäävät koko ajan uusia ominaisuuksia ja korjaavat löydettyjä virheitä. Myös käyttöliittymiä kehitetään koko ajan, jolloin ulkoasu voi olla hyvinkin erilainen kuin mitä tässä opinnäytetyössä on kuvattu.

Tässä opinnäytetyössä käytetyt ohjelmistot ja menetelmät ovat usein peruskäyttäjälle uusia, joten on suositeltavaa tutustua tekstissä viitattuihin asioihin perusteellisemmin ennen kuin järjestelmän rakentaminen aloitetaan. On otettava huomioon myös laitetekniikan nopea kehitys, mikä mahdollistaa eritasoisten palvelinympäristöjen rakentamisen, kevyestä Raspberry Pi-alustasta aina useamman järeän luokan palvelinkoneen keskukseen.

Opinnäytetyössä tehty järjestelmä on sovelias koti- ja pienyrityskäyttöön sellaisenaan, mutta on suositeltavaa tutustua etenkin tietoturva-asioihin tarkemmin ennen palvelun saattamista julkiseksi. Perusasetukset ovat riittävät peruskäyttäjälle, mutta järjestelmää on muistettava ylläpitää myös ohjelmistopäivitysten osalta.

LÄHTEET

Certbot. Electronic Frontier Foundation. 2017. <https://certbot.eff.org/>

Classless Inter-Domain Routing 2017. Wikipedia. 12.8.2017 https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

Database Configuration – Nextcloud 11 Server Administration manual. Nextcloud. 2016. https://docs.nextcloud.com/server/11/admin_manual/configuration_database/linux_database_configuration.html

DY.fi. 2017. <https://www.dy.fi/>

KVM contributors 2017. KVM Main Page. 21.7.2017 https://www.linux-kvm.org/index.php?title=Main_Page&oldid=173792

Let's Encrypt 2017. ISGR. 10.8.2017 <https://letsencrypt.org/>

Linux Users and Groups. 2017. linode. <https://www.linode.com/docs/tools-reference/linux-users-and-groups>

LXC 2017. 21.7.2017 <https://linuxcontainers.org/lxc/introduction/>

Manual installation on Linux – Nextcloud 11 Server Administration manual. Nextcloud. 2016. https://docs.nextcloud.com/server/11/admin_manual/installation/source_installation.html#ubuntu-installation-label

Nextcloud 11 Server Administration Manual. Nextcloud. 2016. https://docs.nextcloud.com/server/11/admin_manual/contents.html

Nextcloud 2017. Nextcloud. 21.7.2017 <https://nextcloud.com/>

Server virtualization management with Proxmox VE 2017. Proxmox Server Solutions GmbH. 21.7.2017 <https://www.proxmox.com/en/proxmox-ve>

SSL Sertifikaatti. Verisign, Inc. 2016. What is an SSL Certificate? 21.7.2017 https://www.verisign.com/en_US/website-presence/website-optimization/ssl-certificates/index.xhtml

What is LAMP (Linux, Apache, MySQL, PHP)? - Definition from WhatIs.com. 2008. TechTarget 30.7.2017. <http://whatis.techtarget.com/definition/LAMP-Linux-Apache-MySQL-PHP>

What is virtualization 2017. opensource.com. 3.10.2017 <https://opensource.com/resources/virtualization>