HAMK
Hämeen ammatti-
korkeakoulu

On premise -virtualisointi ratkaisuna yritykselle

Ammattikorkeakoulututkinnon opinnäytetyö
Tieto- ja viestintätekniikka, insinööri (AMK)
Kevät, 2024
Hannu Pihlajakangas

HAMK
Hämeen ammatti-
korkeakoulu

Tieto- ja viestintätekniikka
Tekijä Hannu Pihlajakangas
Työn nimi On premise -virtualisointi ratkaisuna yritykselle
Ohjaaja Teemu Järvenpää

Tiivistelmä
Vuosi 2024

Opinnäytetyön tarkoituksena oli luoda konseptitoteutus virtualisointiympäristöstä Proxmoxilla, mitä pystyy käyttämään palveluntarjontaan julkisessa verkossa ammattimaisella tasolla. Työssä myös tutkittiin Proxmox ympäristön toteuttamista pienyrityksen käyttötarkoituksia varten paikallisesti ylläpidettävällä palvelininfrastruktuurilla.

Työn alkuosassa käytiin läpi erilaisia virtualisointiin liittyviä teknologisia vaihtoehtoja, ja vertailtiin erilaisia virtualisointiin liittyviä vaihtoehtoja. Näitä teknisiä vaihtoehtoja on eri tyyppien hypervisorit, ja virtualisointitekniikat KVM ja LXC.

Palomuuri- ja reititysratkaisuna ympäristössä oli käytössä Pfsense. Pfsensen avulla tehtiin kaikki tapahtuvan tietoverkkoliikenteen organisointi.

Lopuksi käytiin läpi teoriaa ympäristön parantamista varten, sekä pohdittiin työn onnistuneisuutta. Jatkoehdotukset parantamiseksi koostuvat asioista kuten tietoturvan kehitys, ympäristön valvonta, ja skaalautumisen tutkiminen. Tietoturvan kehitys tapahtui muodostamalla elpymissuunnitelman tueksi varmuuskopioinnin Proxmox backup server nimisellä ohjelmistolla. Ympäristön valvonta toteutettiin Proxmoxin tarjoamalla external metric server toiminnallisuudella, jonka avulla data vietiin Influxdb tietokantaan ja siitä Grafanalle visualisoitavaksi. Skaalautumisessa käsiteltiin työn ympäristön kasvua, ja tuotiin myös esiin pilvipalvelujen mahdollisuuksia. Konkreettisena lopputuloksena on paikallisesti ylläpidettävä virtualisointialusta, jolta pystytään tarjoamaan internetiin virtuaalisia palveluja.

Avainsanat Proxmox, Pfsense, virtualisointi
Sivut 26 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Information and Communication Technology | Abstract
Author Hannu Pihlajakangas | Year 2024
Subject On Premise Virtualization as a Company Solution
Supervisor Teemu Järvenpää

The purpose of the thesis was to create a proof of concept implementation of a virtualization environment using Proxmox that can be used to serve content on the public network on a professional level. The thesis also explored the implementation of the Proxmox environment for the purposes of a small business using locally maintained on-premise server infrastructure.

The initial part of the thesis covered various technological alternatives related to virtualization and compared different options related to virtualization. These technical alternatives included various types of hypervisors and virtualization techniques such as KVM and LXC.

As a firewall and routing solution, Pfsense was used in the environment. Pfsense was used to organize all network traffic.

In the latter part of the thesis, theory was discussed for improving the environment, and the success of the thesis was reflected upon. Suggestions for improving the environment included aspects such as enhancing security, environment monitoring, and investigating scalability. Security enhancement was achieved by creating a backup plan using the Proxmox backup server software. Environment monitoring was implemented using Proxmox's external metric server functionality, which transferred data to an Influxdb database for visualization on Grafana. Scalability addressed the growth of the environment, also highlighting the possibilities of cloud services. The tangible result is a locally maintained virtualization platform capable of offering virtual services to the internet.

Keywords Proxmox, Pfsense, virtualization
Pages 26 pages

Sisällys

1 Johdanto 1
2 Proxmox 2
2.1 Virtualisointi 2
2.1.1 Hypervisor 3
2.1.2 Virtualisointialustan vertailu 4
2.1.3 Pilvipalvelut 7
2.2 Proxmox käytössä 8
3 Pfsense 11
4 Kokonaisuus 14
4.1 Tietoturvan kehitys 14
4.2 Ympäristön valvonta 17
4.3 Skaalautuminen 21
5 Yhteenveto 23
Lähteet 25

Kuvat, taulukot ja kaavat

Kuva 1. Tyypin 1 ja tyypin 2 hypervisorit (Verma, 2016). 3

Kuva 2. Proxmoxin hinnasto ja lisenssiversiot (Proxmox, n.d.-d). 4

Kuva 3. VMware virtualisointiratkaisun hinnasto vuodelta 2023 (VMware, n.d.-b). 5

Kuva 4. Proxmoxin tarjoama graafinen käyttöliittymä. 8

Kuva 5. LXC-virtualisoinnin kerrokset (Oracle, 2016). 9

Kuva 6. KVM-virtualisoinnin tasot (AWS Amazon, n.d.-a). 9

Kuva 7. Pfsensen webbipohjainen graafinen käyttöliittymä. 11

Kuva 8. Diagrammi käytössä olevasta tietoverkosta. 13

Kuva 9. Proxmox klusteritason hallintanäkymä. 17

Kuva 10. Proxmox virtuaalikoneen valvontanäkymä. 18

Kuva 11. Grafanaan tuotu datanäkymä. 20

Kuva 12. Vertikaalisen ja horisontaalisen skaalautumisen ero kuvitettuna (Custer, 2023). 21

Kuva 13. Kuorman tasaaja integroituna infrastruktuuriin (Nginx, n.d.). 22

Taulukko 1. Proxmox ja VMware lisenssien hintavertailu vuodessa. 6

1 Johdanto

Erilaisten tietoteknisten ratkaisujen jatkuva yleistyminen maailmassa on tuonut mukanaan monimutkaisia haasteita liittyen IT-infrastruktuuriin. Organisaatioiden tarve isommalle määrälle koneita kasvaa jatkuvasti, ja tässä erilaiset virtualisointiratkaisut ovat hyvä työkalu.

Opinnäytetyössä toteutetaan virtualisointiympäristö konseptitoteuteksena pienimuotoisolle yritykselle, joka tarjoaa virtuaalisia ohjelmistoja palveluna (engl. Software as a Service) (SaaS) yrityksen omista tiloista käsin (engl. on premise). Opinnäytetyön keskeisenä osana toimii avoimen lähdekoodin virtualisointihallintatyökalu, Proxmox. Proxmoxin avulla käyttäjä pystyy hallitsemaan virtuaalisia tietokoneympäristöjä. Koska työssä palvelimet ovat omatoimisesti ylläpidettyjä, vastuu tietoturvallisuudesta siirtyy enemmän palvelimien ylläpitäjälle. Tämän vuoksi työssä tuodaan esiin myös tietoturvallisuuden aspektia, ja esitellään vaihtoehtoisia ratkaisuja jatkuvan palveluntarjonnan parantamiseksi.

Palomuuriratkaisuna työssä toimii Pfsense. Pfsensen tarjoama palomuuri ja verkkoliikenteen reititys mahdollistaa kokonaisuuden tietoverkkohallinnan ulko- ja sisäverkon välillä. Pfsensen avulla voidaan myös monitoroida verkkoliikennettä, ja suodattaa lähiverkkoympäristöön kohdistuvia pyyntöjä ennakoivasti palomuurin avulla.

Työ tutkii myös erilaisia virtualisointitekniikoihin liittyviä vaihtoehtoja yrityksen näkökulmasta, ja tavoitteena on huomioida myös yrityksen taloudellinen resurssointi. Tämä korostuu työssä avoimen lähdekoodin ohjelmistovaihtoehtojen muodossa.

Lopputuloksena on konseptitoteutus avoimen lähdekoodin virtualisointiympäristöstä, jonka päälle pienyritys pystyy jatkorakentamaan palveluntarjontaa verkkoon asiakkaille hyvin pienellä aloitussijoituksella infrastruktuurin kannalta. Loppupuolella käydään läpi jatkokehitykseen liittyvää teoriaa, joka edistää alustaa toimimaan paremmin käytön lisääntyessä. Työ pyrkii vastaamaan kysymyksiin kuten:

- Onko Proxmox oikea työkalu virtualisointitehtävään?
- Miten Proxmox ympäristö pystyy jatkokehittymään käyttäjämäärän kasvaessa?

2 Proxmox

Proxmox on avoimen lähdekoodin virtualisointiratkaisu. Proxmoxilla voidaan hallinnoida virtuaalikoneita sekä Linux-pohjaisia kontteja.

Virtualisointiratkaisuja on useita. Uuden ympäristön suunnitteluprosessissa oikean ratkaisun valinta on kriittinen. Käytössä oleva ratkaisu yleensä riippuu erilaisista tekijöistä. Tämän tyyppisiä tekijöitä ovat esimerkiksi suorituskyvynvaatimus ympäristössä, ja yhteensopivuusriippuvuus. Seuraavassa luvussa käydään läpi mahdollisia virtualisointiratkaisuja, ja perustellaan Proxmoxin valinta ympäristössä.

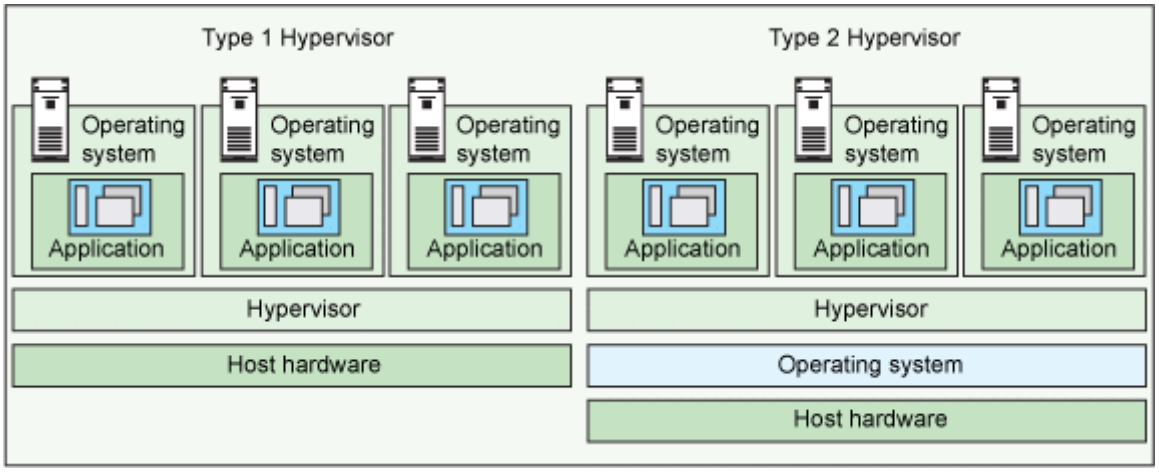
2.1 Virtualisointi

Virtualisointi on ohjelmiston avulla abstraktiokerroksien tekemistä, joka mahdollistaa palvelinkoneen resurssien pilkkomisen osiin omiksi kokonaisuuksiksi. Jokainen virtualisoitu kone toimii täysin omana kokonaisuutenaan tiedostamatta toisiaan, vaikka laskentaresurssit ovat jaettuja. (IBM, n.d.) Käytännössä tämä mahdollistaa työssä monien eri prosessien suorittamisen yhdellä fyysisellä laitteella, vähentäen fyysisen infrastruktuurin määrän tarvetta.

2.1.1 Hypervisor

Virtualisoinnin mahdollistaa ohjelmisto nimeltään hypervisor. Hypervisoreita on kahta erilaista luokkaa kuvan 1 mukaisesti, tyyppi 1 ja tyyppi 2. Näissä erona on se, että tyypin 2 hypervisor toimii jo olemassa olevan käyttöjärjestelmän päällä kuten Windows. Tyyppi 1 toimii suoraan tietokoneen komponenttien kanssa laitteistopohjalla ilman lisättyjä abstraktiotasoja, eli niin sanotusti “raudan tasolla” (engl. bare metal). Tämä tarkoittaa hypervisorin pystyvän toimimaan ilman erillistä käyttöjärjestelmää. Raudan tasolla toiminta mahdollistaa tehokkaamman prosessointiresurssien jakamisen, ja käytön virtuaalikoneklusterissa. (Red hat, 2023)

Kuva 1. Tyypin 1 ja tyypin 2 hypervisorit (Verma, 2016).

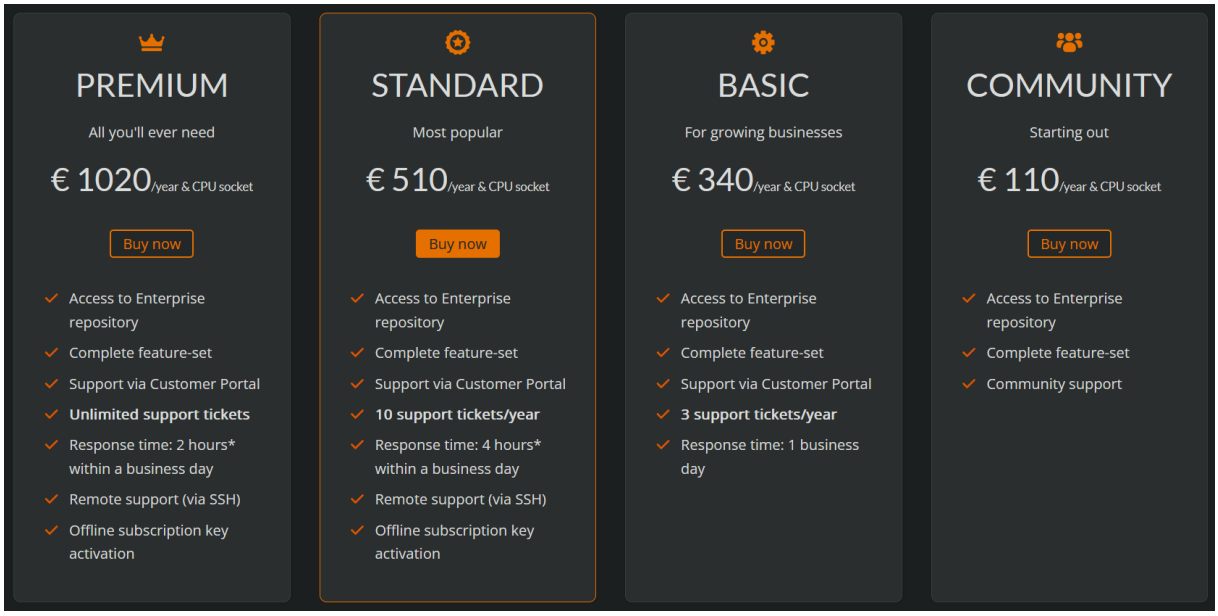


Koska yrityksen tavoite on tarjota virtuaalisia palveluja asiakasrajapinnassa, soveltuu resurssitehokkaampi tyypin 1 hypervisor tähän käyttötarkoitukseen paremmin. Tyypin 1 hypervisoreita on useita, ja yritykselle oikean valinta on tärkeää. Valinnalla voi olla suuri rahallinen vaikutus yritykseen ohjelmistojen lisenssihintojen eroavaisuuksien takia. Asiakasvolyymin kasvaessa isommaksi myös lisenssejä on hankittava enemmän, mikä aiheuttaa lisämaksuja. Lisämaksut on otettava huomioon ennakoivasti opinnäytetyön kaltaisessa ympäristössä, jossa taloudelliset resurssit on rajattu. Seuraavaksi tutkitaan hypervisoreita, ja suoritetaan vertailua parhaan valinnan selvittämiseksi.

2.1.2 Virtualisointialustan vertailu

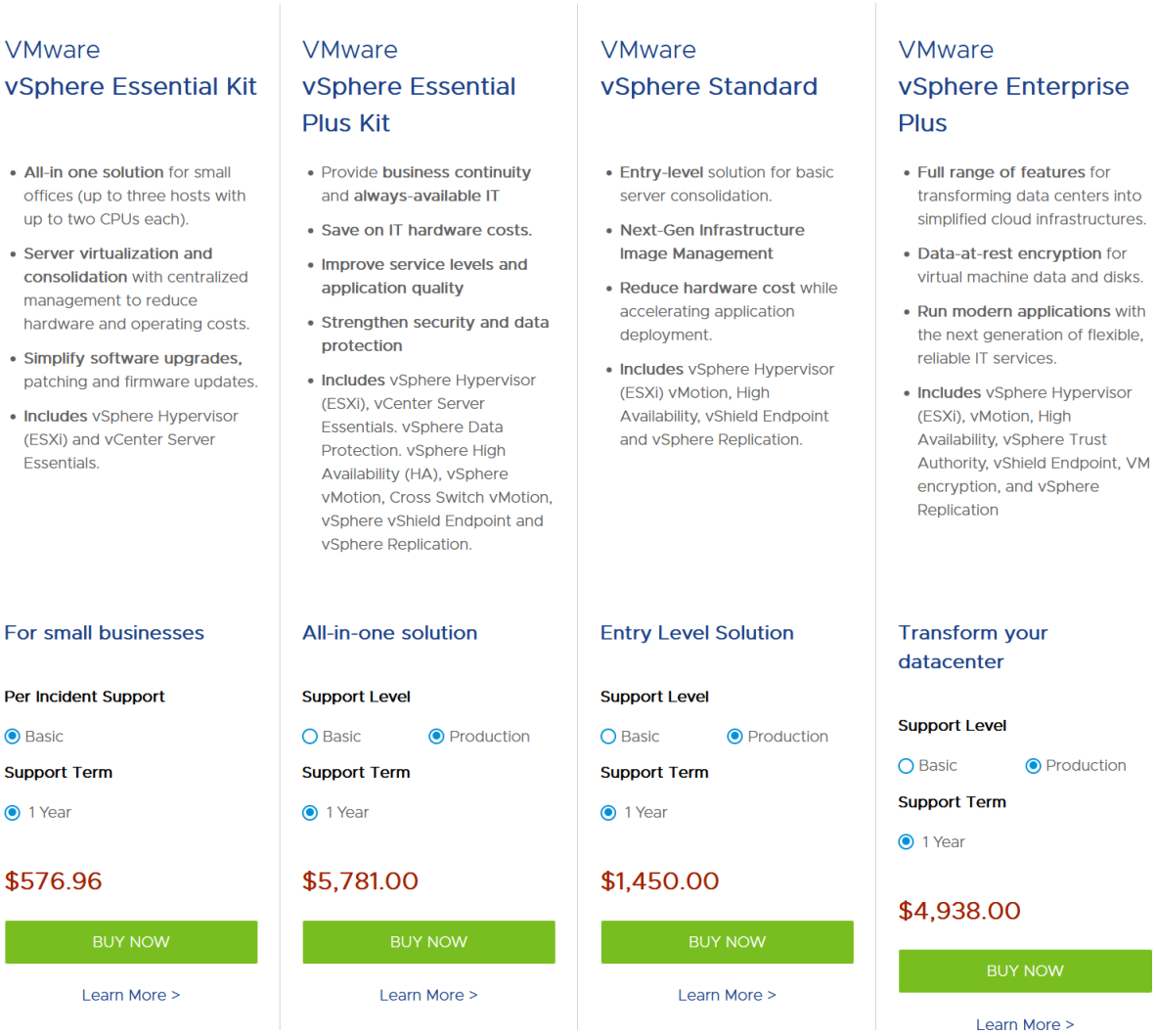
Vertaamalla Proxmoxia sen suosittuun kilpailijaan, VMwaren ESXiin pystymme käymään läpi näitä eroavaisuuksia. ESXistä oli ennen ilmainen versio rajoitetuilla toiminnallisuuksilla, mutta tätä ei enää ole saatavilla (VMware, 2024). Proxmoxin kaikki toiminnallisuudet ovat ilmaisia käytettäväksi asennuksen jälkeen. Halutessaan käyttäjä voi valita neljän erilaisen tukipaketin väliltä, jotka näkyvät kuvassa 2. Teknisestä näkökulmasta hyödyllisin on halvin tukipaketti, community. Communityn oston yhteydessä asiakas saa pääsyn Enterprise Repositoryyn. Enterprise Repositoryn kautta pystyy hakemaan sovelluksista vakaimmat ja testatuimmat versiot, joka turvaa paremman tietoturvallisuuden tuotantokäytössä (Proxmox, n.d.-f). Tarkastelemalla kuvaa 2, voi huomata muiden lisenssipakettien välillä olevan eroavaisuuden olevan pelkästään asiakastukeen liittyvä.

Kuva 2. Proxmoxin hinnasto ja lisenssiversiot (Proxmox, n.d.-d).



Proxmoxin yritystason kilpailija VMware ei ole vielä julkaissut vuoden 2024 uusinta hinnastoa julkiseksi nettisivullaan. Tutkimalla kuvan 3 vuoden 2023 hintoja pystytään saamaan lähtökohtainen arvio lisenssistä, ja sen mukana tulevista toiminnallisuuksista.

Kuva 3. VMware virtualisointiratkaisun hinnasto vuodelta 2023 (VMware, n.d.-b).



Ostamalla halvimman vSphere Essential Kit -lisenssin saa käyttöön ohjelmiston, joka täyttää virtualisointiympäristön minimivaatimukset ympäristöön. Lisenssillä saa käyttöön pelkästään yksinkertaisen virtuaalikoneiden luomisen, ja hallitsemisen kolmelle eri palvelinkoneelle. Basic tason lisenssi on tarkoitettu pelkästään kehitystyöhön (VMware, n.d.-a). Pelkkä kehitystyö tarkoittaa production-tason lisenssin olevan pakollinen, jos halutaan myös VMwaren tarjoamaa asiakastukea tuotantokäytössä.

Tekemällä taulukon 1 kuvan 2 ja kuvan 3 lisenssien vuosihinnoista, on hintojen käsittely helpompaa. VMwaren hinnoissa yhdellä palvelimella voi käyttää kahta suoritinkantaa (engl. CPU socket), mutta tämänhetkinen ympäristössä oleva palvelinkone käyttää vain yhtä. Vertailun helpottamisen vuoksi vertailutaulukossa yksi palvelin käyttää yhtä suoritinkantaa alkuperäisen palvelinkoneen mukaisesti. Proxmoxin ilmainen lisenssi on jätetty vertailusta pois, koska se ei maksa mitään eikä ole riippuvainen palvelimien määrästä. Taulukossa vertaillaan Proxmox community, Proxmox premium, vSphere Essential Kit ja vSphere Standard -lisenssien vuosihintoja. Proxmox Premium -lisenssi vastaa asiakaspalvelun tasoltaan vSpheren Standard -lisenssiä, jonka takia se on valittu mukaan vertailuun. Taulukossa on luettavuuden vuoksi muutettu VMwaren ilmoittamat dollarihinnat euroiksi.

Taulukko 1. Proxmox ja VMware lisenssien hintavertailu vuodessa.

Palvelimien määrä	Proxmox community	Proxmox premium	vSphere Essential Kit	vSphere Standard
1	110,00 €	1020,00 €	534,84 €	1450,00 €
2	220,00 €	2040,00 €	534,84 €	1450,00 €
3	330,00 €	3060,00 €	534,84 €	1450,00 €

Taulukosta 1 voi tulkita, että Proxmox Premium -lisenssi on melkein yli tuplasti kalliimpi verrattuna vSphere Standard -lisenssiin palvelinmäärän ollessa kolme. Tämän datan perusteella VMwaren ratkaisu on kannattava, jos ympäristössä on tarvetta kellon ympäri toimivalle asiakaspalvelulle. Koska ympäristössämme ei ole tarvetta asiakaspalvelulle, vertailukohdiksi jää Proxmoxin ilmainen, Proxmox community, ja vSphere Essential Kit -lisenssi. Työssä on tarkoitus minimoida ylläpitoon liittyviä kuluja, joten Proxmoxin ilmainen lisenssi on näistä paras vaihtoehto.

2.1.3 Pilvipalvelut

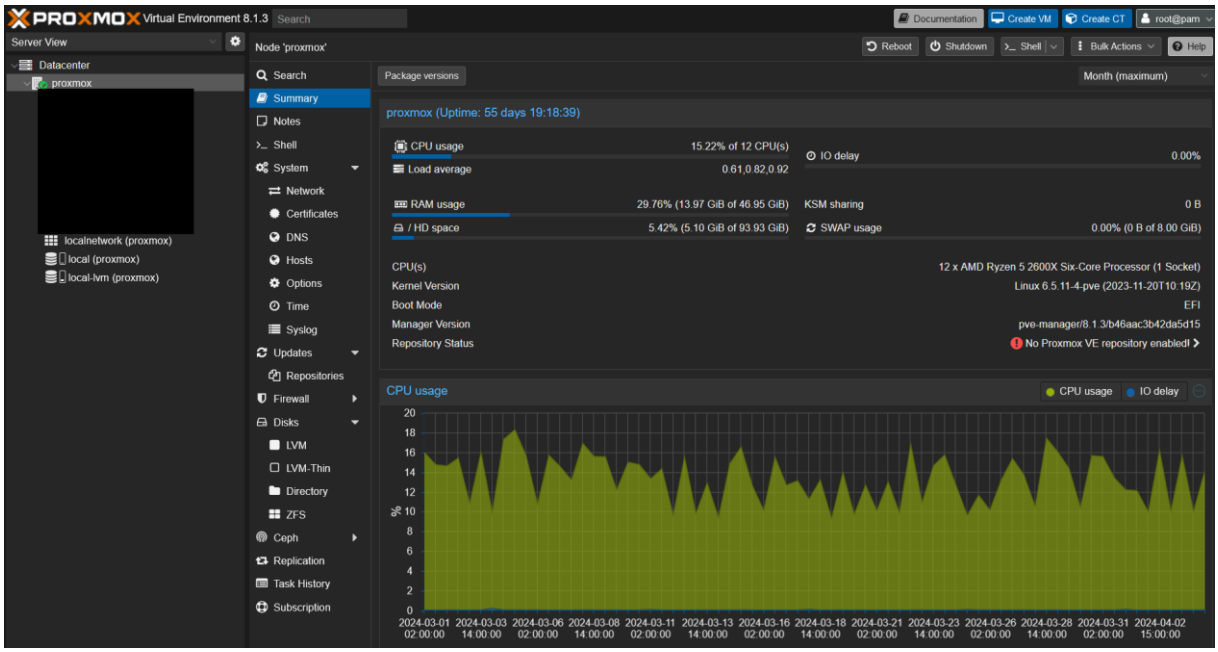
Virtualisoinnin yhteydessä esiintyy usein myös termi pilvipalvelut. Pilvipalvelut ovat käsite etätietokoneresurssien tarjoajille, jotka perustuvat virtualisointiteknologiaan isolla skaalalla. Pilvipalvelujen toimintamallia kutsutaan infrastruktuuriksi palveluna (engl. Infrastructure as a Service) (IaaS). Pilvipalvelussa käyttäjä on eristetty lähes kokonaan fyysisestä palvelinlaitteistosta, ja IaaS-palveluntarjoaja hoitaa lähes kaiken siihen liittyvän. Tämä mahdollistaa pilvipalveluiden asiakasyrityksen keskittymisen pääasiallisesti asiakkaalle tarjottavaan ohjelmistopuoleen. Infrastruktuurin ulkoistaminen ulkopuoliselle palveluntarjoajalle kuitenkin aiheuttaa lisämaksuja verrattuna sen hoitamiseen omatoimisesti ilmaiseksi. Pilvipalveluissa on myös hyvin haasteellista arvioida hintaa tarkasti varsinkin ympäristön jatkuvassa käytön kasvussa erilaisten muuttujien vuoksi.

Opinnäytetyön käyttötarkoitukseen paras vaihtoehto on yrityksen tiloissa sijaitseva palvelinratkaisu, joka hyödyntää Proxmoxin ilmaista lisenssiä. Tällä tavalla palveluntarjonta saadaan pystytettyä minimaalisella ylläpitohinnalla, eikä ympäristössä ole ulkopuolisia riippuvaisuuksia. Yrityksen saatua aloitusasiakkaat, ja ympäristön infrastruktuurin tarpeiden kasvaessa on ajankohtaisempaa harkita sijoitusta maksullisiin. Myös infrastruktuurin osittain pilveen siirtäminen niin sanotuksi hybridiratkaisuksi on mahdollisuus.

2.2 Proxmox käytössä

Proxmox tarjoaa käyttöä varten kuvan 4 kaltaisen selainpohjaisen graafisen hallintakäyttöliittymän, jonka kautta käyttäjä voi luoda ja hallita virtualisoituja koneita. Käyttöliittymä myös tarjoaa näkymän koneen resurssien monitorointia varten.

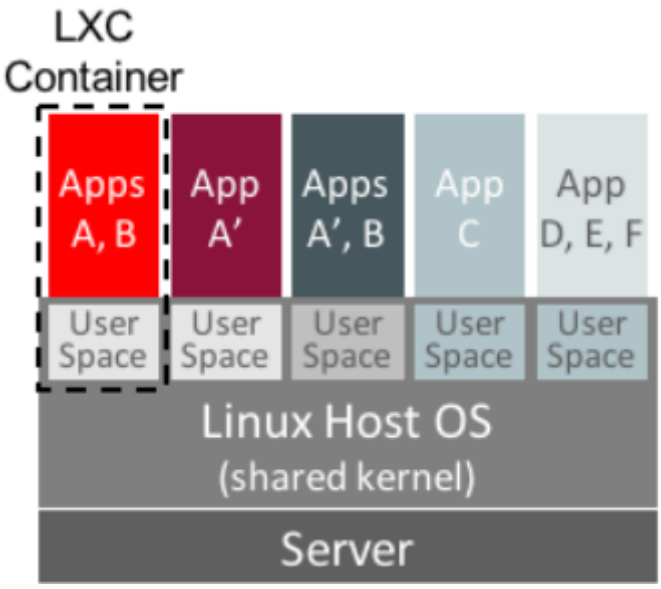
Kuva 4. Proxmoxin tarjoama graafinen käyttöliittymä.



Proxmoxin käyttöliittymän kautta on mahdollista käyttää Linux-kontteihin (LXC) perustuvaa virtualisointiratkaisua, tai kernel-pohjaista virtualisointia (engl. kernel-based virtual machine) (KVM). Näistä kummallakin on omat käyttötarkoituksensa, jotka käydään läpi ymmärtääkseen resurssien tehokasta käyttämistä.

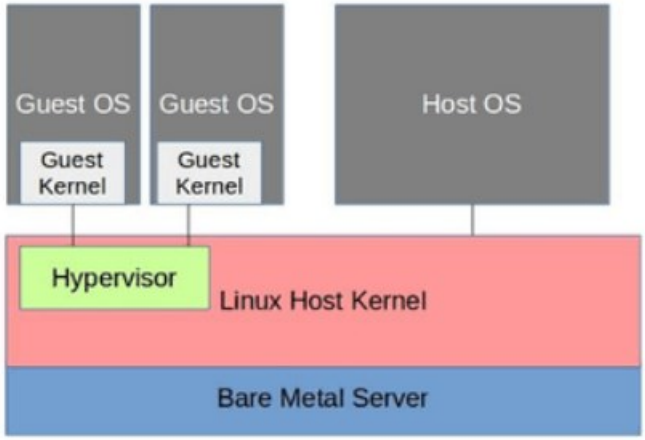
LXC-virtualisoinnissa eroavaisuutena virtualisoidut koneet käyttävät isäntäkoneen (engl. host) omaa kerneliä seuraavan sivun kuvan 5 tapaan. Jaetun kernelin käyttäminen tarkoittaa, että jokaiselle koneelle ei ole tarpeellista luoda uniikkia käyttöjärjestelmäympäristöä. Tämän ansiosta koneelle vapautuu enemmän laskentaresursseja, joka johtaa parempaan myös parempaan kustannustehokkuuteen. Huonona puolena Linux-pohjaisissa konteissa on koneiden välillä oleva heikompi eristys toisistaan tietoturvan näkökulmasta. (Proxmox, 2023)

Kuva 5. LXC-virtualisoinnin kerrokset (Oracle, 2016).



KVM-virtualisoinnissa jokaiselle virtuaalikoneelle tehdään oma vieraskernelinsä (engl. guest kernel) kuvan 6 tapaan (AWS Amazon, n.d.-a). Tämän ansiosta myös jokaisella KVM-pohjaisella virtualisoidulla koneella voi olla omat määrätyt systeemitason komponentit, kuten normaalilla fyysisellä koneella (Red hat, 2022).

Kuva 6. KVM-virtualisoinnin tasot (AWS Amazon, n.d.-a).



KVM-virtualisointi käyttää enemmän resursseja palvelimella, mutta virtualisoidut koneet toimivat täysin omana kokonaisuutenaan. Omana kokonaisuutenaan toimivat virtuaalikoneet tarkoittavat niiden olevan myös parempi vaihtoehto tietoturvan kannalta verrattuna Linux-

kontteihin. Opinnäytetyön ympäristössä KVM-virtualisointiin perustuvia koneita käytetään pohjana kaikkeen, joka on avattuna julkiseen verkkoon päin.

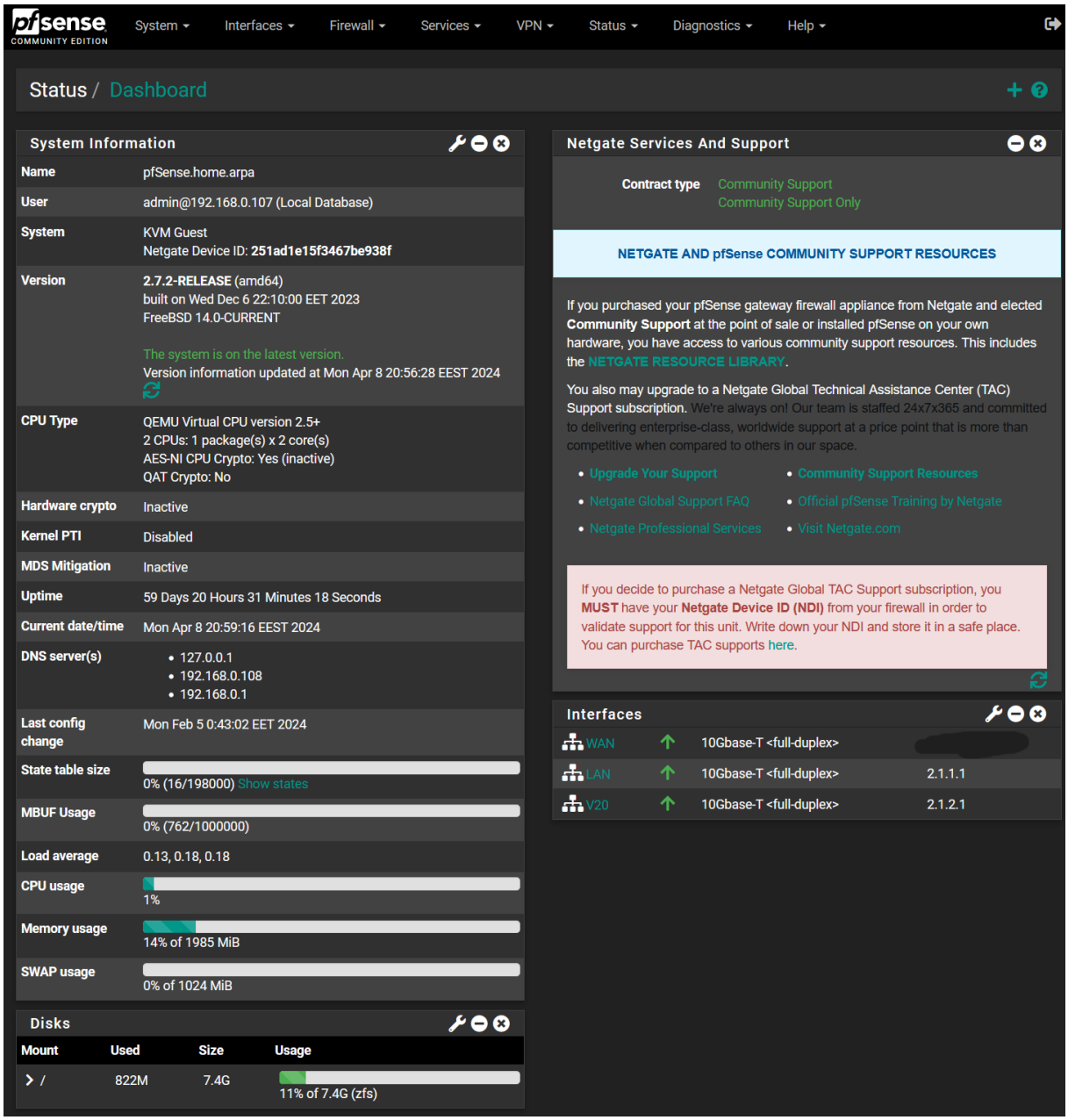
Tällä hetkellä työssä on mahdollista tehdä virtualisoituja palvelimia, joilta pystytään tarjoamaan sisältöä. Palvelimilta ei kuitenkaan vielä tarjota avoimia portteja yhteyksiä varten ulkoverkkoon (engl. wide area network) (WAN), vaan koneet pystyvät yhdistämään palveluun ainoastaan keskenään lähiverkon (engl. local area network) (LAN) sisällä.

Proxmox tarjoaa laajalti perusominaisuuksia tietoverkkojen hallintaan, ja sillä pystyttäisiin tuottamaan toiminnallinen alusta. Tulevaisuutta ajatellen on kuitenkin parempi eriyttää virtualisointiin käytetty alusta omaksi, ja tietoverkkojen hallintaan käytetty alusta omaksi. Tietoliikenteen hallintaan työssä valitaan ohjelmisto nimeltä Pfsense.

3 Pfsense

Pfsense on avoimen lähdekoodin reititin- ja palomuuriratkaisu, joka tarjoaa ominaisuuksia ammattilaistason ympäristöön. Proxmoxin tavoin myös Pfsense tarjoaa hallintamahdollisuuden suoraan kuvan 7 graafisen webbikäyttöliittymän kautta. Pfsense käyttää Apache 2.0 -lisenssiä, joka tarkoittaa vapaata käyttöä henkilökohtaiseen tai kaupalliseen työhön (Snyk, n.d.).

Kuva 7. Pfsensen webbipohjainen graafinen käyttöliittymä.



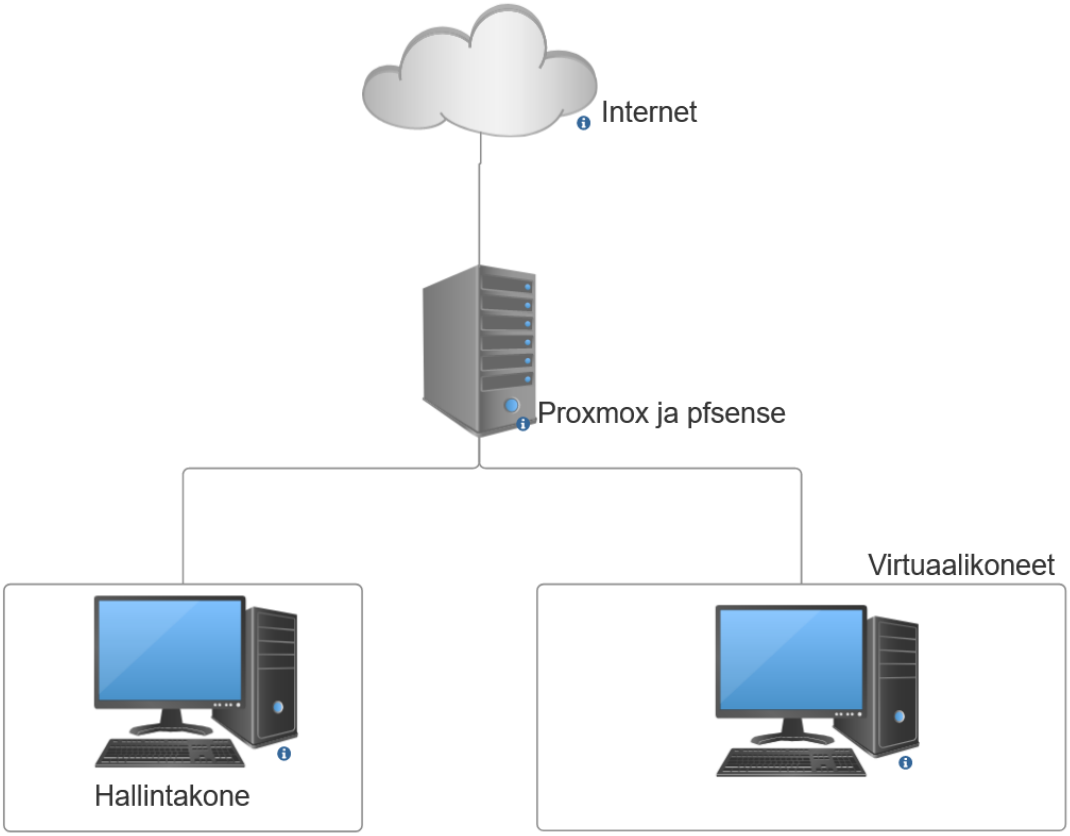
Pfsensen implementointi ympäristöön yleensä tapahtuu kahdella eri tavalla. Ensimmäinen vaihtoehto on virtualisoimalla, tai aiemmin mainitulla raudan tasolla missä sovellus on kokonaan omana laitekokonaisuutenaan. Tässä tapauksessa saatavilla olevat projektin resurssit soveltuvat paremmin virtualisointiin jo olemassa olevan Proxmoxin avulla. Suositellumpi lähestymistapa kuitenkin olisi pitää Pfsense erillään virtualisointialustasta. Pääasiallisena syynä tähän on vältellä yksittäisen palvelimen keskittymää. Jos virtualisointipalvelimen käynnistää uudelleen, myös virtualisoitu Pfsense sammuu. Käytännössä tämä tarkoittaa koko verkon kaatumista, aiheuttaen tilanteen missä yksittäisen palvelimen sammutus keskeyttää palveluntarjonnan kokonaan. Luvussa neljä tutustutaan enemmän ympäristön hajauttamiseen isommaksi kokonaisuudeksi.

Käyttöliittymän kautta pystyy edistämään työn konkreettista tietoverkkopuolta. Tietoverkon reitittämisellä pystyy ohjaamaan verkon liikennettä eri määränpäihin hallitusti, ja palomuurin avulla liikennettä pystyy suodattamaan halutulla tavalla. Käytännössä palomuuri mahdollistaa ennakoivasti jättämään mahdollisesti haitalliset yhteydet palomuurin ulkopuolelle.

Reitittämisellä tarkoitetaan tietoverkon tietopakettien ohjaamisella oikeaan paikkaan. Toisena hyötynä reitityssäännöt myös mahdollistavat koneiden välillä tapahtuvan kommunikaation, ilman että tietopakettien yhteentörmäilyä pääsisi tapahtumaan. Tämä myös estää datan häviämisen tietoliikenteessä. (Cisco, n.d.-b)

Koska virtualisointiympäristössä reitityksien ja verkkoasetuksien tarvittava määrä kasvaa jatkuvasti korrelaatiossa verkon koneiden määrän kanssa, on hyvä tehdä ennakoiva tietoverkkosuunnitelma. Tällä hetkellä ympäristössä on internetiin yksi ulkoverkkoreitti, ja Pfsense ympäristön sisäpuolella oleville palvelimille omat lähiverkkonsa. Seuraavan sivun kuva 8 antaa suuntaa nykyisestä tietoverkkotilanteesta.

Kuva 8. Diagrammi käytössä olevasta tietoverkosta.



Kuvan 8 diagrammista pystyy tulkitsemaan, että hallintakone asetetaan eri lähiverkkoon kuin virtuaalikone. Hallintakoneen ja virtuaalikoneitten erottaminen on tärkeää, koska tarkoituksenamme on avata ulkoverkosta reitti virtuaalikoneille. Ulkoverkkoyhteyden kautta käyttäjät pystyvät yhdistämään palveluun internetin ylitse. Tämä kuitenkin myös tarkoittaa, että myös pahantahtoisesti toimivat yksilöt pystyvät yhdistämään virtuaalikoneeseen. Pahimmassa tapauksessa tietomurron yhteydessä hakkeri pystyy karkaamaan sovelluksen asettamasta ympäristöstä hallitsevaan käyttöjärjestelmään asti, joka tarkoittaisi täydellistä virtuaalikoneen hallintaa. Varotoimena on tärkeätä eristää tietokoneitten yhteydet toisistaan Pfsensen sääntöjen avulla, ja minimoida mahdollista hyökkäyspinta-alaa (engl. attack surface). Hyökkäyspinta-alaksi tulkitaan kaikki auki olevat tietoliikenneportit, ja sitä kautta tarjottavat palvelut (Nixu, 2014).

Tietoverkossa olevat palvelimet pystytään erottamaan tekemällä hallintakoneelle ja virtuaalikoneille omia lähiverkkojaan, sekä hallitsemalla palomuurin kautta läpipäästettävä liikennettä. Hallintakoneilta halutaan ympäristössä päästä hallintakoneen verkosta

Proxmoxiin ja Pfsensen verkkokäyttöliittymiin käsiksi. Virtuaalikoneverkossa olevilta koneilta estetään pääsy kaikkeen lähiverkossa olevaan, ja niiltä pystytään yhdistämään vain avoimeen verkkoon. Virtuaalikoneverkosta pystytään myös vastaanottamaan liikennettä tiettyyn porttiin, josta palveluntarjonta tapahtuu.

4 Kokonaisuus

Proxmoxin ja Pfsensen onnistuneen asentamisen jälkeen on saavutettu minimivaatimukset toimivalle virtualisointiympäristölle, jolta pystyy tarjoamaan sisältöä ulkoverkkoon. Tähän mennessä kokonaisuus kuitenkin on vain konseptitoteutus, ja siitä puuttuu vielä yritykselle kriittisiä asioita sujuvan palveluntarjonnan ylläpitämisen takaamiseksi. Seuraavat luvut käyvät läpi asioita kuten tietoturvan kehittäminen ammattilaisympäristössä, ympäristön valvominen, datan tietoturvaaminen, ja edellytyksiä hyvin skaalautuvaan infrastruktuuriympäristöön.

4.1 Tietoturvan kehitys

Hyvin monessa yrityksessä tietoturva huomioidaan vasta ensimmäisen tietoturvariskin realisoituessa. Riippuen yrityksen toimikuvasta ja vahingon laajuudesta, jo ensimmäinen tapaus voi olla ratkaiseva yritykselle. Tämän takia on suositeltavaa vaalia hyviä käytänteitä aloittamisesta lähtien, ja noudattaa niitä jo ennen julkisen palveluntarjonnan aloittamista.

Tietoturvan kannalta yksi tärkeimmistä asioista on olla valmistautunut jo ennakkoon pahimpiin mahdollisiin skenaarioihin, missä asiakasdataa saattaa hävitä tai palveluntarjonta saattaa katketa. Tätä konseptia kutsutaan toipumissuunnitelmaksi tai elpymissuunnitelmaksi (engl. disaster recovery plan). Toipumissuunnitelma on kirjallinen ohje, miten toimia virhetilanteessa. Erilaisia virhetilanteita voi esimerkiksi olla sähköjen katkeaminen, palvelimen fyysinen tuhoutuminen, tai verkkoyhteyden katkeaminen tuntemattomasta syystä. Dimensional Researchin suorittaman globaalin tutkimuksen mukaan, johon vastasi 1121 IT-alan vastuuhenkilöä, 83 prosentin mukaan 12 tuntia tai alle on hyväksyttävä aikatavoite prosessien palauttamiseksi käyttöön. Kuitenkin vain 52 prosenttia kyselyyn vastanneista on kykenevä tähän aikatavoitteeseen. (Continuity central, 2022)

Hyvässä toipumissuunnitelmassa olennaista on olla laadittuna käytäntöön laitettava varasuunnitelma. Varasuunnitelmassa käydään läpi, miten palvelun tarjonnan pystyy palauttamaan ennalleen vahinkotilanteissa mahdollisimman nopeasti. Varasuunnitelma voi esimerkkinä käsitellä kysymyksiä kuten:

- Keneen ottaa yhteyttä virhetilanteessa
- Miten data pystytään palauttamaan, jos se katoaa
- Miten palveluntarjonnan pystyy eheyttämään ennalleen
- Miten asiakkaiden kanssa kommunikoidaan tilanteen sattuessa

Toipumissuunnitelman tärkein aihe projektin alustan kannalta on tällä hetkellä varmuuskopiointi, ja sen palauttamisen implementointi. Aiemmin viitatussa Dimensional Researchin tutkimuksessa 76 prosenttia vastaajista on jossain vaiheessa menettänyt bisneskriittistä dataa hetkellisesti. Kyselyyn vastanneista 45 prosenttia on kokonaan menettänyt datansa. (Continuity central, 2022)

Varmuuskopiointi tarkoittaa tiedon kopioimista, ja sen tallentamista tiettyyn paikkaan, josta sen voi helposti palauttaa takaisin järjestelmän käytettäväksi. Jos Proxmoxin palvelimen tällä hetkellä tietoa sisältävät kovalevyt tuhoutuisivat, kaikki asiakasdata katoaisi ikuisesti. Yksi parhaista käytänteistä varmuuskopioida välttääkseen datan häviämistä on noudattaa niin sanottua ”3-2-1” sääntöä. Säännön mukaan datasta pitäisi olla kolme kopiota, kahdella eri tallennustavalla, joista yhden varmuuskopion pitäisi olla ympäristön ulkopuolella sijaitseva (engl. off-site). (Vanover, 2024) Monet kiristyshaittaohjelmat pyrkivät lukitsemaan myös yrityksen varmuuskopiot, minkä takia on hyvä olla yksi ympäristöstä irrallinen varmuuskopio (Adam, 2024).

Varmuuskopioiden dataa pystytään tallentamaan kolmella eri tavalla:

- Täysi varmuuskopio (engl. full backup)
- Differentiaalinen varmuuskopio (engl. differential backup)
- Inkrementaalinen varmuuskopio (engl. incremental backup)

Proxmox ympäristössä varmuuskopioinnin pystyy tekemään useammalla tavalla. Yksinkertaisin tapa varmuuskopioida on käyttää Proxmoxin mukana tulevaa varmuuskopiointiin tarkoitettua ominaisuutta. Tämä yksinkertaisempi tapa varmuuskopioida on helppo ottaa käyttöön, mutta tarjoaa vähemmän ominaisuuksia. Kaikki Proxmox backupin kautta tehdyt varmuuskopiot ovat täysiä varmuuskopioita kovalevylle, joka tarkoittaa

pitempää kopiointiprosessia (Proxmox, n.d.-b). Tulevaisuutta ajatellen on ideaalia siirtyä suoraan käyttämään Proxmoxin omaa ohjelmistoa, Proxmox backup serveriä. Proxmox backup -serveriin siirtyminen on kannattavaa, koska se tukee ominaisuuksia kuten reaaliaikainen palautus (engl. live-restore), yksittäisen tiedoston palautus, ja deduplikointi.

Normaalisti varmuuskopion palauttamisen aikana virtuaalikonetta ei pysty käyttämään. Reaaliaikainen ympäristön palauttaminen kuitenkin mahdollistaa virtuaalikoneen käytön samaan aikaan kun varmuuskopioiden palautus tapahtuu. Yksittäisen tiedoston palauttaminen nimensä mukaisesti mahdollistaa ympäristössä yksittäisen tiedoston palauttamisen, jonka ansioista tietyn tiedoston kadotessa palautusta ei ole tarvetta tehdä koko varmuuskopion laajuudella. Molemmat näistä toiminnoista vähentää palvelun seisonta-aikaa (engl. downtime), joka on tarkoitus minimoida ammattilaisympäristössä.

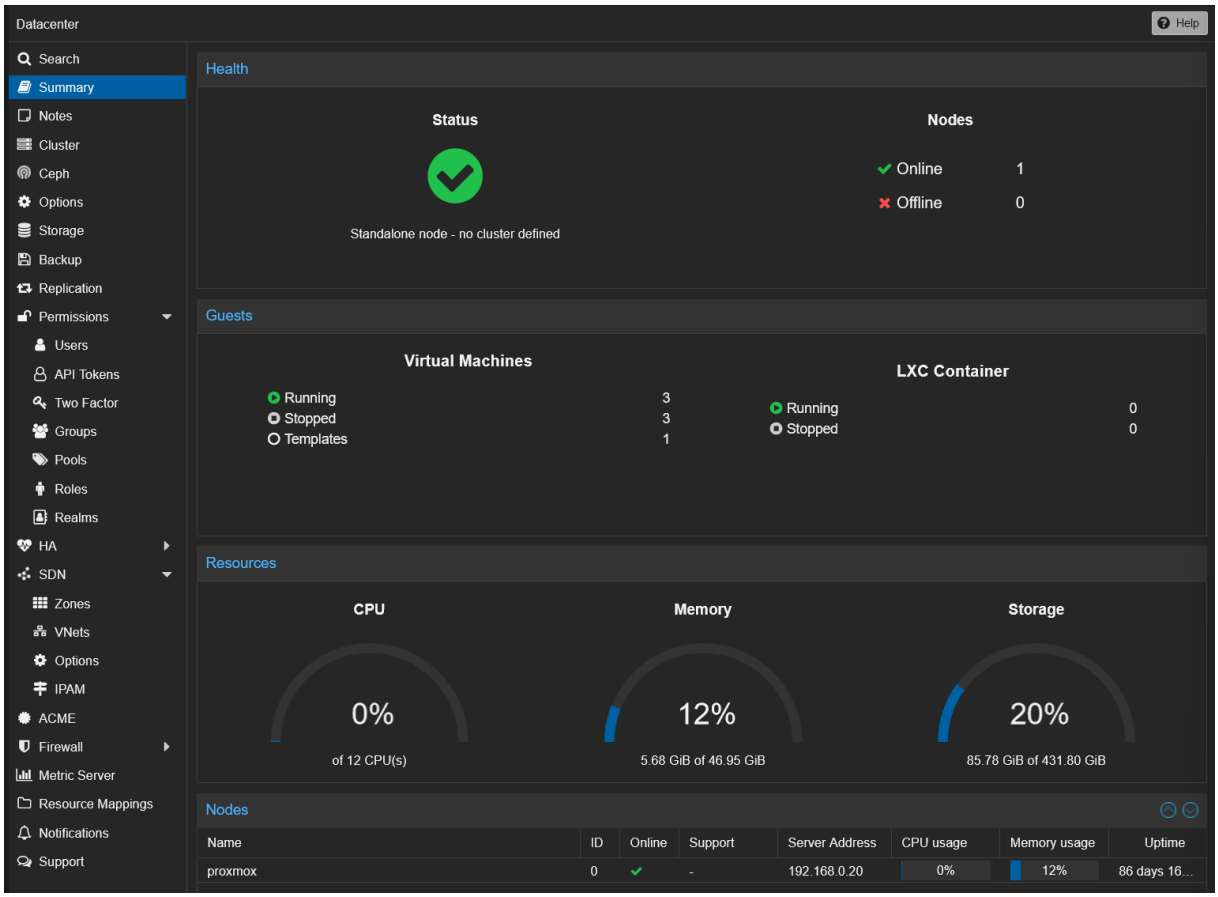
Deduplikointi etsii datasta syntyneet mahdolliset tuplakopiot, ja poistaa ne. Käytännössä tämä vapauttaa enemmän levytilaa, jos useammalta virtuaalikoneelta joudutaan tallentamaan identtistä dataa. (Proxmox, n.d.-e) Tämän avulla Proxmox backup server pystyy tekemään inkrementaalisia varmuuskopioita (Proxmox, n.d.-c), joka tarkoittaa ensimmäisen varmuuskopion olevan täysi varmuuskopio. Ensimmäisen kokonaisen varmuuskopion jälkeen seuraava varmuuskopioprosessi kopioi pelkästään muuttuneen datan. Inkrementaalinen varmuuskopiointi nopeuttaa prosessia huomattavasti verrattuna täyteen varmuuskopiointiin. (Wallen, n.d.) Ympäristöstä jää uupumaan tässä vaiheessa vielä fyysisen ympäristön ulkopuolella sijaitseva varmuuskopio, mutta tämän pystyisi toteuttamaan esimerkiksi viemällä datan kolmannen osapuolen varastoon tietyin aikavälein.

4.2 Ympäristön valvonta

Palvelujen ja palvelimien lisääntyessä määrällisesti alustalla tilanteen valvonta vaikeutuu korrelaatiossa. Hyvän monitorointityökalun ja lokitietojen keräämisen implementointi vähentää manuaalista työtä, antaa tietoa virhetilanteista vastamaalla kysymyksiin kuten milloin, ja missä. Ongelmatilanteiden ilmetessä alustan pitäisi pystyä myös lähettämään ylläpitäjälle ilmoitus automaationa.

Ylläpitäjän täytyy pystyä tarkistamaan palvelimien tilanne helposti. Proxmox tarjoaa tähän käyttötarkoitukseen sisäänrakennettuna valvontanäkymiä monella eri tasolla. Eri tasoja on esimerkiksi jokaista palvelinklusteriin kuuluvaa palvelinta (engl. node) kohden, tai palvelimen sisällä sijaitsevien virtuaalikoneitten tarkastelua varten. Kuva 9 esittelee korkeimman tason hallintanäkymän, jossa näkyy tilanne klusteritasolla.

Kuva 9. Proxmox klusteritason hallintanäkymä.



Kuvasta 9 voi nähdä klusterissa olevien virtuaalikoneiden ja LXC-konttien määrän, sekä käytössä olevat resurssit palvelinkohtaisesti. Valitsemalla virtuaalikoneen pystyy

tarkastelemaan yksittäisen virtuaalikoneen käyttämiä resursseja ja historiaa kuten kuvassa 10 näkyy.

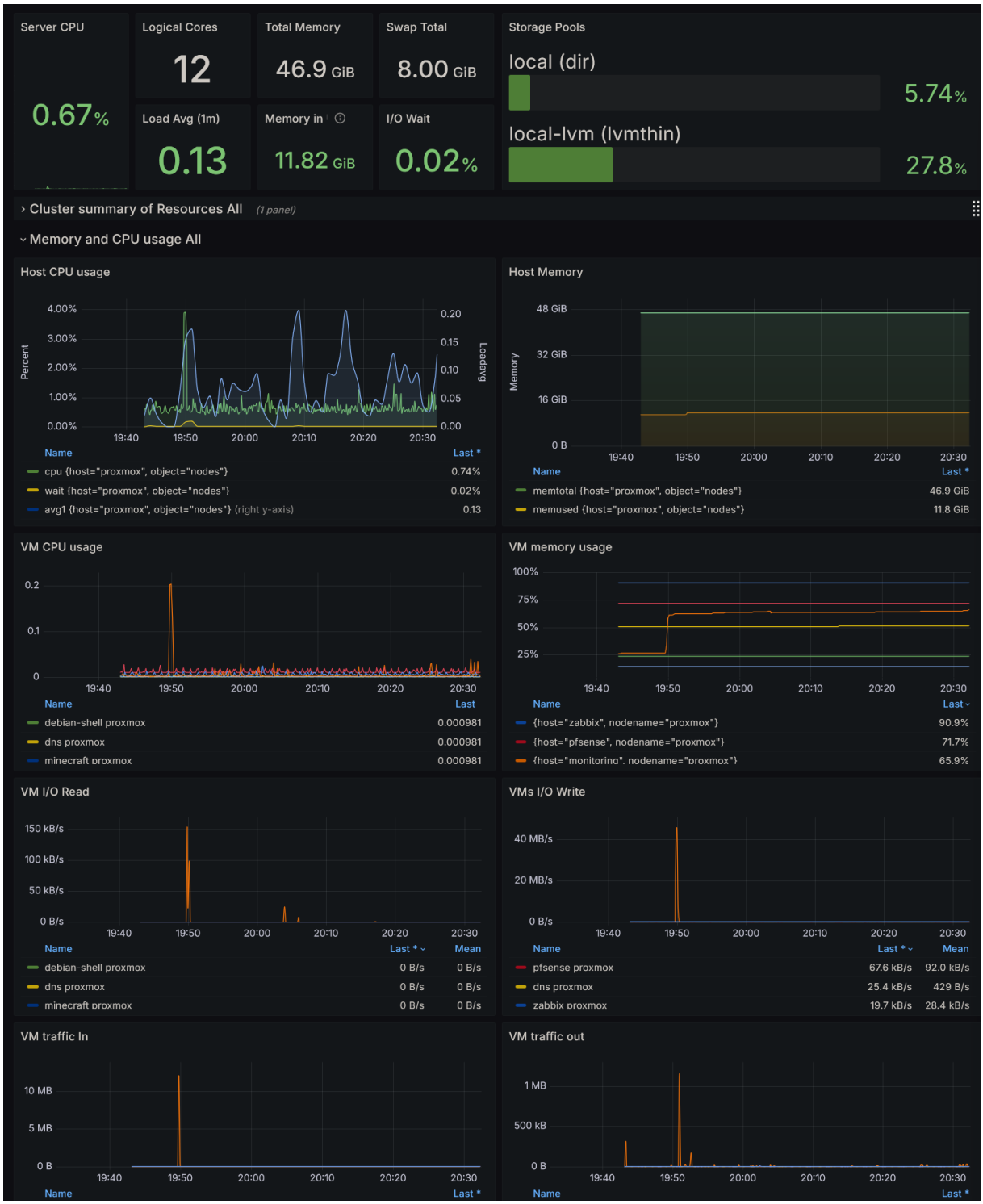
Kuva 10. Proxmox virtuaalikoneen valvontanäkymä.

Vaikka kuvan 9 ja kuvan 10 tapaiset valvontanäkymät ovat selkeitä perusvalvontaan, halutun näkymän muokattavuus on hyvin rajoitettua Proxmoxissa nettiliittymässä verrattuna siihen tarkoitettuun erilliseen ohjelmistoon. Myös tietyn tiedon hakeminen voi olla hyvin työlästä, jos palvelimia ja virtuaalikoneita on ympäristössä useita.

Proxmoxilla on valmis ratkaisu myös tähän, Proxmox external metric server. External metric server -ratkaisun avulla Proxmoxista pystyy keräämään kaiken kerätyn datan ja lähettämään sen suoraan erilliseen tietokantaan. External metric server tukee tällä hetkellä kahta tietokantaa nimeltä Graphite ja Influxdb. Valitulla tietokannalla ei ole kokonaisuuden näkökulmasta väliä, koska molemmat toimivat vain datan säilytyksenä ympäristössä. Ympäristöön kuitenkin valikoitui tässä tapauksessa Influxdb. Influxdb tarjoaa nettikäyttöliittymässä tietokannan datan visualisointia, mutta se on hyvin rajallinen ja epäselvä. Tämän takia on parempi pitää tietokantaratkaisu pelkkänä tietokantaratkaisuna, ja käyttää datan visualisointiin siihen tarkoitettua työkalua Grafanaa.

Grafana on avoimen lähdekoodin datavisualisointiin käytetty työkalu. Grafanassa pystyy käyttämään valmiita datanäkymiä, joita on tarjolla Proxmox ympäristöstä tulevalle datalle. Tällä tavalla ympäristöön pystyy lisäämään nopeasti keskitetyn monitorointialustan, jota pystytään muokkaamaan halutulla tavalla. Seuraavalla sivulla on kuva 11, josta pystyy näkemään käytössä olevan datanäkymän.

Kuva 11. Grafanaan tuotu datanäkymä.



Grafanan avulla pystyy myös luomaan hälytyksiä liittyen erilaisiin tilanteisiin, jos esimerkiksi vaikka virtuaalikone sammuu. Proxmoxista tuodun datan visualisointi Grafanalla mahdollistaa valvonnan tarvittavalla tasolla ympäristössä.

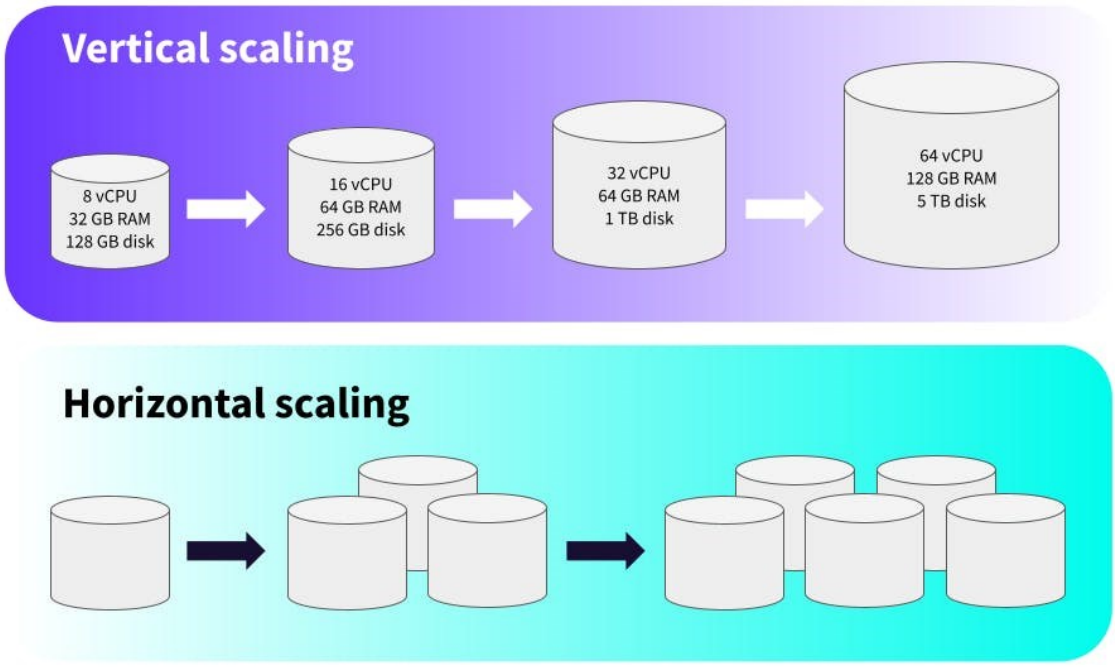
4.3 Skaalautuminen

Ympäristössämme toimii tällä hetkellä yksi tietokone virtualisointia varten, josta tarjotaan palvelua. Voittoa tavoittelevien yrityksien tärkein tavoite on kuitenkin kasvaa, ja palveluntarjontaa ei pysty suorittamaan jatkuvasti kasvavalle määrälle ilman infrastruktuurin rajoituksien huomioon ottamista. Resurssien käyttömäärää suhteessa käyttäjien määrään kutsutaan skaalautumiseksi. Skaalautuminen yleensä tapahtuu kahdella eri tavalla, vertikaalisti tai horisontaalisesti.

Vertikaalisesta skaalautumisesta voi myös puhua ylöspäin skaalautumisena (engl. scaling up) (Custer, 2023). Jos virtualisointiympäristöä halutaan skaalata vertikaalisesti, se tarkoittaa palvelimen laskentaresurssien lisäämistä. Esimerkiksi lisäämällä muistikamman (engl. random-access memory) (RAM) palvelimeen ympäristöä skaalataan vertikaalisesti.

Horisontaalisesta skaalautumisesta puhutaan myös ulospäin skaalautumisena (engl. scaling out) (Custer, 2023). Ympäristön horisontaalinen skaalautuminen tapahtuu lisäämällä enemmän palvelimia ympäristöön. Kuvassa 12 esitellään vertikaalisen ja horisontaalisen ero.

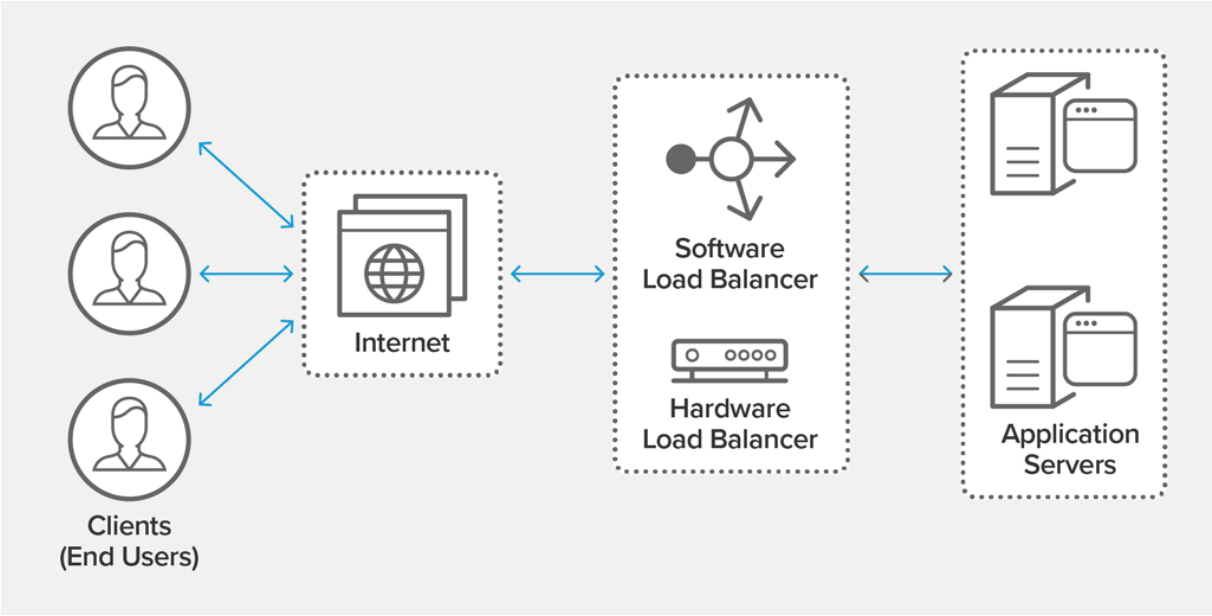
Kuva 12. Vertikaalisen ja horisontaalisen skaalautumisen ero kuvitettuna (Custer, 2023).



Koska palvelinkone on yksittäinen ja paikallinen, on helpompaa skaalata kokonaisuutta vertikaalisesti kuin ostaa kokonaan uusia palvelimia isompaa horisontaalista skaalautumista varten. Yksittäisen palvelinkoneen tapauksessa palveluntarjonta kuitenkin keskeytyy kokonaan, jos palvelimella tapahtuu jonkinlainen virhetilanne. Tästä syystä horisontaalista skaalautumista olisi hyvä toteuttaa ympäristöön sen verran, että varmuuskopioiden varasuunnitelman tyylisesti palvelimella olisi jokin toinen tukipalvelin. Ensisijaisen palvelimen joutuessa virhetilanteeseen, palveluntarjonta jatkuisi tukipalvelimelta, kunnes ympäristö pystytään palauttamaan täyteen kapasiteettiin. Tätä käsitellään enemmän luvun lopussa.

Tulevaisuudessa loppukäyttäjien määrän kasvaessa horisontaalinen skaalautuminen on pakollista, koska vertikaalisessa skaalautumisessa on rajoja, jonka jälkeen päivittäminen ei ole enää sen arvoista rahallisesti tai kokonaan mahdotonta (Custer, 2023). Tässä vaiheessa ympäristöön voi harkita pilvipalveluihin sijoitettua infrastruktuuria uusien palvelimien tekemistä varten. Pilvipalvelujen yksi parhaimpia ominaisuuksia on helppo ratkaisu isoon käyttäjämäärään suorittamalla kuorman tasaamista (engl. load balancing). Kuormituksen tasaaminen tarkoittaa tapaa jakaa loppukäyttäjistä tapahtuvaa liikennettä tasaisesti useamman palvelimen välillä, ohjaten palvelimelle, joka pystyy tarjoamaan yhteyden parhaiten. (AWS Amazon, n.d.-b) Kuva 13 auttaa ymmärtämään kuorman tasaajan paikan infrastruktuurissa.

Kuva 13. Kuorman tasaaja integroituna infrastruktuuriin (Nginx, n.d.).



On premise -ratkaisuna kuorman tasaus on toteutettavissa. Kuorman tasaamisen implementointi kuitenkin edellyttää, että ympäristössä on enemmän kuin yksi palvelin. Tällä

hetkellä ympäristössä palvelimien lisääminen myös edellyttää Pfsensen irrottamista virtualisointipalvelimesta.

Skaalaamalla ympäristöä horisontaalisesti, ja tekemällä kuorman tasausta tavoitellaan työssä mahdollisimman korkeaa saatavuutta (engl. high availability). Korkealla saatavuudella tarkoitetaan pyrkimystä tarjota palvelua asiakkaalle jatkuvasti, ilman keskeytyksiä. Korkeassa saatavuudessa vaatimuksena on ympäristö, joka on klusterissa. Klusteriympäristö tarkoittaa useampaa palvelinta, jotka ovat yhdistetty toimimaan yksittäisenä kokonaisuutena. Klusterissa yhden palvelimen virhetilaan joutuessa, toinen palvelin pystyy ottamaan vastaan tietoliikennettä ilman keskeytyksiä. (Cisco, n.d.-a)

5 Yhteenveto

Opinnäytetyössä keskeisenä tavoitteena oli luoda konseptitoteutus infrastruktuuriympäristöstä rajoitetuilla resursseilla, mistä pystyy kuitenkin tarjoamaan virtuaalisia palveluita ammattimaisella tasolla. Teknologisina tavoitteina oli luoda ympäristö, joka kykenee virtualisoimaan, tarjoamaan sisältöä ulkoverkkoon, ja kasvamaan suhteessa käyttäjämäärään tarpeisiin yrityksen tulevaisuutta ajatellen.

Ongelmia työssä ilmeni ajankäytön kanssa, koska virtualisointiympäristön tekemiseen kulutettava aika oli hyvin vaikeata arvioida ennakoivasti. Alustan rakentamisen jälkeen oli kuitenkin helpompaa kirjoittaa sitä tukevaa teoriaa. Skaalautumista horisontaalisesti oli vaikeampaa tutkia, koska sitä ei pystytty toteuttamaan ympäristöön resurssillisista syistä. Tämä tarkoitti, että jouduin turvautumaan pelkkään teoriaan pitkälti. Myös virtualisointialustojen vertailu Proxmoxin ja VMwaren ESXin välillä oli ongelmallista, koska VMware on lähiaikoina aloittanut toimintamallin muutokset. Esimerkiksi tietoa uusista hinnoista ei ollut julkisesti saatavissa. Myös osa vanhoista VMwaren sivuista oli poistettu käytöstä, mistä olisi pystynyt näkemään tarvittavat tiedot työhön. Työstä jäi myös paljon oleellista asiaa ulkopuolelle, mitä olisi hyvä olla mukana toimivassa ympäristössä. Rajaus aiheesta kuitenkin täytyi tehdä, jotta kokonaisuus pysyisi johdonmukaisena selkeällä alulla ja lopulla.

Työn johdannossa määriteltiin tutkimuskysymyksiksi tutkia Proxmoxia virtualisointivalintana, ja mahdollisuutta jatkokehittää Proxmox ympäristöä. Proxmoxin ilmaisella lisenssillä käyttäen KVM-virtualisointia pystyttiin pääsemään tavoitteeseen, joka oli virtuaalikoneen pystytys ja siltä ohjelmistopalvelun ulkoverkkoon tarjoaminen. Myöskään käyttäjäkunnan kasvaminen ei

ole ongelma Proxmox ympäristössä, sillä käytön lisääntyessä ympäristöä pystyy skaalaamaan tarvittavalla tavalla. Ympäristön korkeaa saatavuutta pystyy myös parantamaan lisäämällä budjettia, jolloin pystyy rakentamaan klustereita ympäristön tueksi.

Yhteenvetona on premise -tyylisellä Proxmox palvelinrakenteella onnistuttiin luomaan kuvailtu ympäristö, joka täytti asetetut tavoitteet yrityksen näkökulmasta. Ympäristöä tullaan myös jatkokäyttämään opinnäytetyön ulkopuolella.

Lähteet

Adam, S. (2024). *Sophos*. The impact of compromised backups on ransomware outcomes. https://news.sophos.com/en-us/2024/03/26/the-impact-of-compromised-backups-on-ransomware-outcomes/

AWS Amazon. (n.d.-a). What is KVM? Kernel-based virtual machine explained – AWS. https://aws.amazon.com/what-is/kvm/

AWS Amazon. (n.d.-b). What is load balancing? https://aws.amazon.com/what-is/load-balancing/

Cisco. (n.d.-a). What is high availability. https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-high-availability.html

Cisco. (n.d.-b). What is routing? https://www.cisco.com/c/en/us/products/routers/what-is-routing.html

Continuity central. (2022). Survey shows that many organizations' disaster recovery plans lack maturity. https://www.continuitycentral.com/index.php/news/business-continuity-news/7699-survey-shows-that-many-organizations-disaster-recovery-plans-lack-maturity#:~:text=29%20percent%20of%20the%20businesses,documented%2C%20tested%2C%20and%20updated.

Custer, C. (2023). *Cockroachlabs*. Vertical vs. horizontal scaling: what's the difference and which is better?. https://www.cockroachlabs.com/blog/vertical-scaling-vs-horizontal-scaling/

IBM. (n.d.). *Virtualization*. https://www.ibm.com/topics/virtualization

Nginx. (n.d.). What Is Load Balancing? https://www.nginx.com/resources/glossary/load-balancing/

Nixu. (2014). Mitä ovat hyökkäyspinta ja hyökkäysvektori? https://www.nixu.com/fi/blog/mita-ovat-hyokkayspinta-ja-hyokkaysvektori

Oracle. (2016). Understanding LXC and Docker Containers on Oracle Linux. https://forums.oracle.com/ords/apexds/post/understanding-lxc-and-docker-containers-on-oracle-linux-7995

Proxmox. (n.d.-a). Administration guide. https://pve.proxmox.com/pve-docs/pve-admin-guide.html#vzdump_restore

Proxmox. (n.d.-b). Backup and Restore. https://pve.proxmox.com/wiki/Backup_and_Restore

Proxmox. (n.d.-c). FAQ. https://pbs.proxmox.com/docs/faq.html#is-the-backup-incremental-deduplicated-full

Proxmox. (2023). Linux container. https://pve.proxmox.com/wiki/Linux_Container

Proxmox. (n.d.-d). Pricing. https://www.proxmox.com/en/proxmox-virtual-environment/pricing

Proxmox. (n.d.-e). Technical overview. https://pbs.proxmox.com/docs/technical-overview.html

Proxmox. (n.d.-f). What is the enterprise repository. https://shop.proxmox.com/index.php?rp=/knowledgebase/23/What-is-the-Enterprise-Repository.html

Red hat. (3. Tammikuu 2023). What is a hypervisor? https://www.redhat.com/en/topics/virtualization/what-is-a-hypervisor

Red hat. (2022). What is KVM? https://www.redhat.com/en/topics/virtualization/what-is-KVM

Snyk. (n.d.). Apache 2.0 license explained. https://snyk.io/learn/apache-license/

Vanover, R. (2024). *Veeam*. What is the 3-2-1 backup rule? https://www.veeam.com/blog/321-backup-rule.html

Verma, G. (2016). *Researchgate*. Type-1 and Type-2 Hypervisor. https://www.researchgate.net/figure/Type-1-and-Type-2-Hypervisor_fig1_310620289

VMware. (2024). End Of General Availability of the Free vSphere Hypervisor (ESXi 7.x and 8.x) (2107518). https://kb.vmware.com/s/article/2107518

VMware. (n.d.-a). VMware Basic Support. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/services/support/vmware-basic-support-datasheet.pdf

VMware. (n.d.-b). vSphere landing page. https://web.archive.org/web/20231127171306/https://store-us.vmware.com/products/data-center-virtualization-cloud-infrastructure.html

Wallen, D. (n.d.). *Spanning*. Types of Backup: Full, Differential, and Incremental Backup. https://spanning.com/blog/types-of-backup-understanding-full-differential-incremental-backup/