

AUTOMAATIOTEKNIIKAN OPPIMISYMPÄRISTÖN PAL-  
VELINVIRTUALISOINTI

Moilanen Nico

Opinnäytetyö  
Sähkö- ja automaatiotekniikka

2021

Sähkötekniikka  
Insinööri (AMK)

---

<b>Tekijä</b>	Nico Moilanen	Vuosi	2021
<b>Ohjaaja</b>	Ins. (YAMK) Markus Palokangas		
<b>Toimeksiantaja</b>	Lapin AMK		
<b>Työn nimi</b>	Automaatiotekniikan oppimisympäristön palvelinvirtualisointi		
<b>Sivu- ja liitesivumäärä</b>	36 + 11		

---

Opinnäytetyö tehtiin Lapin ammattikorkeakoululle. Lapin ammattikorkeakoululle hankittiin kolme palvelinta, joiden ympärille oli tarkoitus rakentaa virtuaalinen oppimisympäristö. Opinnäytetyön tavoitteena oli saada tarvittava tieto palvelinvirtualisoinnista ja soveltaa sitä Lapin AMK:n automaatiotekniikan oppimisympäristön palvelinvirtualisoinnissa. Oppimisympäristöä olisi tarkoitus hyödyntää Lapin ammattikorkeakoululla niin kontakti- kuin etäopiskelussa.

Työssä käsiteltiin palvelinvirtualisointia teoriassa. Opinnäytetyöprojekti koostui kolmesta kokonaisuudesta: palvelimien käyttöönotto ja konfigurointi, palvelimien kytkentä ja projektin dokumentointi. Lisäksi kartoitettiin kameravalvontaohjelmisto, jota hyödynnetään oppimisympäristössä.

Opinnäytetyön tuloksena saatiin täysin toimiva virtuaalinen oppimisympäristö. Opinnäytetyön tuloksia voidaan hyödyntää Lapin ammattikorkeakoulun tekniikan alan opetuksessa. Etenkin virtuaaliset palvelimet helpottavat monimuoto-opiskelijoita ja etänä tapahtuvia opintoja, koska opetus ei ole enää paikkaan eikä aikaan sidottua etätyöskentelyohjelmistojen ansiosta. Palvelinvirtualisointi luo siis joustavuutta niin henkilökunnalle kuin opiskelijoille.

Electrical and Automation Engineering  
Bachelor of Engineering

---

<b>Author</b>	Nico Moilanen	Year	2021
<b>Supervisor</b>	Markus Palokangas, M.Sc.		
<b>Commissioned by</b>	Lapland University of Applied Sciences		
<b>Subject of thesis</b>	Server Virtualization of Automation Technology Learning environment		
<b>Number of pages</b>	36 + 11		

---

The thesis was done for Lapland University of Applied Sciences. Lapland University of Applied Sciences ordered three servers. The servers were intended to build a virtual learning environment. The objective of this thesis was to obtain the necessary information about server virtualization and apply to the server virtualization the automation technology learning environment of Lapland University of Applied Sciences. The virtual learning environment could be utilized in distance learning.

The work discussed server virtualization in theory. The thesis project consists of three entities: server deployment and configuration, server coupling, and project documentation. In addition, the camera surveillance software was surveyed that is being utilized in the learning environment.

The result of the thesis was a fully functional virtual learning environment. The results of the thesis can be utilized in Lapland University of Applied Sciences in teaching in the field of technology. The Virtual servers in particular facilitate multiform studies and distance education because teaching is no longer place- or time-bound, due to remote work programs. The server virtualization brings flexibility to both the staff and students.

Key words

automation, server, virtualization

## SISÄLLYS

1	JOHDANTO .....	7
2	VIRTUALISOINTI.....	8
2.1	Virtualisointi yleisesti.....	8
2.2	Virtualisoinnin hyödyt .....	8
2.3	Virtualisoinnin haasteet.....	9
2.4	Virtualisoinnin historiaa .....	9
3	VIRTUALISOINNIN KÄYTTÖKOHTEET .....	10
3.1.1	Työpöytävirtualisointi.....	10
3.1.2	Verkkovirtualisointi .....	10
3.1.3	Sovellusvirtualisointi .....	11
3.1.4	Tallennusvirtualisointi.....	11
4	PALVELINVIRTUALISOINNIN TAUSTAA .....	12
4.1	VMware.....	13
4.1.1	ESXi .....	13
5	VIRTUAALIYMPÄRISTÖN LUOMINEN.....	14
5.1	Laitteisto .....	15
5.2	Palvelimien käyttöönotto ja konfigurointi.....	16
5.3	RAID5 .....	16
5.4	IDRAC - asetukset .....	17
6	PALVELIMIEN KUNNONVALVONTA.....	18
6.1	Dell OpenManage järjestelmä ja iDRAC.....	19
6.2	Palvelimien varmuuskopiot .....	20
7	PALVELINVIRTUALISOINTI .....	21
7.1	Käyttöönotto ja konfigurointi.....	22
7.1.1	Datastoret.....	23
7.1.2	Kytkimet .....	24
7.1.3	Lähiverkot.....	26
7.1.4	Virtuaalikoneet .....	27
7.1.5	Etäkäytettävyys .....	28
8	KAMERAVALVONTAJÄRJESTELMÄ .....	30

8.1	Agent DVR.....	32
8.2	Viimeistely.....	34
9	POHDINTA.....	35
	LÄHTEET.....	36
	LIITTEET.....	37

## KÄYTETYT MERKIT JA LYHENTEET

GHz	Gigahertz
GB	Gigabit
DNS	Domain Name System
NTP	Network Time Protocol
SSD	Solid-state drive
NFS	Network File System
iDRAC	Integrated Dell Remote Access Controller
PTZ	Pan Tilt Zoom
PoE	Power over Ethernet

## 1 JOHDANTO

On monia syitä, miksi monet yritykset ja koulut investoivat virtuaalipalvelimiin. Hyvänä esimerkkinä on tällä hetkellä koronapandemian tuomat ongelmat, jotka vaikuttavat esimerkiksi koulujen lähiopetuksen järjestämiseen. Virtuaalipalvelimet tarjoavat hyvät puitteet oppilaitoksille etäopiskeluun. Yrityksille ja yhtiöille virtuaalipalvelimet tarjoavat kustannussäästöjä tietotekniikan hankinnassa sekä varmemman ja luotettavamman palvelinympäristön, jota on helpompi päivittää, ylläpitää ja hallita. Palvelin itsessään on erittäin tehokas tietokone, jonka tarkoitus on ajettavien ohjelmistojen avulla ja välityksellä, tarjota erilaisia palveluja muille ohjelmille joko tietokoneverkon välityksellä tai paikallisesti samassa tietokoneessa. Palvelimen virtualisoinnilla saadaan palvelimien resurssit hyödynnettyä tehokkaasti ja ohessa palvelimesta ja sen resursseista tulee helposti etäkäytettäviä

Opinnäytetyön aiheena oli automaatiotekniikan oppimisympäristön palvelinvirtualisointi. Projektin tavoitteena oli saada Lapin ammattikorkeakoululle tilatut palvelimet virtualisoitua toimivaksi oppimisympäristöksi. Opinnäytetyö käsittelee kolmea projektissa toteutettua osa-aluetta: palvelimien käyttöönotto ja konfigurointi, palvelimien kytkentä ja projektin dokumentointi. Lisäksi projektissa tehtiin virtuaalipalvelimien ympärille kameravalvontajärjestelmä, joka myös käsitellään tässä opinnäytetyössä. Opinnäytetyön tuloksia on tarkoitus hyödyntää Lapin ammattikorkeakoulun tekniikanalan opetuksessa.

## 2 VIRTUALISOINTI

### 2.1 Virtualisointi yleisesti

Virtualisointi on tietotekniikan prosessi, jossa jaetaan fyysiset laitteet loogiseksi resurssiseksi, jotka ovat perinteisesti sidoksissa laitteistoon. Virtualisoinnin avulla voidaan siis käyttää fyysisen resurssin, kuten palvelimen tai massamuistin koko kapasiteettia jakamalla sen ominaisuudet monille käyttäjille tai ympäristöille loogisena. Tällä tarkoitetaan sitä, että yhden koneen laitteistoa voidaan käytännössä hyödyntää useampana laitteena. (Ekurssit 2021c.)

### 2.2 Virtualisoinnin hyödyt

Virtualisointi edistää fyysisten laitteiden käyttöastetta, mikä taas lisää kustannustehokkuutta ja pienentää itse laitekannan kokoa, kun fyysisiä palvelimia ja laitteita ei välttämättä tarvitse olla niin paljoa. Ylläpidon kannalta virtualisointi helpottaa hallinnoimaan IT-infrastruktuuria helpommin, nopeammin ja vähemmällä työllä. Virtualisointi parantaa myös IT-infrastruktuurin joustavuutta ja mukautuvuutta. Koska resurssien käyttöä pystyy käyttämään monipuolisemmin ja helpommin, onnistuu hallinta myös etäyhteyden avulla. Suurena etuna ovat myös virtualisoinnin avulla saavutetut pienemmät ylläpitokulut, esimerkkinä fyysisten palvelimien siirtäminen paikasta toiseen lisää merkittävästi työtä, mikä on rahaa kuluttava prosessi. Virtuaalipalvelimet sen sijaan voidaan siirtää helposti suoraan verkon ylitse fyysiseltä virtualisointipalvelimelta toiselle palvelimelle. (Ekurssit 2021c.)



### 2.3 Virtualisoinnin haasteet

Vaikka virtualisointi helpottaa ja nopeuttaa palvelinten ylläpitoa, virtualisointi ei tarkoita, että ylläpitohenkilökunnan pätevydestä voidaan karsia. Virtualisointipalvelinten ylläpitäjien täytyy olla asioihin perehtyneitä ja päteviä, jotta esimerkiksi virtuaalipalvelimen tehokkuus pysyy optimaalisena. Virtuaalisuus voi tuoda tietoturvaongelmia, minkä vuoksi palvelimesta voi tulla haavoittuva haittaohjelmille tai kybervakoilulle, jos palvelinta ei hallita ja päivitetä tarpeellisesti. (Golden 2009, 59–60.)

### 2.4 Virtualisoinnin historiaa

Virtualisoinnin kehittämisen aloitti 1960-luvun alussa IBM:n nimisen yrityksen toimesta. IBM halusi kehittää tavan, jolla yksi fyysinen kone saataisiin jaettua moneen virtuaalikoneeseen. Tuohon aikaan keskusyksiköt olivat kalliita ja sen vuoksi alettiin miettimään, miten yhden koneen resurssit, saataisiin jaettua mahdollisimman tehokkaasti käytön maksimoimiseksi. (Husu 2020.)

### 3 VIRTUALISOINNIN KÄYTTÖKOHTEET

Yritykset ja yhtiöt ottavat virtuaalipalvelimia käyttöön yleensä taloudellisen tai teknisten perusteiden vuoksi. Virtuaalipalvelimilla yhtiöt ja yritykset takaavat varmemman käytettävyyden, tuotekehityksen ja pystyvät parantamaan tai jakamaan yrityksessä olevat resurssit ja sovellukset. Palvelinvirtualisointia voidaan hyödyntää niin suunnittelu- kuin teollisuustehtävissä eli virtualisointi on helppo prosessoida yritykselle sopivaksi. Oppilaitoksille virtualisointi tarjoaa joustavuutta henkilökunnalle opettamiseen ja hyvät puitteet lähi- ja etäopiskeluun.

Virtualisointi voidaan toteuttaa monella eri tavalla, mutta yleisimmät tavat kuitenkin ovat: palvelinvirtualisointi, työpöytävirtualisointi, verkkovirtualisointi, sovellusvirtualisointi ja tallennusvirtualisointi. Virtualisoinnin tekniikat eroavat toisistaan käyttökohteen mukaan. (Ekurssit 2021c.)

#### 3.1.1 Työpöytävirtualisointi

Samaa käyttöjärjestelmää voidaan käyttää monessa eri työpisteessä virtualisoidulla se. Käyttöjärjestelmä ja sovelluskerros voidaan kuitenkin erottaa, joten sovellukset eivät kuluta työaseman kapasiteettia. Tällöin työasemien ei tarvitse olla tehokkaita ja voidaan käyttää edullisempia päätelaitteita. Päivitykset voidaan tehdä yhdeltä koneelta. (Ekurssit 2021c.)

#### 3.1.2 Verkkovirtualisointi

Verkkovirtualisoinnin tarkoitus on yhdistää useat verkot yhdeksi virtuaaliverkoksi, joka joustavuutensa ansiosta voi jakaa tietoliikennettä tarpeen mukaan. Samoin siinä käytetään hieman eri tiedonsiirtotekniikkaa, kuten pakkaus- ja kiihdytystekniikkoja, joten tiedonsiirto tehostuu. Koska tietoverkko on virtuaalista ja joustavaa, virhemarginaalit pienenevät ja tiedostot liikkuvat varmemmin. (Ekurssit 2021b.)

### 3.1.3 Sovellusvirtualisointi

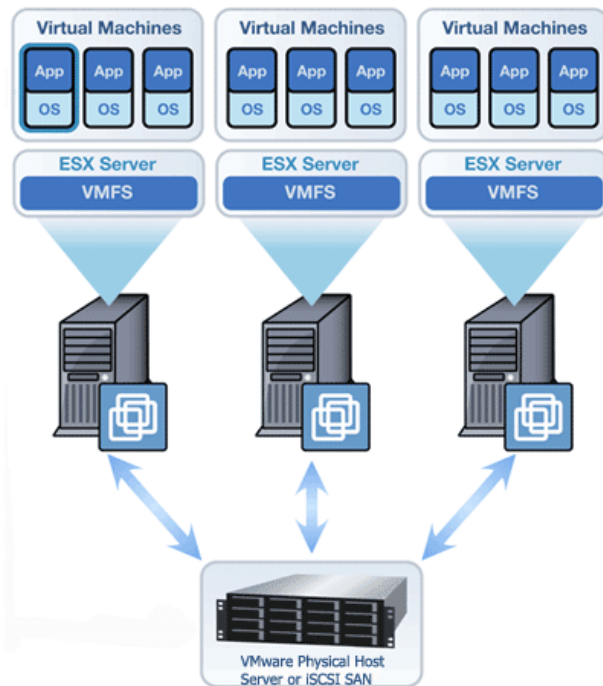
Sovellusvirtualisointi tarkoittaa lähinnä eri ohjelmien ajoa samalla tietotekniikkalaitteella, vaikka nämä eivät olisikaan soveltuvia samalle käyttöjärjestelmälle. Hyötynä sovellusvirtualisoinnille on ohjelmien hallinta perinteistä asennusta helpompaa. Virheet ja konfliktit pienenevät ja ohjelmien ajo jopa eri käyttöjärjestelmissä on varmempaa. Tätä helpottaa myös, jos käytössä on eri ryhmiä, joissa käytetään eri käyttöjärjestelmiä. Myös eri ikäisissä käyttöjärjestelmissä on mahdollisuus käyttää samanlaisia ohjelmia. Tämä mahdollistaa esimerkiksi uusimpien käyttöjärjestelmien vaihdon ilman, ettei tarvitse vaihtaa kaikkia käytössä olevia ohjelmia samalla kertaa. (Ekurssit 2021a.)

### 3.1.4 Tallennusvirtualisointi

Tallennustilan virtualisoinnissa isäntälaitteen fyysinen muisti jaotellaan ja allokoidaan virtuaalilaitteelle dynaamisesti. Tallennusvirtualisointi tällä tavalla on mahdollista myös käyttöjärjestelmän itsensä sisällä, mutta isäntälaitteen muut allokoimattomat muistilohkot eivät näy virtuaalikäyttöjärjestelmälle. Jos tallennettava tieto on tärkeää, voidaan tallennusvirtualisoinnilla mahdollistaa varmennus-, kahdennus- ja etäpeilausratkaisut. Näiden avulla on helppoa tehdä tietoturvaratkaisuja niin, että laitteistot pitävät itse huolen esimerkiksi varmuuskopioinneista. (Ekurssit 2021b.)

#### 4 PALVELINVIRTUALISOINNIN TAUSTAA

Palvelimissa virtualisointi tarkoittaa yksinkertaisesti kuvattuna sitä, että yhdessä fyysisessä laitteessa ajetaan yhden käyttöjärjestelmän sijasta useita virtuaalipalvelimia ja koneita. Niistä kukin pyörittää itsenäisesti omaa käyttöjärjestelmäänsä. Palvelinvirtualisointi on eniten hyödynnetyistä virtualisoinnin osa-alueista. Kuva 1 havainnollistaa, kuinka virtuaalipalvelimet toimivat. (Mäntylä 2008.)



Kuva 1. Palvelinvirtualisoinnin toimintaperiaate (Integrated computer services 2021)

## 4.1 VMware

Yksi lukuisista palvelinvirtualisointi ohjelmiston tarjoajista on VMware Inc. VMware on yhdysvaltalainen yritys, joka toimittaa virtualisointiratkaisuja ja ohjelmistoja IT-yrityksille. Yrityksen tavoite on tarjota asiakkailleen kustannustehokkaita ratkaisuja, jotka takaavat liiketoiminnan jatkuvuuden, ohjelmistojen elinkaaren ja työpöydän hallinnan. Yritys on perustettu 10.02.1998. Yrityksen ensimmäinen tuote oli Workstation 1.0, joka tuotiin esille vuonna 1999. Julkaisun jälkeen VMware on aina ollut virtuaalimaailman kärjessä. (Muetstege 2018.)

VMware on tuonut markkinoille monenlaisia ohjelmistoja. Osa ohjelmistoista on ilmaisia ja kehittyneemmät maksullisia. VMware tunnetaan muun muassa pilvipalveluista, sovellusmodernisaatio- ja tietoturvatuotteista unohtamatta palvelimien virtualisointituotteita. Viimeisestä kastista yksi yleisimmistä tuotteista on VSphere virtualisointialusta. (Muetstege 2018.)

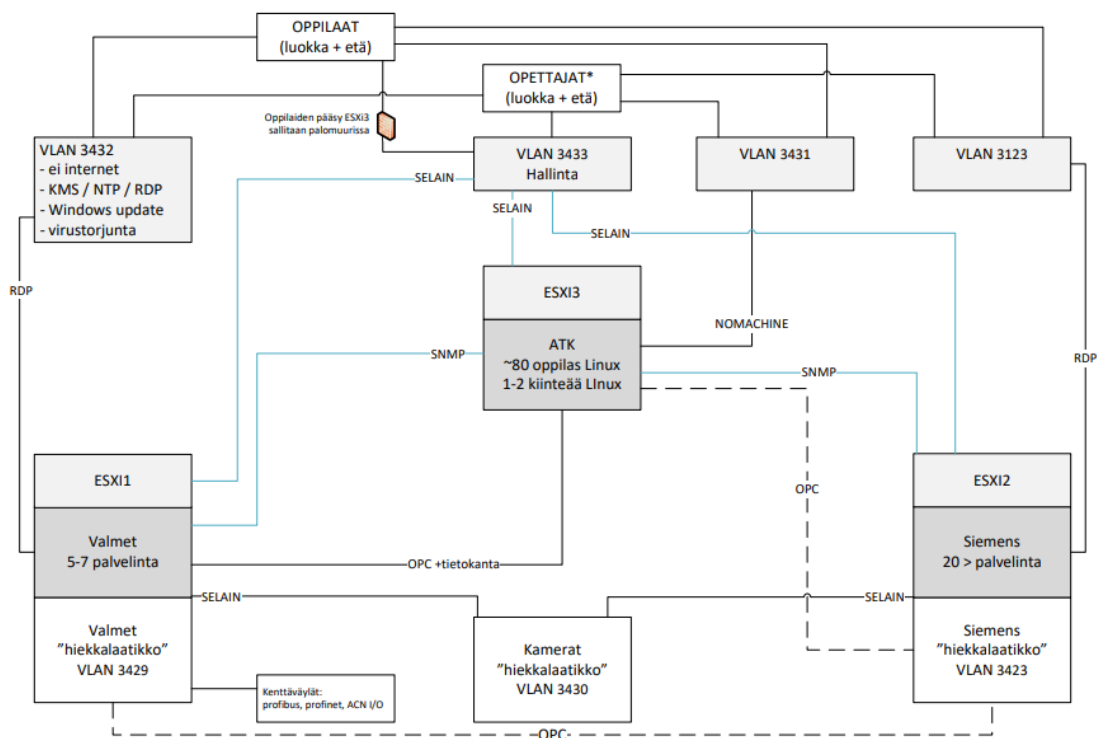
### 4.1.1 ESXi

VMware ESXi on yksi VSpheren tuotepaketin komponenteista. ESXi on tyypin 1 hypervisor, joka käytännössä tarkoittaa, että ESXi ei tarvitse isäntäkäyttöjärjestelmää. ESXi on itsenäinen käyttöjärjestelmä, joka voidaan asentaa suoraan palvelimen kovalevyille tai esimerkiksi USB-muistitikulle. ESXin päälle voidaan asentaa virtuaali- palvelimia ja koneita, joilla on suora yhteys fyysisen palvelimen laitteistoon.

## 5 VIRTUAALIYMPÄRISTÖN LUOMINEN

Virtuaaliympäristöosuudessa käydään läpi, miten virtuaaliympäristö ja valvontakamerajärjestelmä projektissa toteutettiin. Virtuaaliympäristö osuudessa kerrotaan, miten palvelimet konfiguroidaan ja miten VMware ESXi:llä toteutettiin toimiva, kuvan 2 esittämä virtuaalipalvelinympäristö. Palvelinympäristöön tehtiin virtuaalikytkimiä, lähiverkkoja ja virtuaalikoneita.

Valvontakamerajärjestelmän tarkoitus oli parantaa oppimisympäristön etäkäytävyyttä, jotta henkilökunta ja oppilaat pystyvät jatkossa valvomaan koululle tulevaa prosessia etänä. Valvontakamerajärjestelmä tehtiin projektin viimeisessä vaiheessa valmiille virtuaalipalvelimelle.



Kuva 2 Suunnitelma virtuaaliympäristöstä (Palvelinvirtualisointi hankkeen projektidokumentti 2021)

## 5.1 Laitteisto

Virtuaaliympäristöä alettiin perustamaan kolmelle Dellin PowerEdge R740 Server palvelimelle (Kuva 3). Yhdestä palvelimesta löytyi seuraavia komponentteja: Intel Xeon Gold suoritin, jossa on 16 ydintä ja on kellotaajuudeltaan 2.9 GHz. Keskusmuistia palvelimesta löytyi 382 GB ja massamuistia noin 6 teratavua. Lisänä palvelimiin oli valmiiksi asennettu kaksi 32 GB microSD korttia, joihin ESXi oli asennettu. Ohjelmistoa palvelimien mukana tuli seuraavasti: esiasennettu VMware ESXi 6.7 ja lisenssit Dellin OpenManage Enterpriseen ja iDRAC:n, joista kerrotaan tarkemmin luvussa 6.1 iDRAC ja Dell OpenManage järjestelmä.



Kuva 3 Koululle tilatut palvelimet

## 5.2 Palvelimien käyttöönotto ja konfigurointi

Palvelimien käyttöönotto aloitettiin johdottamalla palvelimet. Palvelimet kytkettiin tarvittavilla virtajohdoilla ja verkkokaapeleilla, joilla ne liitettiin kytkimiin. Palvelimet kasattiin aluksi tilapäiseen huoneeseen, josta ne oli tarkoitus siirtää konfiguroituna ja valmiina palvelinhuoneeseen. Palvelintyöt aloitettiin päivittämällä esi-asennettu VMware ESXi 6.7 uudempaan ESXi versioon 7.1. Liitteet 1–8 sisältävät asennusohjeet järjestyksessä. Päivittäminen ei paljoa eronnut Linux käyttöjärjestelmän asennuksesta.

Aluksi ladattiin VMwaren sivuilta uuden ESXi:n tiedostot "buuttaavalle" USB-tikulle ja siirrettiin se palvelimen USB-porttiin. Palvelin käynnistettiin ja F2 - painikkeella avautui Dellin biosmenu. Biosmenun sarakkeesta valitsemalla "Boot Manager" välilehden saatiin auki käynnistyksen päävalikko. "Oneshot UEFI bootaus" sarakkeen valitsemalla edettiin valikkoon, missä hyväksyttiin EULA:n lisenssisopimus. Hyväksymisen jälkeen pystyi valitsemaan tallennuslaitteen, jolle asennus tai päivitys suoritettiin. Tallennuslaitteeksi määritettiin microSD - kortti, jonka jälkeen valittiin ESXi:n asennustapa, projektin tapauksessa pelkkä ESXi:n päivitys riitti.

Palvelimien konfigurointi aloitettiin määrittämällä palvelimien nimet. Palvelimia oli yhteensä kolme ja ne nimettiin AMKESXi1-3. Palvelimille laitettiin salasanat sekä päivitettiin IP-osoitteet, aliverkot, DNS-osoitteet, yhdysverkot ja poistettiin käytöstä IPv6 - osoitteet. Liitteet 9–11 osoittavat osan vaiheista, miten palvelimet konfigurointiin.

## 5.3 RAID5

Palvelimet hyödyntävät RAID5 tekniikkaa, jolla pystyy yhdistämään kaikkien palvelimien kiintolevyt yhdeksi loogiseksi levyksi. RAID5:n käyttöönotto löytyi palvelimien järjestelmä asetuksista. "Disk group properties" sarakkeen alta pääsi kärsiksi asetukseen, mistä Raid laitettiin aktiiviseksi.



#### 5.4 iDRAC - asetukset

iDRAC on fyysisesti asennettu emolevyn ohjainkorttiin, jota voidaan hallita etänä. iDRAC:n avulla järjestelmänvalvojat voivat päivittää ja hallita Dell-järjestelmiä, vaikka eivät itse olisi paikan päällä ja palvelin olisi sammutettu. iDRAC:n avulla voidaan seurata palvelimien tilaa monipuolisesti. Esimerkkinä iDRAC:lla pystyy seuraamaan palvelimen kunnon lisäksi, prosessorin ja muiden komponenttien kuntoa sekä lämpötiloja.

Palvelimien konfiguroimisen lopussa määritettiin iDRAC asetukset. Palvelimien iDRAC asetuksista määriteltiin nimet, verkkotunnukset, IP osoitteet, DNS- serveriosoitteet, josta pääsisi valvomaan iDRACia selaimen kautta. Lisäksi asetuksista valittiin minne IP-osoitteeseen iDRAC lähettää mahdolliset hälytykset ja lokit.

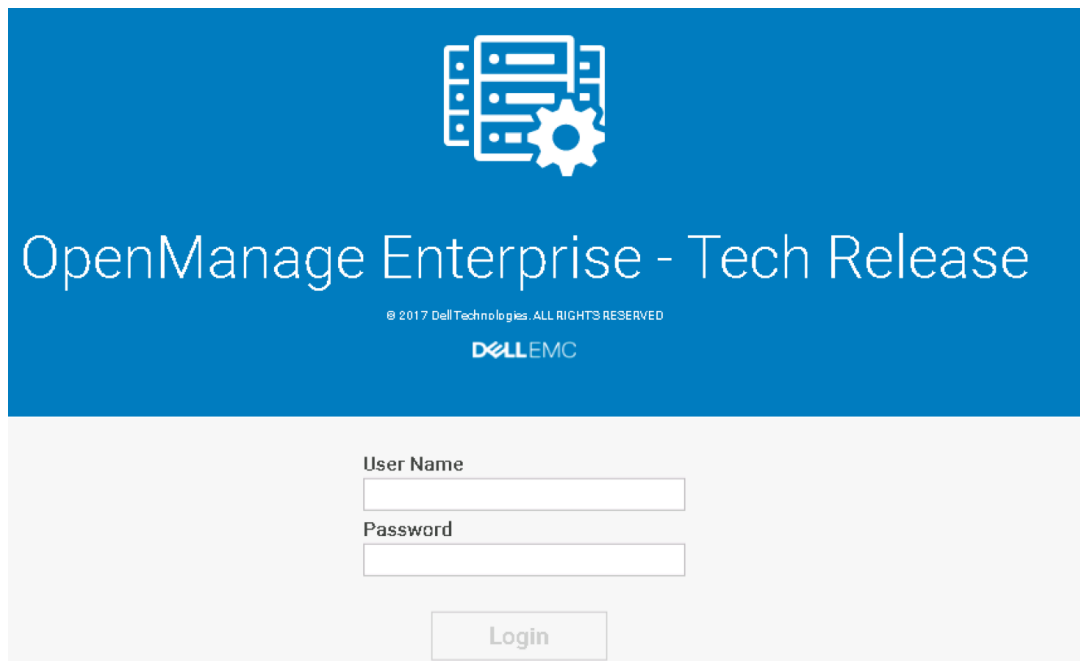
## 6 PALVELIMIEN KUNNONVALVONTA

Palvelimien kuntoa valvotaan, jotta ne pysyvät käyttökuntoisina ja turvallisina. Virheiden sattuessa täytyy palvelimien varmuuskopiointi olla kunnossa, jotta mahdolliset virheet saadaan korjattua. Tapahtuneista virheistä on hyvä saada loikit talteen, jotta virheet voidaan korjata ja niitä ei synny uudestaan. Palvelimien kuntoa on myös hyvä tarkkailla sen suhteen, ettei sinne synny liikaa kuormaa tai esimerkiksi levytila ei lopu kesken. Palvelimet ja sovellukset pysyvät optimaalisina päivittämällä sovellukset ja mahdolliset käyttöjärjestelmät ajan tasalle. Projektin tapauksessa palvelimien kuntoa takaa myös 7 vuoden takuu ja Dell lupasi palvelimien oston yhteydessä tukipalveluita aina seuraavana arkipäivänä 4 vuoden saakka.

Palvelimien kuntoa valvotaan Dellin EMC OpenManage ohjelmistolla. Dell EMC järjestelmä tarjoaa hallintaratkaisuja, jotka auttavat IT-järjestelmänvalvojia asentamaan, päivittämään, valvomaan ja hallitsemaan projektissa käytettyjä fyysisiä ja virtuaalisia palvelimia. Palvelimien etuosassa on myös itsessään led-valot, jotka indikoivat palvelimen kuntoa. Esimerkiksi sininen valo tarkoittaa, että palvelin on kunnossa tai välkkyvä keltainen indikoi, että palvelimen virranlähteessä on ongelma.

## 6.1 Dell OpenManage järjestelmä ja iDRAC

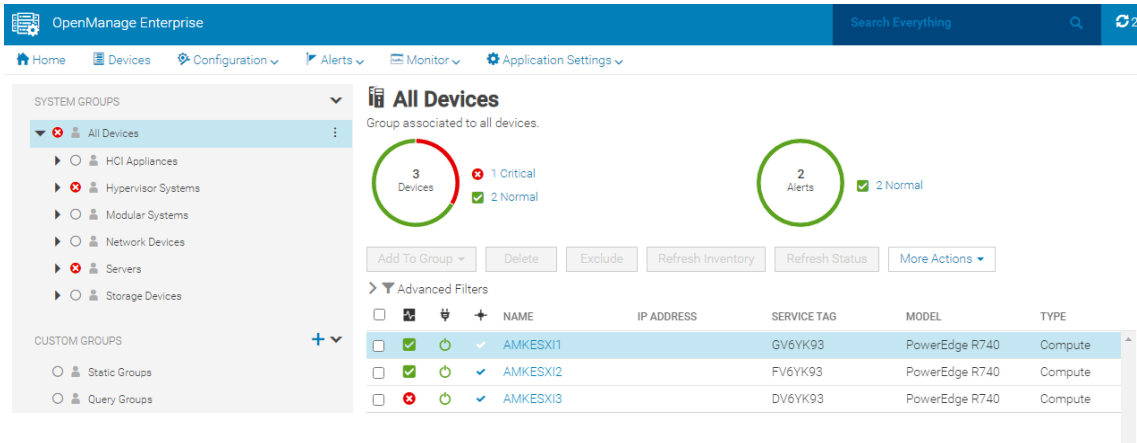
Palvelimien konfiguroinnin jälkeen seuraavana vaiheena oli Dell OpenManagen käyttöönotto. Ohjelmisto ladattiin Dellin sivustolta ja asennettiin AMKESXi1:lle yhdeksi virtuaalikoneeksi. Dellin OpenManage järjestelmään pääsi käsiksi syöttämällä verkkoselaimen hakukenttään, luvussa 5.2 määritetyt palvelimien IP-osoitteet. IP-osoitteen syötettyä aukesi kuvan 4 mukainen kirjautumisnäkyvä, johon kirjautumistunnukset syöttämällä pääsi käyttämään Dell OpenManage järjestelmää.



Kuva 4 Dell OpenManagen kirjautumissivu

OpenManagen konfigurointi aloitettiin etsimällä palvelimet käyttöliittymän "discover Devices"- sarakkeella. "Discover Devices"- välilehden auettua kenttään syötettiin laitteiden IP-osoitteet ja laitteen tyyppi, tässä tapauksessa aiemmin määritetyt ESXi osoitteet ja laitteen tyyppi ESXi palvelin. Laitteiden löydyttyä käyttöliittymä näytti kuvan 5 mukaiselta. Laitteiden kuntoa pystyi valvomaan käyttöliittymän kautta. Laitteille piti vielä määrittellä osoitteet, joihin mahdolliset hälytykset tulisivat, hälytystavat (SMS/sähköposti) ja NTP aika-asetukset. Mahdolliset hälytys - sähköpostit ja virheloki - ilmoitukset osoitettiin menemään suoraan ylläpitä-

jille. OpenManageen tehtiin kaksi käyttäjää "admin" jolla on kaikki oikeudet käyttää ja muokata asetuksia. Toiseksi käyttäjäksi luotiin "student" - käyttäjä, jolla on vain katseluvaltuudet ohjelmaan.



Kuva 5 Dell OpenManage etusivu

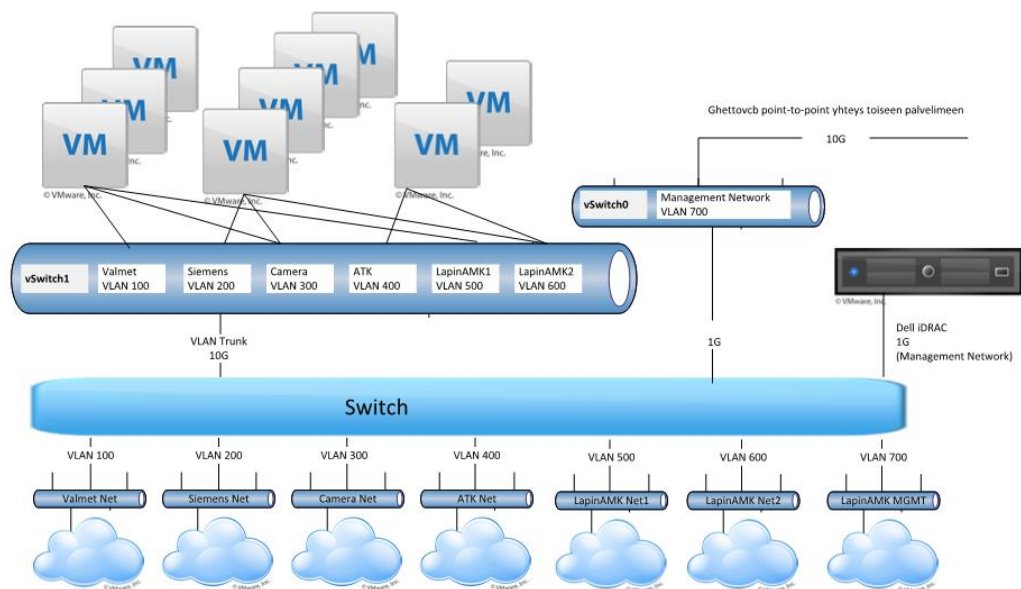
## 6.2 Palvelimien varmuuskopiot

Palvelimista tulee ottaa varmuuskopiot, koska jos joku kolmesta palvelimesta menee vikatilaaan, on kuitenkin tiedostot varmuuskopioitu toiselle palvelimelle. Tässä osiossa käydään läpi, miten palvelimien ESXi1 ja ESXi2 välille tehdään varmuuskopio polku käyttäen GhettoVCB ohjelmaa.

Varmuuskopiointiohjelman tekeminen aloitettiin luomalla palvelimille ESXi1 ja ESXi2 alustoille TrueNas virtuaalikone, jonne määriteltiin yhden teratavun kokoinen NFS-jako. ESXi alustoille määriteltiin oma virtuaalikytkin ja palvelimet liitettiin toisiinsa 10 gigabitin verkkoyhteydellä. Kyseinen verkkoliityntä on erillään muista palvelimien verkkoliikenteistä. GhettoVCB-ohjelma ladattiin heidän kotisivuiltaan. Ohjelma asenettiin palvelinkoneelle käyttäen GhettoVCB lähdekoodia. GhettoVCB-ohjelma ajastettiin lähdekoodilla suorittamaan varmuuskopion tekeminen tietyn aikavälin ajoin tärkeimmistä virtuaalikoneista. GhettoVCB asennettua, alkoi palvelimelle tulemaan ongelmia, koska ohjelma haittasi VMwaren päivityksiä. Ongelma ratkaistiin poistamalla GhettoVCB-ohjelma, mutta kopioimalla GhettoVCB:n käyttämä skripti suoraan palvelimen hakemistoon, saatiin toteutettua ohjelman toiminta palvelimelle ilman haittavaikutuksia.

## 7 PALVELINVIRTUALISOINTI

Tässä osuudessa käydään läpi, miten palvelinympäristö perustettiin käyttämällä ESXi virtuaaliympäristöä. Virtuaaliympäristön luonnissa tehtiin periaatteeltaan kuvan 6 kaltainen ympäristö. Jotta olisi mahdollista tehdä kuvan tapainen toteutus, täytyi virtuaaliympäristö konfiguroida ja tehdä ympäristöön virtuaalikoneita, virtuaalikytkimiä, lähiverkkoja ja datastoreja.



Kuva 6 Suunniteltu virtuaaliympäristö (Palvelinvirtualisointi hankkeen projektidokumentti 2021)

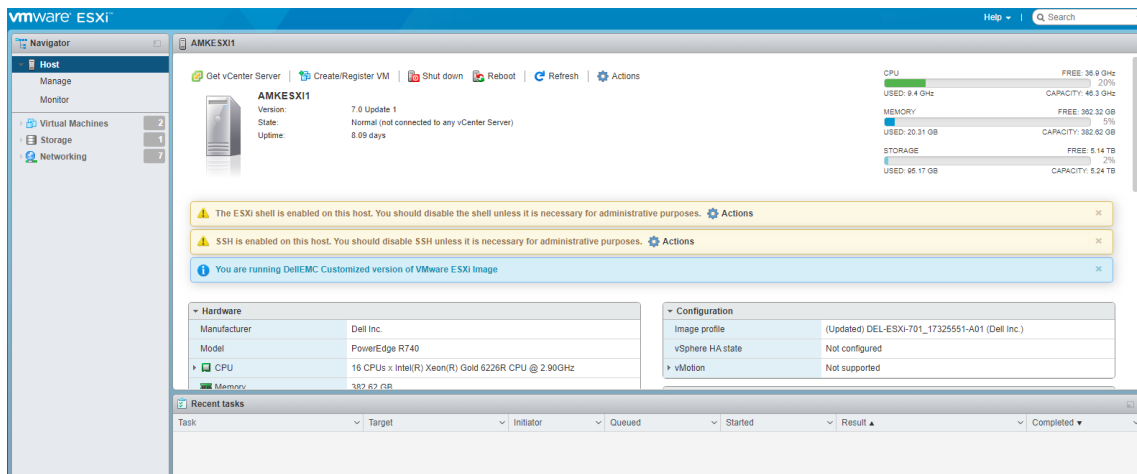
## 7.1 Käyttöönotto ja konfigurointi

Kullekin palvelimelle määriteltiin ESXi - hallintaosoitteet, joilla pääsee ESXi virtuaaliympäristöön. ESXi ympäristöön pääsee samalla tavalla kuin aiemassa kappaleessa Dellin OpenManage - ympäristöön, eli syöttämällä palvelimen hallintaosoite selaimen hakukenttään. Osoitteen syötettyä aukeaa kuvan 7 mukainen kirjautumissivu, johon syöttämällä käyttäjänimen ja salasanan avautuu kuvan 8 kaltainen VMwaren hallinta – sivu.



Kuva 7 VMware kirjautumissivu

Konfiguroiminen aloitettiin asettamalla ESXille oikea NTP- aika. Jokaiselle palvelimelle aktivoitiin VMwaren VSphere 7 hypervisor lisenssi. Lisäksi palvelinympäristöön tehtiin erilaisia käyttäjiä, kuten esimerkiksi opiskelijakäyttäjää, jolla on vain mahdollista luoda virtuaalikone ja katsella ESXi ympäristöä.



Kuva 8 VMware hallintasivu

### 7.1.1 Datastoret

Datastoret ovat palvelimien tietovarastoja, joissa voi tallentaa tai hallita dataa, ohjelmia ja tietokantoja tai vaikka yksinkertaisia tiedostoja.

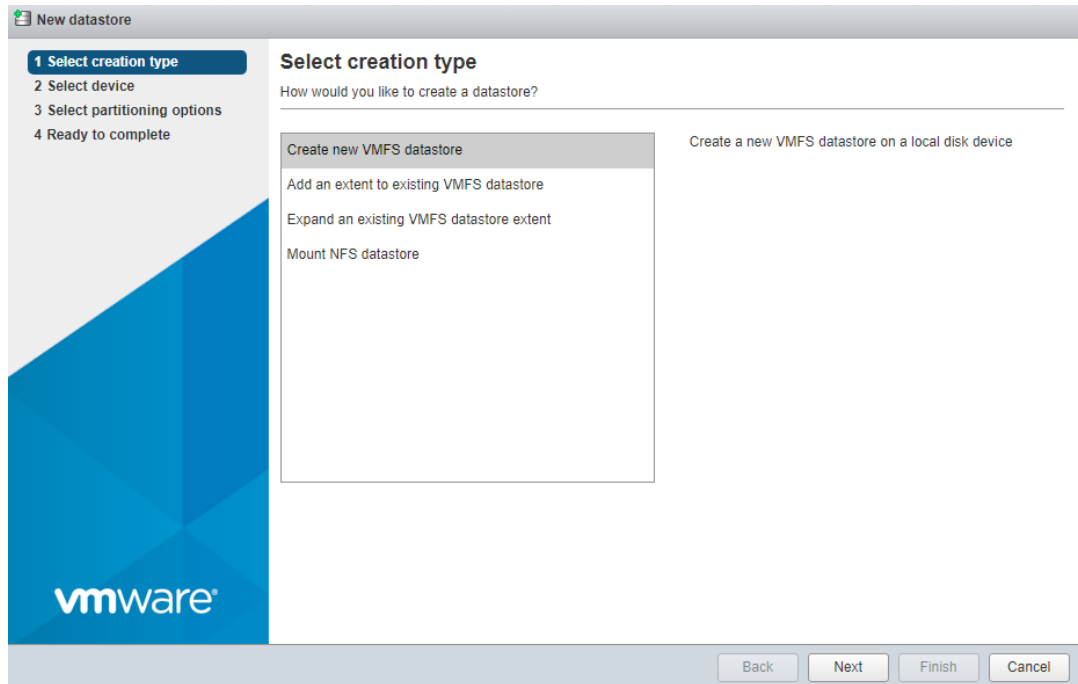
Virtuaalipalvelimelle tehtiin 3 virtuaalista datastorea. Palvelimen SD-levyistä muodostettiin noin 6Tt kokoinen "Datastore1", jota palvelimella olevat virtuaalikooneet hyödyntävät. Kaksi muuta datastorea otettiin käyttöön varmuuskopioinnille, josta on selitetty aikaisemmalla varmuuskopio osuudella.

Datastorejen tekeminen alkoi kuvan 8 vasemmassa reunassa näkyvästä "Storage" -palkista, jota klikkaamalla pääsi kuvan 9 valikkoon.

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin provisioning	Access
Datastore1	SSD	5.24 TB	15.53 GB	5.22 TB	VMFS6	Supported	Single
esxi1nfs	Unknown	984.24 GB	128 KB	984.24 GB	NFS	Supported	Single
esxi2nfs	Unknown	984.24 GB	20.46 GB	963.78 GB	NFS	Supported	Single

Kuva 9 Datastore välilehti

Valikossa näkyy jo 3 mainittua datastorea, joiden yläpuolelta pystyi valitsemaan sarakkeen "Create new storage" avautui kuvan 10 mukainen välilehti. Datastore nimettiin ja sille päätettiin minkälaista muistia datastore on, tässä tapauksessa SSD. Lopuksi datastorelle annettiin tarvittava määrä kapasiteettia.

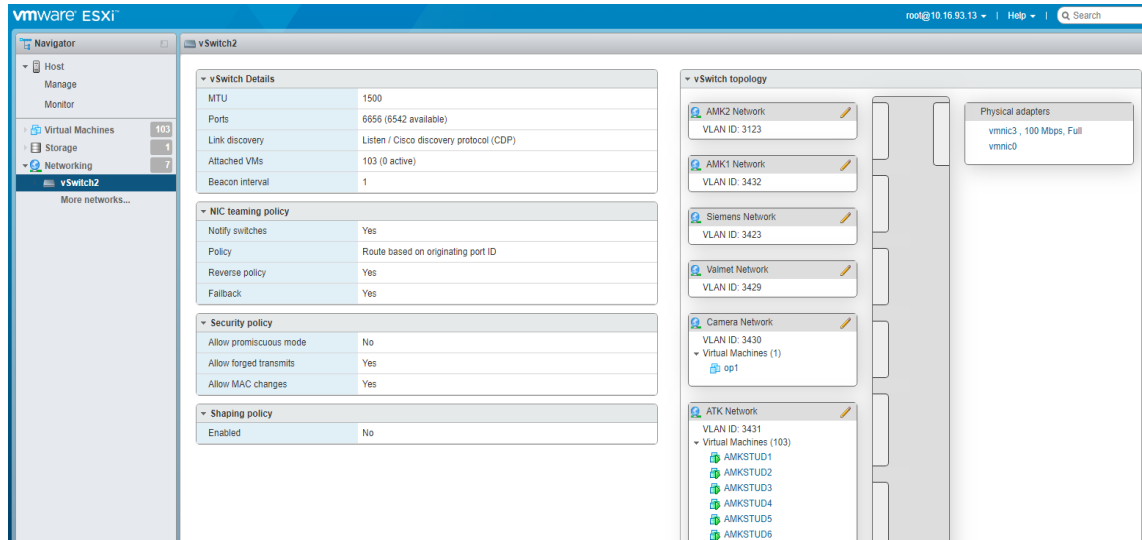


Kuva 10 Datastoren luonti-ikkuna

### 7.1.2 Kytkimet

Palvelimiin tehtiin virtuaalikytkimiä eli vSwitchejä, jotta tietoliikenne pysyy järjestyksessä ja tietyt palvelimet sekä virtuaalikoneet pystyvät käyttämään tarvittavia palvelinympäristön resursseja. Kuva 11 indikoi miten vSwitch2 jakaa lähiverkostolta tulevat tietoliikenteet fyysiselle palvelimelle. Tarkemmin selitettynä vSwitch2:een menee muun muassa kamerajärjestelmän, ATK eli opiskelijakone verkoston ja kahden oppimisympäristön lähiverkot, joiden tietoliikenteen kytkin kuljettaa palvelimeen





Kuva 11 vSwitch2 jakaa lähiverkot kytkimelle

Virtuaalikytkimien tekeminen aloitettiin ESXi liittymän vasemmasta reunasta "Networking" - sarakkeesta. Kuva 8 näyttää vasemmassa reunassa networkin näkymän, jota painalla pääsi "Virtual switches" - sarakkeeseen. Kuvassa 12 huomataan jo kolme projektissa tehtyä virtuaalikytkintä vSwitch0 -vSwitch2. Uuden virtuaalikytkimen tekeminen aloitettiin painamalla "Add standard virtual switch" - saraketta. Virtuaalikytkimelle annettiin nimi, määriteltiin mahdolliset portit eli palvelimien verkkoliitännät mitkä kulkevat kytkimen kautta.

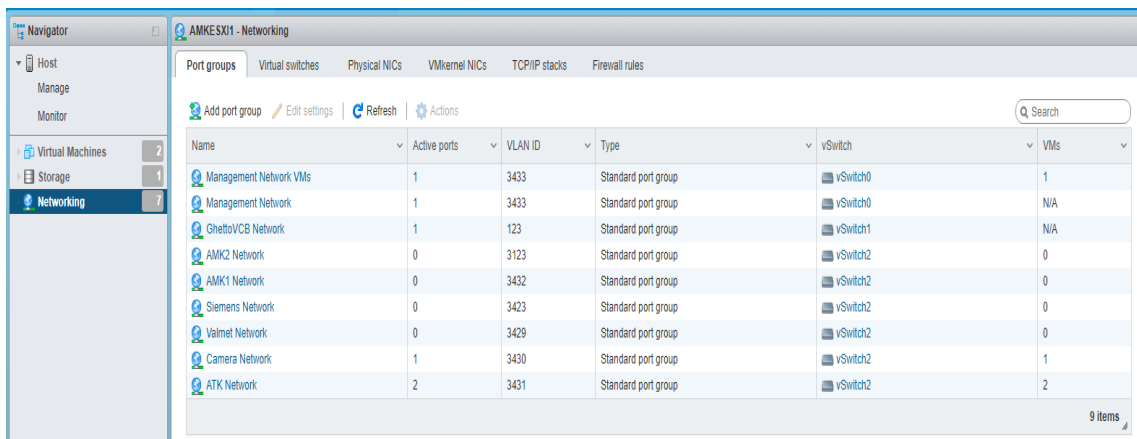
Name	Port groups	Uplinks	Type
vSwitch0	2	1	Standard vSwitch
vSwitch1	1	1	Standard vSwitch
vSwitch2	6	2	Standard vSwitch

Kuva 12 Virtuaalikytkimet vSwitch0-2

### 7.1.3 Lähiverkot

Virtuaaliympäristöön luotiin virtuaaliset lähiverkot eli VLAN:t kaikille verkon osaluueille, jotta tietoliikenne olisi helppo ylläpitää ja siirtää edellä mainittuihin virtuaalisiin kytkimiin. Kuva 13 on hyvä esimerkki, millaisia lähiverkkoja virtuaaliympäristöön toteutettiin. Osuudessa käydään läpi, miten tehtiin ”Management network” eli virtuaalipalvelimien hallinta -lähiverkko.

Lähiverkon luominen aloitettiin ESXi verkkoliittymän navigointi palkin ”Network” -sarakkeesta. Kuvassa 13 näyttäytyy verkkoliittymien yllä ”Add port group” -painike, josta pääsi tekemään uuden lähiverkon. Lähiverkon tekeminen on lyhyt toimenpide, sillä aluksi päätetään mihin virtuaaliseen kytkimeen lähiverkko kytkeytyy. Tämän lisäksi täytyy lähiverkko nimetä ja sille annetaan VLAN ID, millä tietoliikenne tunnistetaan sitä kuljettaessa. Lähiverkon voi myös laittaa kulkemaan useampaan kytkimeen, mutta hallintaverkon kanssa tälle ei ollut tarvetta.



The screenshot shows the vSphere Network configuration page for host AMKESX11. The 'Port groups' tab is selected, displaying a table of existing port groups. The table has columns for Name, Active ports, VLAN ID, Type, vSwitch, and VMs. The 'Add port group' button is visible at the top left of the table area.

Name	Active ports	VLAN ID	Type	vSwitch	VMs
Management Network VMs	1	3433	Standard port group	vSwitch0	1
Management Network	1	3433	Standard port group	vSwitch0	N/A
GhettoVCB Network	1	123	Standard port group	vSwitch1	N/A
AMK2 Network	0	3123	Standard port group	vSwitch2	0
AMK1 Network	0	3432	Standard port group	vSwitch2	0
Siemens Network	0	3423	Standard port group	vSwitch2	0
Valmet Network	0	3429	Standard port group	vSwitch2	0
Camera Network	1	3430	Standard port group	vSwitch2	1
ATK Network	2	3431	Standard port group	vSwitch2	2

Kuva 13 Lähiverkot

#### 7.1.4 Virtuaalikoneet

Palvelimille luotiin useita virtuaalikoneita muun muassa palvelimien- ja kamerajärjestelmän hallintaan. Lisäksi virtuaalikoneita tehtiin oppimisympäristöiksi eri palvelimille. Koululle tilattiin Valmetin automaatiojärjestelmät, joihin pääsisi käsi- virtuaalipalvelimien kautta. Palvelimille tehtiin testin vuoksi noin 100 kappaletta virtuaalikoneita, joita osaa voidaan jatkossa hyödyntää esimerkiksi automaation tietotekniikassa. Virtuaalikoneiden myötä opiskelijan ei tarvitse asentaa omalle koneelle kurssilla tarvittavia ohjelmia, plussana kurssinvetäjät pystyvät myös hallitsemaan virtuaalikoneita ongelmien sattuessa. Tässä osuudessa käydään läpi esimerkkinä kamerajärjestelmä virtuaalikoneen luomisen.

Virtuaalikoneiden tekeminen alkoi VMware ESXi:n etusivulla sarakkeesta ”virtual Machines”. Painamalla ”Create / Register VM” pääsee virtuaalikoneen luonti valikkoon kuva 14. Koneita tehdessä aluksi valitaan koneen nimi ja mitä ESXi-versiota virtuaalikone tukee. Seuraavaksi virtuaalikoneen luonnissa pystyy valitsemaan virtuaalikoneen käyttöjärjestelmän esimerkiksi Windows tai Linux. Viimeisessä sarakkeessa valitaan käyttöjärjestelmän versio Windowsin käyttöjärjestelmien puolelta esimerkiksi Windows 10, Windows Server 2012 tai vaikka Windows XP. Tässä projektissa valvontakamerajärjestelmä virtuaalikoneen nimeksi valikoitui AMKISPY ja käyttöjärjestelmäksi Windows Server 2019.

Name	
<input type="text" value="WINDOWS"/>	
Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.	
Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.	
Compatibility	ESXi 6.7 virtual machine ▼
Guest OS family	Windows ▼
Guest OS version	Microsoft Windows Server 2012 (64-bit) ▼

Kuva 14 Virtuaalikoneen luonti

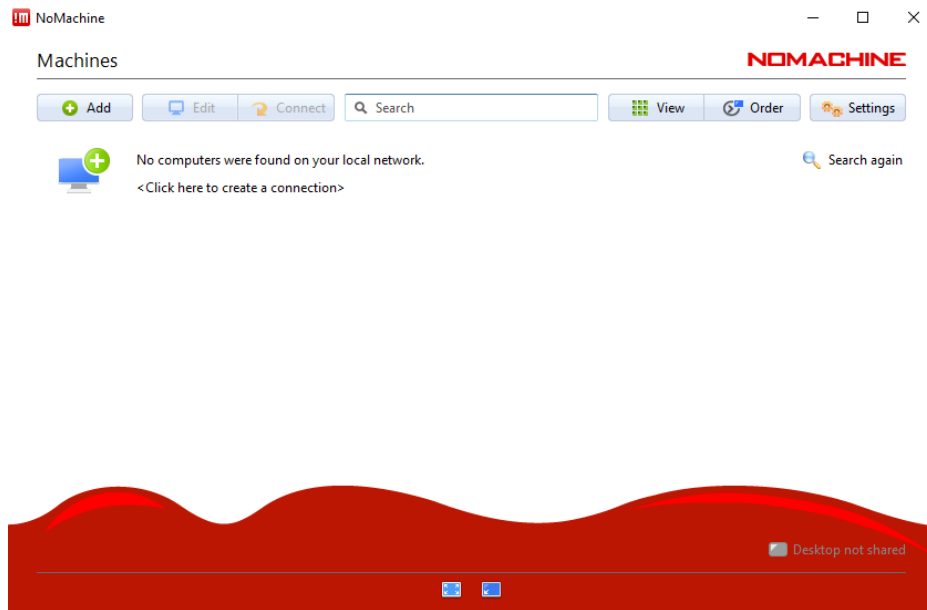
Seuraavaksi virtuaalikoneen luonnissa valitaan, kuinka paljon koneelle annetaan massamuistia. Valvontakamera koneelle asetettiin 200 Gt muistia, mikä on riittävä määrä, jotta kone pystyi tallentamaan valvontakameranauhoituksia runsaasti jatkossa. Virtuaalikoneen luotua, koneelle määriteltiin kuinka paljon prosessoreita ja ram-muistia kone sai ja lisäksi verkot mihin virtuaalikone yhdistettiin. Valvontakamera virtuaalikone yhdistettiin "Camera Network" - verkkoon ja sille annettiin 4 prosessoria ja 4 GB ram muistia, joilla virtuaalikone jaksaisi pyörittää kameraohjelmistoa.

Virtuaalikoneita luotiin myös palvelimien ylläpitoon ja opiskelijakäyttöön. Opiskelijakoneita tehdessä syntyi ongelmia, kun yksittäisen virtuaalikoneen luominen on itsestään pitkä prosessi, koska niitä pitäisi tehdä tuleville kursseille useita kymmeniä. Lapin ammattikorkeakoulun palvelimien mukana tullut VMware lisenssi ei kattanut virtuaalikoneiden kloonauksia, joten virtuaalikoneet täytyi kloonata manuaalisesti skriptien avulla.

#### 7.1.5 Etäkäytettävyys

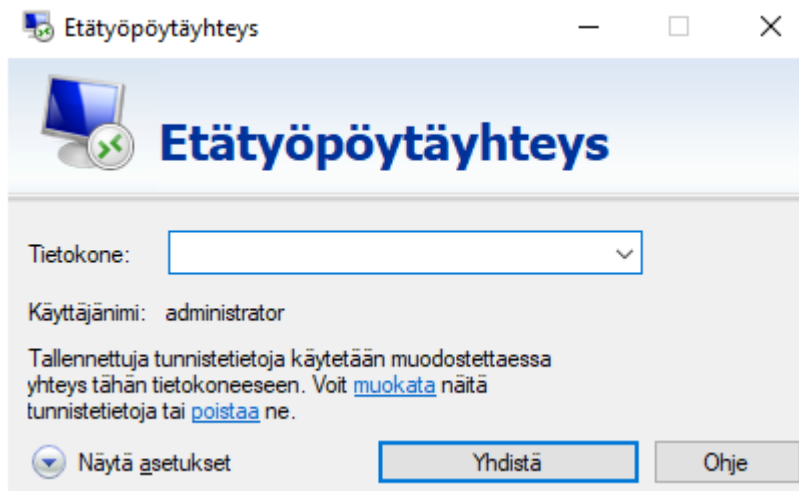
Jotta virtuaalisia koneita pystyy hallitsemaan etänä, niihin täytyy asentaa etätyöpöytäohjelmia. Esimerkiksi Windows-pohjaista virtuaalikonetta pystyy operoimaan Windowsin omalla etätyöpöytäohjelmalla. Osuudessa käydään läpi, miten etätyöpöytä yhteys otettiin käyttöön Windows koneella sekä Linuxilla.

Linux pohjaisten virtuaalikoneiden etähallintaan testattiin NoMachine etätyöpöytäohjelmaa, koska se oli ilmainen ja ennestään tuttu. Ohjelma ladattiin heidän kotisivuiltaan ja ohjelma käynnistyi. Yksinkertaisen asennuksen jälkeen avautui kuvan 15 mukainen ikkuna. "Add" - painikkeella sovellukseen lisättiin etäohjattavan koneen IP-osoite ja virtuaalikone oli näin etäohjattavissa.



Kuva 15 NoMachine kirjautumisikkuna

Windows pohjaisille virtuaalikoneille käytettiin Windowsin omaa etätyöpöytäsovellusta. Sovelluksen löytää jokaisesta suomenkielisestä Windows koneesta hakukenttäsarakeesta hakunimellä Windows ”etätyöpöytäyhteys” tai englanninkielisestä Windowsista hakusanalla ”mstsc”. Windows-etätyöpöytäsovellus ei juuri eroa NoMachinesta. Kuvan 16 tyhjään sarakkeeseen syötetään tietokoneen IP-osoite ja seuraavaan kenttään tietokoneen nimi, jonka jälkeen tietokone on etäohjattavissa.



Kuva 16 Windowsin etätyöpöytäyhteys

## 8 KAMERAVALVONTAJÄRJESTELMÄ

Virtuaalioppiympäristön viimeinen osuus oli tehdä kameravalvontajärjestelmä. Järjestelmän tarkoituksena on, että opettajat ja opiskelijat voivat ohjata koululle tulevaa prosessia etänä ja valvoa sen kulkua IP- kameroitten kautta. Kameravalvonta järjestelmä koostuu palvelimesta, johon kameravalvonnan virtuaalikone tehtiin, IP- kameroista ja lähiverkosta mihin virtuaalikone kytkettiin. Tässä osuudessa käydään läpi, miten palvelimelle AMKESXi1 tehtiin virtuaalikone, joka liitettiin kameraverkkoon. Virtuaalikoneeseen asenettiin Agent DVR niminen ilmainen valvontakameraohjelma, jolla kameroita voisi hallita. Lisäksi osuudessa käydään läpi, miten koululla valmiiksi käytössä olevat IP- kamerat konfigurointiin uuteen käyttötarkoitukseen ja kytkettiin toimiviksi Agent DVR sovellukseen.

Kameravalvontajärjestelmä aloitettiin luomalla palvelimelle AMKESXi1 virtuaalikone. Palvelimelle luotiin Linux pohjainen virtuaalikone, mutta Agent DVR asentamisessa koitui ongelmia, joten koneen käyttöjärjestelmäksi vaihdettiin Windows Server 2019. Koneelle annettiin edellisessä osuudessa mainitut tekniset ominaisuudet. Seuraavaksi asennettiin koneelle Agent DVR valvontakameraohjelma. Ohjelma ladattiin Agent DVR kotisivujen kautta. Jotta ohjelma saatiin toimimaan, täytyi Windows koneesta saada Media Foundation päälle. Ohjelman päälle laittaminen oli helppoa Windowsin PowerShell komentotulkilla. Tulkille syötettiin kuvan 17 mukainen lähdekoodi.

```
Import-Module ServerManager
```

```
Install-WindowsFeature Server-Media-Foundation
```

Kuva 17 Lähdekoodi, jolla Media Foundation saatiin päälle

Seuraavaksi oli aika konfiguroida koululla olevat IP-kamerat. Koulun kamerat ovat kuvan 18 mukaisia Caverionin PTZ- kameroita. Kamerat asennettiin PoE -kytkimeen. PoE -kytkimen etuna oli, että kamerat saatiin lähiverkkoon ja virroitettua yhdellä verkkokaapelilla. Kameroita pääsi käsittelemään syöttämällä kameroihin jo ennestään määritetyt IP-osoitteet verkkoselaimen hakukenttään.



Kuva 18 Caverionin PTZ- kamera

IP-osoitteen syötettyä aukesi kuvan 19 mukainen verkkosivu, johon kirjautumalla pääsi konfiguroimaan IP-kameroiden asetuksia. Kameroiden käyttöjärjestelmät olivat hyvin vanhat, joten ne täytyi päivittää uudempaan versioon. Kyseisille kameroille ei enää löytynyt mistään päivitystiedostoja, mutta etsinnän jälkeen löydettiin eri valmistajan samankaltaiset kamerat, joihin löytyi järjestelmäpäivitykset. Päivitykset ladattiin ja kamerat alkoivat toimimaan. Kameroihin päivitettiin uudet IP-osoitteet ja vaihdettiin NTP- aika-asetukset. Kameroille tehtiin kaksi käyttäjää: "admin", jolla on kaikki oikeudet kameran muokkaamiseen ja käyttämiseen, sekä "view" - käyttäjä, joka nimensä mukaisesti voi ainoastaan katsoa käyttöliittymää ja kameroita. Nämä toimenpiteet toistettiin kaikkiin kahdeksaan IP-kameraan.



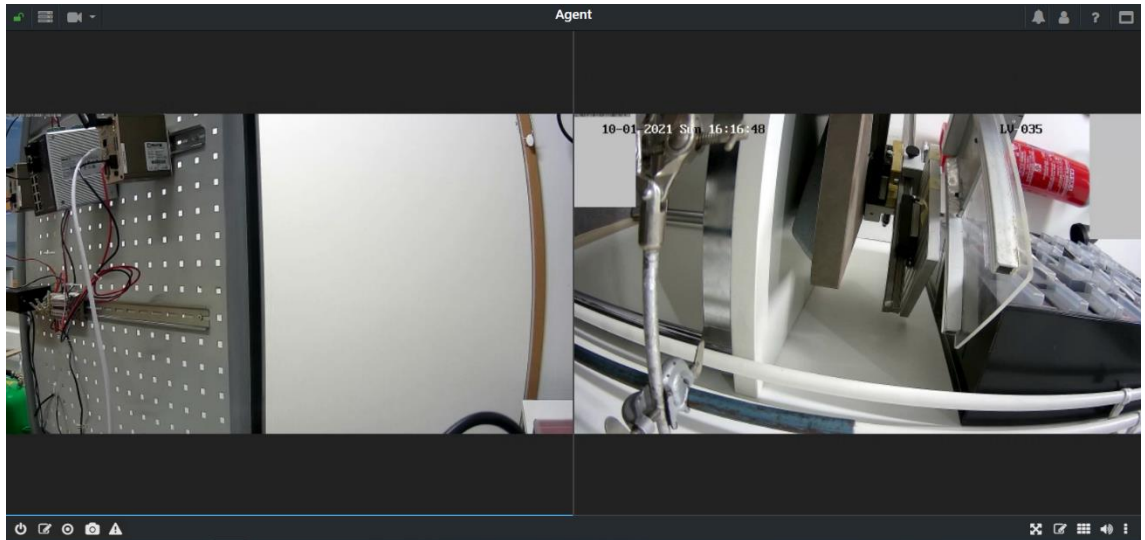
Kuva 19 Kameroiden kirjautumisikkuna

## 8.1 Agent DVR

Kameroiden toimiessa luotiin kameravalvontajärjestelmä Agent DVR - ohjelmaan. Agent DVR - ohjelmaa pääsi käsittelemään syöttämällä verkkoselaimen hakukenttään AMKispy virtuaalikoneen IP-osoitteen ja verkon VLAN ID -osan.

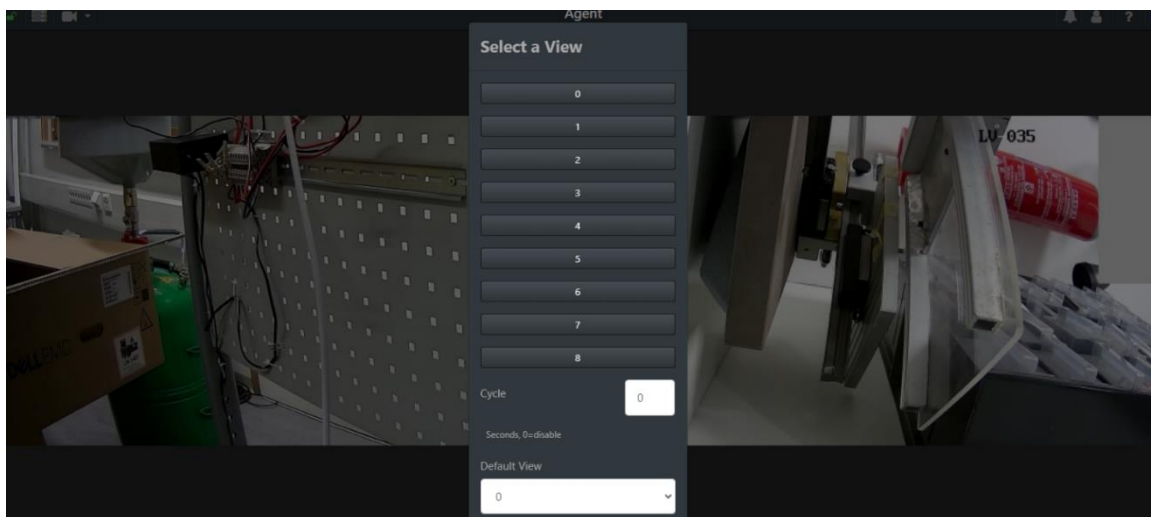
IP:n syöttämisen jälkeen aukesi kuvan 20 mukainen sivu, tosin alkuperäisessä aloitussivussa ei näkynyt kameroiden kuvaa. Sivulta pystyi "ADD device" - painikkeesta lisäämään laitteita järjestelmään. "ADD" - painikkeen jälkeen aukesi ikkuna, johon syötettiin haluttavan kameran tiedot, kuten kameranmalli, nimi ja salasana. Next painikkeella päästiin kameran hakuun, hakukenttään syötettiin kameran IP-osoite ja ohjelma antoi usean linkin kameran suoralähetykseen. Oikean linkin valittua Agent DVR - ohjelma lisäsi kameran järjestelmään. Kuva 20 näyttää toimivan kameran käyttöliittymässä. Kaikki kahdeksan kameraa lisättiin käyttöliittymään ja nimettiin niiden IP-osoitteen mukaan.





Kuva 20 Agent DVR ensinäkymä

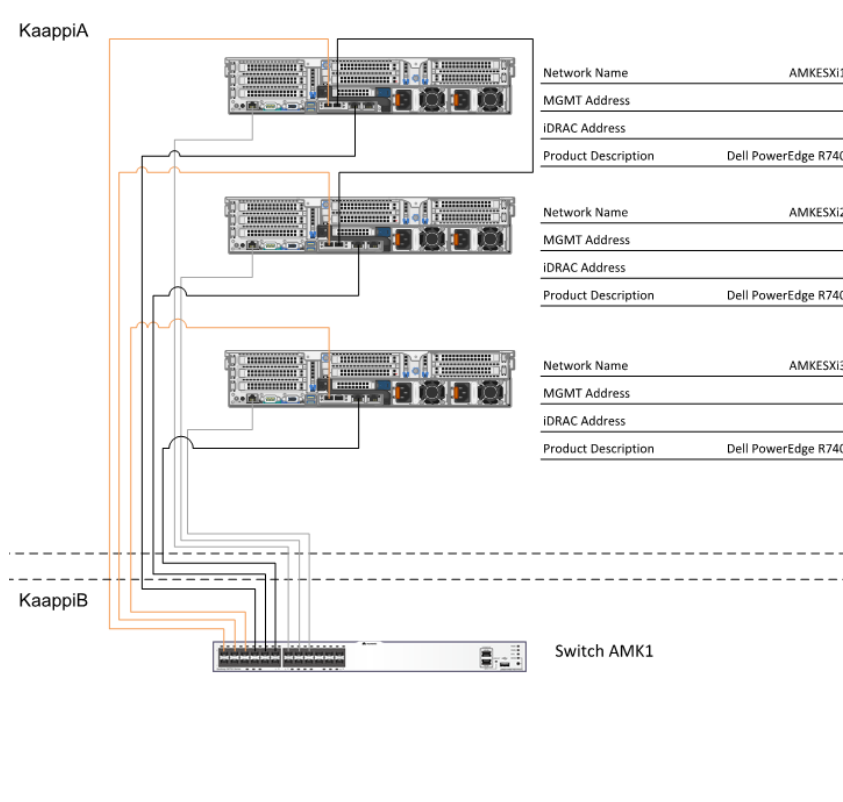
Agent DVR - sovelluksella pystyi tekemään kuvan 21 mukaisia näkymiä, joihin valittiin halutut kamerat ja niiden tarkkailu onnistui yhdestä ruudusta. Kameroilla testattiin myös nauhoittamista ja se toimi moitteettomasti. Kameroilla pystyi tarkentamaan ja niitä pystyi kääntelemään siten, että kuvanlaatu pysyi suhteellisen tarkkana.



Kuva 21 Agent DVR näkymän valinta

## 8.2 Viimeistely

Kun palvelimet oli saatu kokonaan käyttökuntoiseksi, piti palvelimet vielä siirtää palvelinhuoneeseen. Palvelinhuoneessa palvelimet asennettiin niille suunniteltuihin räkkeihin ja liitettiin Lapin ammattikorkeakoulun verkostoon kuvan 22 mukaisesti.



Kuva 22 Mallinnus palvelimien kytkennästä

## 9 POHDINTA

Aiheena oppimisympäristön palvelinvirtualisointi oli kiinnostava, koska palvelinvirtualisointi on yleistymässä ja on läsnä omalla koulutusallani. Virtuaalisten palvelimien potentiaaliset hyödyt voisivat olla merkittäviä tulevaisuuden työpaikoissa niin teollisuudessa kuin yritystoiminnassa.

Opinnäytetyöhön perehtyessä huomasin, miten paljon virtuaalipalvelimista ja niiden käyttöönotosta löytyy materiaalia. Projekti itsessään ei tuottanut kovin paljoa haasteita, vaikka aiheena virtuaaliset palvelimet olivat minulle suhteellisen uusi. Tosin työaikana huomasin palvelimien käyttöönotossa, miten pieninkin virhe saattaa aiheuttaa ylimääräistä työtä. Pienistä ongelmista riippumatta projekti toteutui sille varatulla ajalla.

Opinnäytetyötä tehdessä olen saanut paljon laajemman käsityksen virtuaalipalvelimista ja niiden merkityksestä. Erityisesti siitä, miten paljon hyötyä on virtualisoida palvelimet. Opinnäytetyön tekeminen antoi minulle valmiuksia ajatella omaa osaamista palvelimien parissa ja It-alan jatkuvaa kehitystä

Lopputuloksena saatiin tuotettua toimiva virtuaalinen oppimisympäristö, joka vastasi kaikkia alkuperäisiä odotuksia. Opinnäytetyön myötä Lapin ammattikorkeakoulu sai virtuaaliset palvelimet, jota pystytään hyödyntämään tulevana vuosina sähkö- ja automaatio - opinnoissa. Minulle ehkä tärkeimpänä lopputuloksena on opittu tietotaito virtuaalipalvelimien käyttöönotosta, jota pystyn hyödyntämään tulevaisuudessa työelämässä.

## LÄHTEET

Ekurssit 2021a. Sovellusvirtualisointi. Viitattu 14.02.2021. [http://www.ekurssit.net/kurssit/lk307\\_virtu/sovellusv.php](http://www.ekurssit.net/kurssit/lk307_virtu/sovellusv.php)

Ekurssit 2021b. Tallennus- ja verkkovirtualisointi. Viitattu 14.02.2021. [http://www.ekurssit.net/kurssit/lk307\\_virtu/tallennusv.php](http://www.ekurssit.net/kurssit/lk307_virtu/tallennusv.php)

Ekurssit 2021c. Virtualisointi. Viitattu 14.02.2021. [http://www.ekurssit.net/kurssit/lk307\\_virtu/](http://www.ekurssit.net/kurssit/lk307_virtu/)

Husu, J. 2020. Virtuaaliympäristöllä otat tulevaisuuden mutkattomasti vastaan. Viitattu 18.02.2021. <https://lahtiprecision.com/virtualisointipalvelu/>

Golden, B. 2009. Virtualization for Dummies. 2. HP erikoispainos. Indianapolis, USA: Wiley Publishing, Inc.

Integrated computer services 2021. ICS VMware Virtualization Services Include. Viitattu 20.02.2021. <https://www.icssnj.com/VMWare-installation-support.html>

Muetstege, A. 2018. 20 Years VMware – Past to Present. Viitattu 14.02.2021. <https://vmguru.com/2018/02/20-years-vmware-past-to-present/>

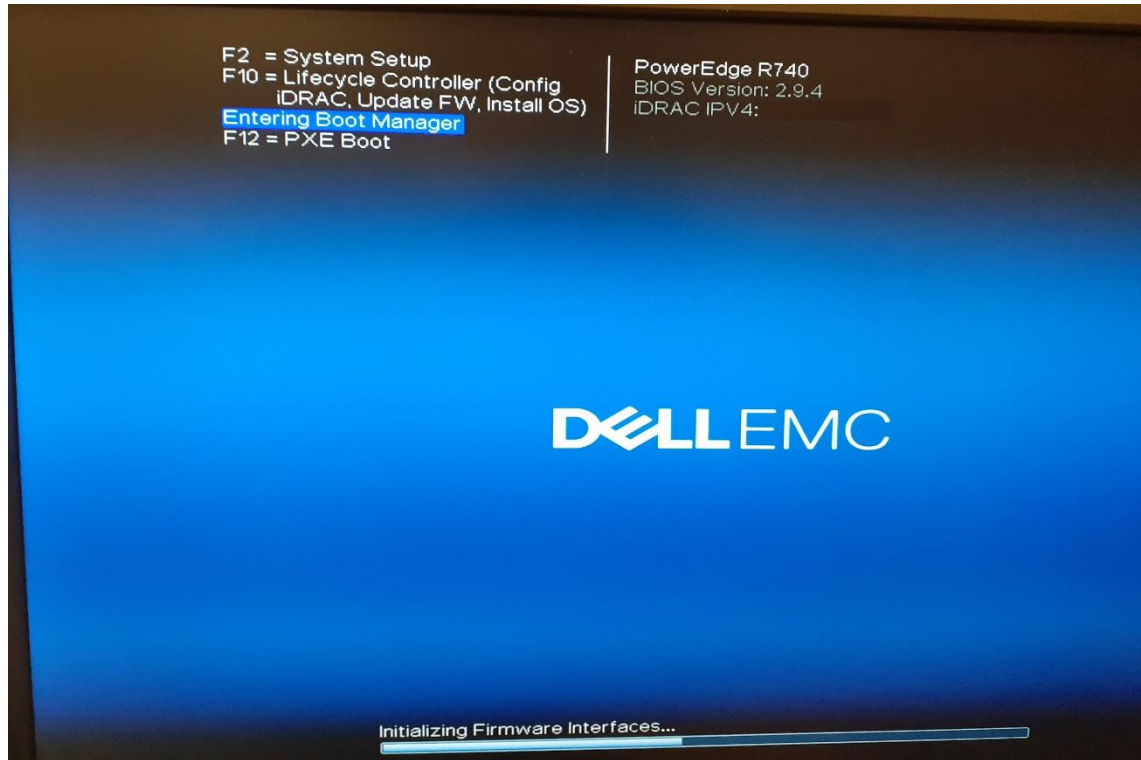
Mäntylä, J. 2008. Virtualisointi mullistaa tietotekniikan. Viitattu 16.02.2021. <https://www.tivi.fi/uutiset/virtualisointi-mullistaa-tietotekniikan/6bfc7845-942e-373d-9797-17bb2226cb73>

Palokangas, 2021. Palvelinvirtualisointi hankkeen projektidokumentti. PDF-tiedosto

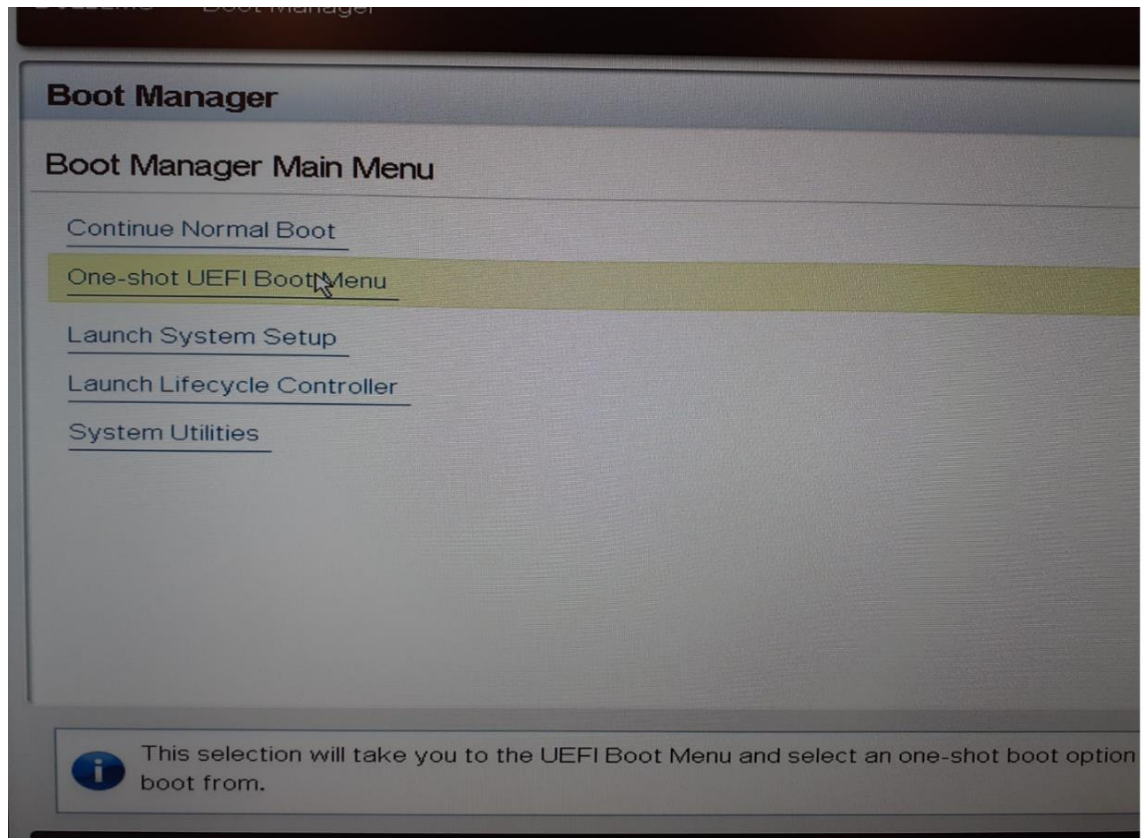
## LIITTEET

- Liite 1. Siirtyminen käynnistysvalikkoon
- Liite 2. Käynnistyksen hallinta- välilehti
- Liite 3. Käynnistyksen valinta- asetukset
- Liite 4. EULA sopimuksen hyväksyminen
- Liite 5. Asennuslevyn valinta
- Liite 6. ESXi päivityksen valinta
- Liite 7. Päivityksen varmistus
- Liite 8. Käyttöjärjestelmän päivityksen latausikkuna
- Liite 9. Palvelimien nimeäminen ja DNS serverin määrittely
- Liite 10. Palvelimen IP-osoitteen, aliverkon ja yhdysverkon vaihtaminen
- Liite 11. IPv6: käytöstä poisto

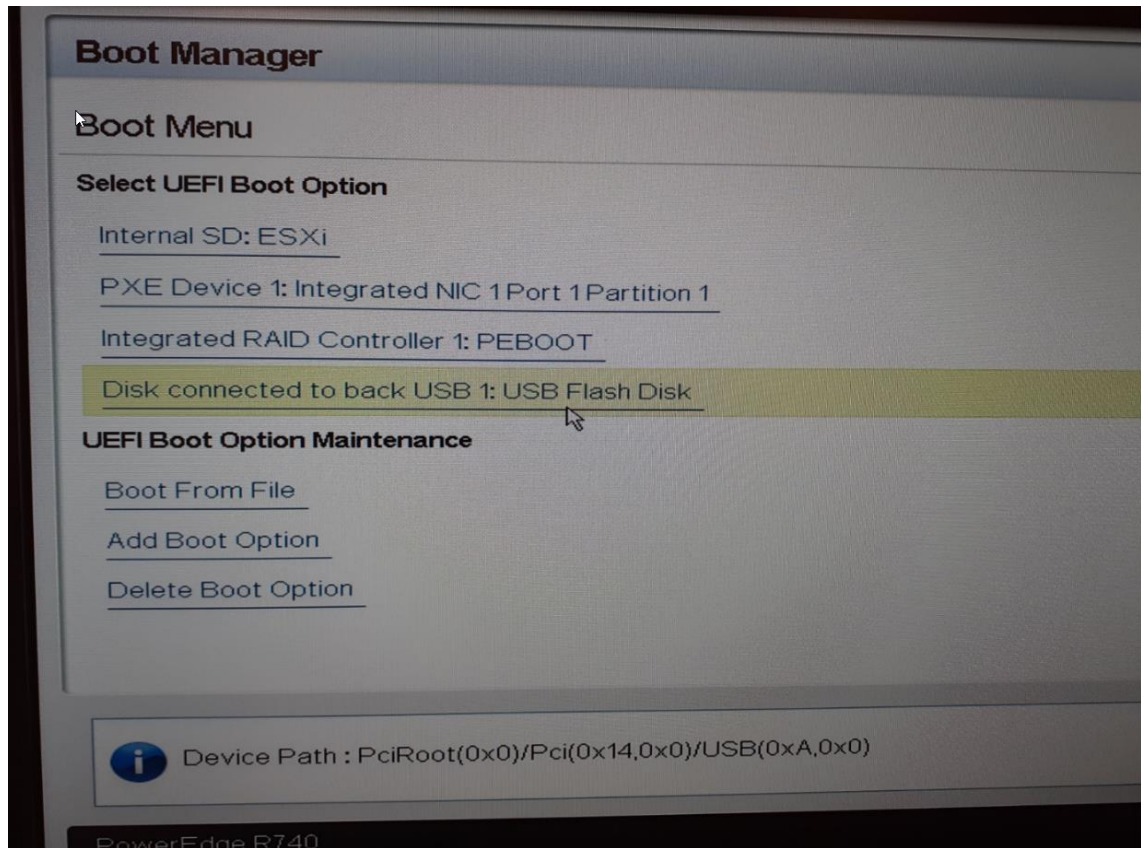
## Liite 1. Siirtyminen käynnistysvalikkoon



## Liite 2. Käynnistyksen hallinta- välilehti

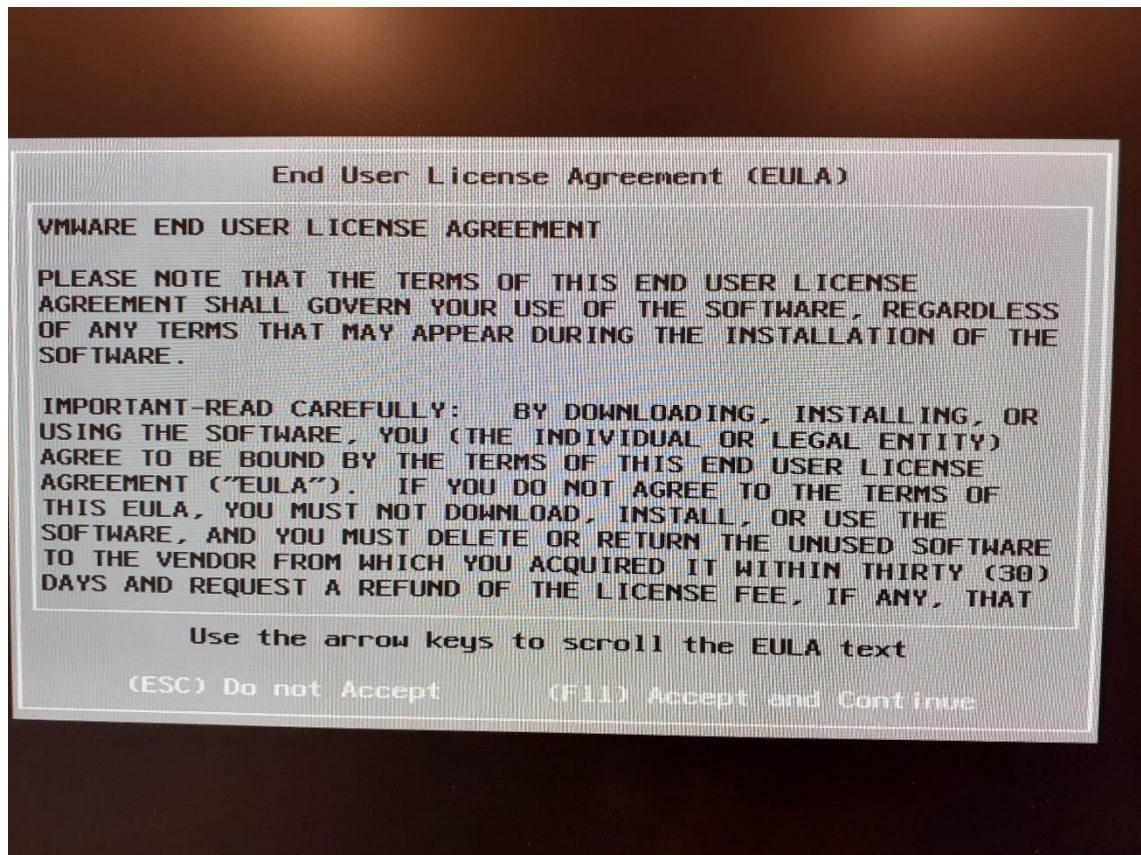


## Liite 3. Käynnistyksen valinta- asetukset

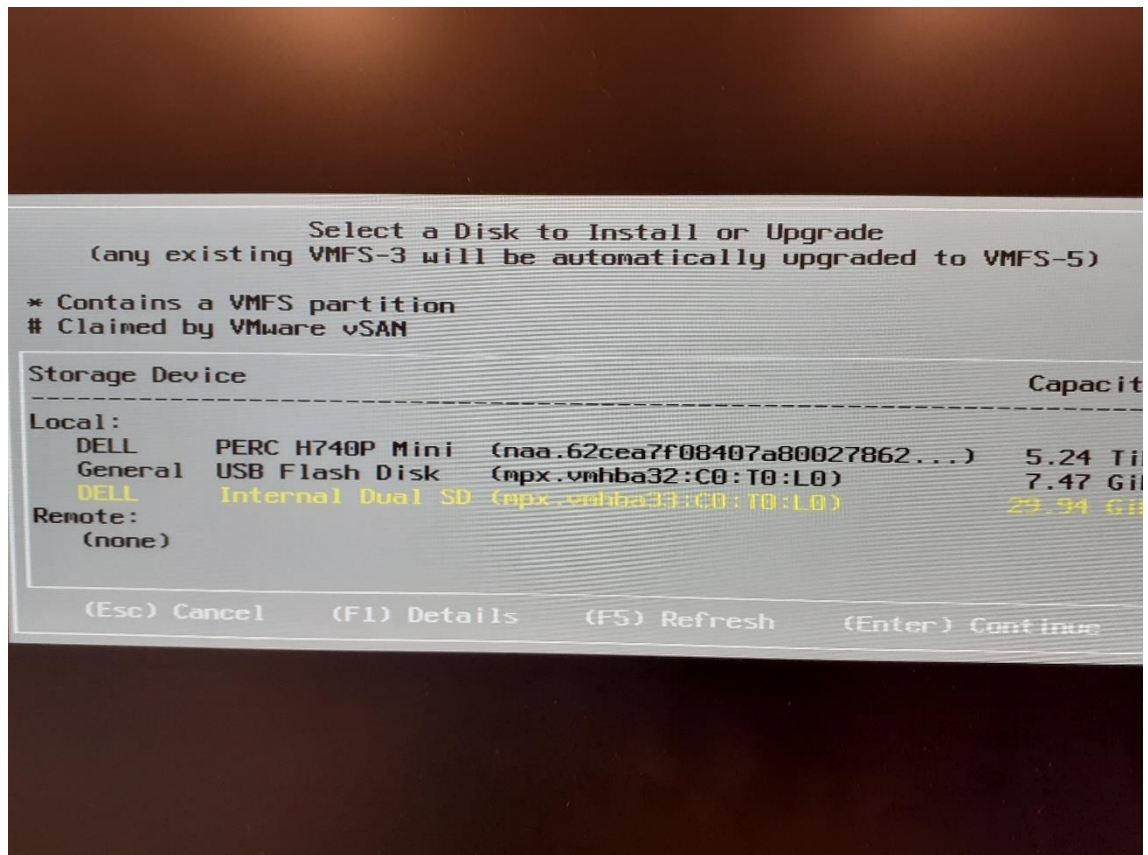




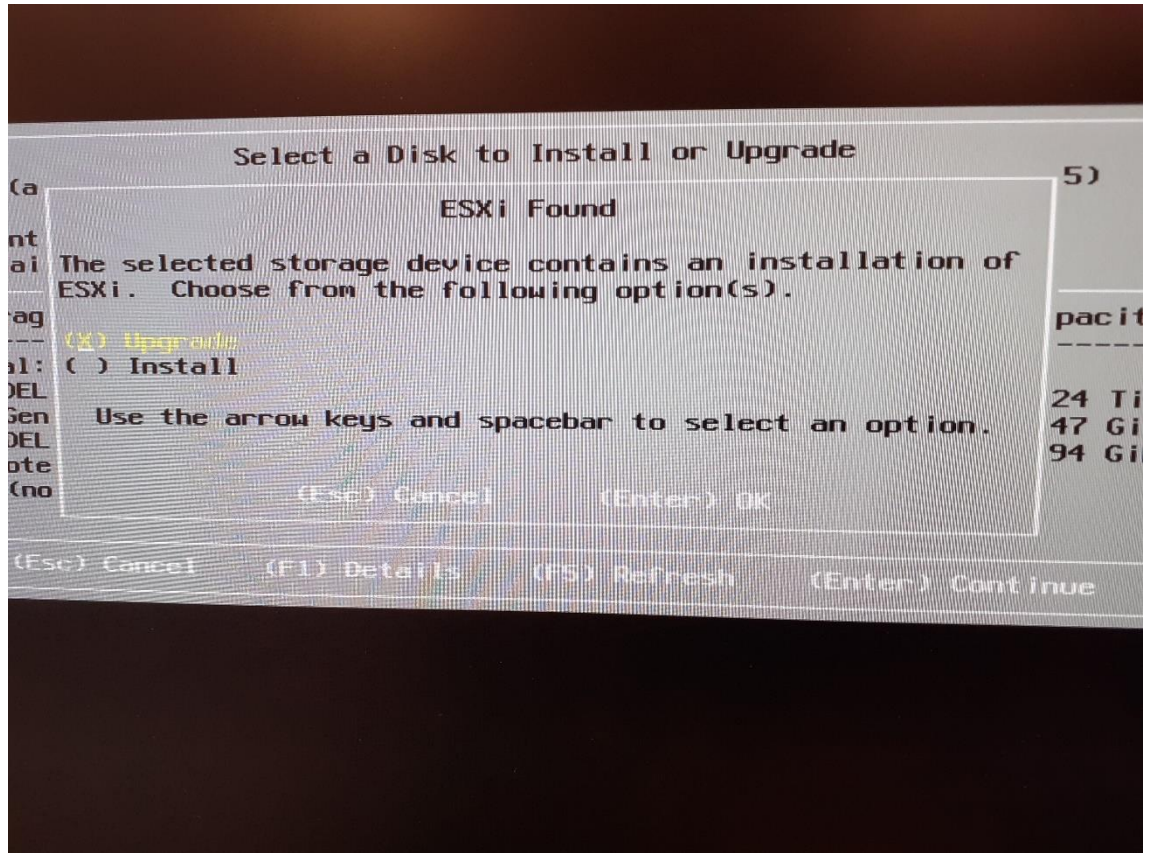
## Liite 4. EULA sopimuksen hyväksyminen



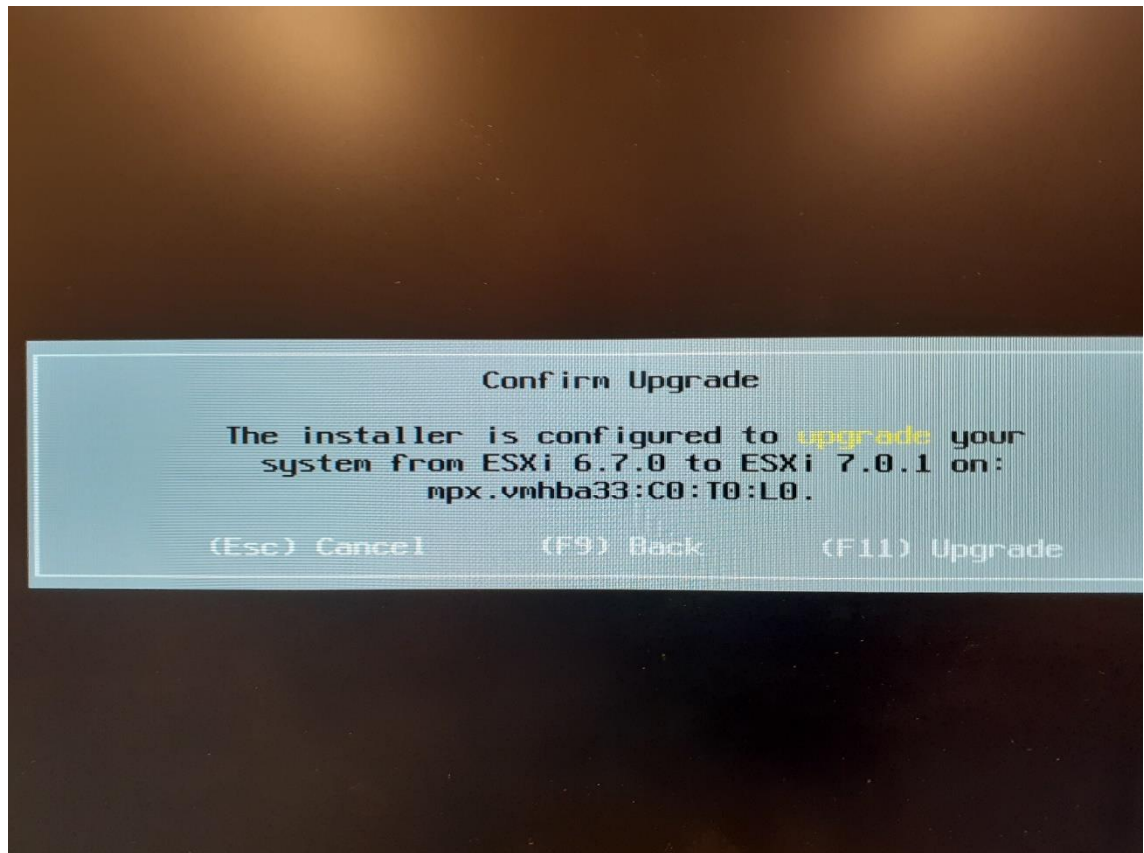
## Liite 5. Asennuslevyn valinta



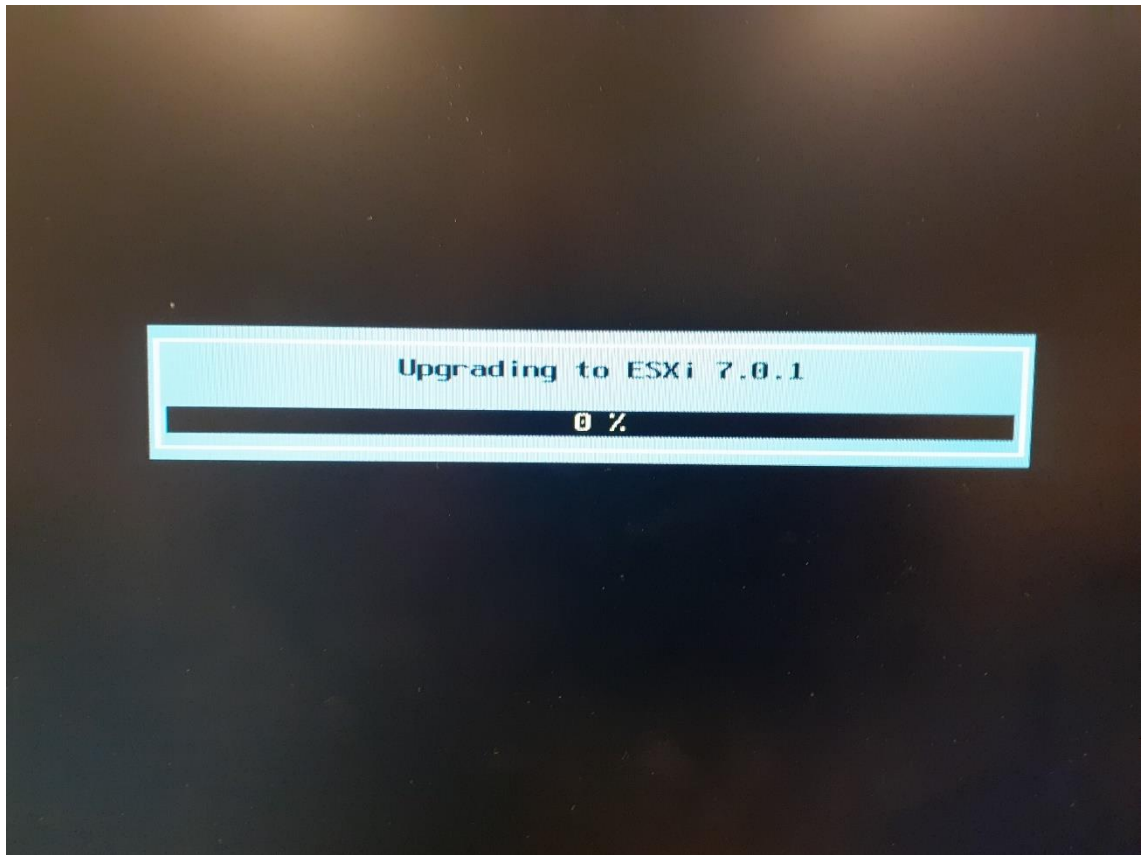
## Liite 6. ESXi päivityksen valinta



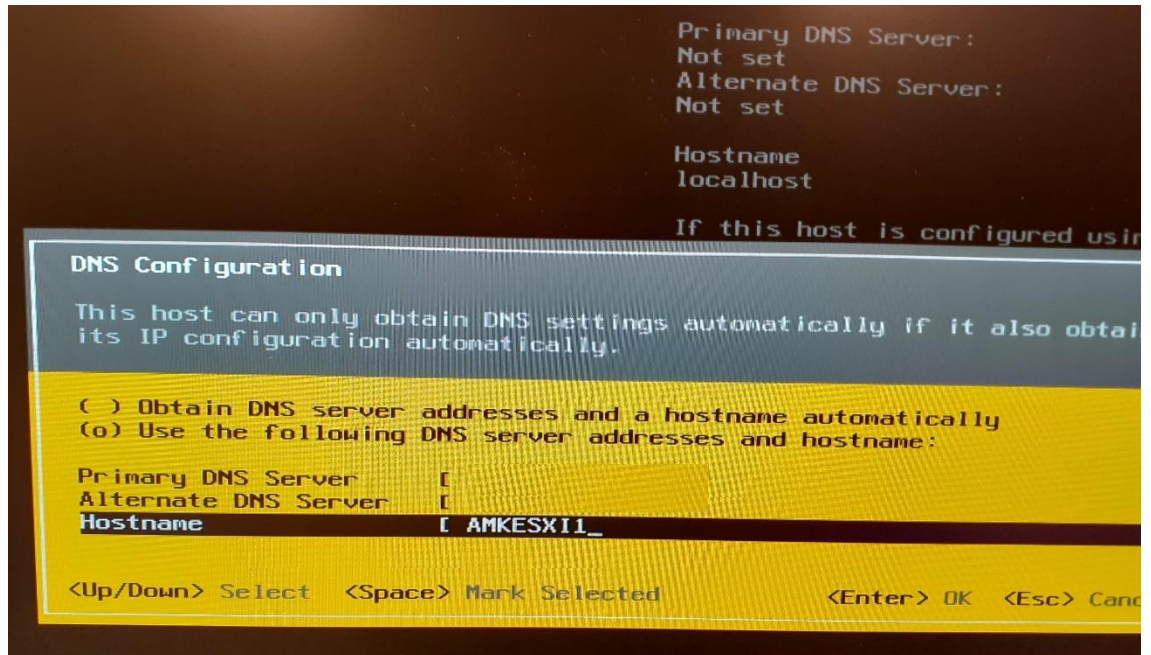
## Liite 7. Päivityksen varmistus



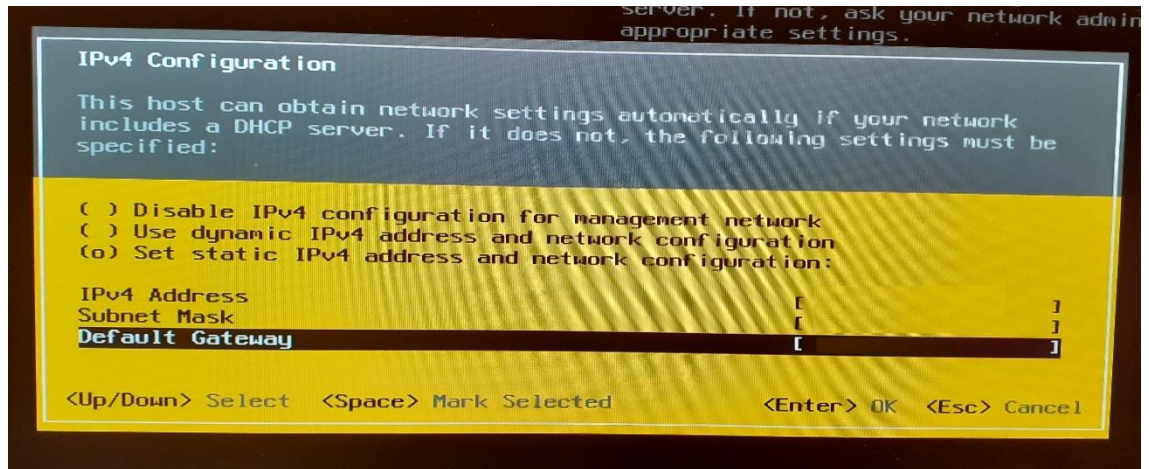
## Liite 8. Käyttöjärjestelmän päivityksen latausikkuna



## Liite 9. Palvelimien nimeäminen ja DNS serverin määrittely



## Liite 10. Palvelimen IP-osoitteen, aliverkon ja yhdysverkon vaihtaminen



## Liite 11. IPv6: käytöstä poisto

