TALLINNA TEHNIKAÜLIKOOL
INSENERITEADUSKOND

Tartu Kolledž

MISSIOONIKRIITILISE ANDMESIDEVÕRGU HALDUSEKS VAJALIKU INFRASTRUKTUURI ÜLESSEADMINE

SETTING UP THE INFRASTRUCTURE OF MISSION CRITICAL DATA NETWORK MANAGEMENT

RAKENDUSKÕRGHARIDUSTÖÖ

Üliõpilane: Gretlin Jõever

Üliõpilaskood: 154619NDFR

Juhendaja: Merik Meriste, dotsent

Tartu, 2019

AUTORIDEKLARATSIOON

Olen koostanud lõputöö iseseisvalt.

Lõputöö alusel ei ole varem kutse- või teaduskraadi või inseneridiplomit taotletud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

“.....” 2019

Autor: .....

/ allkiri /

Töö vastab bakalaureusetöö esitatud nõuetele

“.....” ..... 201…..

Juhendaja: .....

/ allkiri /

Kaitsmisele lubatud

“.....”.....201… .

Kaitsmiskomisjoni esimees .....

/ nimi ja allkiri /

Tartu kolledž

LÕPUTÖÖ ÜLESANNE

Üliõpilane: Gretlin Jõever, 154619NDFR

Õppekava, peaeriala: NDFR14/15, küberfüüsikaline süsteemitehnika

Juhendaja(d): Merik Meriste, dotsent, +3726204808

Konsultant: Tanel Petersell, IP ja VoIP teenuste tehnilise osakonna juht

Tele2 Eesti AS, +37256351272, tanel.petersell@tele2.com

Lõputöö teema:

Missioonikriitilise andmesidevõrgu halduseks vajaliku infrastruktuuri ülesseadmine

Setting Up the Infrastructure of Mission Critical Data Network Management

Lõputöö põhieesmärgid:

1. Vananenud serverite süsteemi üleviimine uuendatud ja automatiseeritud lahenduse peale.

Lõputöö etapid ja ajakava:

Nr	Ülesande kirjeldus	Tähtaeg
1.	Lõputöö eelkaitsmine	08.05
2.	Lõputöö esitamine	27.05
3.	Lõputöö kaitsmine	05.06

Töö keel: eesti keel	Lõputöö esitamise tähtaeg:	27.05.2019
Üliõpilane: Gretlin Jõever	/allkiri/.....	“.....”.....2019
Juhendaja: Merik Meriste	/allkiri/.....	“.....”.....2019
Konsultant:	/allkiri/.....	“.....”.....2019

SISUKORD

EESSÕNA

Lõputöö teema pakuti ettevõtte Tele2 Eesti AS poolt, kus serverite uuendusprotsessi läbiviimine oli kriitiliselt oluline. Algselt oli plaan teostada missioonikriitilise andmesidevõrgu halduse ülesseadmine, kuid töö osutus siiski liiga mahukaks. Otsustati alustada vastava infrastruktuuri loomisega ning jätta andmesidevõrgu teenuste protsess töö jätkuks. Töö pealkiri sõnastati ettevõtte IP ja VoIP teenuste tehnilise osakonna juhi poolt ning töö koostati tehnika osakonnas osaliselt koostöös IT taristu juhiga.

Käesolevas rakenduskõrgharidustöös seatakse üles toimiv IT infrastruktuur missioonikriitilise võrgu halduseks Tele2 Eesti AS näitel. Eesmärgi täitmiseks püstitati loodava keskkonna nõuded ja valikukriteeriumid ning viidi läbi selle paigaldamine, seadistamine ja testimine.

Autor soovib tänada lõputöö juhendajat Merik Meristet, kolleege ja konsultanti Tele2 Eesti AS-st ning õppejõude ja kursusekaaslasi, kes andsid väärtuslikke nõuandeid käesoleva töö valmimiseks.

Märksõnad: server, virtualiseerimine, virtuaalmasin, VMware, rakenduskõrgharidustöö.

LÜHENDITE JA TÄHISTE LOETELU

BIOS	Baasvahetussüsteem (Basic Input/Output System)
CPU	Protsessori jõudlus (Central Processing Unit)
DSL	Internetiühendus (Digital Subscriber Line)
HA	Suur kättesaadavus (High Availability)
HDD	Kõvaketas (Hard Disk Drive)
iDRAC	Dell'i kaughaldusliides (Integrated Dell Remote Access Controller)
ISDN	Primaarühendus vahendusjaamale (Integrated Services Digital Network)
ISKE	Infosüsteemide Kolmeastmeline Etalonturbe Süsteem
KVM	Virtualiseerimise lahendus Linux x86 riistvarale (Kernel-based Virtual Machine)
NIC	Võrgukaart (Network Interface Controller)
OP	Operatsioonisüsteem (Operating System)
PCB	Trükkplaat (Printed Circuit Board)
RAM	Muutmälu (Random Access Memory)
ROM	Püsimälu (Read-Only Memory)
SSD	Pooljuhtketas (Solid State Drive)
VM	Virtuaalmasin (Virtual Machine)

1. SISSEJUHATUS

Tehnoloogia kiire areng toob tahtmatult kaasa süsteemide vananemise ning vananenud IT taristu ei pruugi võimaldada enam piisavalt jõudlust, lihtsust ja kiirust. Need ressursid on aga tänapäeval ettevõtetes olulisel kohal, kuna pakutavate teenuste ja kliendi soovide hulk aja möödudes järjest kasvab. Samuti on üha tähtsamal kohal andmete ja süsteemide turvalisus. Ettevõte peab suutma oma varasid ja kliendi andmeid ohtude eest kaitsta, nii stiihiliste kui ka sihilike sekkumiskatsete eest. Üldiselt ongi uuenduste üks eesmärke likvideerida vana versiooni vead ja puudujäägid, millest võivad tekkida tarkvarale näiteks turvaaugud ja mida omakorda oleks lihtne häkkeril rünnata. Seega seadmete ja masinate kvaliteetse tööshoidmise jaoks on oluline süsteemi ja tarkvara pidevalt uuendada, sest nii välditakse võimalikke ohte ning tagatakse süsteemide käideldavus, terviklikkus ja konfidentsiaalsus.

Käesoleva töö eesmärgiks oli seada üles toimiv IT infrastruktuur missioonikriitilise võrgu halduseks Tele2 Eesti AS näitel. Missioonikriitiline süsteem on ettevõttele elutähtis süsteem, suure tõenäosusega selle töö katkemine katkestaks kogu tegevuse või siis kahjustaks seda oluliselt [1]. Töös viiakse läbi füüsiliste serverite paigaldamine, virtualiseerimine ja virtuaalmasinate seadistamine, kasutades ettevõttepoolsest valikust lähtudes süsteemide virtualiseerimise tarkvara VMware. Tulevikus edasine arendus hõlmab endas kogu andmesidevõrgu teenuste ülekandmist antud töö tulemusena ehitatud infrastruktuuri peale. Pärast seda on missioonikriitiline võrk terviklik ja ettevõtte eesmärk täielikult täidetud. Loodav lahendus on kiirem, paindlikum ja turvalisem ning lihtsustab kindlasti oluliselt ettevõtte protsesse.

Antud rakenduskõrgharidustöö koosneb kolmest olulisest peatükist. Peatükis „Ülevaade serveritest ja neile kohaldatavatest nõuetest“ kirjeldatakse üldiselt füüsiliste serverite olemust, serverite klastrit ja virtuaalserverite lahendust ning kuna Tele2 Eesti AS lähtub suuresti ISKE nõuetest, siis antakse ülevaade ka olulisematest nõuetest IT taristu osas missioonikriitilisele infrastruktuurile. Järgmises peatükis „IT infrastruktuuri ülesseadmine“ kirjeldatakse ettevõttes juba olemasolevat süsteemi ning käesoleva töö ülesandepüstitust ja metoodikat. Alapeatükkides räägitakse füüsiliste serverite paigaldamisest vastavatesse serveriruumidesse, serverite klastri seadistamist kasutades VMware tarkvarat, virtuaalmasinate loomist seadistatud klastrisse ja ka vastavate seadistuste testimist. Lõpetuseks arutatakse töö käigus selgunud tulemuste üle.

2. ÜLEVAADE SERVERITEST JA NEILE KOHALDATAVATEST NÕUETEST

2.1 Füüsilised serverid

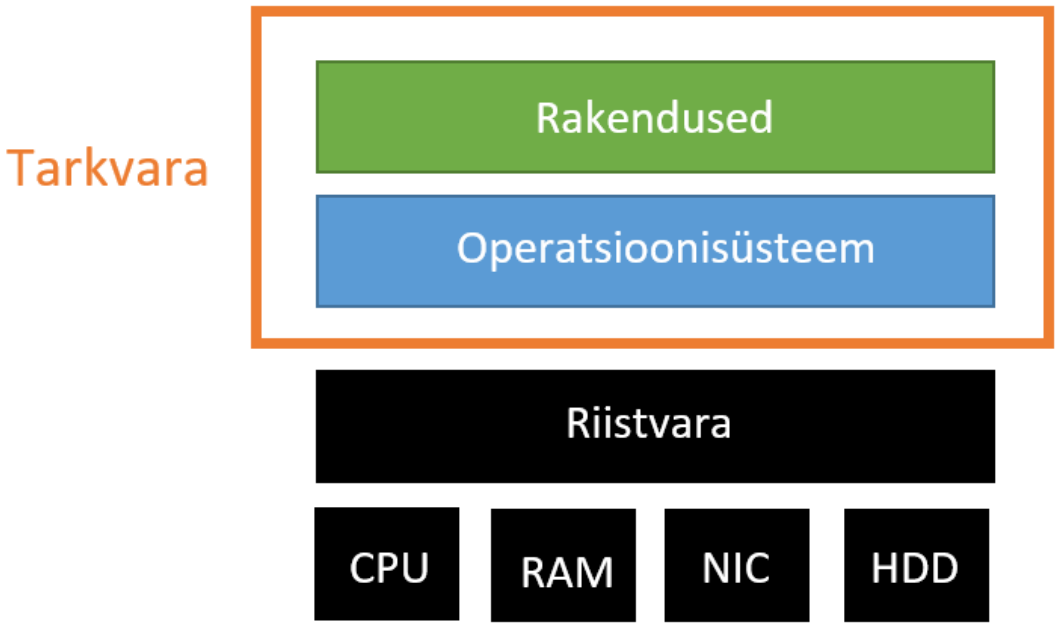
Füüsilised serverid on tänapäeval väga laialdaselt levinud süsteemid. Füüsiliste serverite all mõistetakse infotehnoloogia süsteeme nagu arvuteid, mis võimaldavad teistel infotehnoloogilistel süsteemidel nagu kliendid, serveri poolt pakutavaid teenuseid võrgu kaudu kasutada [2]. Kokkuvõttes kasutatakse füüsilisi servereid nii eraisikuna kui ka ettevõtetes mingit sorti failide või teenuste hoiustamiseks ning neile saavad üle interneti ligi kõik, kellele on määratud vastavad õigused ja arvutitesse installitud klientprogrammid.

Kuna servereid kasutatakse mingisuguste tähtsamate andmete varundamiseks ja neile peab olema igal ajal võimalik üle võrgu ligi pääseda, siis tavalise arvutiga võrreldes vajavad füüsilised serverid kõrgemal tasemel stabiilsust, turvalisust ja jõudlust [3]. Seetõttu hoitakse servereid ka kõrgemate turvenõuetega varustatud ruumides nagu serveriruum või arvutikeskus ning neid kindlasti ei kasutata tööarvutitena [2]. Vastav serveriruum tagab füüsilistele serveritele asukoha mõttes võimalikult ohutu keskkonna ja pakub parimaid võimalusi ka töökeskkonna näol, mis tagab serveritele stabiilsed ja pikaajalised võimalused töötamiseks.

Füüsiline server koosneb riistvarast ja tarkvarast. Tarkvara on vajalik süsteemi riistvarale funktsioneerimiseks. Teenuste tarkvara ütleb süsteemile, millist käsku on vaja täita. Riistvara ehk raudvara kontrollib operatsioonisüsteemi. Riistvara tähtsamad komponendid on järgmised:

- CPU ehk protsessor;
- RAM ehk muutmälu;
- NIC ehk võrgukaart;
- mäluseade nagu HDD- või SSD-ketas. [4]

Joonisel 2.1.1 on välja toodud klassikalise füüsilise serveri struktuur. Füüsilise riistvara peale installitakse vastavalt soovidele ja vajadustele valitud operatsioonisüsteem, mis omakorda jooksutab serveri peal olevaid rakendusi. Rakenduste alla kuuluvad kõik teenused ja aplikatsioonid, mida serveri poolt klientidele pakutakse.



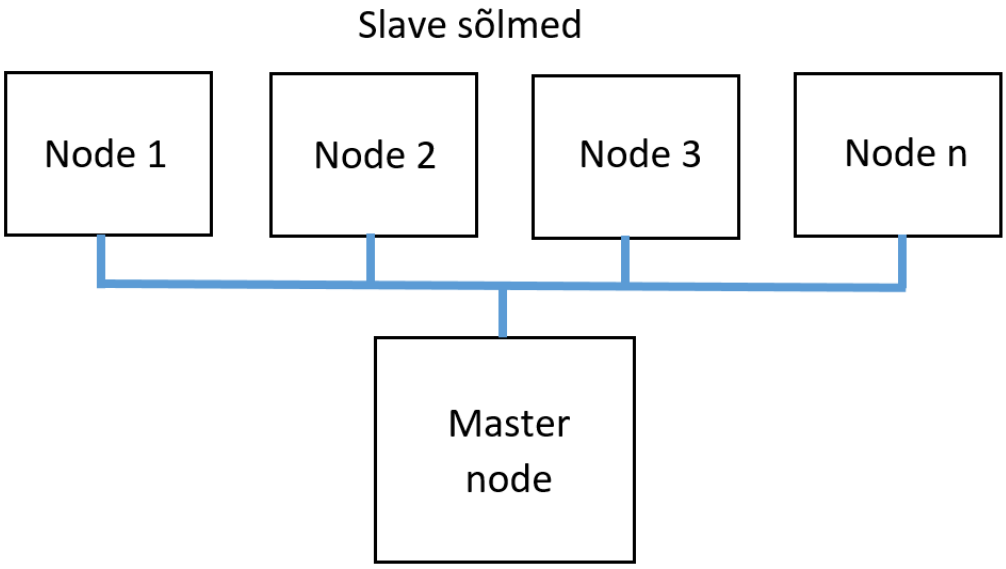
Joonis 2.1.1. Füüsilise serveri struktuur [5]

Operatsioonisüsteem on siis vahekiht serveri riistvara ja lõppkasutajatele mõeldud rakenduste vahel. Tegemist on tarkvaraga, mis haldab serveri mälu, riistvara ja tarkvara. See võimaldab arvutil suhelda riistvara komponentidega nagu kettaseaded, klaviatuur, ekraan, hiir, pinterid, skännerid ja võrk. Operatsioonisüsteem võimaldab mitmetel rakendustel arvutis samaaegselt töötada, lülitades juhtimist nende vahel edasi ja tagasi. Ilma operatsioonisüsteemita on arvuti sisuliselt kasutu. Valida saab 32- ja 64-bitise operatsioonisüsteemi vahel. Nende suurim erinevus seisneb selles, et kui palju mälu on kättesaadav ja kuidas seda mälu hallatakse. Seega rakendused, mis on kirjutatud näiteks 64-bitise operatsioonisüsteemi kasutamiseks, toimivad paremini 64-bitises süsteemis võrreldes 32-bitise süsteemiga. Operatsioonisüsteemid on mitmesuguste suuruste ja keerukuse tasemega. Serverites on võimalik kasutada mitmeid erinevaid operatsioonisüsteeme, millest tuntumad on näiteks Microsoft Windows, Unix, GNU/Linux ja Apple Mac OS X. [6]

2.2 Serverite klaster

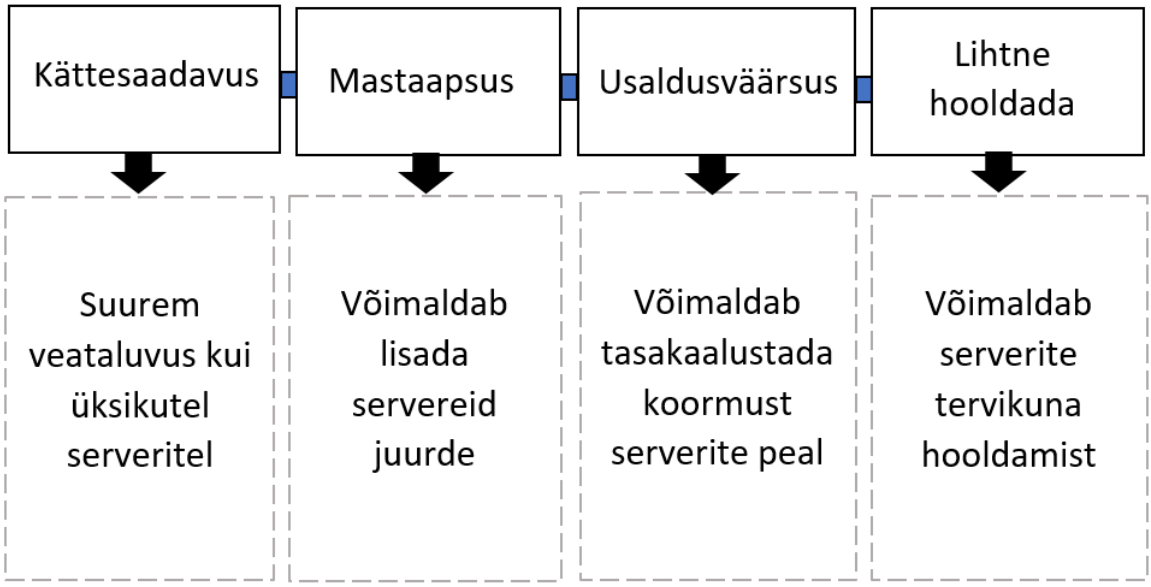
Serverite klaster ehk serverikobar on serveritena töötavate arvutite rühm, millel on ühine asukoht [7]. Serverite klastreid kasutatakse eesmärgiga pakkuda kasutajatele suuremat teenuse kättesaadavust ning seda siis vähendades süsteemide võimalikku seisakut ja katkestust. Klastrid võimaldavad vastava rikke korral järgmisel serveril esimese serveri töö üle võtta. See põhimõte töötab järgmiselt: serverite rühm on ühendatud ühe süsteemiga, hetk kui ühel neist serveritest tekib teenusekatkestus, siis jagatakse töökoormus klastri järgmisele serverile nii kiiresti, et klient ei jõua isegi kogeda vastavat süsteemi seisakut. [4] Serverite üleminek klastris ühelt teise peale võib maksimaalselt aega võtta kuni minut. Manuaalselt võiks selline serverite vahetuse protsess võtta aega keskmiselt kuskil ühe päeva, mis on päris pikk aeg.

Klastris olevaid servereid nimetatakse sõlmedeks (*nodes*). Sõlmed töötavad koos ühe võrguservenina, et pakkuda võrgule koondamist ja koormuse tasakaalustamist, jätkates klastris oleva mistahes nurjunud serveri toiminguid. Klastri serverid võimaldavad juurdepääsu võrgus olevatele võrguressurssidele. Sel moel pakub klaster suuremat kättesaadavust võrguressurssidele ja klastris hostitud teenustele. Ressursside alla kuuluvad klastri teenused ja rakendused. [8] Joonisel 2.2.1 kuvatakse klastri lihtsustatud struktuur, kus on välja toodud mingi n arv *slave* sõlmesid, mis täidavad *master* sõlme poolt edastatud käskluseid.



Joonis 2.2.1. Klastri sõlmed [8]

Üldiselt kasutatakse serverite klastreid teenuste jaoks, kus on sageli uuendatud andmeid koos faili-, printimis-, andmebaasi-, ja sõnumiside serveritega, mis on ka kõige sagedamini kasutatavad klastrid. Klastrite serverikeskkonnas vastutavad kõik serverid ise iga oma seadme omandi ja haldamise eest ning neil on olemas ka operatsioonisüsteemi koopia koos kõigi olemasolevate rakenduste ja teenustega, mida kasutatakse vajadusel klastri teiste serverite käitamiseks. Klastri serverid on programmeeritud töötama koos nii, et suurendada andmete kaitset ja säilitada aja jooksul klastri konfiguratsiooni järjepidavus. [4] Joonisel 2.2.2 on välja toodud klastritele iseloomulikud omadused.



Joonis 2.2.2. Klastrite tugevad küljed [4,9]

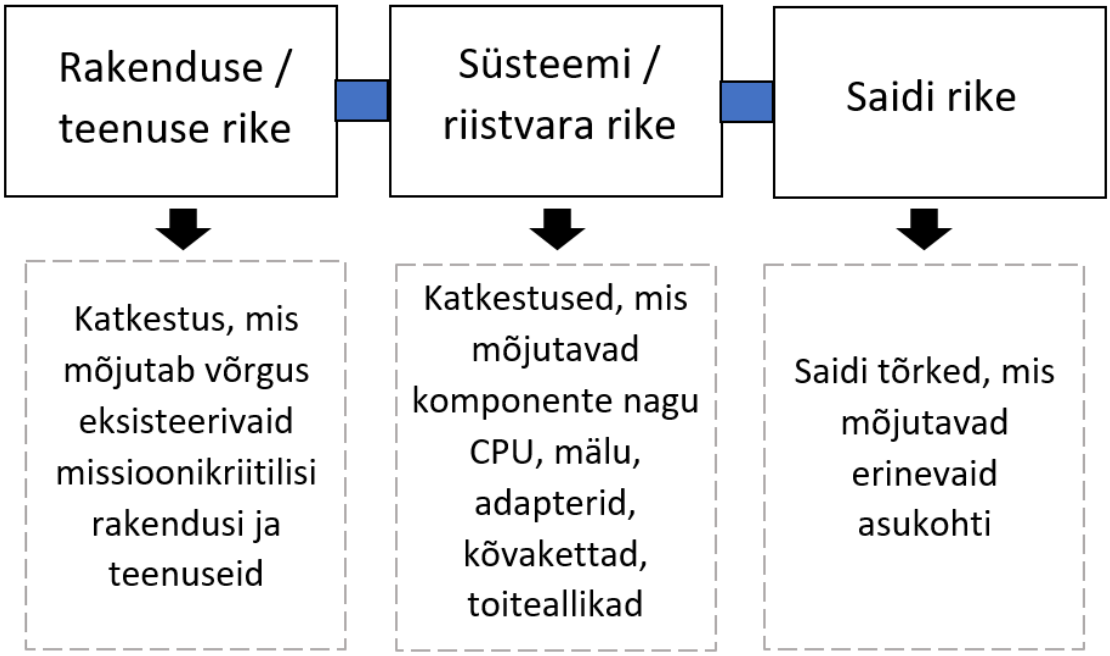
Detailsem kirjeldus serverite klasterdamisest ja nende omadustest on välja toodud järgnevalt:

1) kättesaadavus ehk veataluvus: klastrid võimaldavad tõhusaid tõrketaluvusi serverite puhul. Kui ühe serveri või mingisuguse riistvara osaga tekib probleem, siis teine klastris olev server võtab lihtsalt tööjärje üle. Vigu võib esineda klastris mitmeid ilma, et see mõjutaks kättesaadavust ehk serverite seisakud üldises plaanis puuduvad;
2) mastaapsus ehk klastrid võimaldavad ajapikku suurenemist: kõiki serveriressursse jagatakse ja hallatakse ühise raamistiku abil ning uusi servereid saab igal ajal klastrisse juurde lisada;

3) usaldusväärsus ehk klastrite järjepidavus: klasterdamine võimaldab maksimaalset jõudlust läbi koormuse tasakaalustamise. Suure liiklusega rakenduste, suurte andmebaaside või ulatuslike programmidega, mis vajavad ulatuslikke ressursse, saab klastrit konfigureerida nii, et erinevad koormused jagunevad ühtlaselt kõikidele kaasatud serveritele;
4) lihtne hooldada: klastrit on lihtsam hooldada kui üksikuid süsteeme. Hostinguteenused võivad teostada hooldus- ja muid ülesandeid klastris tervikuna. Kui peaks olema vajalik siiski hooldada üksikuid servereid, siis saab need kergesti klastrist lahti ühendada ilma, et see mõjutaks füüsiliste serverite jõudlust ja kättesaadavust. Lihtne hooldus tähendab üldises plaanis ka vähem probleeme ja väiksemaid kulusid ettevõttele. [4,9]

Servereid ohustavad teatud rikked. Serverite klastrid kaitsevad servereid kolme peamise katkestuse tüübi eest, mis on kuvatud hiljem ka joonisel 2.2.3. Neid kirjeldatakse alljärgnevalt:

1) Esimeseks võimalikuks tüübiks on rakenduse või teenuse rike. See on katkestus, mis mõjutab otseselt missioonikriitilisi rakendusi ja selles võrgus olevaid teenuseid.
2) Teiseks tüübiks on süsteemi või riistvara rike. Need on katkestused, mis mõjutavad komponente nagu CPU, RAM, adapterid, kõvakettad ja toiteallikad.
3) Kolmas rikke tüüp on saidi rike. Need on saidi tõrked, mis mõjutavad süsteemi mitut asukohta. Tihti võivad need olla põhjustatud loodusõnnetustest, mis omakorda tekitavad olukordi nagu elektrikatkestused. [10]



Joonis 2.2.3. Serverite tegevuse katkestuste tüübid [4]

2.3 Virtuaalserverid

Tänapäeval kogub üha enam populaarsust virtuaalserverite kasutamine, kuna lisaks ettevõtetele, kasutatakse neid ka väga palju isiklikus elus. Ettevõtete poolelt vähendavad virtualiseerimislahendused üldiselt IT-kulusid ja suurendavad samal ajal tootlikkust, riistvara tõhusust ja paindlikkust [11]. Seega on riistvara virtualiseerimine väga mõistlik protsess, mida kindlasti läbi viia, kui tegeleda tuleb suurte andmemahtudega nende haldamise kui ka varundamise eesmärgil.

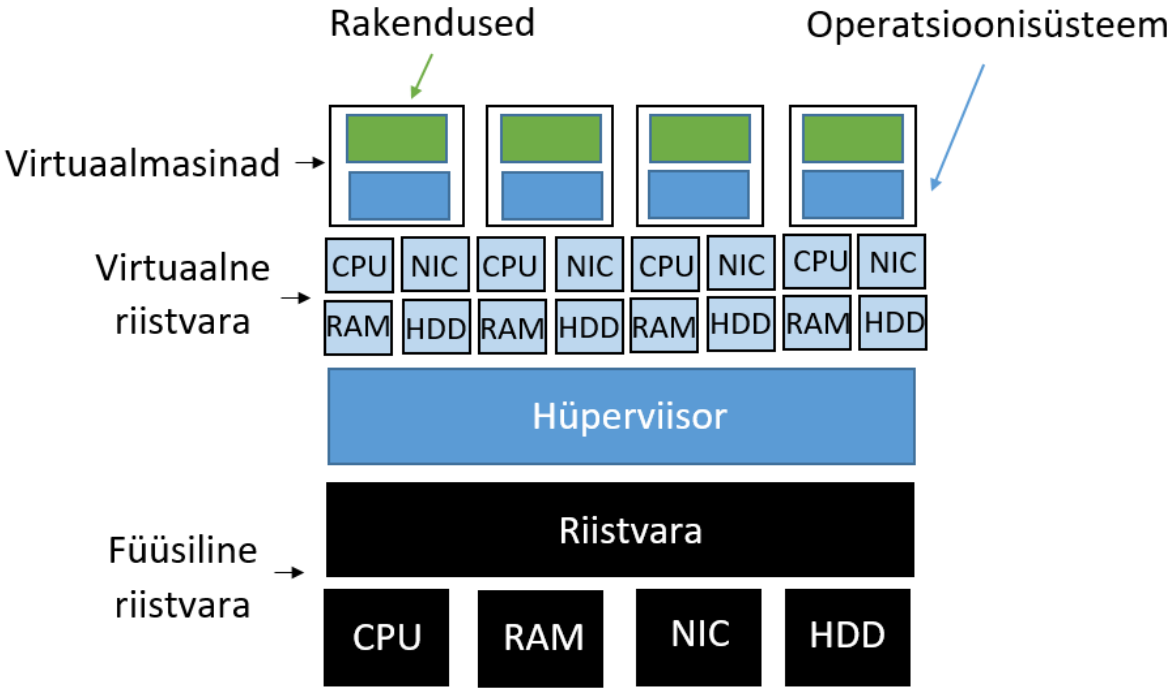
Virtuaalserver on sarnane keskkond omaette serverile, mis näiliselt tundub kui eraldiseisev server, aga tegelikult paikneb teenusepakkuja füüsilises serveris. Ettevõtete puhul on tänapäeval väga tavapäraseks saanud virtuaalserverite teenuse sisseostmine, kus kliendile eraldatakse teatud kogus serveri ressursse ning seejuures tagatakse nende pidev ja stabiilne kättesaadavus. Virtuaalserveri teenuse kasutamine toob väiksematele ettevõtetele kaasa väiksema kogukulu, kui seda teeb enda

serveri ülespanemine ja selle haldamine. [12] Samas suuremate ettevõtete puhul, kellel on võimalus lubada seesuguseid väljaminekuid, tuleb lõppkokkuvõttes oma serveri pidamine siiski soodsam. Virtuaalse serveri peaeesmärk on sama nagu ka füüsilisel serveril, hoiustada mingit sorti faile või teenuseid, mida pole mõistlik ja turvaline pelgalt paberkujul hoida. [13]

Virtuaalserverile on iseloomulikud omadused nagu optimeeritud ressursijaotus ja dünaamilisus. Tänu ressursside optimeeritud jaotusele on süsteem tasakaalus: ei ole millestki puudus ega ei jää ka midagi üle, mis on süsteemi efektiivsuse mõttes väga oluline. Seejuures tagab dünaamilisus võimaluse vastavalt vajadusele ressursside mahtu ka modifitseerida, kui kliendi vajadus peaks siiski muutuma. Virtuaalserverid käituvad ja on käideldavad samamoodi nagu füüsilised serverid, kusjuures virtuaalserverisse saab paigaldada samuti sobiva operatsioonisüsteemi ja rakendustarkvara. [14]

Virtualiseerimine on tehnoloogia kiht, mis paikneb seadme füüsilise riistvara ja operatsioonisüsteemi vahel. Tänu sellele kihile on võimalik luua füüsilist riistvara kloonides virtuaalne riistvara. Hüperviisor omakorda kasutab virtuaalset riistvara, et luua virtuaalmasin. Virtuaalmasin on lühidalt öeldes failide kogum, mis koosneb operatsioonisüsteemist ja serveri peal paiknevatest rakendustest. Hüperviisori ja virtuaalmasinaga saab üks arvuti samaaegselt jooksutada mitmeid erinevaid operatsioonisüsteeme. [15]

Joonisel 2.3.1 kuvatakse virtuaalserveri struktuur, kus on välja toodud kõikide kihtide paiknevus serveris. Füüsilise serveri peal paikneb hüperviisori vahekiht ning hüperviisori abil installitakse virtuaalsest riistvarast lähtudes operatsioonisüsteem ja valitud rakendused, mis omakorda moodustavad kokku virtuaalmasina. Kusjuures füüsilise serveri riistvara komponendid ja virtuaalse riistvara komponendid on täpselt samad. Neid eristab üksteisest see, et virtuaalse riistvara ressursse on võimalik modifitseerida vastavalt vajadusele. Füüsiliste serverite puhul on see protsess tunduvalt keerulisem.

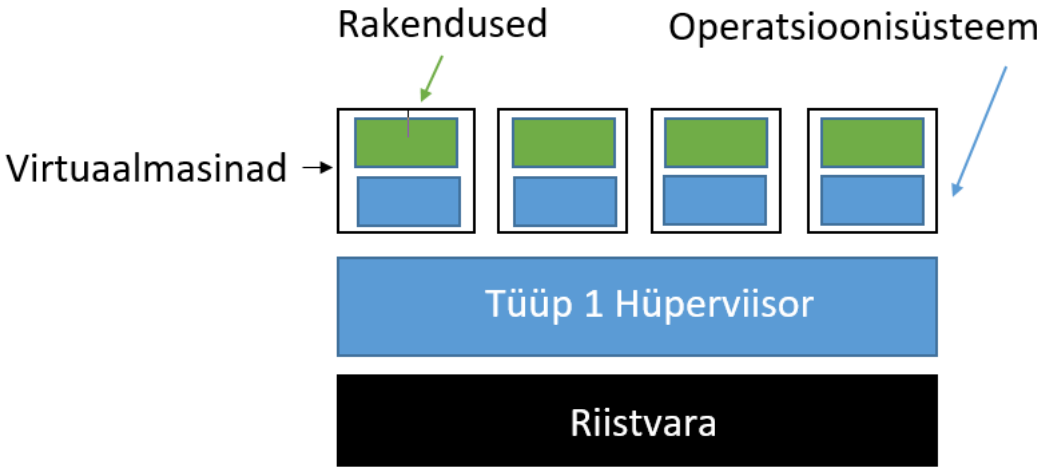


Joonis 2.3.1. Virtuaalserveri struktuur [16,17]

Hüperviisor on täpsemalt kirjeldades tarkvara, mis on installitud riistvara peale ja mille abil luuakse virtualiseerimiskiht. See omakorda eraldab virtuaalsed masinad serveri füüsilisest riistvarast, mis teeb võimalikuks virtuaalmasinate installimise mis tahes operatsioonisüsteemiga ilma, et peaks muretsema riistvaraplatvormi jaoks õige seadme draiveri hankimise pärast. Hüperviisor eraldab ka virtuaalsed masinad üksteisest. Seega, kui ühel virtuaalsel masinal peaks esinema mingisuguseid probleeme, siis ei mõjuta see teiste virtuaalmasinate tööd. Kategoorialt jagatakse hüperviisorid tavaliselt kaheks:

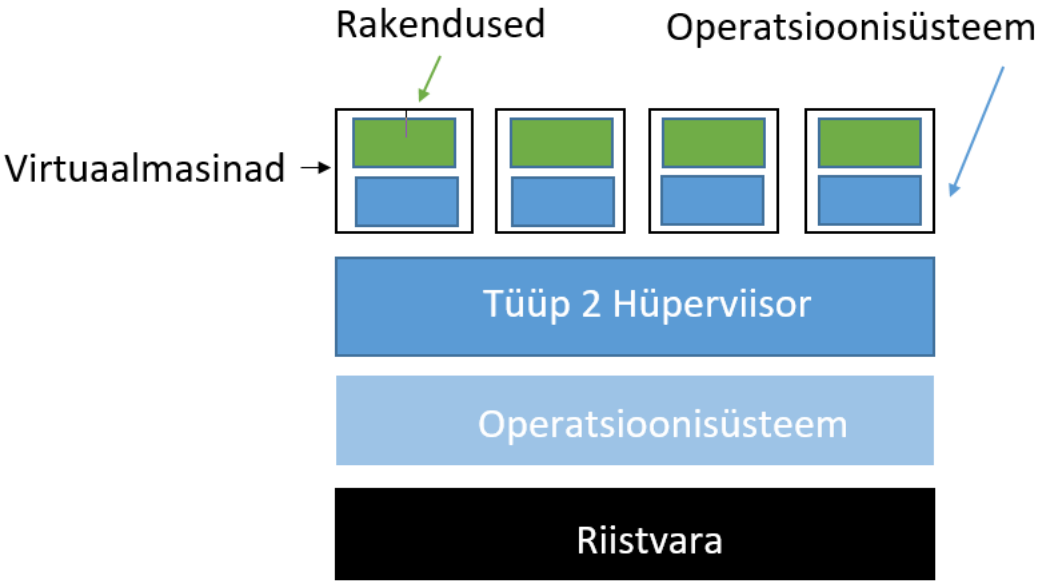
1) tüüp 1 – palja metalli hüperviisor (*bare metal hypervisor*);
2) tüüp 2 – hostitud hüperviisor (*hosted hypervisor*).

Esimest tüüpi hüperviisor töötab otse riistvara peal ja pakub külalistele vajalikke funktsioone. Kuna seda tüüpi hüperviisorid on installitud otse riistvara peale, siis esineb neil tavaliselt vähem üldkulusid kui tüüp 2 hüperviisoritel. See võib suurendada ka süsteemi võimsust ja üldist jõudlust. Esimest tüüpi hüperviisorid on näiteks VMware ESX, KVM ja Microsoft Hyper-V. Joonisel 2.3.2 kuvatakse tüüp 1 hüperviisori üldine struktuur.



Joonis 2.3.2. Tüüp 1 hüperviisor [18]

Teist tüüpi hüperviisor töötab olemasoleva operatsioonisüsteemi peal ja kasutab selle sama operatsioonisüsteemi funktsioone. Need on tarkvarataseme hüperviisorid. Kuna teist tüüpi hüperviisorid on installitud olemasoleva operatsioonisüsteemi peale, siis on nad ka mugavamad kui tüüp 1 hüperviisorid. Teist tüüpi hüperviisor on näiteks VMware GSX Server. [15,19] Joonisel 2.3.3 kuvatakse tüüp 2 hüperviisori üldine struktuur, mis erineb esimest tüüpi hüperviisorist siis operatsioonisüsteemi kihi poolest, mis asub riistvara ja hüperviisori vahel.



Joonis 2.3.3. Tüüp 2 hüperviisor [14]

Virtuaalmasinaid saab eksportida ja viia teistesse hostidesse üle. Failid luuakse hüperviisori poolt ja varundatakse kataloogis. Näiteks on olemas järgmised virtuaalmasinate failide tüübid:

- logi fail, mis sisaldab virtuaalmasina tegevuse logi;
- ketta fail, mis varundab virtuaalmasina kettaseade sisu;
- *snapshot* ehk momentvõtte fail, mis varundab informatsiooni salvestatud virtuaalmasina oleku kohta;
- konfiguratsiooni fail, mis varundab informatsiooni virtuaalmasina nime, BIOS-i, külalisoperatsioonisüsteemi ja mälu kohta. [15]

Snapshot ehk momentvõte on mingisugune virtuaalmasina progress või olek, mis töö käigus varundatakse failidena virtuaalmasina kaustas. Momentvõtte käigus salvestatakse virtuaalmasina ketta olek, mälu sisu ja seaded. [15]

2.4 ISKE nõuded IT taristu osas missioonikriitilisele infrastruktuurile

Infotehnoloogia infrastruktuur koosneb kõigist elementidest, mis toetavad andmete ja teabe haldamist ning kasutatavust. Nende hulka kuuluvad füüsiline riistvara ja rajatised nagu andmekeskused, andmete varundamine ja taastamine, võrgusüsteemid, liidesed ja tarkvara toetamaks ettevõtte ärieesmärke. Infotehnoloogia infrastruktuuri haldus on oluliste tööelementide administreerimine ja haldamine selliselt, et kasutada võimalikult efektiivselt, produktiivselt ja ennetavalt vastavat tehnoloogiat, informatsiooni ja andmeid. [20] Missioonikriitiline süsteem peab toimima hoolimata püsivatest rünnakutest kogu lähetustsükli vältel. Turvaline süsteem ei saa lubada ühtegi riket ei oma kriitilises funktsionaalsuses ega ka peamises kaitsvas infrastruktuuris. [10] Käesolevas peatükis antakse lühiülevaade olulisematest nõuetest ja kaitsemeetmetest IT-infrastruktuurile.

IT-kaabeldus moodustab sisekommunikatsioonivõrgu füüsilise aluse, mille alla kuuluvad välisvõrkude ühenduskohad nagu ISDN-ühendus, mida kasutatakse vahendusjaamades

primaarühenduseks, Interneti DSL-ühendus ning sisevõrgu kasutajate ühenduskohad. IT-kaabeldus sisaldab kommunikatsioonikaableid ja erinevaid passiivseid komponente nagu ristühendused, jätkud ja kaablijaotusseadmed. Kõigepealt pannakse paika võrgu struktuur, mis seejärel sobitatakse kokku hoone võimalustega. Kaablitüüpide valiku järgi määratakse hiljem kaabelduse mehaanilised ning elektrilised omadused. Tuleohutuse tagamiseks tuleb kaablikanalid õigesti paigutada, et tuletõke õiges kohas vajadusel olemas oleks. Kaablite paigaldamisel on kindlasti oluline koostada vastav dokumentatsioon, et hiljem oleks näha kõikide kaablite asukoht ja ka mida nad omavahel ühendavad. Kaableid paigaldades tuleb jälgida, et kaablid ei saaks kuidagimoodi kahjustada. Lisaks tuleb arvestada, et kaablid on paigaldatud nii, et hilisem hoone kasutamine ei kahjustaks neid samuti. IT-kaablid tuleb paigaldada eraldi elektrikaablitest, et vältida viimaste võimalikku mõju IT-kaablitele. [2]

Serveriruum, kus füüsilised serverid paiknevad, tuleb valida selliselt, et keskkonnamõjuritest tingitud potentsiaalsed ohud oleksid võimalikult väikesed ja et vee või mõne muu liini trassid ei paikneks serveriruumile liiga lähedal. Serveriruum peaks sisaldama kõikvõimalikke vahendeid nagu elektrivarustus, õhukonditsioneeri- ja tuleohutusseadmed, et tõrjuda vääramatute jõudude poolt tekkivaid ohte ja ka kindlustada jätkusuutlikkus tehnilistest riketest tulenevate katkestuste korral. Vääramatute jõudude all mõistetakse tulekahju, veest tingitud kahjustusi, lubamatut temperatuuri ja niiskust ning kaablijaotusseadmete väljalangemist vastava põlengu tõttu. Tehniliste rikete alla kuuluvad näiteks toitevõrgu ja sisevõrkude katkestused ning pinge kõikumine, ülepinge või vaegpinge. Serveriruum tuleb kavandada kui suletud turvatsoon, mida hoitakse valve all ja millel on kaitstavad uksed ja aknad. Samuti peaks sissepääs olema reguleeritud vastavate kontrollimehhanismidega, et tagada ligipääs ainult selleks ettenähtud õigustega isikutele. Lisaks ei tohiks serveriruum sisaldada kontoritarbeid, mis kujutavad endast hästi põlevat materjali või kontorivarustust, millele on juurdepääs väga paljudel kasutajatel. Kui ruumis isikuid ei viibi, peab see turvalisuse tagamiseks alati lukustatud olema. [2]

Arvutuskeskus, kus näiteks serveriruum võib paikneda, peab olema kindlasti varustatud vastava valve- ja tuletõrjesignalisatsiooniga ning peab ka olema eraldiseisev elektritoide. Arvutuskeskuse kaitseks tuleb hoonesse paigaldada samuti kõiksugused meetmed, mis minimiseerivad võimalikke ohte keskusele ja selles paiknevatele IT-süsteemidele. Hoone peaks olema kavandatud suletud turvatsoonina, millel võimaluse korral peaks olema ainult üks uks ja mitte ühtegi akent, nii on sissepääsuteede üle parem kontroll. Hoonesse sissepääs peaks olema vaid administraatoritele. Samuti peaks hoonel olema vastav sissemurdmiskaitse. Kindlasti tuleb omada tehnilise infrastruktuuri varukomponente juhuks, kui vastava tippkoormuse ajal mõni peaks näiteks riknema.

IT-süsteemide turvalisuse tagamiseks peaksid hoones olema topeltpõrandad, spetsiaalne valve riistvaralistele objektidele ja tuletõrjesüsteem tulekahju algfaasi tuvastamiseks. Lisaks tuleb elektritoide ja kliimatehnika arvutitest eraldi ruumidesse paigutada, et vältida nende segamini paigutamist. Üks olulisemaid nõudeid käideldavuse garanteerimiseks on kindlasti viia ka kommunikatsiooni- ja infotehniliste komponentide kaitsetarve vastavusse arvutikeskuse kaitsetarbega. Veel on soovitatav paigutada informatsioonitehnika, kliima- ja õhutusseadmed, energiatoide, ladu ning teised taolised seadmed ja ruumid üksteisest eraldi, vajadusel ka erinevatesse tuletõkkesektsioonidesse. Andmete kättesaamiseks vastava avarii korral, on oluline juba algselt varundada neid eraldiseisvasse avariiarhiivi. [2] Teatud määral ühtivad serveriruumi ja arvutuskeskusele rakendatavad turvalisuse nõuded ja kaitsemeetmed.

3. IT INFRASTRUKTUURI ÜLESSEADMINE

3.1 Hetkeseis ja soovitud tulemus

Ettevõttes olemasolev alajaama serverite süsteem oli juba ajale jalgu jäänud. See tähendab seda, et töövahendid olid oma aja ära olnud: füüsilised serverid vanamoodi, tarkvara versioonid uuendamata ja uuendusprotsessi läbiviimiseks olid vajalikud litsentsid kohati puudulikud. Süsteem ei olnud enam tänapäevamõistes piisavalt turvaline. Tarkvara versioonide uuendamata jätmine võib süsteemidele kaasa tuua suurema vastuvõtlikkuse võimalikele rünnetele läbi turvaaukude. Lisaks väheneb ajaga serverite enda võimekus ja on oht, et ka mälu saab täis. Kokkuvõttes oli tegemist juba mitte enam piisavalt efektiivse, töökindla ja turvalise süsteemiga, mis vajas viivitamata uuenduste läbiviimist.

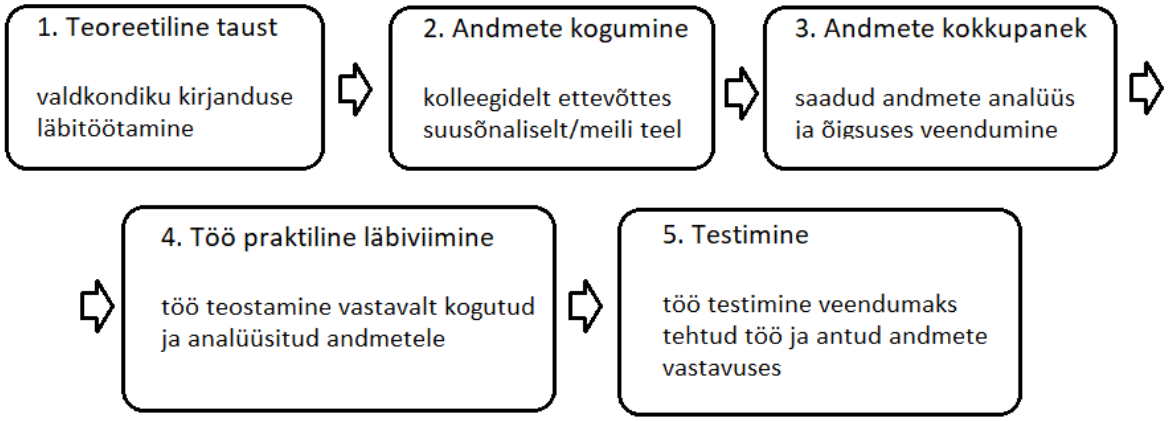
Teema valitigi ettevõtte poolsest vajadusest uuendada vananenud serverite süsteemi. Soovitud tulemus oli saada töötav infrastruktuur missioonikriitilise andmesidevõrgu halduseks, mis vastaks eelnevalt loetletud omadustele. Lisaks hiljem ehitada käesolevas töös loodud infrastruktuuri peale alajaamade rakenduste ja teenuste komplekt, et kogu süsteem oleks lõpuks terviklik.

3.2 Ülesandepüstitus ja metoodika

Käesoleva lõputöö puhul on tegemist arendustööga. Seega kasutatakse töös praktilist lähenemist installimise, virtualiseerimise, nõuete seadistamise ja nende testimise näol. Töös antakse ülevaade, mis on vajalik serveri riistvara ja tarkvara uuendamiseks ning kuidas see protsess on lõppkokkuvõttes teostatud.

Töö metoodika etapiline kirjeldus on välja toodud joonisel 3.2.1. Töö autor alustas kõigepealt antud valdkonna kirjanduse ja mõningate ettevõttepoolsete materjalide läbitöötamisest, et saada aimu eesootava töö sisust, keerukusest ja mahukusest ning ettevõttes juba olemasolevast platvormist. Lisaks tuli hankida vajalikke teadmisi töö läbiviimiseks. Tutvunud teemaga, jätkas autor andmete ja informatsiooni kogumisega ettevõttes töötavatelt kolleegidelt, et järgmisena panna kokku nõuded,

mille järgi hiljem kogu tööprotsess läbi viia. Tuli arvestada, et andmete kogumisprotsess on omajagu aeganõudev töö, eriti kui suhtlus käib ringiga erinevate inimeste vahel, mitte otsese kontakti teel. Samuti vastavate litsentside hankimisele kulub oma aeg. Kui töö oli teostatud, tuli süsteemile seadistatud nõuded läbi testida, et veenduda nende õigses toimivuses ettevõttele soovitud ja kõige sobivamal moel.

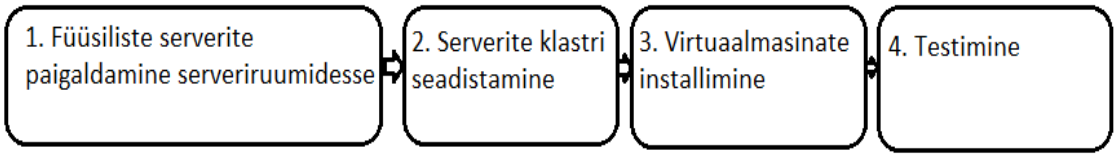


Joonis 3.2.1. Metoodika protsess [autori koostatud]

Töö läbiviimine toimus ettevõtte kontori erinevates koosolekuruumides, mis olid varustatud suurte ekraanide ja tahvlitega, et kogu tegevuse teostust oleks hea jälgida. Erandiks oli füüsiliste serverite paigaldamine serveriruumidesse, mille viisid läbi ettevõtte tehnikud vastavates serverikeskustes. Kogu infotehnoloogiline töö osa toimus koostöös IT taristu juhiga, tema juhendamisel ja jälgimisel. Missioonikriitiliste süsteemidega ümberkäimisel lähtuti ISKE nõuetest IT taristule. Füüsiliste serverite virtuaaliseerimiseks kasutati VMware tarkvara, täpsemalt siis haldustarkvara vCenter Server ning lisaks kasutati firma Dell servereid ja nende haldamiseks vastavat kasutajaliidest Dell iDRAC. Kõik valikud tarkvarale ja masinatele olid ettevõttepoolsed, põhjusel, et need olid ettevõttele endale teatud aspektidest lähtudes parimaks lahenduseks.

Töö praktiline osa koosneb neljast olulisemast etapist, et saavutada algselt püstitatud eesmärk. Vastav tööülesannete järjekord kuvatakse joonisel 3.2.2. Tööd alustati füüsiliste serverite paigaldamisega vastavate nõuetega varustatud serveriruumidesse, kus on tagatud neile sobiv keskkond töös püsimiseks. Järgmisena sai viia läbi sobiva serverite klastri seadistamise eelnevalt kogutud ja analüüsitud informatsiooni põhjal, kasutades ettevõtte poolt selleks valitud tarkvara

VMware. Kui klaster oli seadistatud, installiti sinna keskkonda virtuaalmasinad, samuti kindlate parameetrite järgi, et kogu süsteem lõpuks töötaks nii nagu soovitud. Viimaks testiti süsteemi töötavust, et veenduda seadistatud nõuete toimimises ning vajadusel veel saaks läbi viia korrektuurid. Viimane protsess on väga oluline ja kindlasti ei tohiks seda ära unustada. Kõik etapid kirjeldatakse ükshaaval lähemalt lahti lõputöö järgmistes peatükkides.



Joonis 3.2.2. Arenduskäigu protsess [autori koostatud]

3.3 Paigaldamine serveriruumidesse

Üks oluline etapp on tagada serveritele nende tööks vajalik ja sobiv keskkond. Käesoleva töö käigus paigaldati füüsilised serverid ettevõttepoolsetesse kõrgete turvanõuetega kindlustatud serveriruumidesse. Serveriruumides kasutatakse ISKE nõudeid. Töös käsitletavaid füüsilisi servereid, mis tuli serveriruumidesse paigaldada, oli kokku kaks tükki. Protsessi viisid läbi vastava tehnilise taustaga ettevõtte enda tehnikud.

Üks serveritest paigaldati serveriruumi asukohaga A ja teine server serveriruumi asukohaga B. Antud serveriruumid asuvad turvalisuse aspektidest lähtuvalt üksteisest kaugel ja eraldi asukohtades. Kõrge kriitilisusega süsteemide puhul on mõistlik viia serveriruumid üksteisest nii kaugele kui võimalik, vajaduse korral kasvõi eraldi riikidesse, sest see tagab suuremate riskifaktorite korral süsteemidele veelgi kindlama turvalisuse. Erinev asukoht on väga oluline järgneval põhjusel, et kui ühe serveriruumiga, kus üks füüsiline server asub, peaks mingil põhjusel midagi juhtuma, siis on teine füüsiline server olemas turvaliselt teises asukohas ja töötab vastava seadistatuse korral

ikka samamoodi edasi. Kindlasti ei ole mõistlik otsus antud olukorras paigaldada mõlemat füüsilist serverit ühte ja samasse serveriruumi, ükskõik, kui turvaline see ruum ka poleks.

Ettevõtte poolt kasutatav serveriruum on ehitatud lähtuvalt ISKE nõuetest. Serveriruum on turvatud ööpäevaringse valvega, varustatud võimsate elektri- ja andmesideühendustega ning ka Päästeametiga on tehtud vastavad erikokkulepped. Seal on kasutusel veekindlad topeltlaed, tõstetud põrandad ja ülivõimsad jahutusseadmed. Seadmeruumi jõudev elektritoide pärineb mitmest sõltumatust elektrijaamast ning muidugi on see ka dubleeritud elektrigeneraatoriga. Elektrikatkestuse korral on generaatorist väga palju abi, kuna see asendab teatud ajajooksul elektritoidet. Ruumis rakendatud monitooringusüsteem möödab omakorda serveripargi temperatuuri, seadmeruumi õhukvaliteeti, niiskust ja muid olulisi näitajaid. Mõõtmine toimub kõigest paarisekundilise intervalliga, seega on saadav informatsioon vägagi täpne. Kui peaks tekkima mingisugune kõrvalekalle, siis andmed jõuavad juba ennetavalt juhtimiskeskusesse, kus saadud infot analüüsitakse ja tänu sellele jõutakse ka vajadusel kiiresti reageerida tekkinud olukorrale [21]. Lisaks on ISKE nõuetest lähtuvalt serveriruumi sissepääs reguleeritud vastavate kontrollimehhanismidega, et tagada ligipääs ainult selleks ettenähtud õigustega isikutele. Kõik eelnevalt mainitud aspektid muudavad igasuguse võimaliku kahju serveritele minimaalseks.

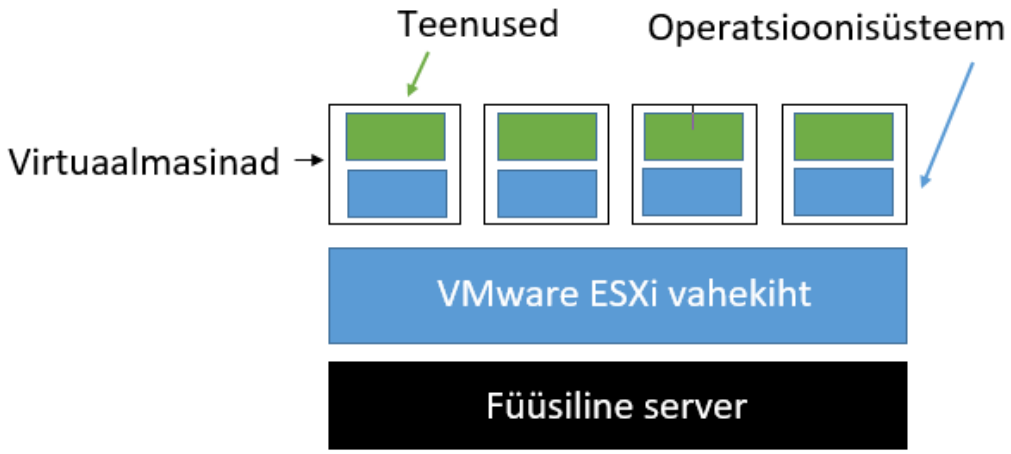
Tänu korralikule serveriruumile on võimalik vältida hilisemaid võimalikke kulutusi kahjude hüvitamiseks. Samuti suutes säilitada serverite jätkusuutlikuse selliste serveriruumide näol, välditakse ka hilisemaid võimalikke komplikatsioone ettevõtte klientide ja partneritega. Seega kindlasti tasub servereid hoida hästi turvatud serveriruumides, mis on ehitatud järgides rangeid turvanõudeid ja –eeskirju ning kohaldatud vastava eesmärgiga võimaldada töökindlaim keskkond serveritele.

3.4 Klastri seadistamine

Töö järgmine osa oli serverite klastri seadistamine, kuhu tuli ühendada serveriruumidesse paigaldatud füüsilised serverid ning hiljem nende peale ehitada vastav arv virtuaalmasinad. Mõlemad füüsilised serverid seadistati ühtemoodi. Käesolevas töös kasutati ettevõttepoolsel

valikul kõige uuemat versiooni VMware virtuaalserverite tarkvarast, kus masinate haldusliideseks oli vSphere Web Client. vCenter on VMware tarkvaral põhinev virtualiseerimisplatvorm, kus toimub virtuaalmasinate seadistamine ja monitoorimine.

Käesolev töö nägi ette ESXi-te ettevalmistamist, nende vCenter'sse lisamist ja selle keskkonna seadistamist vastavate nõuete ja andmete põhjal. VMware ESXi on siis vahekiht füüsiliste serverite ja virtuaalmasinate vahel. See kiht ehitatakse füüsiliste serverite peale ja tänu sellele kihile ei pea operatsioonisüsteemid enam olema otseselt seotud füüsiliste serveritega, mis on väga kaslik aspekt. Antud töö käigus loodi füüsiliste serverite peale virtuaalne vahekiht nimetusega hüperviisor, mille peal jooksutada serveri operatsioonisüsteemi. Sinna peale sai tekitada VM-d, kuhu edasi installida operatsioonisüsteemid ja kõik ettevõtte poolt soovitud rakendused. Antud virtuaalse süsteemi struktuur kuvatakse joonisel 3.4.1.



Joonis 3.4.1. Serverite virtualiseerimine [11]

Kõigepealt installiti ESXi'd uusima versiooniga 6.7.0. Selleks tuli kasutada vastavat liidest, läbi liidese oli võimalik serverit sisse- ja väljalülitada. Kuna töös kasutati Dell'i servereid, siis selleks tuli minna läbi Dell iDRAC'i liidese, mis on mõeldud veebipõhiseks või käsurea pealt kaughaldusülesannete teostamiseks. Autor kasutas esimest võimalust ehk serveri administreerimiseks tuli kirjutada vastava hostinimi või IP aadress veebilehitsejasse. Kasutamiseks tuli server kõigepealt restartida (*reboot*). Nüüd oli võimalik lõpuni viia ESXi-te installimine.

Edasi kasutati VMware vSphere Client liidest. Sinna sai autor ligi vastava IP aadressiga. ESXi tarkvara oli nüüd võimalik välja lülitada ilma, et see mõjutaks füüsilisi servereid, need jäid muudatuste teostamisel endiselt tööle. Läbi selle liidesese sai teostada kõikvajalikke seadistusi klastrile ja hakata looma uusi või registreerima juba olemasolevaid virtuaalmasinaid. Antud töö käigus tekitati vastavad haldusgrupid, mille tarbeks loodi ka eraldi masinad.

VMware vSphere replikatsioon teeb koopiaid virtuaalmasinatest erinevas füüsilises asukohas, mis on kaslik andmekaitseks ja katastroofidest taastumiseks [15]. Töös seadistati vastav momentvõtte (*Snapshot*) lahendus. See on üks võimalus, kuidas varundada mingit kindlat olekut. Nendest on kasu, kui administreerimisel läheb midagi valesti, siis saab väga lihtsasti minna tagasi algsesse olekusse, mis eelnevalt varundatud sai. Nende tegemiseks määrati järgmised parameetrid: kordade arv kuus, nädalapäev ja kellaaeg. Näiteks pühapäeval kell 21:00 ja hoitakse 30 päeva. *Snapshot* oleks kasulik ka ära kustutada, muidu hakkab see hiljem pidurdama masina enda tööd. Nende varustamise maksimaalne soovitatav aeg on umbes 15 minutit, selle ajaga peaks jõudma vastava ülevaate ja korrektuurid ära teha.

Lisaks tutvuti masina kustutamise protsessiga vCenter-is. Selleks tuli lihtsalt server välja lülitada ja kustutada kettalt. Sellisel juhul kogu konfiguratsioon ja kettad kustutati. Ainult klastrist kustutamiseks piisas masina eemaldamisest inventuurist. Kokkuvõttes on läbi vastava tarkvara vägagi lihtne virtuaalmasinaid installida, hallata, seadistada ja eemaldada.

3.5 Virtuaalserverite install

Lõputöö käsitleb virtuaalmasinate loomist füüsiliste serverite peale. Virtuaalmasinaid on võimalik luua vastavalt vajadusele mitmeid, igaühele installida oma operatsioonisüsteem ja kõik panna jooksma sama füüsilise serveri peal ning seda siis tänu eelnevalt nõuete järgi seadistatud hüperviisorile. Käesolevas töös tuli tähelepanu pöörata asjaoludele, et loodav süsteem sarnaneks oma tööpõhimõttelt vanale süsteemile. Selleks oli mõistlik panna uus süsteem käima paralleelselt vanaga. Virtuaalmasinaid tuli mõlema füüsilise serveri peale installida sama arv ja üksteisele tehtavate samasuguste seadistustega.

Kui virtuaalserverite klaster oli tekitatud ja vastavalt seadistatud, siis tegeleti ESXi-te peale virtuaalmasinate installimisega. Masinate installimisel määrati neile ettevõttepoolsete andmete põhjal sobilikud ressursid nagu CPU, RAM, kõvaketta mälu ja andmemassiiv ning installeeriti vastavad operatsioonisüsteemid. Antud töös kasutati ettevõttepoolsest valikust lähtudes masinatel Linux operatsioonisüsteemi versiooniga Debian GNU 9.0. Kontrolli mõttes tuli ka üle vaadata, kas masinad ikka tekkisid sinna klastrisse, kuhu soovitud oli.

Võrgukaart (NIC) ehk võrguliidese kaart on arvuti ja sideliini vaheline liides, mis saadab ja võtab vastu infot [22]. Esialgu jäid masinatele teatud põhjusel võrgukaardid lisamata. Ajutiselt on võimalus valida mäluseadeks (*Storag*e) localDS, mida üldiselt kasutatakse vähemtähtsamate andmete jaoks. Hiljem pandi masinatele külge ka võrgukaardid, seda järgmisel põhjusel, et kaks masinat pääseksid mõlemad üle IP võrgu ühele võrgukettale ligi. See on vajalik selleks, et kui ühe masinaga peaks midagi juhtuma, saaks teine masin jätkata esimese tööd. Sellega olid virtuaalmasinate mäluseaded ka seadistatud.

Seadmete konfigureerimisel tuli vanade serverite IP-aadressid uutega asendada. Kõik võrgud pidid üksteisest erinema kasutades igaüks isemoodi IP-aadressi. IP-aadress on oluline põhjusel, et oleks võimalik adresseerida antud masinaid. Käesolevat serverite süsteemi uuendades oli oluline jälgida, et uued serverid oleksid ühendatud kõikidesse võrkudesse, kus vanad asusid ning kust ja kes vastavatele masinatele ligi pääsevad, et süsteem ei kaotaks oma vana konfiguratsiooni, mis on kindlasti väga tähtis antud töös.

VMware vMotion lahendus võimaldab teisaldada töötavaid virtuaalmasinaid ühelt ESXi hostilt teisele ESXi hostile ilma teenust katkestamata ehk tegemist on reaalaja migratsiooniga. See suurendab andmete ja andmetöötluse ressursside kättesaadavust. [15] Kokkuvõttes oli antud juhul oluline kasutada vMotioni lahendust, et masinad suudaksid üksteise mälu lugeda, kui seda hiljem vaja peaks minema. Samuti toimetab vMotion ressurssidega, seades ritta tähtsamad ja vähemtähtsamad asjad ning tehes vastavaid muudatusi selle järgi, mis kasulik on ehk kus parasjagu rohkem ressurssi nagu näiteks mälu on.

Suur kättesaadavus (HA) ühendab serverite hoste ja nendel asuvaid virtuaalmasinaid klastris nii, et vastava rikke korral virtuaalmasinad nurjunud hosti peal taaskäivitatakse asendushosti peal. Suure kättesaadavusega klastreid on oluline jälgida. Selleks rakendab VMware vSphere DRS jagatud haldusliidest, et oleks võimalik vastava klastri ressursse monitoorida ja hallata. [15] Antud töös nähti vajadust lülitada DRS kindlasti sisse.

Kogu automaatiseerituse poolt aga ei ole alati otstarbekas sisse lülitada, kuna pisemate hädade korral võib see osutuda hoopis kahjulikuks ehk lahendus võib hakata iga lihtsama asja peale süsteemi restartima. Siin oli veel nii mõningaid väiksemaid seadistusi. Tänu valitud tarkvarale oli aga virtuaalserverite installimise näol tegemist vägagi kiire ja lihtsa protsessiga.

3.6 Testimine

Testimine on samuti üks olulisemaid protsesse antud töö tegemise juures, et hinnata vastava töö kvaliteeti ja nõuetele vastavust. Läbi selle on võimalik kontrollida kogu süsteemi toimimist ja tuvastada võimalikud vead. Testimise käigus on näha, kuidas süsteemi erinevad osad üksteisega käituvad ja koostööd teevad. Vastavalt vajadusele on viimane aeg teha veel vajaminevad korrektuurid enne süsteemi kasutuselevõttu. Käesolevas töös testiti serverite dubleerituse töötavust.

Dubleeritus on süsteemi turvalisuse võtmes väga oluline seadistus, sest see suurendab süsteemi töökindlust ja kiirust. Serveri maasolek või probleemid seoses jõudlusega võivad kaasa tuua väga suuri kahjusid ja häiriksid ka ettevõtte poolt pakutava teenuse kvaliteeti, mis omakorda pahandaks kliente. Dubleerituse tööpõhimõte seisneb selles, et kui süsteemis peaks esinema mingisugune rike ja üks server lõpetab tänu sellele töö, siis järgmine server võtab üle esimese serveri töö ja teenus töötab samamoodi edasi. Lisaks serveritele on võimalik dubleerida ka näiteks erinevaid ühendusteid ja võrguseadmeid. [22]

Dubleerituse testimiseks lülitati *master* masin välja, et vaadata, kas *slave* masin asub master masina asemele. Algselt oli esimene masin seadistatud *master* rolli ja teine masin oli rollis *slave*, mis tähendab lühidalt, et esimene oli töös ning teine lihtsalt varuks. Sama protsessi testiti ka vastupidi ehk lülitati teine masin välja ja vaadati, kas süsteem läheb esimese masina peal uuesti käima. Tulemusena toimis kogu protsess nii nagu pidi, küll aga väikese viiteajaga (*down time*) nagu ette nähtud ka oli. Viiteaeg oli umbkaudselt kuskil alla minuti ehk väga lühike ja halba see endaga kaasa lihtsalt ei jõudnudki tuua. Pigem on see väga positiivne külg dubleerituse juures, sest manuaalprotsessina võib masinate vahetamine võtta väga kaua aega.

3.7 Tulemused ja arutelu

Käesolevas lõputöös viidi läbi füüsiliste serverite uuendusprotsess virtuaalserverite loomise näol. Esialgu tutvuti valdkonna kirjandusega, ettevõtte materjalidega ja koguti kokku andmed ja nõuded ettevõtte töötajatelt vastava töö tegemiseks. Töös viidi läbi füüsiliste serverite paigaldamine serveriruumidesse, mis olid sätestatud vastavate turvanõuetega. Seejärel serverite klastri installimine ja seadistamine, virtuaalmasinate klastrisse loomine ja seadistamine järgides etteantud nõudeid. Viimaks testiti süsteemi, et veenduda vastavate seadistuste toimivuses. Tulemused ja järeldused põhinevad tehtud tööl.

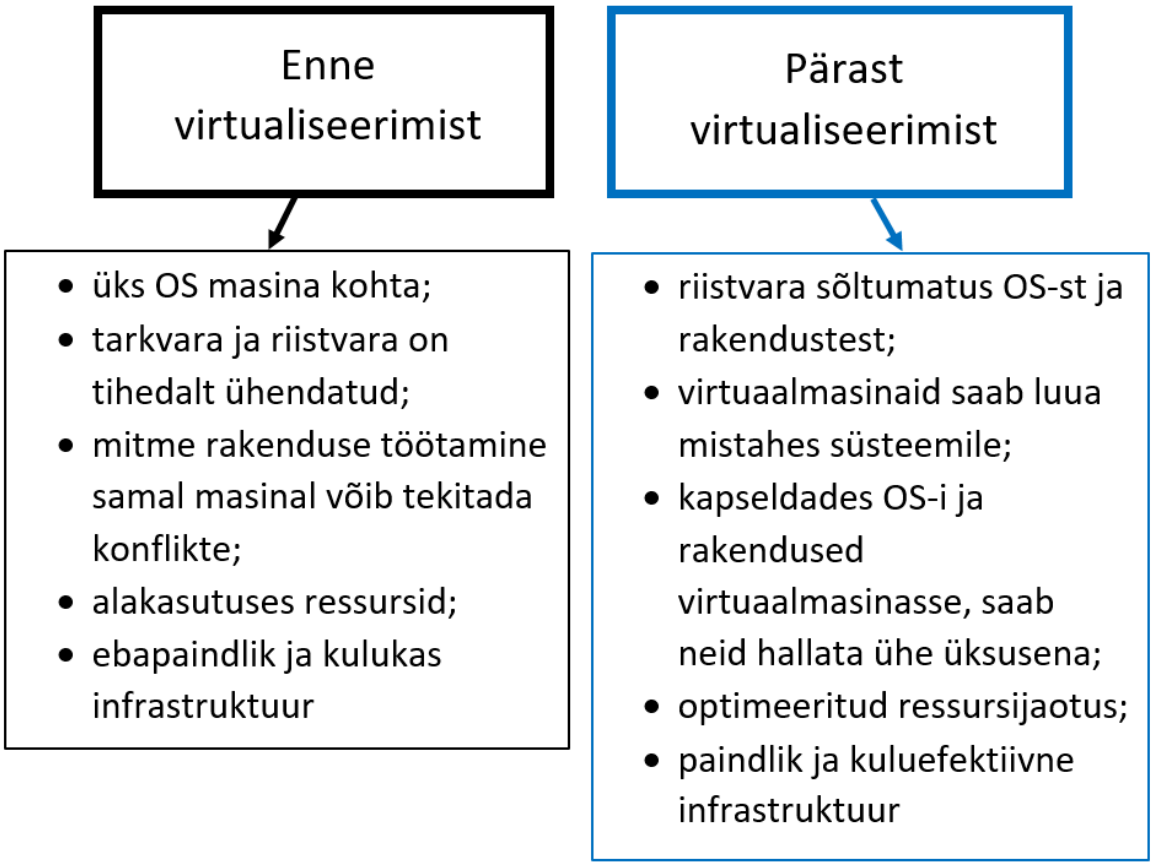
Autor seadis üles missioonikriitilise võrgu halduseks vajaliku IT infrastruktuuri Tele2 Eesti AS näitel. Kogu protsess kulges üldiselt suuremate tõrgeteta. Vahepeal viibis protsess küll pelgalt litsentside puudumise tõttu või kuna suhtlusliin käis läbi mitmete inimeste, siis võttis aega ka vajaliku informatsiooni kogumine ja kooskõlastamine. Samas saab autor välja tuua, et antud protsessi läbiviimist hõlbustasid oluliselt ettevõttes varem praktikal olles saadud ligipääsud süsteemidele ja varasem kokkupuude antud süsteemidega töötades. Ligipääsude ja varasema kokkupuute puudumisel oleks autoril kindlasti ettevõttes töö läbi viimiseks rohkem aega kulunud.

Töö esimeses etapis paigaldati füüsilised serverid serveriruumidesse. Autori arvates on serverite hoiustamine hästi korraldatud serveriruumides väga roluline ja kasulik ettevõttele endale. Sarnases olukorras tasub sellele kindlasti mõelda näiteks kapiserverite kasutamise asemel, mis võib tuua rikete korral kaasa väga suuri kulutusi nii finantsiliselt, ajaliselt kui ka klientide ja partnerite vajadusi arvestades.

Töö teises etapis viidi läbi virtuaalserverite klastri seadistamine kasutades VMware tarkvara. Autori arvates tegi valitud tarkvara kasutamine kogu serverite klastri virtualiseerimise ja seadistamise protsessi väga kiireks ja lihtsustas seda oluliselt. Vajadusel on muudatuste läbi viimine süsteemis samuti väga kiiresti teostatav.

Töö kolmandas etapis installiti klastrisse vajalikud virtuaalserverid. Autor arvab samuti, et virtuaalserverid vastavate seadistustega muudavad süsteemi igati turvalisemaks ja kuna ressursse saab vastavalt vajadusele igal ajal kohandada, siis on süsteem ka palju efektiivsem. Tarkvara pakub erinevaid võimalusi ka süsteemis teatud tegevuste automatiseerimiseks, mis võib mõningatel juhtudel tulla samuti igati kasuks. Joonisel 3.7.1 kuvatakse virtualiseerimisprotsessi tulem. Pärast virtualiseerimisprotsessi läbiviimist oli võimalik ühe füüsilise serveri peale luua mitmeid virtuaalmasinaid, millel on igaühel oma operatsioonisüsteem. Seega serveri tarkvara ja riistvara ei

ole enam tihedalt ühendatud. Samuti jäävad olemata mitme rakenduse põhjustatud konfliktid samal masinal töötamisest. Lisaks tõi virtualiseerimine kaasa ressursside paindliku ja optimeeritud kasutuse, mis aitab hoida kulusid kokku. Kokkuvõttes on süsteem nüüd dünaamiline ja kuluefektiivne.



Joonis 3.7.1 Virtualiseerimisprotsessi tulemi võrdlus esialgse süsteemiga

Töö neljandas etapis testiti vastavate seadistuste toimivust süsteemis. Autor arvab, et testimise protsessi ei tohiks selliste tööde käigus kindlasti ära unustada. Selles etapis võivad tulla välja tegemata jäänud seadistused või andmete puudulikkus, mis on enne süsteemi tööle laskmist kindlasti oluline veel üle vaadata ja vastavad korrektuurid teha, veendumaks hilisemaks süsteemi soovitud toimimiseks.

Kokkuvõttes sai käesoleva lõputöö käigus töö peaeesmärk täidetud ning samuti ka kõik väiksemad etapid edukalt sooritatud.

KOKKUVÕTE

Käesoleva rakenduskõrgharidustöö eesmärk oli seada üles IT infrastruktuur missioonikriitilise võrgu halduseks ettevõtte Tele2 Eesti AS näitel, põhjusel, et süsteemid ja töövahendid vananevad ning pole enam nii võimekad. Antud probleem oli ettevõtte jaoks kriitiliselt oluline. Lõputöö pealkiri sõnastati ettevõtte IP ja VoIP teenuste tehnilise osakonna juhi poolt ning töö koostati tehnika osakonnas osaliselt koostöös IT taristu juhiga.

Töös viidi läbi füüsiliste serverite paigaldamine serveriruumidesse, serverite virtualiseerimine ja virtuaalmasinate seadistamine VMware tarkvarat kasutades. Lõpuks testiti süsteemile seadistatud tingimuste töökindlust. Tulemusena seadis autor üles vastava infrastruktuuri arvestades ettevõttepoolseid võimalusi ning töö käigus väljaselgitatud nõudeid. Testides süsteemi, toimis kõik nii nagu pidi.

Töö edasiarendusena on plaanitud alajaamade andmesidevõrgu teenused kanda üle loodud keskkonda, siis on ka ettevõtte poolne eesmärk täielikult täidetud ja saab kogu süsteem tervikuna kasutusse võetud.

SUMMARY

The professional higher education thesis is written with the purpose of setting up the infrastructure of mission critical data network management based on the example of company named Tele2 Estonia AS due to old servers, old tools and lack of capacity on servers. This problem was critically important for the company. The title of the thesis was worded by the company's IP and VoIP Services Technical Department Manager and was created in Technical Department and in cooperation with IT Infrastructure Manager.

The work was related to setting up the physical servers to the server environement, server virtualization and setting up virtual servers by using the VMware software. For the results the author did the described infrastructure setup by considering company's opportunities and given specifications clarified in this process. System test results were positive.

The future work will be configuring all the substation network applications as monitoring and management tools. After that would be the company's main purpose fully complete and the system as whole would be in use.

KASUTATUD KIRJANDUSE LOETELU

1. **Andmekaitse ja infoturbe leksikon** [*WWW*] https://akit.cyber.ee/term/ (09.05.2019).
2. **Infosüsteemide turvameetmete süsteem ISKE.** (2014) [*WWW*] https://iske.ria.ee/7_01 (28.04.2019).
3. **Tian W., Zhao Y.** (2015) Optimized Cloud Resource Management and Scheduling – Theory and Practice. Chapter 3, pp. 51-77 [*WWW*] https://www.sciencedirect.com/topics/computer-science/physical-server (10.05.2019, in English).
4. **VMware, Inc.** (2006) Virtualization Overview [*WWW*] https://www.vmware.com/pdf/virtualization.pdf (19.05.2019, in English).
5. **Saar J.** (2011) 2 Operatsioonisüsteemid [*WWW*] https://eopearhiiv.edu.ee/e-kursused/eucip/haldus/2_operatsioonissteemid.html (23.05.19).
6. **Schmidt R. W. Rajagopal S.** (2014) High availability virtual machine cluster [*WWW*] https://patents.google.com/patent/US8554981B2/en (19.05.2019, in English).
7. **Mulla H.** Serverivalik – kapike nurgas või pilveke taevas? [*WWW*] http://www.proit.ee/tag/miks-on-virtuaalserver-parem-kui/ (06.05.2019).
8. **Tech-FAQ.** Server Clustering Technologies and Concepts [*WWW*] http://www.tech-faq.com/server-clustering-technologies-and-concepts.html (23.05.2019, in English).
9. **Volico.** (2014) When Your Business Might Need Server Clustering [*WWW*] https://www.volico.com/when-your-business-might-need-server-clustering/ (20.05.2019, in English).
10. **Chong J., Pal P., Atigetchi M., Rubel P., Webber F.** (2005) Survivability Architecture of a Mission Critical System: The DPASA Example [*WWW*] https://www.acsac.org/2005/papers/136.pdf (28.04.2019, in English).
11. **Wmware, Inc.** (2014) Virtualization Essentials [*WWW*] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/ebook/gated-vmw-ebook-virtualization-essentials.pdf (08.05.2019, in English).
12. **Haberst Infra AS.** Mis on virtuaalserver? [*WWW*] http://www.haberst.ee/et/mis-virtuaalserver (09.05.2019).
13. **Mulla H.** Serverivalik – kapike nurgas või pilveke taevas? [*WWW*] http://www.proit.ee/tag/miks-on-virtuaalserver-parem-kui/ (06.05.2019).
14. **Termnet Eesti OÜ.** Pilveteenuse eelised [*WWW*] https://www.termnet.ee/pilveteenus/pilveteenuse-eelised (09.05.2019).

15. **VMware IT Academy.** Introduction to Virtualization [*WWW*] https://www.netdevgroup.com/support/documentation/ndg_introduction_to_virtualization_web.pdf (08.05.2019, in English).
16. **VMware, Inc.** (2006) Virtualization Overview [*WWW*] https://www.vmware.com/pdf/virtualization.pdf (19.05.2019, in English).
17. **Reed J.** (2018) Physical Servers vs. Virtual Machines: Key Differences and Similarities [*WWW*] https://www.nakivo.com/blog/physical-servers-vs-virtual-machines-key-differences-similarities/ (26.05.2019, in English).
18. **Tholeti B. P. R.** (2013) Handbook of Fiber Optic Data Communication (Fourth Edition) – A Practical Guide to Optical Networking. Chapter 16, pp. 387-416 [*WWW*] https://www.sciencedirect.com/topics/computer-science/service-virtualization (23.05.19, in English).
19. **Sitaram D., Manjunath G.** (2012) Moving To The Cloud – Developing Apps in the New World of Cloud Computing. Chapter 9, pp. 351-387 [*WWW*] https://www.sciencedirect.com/science/article/pii/B9781597497251000093 (23.05.2019, in English).
20. **Smartsheet.** Infrastructure Management 101: A Beginner's Guide to IT Infrastructure Management [*WWW*] https://www.smartsheet.com/it-infrastructure-management-services-guide (19.05.2019, in English).
21. **Pau A.** (2016) Tele2 investeeris 1,3 miljonit uude tehnokeskusesse [*WWW*] https://tehnika.postimees.ee/3713187/tele2-investeeris-1-3-miljonit-uude-tehnokeskusesse?fbclid=IwAR0WzP0HRair0TvAYO5_Wxqz6RkeMIXeLF4inR64V6FeExcExP7J7e7VXwE (08.05.2019).
22. **Laaneoks E.** (2010) Sissejuhatus võrgutehnoloogiasse [*WWW*] http://www.vorgud.ee/wp-content/uploads/2014/08/Sissejuhatus_vorgutehnoloogiasse.pdf (26.05.2019).