

**Tartu Rakenduslik Kõlleđ**

**IKT-osakond**

**Iso21**

**Karl Jaagola ja Martin Tambets**

**SEIRESÜSTEEMI PAIGALDAMINE JA SEADISTAMINE SERVER MANAGEMENT  
OÜ KLIENTIDE TEENUSTE MONITOORINGUKS**

**Lõputöö**

**Juhendaja Timo Puistaja**

**Tartu 2023**

Oleme koostanud kursuse lõputöö iseseisvalt. Kõik koostamisel kasutatud teiste autorite tööd, põhimõttelised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

Tartus,

„Seiresüsteemi paigaldamine ja seadistamine Server Management OÜ klientide teenuste  
monitooringuks“ 2023. a

Karl Jaagola

Tartus,

„Seiresüsteemi paigaldamine ja seadistamine Server Management OÜ klientide teenuste  
monitooringuks“ 2023. a

Martin Tambets

Kaitsmisele lubatud:

„Seiresüsteemi paigaldamine ja seadistamine Server Management OÜ klientide teenuste  
monitooringuks“ 2023. a

Juhendaja Timo Puistaja

# SISUKORD

Sissejuhatus .....	5
1 Planeerimine.....	6
1.1 Hetkeolukord .....	6
1.2 Aja planeerimine.....	6
1.3 Serverite ja seiresüsteemide valik .....	7
1.4 Ettevõtte klientide andmebaasi analüüs .....	8
1.5 Suhtluskanalid ja töövahendid.....	9
1.6 Riskianalüüs .....	9
2 Praktiline teostus.....	10
2.1 VPSide soetamine ja turvamine.....	10
2.2 Uptime Kuma .....	12
2.2.1 Seiresüsteemi paigaldamine.....	12
2.2.2 Hostide seiresse lisamine .....	14
2.2.3 Teavituste seadistamine.....	14
2.3 Zabbix.....	15
2.3.1 Seiresüsteemi paigaldamine.....	15
2.3.2 Hostide seiresse lisamine .....	16
2.3.3 Teavituste seadistamine.....	22
2.4 Testimine.....	25
3 Meeskonnatöö ja eneseanalüüs.....	27
3.1 Meeskonnaanalüüs.....	27
3.2 Martin Tambets .....	27
3.3 Karl Jaagola .....	28
Kokkuvõte.....	29
Kasutatud allikad .....	30
Lisad .....	32
Lisa 1 Uptime Kuma skeem Miros .....	32
Lisa 2 Zabbixi skeem Miros .....	33
Lisa 3 Uptime Kumasse veebilehe lisamine (andmed pildil on näitlikud) .....	34
Lisa 4 Uptime Kumasse ruuteri lisamine (andmed pildil on näitlikud).....	35

Lisa 5 Uptime Kuma teavitus (andmed pildid on näitlikud) .....	36
Lisa 6 ChatGPT sisend (Zabbixi serveri paigaldamise skript) .....	37
Lisa 7 ChatGPT väljund (Zabbixi serveri paigaldamise skript) .....	38
Summary.....	39

## SISSEJUHATUS

Käesolev projekt tehti IT-ettevõtte Server Management OÜ jaoks. Server Management OÜ on tegutsenud aastast 2016, ettevõttes töötab üks isik, kelleks on omanik Timo Puistaja. Ettevõtte pakub Eestis erinevaid IT-teenuseid terviklahenduste näol, näiteks pilveteenuseid, varundust, serveriteenuseid, valvekaamerate paigaldust ning haldust ja palju muud.

Aastate jooksul on Server Management OÜ-l tekkinud arvestatav hulk erinevaid kliente, kelle infrastruktuuri hooldamise ja haldamisega ettevõtte tegeleb. Tulenevalt seadmete arvukusest soovib Server Management OÜ keskset seiresüsteemi, mis tagaks ülevaate olukorrast ning parandaks reageerimiskiirust tõrgete puhul.

Projekti eesmärgiks oli ettevõttele luua puuduolev lahendus seiresüsteemi näol. Projekt hõlmas endas ettevõtte vajadustest lähtuvalt seiresüsteemide ja serverite valikut, nende seadistamist, ettevõtte klientide seadmete seiresse lisamist ja vastavate automaatteavituste seadistamist. Projekt lõppes ettevõttele seiresüsteemi ja dokumentatsiooni üle andmisega.

# 1 PLANEERIMINE

## 1.1 Hetkeolukord

Projekti algushetkel puudus ettevõttel keskne seiresüsteem, mille abil saaks monitoorida klientide võrguseadmeid, kodulehekülgi ja servereid. Ettevõttel puudus ka server, millele seiresüsteem paigaldada. Ettevõtte ei olnud veel otsustanud, millised kliendid ja millised nende seadmed seiresse lähevad.

## 1.2 Aja planeerimine

Projekti teostajateks olid Martin Tambets ja Karl Jaagola ning teostamise ajavahemikuks oli 11.01.2023-21.05.2023. Õigeaegselt lõpptulemuseni jõudmiseks koostati ka esialgne ajagraafik, milles olid välja toodud kõik vajalikud tegevused (vt Sele 1).

12.01.2023	Hinna ja kvaliteedi suhte alusel parima virtuaalse privaatserveri teenusepakkuja valimine	Karl Jaagola Martin Tambets
12.01.2023	Virtuaalse privaatserveri soetamine	Karl Jaagola Martin Tambets
12.01.2023	Virtuaalse privaatserverile operatsioonisüsteemi valik ja paigaldus	Karl Jaagola Martin Tambets
17.01.2023	Virtuaalse privaatserveri seadistus ning Uptime Kuma seiresüsteemi paigaldus ja seadistus	Karl Jaagola Martin Tambets
02.03.2023	Seiresüsteemi lisatavate serverite ja muude teenuste kaardistamine	Karl Jaagola Martin Tambets
31.03.2023	Klientide võrguseadmete seadistamine	Karl Jaagola Martin Tambets
07.04.2023	Ettevõtte klientide serverite ja teenuste lisamine seiresüsteemi	Karl Jaagola Martin Tambets
14.04.2023	Teavituste seadistamine seiresüsteemis	Karl Jaagola Martin Tambets
14.04.2023	Ettevõttele tehtud tegevuste kohta dokumentatsiooni loomine	Karl Jaagola Martin Tambets
Kirjaliku töö kirjutamine		
28.04.2023	Lõputöö kirjutamine	Karl Jaagola Martin Tambets
Kirjaliku töö vormistamine		
19.05.2023	Lõputöö vormistamine	Karl Jaagola Martin Tambets

Sele 1 Esialgne projekti ajagraafik

### 1.3 Serverite ja seiresüsteemide valik

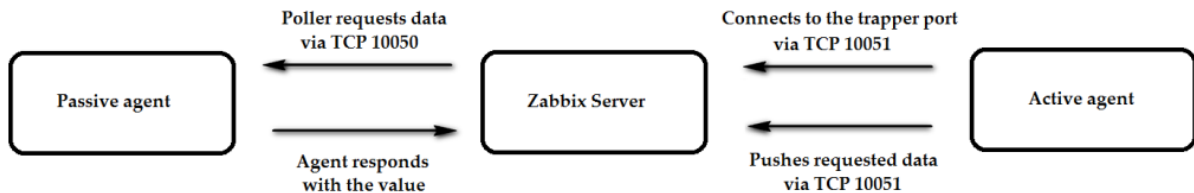
Esmalt soovis ettevõtte, et võrreldaks Euroopas tegutsevaid VPS-teenuspakkujaid (sh Contabo, Ultrahost, Cloudways, Hostinger, A2 Hosting, Kamatera, Bluehost ja Hostika) hinna ja kvaliteedi suhte alusel. VPS-teenusepakkujatest osutus valituks Contabo, sest nad pakkusid samaväärsete näitajatega serverit ligi poole odavamalt kui teised teenusepakkujad. Antud projekti raames füüsilise serveri ostmist ei kaalutud, sest virtuaalse privaatserversi hooldamisega ei pea ettevõtte ise tegelema. Lisaks oleks pikemas perspektiivis füüsilise serveri ülevälvaldamine ja uuendamine osutunud kulukamaks kui VPS-teenusepakkujale makstav kuumakse.

Esialgvalt valiti projekti lõppeesmärgi saavutamiseks avatud lähtekoodiga isehostitav seiresüsteem Uptime Kuma. Sellega on võimalik jälgida võrguseadmete, serverite, andmebaaside, konteinerite ning veebilehtede ülevälvaloleku aega, kasutades protokolle HTTP, HTTPS, ICMP ja TCP. Uptime Kumaga saab teavituste saatmiseks kasutada SMSi, e-posti ja rakendusi, nagu Discord, MS Teams, Telegram jne. Programmi loojaks on Hong Kongist pärit arendaja Louis Lam, kelle eesmärgiks oli luua tasuta alternatiiv Uptime Robotile. [1] Uptime Kuma *live* demo versioon sai kõigile kättesaadavaks 2021. aasta septembris. [2]

Kuigi alguses oli mõtte kasutada ainult seiresüsteemi Uptime Kuma, siis juba planeerimisfaasis jõuti koos ettevõttega järeldusele, et klientide serverite jälgimiseks oleks vaja klientide tulemüüridesse tekitada liiga suur arv potentsiaalseid turvaauke. Nimelt oleks Uptime Kuma puhul serverite jälgimine toimunud üle TCP portide ja iga jälgitava seadme või teenuse jaoks oleks tulnud tulemüüris avada uus port. Seetõttu otsustati Uptime Kuma kõrval kasutusele võtta ka seiresüsteem Zabbix, mille jaoks osteti teine eelmisega identne Contabo VPS.

Sarnaselt Uptime Kumale on Zabbix avatud lähtekoodiga seiresüsteem. Zabbixi abil on võimalik reaajas jälgida IT-infrastruktuuri, sh servereid, virtuaalmasinaid, rakendusi, teenuseid, andmebaase ja võrke. [3] Võrreldes Uptime Kumaga on Zabbixi suur eelis see, et lisaks seadmete ülevälvaloleku ajale on võimalik ka jälgida protsessori- ja mälu kasutust, kasutusel olevat andmepinda, võrgu koormust ning palju muud. Veelgi olulisem on aga see, et erinevalt Uptime Kumast on Zabbixil seadmete jälgimiseks meetod, mis ei nõua klientide tulemüürides aukude tegemist. Zabbixi kolmest põhilisest jälgimismeetodist on selle projekti raames kõige olulisem Zabbixi aktiivne agent (inglise keeles *active agent*).

Aktiivse agendi põhimõte seisneb selles, et seadmelt saadetakse serverile info ilma, et server seda ise küsiks. [4] Suhtlus algatatakse agendi poolt ja seega ei ole vaja kliendi tulemüüris iga seadme kohta uut porti avada. Passiivse agendi puhul käib aga Zabbixi server agendi käest infot küsimas ning agent vastab (vt Sele 2). Nii aktiivse kui ka passiivse agendi näol on tegemist programmiga, mis paigaldatakse jälgitavasse seadmesse.



Sele 2 Passiivse ja aktiivse agendi tööpõhimõte [4]

Kolmandaks jälgimismeetodiks on SNMP (*Simple Network Management Protocol*). SNMP tööpõhimõte sarnaneb passiivse agendi omale, aga SNMP-d kasutatakse seadmetes, kus puudub toetatud operatsioonisüsteem. SNMP-ga jälgitakse näiteks seadmeid nagu printereid, *switch*e, ruutereid ja UPS-e. [5]

Zabbixilt teavituste saamiseks saab kasutada e-posti, SMS-i ja rakendusi, nagu näiteks Office365, Jira, Discord ja Mattermost. Zabbixi loojaks on Lätist pärit arendaja Alexei Vladishev, kelle esialgne soov oli tema enda halduses olevaid seadmeid jälgida. [6] Zabbixi esimene versioon lasti välja 2001. aastal ja ettevõtte asutati Lätis aastal 2005. [7]

Projektis võeti kasutusele nii Uptime Kuma kui ka Zabbix, sest mõlemad pakkusid ettevõttele meelepäraseid võimalusi. Hoolimata sellest, et kõiki jälgitavaid seadmeid ei olnud turvakaalutlustest lähtudes mõistlik Uptime Kumasse lisada, otsustati, et tänu elegantsele ja ülevaatlikule *dashboard*ile hakatakse seda kasutama klientide ruuterite ja kodulehekülgede ülevaleoleku aja jälgimiseks. Zabbixisse lisati aga serverid ja võrgusalvestid, mille kohta oleks vaja koguda detailsemat infot.

#### 1.4 Ettevõtte klientide andmebaasi analüüs

Selleks, et saada ülevaade, millised klientide seadmed lisatakse seiresse, oli vaja ettevõtte poolt kasutatavas paroolihaldustarkvaras sorteerida kliendid ja nende seadmed ning koostatud nimekiri koos ettevõtte omanikuga üle vaadata. Peale arutelu otsustati, et klientide ruuterid ja koduleheküljed lisatakse Uptime Kumasse ning serverid ja võrgusalvestid lisatakse Zabbixisse. Nimekirja alusel kuulus Uptime Kumasse lisamisele ■ ruuterit ja ■ kodulehekülge



ning Zabbixisse ■ seadet (sh ■ Linuxi serverit, ■ Windowsi serverit. ■ VMware ESXI hosti ning ■ Synology võrgusalvesti).

Projekti visualiseerimiseks kasutati projektijuhtimistarkvara Miro. Koostati kaks erinevat joonist Uptime Kuma ja Zabbixi kohta (vt Lisa 1 ja Lisa 2). Joonisele kanti seadmete IP-aadressid, tootja- ja mudelinimed, operatsioonisüsteemide tüübid ja versioonid ning seadmete rollid.

## 1.5 Suhtluskanalid ja töövahendid

Projekti alguses lepidi kokku, et suhtluskanaliteks on e-post, Microsoft Teams ja mobiiltelefon. Töövahenditena kasutati Tartu Rakendusliku Kolledzi virtualiseerimiskeskonda, kus toimus testimine, Contabo virtuaalseid privaatservereid, kuhu paigaldati seiresüsteemid, projekti haldustarkvara Miro, millega visualiseeriti projekti kulg ning programmid PuTTY, PuTTY KeyGen, RDP, OpenVPN, Cisco AnyConnect ja WinBox. Lisaks kasutasid projekti teostajad oma isiklikke süle- ja koduarvuteid.

## 1.6 Riskianalüüs

Potentsiaalsete riskide tuvastamiseks ning ennetamiseks koostati projekti planeerimisfaasis riskimaatriksi. Riskimaatriksis on välja toodud riskid ja nende kirjeldused, nende tagajärjed, realiseerumise tõenäosus ja mõju ning võimalikud vastumeetmed (vt Sele 3).

nr	Risk ja kirjeldus	Tagajärjed	Tõenäosus	Mõju	Vastumeetmed	Vastutaja
<b>Planeerimine ja juhtimine</b>						
1	Halb aja planeerimine	Ei saa seatud tähtaegadeks ülesandeid lõpetatud	Keskmine	Kriitiline	Hetkeolukorra hinnang ning vajadusel uute realistlike tähtaegade püstamine	Karl ja Martin
2	Ebapiisav info vahetus (koostöö)	Ebaefektiivne aja kasutus	Vaike	Keskmine	Iganädalasele koosolekud	Karl ja Martin
3	Koostöö konfliktid	Projekt jääb lõpetamata	Vaike	Kriitiline	Konkreetsed rollide jaotus, paika pandud vastutused	Karl ja Martin
<b>Nõuded ja skoop</b>						
4	Projekt muutub liiga mahukaks	Projekt saab valmis, kuid osaliselt	Keskmine	Keskmine	Kliendiga koostöös realistlike eesmärkide püstamine, arvestades etteantud ajakava	Karl, Martin ja Timo
5	Nüüete jooksvalt muutumine	Esialgse projekti eesmärgid jäävad saavutamata	Keskmine	Kriitiline	Kliendiga konkreetne suhtlus püsivaks esialgses eesmärkides	Karl, Martin
6	Kolmanda osapoolse ligipääs süsteemile	Praktikaettevõtte klientide andmete lek (võrk)	Vaike	Kriitiline	Seadmete turvamine kasutades parimaid praktikaid	Karl ja Martin
<b>Kompetents</b>						
7	Puudulikud teadmised	Aeglane tööprotsess	Keskmine	Keskmine	Dokumentatsiooni läbi töötamine	Karl ja Martin
8	Serveri uuenduste tegemine/vale seadistamine	Andmete kadu	Vaike	Kriitiline	Snapshoti tegemine vahetult enne uusi seadistusi	Karl ja Martin

Sele 3 Riskimaatriks

## 2 PRAKTILINE TEOSTUS

### 2.1 VPSide soetamine ja turvamine

Töö teostamiseks osteti Contabo koduleheküljelt kaks identset VPSi. Serveritel on neljatuumalised protsessorid, 8 GB operatiivmälu ja 200 GB SSD (vt Sele 4). Antud tehnilised spetsifikatsioonid on sobivad nii Ubuntu 22.04 operatsioonisüsteemi kui ka Uptime Kuma ja Zabbixi tarkvarade sujuvaks töötamiseks. Ubuntu serveri minimaalsed süsteeminõuded on 1 Ghz CPU, 1 GB RAMi ja 2,5 GB andmepinda. Uptime Kuma vajab minimaalselt 1 Ghz CPU, 512 MB RAMi ja 10 GB andmepinda. Zabbixi puhul sõltuvad süsteeminõuded mõõdikute arvust. Ühe mõõdiku all mõeldakse ühte jälgitavat seadet koos ühe *triggeri* ja graafikuga. Tulenevalt Zabbixi dokumentatsioonist peaks 1000 mõõdiku puhul vaja minema minimaalselt kahetuumalist protsessorit ning 8 GB RAMi.

Kummagi VPSi esmakordne seadistustasu oli 5,99 eurot koos kuutasuga 5,99 eurot. Seega tuli ettevõttel kahe VPSi eest maksta 23.96 eurot. Ettevõttel tuleb lisaks maksta igakuist kuutasu 11,98 eurot.

**Cloud VPS S** Monthly Base Price €5.99

CPU	RAM	STORAGE	SNAPSHOT
4 vCPU Cores	8 GB RAM	50 GB NVMe or 200 GB SSD	1 Snapshot

**1. Select your term length**

1 Month

**2. Region**

European Union (Germany)

United Kingdom €1.20

**Order Summary** Share

**Cloud VPS S**

Server Quantity: 1

**Details**

- Contract Period: 1 Month
- European Union (Germany)
- 200 GB SSD
- Ubuntu 22.04
- 32 TB Out + Unlimited In

Monthly €5.99

One-Time Setup Fee €5.99

Due Today €11.98

Next

Sele 4 Contabo VPSi tehnilised andmed ja hind

Esmane sisselogimine serverisse toimus üle SSH-ühenduse, mis loodi programmi PuTTY abil. Sisse logiti masinasse *root*-kasutaja ja parooliga, mis määrati *root*-kasutajale ostmisprotsessi käigus. Kuna serverid on kättesaadavad avalikus võrgus, siis oli ülesandeks serverite turvamine vastavalt parimatele praktikatele. Linux operatsioonisüsteemidel on alati olemas administraatoriõigustega *root*-nimeline juurkasutaja ja seega proovivad pahatahtlikud

osapooled esimese asjana võõrastesse seadmetesse just selle kasutajaga sisse murda. Esimese sammuna loodi serveris uus administraatori õigustega kasutaja. Selleks kasutati Linuxi käsurea käske `#adduser` ja `#usermod -aG`, mis lisab loodud kasutaja sudo gruppi (vt Sele 5).

```
root@vmill155860:~# adduser
Adding user `admin' ...
Adding new group `admin' (1000) ...
Adding new user `admin' (1000) with group `admin' ...
Creating home directory `/home/admin' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
root@vmill155860:~# usermod -aG sudo admin
root@vmill155860:~#
```

Sele 5 Administraatori õigustega kasutaja loomine

Seejärel keelati `root`-kasutajal serverisse logimine üle SSH-ühenduse. Konfiguratsioonifailis „`/etc/ssh/sshd_config`“ aktiveeriti rida „`PermitRootLogin prohibit-password`“ ning olemasoleva väärtuse asemele sisestati „`no`“ (vt Sele 6). Muudatuste jõustumiseks tehti SSH-teenusele restart.

```
GNU nano 6.2 /etc/ssh/sshd config
# ForceCommand cvs server
PermitRootLogin no
HostKeyAlgorithms +ssh-rsa
```

Sele 6 Root kasutajal üle SSH serverisse sisse logimise keelamine

Kolmanda sammuna keelati serverisse üle SSH sisse logimine paroolidega ning SSH-ühendus lubati ainult ettevõtte poolt paika pandud IP-aadressidelt. Enne paroolidega sisse logimise keelamist oli aga vaja leida serverisse üle SSH sisselogimiseks alternatiivne lahendus. Programmiga PuTTY Key Generator loodi mõlema meeskonnaliikme jaoks RSA-tüüpi turvaline võtmepaar. Genereeritud avalikud võtmed tõsteti faili „`~/ssh/authorized_keys`“ ning käsuga `#chmod 600 ~/ssh/authorized_keys` anti ainult faili omanikule lugemis- ja kirjutamisõigused (vt Sele 7).

```

@vmill155860:~$ sudo nano ~/.ssh/authorized_keys
[sudo] password for :
@vmill155860:~$ sudo chmod 600 ~/.ssh/authorized_keys
--@vmill155860:~$ █

```

Sele 7 Võtmete serverisse paigaldus

Paroolidega üle SSH serverisse sisse logimise keelamiseks aktiveeriti konfiguratsioonifailis „/etc/ssh/sshd\_config“ read „PasswordAuthentication yes“ ja „PermitEmptyPasswords no“ ning „PasswordAuthentication“ väärtuseks seati „no“ (vt Sele 8). Muudatuste jõustumiseks tehti SSH-teenusele restart.

```

GNU nano 6.2 /etc/ssh/sshd config
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
PermitEmptyPasswords no█

```

Sele 8 Paroolidega üle SSH sisse logimise keelamine

Nagu eelpool mainitud, oli lisanduvaks turvameetmeks SSH-ühenduse loomine ainult teatud IP-aadressidelt. Selleks lubati tulemüüris IP-aadressid käsuga `#ufw allow from <IP-AADDRESS> to any port <PORTI NUMBER>`. Seejärel lülitati tulemüür sisse (vt Sele 9).

```

--@vmi1155860:~$ sudo ufw allow from [redacted] to any port
Rules updated
--@vmi1155860:~$ sudo ufw allow from [redacted] to any port
Rules updated
--@vmi1155860:~$ sudo ufw allow from [redacted] to any port
Rules updated
--@vmi1155860:~$ sudo ufw allow from [redacted] to any port
Rules updated
--@vmi1155860:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y/n)? y
Firewall is active and enabled on system startup
--@vmi1155860:~$ sudo ufw status
Status: active

To Action From
--
ALLOW [redacted]
ALLOW [redacted]
ALLOW [redacted]
ALLOW [redacted]

```

Sele 9 Tulemüüri sisse lülitamine

## 2.2 Uptime Kuma

### 2.2.1 Seiresüsteemi paigaldamine

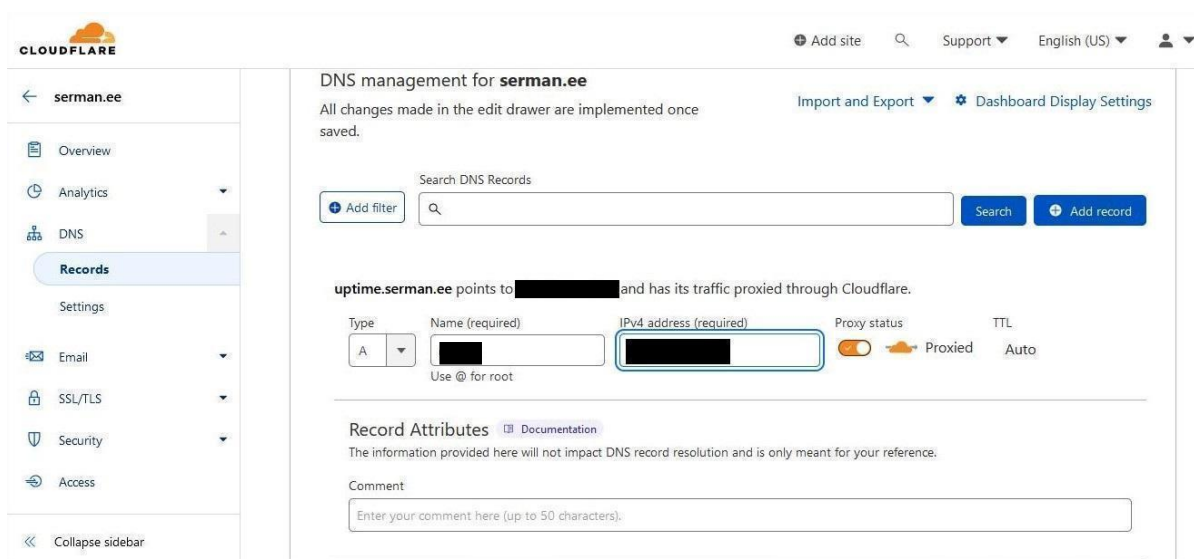
Uptime Kuma paigaldamiseks kasutati juhendit, mis on leitav veebilehelt [linux.how2shout.com](https://linux.how2shout.com). [8] Uptime Kuma installimiseks paigaldati serverisse Nodejs, Git, PM2 ja Apache2 (vt Sele 10). Nodejs paigaldamine oli vajalik selleks, et server oskaks JavaScriptis kirjutatud Uptime Kuma käivitada. Giti abil klooniti GitHubist serverisse Uptime Kuma

repositoorium. PM2 oli vajalik selleks, et Uptime Kuma töotaks taustal ning Apache2 veebiserverit selleks, et töotaks Uptime Kuma veebiliides.

```
156 sudo apt update
157 sudo apt upgrade
158 curl -fsSL https://deb.nodesource.com/setup_lts.x | sudo -E bash -
159 sudo apt-get install -y nodejs
160 sudo apt install git
161 git clone https://github.com/louislam/uptime-kuma.git
162 ls -la
163 cd uptime-kuma
164 npm run setup
165 sudo npm install pm2 -g && pm2 install pm2-logrotate
166 pm2 start server/server.js --name uptime-kuma
167 pm2 startup
168 sudo env PATH=$PATH:/usr/bin /usr/lib/node_modules/pm2/bin/pm2 startup sy
stemd -u admin --hp /home/admin
169 systemctl status uptime kuma
170 sudo apt install apache2
171 sudo a2enmod ssl proxy proxy_ajp proxy_wstunnel proxy_http rewrite deflat
e headers proxy_balancer proxy_connect proxy_html
172 sudo systemctl restart apache2
173 sudo nano /etc/apache2/sites-available/kuma.conf
174 sudo a2dissite 000-default.conf
175 sudo a2ensite kuma.conf
176 sudo systemctl reload apache2
```

Sele 10 Uptime Kuma paigaldus

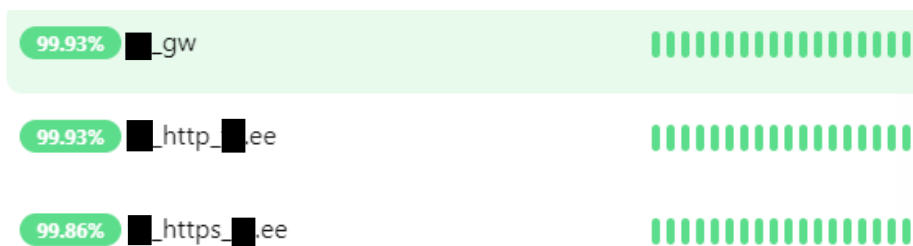
Eelnimetatud tegevuste järel avati serveri tulemüüris HTTP (80) ja HTTPS (443) pordid, et Uptime Kuma veebiliidesele pääseks ligi. Selleks, et server oleks avalikult kättesaadava nimelahendusega, tehti Cloudflare'i domeenihalduskeskkonas vajalik A-kirje, mis viitab serveri IP-aadressile. Lisaks pandi turvalisuse huvides server Cloudflare'i proksi taha, et päringud ega potentsiaalsed rünnakud ei läheks otse serveri pihta (vt Sele 11).



Sele 11 Cloudflare'is DNS-kirje tegemine

## 2.2.2 Hostide seiresse lisamine

Kuna Uptime Kuma *dashboard*il ei ole võimalik jälgitavaid seadmeid ja lehekülgi grupeerida, siis oli vaja välja töötada loogiline nimetussüsteem, et seiresüsteemi kasutajal oleks võimalik kiiresti nimekirjast tuvastada, millise kliendi ja teenusega on tegemist. Nii veebilehtede kui ka ruuterite lisamisel alustati kliendi nimest või nime lühendist. Kui tegemist oli ruuteriga, siis järgnes nimele lühend „gw“ (inglise keeles *gateway*) ning veebilehe puhul protokollide nimi (HTTP/HTTPS) ja lehekülje aadress (vt Sele 12).



Sele 12 Uptime Kuma nimetussüsteem

Ruuteri või veebilehe jälgimise lisamise puhul valiti sobiv protokoll (*Monitor Type* ping või HTTP/HTTPS), määrati kuvatav nimi (*Friendly Name*) ning IP-aadress või veebilehe aadress (*Hostname/URL*) (vt Lisa 3 ja Lisa 4).

## 2.2.3 Teavituste seadistamine

Ettevõtte omanik soovis saada Uptime Kumalt teavitusi Server Management OÜ e-postile juhul kui jälgitav seade või teenus on pärast kolme järjestikkust testi endiselt maas. Iga testi vahemikuks määrati 60 sekundit (vt Sele 13).

Heartbeat Interval (Check every 60 seconds)

60

Retries

2

Maximum retries before the service is marked as down and a notification is sent

Heartbeat Retry Interval (Retry every 60 seconds)

60

Sele 13 Uptime Kuma testide vahemik ja korduste arv

Teavituse pealkirjaks määrati „Alert from Uptime Kuma – Service Down“. Maas oleva teenuse nimi ja IP-aadress kajastusid automaatselt kirja sisus (vt Lisa 5).

## 2.3 Zabbix

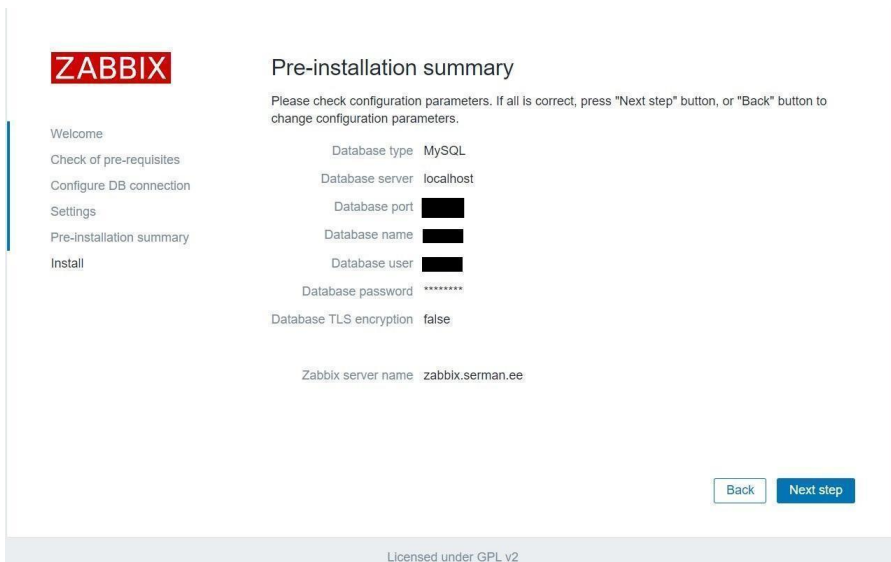
### 2.3.1 Seiresüsteemi paigaldamine

Zabbixi serveri paigaldamiseks kasutati Zabbixi koduleheküljel olevat juhendit. [9] Esmalt laeti `#wget` käsuga Zabbixi repositooriumist alla kõige uuem Zabbixi versioon (6.4). Käsuga `#dpkg` paigaldati Ubuntu 22.04 operatsioonisüsteemile mõeldud Zabbixi pakett ning seejärel installiti Zabbixi server ja Apache veebiserver. Eraldi installiti ka juurde MySQL server. MySQL käsureal loodi Zabbixi andmebaas koos kasutaja ja parooliga. Käsuga `#zcat` imporditi Zabbixi andmebaasi andmed MySQLi ning seoti eelnevalt loodud andmebaasi kasutaja ja parooliga. Viimasteks sammudeks olid Zabbixi konfiguratsioonifaili „etc/zabbix/zabbix\_server.conf“ sees andmebaasi parooli lisamine ja muudatuste jõustumiseks Zabbixi serverile, agendile ja Apache veebiserverile restardi tegemine (vt Sele 14).

```
wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb
sudo dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
sudo apt update
sudo wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb
sudo dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
sudo apt update
sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
sudo apt install mysql-server
sudo mysql -uroot -p
mysql -uroot -p
sudo systemctl status mysql.service
sudo systemctl restart mysql.service
sudo mysql -uroot -p
sudo zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
sudo mysql -uroot -p
sudo nano /etc/zabbix/zabbix_server.conf
systemctl restart zabbix-server zabbix-agent apache2
systemctl enable zabbix-server zabbix-agent apache2
```

Sele 14 Zabbixi serveri paigaldus

Sarnaselt Uptime Kuma serverile, tehti domeenihalduskeskkonnas vajalik A-kirje, et server oleks nimelahendusega kättesaadav. Seejärel viidi Zabbixi seiresüsteemi paigaldus lõpule läbi veebiliidese (vt Sele 15).



Sele 15 Zabbixi paigaldus veebibrauseris

### 2.3.2 Hostide seiresse lisamine

Enne ettevõtte klientide seadmete Zabbixi seiresüsteemi lisamist loodi iga kliendi jaoks *host group*. Antud tegevus võimaldab administraatoril filtreerida ettevõtte klientide seadmeid gruppide järgi. Seadmete seiresse lisamisel kasutati nende olemasolevaid hosti- ja domeeninimesid (vt Sele 16).

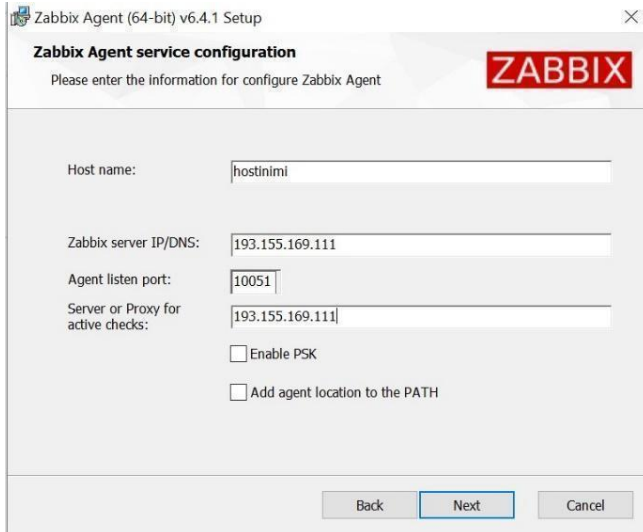


Sele 16 Nimetussüsteem Zabbixis

Selleks, et paigaldada ettevõtte klientide seadmetesse Zabbixi aktiivne agent, oli vaja esmalt luua VPN-ühendused klientide võrkudesse. Ettevõtte paroolihaldustarkvara abil saadi klientide ruuterite sisselogimisandmed. Kasutades programmi WinBox, logiti ruuteritesse sisse ning lisati neisse uus VPN-kasutaja ning laeti alla vajalikud sertifikaadid VPN-ühenduse

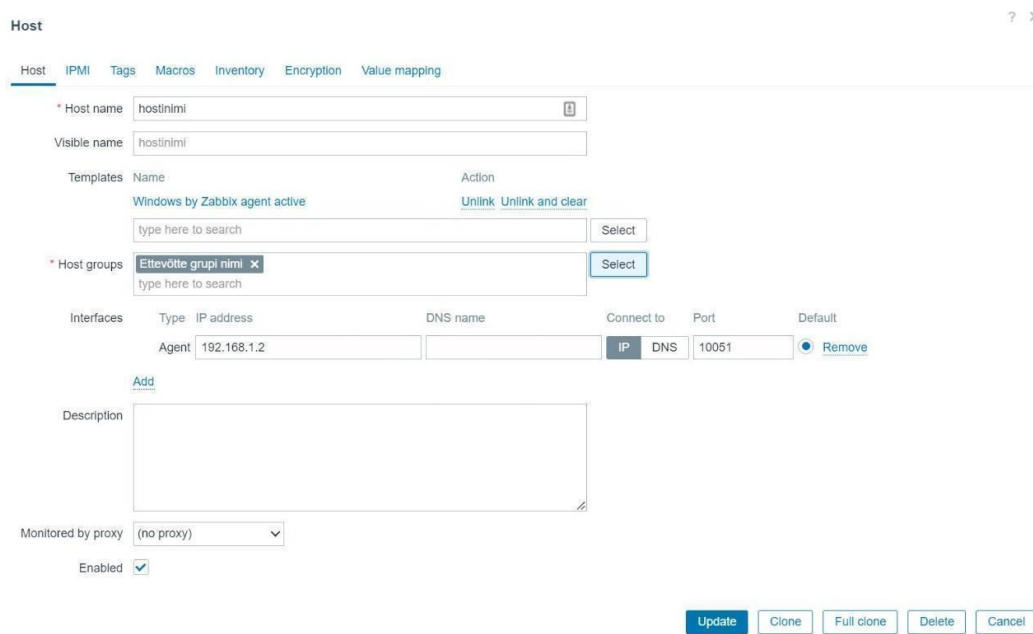


loomiseks. Vastavalt operatsioonisüsteemile kasutati seejärel PuTTY-t ja RDP-d, et kaugelt klientide seadmetesse sisse logida. Windowsi operatsioonisüsteemi puhul laeti Zabbixi koduleheküljelt alla .msi-faililaiendiga agendi paigaldusfail. Paigalduse ajal tuli määratleda pordi number, mis on aktiivse agendi puhul 10051, seadme hostinimi ja Zabbixi serveri IP-aadress (vt Sele 17).



Sele 17 Zabbixi agendi paigaldus Windowsi serveris (pildil olevad andmed on näitlikud)

Seejärel tuli seade lisada Zabbixi serverisse (*Monitoring->Hosts->Create Host*), kus peab olema määratletud seadme IP-aadress, port ning hostinimi (vt Sele 18). Selleks, et agent toimiks, peavad hostinimi ja pordinumber olema identsed nii agendi konfiguratsioonifailis kui ka serveris.



Sele 18 Zabbixi serveris hosti lisamine (pildil olevad andmed on näitlikud)

Zabbixi agendi paigaldamine Linuxi serverites toimus käsurealt. Agendi paigaldamisel jälgiti Zabbixi koduleheküljel olevat juhendit.[9] #Wget käsuga laeti Zabbixi repositooriumist alla kõige uuem versioon Zabbixi agendist ning käsuga #dpkg paigaldati vajalik pakett, mille järel agent installiti. Lisaks tehti vajalikud muudatused konfiguratsioonifailis „etc/zabbix/zabbix\_agentd.conf“, sh hostinimi, pordi number ja Zabbixi serveri IP-aadress. Viimaks tehti agendile taaskäivitus ja lülitati teenusena sisse (vt Sele 19).

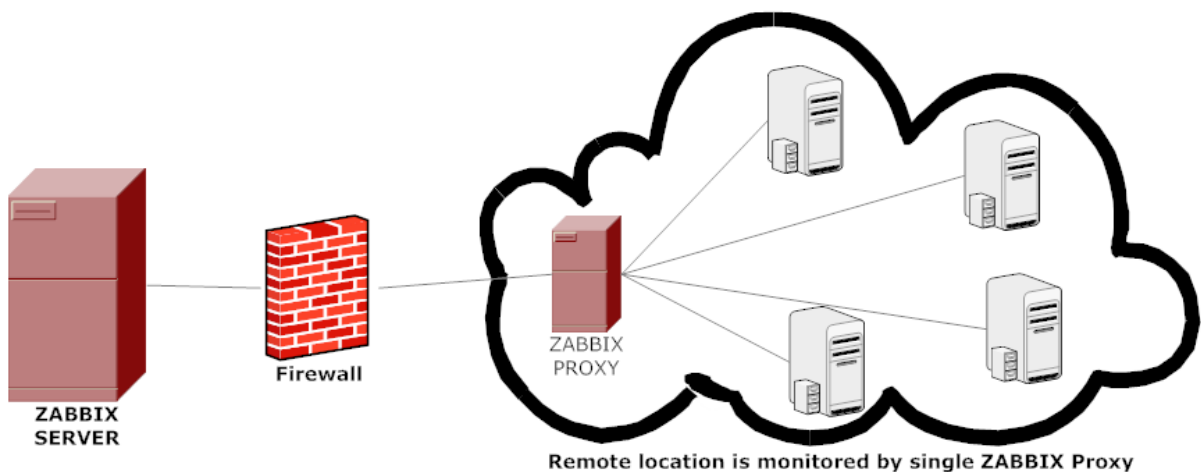
```

282 lsb_release -a
283 ls -la
284 wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release
/zabbix-release_6.4-1+ubuntu22.04_all.deb
285 dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
286 sudo dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
287 sudo apt update
288 apt install zabbix-agent
289 sudo apt install zabbix-agent
290 sudo nano /etc/zabbix/zabbix_agentd.conf
291 sudo hostnamectl
292 sudo nano /etc/zabbix/zabbix_agentd.conf
293 systemctl restart zabbix-agent
294 systemctl enable zabbix-agent
295 sudo systemctl status zabbix-agent.service

```

Sele 19 Linuxi serveris Zabbixi agendi paigaldus

Seadmetes, kus puudus võimalus paigaldada Zabbixi agendi, kasutati seireinfo kogumiseks SNMP-d. Kuna SNMP-ga jälgitavad seadmed asusid Tartu Rakendusliku Kolledži tulemüüri taga, siis kasutati seireinfo kogumiseks Zabbixi proksit. Zabbixi proksi võimaldab seireinfo kogumist tulemüüri taga olevast kohtvõrgust (vt Sele 20).



Sele 20 Zabbixi proksi tööpõhimõte [10]

Kui Zabbixi server panna käima aktiivses režiimis toimib see sarnaselt Zabbixi aktiivse agendiga ehk Zabbixi proksi algatab võrguliikluse kliendi võrgust Zabbixi serveri suunas. [11] Zabbixi

proksi paigaldas ja seadistas Tartu Rakendusliku Kolledži sisevõrgus projekti juhendaja. Seejärel tuli seadistada SNMP jälgitavates seadmetes.

Synology võrgusalvesti puhul oli vaja veebiliideses aktiveerida SNMP teenus (*Control Panel -> Terminal & SNMP -> SNMP*). Autentimiseks tuli ka määrata *Community* (jagatud salasõna seadme ja serveri vahel) (vt Sele 21).

**Terminal** **SNMP**

Enable SNMP to monitor the server with network management software.

Enable SNMP service

SNMPv1, SNMPv2c service i

Community:  i

SNMPv3 service

Username:

Protocol:  ▼

Password:

Enable SNMP privacy

Protocol:  ▼

Password:

SNMP Device Information

Device Name:

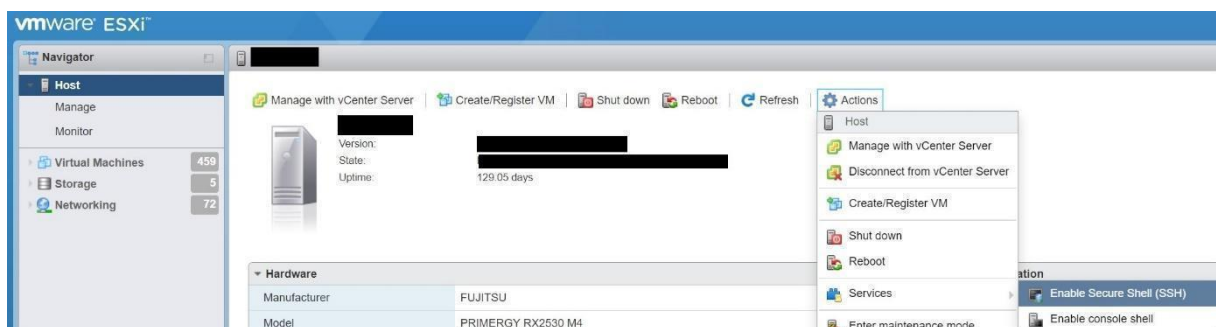
Device Location:

Contact:

Visit [Synology's website](#) to download the Synology MIB files.

Sele 21 SNMP seadistamine Synology võrgusalvestis

VMware ESXI hostide puhul tuli kõigepealt veebiliideses lubada SSH ühenduse loomine (*Host -> Actions -> Services -> Enable Secure Shell (SSH)*) (vt Sele 22).



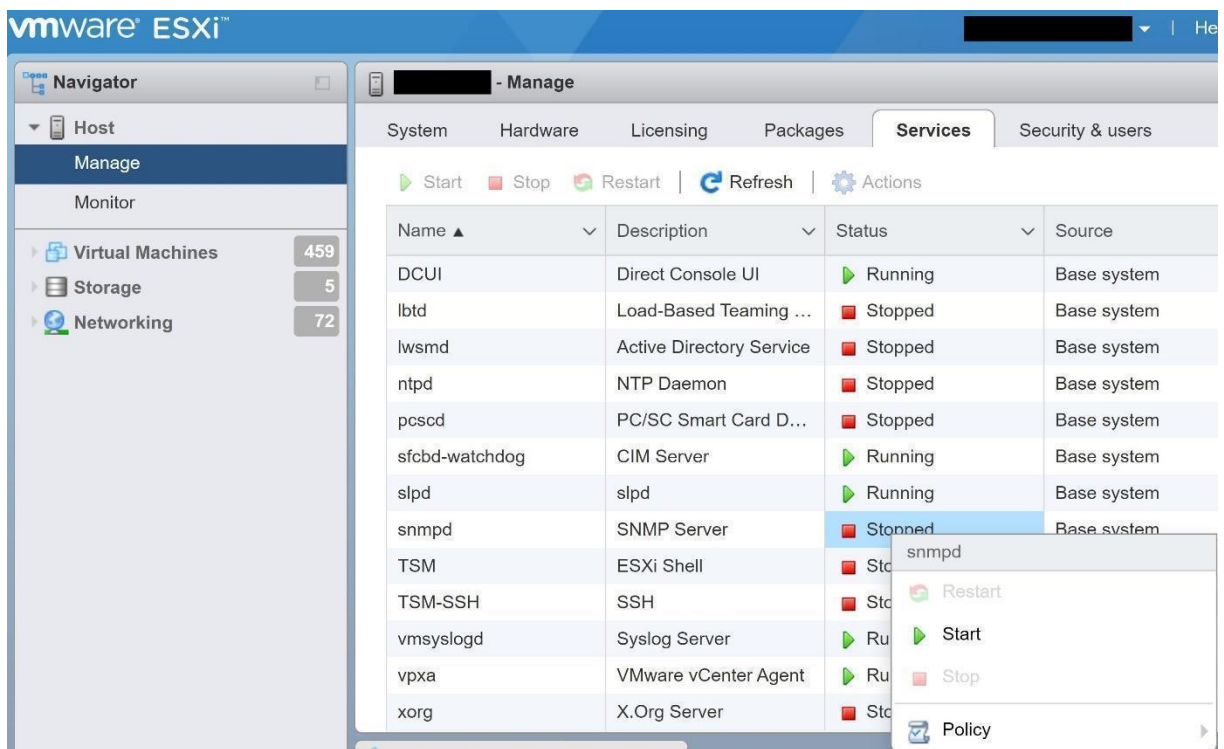
Sele 22 SSH ühenduse lubamine ESXI hostis

Seejärel siseneti seadmesse üle SSH-ühenduse ning aktiveeriti (kuna vaikumisi on SNMP teenus välja lülitatud) ja seadistati SNMP käsurealt (vt Sele 23).

```
0 esxcli system snmp get
1 esxcli system snmp set --communities [redacted]
2 esxcli system snmp set --syslocation [redacted]
3 esxcli system snmp set --syscontact [redacted]
4 esxcli system snmp set --enable true
5 esxcli system snmp get
6 /etc/init.d/snmpd restart
7 /etc/init.d/snmpd status
8 esxcli system uuid get
```

Sele 23 SNMP seadistamine ESXI hostis käsurealt

Pärast seda käivitati SNMP teenusena veebiliideses (*Manage -> Services -> SNMPD -> Start*) (vt Sele 24).



Sele 24 SNMP käivitamine ESXI hosti veebiliideses

SNMP-ga monitooritavate seadmete lisamine Zabbixi serverisse toimus sarnaselt Windowsi ja Linuxi serveritega. Hostide lisamisel oli aga vaja täpsustada, et kasutatakse SNMP-d ning sisestada *Community* salasõna (vt Sele 25).

New host ? X

Host IPMI Tags **Macros 1** Inventory Encryption Value mapping

\* Host name  E

Visible name

Templates

Name	Action
Generic by SNMP	<a href="#">Unlink</a>
<input type="text" value="type here to search"/>	<input type="button" value="Select"/>

\* Host groups  X

Interfaces

Type	IP address	DNS name	Connect to	Port	Default
SNMP	10.10.2.11	<input type="text"/>	<input checked="" type="radio"/> IP <input type="radio"/> DNS	161	<input checked="" type="radio"/> <a href="#">Remove</a>

\* SNMP version

\* SNMP community

Max repetition count  ?

Use combined requests

[Add](#)

Description

Monitored by proxy

Enabled

Sele 25 Zabbixi serveris SNMP hosti lisamine (pildil olevad andmed on näitlikud)

ESXI hostide puhul oli lisaks vaja sisestada varasemalt käsurealt saadud seadmele ainulaadne ID (inglise keeles *universally unique identifier*) (vt Sele 26).

New host ? X

Host IPMI Tags **Macros 1** Inventory Encryption Value mapping

Host macros

Macro	Value	Description	
{VMWARE.HV.UUID}	seadmele ainulaadne ID	<input type="text" value="description"/>	<input type="button" value="Remove"/>

[Add](#)

Sele 26 ESXI hosti UUID sisestamine

Hostide lisamise hetkel või pärast lisamist tuli ka igale hostile määrata teatud mall (inglise keeles *template*). Windowsi operatsioonisüsteemidel jooksvatele serveritele lisati mall „Windows by Zabbix agent active“, Linuxi peal jooksvatele serveritele mall „Linux by Zabbix Agent Active“ ning ESXI hostidele „Linux by SNMP“. Synology jaoks oli vaja GitHubist eraldi alla laadida mall „Synology DiskStation“ ja see Zabbixi veebileidese kaudu serverisse importida (vt Sele 27).

**Import** ? X

\* Import file

Advanced options

Rules

All  Update existing  Create new  Delete missing

Sele 27 Synology jaoks malli importimine

Malli abil on võimalik määrata, millist infot server jälgitava hosti kohta näitab. Vastavalt hosti operatsioonisüsteemile ja jälgimismeetodile, kasutatakse teatud malle. Mall sisaldab mõõdikuid, päästikuid ja vastavalt mallist ka graafikuid.

### 2.3.3 Teavituste seadistamine

Ka Zabbixi puhul seadistati teavitused e-postile. Esmalt tuli määrata, millist e-posti aadressi hakatakse kasutama teavituste saatmiseks. See käis menüüst *Alerts -> Media Types*. Kuna ettevõttel oli kirjade saatmiseks juba olemas Outlooki postkast, siis valiti Office365 *media type* (vt Sele 28).

**Media types**

Media type Message templates 5 Options ●

\* Name

Type

Email provider

\* Email

\* Password

Message format

Description

Enabled

Sele 28 E-posti teavituste seadistamine

Lisaks kohandati teavituste sisu *Message Templates* tabist (vt Sele 29).

## Message template



Message type

Subject

Message

Sele 29 Teavituse sisu seadistamine

Teiseks sammuks oli seadistatud *media type*'i kasutajaprofiiliga sidumine, mis käis menüüst *User Settings -> Profile -> Media*. Kasutajale Zabbix Administrator lisati Office365 *media type* ning määrati, millisele e-posti aadressile hakkavad teavitused saabuma (vt Sele 30).

## Media



Type

\* Send to  [Remove](#)

[Add](#)

\* When active

Use if severity  Not classified  
 Information  
 Warning  
 Average  
 High  
 Disaster

Enabled

Sele 30 E-posti teavituste sidumine Zabbixi admin kasutajaga

Kolmandaks määrati menüüst *Alerts -> Actions -> Trigger Action*, mis tüüpi probleemide korral hakkab ettevõtte Zabbixilt teavitusi saama. Ettevõtte soovis teavitusi juhul kui host ei ole enam serverile kättesaadav ning kui hosti CPU, RAMi või ribalaiuse (*bandwidth*) kasutus on tavapärasest kõrgemad. Lisaks sooviti saada teavitusi siis, kui hosti kettapind hakkab täis

saama. Selleks kontrolliti enne üle kõigi oluliste päästikute täpsed nimed ja seejärel määrati teavituste saatmise tingimusteks (vt Sele 31).

**Action** ? x

Action Operations 3

\* Name

Type of calculation  A or B or C or D or E or F or G or H or I or J

Label	Name	Action
A	Trigger name contains <i>Zabbix agent is not available</i>	<a href="#">Remove</a>
B	Trigger name contains <i>Unavailable by ICMP ping</i>	<a href="#">Remove</a>
C	Trigger name contains <i>No SNMP data collection</i>	<a href="#">Remove</a>
D	Trigger name contains <i>Lack of available memory</i>	<a href="#">Remove</a>
E	Trigger name contains <i>High memory utilization</i>	<a href="#">Remove</a>
F	Trigger name contains <i>High CPU utilization</i>	<a href="#">Remove</a>
G	Trigger name contains <i>High bandwidth usage</i>	<a href="#">Remove</a>
H	Trigger name contains <i>Disk space is low</i>	<a href="#">Remove</a>
I	Trigger name contains <i>Disk space is critically low</i>	<a href="#">Remove</a>
J	Trigger name contains <i>active checks are not available</i>	<a href="#">Remove</a>

Sele 31 E-posti teavituste saatmise tingimused

*Operations* tabi alt pandi paika, et nii probleemi tekkimise kui ka selle lahenemise korral saadetakse koheselt teavitus Zabbixi administraatori postkasti (vt Sele 32, 33 ja 34).

**Action** ? x

Action Operations 3

\* Default operation step duration

Operations	Steps	Details	Start in	Duration	Action
	1	Send message to users: Admin (Zabbix Administrator) via Office365	Immediately	Default	<a href="#">Edit</a> <a href="#">Remove</a>

[Add](#)

Recovery operations

Details	Action
Notify all involved	<a href="#">Edit</a> <a href="#">Remove</a>

[Add](#)

Sele 32 E-posti teavituste seadistus

Problem started at 05:38:43 on 2023.05.07  
Problem name: Zabbix agent: active checks are not available  
Host: [dc001.████████.ee](#)  
Severity: High  
Operational data: Current state: not available (2)  
Original problem ID: 20972

Sele 33 Saabunud teavitus probleemi tekkimisest



Problem has been resolved at 05:42:43 on 2023.05.07  
Problem name: Zabbix agent: active checks are not available  
Problem duration: 4m 0s  
Host: dc001.██████.ee  
Severity: High  
Original problem ID: 20972

Sele 34 Saabunud teavitus probleemi lahenumisest

## 2.4 Testimine

Projektis kasutusele võetavate lahenduste testimine toimus Tartu Rakendusliku Kolledži virtualiseerimiskeskonnas. Testiti nii seiresüsteemide paigaldamist kui ka Zabbixi agentide paigaldust klientseadmetesse. Lisaks kasutati virtualiseerimiskeskonda, et läbi katsetada jälgitavate seadmete ja teenuste seiresüsteemidesse lisamist ja teavituste korrektset seadistamist. Kuna mõlemal meeskonnaliikmel oli vaja korduvalt üles seada testimiskeskond, siis protsessi kiirendamiseks loodi ChatGPT tekstiroboti abil *bash* skript, mis paigaldab Zabbixi seiresüsteemi Ubuntu serverile. Zabbixi serveri paigaldamise käsud võeti Zabbixi koduleheküljelt ning ChatGPT-l paluti nendest skript luua (vt Lisa 6 ja Lisa 7). [12] ChatGPT väljastatud skripti kasutamisel tekkisid aga veateated ning logifaile lugedes jõuti järeldusele, et skripti tuleb juurde lisada käsk, mis käivitaks enne MySQLi andmebaasi loomist MySQLi serveri. Skripti lõplikus versioonis muudeti ka ingliskeelsed kommentaarid eestikeelseteks (vt Sele 35).

```
GNU nano 6.2                                script.sh
~/bin/bash

# Laen alla ja paigaldan Zabbixi repositooriumi
wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb
sudo dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb

# Teen operatsioonisüsteemile uuenduse ning paigaldan vajalikud teenused
sudo apt update -y
sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent mysql-server -y
sudo apt install mysql-server -y

# Käivitan MySQL andmebaasihaldussüsteemi
sudo systemctl start mysql

# Loon MySQL andmebaasihaldussüsteemis uue andmebaasi, kasutaja ning selle parooli ja annan kasutajale kõik õigused loodud andmebaasi jaoks
sudo mysql -u      -p      <<EOF
CREATE DATABASE      CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER '      '@'      IDENTIFIED BY '      ';
GRANT ALL PRIVILEGES ON *.* TO '      '@'      ;
SET GLOBAL log_bin_trust_function_creators = 1;
EOF

# Seon omavahel Zabbixi andmed ja MySQLis loodud andmebaasi kasutaja ja parooliga
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -u:      -p :

# Lülitan välja MySQL andmebaasihaldussüsteemis SUPER õiguste kontrolli
sudo mysql -u      -p      <<EOF
SET GLOBAL log_bin_trust_function_creators = 0;
EOF

# Zabbix serveri konfiguratsiooni failis uuendan andmebaasi salasõna
sudo sed -i 's/# DBPassword=DBPassword=      /' /etc/zabbix/zabbix_server.conf

# Taaskäivitan ja lülitan sisse Zabbix serveri, agendi ja apache veebiserveri
sudo systemctl restart zabbix-server zabbix-agent apache2
sudo systemctl enable zabbix-server zabbix-agent
```

Sele 35 Lõplik skript Zabbixi serveri paigaldamiseks

Kuna Tartu Rakendusliku Kolledži virtualiseerimiskeskonnas oli Zabbixi serveri paigaldamine ning klientseadmete seiresse lisamine edukas, siis otsustati edasi liikuda reaalse virtuaalse

privaatserveri seadistamisega ja Zabbixi serveri paigaldamisega. Kuna testimise faasis toimis Zabbixi agent 6.4.2, siis otsustati, et just see versioon võetakse kasutusele. Kuigi esialgselt oli andmete edastamine edukas, siis peale paari nädalat hakkasid tekkima tõrked. Nimelt lakkasid agendid Windowsi serverites töötamast korduvalt. Probleemi tuvastamiseks loeti serverites Zabbixi agentide logifaile. Logifailidest leitud veateateid *“Unhandled exception c0000005 detected”* ja *“Unhandled exception 6ba detected”* guugeldades selgus Zabbixi *support-leheküljelt*, et sama probleem on esinenud ka varasemate agentide versioonidega ning Zabbixi arendajad on vanemates versioonides probleemi lahendanud. [13] Seega otsustati stabiilsuse saavutamiseks kasutada veidi vanemat agendi versiooni. Esialgu paigaldati 6.2.9 agent ainult nelja Windowsi serverisse ja ülejäänud serverites taaskäivitati agent 6.4.2. Järgmise paari nädala jooksul lakkasid 6.4.2 agendid jälle töötamast, kuid 6.2.9 agentidega probleem ei kordunud. Seetõttu paigaldati Zabbixi agendi 6.2.9 versioon hiljem kõikidesse Windowsi serveritesse.

## 3 MEESKONNATÖÖ JA ENESEANALÜÜS

### 3.1 Meeskonnaanalüüs

Meeskonnaliikmed ja juhendaja kohtusid ajavahemikus 11.01.2023-21.05.2023 iga neljapäev ja reede Tartu Rakenduslikus Kõlledžis IKT osakonnas. Ülejäänud päevadel toimus suhtlus kokkulepitud kuupäevadel ja kellaaegadel Microsoft Teamsis.

Rollide jaotus toimus projekti vältel jooksvalt vastavalt meeskonnaliikmete ajalistele võimalustele. Teoreetiliste materjalide läbitöötamine toimus tihti individuaalselt, kuid praktiliste ülesannete teostamine toimus alati meeskonnana koolis või üle MS Teamsi.

Meeskonnatöös konflikte ei esinenud kuid tihti tuli leida teatud olukordades mõlemale sobiv kompromiss.

### 3.2 Martin Tambets

Projekti lõpus autor analüüsis end ning kirjeldas mis oli tema sõnul kõige suurem areng, lisaks mis läks hästi isikuliselt ning mis vajab veel lihvi.

Terve projekti vältel toimus pidev areng. Kõige paremini oli seda näha Linuxi seadmete kasutamise oskuse paranemises. Kui varasemalt tuli väga palju mõelda, mida seadme sees on vaja teha ning kus, erinevate ülesannete lahendamiseks, siis projekti lõpus toimusid tegevused juba pea automaatselt ning olulisemalt vähem otsiti abi internetist. Lisaks tekkis harjumuspärane tegevus logifailide lugemisel tõrgete korral ning kui suurt rolli see endas peidab tõrgete lahendamise korral.

Kui varasemalt tehti enamus kodutööd iseseisvalt, siis lõputööd otsustati teha koos kursusekaaslasega. Tagasi mõeldes ajale mis möödus koos kaaslasega projekti tehes, siis võib öelda, et see oli väga suur väljakutse isikuliselt. Varasemad tegevused toimusid autori enda äranägemise järgi siis nüüd vajab väga palju harjumist see, et ollakse olukorras kus tuli arutleda ning leida kompromisse. Olenemata sellest, et oli küll pingelisi hetki, siis autor leiab, et koostöö oli edukas ning autori meeskonnatöö oskused arenesid ühe suure kogemuse võrra edasi.

Analüüsi tulemusena leiti, et põhjalikum ajaplaneerimine ja detailsemate tähtaegade seadmine oleks olnud see, mis oleks lihtsustanud projekti tegemist.

### 3.3 Karl Jaagola

Projekt andis võimaluse õpingute jooksul omandatud oskuste ja teadmiste kinnistamiseks ning rakendamiseks. Kuna projekt hõlmas endas erinevaid tegevusi (sh serverite turvamine, seiresüsteemide paigaldamine, domeenihalduskeskkonnas DNS-kirjete tegemine, klientide kohtvõrkudesse VPN ühenduste loomine, kaughalduse teel klientide seadmetesse agentide paigaldamine ja seiresüsteemides vajalike seadistuste tegemine), siis tekkisid ka selgemad seosed varasemalt õpitud teadmiste vahel.

Projekti käigus tuli läbi töötada hulgaliselt teoreetilist materjali ning testida võimalikke lahendusi. Kuigi pinnapealne kogemus oli varasemalt Zabbixi ja Uptime Kumaga olemas, siis projekti eesmärgi saavutamiseks tuli nendesse tunduvalt põhjalikumalt süveneda. Võrreldes Uptime Kumaga oli Zabbixil märgatavalt järsem õppimiskurv ja seega kulus ka rohkem aega Zabbixi tundma õppimise peale.

Üllatavalt aeganõudvaks osutus planeerimisfaas, kus tuli koos juhendajaga otsustada, millised kliendid ja millised seadmed lähevad seiresse. Aega võttis ka ettevõtte paroolihaldustarkvaras ja wikis orienteeruma õppimine ning klientide seadmetesse pääsemiseks vajalike andmete leidmine.

Projekti alguses oli palju enesekahtlust, mis samuti aeglustas teatud tegevusi. Järjestikuste edukate sammude tulemusel meeskonnaliikme enesekindlus aga pidevalt kasvas ning lõpu poole tegutseti juba palju julgemalt.

Meeskonnaliikmega koos oli hea koos töötada, sest lahenduste otsimisel oli pidevalt võimalik mõtteid vahetada ja tuge saada. Omavaheline läbisaamine läks projekti dokumenteerimise käigus veidi pingelisemaks, sest meeskonnaliikmetel oli kirjalikust tööst erinev nägemus, aga kokkuvõttes leiti mõlemale osapoolle sobiv kompromiss. Ka juhendaja suhtus meeskonnaliikmesse alati positiivselt ning pakkus vajadusel omapoolset abi ja nõu.

Projekti eesmärk sai saavutatud ning teadmine, et paigaldatud ja seadistatud seiresüsteemid on juba igapäevases kasutuses ning pakuvad ettevõttele lisaväärtust andis meeskonnaliikmele positiivse elamuse.

## KOKKUVÕTE

Projekti eesmärgiks oli luua ettevõtte Server Management OÜ jaoks seiresüsteem, mis võimaldaks ettevõtte klientide seadmete kohta seireinfo kogumist ja seeläbi tõsta hooldus- ja haldusteenuse kvaliteeti. Tänu toimivale seiresüsteemile on ettevõttel võimalik probleeme ennetada ja nende tekkimise korral väga kiiresti reageerida.

Projekti teostamiseks soetati kaks VPSi, millele paigaldati Uptime Kuma ja Zabbixi avatud lähtekoodiga seiresüsteemid. Ettevõtte omanikuga otsustati, et Uptime Kuma kasutatakse ettevõtte klientide ruuterite ja veebilehtede jälgimiseks ning Zabbixit serverite ja võrgusalvestite seireks. Zabbixiga jälgitavatele seadmetele paigaldati kaughalduse teel Zabbixi aktiivsed agendid või seadistati SNMP teenus. Mõlemas seiresüsteemis seadistati e-posti teavitused. Zabbixis seadistati teavitused juhul kui jälgitavate hostide näitajad on ebatavaliselt kõrged või kui hostid ei ole kättesaadavad.

Projekti eesmärgid täideti edukalt ning ettevõtte omanik on projekti tulemiga väga rahul. Ettevõttel on kaks toimivat seiresüsteemi, mis on praeguseks igapäevases kasutuses.

Zabbixi seiresüsteemi puhul on edasiarenduseks veel aga mitmeid võimalusi. Näiteks VMware ESXI hostide kohta oleks võimalik põhjalikema seadistuste teel saada veel detailsemat seireinfot. Lisaks võiks veel Zabbixi veebiliideses nähtavate probleemiteavituste prioriteetsust üksikasjalikumalt seadistada kasutaja jaoks.

## KASUTATUD ALLIKAD

- [1 L. Lam, „Uptime Kuma,“ [Võrgumaterjal]. Available:  
] <https://github.com/louislam/uptime-kuma>. [Kasutatud 15. 04. 2023].
- [2 L. Lam, „Updates,“ [Võrgumaterjal]. Available: <https://opencollective.com/uptime-kuma/updates>. [Kasutatud 15. 04. 2023].
- [3 Zabbix, „What is Zabbix?,“ [Võrgumaterjal]. Available:  
] <https://www.zabbix.com/documentation/current/en/manual/introduction/about>. [Kasutatud 15. 04. 2023].
- [4 D. Lambert, „Zabbix Agent: Active vs. Passive,“ [Võrgumaterjal]. Available:  
] <https://blog.zabbix.com/zabbix-agent-active-vs-passive/9207/>. [Kasutatud 18. 05. 2023].
- [5 Zabbix, „2 SNMP agent,“ [Võrgumaterjal]. Available:  
] <https://www.zabbix.com/documentation/current/en/manual/config/items/itemtypes/snmp>. [Kasutatud 16. 04. 2023].
- [6 M. Wolff, „Interview with Alexei Vladishev, CEO of Zabbix,“ [Võrgumaterjal]. Available:  
] [https://penseemti.com.br/interview\\_alexei/](https://penseemti.com.br/interview_alexei/). [Kasutatud 16. 04. 2023].
- [7 Zabbix, „About Zabbix LLC,“ [Võrgumaterjal]. Available: <https://www.zabbix.com/about>.  
] [Kasutatud 16. 04. 2023].
- [8 H. Maurya, „How To Install Uptime Kuma on Ubuntu 22.04 LTS Jammy,“ [Võrgumaterjal].  
] Available: <https://linux.how2shout.com/how-to-install-uptime-kuma-on-ubuntu-22-04-lts-jammy/>. [Kasutatud 15. 01. 2023].
- [9 Zabbix, „Download and install Zabbix,“ [Võrgumaterjal]. Available:  
] [https://www.zabbix.com/download?zabbix=6.4&os\\_distribution=ubuntu&os\\_version=2.04&components=server\\_frontend\\_agent&db=mysql&ws=apache](https://www.zabbix.com/download?zabbix=6.4&os_distribution=ubuntu&os_version=2.04&components=server_frontend_agent&db=mysql&ws=apache). [Kasutatud 14. 02. 2023].
- [1 Zabbix, „1 Why use Proxy?,“ [Võrgumaterjal]. Available:  
0] [https://www.zabbix.com/documentation/1.8/en/manual/proxies/why\\_use\\_proxy#why-use-proxy](https://www.zabbix.com/documentation/1.8/en/manual/proxies/why_use_proxy#why-use-proxy). [Kasutatud 12. 05. 2023].

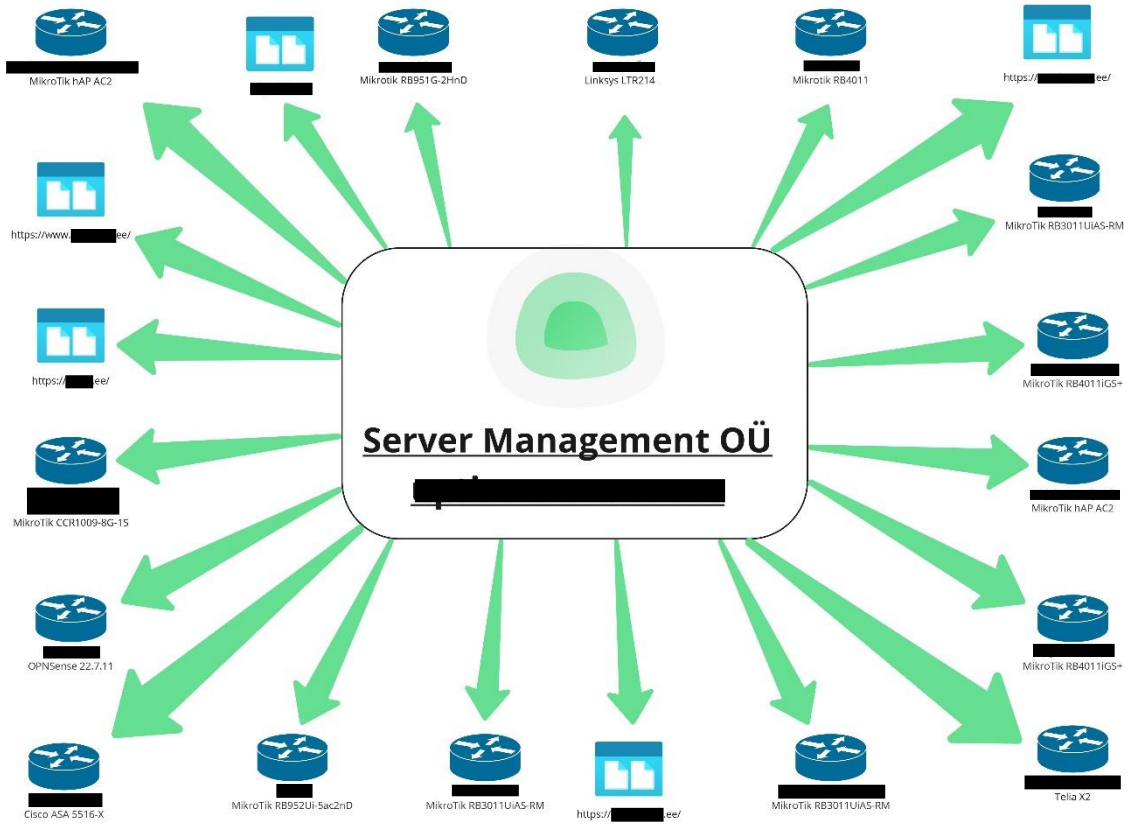
[1 Best Monitoring Tools, „Zabbix Proxy: Install on Ubuntu 22.04 / 20.04 in 10 minutes!“,  
1] [Võrgumaterjal]. Available: <https://bestmonitoringtools.com/install-zabbix-proxy-on-ubuntu/>. [Kasutatud 12. 05. 2023].

[1 OpenAI, „Isklik suhtlus,“ [Võrgumaterjal]. Available: <https://openai.com/blog/chatgpt>.  
2] [Kasutatud 18. 04. 2023].

[1 Zabbix, „Zabbix Agent Crashes with Windows Server 2022,“ [Võrgumaterjal]. Available:  
3] <https://support.zabbix.com/browse/ZBX-19926>). [Kasutatud 20. 04. 2023].

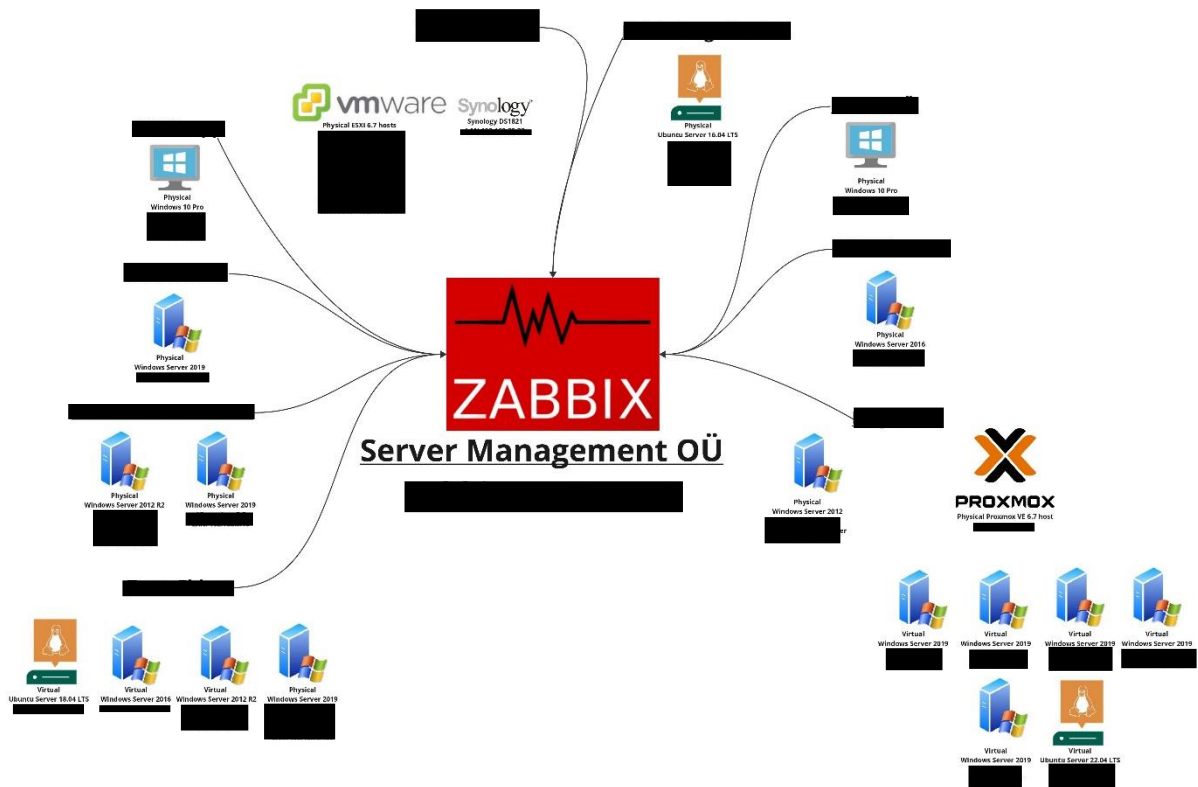
# LISAD

## Lisa 1 Uptime Kuma skeem Miros





## Lisa 2 Zabbix skeem Miros



## Lisa 3 Uptime Kumasse veebilehe lisamine (andmed pildil on näitlikud)

New Update

Status Pages

Dashboard

### Add New Monitor

#### General

Monitor Type

HTTP(s)

Friendly Name

voco\_https\_voco.ee

URL

https://voco.ee

Heartbeat Interval (Check every 60 seconds)

60

Retries

3

#### Notifications

Alert from Uptime Kuma [Edit](#)

Setup Notification

#### Proxy

Not available, please setup.

Setup Proxy

#### HTTP Options

Method

GET

## Lisa 4 Uptime Kumasse ruuteri lisamine (andmed pildil on näitlikud)

[New Update](#)

[Status Pages](#)

[Dashboard](#)

### Add New Monitor

#### General

Monitor Type

Ping

Friendly Name

voco\_gw

Hostname

[REDACTED]

Heartbeat Interval (Check every 60 seconds)

60

Retries

3

#### Notifications

Alert from Uptime Kuma [Edit](#)

[Setup Notification](#)

## Lisa 5 Uptime Kuma teavitus (andmed pildid on näitlikud)


Uptime Kuma Alert - Service Down  

---





To: 

[ettevõtte\_nimi] [ Down] PING 11.111.111.113 (11.111.111.113) 56(84) bytes of data.

--- 11.111.111.113 ping statistics ---

10 packets transmitted, 0 received, 100% packet loss, time 9208ms

Time (UTC): 2023-05-02 11:25:38.776

 Reply

 Forward

---

## Lisa 6 ChatGPT sisend (Zabbix serveri paigaldamise skript)

create bash script in ubuntu 22.04 using these commands

```
# wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-  
release_6.4-1+ubuntu22.04_all.deb  
# sudo dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb  
# sudo apt update -y  
# sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-  
sql-scripts zabbix-agent -y  
# sudo apt install mysql.server -y  
# sudo mysql -u [REDACTED] -p [REDACTED]  
mysql> create database [REDACTED] character set utf8mb4 collate utf8mb4_bin;  
mysql> create user [REDACTED]@[REDACTED] identified by '[REDACTED]';  
mysql> grant all privileges on [REDACTED].* to [REDACTED]@[REDACTED];  
mysql> set global log_bin_trust_function_creators = 1;  
mysql> quit;  
# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-  
set=utf8mb4 -u [REDACTED] -p [REDACTED] [REDACTED]  
# sudo mysql -u [REDACTED] -p [REDACTED]  
mysql> set global log_bin_trust_function_creators = 0;  
mysql> quit;  
# Edit file /etc/zabbix/zabbix_server.conf  
DBPassword=[REDACTED]  
  
# systemctl restart zabbix-server zabbix-agent apache2  
# systemctl enable zabbix-server zabbix-agent apache2
```

## Lisa 7 ChatGPT väljund (Zabbix serveri paigaldamise skript)

```
#!/bin/bash

# download and install zabbix repository package
wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb
sudo dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb

# update the package list
sudo apt update -y

# install zabbix and mysql
sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent mysql-server -
y

# create zabbix database and user in mysql
sudo mysql -u████ -p████ << EOF
CREATE DATABASE █████ character set utf8mb4 collate utf8mb4_bin;
CREATE USER █████@████ IDENTIFIED BY '████';
GRANT ALL PRIVILEGES ON █████* TO █████@████;
SET GLOBAL log_bin_trust_function_creators = 1;
EOF

# import zabbix server schema to the zabbix database
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -u████ -p████

# disable log_bin_trust_function_creators in mysql
sudo mysql -u████ -p████ << EOF
SET GLOBAL log_bin_trust_function_creators = 0;
EOF

# update the zabbix server configuration file with the mysql password
sudo sed -i 's/# DBPassword=/DBPassword=████/' /etc/zabbix/zabbix_server.conf

# restart the zabbix server, agent and apache
sudo systemctl restart zabbix-server zabbix-agent apache2

# enable the zabbix server, agent and apache to start at boot
sudo systemctl enable zabbix-server zabbix-agent apache2
```

## SUMMARY

The aim of the project was to set up and implement a monitoring system for Server Management OÜ so that the company could offer higher quality IT administration and maintenance services to their clients. The relevance of the project stems from the fact that a well-implemented monitoring system has the potential to help prevent and quickly solve problems related IT infrastructure as well as network security.

In the first chapter, information regarding the planning phase of the project is outlined, including preliminary deadlines, an analysis of potential risks and the security reasons for the choice to use two separate monitoring systems – Uptime Kuma and Zabbix.

The second chapter includes the detailed description of the practical work that was carried out, including the purchase and the securing of virtual private servers, the installation of Uptime Kuma and Zabbix on said servers and the configurations on both the servers' and the clients' side necessary for successful monitoring. The testing phase of the project is also summarized.

In the third chapter the authors provide their individual perspectives on their experience while working on the project.