TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Martin Erik Pille 175859IAAB

Keskse logilahenduse teenuse loomine Telia ärikliendile

Bakalaureusetöö

Juhendaja: Siim Vene
Magister
Kaasjuhendaja: Matis Palm
Rakenduskõrgharidus

Tallinn 2024

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Martin Erik Pille

04.01.2024

Annotatsioon

Lõputöö eesmärgiks on luua Telia ärikliendile logilahendus vastavalt Telia esitatud nõuetele ja parameetritele. Alustuseks kirjeldatakse ära Telia tüüpklientuuri eeldused ja määratletakse nõuded, millele logilahendus peab vastama. Edasi leitakse logilahenduse jaoks vajalikud arvutiprogrammid, kasutades võrdlus- ja analüüsimeetodeid.

Erinevate arvutiprogrammide analüüsi tulemusena valitakse välja sobivad programmid logilahenduseks. Välja valitud programmid paigaldatakse ja konfigureeritakse töötama Telia testkeskkonnas. Töö tulemusena luuakse töötav logilahenduse prototüüp ja logilahenduse paigaldamise juhend.

Lõputöö suurimateks väljakutseteks oli erinevate programmide dokumentatsiooni mõistmine ja paigaldamine töötavaks konfiguratsiooniks. Töö käigus tekkinud probleemidele logifailide rotatsiooni ja varundamise osas leiti töötavad lahendused.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 38 leheküljel, 9 peatükki, 9 joonist, 4 tabelit.

Abstract

Creation of a Central Logging Solution for Telia's Business Client

The aim of the thesis is to create a logging solution for Telia’s business client according to the requirements and parameters provided by Telia. To begin with, the prerequisites of Telia’s standard clientele are described and the requirements for a logging solution are determined. Next, the computer programs needed for the logging solution are found using comparison and analysis methods.

As a result of the analysis of various computer programs, suitable programs are selected for the logging solution. The selected programs are installed and configured to work in Telia’s test environment. As a result of the work, a working log solution prototype and a installation guide is created.

The biggest challenges of the thesis were understanding the documentation of various programs and installing them into a working configuration. Working solutions were found for the problems that arose during the work regarding the rotation and backup of log files.

Using a lightweight program, logs are collected from the client machine and sent to a centralized log collector server. The log collector manages the log files by saving them to a self-hosted network drive on another server. A monitoring server is setup on a monitoring workstation to track logfiles and display informaton on events.

The thesis is in Estonian and contains 38 pages of text, 9 chapters, 9 figures, 4 tables.

Lühendite ja mõistete sõnastik

CSV	*Comma-separated values*, komaga eraldatud väärtused
DHCP	*Dynamic Host Configuration Protocol*, dünaamiline hostikonfiguratsiooni protokoll
DNS	*Domain Name System*, domeeninimede süsteem
HTTP	*Hypertext Transfer Protocol*, hüperteksti edastusprotokoll
HTTPS	*Hypertext Transfer Protocol Secure*, turvaline hüperteksti edastusprotokoll
I/O	*Input/Output*, sisend/väljund
IaaS	*Infastructure as a service*, infrastruktuur teenusena
IPv4	*Internet Protocol version 4*, internetiprotokolli versioon 4
IPv6	*Internet Protocol version 6*, internetiprotokolli versioon 6
Kerberos	Autentimisprotokoll
MB	*Megabyte*, megabait
Mbps	*Megabit per second*, megabitti sekundis
MSSQL	*Microsoft Structured Query Language Server*, microsofti struktuurpäringukeele server
MySQL, Oracle, SQL Server	Relatsiooniline andmebaasi haldamise süsteem
OSS	*Open-source software*, avatud lähtekoodiga tarkvara
PowerShell	Käsuinterpretaator ja skriptimiskeel
SQL	*Structured Query Language*, struktuurpäringukeel
SSL/TLS	*Secure Sockets Layer/Transport Layer Security*, turvasoklite kiht/transpordikihi turbeprotokoll
TCP	*Transmission Control Protocol*, edastusohje protokoll
TSV	*Tab-separated values*, tabeldusmärgiga eraldatud väärtused
UDP	*User Datagram Protocol*, kasutajadatagrammi protokoll
WEC	*Windows Event Collector*, Windows sündmuste koguja
WEF	*Windows Event Forwarder*, Windowsi sündmuste edastaja
WinRM 2.0	*Windows Remote Management*, Windowsi kaughaldus
XML	*Extensible Markup Language*, laiendatav märgistuskeel

Sisukord

1 Sissejuhatus 9
2 Telia tüüpklientuuri kirjeldamine ja nõuete määramine 11
2.1 Telia tüüpkliendi kirjeldamine 11
2.2 Telia tüüpkliendi nõuded 13
3 Logide töötlemine 15
3.1 Logide rotatsioon 15
3.2 Logide varundamine 16
3.3 Logide monitooring ja analüüs 17
4 Microsofti ja vabavaraliste logimistarkvarade analüüs 20
4.1 Microsofti ja vabavaraliste logimistarkvarade võrdlus ja analüüsi tulemus 25
5 Failipõhiste ja andmebaasipõhiste salvestussüsteemide võrdlus 27
5.1 Salvestussüsteemide võrdlus ja analüüsi tulemus 29
6 Pilvesalvestusteenuste analüüs 31
6.1 Pilvesalvestusteenuste võrdlus ja analüüsi tulemus 34
7 Monitoorimisprogrammide analüüs 36
7.1 Monitoorimisprogrammide võrdlus ja analüüsi tulemus 37
8 Logilahenduse paigaldamine testkeskkonnas 39
8.1 Pilveteenuse serveri konfiguratsioon 39
8.2 Kollektorserveri konfiguratsioon 40
8.3 Kliendiagendi konfiguratsioon 42
8.4 Monitoorimisarvuti konfiguratsioon 42
9 Kokkuvõte 47
Kasutatud kirjandus 49

Jooniste loetelu

Joonis 1. Windowsi lauaarvutiversiooni turuosa kogu maailmas alates aprill 2022 - märts 2023 [5]..... 13
Joonis 2. Lõputöö testkeskkonna diagramm. 39
Joonis 3. Seafile serveri konfiguratsiooni käsud. 39
Joonis 4. Kollektorserveri konfiguratsioon. 41
Joonis 5. Klientagendi konfiguratsioon. 42
Joonis 6. Telegrafi konfiguratsioon. 43
Joonis 7. Grafana andmete allika seadistus. 44
Joonis 8. Grafana andmete viimine õigele kujule..... 45
Joonis 9. Grafana lõppseadistused. 46

Tabelite loetelu

Tabel 1. Erinevate Microsofti ja vabavaraliste logimistarkvarade komponentide võrdlus. 20
Tabel 2. Failipõhiste ja andmebaasipõhiste salvestussüsteemide omadused. 27
Tabel 3. Pilvesalvestusteenuste omadused. 31
Tabel 4. Monitoorimisprogrammide omadused. 36

1 Sissejuhatus

Autori lõputöö teema käsitleb logilahenduse teenuse tehnilist juurutamist Telia ärikliendile. Logilahenduse paigaldamine ja seadistamine labori keskkonnas on autori arvates hea lähtekoht, et luua töötav logilahenduse prototüüp arvestades etteantud parameetreid. Lahenduse testimisest ja valideerimisest saan teadmisi, mida saan tulevikus arvestada reaalsetes toodangusüsteemides. Lõputöö annab kogemusi, mida saan kasutada tulevases süsteemi-administreerimise karjääris.

Logilahenduse moodustavad koos töötavad tarkvarad, mis koguvad klientmasinatest kokku vajaminevad logikirjed. Järgnevalt salvestatakse logid kettapinnale ja neid hoitakse seal ettemääratud aja vältel. Terviklahenduse abil tehakse järgnevaid tegevusi: logisid jälgitakse, veendutakse nende tekkimises, kogumises ja salvestumises vastavalt etteantud parameetritele. Kui logidele etteantud salvestusperiood on ületatud, siis kustutakse logid ära. Logilahenduse tervikpakett koosneb kolmest komponendist:

- Logide kogumine
- Logide salvestamine
- Logide kogumise monitooring

Logilahenduse olemasolu annab ettevõttele võime kiiresti ja mugavalt leida lahendusi esinevatele võimalikele anomaaliatele ja probleemidele. Kui ettevõttele tehakse küberrünnakuid, mis häirivad või tekitavad kahju firma IT infrastruktuurile, siis kasutades logisid saab reageerida nendele intsidentidele ja lahendada tekkinud olukordi ning leida juurpõhjused katkestustele ja probleemidele. Tänase seisuga on maailmas kõige populaarsemad logilahendused turul Gartneri hinnangul näiteks Paessler PRTG, OpManager, Zabbix ja Datadog [1].

Lõputöö põhiprobleem on, et kõik turul olevad populaarsemad lahendused eeldavad kliendipõhist logiklastri paigaldamist, mida Telia ei soovinud. Samas ei ole turult leida lihtsalt paigaldatavat ja hallatavat logilahendust. Telial on vaja luua minimaalsete

ressurssidega jagatav logilahendus ärikliendile, lähtudes töö 2. peatükis kirjeldatud kriteeriumitest.

Situatsiooni kirjelduseks on olukord, kus puudub tsentraalne lahendus, mida saaks kasutada samaaegselt mitmel Telia ärikliendil IT süsteemide ja tööjaamade logide salvestamiseks, seda kõike kliendi jaoks võimalikult väikese kuluga. Lõputöö tulemusena luuakse logilahenduse prototüüp, mis on odav, kergesti hallatav, skaleeritav ja ei eelda logiklastri paigaldamist ja haldamist.

Lõputöös kasutan võrdlus- ja analüüsimeetodit, mille käigus võrdlen erinevaid logide kogumis-, pilveteenuse- ja monitoorimisprogramme. Võrdlus- ja analüüsimeetod seisneb valitud programmide kõige olulisemate kriteeriumite omavahelises võrdlemises, et leida parim lahendus. Võrdlen Telia poolt turult pakutavatest programmidest välja valitud vabavaralisi ja tasulisi logilahenduste tarkvarasid ja hakkan neid omavahel analüüsima. Pärast analüüsi valin kriteeriumite alusel välja parima lahenduse ja rakendan seda Telia testkeskkonnas. Selle tulemusena loon juhendi äriklientide vastutavatele süsteemi administraatoritele, mida saab kasutada logilahenduse paigaldamiseks soovitud IT keskkonnas.

Lõputööga hakkan ma looma logilahendust lähtudes Telia nõuetest ja kirjeldatud probleemidest. Tutvustan Telia tüüpklientuuri ja nende nõudeid logilahendusele. Lõputöö tulemusena luuakse juhend logilahenduse seadistamiseks ja paigaldatakse logilahenduse prototüüp testkeskkonnas.

2 Telia tüüpklientuuri kirjeldamine ja nõuete määramine

Logilahendus peab sobima võimalikult paljudele Telia IT klientidele ja seetõttu tuleks kirjeldada, milline on tüüpiline klient, kelle vajadustele vastavalt keskne logilahendus luuakse. Määratakse ära Telia poolsed nõuded logilahendusele, et tulemus vastaks antud kriteeriumitele. Analüüsi aluseks on võetud Telia poolt soovitatud logimistarkvarad.

2.1 Telia tüüpkliendi kirjeldamine

Telia Microsofti süsteemiadministraatoritelt on tulnud lähteülesande edastamise käigus info, et Telia kliendid kasutavad tööjaamadena ja serveritena enamasti Windowsi operatsioonisüsteeme. Sellest tulenevalt peaks logilahendus töötama peamiselt Windowsi süsteemides ja toetama erinevaid Windowsiga seotud logitüüpe. Lahendus peab olema skaleeritav ja lahenduse ülalpidamise ja juurutamise kulud peaksid olema minimaalsed. Igal kliendil on erinevad vajadused, nõuded ja töömetoodika ja seega peame arvestama erijuhtudega, kui on vaja logilahendusse konfigureerida teatud kliendipõhised erisused. Arvesse tuleb võtta, et Windowsi OS-il on vaikimisi sisse lülitatud rakenduse, turvalisuse ja süsteemi logid [2]. Windows salvestab logisid, kuni konfigureeritud logifaili maht on täis. Vaikesättega on tööjaamas oleva logifaili maht tavaliselt 20 MB (Megabyte). Microsofti praktika järgi hoitakse serveri operatsioonisüsteemi puhul tavaliselt 4194.24 MB ulatuses logikirjeid iga logitüübi kohta [3].

Telial on suur hulk IT teenuste (operatsioonisüsteemide haldusteenus ja arvuti töökohateenus) ja infrastruktuuri, kui teenuse (IaaS) kliente, kellel on erinevad nõudmised ja vajadused. Tüüpiline Telia äriklient on 20 kuni 50 töötajaga ettevõte, kes majutab ühte kuni viite virtuaal- või füüsilist serverit Telia andmekeskustes ja kelle tööjaamu haldab Telia (parandamine, uuendamine, kasutajatugi). Enamikel klientidel on virtuaalmasinate jaoks kasutusel Windowsi Serveri operatsioonisüsteemid, operatsioonisüsteemi versioonid on kaetud vahemikus Windows Server 2003 kuni 2022. Kõige tavalisemad serveri rollid Telia klientidel on järgmised:

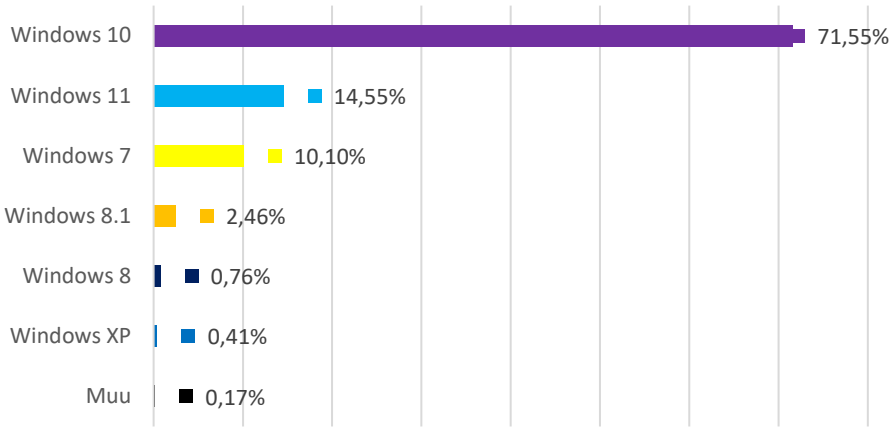
- Domain Controller teenus

- DNS/DHCP
- Failiserveri teenus
- MSSQLi andmebaasi teenus

Lisaks on enamikel klientidel ka Windowsi-OSi põhised tööjaamad, mille logisid oleks vaja keskselt koguda. Logisid peab koguma, sest siis saab efektiivsemalt probleeme ülesse leida ja lahendada tekkinud intsidente. Tööjaamad salvestavad logisid vaikimisi lokaalselt, samal ajal puudub keskne süsteem logide kogumiseks ja analüüsimiseks ning kättesaadavaks tegemiseks. Sellest tulenevalt on tekkinud vajadus koguda nõutud logid ühtsesse logiserverisse, mille käideldavus ja logisalvestuse perioodi oleks võimalik kliendipõhiselt ja -vajadustele vastavalt seadistada. Windowsi põhilistes operatsioonisüsteemides tuleks juurde koguda Windows Security logid, Sysmon logid ja PowerShell logid [4]. Kokku tuleks koguda ka rakenduse, turvalisuse ja süsteemi logid.

Üks probleem on, et Windows Event logisid on keeruline analüüsida. Keskkonnas, kus asub näiteks 20 serverit ja 100 tööjaama, tekivad aja jooksul suur hulk logisid, millest on keeruline üles leida vajaminev teave. Samas ei pruugi vajaminev logi eksisteerida, kuna logimist ei teostata piisavalt pikalt või õige seadistusega, näiteks Windows Security logides, Sysmon (eraldi Sysinternalsi tarkvara) logides ja PowerShell logides. Selle tulemusena ei pruugi jääda potentsiaalse küberturbe rünnaku või intsidendi tõttu maha jälge, mille abil saaks tuvastada rünnaku allika, mis programmi selleks kasutati ja millise rünnakuga oli tegemist.

Telial on vajadus leida lahendus, kuidas pakkuda väikestele ja keskmise suurusega äriklientidele kuluefektiivset, logivarunduse nõudeid ja parimaid praktikaid täitvat platvormi. Kõige populaarsemad Windowsi (keskmine statistika maailmas) tööjaamad on nähtavad Joonis 1 [5]:



Joonis 1. Windowsi lauaarvutiversiooni turuosa kogu maailmas alates aprill 2022 - märts 2023 [5].

2.2 Telia tüüpkliendi nõuded

Telia süsteemiadministraatorite käest on lõputöö autor saanud ülevaate „Telia tüüpkliendi nõuete ja vajaduste kohta“, seega saame välja tuua nõuded, millised peavad olema vastava logilahenduse kriteeriumid ja võimekus.

Telia tüüpkliendi jaoks loodava logilahenduse nõuded on kokkuvõtvalt järgmised:

- Logide edastamine minimaalsete muudatustega tööjaamas ja serveris
- Võimeline keskselt logisid salvestama odavale kettapinnale
- Logilahendus oleks minimaalsete kuludega nii klientidele, kui ka Teliale
- Skaleeritav sõltuvalt klientide tööjaamade ja serverite arvust
- Klientide logisid on võimalik loogiliselt eraldada
- Peab olema võimalik määrata salvestusaeg sõltuvalt ettevõtte nõuetest ja kehtivast seadusandlusest
- Luuakse majasisene logide kättesaamise kasutajaliides

Telia peamine äriline vajadus on huvi pakkuda paremat ja kvaliteetsemat teenust, mille läbi on ka klientide huvid ja probleemid efektiivsemalt lahendatavad.

Logiedastamine peaks toimuma minimaalsete muudatustega tööjaama või serveri jaoks. Logilahendus ei tohi muuta tööjaamu ega serverit nii, et tema esialgne funktsioon oleks piiratud ja ta ei ole enam võimeline oma etteantud ülesandeid teostama. Serverit ja tööjaamu võib logilahendus koormata maksimaalselt 5-10%. Logide kogumises ei ole logide edastamise kiirus ja järjepidevus kriitilise tähtsusega, sest peamine probleem on

logide keskse salvestusvõimekuse puudumine, mistõttu on potentsiaalsete ohtude ülesleidmine ja lahendamine raskendatud.

Logide kogumise keskkond peaks olema väikese ressursivajadusega ja seda peab saama skaleerida mitmetele klientidele samadel alustel. Üks virtuaalmasin peab olema võimeline koguma logisid mitmetelt klientidelt korraga, et optimeerida ressursse. Siin võiks olla lahenduseks tsentraalne server, mis suudaks teenindada vähemalt 10 kuni 20 klienti samaaegselt. Vajadusel saab juurde lisada koormusjaoturi, et veenduda logikogumise süsteemi käideldavuses.

Telia poolt on antud nõudeks, et otsitaval logilahendusel peab olema võimekus logisid salvestada võimalikult odava ketta pinna peale. Telia näitel oleks lahenduseks S3-standardil või SAS-ketastel põhinev salvestuskeskkond. Telial endal on kasutusel Cloudian S3-Compatible Object Storage.

Lahendada küsimused, kuidas keskset logilahendust seadistada ja hallata ning kuidas liidestada klient keskse logisüsteemiga. Samas peab olema võimalus erinevate klientide logisid loogiliselt eraldada ja määrata salvestusaeg, kui kaua logisid salvestatakse, näiteks 30 päeva, 60 päeva, 90 päeva jne. Vajalik on luua majasiseselt logide kättesaamiseks kasutajaliides, et vastava olukorra tekkimisel saavad ettevõtetes töötavad administraatorid logidele ligi. Üks vabavaraline variant selle teostamiseks on NextCloud. Luuakse juhend äriklientide vastutavatele administraatoritele logilahenduse paigaldamiseks, et saada kätte vajalikud logid nende analüüsimiseks.

Pikemas skoobis võivad oma logidele ligi pääseda ka kliendid ja selleks tekitatakse vastav kasutajaliides. Meeles tuleks pidada, et klient saaks ligi ainult oma logidele. Kui klient saab näha teiste klientide logisid, mida ta ei tohiks näha, võivad tekkida turvalisuse riskid ja privaatsusega seotud probleemid. Kasutusele võetakse rollipõhine juurdepääsukontroll, kus kasutajaid luuakse ja autoriseeritakse. Lõputöö skoobis ei ole logianalüüsi platvormi valideerimine, mis suudaks näiteks Windows Event logidest süntaksipõhist otsingut teha.

3 Logide töötlemine

Logilahenduses on vaja logifaile ja salvestatud sündmusi hallata kasutades logide rotatsiooni protsessi, et ei tekiks probleeme logifailide suurustega. Logide varundamine on logifailide varundamise poliitika, mis ütleb, kui kaua teatud logifaile hoitakse, enne kui need ära kustutatakse. Logilahendus peab olema võimeline kokkukorjatud logisid monitoorima ja selle tulemusena saab vajadusel teostada logidele analüüsi. Logide monitooring ja logide analüüs on omavahel tihedalt seotud ja käivad logilahenduses käsikäes. Monitooring jälgib logikirjeid ja nende sisu ja annab teada probleemidest. Logide analüüsi teostavad tavaliselt administraatorid ja IT'ga seotud inimesed [6] [7].

3.1 Logide rotatsioon

Logilahenduses kasutatakse põhiliselt rotatsiooni protsessi logifailide suuruste haldamiseks. Kui logi fail on liiga suur, võivad tekkida erinevad probleemid logide protsessimisel ja töötluses. Administraatorid ei pruugi saada ligi logifailidele, et neid analüüsida. Võivad tekkida probleemid logide leidmisega, kui logifailid ei ole kuidagi ajaliselt kategoriseeritud.

Logide rotatsiooni protsess on tavaliselt kiire, võtab paar sekundit aega ja sell käigus muudetakse ära mahu ületanud logifaili nimi, luuakse tühi logifail uute logide kogumiseks ning hakatakse sinna logifaili edasi kirjutama. Logifailide levinumaks nimereegliks on failide nimedesse kirjutatav kuupäev, kuu ja aasta, näiteks „apache_log13_10_2023.log“ [8].

Logifailide rotatsioon on vajalik järgnevatel põhjustel:

- Kettaruumi kokkuhoid
- Jõudluse tagamine
- Reaalajas hoiatuste tuvastamine

Kui logifailide rotatsiooni ei tehta või tehakse liiga harva, siis võivad kaasneda erinevad probleemid. Serveri kettaruum võib virtuaalserverite puhul logisid salvestades kiiresti täis

saada. Kriitilised funktsioonid võivad lõpetada funktsioneerimise ja uusi logisid saab kirjutada ainult siis, kui tekib ruumi juurde. Intsidendi korral ei pruugi olla kirjeid, mida on vaja probleemi lahendamiseks.

Suurte logifailide korral ei pruugi serveris töötavad programmid enam suuta lugeda logifaile. Logifailide avamine, lugemine ja kirjutamine võib võtta liiga kaua aega. Manuaalsed operatsioonid suurte logifailide lugemiseks võivad võtta liiga palju aega ja selline aeglane tegevusviis ei ole eelistatud, kui on tegemist kriitiliste lahendamist vajavate intsidentidega.

Kui logifailid on liiga suured, siis on nende töötlemine aeganõudev. Rünnaku korral võtab logifailide töötlemine niikaua aega, et otsitava sündmuse leidmine suurest logifailist on raskendatud, sündmus võib jääda mitmeks päevaks nähtamatuks ja selle tulemusena võib hoiatus tulla liiga hilja.

3.2 Logide varundamine

Logifailid varundamise käigus kas kustutatakse, surutakse kokku (pakitakse) või arhiveeritakse. Logide kustutamine võib tunduda kõige kiirem ja mugavam viis logilahenduse kettaruumi säästmiseks, aga sellega võivad kaasneda probleemid. Kustutatud logides võib olla informatsiooni, mis aitavad tekkinud intsidenti lahendada ja selleks oleks vaja kokku leppida, kui kaua logisid hoitakse enne nende kustutamist. See sõltub firma logipoliitikast, mis tuleb kokku leppida IT administraatori(te)ga.

Logifailide kokkusurumine on protsess, kus failid pakitakse kokku nii, et failimaht väheneb, aga faili lugemine ja kirjutamine võtab rohkem aega. Seda tehakse tavaliselt vanades logides, mille järgi on potentsiaalne vajadus tulevikus, aga mida ei kasutata pidevalt.

Arhiveerimine on vanade logide liigutamine eraldi salvestussüsteemi, kas teise masinasse, pilvepõhisesse teenusesse või võrgukettale. Tavaliselt tehakse seda koos logifailide kokkusurumisega, et säästa kettaruumi ja arvestades vajadusega, et logisid saaks tulevikus töödelda.

Kõige tähtsamad logid on infoturbega seotud logid. Rünnakud ja pahavara võivad tekitada enim kahju kliendile. Sellest tulenevalt peaks turvalogisid ära kustutama ja arhiveerima kõige viimasena.

Ettevõte peaks ise hoidma logisid, mida ta enda jaoks peab vajalikuks. Juhul kui tekivad turbe- või käideldavusintsidendid, siis ei tekiks olukorda, kus ettevõttel puuduvad logid intsidentide juurpõhjuste analüüsiks ja probleemide lahendamiseks. Kõik logid, mida ettevõte enam ei kasuta või on vananenud, tuleks süsteemist ära kustutada, säästmaks kettaruumi ja jõudlust [9].

Logifailide säilitamise periood sõltub kliendist. Mõned ettevõtted peavad hoidma kõiki logisid paar aastat, teised võivad hoida logisid paar kuud, ajapiirangud sõltuvad ettevõtte tüübist ja nende logivarundamise poliitikast. Enamik ettevõtetest peaksid enda süsteemilogisid hoidma vähemalt ühe aasta. Sellest tulenevalt peaksid ettevõtted teadma ka kehtivaid tööstusstandardeid, määrusi, seadusi ning põhilisi ettevõtete küberturvalisuse ohtusid ja probleeme. Samas tuleks analüüsida ja arutleda IT administraatoritega ettevõtte vajaduste üle ja koostada igale kliendile just tema ettevõttele sobiv logivarundamise poliitika.

3.3 Logide monitooring ja analüüs

Logide monitooring on pidev protsess, mis jälgib konkreetseid sündmusi või mustreid, et oleks võimalik identifitseerida intsidente ja probleeme. Kasutades logide jälgimist saab tagada süsteemide stabiilsuse, leida üles turvaohud, jälgida muudatusi ja uuendusi süsteemides. Logide kogumine ja sellest tulenevalt hoiatuste ja teadete ettekuvamine annab administraatoritele võimaluse kiiresti ja ennetavalt reageerida sündmustele ning võimalikele ohtudele. Logide monitooring on oluline järgnevates valdkondades:

- Seadustest tulenevate nõuete järgimine
- Intsidentidele reageerimine ja lahenduste leidmine
- Infoturbe toimimine
- Tehnilise tiimi jõudlus ja koostöö võimalused probleemide lahendamisel
- Protsesside automatiseeritus

Sõltuvalt ettevõttest ja seadustest tuleb varundada teatud logisid kindla perioodi jooksul. Logide monitooring näitab kiiresti ja mugavalt ära, kas ettevõtte eeskirju järgitakse.

Logilahendus tekitab logid vajalikest sündmustest, nagu näiteks kasutajate sisselogimistest, kasutajate haldamisest, süsteemi tööst ja jõudlusest.

Monitooring annab võimaluse teatud sündmuste ja anomaalsete mustrite esinemisel saata administraatoritele välja teateid, et leida kiiremini lahendused intsidentidele ja probleemidele. Samas, saab ennetada intsidenti või probleemi tekkimist tänu logide monitoorimisele. Monitoorimise käigus leitakse üles nõrgad kohad süsteemides, mille jõudlus ei ole piisav, ja lisatakse vajadusel juurde rohkem süsteemiressursse nagu mälu, protsessorivõimsust või kõvakettapinda. Samal ajal tuvastatakse ka turvaaugud ja sisselogimiskatsed. Tehnilised tiimid saavad kokkukorjatud logide abil teostada logianalüüsi, mis annab võimaluse muuta või suurendada süsteemide mahte ja jõudlust. Administraatorid saavad ennetavalt teostada parandusi välistades olukorra enne, kui lõppkasutaja saab mõjutatud.

Logide monitoorimisele aitavad kaasa mitu tegurit, mis mõjutavad logisid:

- Logide struktureering
- Unikaalsed identifikaatorid
- Reaalajas monitooring
- Hoiatused

Struktureeritud logid aitavad kaasa intsidentide ja probleemide leidmisele. Logidel on küljes info:

1. Kus kohast logi tuli? (Where?)
2. Millal logi tekkis? (When?)
3. Missugune on logi tase? (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug) - „Criticality level“ [10]
4. Mis programm või teenus logi väljastas? (Who, what?)

Logidele saab lisada silte ja unikaalseid identifitseerijad, mis aitavad logisid filtreerida ja leida vastav sündmus. Reaalajas logide monitooring aitab ennetada intsidente ja probleeme ja edastab info sündmustest kiiresti administraatoritele. Seadistades monitoorimise programmis automaatsed hoiatused, aitavad need intsidentide tekkel teavitada administraatoreid olukordadest, mis vajavad sekkumist. Administraatoritel on

võimatu jälgida igat monitoorimise mõõdikut ja sellepärast on mõistlik panna üles automaatteavituste süsteem, seadistades selle vastavalt monitoorimise vajadustele.

Logide analüüs on vajalik tagamaks logide asjakohase tõlgendamise ja tekkinud probleemide mõistmise. Peamiselt teostavad logide analüüsi süsteemiadministraatorid ja infoturbega seotud inimesed. Logide monitoorimise automaatika saadab administraatoritele edasi teavituse olukorrast, mis võib mõjutada tervet süsteemi või selle teatud osa. Saadud infost tulenevalt teostatakse analüüs, mis on intsidendi või probleemi algpõhjus ja pakutakse välja lahendus. Ilma logide monitoorimisteta on analüüsi keeruline teostada ja ei ole võimalik ennetada intsidentide teket. Pärast logilahenduse juurutamist saab vajadusel uuendada logide monitoorimise programmi mõõdikuid, et tulevikus kiiremini ja mugavamalt sooritada logide analüüsi.

4 Microsofti ja vabavaraliste logimistarkvarade analüüs

Logilahenduse loomise esimeseks sammuks on vaja analüüsida ja uurida erinevaid Telia poolt soovitatud logimistarkvarasid. Üheks otsitavaks kriteeriumiks on vajadus piirata logilahenduse komplekssust ja maksumust. Koos Teliaga on valitud välja logimistarkvarad, mis annaksid võimaluse lõputöö peatükis 2 ja püstitatud probleemi lahendada. Tabel 1 on esitatud logimistarkvarad ja võrreldud nende vastavust esitatud kriteeriumitele [11] [12] [13] [14] [15] [16] [17] [18].

Tabel 1. Erinevate Microsofti ja vabavaraliste logimistarkvarade komponentide võrdlus.

Kriteerium	**Windows Event Forwarder (WEF)**	**Windows Event Collector (WEC)**	**NXLog Community edition**	**WinSyslog**
Toetatud operatsiooni-süsteemid	Windows XP/7/8/10/2008, Windows Server 2003/SP1/SP2, Vista SP1	Windows 7, Windows Server 2008 R2/2012+, Vista SP1	Windows 7/8/9/10/11, Windows Server 2008/2012/2016 /2019/2022, Nano Server, Vista, Linux	Windows 7/8/10, Windows Server 2008 R2/2012/2016/2 019, Vista
Push või Pull	Mõlemad	Mõlemad	Mõlemad	Push
IPv4 ja Ipv6	Mõlemad	Mõlemad	Mõlemad	Mõlemad, ainult üks korraga
Sõnumite krüpteering	Kerberos ja HTTP/HTTPS	Kerberos ja HTTP/HTTPS	SSL/TLS	SSL/TLS
Sündmuse puhvri suuruse määratlemine	Saab suurendada, ei anna teada, kui saab täis		Jah	1024 MB puhver kuni 100000 - 200000 MB sõnumit
Sündmuste formaat	Tavatekst või XML (EVTX, Windows Event Log format)	Tavatekst või XML (EVTX, Windows Event Log format)	CSV, JSON, Syslog, XML jpm.	Tava tekst, JSON, XML, CSV

Kriteerium	**Windows Event Forwarder (WEF)**	**Windows Event Collector (WEC)**	**NXLog Community edition**	**WinSyslog**
Sündmuste sagedus	Tavaline, Väikseim võrgukoormus, Väikseim ooteaeg, Kohandatud		Väljas, madal, keskmine, kõrge	
Mitu sündmuste kogujat võrgus	Jah	Ei		
Sündmusi sekundis		Keskmiselt 3000	Võimalik 500000	33000 UDP 128000 TCP
Salvestus-formaadid		Puhvrid, siis EVTX fail	Vana: BSD Syslog (RFC 3164) Uus: IETF Syslog (RFC 5424) Andmebaasid	Üks fail päevas, uue faili seadistamine, kui suuruselimiit on täidetud, maksimaalne failimaht, failide arv (ringiline logimine)
Vajalikud tulemüüri reeglid	WinRM 2.0 HTTP port: 5985 ja HTTPS Port: 5986	WinRM 2.0 HTTP port: 5985 ja HTTPS Port: 5986	TCP, UDP, Mitu NXLog Manageri	Sama masin, mitu serverit, erinevad syslog pordid, TCP või UDP
Registri suurus	>1000 WEF arvutit, Event Viewer võtab paar minutit aega laadimisega >50,000 WEF arvutit, peab konfigureerima wecutil.exe >100,000 WEF arvutit, registrit ei saa lugeda WEC server tuleb ümber ehitada	Üks WEC 2000 - 4000 tööjaamale Keskmine vajalik ressurss 4000 logiedastaja kohta: 16 GB muutmälu, 4 protsessorid keskmise koormusega	Kaks protsessori tuuma Muutmälu: miinimum: 2048 MB soovitatud: 4096 MB Kettaruum: miinimum: 300 MB soovitatud: 1024 MB	33000 UDP 128000 TCP Intel i7-4790S @ 3.2GHz 32GB Muutmälu SSD ketas Windows 10

Kriteerium	Windows Event Forwarder (WEF)	Windows Event Collector (WEC)	NXLog Community edition	WinSyslog
Logide edastuse tüübid	Algeline: vaikimisi Sihitud: lisab sissetungijaga seotud tegevused		Agendipõhine kogumine: süsteemi logiandmetel Agendita kogumine: logi andmed võrgus olevasse NXLogi serverisse Võrguühenduseta logitöötlus: pakettlogi töötlemine	
Hind	Valikuline funktsioon Windowsi operatsiooni-süsteemiga, mis tuleb lubada	Valikuline funktsioon Windowsi operatsioonisüsteemiga, mis tuleb seadistada	Avatud lähtekoodiga, Enterprise edition	30-päevane tasuta prooviperiood, Maksudeta: Professional: 129€ Enterprise: 699€

Windows Event Forwarder on Microsofti logimistarkvara, mis võimaldab kliendi masinas lugeda ja seejärel saata kliendiseadmes (tööjaam või server) toimuvaid sündmusi keskserverisse, kus eeldusena peab töötama Windows Event Collector. Tarkvara on eelpaigaldatud Windowsi operatsioonisüsteemides ja seega ei vaja paigaldamist ega eraldi litsentsi ostmist. Windows Event Viewer on saadaval kõikides Windows masinates alates Windows NT 3.1, mille väljalaske aasta oli 1993. Windows Event Forwarder töötab loogiliselt koos Windows Event Collector'iga, seega on vaja mõlemat tarkvara, et üles ehitada töötav logilahendus. Kohalikus masinas kogutakse kokku soovitud sündmused teksti või XML (Extensible Markup Language) kujul ja vastavalt konfiguratsioonile saadetakse kas iga 30 sekundi, 15 minuti, 6 tunni, või omale kohandatud aja vahemiku tagant logid Windows Event Collector (WEC) serverisse. Logide saatmissagedust saab seadistada ja võimalik on luua oma vajaduste järgi kohandatud sõnumite saatmissagedus. Saab valida ka kolm erinevat eelkonfigureeritud võrgu kasutuse seadistust: standardne, minimaalne võrgu kasutus ja minimaalne viivitus. Standardne kasutab Pull meetodit ja saadab välja sõnumeid iga 15 minuti jooksul. Minimaalne võrgu kasutuse meetod kasutab

Push meetodit ja saadab välja sõnumeid iga 6 tunni tagant. Viimane mainitud meetod koormab võrku kõige vähem, aga selle tulemusena ei pruugi teatud logid kohale jõuda. Minimaalse viivitusega meetod saadab välja sõnumeid iga 30 sekundi tagant ja kasutab võrku pidevalt, ning selle tulemusena on suurem tõenäosus, et kõik logid jõuavad keskserverisse korrektselt kohale.

Standardselt logitakse igast masinast kokku kõik baas-defineeritud logid ja vajadusel veel spetsiifilised logid kasutatavatest arvutitest. Suunatud logide kogumise tüüpi on soovitatud seadistada arvutitele, milles võivad esineda turvalisuse riskid. Kohalike sündmuste logil on puhver ja kui juhtub, et logisid ei saa saata ja puhver saab täis, siis hakkab Windows Event Forwarder puhvrit üle kirjutama ja soovitud logid kustutatakse. Kohaliku puhvri suurust on vaja seadistada, et logisid ei kustutataks ära. Samuti ei teavitata keskselt, kas kohalik puhver on hakanud logisid üle kirjutama. Puudub võimalus korrektselt monitoorida puhvri suurust. Sündmuste formaadiks on töödeldud tekst koos sündmuse kirjeldusega, mis suurendab iga sündmuse suurust kaks kuni kolm korda või kompaktne binaarne XML formaat, mis on väiksema mahuga. Logisid saab saata välja kasutades IPv4 (Internet Protocol version 4) või IPv6 (Internet Protocol version 6) protokolle, nii Push, kui ka Pull meetodit kasutades, Microsofti poolt on soovitatud kasutada Push meetodit.

Windows Event Collector tuleb paigaldada serverile eraldi rollina. Windows Event Collector saab kätte Windows Event Forwarder'i poolt saadetud logid ja salvestab need kohaliku sündmuste logisse. Kohalikus võrgus saab töötada mitu Windows Event Collector'it ja see on võimeline töötlema keskmiselt 3000 sündmust sekundis. Ühes Windows Event Collectoris saab olla korraga lahti nii palju võrguühendusi, kui palju on TCP (Transmission Control Protocol) porte avatud. Ühe Windows Event Collector serveriga on soovitatud pakkuda logikogumis teenust 2000le kuni 4000le tööjaamale. Kui pakutakse logide vastuvõtmise teenust väga paljudele arvutitele korraga võivad tekkida erinevad probleemid. Kui logitakse kokku üle 1000 arvuti ei pruugi Event Viewer logide avamise puhul mitu minutit reageerida. Üle 50 000 arvuti puhul on vaja konfigureerida Windows Event Collector utility, kuna Event Viewer ei ole enam võimeline logisid haldama. Üle 100 000 kliendi puhul ei saa enam logisid hallata ja Windows Event Collector server on vaja ümber ehitada [11].

NXLog Community edition on avatud lähtekoodiga logimise tööriist, mis on võimeline töötama ja koguma logisid nii Windows'i, Unix'i, Apple, jpt operatsioonisüsteemidest [19]. Kogutud logid saadetakse läbi SSL/TLS (Secure Sockets Layer/Transport Layer Security) krüpteeringu võrgus olevasse logiserverisse kasutades IPv4 ja/või IPv6 protokolle. Sündmuste puhvri suurust saab muuta ja salvestusformaatideks võivad olla: CSV (Comma-separated values), JSON, Syslog, XML jpt formaadid. Samuti annab tarkvara võimaluse protsessida saadud sündmusi soovitud formaati. Konfigureerida saab ka sündmuste saatmissagedust. NXLog on võimeline töötlema kuni 500 000 sündmust sekundis ühes võrgus. Mitu NXLog serverit saab olla korraga ühes võrgus ja nad on võimelised saatma logisid nii TCP, kui ka UDP (User Datagram Protocol) formaatides. Logisid saab salvestada erinevates andmebaasisüsteemides ja/või kasutades vana BSD Syslog (RFC 3164) või uut IETF Syslog (RFC 5424) standardit. NXLog'i agendipõhine logide kogumine toimub samas süsteemis, kus logisid korjatakse. Samas saavad seadmed agendita logisid saata võrgus olevale NXLog serverile. Vajadusel saab logisid manuaalselt töödelda, mille käigus logid muudetakse teise formaati, filtreeritakse välja vajalikud logid ja/või analüüsitakse vajalike logisid, mis on juba olemas.

WinSyslog on täiustatud syslog server Windows'ile. WinSyslog'il on sama põhimõte Unix RSyslog'iga ja tarkvaraga saab luua tsentraalse süsteemi, mis annab ülevaate sündmustest. WinSyslog on tasuline tarkvara, esimesed 30 päeva saab proovida tasuta ühe seadme peal ja seejärel peab ostma litsentsi. Ilma käibemaksuta on ühe Professional litsentsi versiooni hind Eestis 129 eurot ja Enterprise versioonil 699 eurot, mille kasutusaeg on üks aasta. Professional litsents lubab logida kokku 100 masinat ja Enterprise versioon lubab logimist seadistada lõpmatus koguses masinatel. Sinna hulka ei kuulu aastane uuenduste tasu. Sündmuste saatmine toimub kasutades Push meetodit ja seda saab ainult kasutada kas IPv4 või IPv6 protokolliga, ei saa kasutada mõlemat korraga. Logid saadetakse välja krüpteeritult SSL/TLS meetodit kasutades. 1024 MB suurune kohalik puhver on võimeline hoidma 100 000 kuni 200 000 sündmust lihtteksti, JSON, XML või CSV formaatides. Kasutades UDP protokolli on WinSyslog võimeline töötlema 33 000 sündmust sekundis ja TCP-d kasutades 128 000 sündmust sekundis. Logid salvestatakse ühte faili, mille suurus on ette määratud ja järgmisel päeval tekitatakse uus fail. Kui faili suuruse limiit saab täis luuakse uus fail. Seadistada saab programmi ka nii, et tekitatakse mitu faili ühes päevas. Kui kõikide seadistatud failide mahulimiit on täis kirjutatud ja süsteem ei saa rohkem faile juurde luua vastavalt

konfiguratsioonile, minnakse kõige vanemasse faili ja hakatakse logisid üle kirjutama. Ühes masinas saab töötada mitu WinSyslog serverit aga üks nendest peab kasutama TCP'd ja teine UDP'd.

4.1 Microsofti ja vabavaraliste logimistarkvarade võrdlus ja analüüsi tulemus

Pärast logimistarkvarade erinevate parameetrite võrdlust, saame tulemusi omavahel analüüsida ja välja pakkuda parima variandi vajaminevale logilahendusele.

Windows Event Forwarder ja **Windows Event Collector** töötavad koos ühtse paketina ja tulevad Telia äriklientidele koos Windows operatsioonisüsteemi litsentsidega. Üheks suureks miinuseks on see, et kui on vaja kokku koguda logisid paljudest seadmetest, hakkavad tekkima anomaaliad keskhalduse serveris seoses logide haldamisega. Event viewerit ei saa enam korrektselt kasutada ja logide lugemine võib muutuda ebapraktiliseks. Samuti ei ole süsteem võimeline töötlema suuri sündmuste koguseid.

NXLog Community edition on avatud lähtekoodiga tarkvara, mis pakub võrreldes Windows Event Forwarder'iga ja Windows Event Collector'iga rohkem võimalusi logilahendust skaleerida vastavalt ettevõtte vajadustele. Samuti saab tarkvara töötada Windows'i, Unix'i, Apple ja paljudest muudes operatsioonisüsteemides [19]. Sündmusi salvestatakse vajalikus formaadis ja saab salvestada vanas BSD Syslog (RFC 3164) formaadis või uues IETF Syslog (RFC 5424) formaadis. Lahendus on võimeline koguma 500 000 sündmust sekundis, mis on kordades rohkem kui eelnevalt võrreldud tarkvaradel. Ühes võrgus saab olla ka mitu NXLog serverit. NXLog annab võimaluse saata logisid kliendi masinas ilma agendita ja vajadusel saab logisid manuaalselt töödelda. Logid muudetakse soovitud formaati, filtreeritakse välja vajalikud logid ja/või analüüsitakse logisid, mis on olemas.

WinSyslog on sarnane NXLog Community edition'iga ja on mõeldud töötama Windows masinatel. WinSyslog suudab ainult töötada kas IPv4 või IPv6'ga. Logid on vaja salvestada faili ja konfigureerida, kui palju saab päevas faililogisid salvestada. Tarkvara saab kasutada ainult kas UDP või TCP'iga. Võrreldes NXLog'iga on WinSyslog võimeline saatma 128 000 sõnumit sekundis, mis on palju vähem. Üheks suureks miinuseks on, et WinSyslog on tasuline tarkvara, mille üks litsents maksab ilma

maksudeta 129 eurot üheks aastaks ja üks Professional litsents võimaldab monitoorida ainult 100 masinat korraga. Võrgus, kus on vaja hallata rohkem kui 100 masinat võib logilahendus aja jooksul osutuda ettevõttele päris kulukaks.

Parameetrite võrdluse tulemusena on NXLog Community edition hetkel kõige parem tarkvara vastavalt antud logilahenduse nõuetele ja oodatud parameetritele. Olles avatud lähtekoodiga ei ole vaja Telial NXLog Community edition'i eest litsentsikulusid maksta. Samas on logiprogramm kõige kiirem võrreldes teiste logilahendustega. NXLog töötab nii Windows kui ka Unix laadsetes operatsioonisüsteemides. Üldist konfiguratsiooni muutmata saab antud logilahendusse klientmasinaid kergesti juurde lisada.

5 Failipõhiste ja andmebaasipõhiste salvestussüsteemide võrdlus

Logilahendus korjab kokku logisid erinevatest seadmetest. Selleks, et logisid saaks kasutada ja vajadusel läbi töödelda, oleks vaja logisid salvestada. Põhiliselt on kasutuses kaks erinevat süsteemi, mis kujul logid salvestatakse. Selleks on kas failipõhine süsteem või andmebaasi põhine süsteem logide salvestamiseks. Mõlemad süsteemid on võimelised logisid salvestama soovitud kujul. Mõlemal lahendusel on omad negatiivsed ja positiivsed omadused, mis võivad mõjutada, kumb süsteem sobib paremini logilahenduse logide salvestamiseks. Tabel 2 on esitatud failipõhiste ja andmebaasipõhiste süsteemide erinevad omadused [20].

Tabel 2. Failipõhiste ja andmebaasipõhiste salvestussüsteemide omadused.

Omadus	**Failipõhine**	**Andmebaasipõhine**
Struktuur	Lihtne, struktureerimata formaat, salvestatud lihtfailidena	Struktureeritud formaat tabelite, ridade ja veergudega
Organisatsioon	Üks või mitu faili, puudub seos failide vahel	Kirjed on tabelites, seosed luuakse võtmete ja indeksite kaudu
Juurdepääs	Loetakse sisse kogu fail	SQL käskude abil, parem otsitavus ja töötlemine
Skaleeritavus	Limiteeritud, tuleb lisada uusi faile ja suurendada nende suurusi	Andmeid saab lisada, uuendada ja kustutada ilma, et mõjutatakse struktuuri
Turvalisus	Limiteeritud, andmed võivad kaduda, kui pole varundust	Sisseehitatud kasutajad ja õigused, andmed on kaitstud automaatse varundusega ja tehingulogidega
Näited	CSV, TSV	MySQL, Oracle, SQL Server andmebaasid

Failipõhine logide salvestussüsteem on oma olemuselt lihtne. Logi sündmused on salvestatud tavateksti kujul faili, mille kirjed võivad olla üksteisest eraldatud kas komadega või tabeldusmärkidega eraldatud väärtustega, ning iga uus rida algab uue kirjega. Kasutusel on veel erinevaid eraldussüsteeme. Logikirjed on salvestatud, sõltuvalt kuidas logilahendus on üles ehitatud, kas ühte või mitmesse faili korraga. Failidest andmete lugemiseks on vaja avada ja lugeda terve faili sisu. Kui logifail on väga suur, siis ei pruugi teatud programmid olla võimelised logifaile lugema. Selle probleemi üheks lahenduseks on logifailide rotatsioon, millega teatud aja jooksul vahetatakse ära fail, kuhu logi kirjutatakse ja lisatakse kuupäev koos kuu ja aastaga faili nimesse. Kui on vaja lisada rohkem seadmeid logilahendusse, siis on vajadus suurendada rotatsioonide arvu, mis tekitaks rohkem faile või suurendada failide suurusi. Kuna tegemist on lihtsa failiga, siis turvalisus sõltub esiteks logikogumisagendi ja serveri võrguühenduse turvalisusest ja teiseks, et kuidas toimub seadmetele ligipääsude loomine ja haldamine. Võib esineda ka andmete kadu, kui ei ole paigas varukoopiate loomise süsteem. Failipõhistest süsteemidest on populaarseimateks CSV ja TSV (Tab-separated values) failid.

Andmebaasipõhine logide salvestussüsteem on keerulisem, kui failipõhine salvestussüsteem. Kõigepealt tuleb paigaldada ja seadistada andmebaas koos vastavate kasutajatega ja õigustega. Siis tuleb luua vastavad tabelid, milles logikirje erinevad info osad on salvestatud erinevatesse veergudesse. Vajadusel saab ka logikirjed jaotada erinevatesse tabelitesse sõltuvalt nende logitasemest või muudest omadustest. Tabelid saab siis omavahel siduda võtmete ja indekseerimise kaudu. Andmetele saab ligi kasutades SQL (Structured Query Language) käske, mille abil on võimalik kiiresti läbi töödelda suuri andmekogumeid. Logikirjeid saab kergesti juurde lisada, kustutada ja vajadusel ka uuendada nii, et üldine andmebaasi struktuur ei muutuks. Andmebaasis peavad olema loodud kasutajad korrektsete õigustega, et kasutajad saaksid ligi soovitud andmetele. Samas saavad ka andmebaasid teha automaatset varundust ja peavad ise tehingulogisid, mis on tehtud andmebaasis. Üheks probleemiks on andmebaasi esmane ülesseadmine ja töösoleku tagamine. Tavakasutaja peab teadma andmebaaside tehnilise omadusi ja SQL käske, kui soovitakse logikirjeid töödelda. Andmebaasi mootor kasutab väga palju mälu ja seab kõrged nõuded ketta I/O-le (input/output) ehk peab võimaldama kiirelt kirjutamisi ja lugemisi. Tulemusena võib logikirjete andmebaasi jõudlus aja jooksul langeda sinnamaani, et andmebaasimootor lihtsalt ei suuda tulevaid logikirjeid tabelitesse sisestada. Andmebaas kasutab andmete sisestamiseks lukke ja kui on vaja

sisestada infot mitmetest ühendustest korraga ei suuda andmebaas seda piisavalt kiiresti töödelda. Andmebaas kirjutab kirjeid järjest, mitte paralleelselt. Kui kaob ühendus andmebaasiga võivad logikirjed kaduma minna [21]. Andmebaasi süsteemid on näiteks MySQL, Oracle ja MSSQL Server andmebaasid.

5.1 Salvestussüsteemide võrdlus ja analüüsi tulemus

Olles võrrelnud failipõhiste ja andmebaasipõhiste logide salvestussüsteeme, on mõlemal omad plussid ja miinused, millest tuleks teadlik olla. Saanud infot süsteemide omaduste kohta saab teostada analüüsi.

Failipõhist salvestussüsteemi on lihtne kasutada ja paigaldada. Faili kujul salvestamist saab teostada ilma kolmanda osapoole programme kasutamata. Suures süsteemis võivad logifailid minna väga mahukaks, aga peamine on see, et logifailid oleksid olemas, et neid saaks intsidendi tekkel kasutada. Uute seadmete lisamisel logilahendusse suurenevad olemasolevate failide mahud ja selle tulemusena on soovitatud tõsta failide rotatsiooni sagedust. Logifailidel puudub varundamine, aga seda saab kergesti teostada erinevate muude programmidega ja funktsioonidega. Varundamist saab tagada näiteks pilves hoidmisega ja kopeerimisega teisele kettale kasutades automaatskripte. Ligipääs failipõhisele salvestussüsteemile on tagatud logikollektori seadme enda kasutajaõigustega.

Andmebaasipõhine salvestussüsteem vajab väga palju tehnilisi teadmisi andmebaasidest, kuidas neid hallata ja milliseid eripärasusi võivad need tekitada. Logikirjed tuleb korrektselt tabelitesse panna nii, et nende struktuur ei muutuks. Kuigi andmeid saab kiiresti analüüsida kasutades SQL käske, peavad igal kasutajal olema teadmised, kuidas neid kasutada. Andmebaasid on peamiselt mõeldud suurte andmemahtude hoidmiseks ja logilahendused kasutavad andmebaase peamiselt sinna kirjutamiseks. Logisüsteemid võivad andmebaasi korraga niipalju infot sisse kirjutada, et serveri kõvaketta kirjutusmaht ja mälukasutus kasvavad liiga kiiresti ja logikirjeid ei jõuta enam kirjutada andmebaasi. Andmebaas peab kirjutama andmeid järjest ja ei saa kirjutada paralleelselt. Kui logilahendussüsteemis on väga palju logisid edastavaid seadmeid, mis vajavad ligipääsu andmebaasile kirjutamise eesmärgil, võivad andmebaasi lukud takistada süsteemi toimimist. Kui juhtub, et kaob ühendus andmebaasiga, võivad teatud logikirjed kaduma minna, kui ei kasutata cachimist ehk puhverdamist.

Andmebaasisüsteeme on keeruline üles seada, tuleb teada SQL keelt ja tehnilisi iseärasusi, et andmebaas korrektselt tööle saada.

Salvestussüsteemide võrdluse tulemusena on failipõhine salvestussüsteem parim valik logilahendusteks. Failisüsteemide konfigureerimine ja nende ülesseadmine ei vaja suuri tehnilisi oskusi aga sellest hoolimata tuleks teada ka nende iseärasusi, kuidas soovitud süsteemi üles seada. Samas on peamine logilahenduse ülesanne kirjete kirjutamine, mitte lugemine ja failisüsteem on selleks kõige mugavam. Logilahenduses tavaliselt ei teki anomaaliaid ja intsidente piisavalt palju lühikese aja jooksul, mis nõuaks seda, et logikirjed oleks vaja salvestada andmebaasisüsteemi. Peamine on logifailide olemasolu, salvestusperiood ja hoiustamine, et need oleksid kättesaadavad intsidentide lahendamisel.

6 Pilvesalvestusteenuste analüüs

Logimistarkvara poolt kokku korjatud logid on vaja salvestada ja sünkroonis hoida. Pilvesalvestusteenused annavad võimaluse salvestatud logisid kergemini hallata, muuta, kustutada, klastrisse lisada jne. Turul on mitu tuntud pilvesalvestusteenust nagu näiteks Dropbox, Google Drive ja Microsoft OneDrive. Nende populaarsete pilvesalvestusteenustega on selline probleem, et nad ei anna võimalust kohalikus võrgus ise oma salvestuskeskkonda paigaldada. Seadistades kohalikus võrgus oma pilveteenuse saab ise hallata ja vajadusel ka suurendada pilve. Samas ei pea muretsema teenuste lisakulude pärast, mis tekivad näiteks Google Drive'i kasutades. Selleks on välja valitud pilvesalvestusteenused, mis annavad võimaluse ise seadistada oma pilve kohalikus võrgus. Tabel 3 on esitatud pilvesalvestusteenused ja nende omadused [22] [23] [24] [25] [26] [27] [28] [29] [30].

Tabel 3. Pilvesalvestusteenuste omadused.

Pilvesalvestusteenus	**NextCloud**	**ownCloud**	**Seafile**
Klient OS	Windows, macOS, Linux, Android, iOS	Windows, macOS, Linux, Android, iOS	Windows, macOS, Linux, Android, iOS
Server OS	Linux	Linux	Linux
Failide sünkroniseerimine	Jah	Jah	Jah
Klient/serveri vahelise liikluse krüpteerimine	Jah	Jah	Jah
Kahe astmeline autentimine	Jah	Jah	Jah
Failide juurdepääsu kontroll	Jah	Jah	Jah
Kerberose tugi	Jah	Jah	Jah
Faili versioonid ja taastamine	Jah	Jah	Jah

Pilvesalvestusteenus	**NextCloud**	**ownCloud**	**Seafile**
Jagamine	Individuaalne, grupiga, avaliku lingina, salasõnaga	Individuaalne, grupiga, avaliku lingina, salasõnaga	Individuaalne, grupiga, avaliku lingina salasõnaga
Rakendused ja integratsioonid	Võrgu tekstitöötlus, meil, kalender, kontaktid jmt, 150+ rakendust	Võrgu tekstitöötlus, meil, kalender, kontaktid jmt, 200+ rakendust	Puudub
Jõudlus	Üleslaadimine 80 Mbps Allalaadimine 240 Mbps		Üleslaadimine 100 Mbps Allalaadimine 300 Mbps
Hind	Avatud lähtekoodiga, Enterprise edition alustades 100 kasutajast: Basic: 36€/kasutaja/aastas Standard: 65€/kasutaja/aastas Premium: 95.50€/kasutaja/aastas	Avatud lähtekoodiga, oma pilv: Enterprise alustades 25 kasutajast: 12€/kasutaja/kuus Standard alustades 25 kasutajast: 5€/kasutaja/kuus Teise pilv: Teams: 13€/kasutaja/kuus Single user: 15€kasutaja/kuus	Avatud lähtekoodiga, Pro edition ja Educational litsents: 3 kasutajat: tasuta 9 kasutajat: 100$ 10 kuni 249 kasutajat: PRO: 48$/kasutaja EDU: 24$/kasutaja, jne.

Nextcloud on pilvesalvestusteenus, mis lubab ise seadistada oma pilveteenuse kohalikus võrgus. Klient operatsioonisüsteemideks võivad olla Windows, macOS ja Linux seadmed, kui ka Android ja iOS nutiseadmed. Selletõttu saab Nextcloud'is olevatele failidele ligi igast populaarsemast operatsioonisüsteemist. Üheks puuduseks on see, et server, millele saab paigaldada seadistatud pilvetarkvara, peab olema Linux'i laadne operatsioonisüsteem. Nextcloud hoiab logifailid sünkroonis erinevate seadmetega ja sinna saab lisada vajadusel rohkem kettaid, et suurendada mahte, hoides suuremat hulka logisid. Logifailid saab vajadusel ära krüpteerida, et faile ei saaks kergesti lugeda ilma korrektsete õigustega. Sisse saab lülitada kaheastmelise autentimise kasutajatele ja administraatoritele. Teatud logifailidele saab lisada juurdepääsuõigused. Pilveplatvormil saab teha piiranguid lubatud failitüüpide kohta või luua reeglid, mis lubavad või keelavad failidele ligipääsu. Samuti saab sisse lülitada failide versioneerimise ja taastamise. Juhul, kui tekib vajadus vaadata failide muudatuste ajalugu või taastada kustutatud logifaile, on see võimalus olemas. Logifaile saab jagada erinevatel viisidel, kas individuaalse

inimesega, grupi administraatoritega, kellel on õigus neid vaadata või vajadusel ka avaliku lingiga, millele saab soovi korral lisada salasõna, kui on vaja jagada kellegagi väljast poolt ettevõtet. Nextcloud'i omapära on see, et tal on mitu lisafunktsiooni, nagu näiteks võrgufaili tekstitöötlus, kalender, meil, kontaktid, vestlus, videoesitamise programmid jmt. Jõudlus Nextcloud'il on keskmiselt üleslaadimiskiirusega 80 Mbps (Megabit per second) ja 240 Mbps allalaadimiskiirusega [30]. Muidugi sõltuvad kiirused ka internetiühendustest, riistvarast jmt, seega ei pruugi kiirused olla täpsed. Samuti on esile tõstetud, et suurte mahtude korral võib Nextcloud hätta jääda: failide sünkroniseerimine võib võtta terve päeva aega. Nextcloud on avatud lähtekoodiga, aga vajadusel on olemas ka Enterprise edition, mis annab rohkem valikuid ja funktsioone.

OwnCloud on väga sarnane Nextcloud'iga. OwnCloud lubab oma privaatpilve lahenduse paigaldada kohalikus võrgus. Toetatud operatsioonisüsteemid on Windows, macOS ja Linux. Nutiseadmetest saab ownCloud'i kasutada nii Android, kui ka iOS. Sarnaselt Nextcloud'iga peab pilveserver töötama ainult Linux'i-laadses serveri operatsioonisüsteemis. Pilveplatvormina pakub ownCloud sarnaseid funktsioone nagu Nextcloud: failid hoitakse sünkroonis, faile saab vajadusel krüpteerida, on olemas kahe astmeline autentimine, kaotatud või kustutatud faile saab taastada ja faile saab jagada organisatsioonist väljapoole. Owncloud pakub palju rohkem rakenduste integratsioone, kui Nextcloud. Üheks miinuseks on seemonito, et kui tegemist on väikeettevõttega ja soovitakse rohkem funktsionaalsust, peab hakkama maksma litsentsi eest rohkem, kui Nextcloud'il.

Seafile on samuti pilvesalvestusteenus, väga sarnane Nextcloud'iga, mida saab paigaldada kohalikus võrgus. Lõppklient võib töötada nii Windows, macOS ja Linux seadmetel kui ka Android ja iOS nutiseadmetel. Serveriks saab olla ainult Unix'i põhine operatsioonisüsteem. Seafile on võimeline faile sünkroonis hoidma. Logifaile saab vajadusel hoida serveris krüpteeritud kujul. Administraatoritele ja klientidele on võimalik sisse lülitada kaheastmeline autentimine. Sisse võib lülitada logifailide juurdepääsu kontrolli, mis limiteerib, missugustele failitüüpidele ja failidele on ligipääs olemas. Seafile'is on võimalik logifaile versioneerida ja vajadusel ka kustutatud logifaile taastada. Faile saab jagada individuaalselt, teatud grupile või avaliku lingiga, mis on salasõnaga kaitstud. Jõudlus on üleslaadimiskiirusega 100 Mbps ja allalaadimiskiirusega 300 Mbps [30]. Kiirused ei pruugi olla täpsed ja võivad varieeruda sõltuvalt riistvara ja tarkvara

konfiguratsioonist. Seafile on avatud lähtekoodiga, aga vajadusel on olemas ka Enterprise edition, mis annab rohkem valikuid ja funktsioone.

6.1 Pilvesalvestusteenuste võrdlus ja analüüsi tulemus

Olles võrrelnud pilvesalvestusteenuseid saab teostada analüüsi. Logilahenduseks on vaja lihtsat pilvesalvestusteenust, mis lubaks logifaile paremini hallata. Kasutades leitud infot pilvesalvestusteenuste kohta on teostatud analüüs.

Nextcloud teeb oma olemuselt sama, mida mitmed avalikud pilvesalvestusteenused juba teevad. Ta hoiab failid sünkroonis, logifaile saab hoida serveris krüpteeritud kujul, on olemas mitu turvafunktsiooni ja platvorm lubab jagada faile mitmel viisil teiste administraatoritega või klientidega. Vajadusel saab faile ka taastada ja versioneerimise abiga vaadata üle muudatusi. Üheks suureks erinevuseks võrreldes Seafile'iga on Nextcloud'il olemas funktsioonid mitme integratsiooni rakendusega, mis lubavad pilves ülal pidada meili, kalendrit, kontakte, teostada videokõnesid. Logilahenduseks ei ole vaja neid erinevaid funktsioone ja need võivad logilahenduse keerulisemaks teha, mis omakorda võib Nextcloud'i haldamise administraatori jaoks komplitseeritumaks muuta. Samuti on väljatoodud jõudluse probleemid võrreldes Seafile'iga [30]. Failide üleslaadimine võib võtta rohkem aega ja logilahenduse korrektseks toimimiseks ei ole see soovitatud. Nextcloud on avatud lähtekoodiga, kui ei taheta lisafunktsioone.

OwnCloud on väga sarnane võrreldes Nextcloud'iga. OwnCloud pakub sarnaseid funktsionaalsusi ja lahendusi. Üheks eeliseks on see, et ownCloud pakub rohkem integratsioone teiste rakendustega, kui Nextcloud. Miinuseks on see, et kui soovitakse rohkem funktsionaalsust ja lisafunktsioone, siis tuleb hakata lisateenuste eest maksma. Võrreldes Nextcloud'i hindadega on ownCloud'i hind kasutaja kohta palju kallim. Sellest tulenevalt on hinda arvesse võttes odavam kasutada Nextcloud'i, kuigi sellel pilveteenusel on vähem integratsioone, kui ownCloud'il. Logilahendust ei ole vaja integreerida erinevate teiste teenustega, tähtis on see, et logifailid on olemas ja kättesaadavad nii kiiresti, kui võimalik.

Seafile teeb pilvesalvestusteenusega peaaegu kõike seda sama, mida teeb ka Nextcloud. Üheks peamiseks erinevuseks on see, et Seafile'il puuduvad erinevad integratsioonid ja funktsioonid teiste programmidega. Seafile on mõeldud, kui failide sünkroonis hoidmise

ja jagamisteenus. Samuti on jõudlus võrreldes Nextcloud'iga palju parem. Seafile hoiab suuri logifaile kiiremini sünkroonis ja ei võta selleks kaua aega. Samuti on ka Seafile avatud lähtekoodiga, mille eest ei ole vaja tasuda lisakulusid. Kui soovitakse lisada pilveteenusele lisafunktsioone, tuleb selle eest hakata maksma litsentsikulusid. Seafile`i saab kergesti paigaldada automaatskriptiga. Kuna tegemist on serveriga, mida haldavad tavaliselt administraatorid, mitte kliendid ise, siis ei pea server olema seadistatud kohalikus ettevõttes vaid võib vajadusel töötada ise ettevõtte väliselt kuskil teises pilves. Uusi arvuteid saab ühendada pilvega kasutades Seafile desktop drive klienti, kuhu sisselogides on juba logifailidele ligipääs tagatud.

Pilvesalvestusteenuste võrdluse ja analüüsi tulemusena on Seafile hetkel kõige parem valik. Seafile on palju kiirem, kui Nextcloud ja tal puuduvad erinevad integratsioonid ja lisad, mis tulevad kaasa Nextcloud'iga. Logilahendus ei vaja programme, nagu meil, kontaktid ja kalender, et saaks efektiivsemalt logisid kokku koguda. Kasutades automaatskripti saab Seafile'i kiiresti paigaldada. Seafile teeb seda, mida ta on mõeldud tegema väga kiiresti ja sellepärast sobib see logilahenduseks kõige paremini.

7 Monitoorimisprogrammide analüüs

Logilahenduse logid on kokku korjatud ja salvestatud kohalikus võrgus pilvesalvestusteenusesse. Vaja on seadistada veel monitoorimisprogrammid, et saaks logide kogumist kiiremini ja efektiivsemalt vaadelda ning vajadusel konfigureerida hoiatusi, kui tekib anomaaliaid logide kogumisega. Tabel 4 on esitatud võimalikud monitoorimisprogrammid ja nende omadused [31] [32] [33].

Tabel 4. Monitoorimisprogrammide omadused.

Monitoorimisprogramm	**Grafana**	**Prometheus**
Toetatud OS	Windows, macOS, Linux	Windows, macOS, Linux
Teenuse tüüp	Graafika, joonised andmetest	Andmete kogumine, monitooring
Pistikprogrammid, integratsioonid	150+	Jah
Hoiatused	Jah	Jah
Avalik graafika	Jah	Ei
Andmete visualiseerimine	Jah	Jah
Märkused	Jah	Ei
Hind	Avatud lähtekoodiga, Cloud Free Cloud Pro 29$/kuu ja kasutus Cloud Advanced 299$/kuu ja kasutus	Avatud lähtekoodiga

Grafana on erinevate arvutite meetrika või muu mõõdikute programm, mis saadud andmete tulemusena loob automaatselt graafikat ja jooniseid. Sõltuvalt vajadusele saavad administraatorid luua ja muuta töölaudasid, et saaks parema ülevaate teenusest või süsteemist. Grafanaga saab luua igasugustest andmetest graafikat: hoone energiatarbimisest, veebilehe jõudlusest, sissetulekutest, jpm. Kui on olemas andmed, vahet pole milliselt erialalt või valdkonnast, saab Grafanat seadistada tegema sellest graafikat ja jooniseid. Kasutades rohkem kui 150 pistikprogrammi saab Grafanat ühendada igasuguse vajaliku süsteemi või teenusega. Samas saab seadistada automaatsed

hoiatused, kui mingi näidik läheb üle soovitud parameetri. Andmetele saab lisada juurde märkused, kuhu saab kirjutada, miks tekkis selline anomaalia. Vajadusel saab visualiseeritud andmeid jagada avalikult teiste kasutajatega või inimestega. Grafana on avatud lähtekoodiga ja selle saab vajadusel ise oma võrgus paigaldada. Pakutakse ka tasuta pilveteenust, kui ei soovi ise teenust ja platvormi hallata. Kui on vajadust suurendada pilves olevaid mahte peab nende eest maksma.

Prometheus on monitoorimise programm, mis kogub kokku ja salvestab andmeid ja infot. Kasutades mitme integratsiooniga olevaid andmeeksportijaid või pistikprogramme saab Prometheus kokku koguda andmeid erinevatest allikatest. Andmed kogutakse kokku ja salvestatakse Prometheuse endale kohandatud salvestussüsteemi. Lisaks saab anomaaliate tekkel luua hoiatused, mis annavad administraatoritele teada, kui mõõdetud meetrika on läinud üle arvestatud piiri. Kui on vaja, saab ka andmeid visualiseerida graafiliselt sisse ehitatud brauseriga. Prometheus on avatud lähtekoodiga.

7.1 Monitoorimisprogrammide võrdlus ja analüüsi tulemus

Olles võrrelnud monitoorimisprogramme saab teostada analüüsi. Logilahenduseks on vaja logifaile pidevalt jälgida, et anomaaliate tekkel saaks kiiresti lahenduse leida. Monitoorimisprogrammide kohta leitud info osas on teostatud analüüs.

Grafana on peamiselt graafika ja jooniste loomise ja nende andmete täitmise programm. Sõltuvalt, kuidas on töölauad seadistatud näitab Grafana, kus võivad olla anomaaliad. Saab seadistada automaatsed hoiatused, et kui tekib intsident või probleem, antakse administraatoritele automaatselt teada, milles probleem võib olla. Saab kiiresti vaadelda ja uurida logifaile, kus võis tekkiv probleem alguse saada. Andmetele saab lisada juurde ka märkused, kui tekib anomaalia teatud meetrikas. Grafana ise andmeid kahjuks ei kogu, aga on võimas tööriist nende visualiseerimiseks. Avatud lähtekoodiga Grafana saab paigaldada enda võrgus minimeerides kulusid.

Prometheus on andmete ja info monitoorimisprorgamm. Kogutakse kokku vajalikke meetrikat ja salvestatakse Prometheuse enda loodud salvestussüsteemi. Vajadusel saab luua ka automaatsed hoiatused. Sarnaselt Grafanaga saab ka Prometheus andmeid vajadusel visualiseerida. Programm on avatud lähtekoodiga ja ei vaja eraldi litsentsi ostmist.

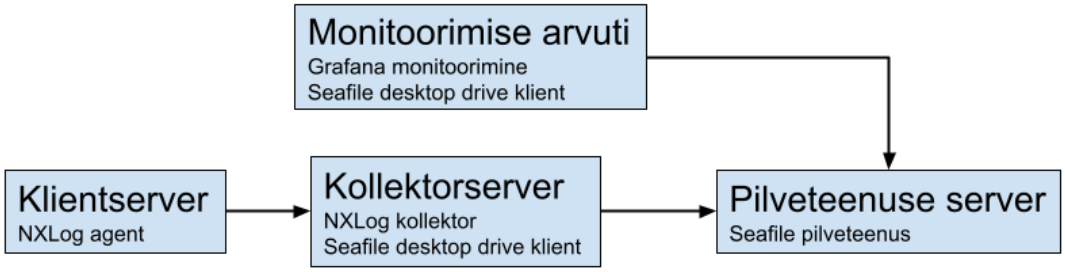
Monitoorimisprogrammide võrdluse ja analüüsi tulemusena täidab Grafana kõiki nõudeid, mis on vaja logilahenduse monitoorimiseks. Grafana on võimas tööriist, mis visualiseerib andmed ja info mugavamale kujule. Sellest tulenevalt on logilahenduseks parim variant kasutada Grafanat andmete ja meetrikute visualiseerimiseks ja pistikprogramme meetrikute kogumiseks.

8 Logilahenduse paigaldamine testkeskkonnas

Testkeskkonnaks on järgnev :

- üks Windows Server (2019 Standard) kollektori rollis
- üks Windows Server (2019 Standard) kliendi rollis
- üks Ubuntu Server (22.04) pilveteenuse rakendusserveri rollis
- üks Windows 10 Pro (22H2) monitoorimise rollis

Testkeskkonda kirjeldab ka loodud diagramm Joonis 2:



Joonis 2. Lõputöö testkeskkonna diagramm.

8.1 Pilveteenuse serveri konfiguratsioon

Seafile'i paigaldamiseks Ubuntu serveris kasutame loodud skripti [34] [35]. Skript paigaldab automaatselt Seafile'i. Kui on uuem versioon Seafile'ist, siis asendada käskudes versiooni number. Seafile bash käsu viimase versiooni number tuleks võtta Seafile allalaadimislingilt [36]. Ubuntu terminalis tuleks käivitada järgmisi käske root õigustes, mis on kujutatud Joonis 3:

```
cd /root
wget --no-check-certificate https://raw.githubusercontent.com/haiwen/seafile-server-installer/master/seafile-10.0_ubuntu
bash seafile-10.0_ubuntu 10.0.1
```

Joonis 3. Seafile serveri konfiguratsiooni käsud.

Skript paneb automaatselt paika Seafile'i Ubuntu serveris. Samuti paigaldatakse vajalikud programmid, sõltuvused ja seaded. Nendeks on puhverserver, Seahub ja Seafile WebDAV koos veebiserveri lüüsi liidestega, MariaDB, Memcached, Seafile automaatne

startimine ja tulemüüri seaded. Kui skript on lõpetanud, näidatakse Seafile administraatori kasutajanime ja salasõna, need tuleks salvestada, et saaks ligi Seafile serveri administraatori liidesele. Pärast skripti käivitamist on soovitatud skript ära kustutada kasutades käsku „rm seafile-10.0_ubuntu“. Seafile administraator leheküljele saab ligi minnes brauseriga „http://127.0.0.1” või Seafile serveri ip aadressiga. Sisse saab logida, kasutades eelnevalt saadud Seafile administraatori kasutajat ja salasõna. Pärast sisselogimist tuleb luua uus Library ja nimetada see näiteks “Log files”. Üheks probleemiks on see, et kollektor serveris kustutatud logifailid jäävad Seafile’i serverisse alles ja seetõttu on Seafile serveris aegunud logifailid.

8.2 Kollektorserveri konfiguratsioon

Seafile desktop drive klient tuleb paigaldada kollektorserverisse [36] [37]. Pärast paigaldamist logida oma administraatori kasutajaga sisse, mille info asub peatükis 8.1 ja serveri IP aadressiks panna server, kus töötab Seafile. Pärast sisselogimist ja Seafile serverist info saamist peaks tekkima „SeaDrive“ ikoon Windows file explorer’isse, kuhu saab hakata lisama logifaile.

NXLog Community editioni paigaldamiseks on laetud alla Windowsi NXLog paigaldus pakett [29]. Seejärel paigaldati programm administraatori õigustes vajaminevasse serverisse või arvutisse. Kasutati agendipõhist logide kogumist, ehk klientmasinas töötab NXLog agent, mis saadab kohalikud logid konfigureeritud logide kogumisserverisse. NXLog konfigureerimise fail on nxlog.conf, mille vaikimisi failiteekond on „C:\Program Files\nxlog\conf\nxlog.conf“.

Selleks, et NXLog server saaks vastu võtta ühendusi tuleb konfiguratsiooni faili lisada Joonis 4 olev konfiguratsioon:

```
<Input tcp>
    Module  im_tcp
    Host    0.0.0.0
    Port    1514
</Input>

define LOGPATH C:\Users\Administrator\seadrive_root\admin\My Libraries\Log
files\\nxlog

<Output out>
    Module       om_file
    File         "%LOGPATH%.txt"
    CreateDir    TRUE

    <Schedule>
        When @daily
        Exec    rotate_to("%LOGPATH%" + strftime(now(), '_%Y-%m-%d') +
'.txt');
             Exec    file_remove("%LOGPATH%" + strftime(now() - 259200, '_%Y-
%m-%d') + '.txt');
    </Schedule>
</Output>

<Route 1>
    Path        tcp => out
</Route>
```

Joonis 4. Kollektorserveri konfiguratsioon.

Kasutatud on TCP moodulit, sest siis ei teki probleeme sõnumite kaotamisega. Testkeskkonnas kogutakse logikirjed Seafile pilvekausta „Log files“ faili nimega „nxlog“. Iga päeva tagant lisatakse failile aasta, kuu ja kuupäev kujul „nxlog_%Y-%m-%d“ ja luuakse uus fail „nxlog“ ja hakatakse logima sinna faili. Iga päeva järel kontrollitakse, kas on olemas logid, mis on vanemad kui kolm päeva ja eemaldatakse vastavad logid. Konfiguratsioonis on ajaks kasutatud sekundeid ja administraator peab soovitud aja välja arvutama. Defineeritud on ka „LOGPATH“ keskkonna muutuja, et kui vajadusel soovitatakse muuta logifaili nime või asukohta, saab seda kiiresti teha. Kui on vaja testida konfiguratsiooni faili süntaksit tuleks käivitada käsku:

„C:\Program Files\nxlog\nxlog.exe“ -v

Soovitatud on NXLog teenus taaskäivitada, selleks tuleb minna Windowsi puhul Services.msc programmi ja üles leida „nxlog service“ ja see taaskäivitada. Siis tuleks avada NXLog süsteemi-logimise fail, mille vaikimisi faili teekond on

„C:\Program Files\nxlog\data\nxlog.log“

ja veenduda konfiguratsiooni töösolekus. Kollektorserveril on vaja lubada sissetulev TCP port 1514, selleks on vaja Windowsi tulemüüri sissetulevatesse ühenduste reeglitesse lisada TCP port 1514 ning määrata selle reegli nimeks „Nxlog log input“ või sarnane.

8.3 Kliendiagendi konfiguratsioon

Klientarvuti, millest on soov saata logisid kollektorserverisse tuleks samamoodi paigaldada nagu NXLog Community edition [38]. Paigaldamine käib täpselt samamoodi kui serveril. NXLog agendi standardkonfiguratsioon on kujutatud Joonis 5:

```
<Extension json>
    Module    xm_json
</Extension>

<Input eventlog>
    Module    im_msvistalog
    Exec      to_json();
</Input>

<Output tcp>
    Module    om_tcp
    Host      10.110.66.101
    Port      1514s
</Output>

<Route 1>
    Path        eventlog => tcp
</Route>
```

Joonis 5. Klientagendi konfiguratsioon.

NXLog kogub kohalikus masinas kokku Windows Event logid. Logi kirjed muudetakse JSON formaati ja saadetakse 10.110.66.101:1514 IP:port kombinatsiooniga asuvale serverile.

8.4 Monitoorimisarvuti konfiguratsioon

Seafile desktop drive klient tuleb paigaldada kollektorserverisse [36] [37]. Pärast paigaldamist logida oma administraatori kasutajaga sisse, mille info asub peatükis 8.1 ja serveri IP aadressiks panna server, kus töötab Seafile. Pärast sisselogimist ja Seafile serverist info saamist peaks tekkima tekkima „SeaDrive“ ikoon Windows file explorer’isse, kust saab ligi logifailidele.

Grafana paigaldamiseks Windowsi monitoorimise arvutisse kasutame alla laetud paigaldamispaketti [39] [40]. Vali kõige uuem versioon, OSS (Open-source software) väljaanne ja Windows paigalduspakett. Seejärel paigalda programm administraatori õigustes. Grafana käivitamiseks käivitada „grafana.exe“, mis asub „bin“ kaustas. Peale paigaldamist on veebibrauseris vaja minna Grafana pordile, mis on vaikimisi „http://localhost:3000/“. Sisse saab logida kasutajanimega „admin“ ja salasõnaga „admin“, salasõna on soovitatud ära muuta peale sisenemist.

Et Grafana saaks koguda meetrikat, tuleb peale panna pistikprogramm Telegraf [41]. Programm kogub ja saadab meetrikat vajaminevasse programmi. Laadida alla Windows kokkupakitud binaarfail. Seejärel luua kaust „C:\Program Files\InfluxData\telegraf“ ja allalaetud fail pakkida kaustas lahti. Luua uus Telegraf konfiguratsiooni fail „telegraflogtail.conf“ ja sisestada konfiguratsioon, mis on kujutatud Joonis 6:

```
[agent]
  interval = “30s”
  flush_interval = “30s”

[[inputs.filecount]]
  directories = [“C:/Users/martinerik/seadrive_root/admin/My Libraries/Log
files”]

[[outputs.http]]
  url = “http://localhost:3000/api/live/push/logtail”
  data_format = “influx”
  username = 'admin'
  password = '<salasõna>' #muuda vastavalt oma seadistatud paroolile
```

Joonis 6. Telegrafi konfiguratsioon.

Selle seadistusega saadab Telegraf infot iga 30 sekundi tagant Grafanale konfiguratsioonis oleva kausta kohta, sealhulgas kui palju faile seal on, kui suur on kaust ja kõige uuema ja vanema logifaili loomisaeg. Kui on vaja testida konfiguratsiooni, tuleks käivitada „telegraf“ kaustas Powershell ja käivitada käsk:

„.\telegraf.exe ` --config C:\"Program Files"\InfluxData\telegraf\telegraflogtail.conf --test“

või: „.\telegraf.exe --config telegraflogtail.conf --once.“

Telegraf Windows teenuse paigaldamiseks käivitada käsk:

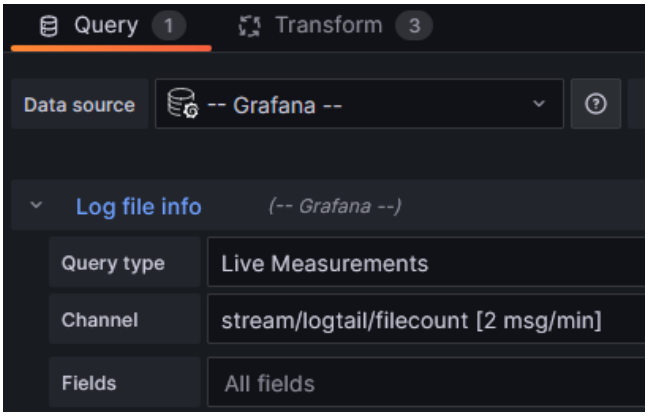
„.\telegraf.exe --service install ` --config "C:\ProgramFiles\InfluxData\telegraf\telegraflogtail.conf"“.

Telegrafi käivitamiseks kasutada käsku: „.\telegraf.exe --service start“.

Kui on vaja kontrollida teenuslogisid siis neid saab vaadata järgmises failis:

„C:\Program Files\GrafanaLabs\grafana\data\log\grafana.log“

Grafana seadistamiseks, et näidata kaustas olevate failide infot tuleb enne Grafanasse sisse logida. Järgmisena tuleb luua uus Dashboard, mille andmete allikas on Grafana ja asukoht, kust infot saab on „stream/logtail/filecount“. Joonis 7 näitab Grafana andmete allika seadistust.



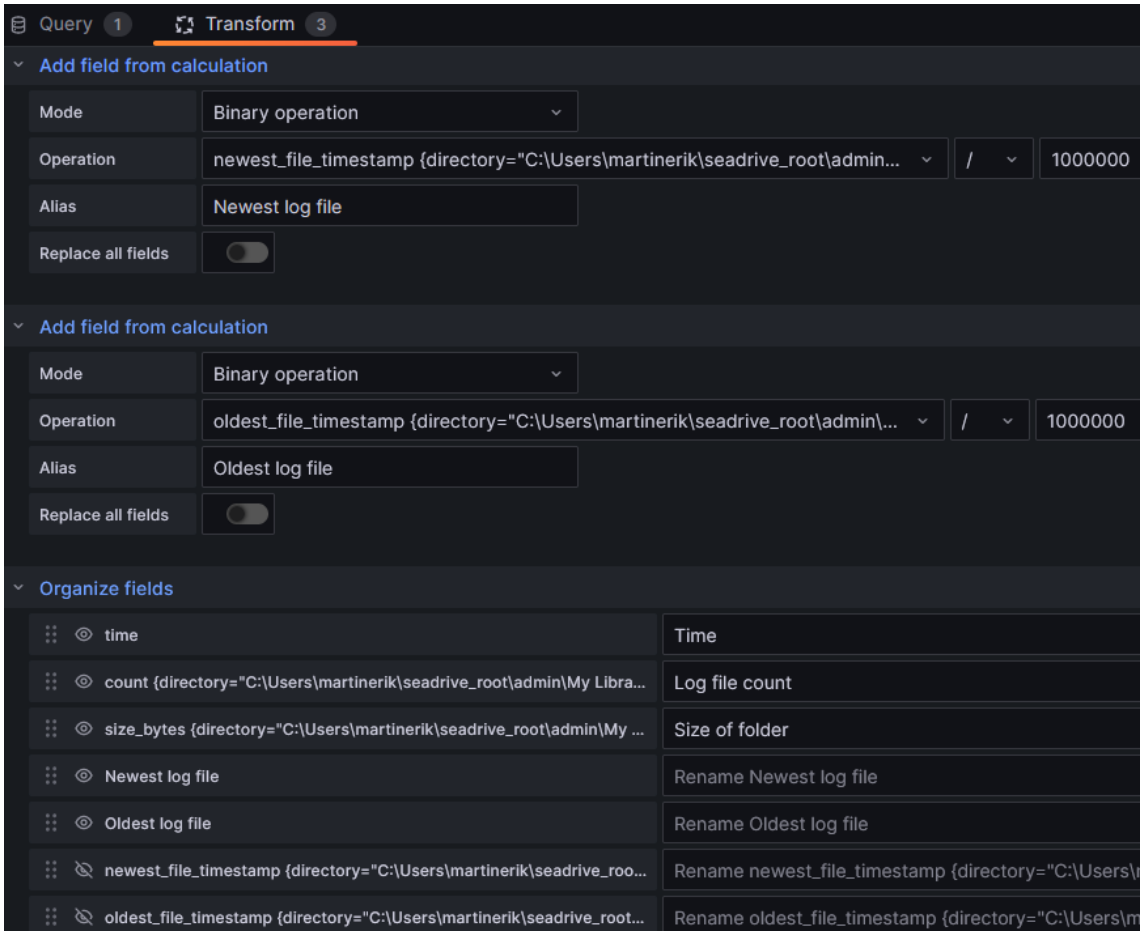
Joonis 7. Grafana andmete allika seadistus.

Pärast seda peaks esimesed andmed Grafanasse jõudma, aga andmed ei ole soovitud kujul ja tuleks teisendada õigele kujule. Selleks tuleb minna menüüsse „Transform“ ja lisada uus „Field from calculation“ milleks on „Binary operation“. Operatsiooniks valida „newest_file_timestamp“, kasutada jagamist ja numbriks panna 1000000. Kuna timestamp on Unix-i laadne, mis on nanosekundites, aga Grafana loeb millisekundites, seega tuleb see info ära teisendada. Aliaseks panna „Newest log file“. Kasutades sama meetodit tuleb luua veel üks „Field from calculation“, aga nüüd võtta operatsiooniks „oldest_file_timestamp“ ja aliaseks „Oldest log file“. Nüüd tuleks väljad panna õigesse järjekorda, parandada nimed ja peita ära vanad väljad. Selleks valida „Organize fields“, mille järjekord ja uued nimed on järgmised:

1. time, nimega: Time
2. count, nimega: Log file count

3. size_bytes, nimega: Size of folder
4. Newest log file
5. Oldest log file

Peita ära järgmised väljad: „newest_file_timestamp“ ja „oldest_file_timestamp“. Tegevusi näitab ka Joonis 8.

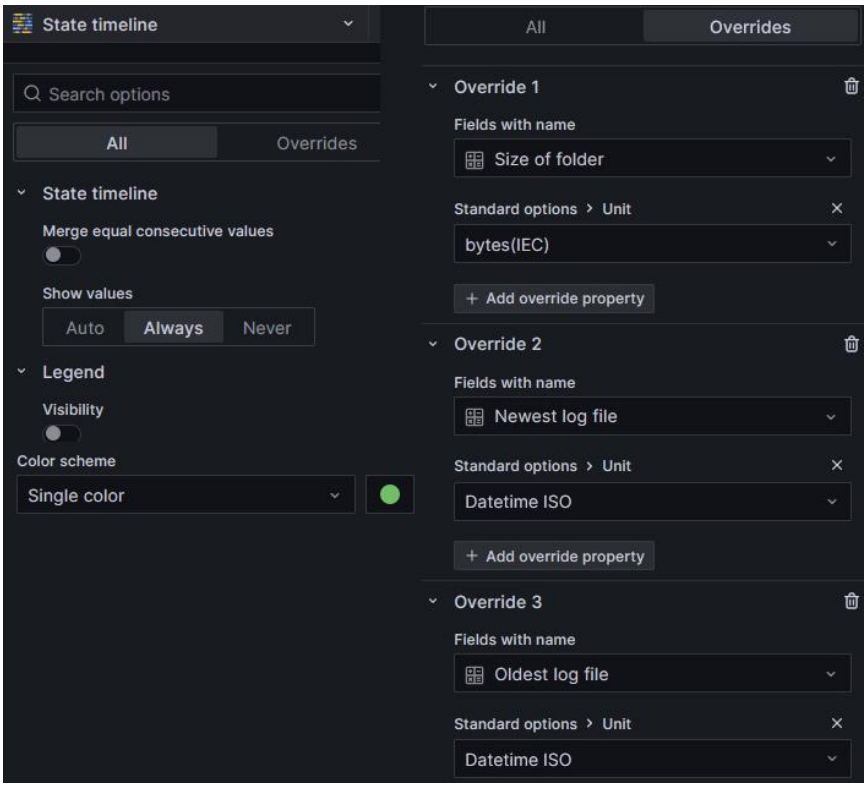


Joonis 8. Grafana andmete viimine õigele kujule.

Grafana paremal paneelil valida „State timeline“, lülitada välja „Merge equal consecutive values“ ja alati näidata väärtusi. Legendid lülitada välja ja „Standard optionite“ alt „Color scheme’iks“ valida „Single color“. Lisada 3 „override’i“ nimedega:

- Size of folder, andmetüübiks: bytes(IEC)
- Newest log file, andmetüübiks: Datetime ISO
- Oldest log file, andmetüübiks: Datetime ISO

Joonis 9 näitab Grafana lõppseadistusi.



Joonis 9. Grafana lõppseadistused.

Graafika peaks nüüd õigesti näitama infot iga 30 sekundi tagant ja nüüd saab konfiguratsiooni salvestada.

9 Kokkuvõte

Lõputöö põhieesmärgiks oli luua Telia keskmise suurusega ärikliendile töötav logilahendus testkeskkonnas, arvestades Telia poolseid ootuseid, nõudeid ja soove. Teostatud analüüside ja testimise tulemusena loodi kliendile ja Telia administraatoritele juhend, mille abil saab teenusepakkuja (nt Telia) või ettevõte ise seadistada logilahenduse. Testkeskkonnas paigaldatud logilahendus on alus, mida saab konkreetse ettevõtte jaoks vastavalt vajadusele edasi seadistada.

Töö käigus kirjeldati alustuseks Telia tüüpkliendi vajadused. Määrati nõuded logilahendusele järgides Telia tüüpkliendi kirjeldust ja Telia oma soove. Seejärel teostati analüüs ja võrreldi erinevaid programme, mis võiksid sobida logilahenduseks.

Kõigepealt analüüsiti Telia poolt väljapakutud logimistarkvarasid, mis koguvad kokku logikirjeid ja valiti välja logimistarkvara NXLog. Edasi analüüsiti, kas on parem kasutada failipõhist või andmebaasipõhist logide salvestamist ja valiti failipõhine logide salvestamine.

Järgnevalt analüüsiti erinevaid pilvesalvestusteenuseid ja valiti välja Seafile. Lõpuks analüüsiti monitoorimisprogramme ja valiti välja Grafana. Pärast erinevate programmide selekteerimist hakati paigaldama ja seadistama programme Telia testkeskkonnas. Seadistamise tulemusena loodi juhend, mida saab kasutada IT keskkonnas logilahenduse rakendamiseks

Töö käigus esinesid probleemid logifailide rotatsiooni ja kustutamisega, probleemi olemust kirjeldavad peatükid 3.1 ja 3.2. Logide monitoorimine ja analüüs on lahti kirjutatud peatükis 3.3.

Lõputöö ühe eesmärgina loodi töötav logilahenduse prototüüp, mis ei eelda logiklastri olemasolu. Loodud logilahendus on kergesti hallatav, vajadusel skaleeritav ja sellega ei kaasne litsentsikulusid. Kuna kasutatud programmidel puuduvad litsentsitasud, säästavad kuludelt Telia ja tema kliendid. Muudatused tööjaamas ja serveris on minimaalsed. Logilahenduses saab määrata salvestusaja logidele. Lahendust peaks saama pakkuda ja

paigaldada kõikidele Telia väikestele ja keskmistele klientidele, kelle vajadused see peaks täitma. Töö tulemusena loodi juhend logilahenduse paigaldamiseks IT keskkonnas.

Lõputöö skoobiks ei olnud see, et milliseid konkreetseid logifaile kogutakse ja kui kaua neid logitüüpe salvestatakse. Samas ei olnud skoobis ka logide sündmuste veatase. Ei testitud salvestamist odavamale kettapinnale (S3 protokolliga). Kuna testkeskkonnas oli ainult üks klientmasin, ei sooritatud koormusteste ega rakendatud klientide logide loogilist eraldamist. Ei testitud logilahenduse skaleeritavust, kuigi skaleeritavuse võimekus on olemas vastavalt tehnilisele dokumentatsioonile. Ei loodud ka kasutajaliidest, et majasiseselt tagada logide ligipääsu formaat.

Töös loodud logilahendus ei ole lõplik, sest tegemist on ainult logilahenduse prototüübiga, kuid esialgne töötav lahendus on nüüd olemas. Sellest tulenevalt tuleks Telial järgnevalt arvestada kliendi soovidega ja vajadustega, ning seadistada logilahendus vastavalt kliendi ootustele. Antud lõputöös on loodud juhend peatükis 8, mis annab võimaluse administraatoritel paika panna logilahenduse alus ja sealt ise, vastavalt kliendi vajadustele, luua soovitud seadistused.

Kasutatud kirjandus

[1] Gartner, Inc., „Best Infrastructure Monitoring Tools Reviews 2023 | Gartner Peer Insights,“ Gartner, Inc., 2023. [Võrgumaterjal]. Available: https://www.gartner.com/reviews/market/infrastructure-monitoring-tools. [Kasutatud 1 detsember 2023].

[2] Microsoft, „Monitor Event Log | Microsoft Learn,“ Microsoft, 23 märts 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/system-center/orchestrator/standard-activities/monitor-event-log?view=sc-orch-2022. [Kasutatud 16 aprill 2023].

[3] Microsoft, „Event Log | Microsoft Learn,“ Microsoft, 13 detsember 2019. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd349798(v=ws.10). [Kasutatud 16 aprill 2023].

[4] B. Hymer, „Log Monitoring, which workstation logs to monitor and why. - Microsoft Platform Management - Blogs - Quest Community,“ Quest Software, 19 juuli 2018. [Võrgumaterjal]. Available: https://www.quest.com/community/blogs/b/microsoft-platform-management/posts/why-and-how-to-monitor-your-workstations. [Kasutatud 20 aprill 2023].

[5] StatCounter, „Desktop Windows Version Market Share Worldwide | Statcounter Global Stats,“ Statcounter, märts 2023. [Võrgumaterjal]. Available: https://gs.statcounter.com/windows-version-market-share/desktop/worldwide/#monthly-202204-202303-bar. [Kasutatud 16 aprill 2023].

[6] MW Team, „What Is Log Monitoring? A Detailed Guide (Updated) | Middleware,“ Middleware Lab, Inc., 20 juuni 2023. [Võrgumaterjal]. Available: https://middleware.io/blog/what-is-log-monitoring/. [Kasutatud 7 september 2023].

[7] SentinelOne, „Log Monitoring: A Crash Course in the What, Why, and How | Scalyr,“ SentinelOne, 18 august 2020. [Võrgumaterjal]. Available: https://www.sentinelone.com/blog/log-monitoring/. [Kasutatud 7 september 2023].

[8] A. Sharif, „What Is Log Rotation? - CrowdStrike,“ CrowdStrike, 21 detsember 2022. [Võrgumaterjal]. Available: https://www.crowdstrike.com/cybersecurity-101/observability/log-rotation/. [Kasutatud 28 juuli 2023].

[9] LogicMonitor Inc., „What Is Log Retention? | LogicMonitor,“ LogicMonitor Inc., [Võrgumaterjal]. Available: https://www.logicmonitor.com/blog/what-is-log-retention. [Kasutatud 28 juuli 2023].

[10] A. Isaiah, „Log Levels Explained and How to Use Them | Better Stack Community,“ Better Stack, Inc., 4 august 2023. [Võrgumaterjal]. Available:

https://betterstack.com/community/guides/logging/log-levels-explained/. [Kasutatud 7 september 2023].

[11] Microsoft, „Use Windows Event Forwarding to help with intrusion detection (Windows 10) | Microsoft Learn,“ Microsoft, 9 märts 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection. [Kasutatud 16 aprill 2023].

[12] Microsoft, „Installation and configuration for Windows Remote Management - Win32 apps | Microsoft Learn,“ Microsoft, 9 veebruar 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management. [Kasutatud 14 november 2023].

[13] Microsoft, „Best practice of configuring EventLog forwarding performance - Windows Server | Microsoft Learn,“ Microsoft, 2 veebruar 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/troubleshoot/windows-server/admin-development/configure-eventlog-forwarding-performance. [Kasutatud 16 aprill 2023].

[14] TechiBee, „How to configure windows event forwarding in Windows 7/2008 – Part-1,“ TechiBee, 5 aprill 2012. [Võrgumaterjal]. Available: https://techibee.com/windows-2008/how-to-configure-windows-event-forwarding-in-windows-72008-part-1/1570. [Kasutatud 15 november 2023].

[15] NXLog, „NXLog documentation collections :: NXLog Documentation,“ NXLog, 29 märts 2023. [Võrgumaterjal]. Available: https://docs.nxlog.co/userguide/documentation.html. [Kasutatud 16 aprill 2023].

[16] Adiscon, „About WinSyslog — WinSyslog 17.1 documentation,“ Adiscon, 2020. [Võrgumaterjal]. Available: https://www.winsyslog.com/files/manual/current/index.winsyslog.html. [Kasutatud 16 aprill 2023].

[17] WinSyslog, „Edition Comparison - WinSyslog,“ WinSyslog, 2023. [Võrgumaterjal]. Available: https://www.winsyslog.com/product-info/edition-comparison/. [Kasutatud 16 aprill 2023].

[18] WinSyslog, „Order Now - WinSyslog,“ WinSyslog, 2023. [Võrgumaterjal]. Available: https://www.winsyslog.com/order-and-pricing/order-now/. [Kasutatud 16 aprill 2023].

[19] NXLog, „Supported platforms :: NXLog Documentation,“ NXLog, 2023. [Võrgumaterjal]. Available: https://docs.nxlog.co/userguide/deploy/platforms.html. [Kasutatud 16 aprill 2023].

[20] DatabaseTown, „Difference Between Flat File VS Database - DatabaseTown,“ DatabaseTown, 2023. [Võrgumaterjal]. Available: https://databasetown.com/difference-between-flat-file-vs-database/. [Kasutatud 9 august 2023].

[21] M. Waszlavik, „Why you shouldn’t log into db. From time to time, I see systems… | by Márton Waszlavik | Medium,“ Medium, 11 september 2018. [Võrgumaterjal]. Available: https://medium.com/@marton.waszlavik/why-you-shouldnt-log-into-db-e700c2cb0c8c. [Kasutatud 9 august 2023].

[22] NextCloud GmbH, „Nextcloud features that put you in control,“ Nextcloud GmbH, 2023. [Võrgumaterjal]. Available: https://nextcloud.com/features/. [Kasutatud 22 august 2023].

[23] Nextcloud GmbH, „Nextcloud Enterprise pricing,“ Nextcloud GmbH, 2023. [Võrgumaterjal]. Available: https://nextcloud.com/pricing/. [Kasutatud 21 september 2023].

[24] ownCloud GmbH, „ownCloud - share files and folders, easy and secure,“ ownCloud GmbH, 2023. [Võrgumaterjal]. Available: https://owncloud.com/. [Kasutatud 31 oktoober 2023].

[25] ownCloud GmbH, „48 Features make ownCloud the exciting sovereign workspace,“ ownCloud GmbH, 2023. [Võrgumaterjal]. Available: https://owncloud.com/features/. [Kasutatud 31 oktoober 2023].

[26] Seafile Ltd., „Seafile - Open Source File Sync and Share Software,“ Seafile Ltd., 2023. [Võrgumaterjal]. Available: https://www.seafile.com/en/features/. [Kasutatud 22 august 2023].

[27] Seafile Ltd., „Private Server - Seafile,“ Seafile Ltd., 2023. [Võrgumaterjal]. Available: https://www.seafile.com/en/product/private_server/. [Kasutatud 21 september 2023].

[28] A. KS, „Tag Cloud Storage Comparison: Nextcloud vs. OwnCloud vs. Seafile - Hongkiat,“ Hongkiat, 6 aprill 2023. [Võrgumaterjal]. Available: https://www.hongkiat.com/blog/self-hosted-cloud-storage-nextcloud-owncloud-seafile/. [Kasutatud 22 august 2023].

[29] N. Congleton, „Nextcloud vs. OwnCloud vs Seafile: The Best Self-Hosted File-Syncing Service - Make Tech Easier,“ Uqnic Network Pte Ltd., 5 detsember 2018. [Võrgumaterjal]. Available: https://www.maketecheasier.com/nextcloud-vs-owncloud-vs-seafile/. [Kasutatud 22 august 2023].

[30] Flare Compare, „Seafile vs Nextcloud | Flare Compare,“ Flare Compare, 18 märts 2022. [Võrgumaterjal]. Available: https://flarecompare.com/Cloud%20Storage/Seafile%20vs%20Nextcloud/. [Kasutatud 22 august 2023].

[31] Grafana Labs, „Grafana | Query, visualize, alerting observability platform,“ Grafana Labs, 2023. [Võrgumaterjal]. Available: https://grafana.com/grafana/. [Kasutatud 21 september 2023].

[32] Grafana Labs, „Grafana Pricing | Free, Pro, Advanced, Enterprise,“ Grafana Labs, 2023. [Võrgumaterjal]. Available: https://grafana.com/pricing/. [Kasutatud 21 september 2023].

[33] Prometheus, „Prometheus - Monitoring system & time series database,“ Prometheus Authors, 2023. [Võrgumaterjal]. Available: https://prometheus.io/. [Kasutatud 21 september 2023].

[34] A. Jackson, „GitHub - haiwen/seafile-server-installer: Script collection to setup production-ready Seafile server installations with HTTPS,“ GitHub, Inc., 2023. [Võrgumaterjal]. Available: https://github.com/haiwen/seafile-server-installer. [Kasutatud 31 august 2023].

[35] Seafile Ltd., „Seafile Admin Manual,“ Seafile Ltd., [Võrgumaterjal]. Available: https://manual.seafile.com/. [Kasutatud 31 august 2023].

[36] Seafile Ltd., „Download - Seafile,“ Seafile Ltd., 2023. [Võrgumaterjal]. Available: https://www.seafile.com/en/download/. [Kasutatud 31 august 2023].

[37] Seafile Ltd., „Seafile User Manual,“ Seafile Ltd., [Võrgumaterjal]. Available: https://help.seafile.com/. [Kasutatud 31 august 2023].

[38] NXLog, „Download - Nxlog Community Edition,“ NXLog, 2023. [Võrgumaterjal]. Available: https://nxlog.co/downloads/nxlog-ce#nxlog-community-edition. [Kasutatud 20 aprill 2023].

[39] Grafana Labs, „Download Grafana | Grafana Labs,“ Grafana Labs, 19 september 2023. [Võrgumaterjal]. Available: https://grafana.com/grafana/download. [Kasutatud 28 september 2023].

[40] Grafana Labs, „Grafana documentation | Grafana documentation,“ Grafana Labs, 2023. [Võrgumaterjal]. Available: https://grafana.com/docs/grafana/latest/. [Kasutatud 28 september 2023].

[41] InfluxData Inc., „Telegraf | InfluxData,“ InfluxData Inc., 2023. [Võrgumaterjal]. Available: https://www.influxdata.com/time-series-platform/telegraf/. [Kasutatud 28 september 2023].

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]
Mina, Martin Erik Pille

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Keskse logilahenduse teenuse loomine Telia ärikliendile“ , mille juhendaja on Siim Vene
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

04.01.2024

1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.