TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Dmitri Kiriljuk 176110IDAR

VÕRGU MONITOORINGU- JA VARUNDUSSÜSTEEMI JUURUTAMINE CABELNETWORK AS-I NÄITEL

Diplomitöö

Juhendaja: Žan Kotenjev
Bakalaureusekraad

Kaasjuhendaja: Siim Vene
MSc

Tallinn 2020

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: Dmitri Kiriljuk

30.04.2020

Annotatsioon

Käesoleva diplomitöö raames selgitatakse, kuidas saab juurutada võrgu monitooringu- ja varundussüsteemi ettevõttes CabelNetwork AS.

Töö esimeses pooles analüüsitakse lahendusi. Seejärel valitakse sobiv lahendus ja kirjeldatakse vajalikud monitooringu parameetrid, et tagada võrgu stabiilne töö.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 37 leheküljel, 6 peatükki, 14 joonist, 4 tabelit.

Abstract

IMPLEMENTATION OF A NETWORK MONITORING AND BACKUP SYSTEM ON THE EXAMPLE OF CABELNETWORK AS

This diploma thesis explains how the network monitoring and backup system can be implemented in CabelNetwork AS.

The first half of the work analyses the solutions. The appropriate solution is then selected, and the necessary monitoring parameters are described to ensure stable operation of the network.

The dissertation is written in Estonian and contains text on 37 pages, 6 chapters, 14 figures, 4 tables.

Lühendite ja mõistete sõnastik

NMS	Network Monitoring System
MPLS	Multiprotocol Label Switching
BGP	Border Gateway Protocol
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention System
SNMP	Simple Network Management Protocol
SSH	Secure Shell / Turvatekst
CDP	Cisco Discovery Protocol
FDP	Foundry Discovery Protocol
LLDP	Link Layer Discovery Protocol
OSPF	Open Shortest Path First
OID	Object identifier
MIB	Management Information Base
NOC	Network operations Center / Võrgu juhtimiskeskus

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Tänapäeva ettevõtte infrastruktuur on keeruline mehhanism, mis koosneb erinevatest süsteemidest ja võrkudest. Selleks, et tagada nende hästi koordineeritud ja efektiivne töö, on vaja süsteeme koos integreeritud tööriistadega.

CabelNetwork AS on ettevõte, mis pakub oma klientidele Interneti ühendust. Selle ettevõtte võrk kasvab kiiresti ja selleks, et hakkama saada tänapäeva olukorras, kus on palju kitsaskohti võrgus (võrguseadme olek, kas kliendiühendused on töökorras), siis on vaja monitoorida ja tuvastada kiiresti rikked. Seda saab teha ainult siis, kui on teada, millised seadmed on võrgus ja milline on nende staatus.

Käesoleva diplomitöö raames selgitatakse, kuidas saab juurutada võrgu monitooringu- ja varundussüsteemi ettevõttes CabelNetwork AS. Töö esimeses pooles analüüsitakse lahendusi. Seejärel valitakse sobiv lahendus ja kirjeldatakse vajalikud monitooringu parameetrid, et tagada võrgu stabiilne töö.

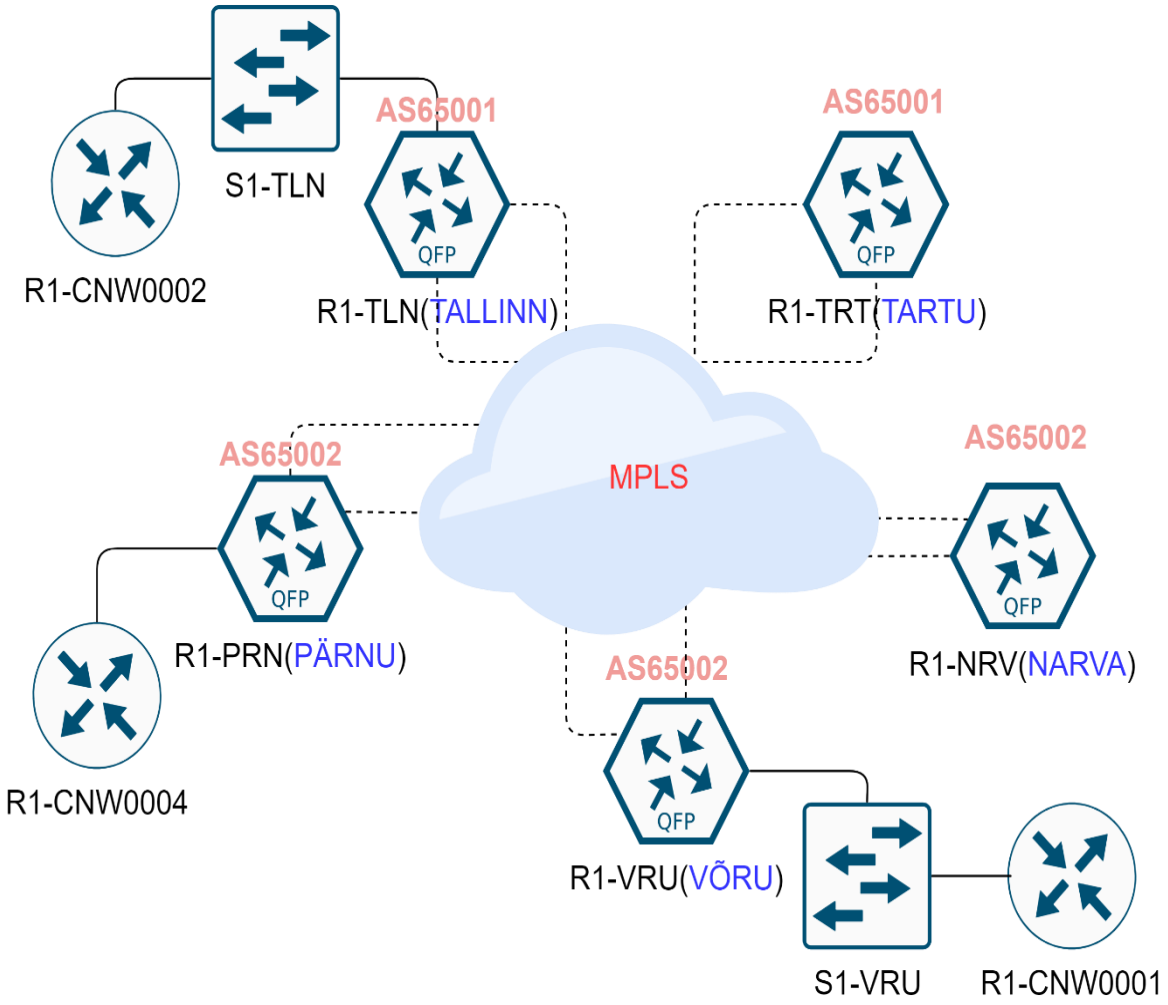
"Kohaliku võrgu diagnostika" on infovõrgu staatuse (pideva) analüüsimise protsess. Võrguseadmete häire korral registreeritakse rike, määratakse selle koht ja tüüp. Rikketeade edastatakse, võrguseade lülitatakse välja ja asendatakse uuega.

Võrguadministraator peab meeles pidama, et kasutajate tagasiside määrab võrgu kvaliteedi. Kõik muud kriteeriumid, näiteks andmeedastusvigade arv, võrguressursside ülekoormus, seadmete jõudlus jne, on sekundaarsed. Ülekoormatud võrk ei ole hea võrk „Hea võrk“ on see võrk, mille kasutajad ei märka, kuidas see töötab.

2 Käsitletav probleem

CabelNetwork AS pakub Interneti-juurdepääsu teenuseid järgmistes linnades: Tallinn, Tartu, Pärnu, Narva, Võru. CabelNetwork AS-i ettevõtlusvõrgu peamine eripära on MPLS-tehnoloogia, mis omakorda ühendab kõik sidusettevõtte linnad üheks suureks MPLS-domeeniks. Ettevõtte võrk hõlmab selliste ettevõtete seadmeid nagu Cisco Systems, Inc. ja Juniper Networks.

Peamine kanal, mis ühendab sise-MPLS domeeni internetiühendusega, asub Tallinnas. Joonisel 1 on CabelNetwork AS ettevõtte võrguinfrastruktuur.



Joonis 1 CabelNetwork AS ettevõtte võrguinfrastruktuuri skeem

Võrgu juhtimiskeskus (NOC) lahendab antud ettevõttes järgmisi ülesandeid:

- Interneti-ühenduse pakkumise sissehelistamis- ja erikanalite kaudu tehniline ja tehnoloogiline korraldus
- Interneti-ühenduse tehniline ja tehnoloogiline korraldus
- kliendiseadmete paigutamine klientide saidile
- eraettevõtete korporatiivsete võrkude juurutamine ja haldamine

Tegevuse ja teenuste pakkumise mahu suurenemisel tekkis probleem rikete ja võrgu korralduse nõrkade külgede tuvastamisel, see tähendab, et ülesandeks on leida lahendus, mis võimaldab ennustada võrgusektsioonide väljavahetamise või moderniseerimise vajadust enne, kui rikked mõjutavad kliendi võrgu seadmete tööd. Selliste probleemide lahendamiseks on vaja leida monitooringusüsteem.

Samuti on üheks ülesandeks leida lahendus, mis oleks võimeline salvestama muudatusi kõigi ettevõtte võrgus asuvate võrgu seadme konfiguratsioonidest. See lahendus peaks seadme konfiguratsiooniversioonid salvestama, kui seadme konfiguratsioon on vale, aitab versioonikontroll kiiresti tagasi konfiguratsiooni eelmise versiooni juurde, mis töötas seadmes probleemideta. Konfiguratsiooni varukoopia aitab ettevõttel rikke korral katki läinud seadme asendada uuega, kuna viimane konfiguratsioon on varundussüsteemis salvestatud. Selle probleemi lahendamiseks on vaja leida varundussüsteem.

Võrgu rikete tuvastamise süsteem peab vastama järgmistele tingimustele:

- Seadme staatuse monitoorimine
- BGP-seansi staatuse monitoorimine
- OSPF-seansi staatuse monitoorimine
- Kliendiportide staatuse jälgimine vastavalt SLA lepingu tüübile (SLA1 - reageerimisaeg on tööpäeva jooksul ; SLA2 – reageerimisaeg on 4 tunni jooksul; SLA3 – reageerimisaeg on 1 tunni jooksul)

- Pidev andmete kogumine pordi koormuse kohta ja teavitamine pordi 90% koormusest
- Võrguhalduskeskuse teavitamine probleemist e-kirjaga
- Varundamissüsteemi juurutamine seadme konfigureerimiseks, võrgu infrastruktuuri vigase võrguseadme asendamiseks

2.1 Lähtetingimused süsteemide valimiseks

Probleemi edasise sõnastamise ja teemavaldkonna uurimise käigus täpsustati lähtetingimusi, võttes arvesse majanduslikke ja ajalisi investeeringuid.

Monitooringusüsteem peab vastama järgmistele nõuetele:

- Vabavaraline
- Kõik kasutatavad tarkvaralised komponendid peavad olema avatud lähtekoodiga
- Süsteemi skaleeritavus ehk süsteem suudab monitoorida nii 10 seadet kui ka 3500 seadet
- Standardsed diagnostikaaruande raportid (pordi staatused, kanali koormusgraafikud jne)
- Kõigi kasutatud tarkvaratoodete üksikasjaliku dokumentatsiooni kättesaadavus
- Võime toetada erinevate tootjate võrgu seadmeid ehk monitoorib erinevate tootjate seadmeid
- SNMP jälgimine

Varundussüsteem peab vastama järgmistele nõuetele:

- Vabavaraline
- GIT tugi – (versioonihaldus ja konfiguratsiooni salvestamine GIT repositooriumisse)

- SSH tugi – (võrguseadme konfiguratsiooni varundamine SSH kaudu)
- Varundussüsteemi integreerimine monitooringusüsteemiga

Monitooringusüsteem ja varundussüsteem peavad olema vabavaralised, kuna ettevõttel ei ole vahendeid eelarves, et osta tasulist tarkvara. Süsteemid peavad olema avatud lähtekoodiga, et võimalusel ise arendada funktsionaalsust juurde. Süsteemi skaleeritavus on vajalik, kuna ettevõtte võrk kasvab iga päev ning süsteem peab olema suuteline kasvava võrguga kaasas käima. Põhifunktsioonid, mida peab monitooringusüsteem oskama, on jälgida võrgukanali koormust, selle alusel saab koostada raporteid ja leida kitsaskohad. Süsteemid peavad toetama erinevate tootjate võrguseadmeid (põhiliselt Cisco ja Juniper, kuid ei välistata ka teiste tootjate seadmeid).

Monitoorimine peab toimima läbi SNMP protokolli, kuid peab olema võimalik tuvastada võrguseadmeid ping-i abil. Samas ping ei ole nii informatiivne kui SNMP. SNMP võimaldab saada sellist infot nagu võrguseadme nimi, seeria number, pordi kirjeldus, võrgukanali koormuse andmed ja palju muud.

Varundussüsteem peab toetama versioonihaldust ja konfiguratsiooni salvestamist GIT repositooriumisse.

GIT on süsteemikonfiguratsiooni muudatuse salvestamise süsteem, mis salvestab praeguse ja varasema konfiguratsiooniversiooni, GIT pakub ka võimalust leida võrguseadme konfiguratsiooni varasematest aegadest või alternatiivseid versioone.

Varundussüsteem ja monitooringusüsteem peavad olema omavahel integreeritud, et kasutada varundussüsteemi funktsionaalsust monitooringusüsteemis. Väga mugav on monitooringusüsteemis jälgida võrguseadmete konfiguratsioone.

2.2 Mis on monitooringusüsteemid?

Võrgu monitooringusüsteemidel (Network Monitoring System, NMS) on oluline roll erinevate sissetungimiste tuvastamisel (Intrusion Detection System, IDS) või sissetungi ennetamisel (Intrusion Prevention System, IPS). Viimased tuvastavad rünnet ja hoiavad ära volitamata kasutajate potentsiaalselt ohtliku tegevuse. NMS võimaldab kindlaks teha, kui efektiivselt toimib võrk tavapäraste toimingute ajal, aga ei vastuta turvalisuse eest.

Monitoorida saab peaaegu kõiki pakutavaid juhtmega ja juhtmevabu kohtvõrke ning virtuaalset privaatvõrku. Monitooring võib hõlmata mitmesuguseid op-süsteeme ja paljude funktsioonidega seadmeid – VoIP seadmed, serverid, ruuteritest kommutaatoriteni. NMS aitab tuvastada volitamata tegevust võrgus, määrata monitooritavaid parameetreid ja väljastavad raporteid, mis võimaldavad lahendada paljusid erinevaid ülesandeid, hoiatada ohtude eest ja tagada võrgu toimingute läbipaistvus.

2.3 Mis on võrgu varundussüsteemid?

Varundamine on stabiilse infrastruktuuri oluline komponent, kuna probleemi ilmnemisel, näiteks seadme füüsiline riknemine või tänapäeval väga levinud seadme loata krüpteerimine, on võimalik süsteemi või võrguseadme konfiguratsiooni taastada salvestatud varukoopiatest.

Kuna võrguseadmed on harva ühelt müüjalt ja kogu võrgu jaoks on sageli võimatu leida ühte seadistamismeetodit, on võrguseadmete varundamine administraatorite jaoks keeruline.

Võrguseadmete konfiguratsioonide varundamise automatiseerimiseks kasutavad insenerid tihti versioonikontrollisüsteeme. See lähenemisviis võimaldab mitte ainult konfiguratsiooni ajakohastatud koopiat, vaid ka kiiret seadmetes tehtud muudatuste leidmist, mis võivad põhjustada võrgu valesti töötamist.

3 Analüüs

Analüüs on üks olulisemaid osi monitooringu- ja varundussüsteemi valimisel. Praegu on monitooringusüsteemide turg erinevate lahenduste osas väga rikkalik. Seal on nii tasulisi kui ka tasuta lahendusi erineva funktsionaalsusega.

Kuna CableNetwork AS pakub ainult võrguteenust (klient, juurdepääsu ja juurvõrgu seadmeid), on monitooringusüsteemi valimisel peamine aspekt võrgu jälgimine.

Selles peatükis käsitletakse kolme monitooringusüsteemi, mille valik põhineb Google'i otsingul päringu “Free and Open Source Network Monitoring Tools” alusel.

Allpool on toodud lingid allikatele, kus artiklite autorite sõnul on valitud parimad võrgu monitooringusüsteemid:

https://www.dnsstuff.com/open-source-network-monitoring-tools

https://www.ittsystems.com/best-open-source-network-monitoring-tools/

https://www.networkstraining.com/best-open-source-free-network-monitoring-tools/

Otsingu põhjal tuvastati kolm monitooringusüsteemi tootjat – Nagios Core, Zabbix ja LibreNMS.

Samuti tehti turuanalüüs seadme konfiguratsiooni varusüsteemide kohta ning Google'i otsingu põhjal tuvastati kolm pakkujat: Unimus, Oxidized ja Rancid.

Lisaks oli uuritud lõputööd Eesti Infotehnoloogia Kolledži vilistlased, mis eelistasid oma töös selliseid süsteeme nagu Nagios või Zabbix. Sel juhul on vaja leida MPLS-tehnoloogiat kasutava võrgu monitoorimiseks optimaalne lahendus, BGP ja OSPF seansside monitoorimine. Uuritud töödes ei olnud kirjeldatud ka võrguseadmete konfiguratsioonide salvestamise protsessi, selle töö eesmärk on leida terviklik lahendus CableNetwork AS ettevõtte probleemide lahendamiseks.

Monitooringusüsteem peab tagama järgmised funktsionaalsused:

- Veebipõhine kasutajaliides
- Võrguseadme automaattuvastus
- Kohandatav hoiatusteade ja teavitused
- Vabavaraline

Varundussüsteem peab tagama järgmised funktsionaalsused:

- Veebipõhine kasutajaliides
- Võrguseadmesse sisselogimine SSH kaudu
- Võrguseadme konfiguratsiooni salvestamine GIT repositooriumis
- Vabavaraline

3.1 Monitooringusüsteemid

3.1.1 Nagios Core

Nagios Core on populaarne avatud lähtekoodiga arvutisüsteemide ja võrkude monitooringu tarkvara. See jälgib määratud seadmeid ja teenuseid, teavitades omanikku, kui asjad lähevad halvaks ja/või kui need muutuvad taas paremaks. [1]

Nagios Core oli algselt mõeldud kasutamiseks Linuxis, kuid töötab hästi ka teiste Unixi variantide korral. [1]

Nagios Core on tasuta tarkvara, mille litsents vastab GNU General Public License versiooni 2 tingimustele, mille on avaldanud Free Software Foundation. [1]

Nagios Core omadused:

- Võimalus jälgida ühe tööriistaga rakendusi, teenuseid, op-süsteeme, võrguprotokolle, süsteemimõõdikuid ja infrastruktuuri komponente

- Võimsad skriptiliidesed API-s võimaldavad ettevõtte siseseid ja kohandatud rakendusi, teenuseid ja süsteeme hõlpsalt jälgida
- Raportid tagavad, et SLA-sid täidetakse
- Raportid sisaldavad teateid häirete, teatiste, katkestuste ja häirete reageerimise kohta
- Kolmanda osapoole lisad laiendavad aruandlusvõimalusi
- Avatud lähtekoodiga tarkvara
- Välja antud GPL-i litsentsi alusel [2]

3.1.2 LibreNMS

LibreNMS on avatud lähtekoodiga serverite ja võrguriistvara automaatse tuvastamisega monitooringu tarkvara. See toetab laias valikus võrguriistvara (näiteks Cisco, Juniper, Brocade, Foundry, HP) ja op-süsteeme, sh Linux ja Windows. LibreNMS on kogukonnapõhine võrgumonitooringu vahend, mis on välja antud GPLv3 tingimustega. [3]

LibreNMS põhineb AMP (Apache, MySQL ja PHP) / EMP (Nginx, MySQL ja PHP) pinul ja kogub monitooringu mõõdikuid SNMP protokolli kaudu. [4]

LibreNMSi omadused:

- Automaattuvastus: avastab võrguseadmed automaatselt, kasutades CDP, FDP, LLDP, OSPF, BGP, SNMP ja ARP
- Kohandatav hoiatusteade: väga paindlik hoiatussüsteem, teated e-postiga, irc, slack ja muud
- API Access: täielik API oma paigaldusandmete haldamiseks, graafikute kuvamiseks
- Automaatsed värskendused

- iPhone App: saadaval iPhone'i rakendus, mis pakub põhifunktsioone võrgu oleku jälgimiseks
- Android App: saadaval Android rakendus, mis pakub põhifunktsioone võrgu oleku jälgimiseks [3]

3.1.3 Zabbix

Zabbix on avatud lähtekoodiga monitooringutarkvara erinevate IT-komponentide jaoks, sh võrgud, serverid, virtuaalmasinad (VM) ja pilveteenused. Zabbix pakub monitooringu mõõdikuid, sh võrgu kasutamist, protsessori koormust ja kettaruumi täituvuse olekut.

Tarkvara jälgib operatsioonisüsteemides Linux, Hewlett Packard Unixis (HP-UX), Mac OS X, Solaris ja teistes op-süsteemides (OSes); Windowsis jälgimine on aga võimalik ainult agentide kaudu. [5]

Zabbix kasutab andmete salvestamiseks MySQL, MariaDB, PostgreSQL, SQLite, Oracle või IBM DB2 andmebaase. Zabbix on kirjutatud C-keeles ja veebirakendus PHP-ga. [5]

Zabbix pakub mitmeid monitooringu võimalusi:

- Saab kontrollida standardteenuste (nt SMTP või HTTP) kättesaadavust
- Zabbixi agendi saab installida ka UNIX-sse ja Windows-i, et jälgida statistikat nagu protsessori koormus, võrgu kasutamine, kettaruum jne
- Alternatiivina agendi installimisele sisaldab Zabbix võimalust monitoorida SNMP, TCP ja ICMP protokollide, samuti SSH, Telneti ja kohandatud parameetrite kasutamise kaudu [5]

3.1.4 Monitooringusüsteemide funktsionaalsuse võrdlemine

Monitooringusüsteemi valiku paremaks mõistmiseks uuriti monitooringusüsteemi funktsionaalsusi ja selle põhjal koostati võrdlustabel.

Tabelis 1 on välja toodud kolme erineva monitooringusüsteemi funktsionaalsuse tabel.

Tabel 1 Monitooringusüsteemide funktsionaalsuse võrdlemine

Kategooria	**Nagios Core**	**LibreNMS**	**Zabbix**
Veebiliides	+	+	+
Töökeskkond ja kasutajaliides	Funktsionaalne töökeskkond. Nagios Core töökeskkond pakub põhiteavet, näiteks seadmete staatus, kuid see ei paku samal tasemel selgust ja informatsiooni süstematiseeritust kui Zabbix ja LibreNMS.	Funktsionaalne töökeskkond. LibreNMSi töökeskkonda saab kohandada ja see pakub geograafilist kaarti koos seadme asukohtadega.	Funktsionaalne töökeskkond. Zabbixi töökeskkondadel saab kuvada võrguseadme oleku, hoiatused, pordi graafikud ja jne.
Süsteemi seadistamine	Konfiguratsioon tekstifailidena	Veebipõhine	Veebipõhine
Visualiseerimine (Võrguseadme pordi liiklus graafikuid)	Nagios Core vaikimisi graafikuid ei paku.	LibreNMS-il on oma graafikud.	Zabbixil on oma graafikud.
Võrguseadme automaattuvastus	Ei ole võimalik.	LibreNMS toetab vaikimisi automaattuvastust järgmiste protokollide kaudu - BGP, LLDP, CDP.	Ei ole võimalik.
Protokollitugi	Pakub tuge HTTP, FTP, SMTP, SNMP, POP3, SSH jah MySQL jaoks.	Pakub tuge HTTP, FTP, SMTP, SNMP, POP3, SSH jah MySQL jaoks.	Pakub tuge HTTP, FTP, SMTP, SNMP, POP3, SSH jah MySQL jaoks.
Hoiatused ja teatised	+	+	+
Mallid	Ei ole, aga internetis saadaval kasutajate poolt valmis kirjutatud reeglistikud.	LibreNMS pakub portide malle monitooringuks, BGP jälgimiseks, OSPF-i lingi staatuse monitooringuks.	Zabbix pakub malle FTP, HTTP, HTTPS, IMAP, LDAP, MySQL, NNTP, SMTP, SSH, POP.

Kategooria	Nagios Core	LibreNMS	Zabbix
Pistikprogrammid	Nagios Core pakub laia valikut täiendavaid pistikprogramme.	LibreNMS toetab suurt hulka Nagiose pistikprogramme.	Ei ole.
Kogukond	Suur kogukond	Suur kogukond	Suur kogukond
Hind	Vabavaraline	Vabavaraline	Vabavaraline

Tabelist 1 näeme, et kõigil võrdluseks valitud süsteemidel on veebiliides, LibreNMS-il ja Zabbixil on funktsionaalne töökeskond, kus kuvatakse erinevaid graafikuid, paneel probleemide teatisega ja kaart seadme täpse asukohaga.

Süsteemi konfiguratsioonid erinevad üksteisest, Nagios Core konfigureeritakse tekstifaili kaudu, kui LibreNMS ja Zabbix on konfigureeritavad veebiliidese kaudu.

Nagios Core ei anna kahjuks võimalust karbist väljas tootega graafikut joonistada, kuid see on võimalik kolmanda osapoole pistikprogrammide paigaldamisel.

Erinevalt teistest võrreldavatest rakendustest suudab LibreNMS võrguprotokollide, näiteks BGP, LLDP, CDP abil teisi võrguseadmeid automaatselt tuvastada.

Kõik seadmed toetavad hoiatuste saatmist e-posti teel ning LibreNMS ja Zabbix on tootja poolt sisseehitatud hoiatuste mallid kiirete teavitussätete jaoks.

Üks olulisi kriteeriume, millele kõik süsteemid vastavad, on, et toode on vabavaraline.

3.2 Varundussüsteemid

3.2.1 Unimus

Arendanud Tomas Kirnak - Mikrotik USA treener. Süsteem kirjutati Tomase vajaduste alusel tema 1500 RouterOS-i võrgu seadme konfiguratsiooni salvestamise jaoks.

Unimus’t saab installida Windows ja Unix OS.

Unimus toetab 58 võrguseadme tootjat, konfiguratsiooni salvestamine toimib GIT repositooriumisse. [6]

3.2.2 Oxidized

Sarnane eelmisele süsteemile. Vähem meeldiv veebiliides, mis ei sega Oxidized põhifunktsiooni. Oxidized toetab 91 võrguseadme tootjat, sealhulgas Cisco, Juniper, Mikrotik, D-Link, Cumulus Linux, pfSense.

Oxidized lõid kaks arendajat: Saku Ytti ja Samer Abdel-Hafez alternatiivina RANCID-ile. Selge eelis RANCIDi ees on selle kasutajasõbralik veebiliides. [7]

Tarkvara, mis kasutab Oxidized kogutud konfiguratsioone:

- LibreNMS [7]

3.2.3 RANCID

RANCID (Really Awesome New Cisco confIg Differ) on võrguhaldusrakendus ja varundussüsteem. RANCIDi kasutatakse marsruuteritega ühenduse loomiseks ja mõne käsu saatmiseks.

RANCID teeb seda väga lihtsa protsessi abil, mille kokkuvõte on järgmine:

- igasse seadmesse sisselogimine
- salvestatava teabe saamiseks käivituvad mitmesugused käsud
- salvestakse väljund
- saadab kõik erinevused eelmisest kollektsioonist e-posti aadressile
- viib need muudatused GIT repositooriumisse [8]

Tarkvara, mis kasutab RANCID-i kogutud konfiguratsioone:

- LibreNMS [9]
- Observium [10]
- OpenNMS [11]

3.2.4 Varundussüsteemide funktsionaalsuse võrdlemine

Süsteemi valiku paremaks mõistmiseks uuriti võimaliku monitooringusüsteemi funktsionaalsust ja selle põhjal koostati võrdlustabel.

Tabelis 2 on välja toodud kolme erineva varundussüsteemi funktsionaalsus.

Tabel 2 Varundussüsteemide funktsionaalsuse võrdlemine

Kategooria	**Oxidized**	**Rancid**	**Unimus**
Veebiliides	Vaikimisi lihtne ja kaasaegne veebiliides	Lihtne ja vana veebiliides	Vaikimisi lihtne ja kaasaegne veebiliides
Seadistamine	Oxidized kasutab YAMLi-põhist konfiguratsioonifaili	Teksti konfiguratsioonifail	Konfigureerimine veebiliidese kaudu
Saadab kõik erinevused e-posti teel	Toetab	Toetab	Toetab
SSH tugi	+	+	+
GIT tugi	+	+	+
API	API tugi vaikimisi	API ei toetata	API tugi vaikimisi
Avatud lähtekoodiga projekt	+	+	-
Hind	Vabavaraline	Vabavaraline	3400 €/1000 seadet

Tabeli 2 põhjal on kõigil valitud süsteemidel veebiliides, mis vastab esitatud nõudmisele.

Kolme süsteemi konfiguratsioon on erinev, Oxidized kasutab sätete jaoks tänapäevast Yamli märgistuskeelt, Rancid salvestab sätted tekstifaili, Unimus konfigureeritakse veebiliidese kaudu.

Konfiguratsioon kogutakse ja salvestatakse GIT repositooriumisse SSH-protokolli abil. Konfiguratsioonimuudatused saadetakse e-postiga.

Unimuse üks, kuid põhiline puudus on see, et toode on tasuline. Kuna funktsionaalsuse osas pole palju sarnaseid süsteeme nagu Oxidized või Rancid, valiti Unimus turu ja erinevate süsteemide funktsionaalsuse uurimiseks, aga kuna see on tasuline, siis Unimust edasi ei võrrelda.

4 Analüüsi tulemus

4.1 Monitooringusüsteemi analüüs

Monitooringusüsteemi ja varundussüsteemi valimiseks on vaja teha SWOT-analüüs eelnevalt saadud andmete põhjal süsteemide funktsionaalsuse kohta.

Süsteemi valimise fookus on võrgu monitoorimine. Seetõttu on SWOT-analüüs suunatud võrgu monitooringusüsteemi valimisele.

Tabelis 3 on toodud valitud süsteemide tugevused, nõrkused, võimalused ja ohud.

Tabel 3 Monitooringusüsteemide SWOT analüüs

SWOT-analüüs	**LibreNMS**	**Nagios Core**	**Zabbix**
Tugevused	1. Tarkvara on rohkem suunatud Interneti-teenuse pakkujatele 2. Uus ja huvitav projekt 3. Suur funktsionaalsus (andmete kogumine seadmetest ja koormusgraafikud, automattuvastus, pistikprogrammid jne) 4. Kaardirakendus on sisse ehitatud 5. Igal kuul liitub projektiga palju uusi arendajaid.	1. Laialdane funktsionaalsus (sobib serverite ja võrguseadmete jälgimiseks) 2. Stabiilne rakendus, pikaajaline projekt (olemas kaua turul). Stabiilne sissetulek lisafunktsioonide ja juurutuse tellimisega äriettevõtetelt	1. Suudab töödelda suuremaid mahtusid (st kordades rohkem monitooritavaid seadmeid kui teistel võrreldavatel) 2. Parem skaleeritavus

SWOT-analüüs	**LibreNMS**	**Nagios Core**	**Zabbix**
Nõrkused	1. Suur arendajate liikuvus 2. Võimetus testida oma toodet (alfa-beeta) 3. Võimalik et kaotab turgu, kuna on väga spetsiifiline toode (ainult NMS) 4. Testkogukonna väiksus 5. Võimalikud vead süsteemis	1. Sisseehitatud graafikute puudumine 2. Nagios Core põhifookus on serverite monitooringu süsteem ning Nagios Core oskab hästi monitoorida serverite teenuseid nagu veebi-server (Apache2) või MySQL andmebaas jne. 3. Võrguseadme automaattuvastuse puudumine 4. Ainult skriptipõhine, mis tähendab, et vajab head IT-spetsialisti või on teenuse juurutamine kulukas 5. Pistikprogrammide jaoks vaja rohkem dokumentatsiooni 6. Töökeskkond võiks olla kasutajasõbralikum	1. Võimalikud vead süsteemis, foorumite uurimisel on tuvastatud, et süsteemis ei toimi hästi võrgu monitoorimine, ei näita õiget võrgugraafikut 2. Tarkvara on rohkem serverite jaoks (nt kui teeb kõike, siis ei tee mitte midagi väga hästi - puudub spetsialiseerumine ja fookus on mitme erineva funktsiooni peal) 3. Väikeettevõtte jaoks liiga mahukas ja juurutamine keeruline

SWOT-analüüs	**LibreNMS**	**Nagios Core**	**Zabbix**
Võimalused	1. Uute võimaluste ja funktsioonide kasutuselevõtt on lihtne 2. Kuna on spetsiifiline ja uus, siis on turu kasv keskmisest suurem 3. Ei pea keskenduma ajaloolise peale	1. Pilve kolimine ehk tõstab oma funktsioonid pilve ja kogu monitooringu protsess toimib niimoodi, et serverid suhtlevad pilvega 2. Fookuse muutmine, mis annab võimaluse suurendada kasutajate arvu	1. Zabbix võib pakkuda kliendile modulaarsust, näiteks kui on vaja võrgu monitooringu süsteemi, siis vaja paigaldada ainult „Zabbix Network“; kui on vaja monitooringusüsteemi serverite jaoks, siis „Zabix for Servers“
Ohud	1. Uudsus kaob ja kasutajad pettuvad ning selle tagajärjel loobuvad 2. Üleminek tasuta tootelt tasulisele 3. Peatatakse tootearendus 4. Finantseerimise lõpetamine	1. Kasutajate vähenemine - paljud otsivad spetsiifilist tarkvara (nagu LibreNMS) ja kolivad 2. Funktsionaalsuse laiendamine viivitusega (pikk arendamise periood) 3. Kasutajad kolivad toote peale, mis on seadistuse mõistes paremini arusaadav ega nõua spetsiifilisi teadmisi 4. Nagios XI on tasuline versioon, võimalik, et kaob Nagios Core	1. Kasutajate vähenemine - paljud otsivad spetsiifilist tarkvara 2. Kasutajad kolivad toote peale, mis on seadistuse osas paremini arusaadav ega nõua lisateadmisi 3. Uute funktsioonide lisamine muudab keskkonna kasutuskõlbmatuks või keeruliseks jne 4. Kaob süsteemi skaleeritavus

Pärast monitooringusüsteemide SWOT-analüüsi selgus, et LibreNMS on CabelNetwork AS-i jaoks kõige sobivam toode, kuna tarkvara põhifookus on võrgu monitoorimine ja võrreldes teistega on toode uus, mis tähendab seda, et arendajad arendavad kiiremini ja tekitavad uusi funktsioone, et nende toode oleks parem ning suurema kasutajaskonna jaoks sobivam.

Nagios Core ja Zabbix on rohkem serverite jaoks, puudub spetsialiseerumine ja fookus on mitme erineva suuna peal. Nagios Core ja Zabbix arendus ei ole nii kiire, kuna nende põhieesmärk on töökindlam süsteem.

LibreNMS on tavakasutajale lihtsamini arusaadav kui Zabbix või Nagios Core. LibreNMSi puhul pole vaja erilisi teadmisi, et seda juurutada. LibreNMS'is on uute võimaluste ja funktsioonide kasutuselevõtt lihtne, seetõttu võtavad kasutajad kergemini muudatusi vastu.

Nagios Core ja Zabbix peavad fookust muutma, sest paljud otsivad spetsiifilist tarkvara (nagu LibreNMS) ja võimalusel siirduvad kindlat funktsiooni pakkuvale rakendusele. Nagiosel ja Zabbixil on võimalus oma tooted struktureerida või eraldada mitmeks eraldi funktsioneerivaks osaks, ehk tekitada moodulid, mis annavad kasutajatele valida, mida nad täpselt soovivad. Kui on vaja näiteks monitoorida võrku, siis paigaldavad võrgumooduli; kui on vaja servereid ja serveriteenuseid monitoorida siis paigaldavad serverite moodul jne.

LibreNMSil on palju ohtusid, uudsus kaob ja kasutajad pettuvad ning loobuvad. Võimalik, et LibreNMS tulevikus hülgab tasuta jagatava teenuse mudeli, kuna vajab finantseerimist (mingil hetkel peab muutuma hobiprojektist kasumlikuks äriteenuseks). Nagios Core ja Zabbixil on ohud, et kuna mõlemad süsteemid on piisavalt kaua turul olnud ja mastaapsed projektid, tuleb iga arendatav versioon viivitusega. Nagiose ja Zabbixi eesmärgid on suunatud rohkem töökindlusele, et uued funktsionaalsused oleks võimalikult väikeste vigadega.

4.2 Varundussüsteemi analüüs

Kuna Unimus on tasuline, siis seda SWOT analüüsis ei ole.

Tabelis 4 on toodud valitud varundussüsteemide tugevused, nõrkused, võimalused ja ohud.

Tabel 4 Varandussüsteemide SWOT analüüs

SWOT-analüüs	**Rancid**	**Oxidized**
Tugevused	1. Tugi Cisco ja Juniper seadmetele 2. Hea funktsionaalsus, aga vähem funktsioone kui Oxidized 3. Vana projekt, mis pakub kasutajatele juba aastaid oma lahendust	1. Uus ja huvitav projekt 2. Suur tugi erinevatele võrguseadmetele 3. Toote funktsionaalsuse pidev arendamine 4. Suur funktsionaalsus (võrguseadme konfiguratsiooni salvestamine GIT repositooriumisse, konfiguratsiooni salvestamine tekstifailidesse, muudatuse saatmine e-posti teel jne)
Nõrkused	1. Arengu aeglustumine 2. Vana veebiliides 3. Väike valik toetatud seadmeid 4. API puudumine	1. Võimetus testida oma toodet (alfa ja beta testimine) 2. Testkogukonna väiksus 3. Integreeritav ainult LibreNMSiga, Zabbix ja Nagios ei ole toetatud
Võimalused	1. Funktsionaalsuse laiendamine 2. Veebiliidese uuendamine 3. Projekti uuestisünd 4. API arendamine 5. Toetatavate seadmete nimekirja laiendamine	1. Funktsionaalsuse laiendamine 2. Pilvelahenduse pakkumine 3. Integreeritav paljude monitooringusüsteemidega
Ohud	1. Kasutajate vähenemine, kuna projekt on liiga vana 2. Projekti funktsionaalsus ei kasva 3. Tootearenduse peatumine	1. Üleminek tasuta tootelt tasuliseks 2. Finantseerimise puudumine 3. Liigne fokuseerimine uutele funktsioonidele või lahendustele

Oxidized toetab suuremat arvu erinevate tootjate seadmeid, pakub suurt funktsionaalsust: võrguseadme konfiguratsiooni salvestamine GIT repositooriumisse, konfiguratsiooni salvestamine tekstifailidesse, muudatuse saatmine e-posti teel.

Rancid ei paku sama suurt funktsionaalsust nagu Oxidized. Rancidil on vananenud veebiliides, konfiguratsioone hoiab tekstifailis, ei ole API moodulit.

Mõlemad projektid on integreeritavad LibreNMSiga. LibreNMS suhtleb Rancidiga scripti vahendusel, aga Oxidized ja LibreNMS suhtlevad oma vahel API kaudu.

Rancidi suur nõrkus on arengu puudumine, vana projekti täiendatakse ainult Linuxi uute versioonide toetamiseks, kuid uusi funktsionaalsusi ei looda.

Oxidized on tänasel päeval kõige parem toode, mis annab laia funktsionaalsuse ning mis tulevikus võib kasvada väikesest projektist suuremahuliseks.

SWOT-i alusel valiti Oxidized, kuna Oxidized on kõige paremini sobiv võrguvarundussüsteemiks.

4.3 Monitooringusüsteemi paigaldamine ja konfigureerimine

Monitooringusüsteemi ja varundussüsteemi riistvara valik langes tavalisele personaalarvutile, millel oli juba litsentsitud Windows 10 järgmiste parameetritega:

- CPU: Intel Core i5 4 tuuma
- RAM: 16GB DDR4
- Ketas: 1TB SATA (mitte SSD)

Selles etapis valiti virtualiseerimiskeskkonnaks VirtualBox. VirtualBoxi keskkonnas luuakse kaks virtuaalset masinat:

- Librenms.cnw.ee
- Oxi.cnw.ee

Librenms.cnw.ee virtuaalmasina jaoks eraldati 3 tuuma, 12 GB muutmälu ja 500 GB kettaruumi.

Oxi.cnw.ee virtuaalmasina jaoks eraldati 1 tuum, 2 GB muutmälu ja 100 GB kettaruumi.

Mõlemasse virtuaalsesse masinasse installiti Linuxi op-süsteem - Ubuntu 18.04.4 LTS.

Mõlemale virtuaalmasinale seadistati haldusvõrk, kus on nähtavad kõik võrguseadmed.

Monitooringusüsteemi paigaldamine ja seadistamine on näidatud Lisas 1.

4.4 Varundussüsteemi paigaldamine ja konfigureerimine

Varundussüsteemi paigaldamine ja seadistamine on näidatud Lisas 2.

4.5 Võrguseadme monitoorimine

Seadmete monitoorimine ja andmete kogumine LibreNMS-is toimub läbi SNMP. LibreNMS toetab SNMP versiooni 3, mis tähendab, et iga päring sisaldab turvaparameetreid, mis on kodeeritud oktetstringina.

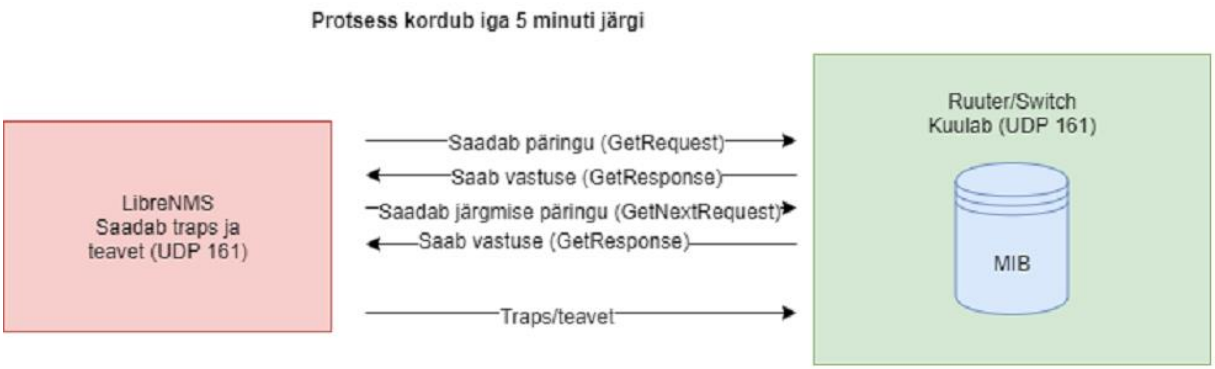
SNMPv3 pakub olulisi turvafunktsioone:

- Autentimine - sõnumi allika tuvastamine
- Konfidentsiaalsus - pakettide krüptimine kaitseks pealtkuulamise eest
- Terviklikkus - edastatavate sõnumimuutuste ärahoidmine, sealhulgas täiendav mehhanism kaitsmaks hõivatud paketi uuesti edastamise eest

SNMP-d kasutades saab LibreNMS kuvada järgmisi parameetreid:

- Seadme mudel
- Seerianumber
- Seadme tööaeg
- Paigaldatud tarkvara
- Pordid ja seadme koormusgraafik
- IP-aadress ja MAC-aadress
- VLAN
- Marsruutimisprotokollid (BGP, OSPF)

SNMP tööskeemi koos võrgu monitooringusüsteemiga näeb Joonisel 2.



Joonis 2 SNMP päringu protsess

Päring algatatakse LibreNMS'i poolt, mis saadab selle päringu agendile. Agent võtab päringu vastu ja töötleb seda.

Agent saadab päringule vastuse kasutades GetResponse operatsiooni ja LibreNMS töötleb saabunud andmeid. Üks osa Get päringust on muutuja, millega defineeritakse MIB objekt, mida päringu saatja teada soovib. Muutuja on seotud OID nimega. Protsessi korratakse iga 5 minuti järel.

Näiteks võivad Trap teated sisaldada eeldefineeritud infot:

- Külm start (Cold Start) - hallatav seade taaskäivitus, mis võib kaasa tuua seadme ümberkonfigureerimise
- Kuum start (Warm Start) - hallatav seade tegi taaskäivituse ilma alglaadimiseta
- Ühendus puudub (Link Down) - üks võrguliides ei tööta
- Ühendus olemas (Link Up) - liides on veaolukorrast taastunud
- Autentimisviga (Authentication Failure) - tööjaam üritab seadmega ühenduda, aga ei suuda korrektselt autentida [12]

Hallatavad objektid on organiseeritud puukujulisse hierarhiasse. Sellel struktuuril baseerub SNMP nimeskeem. Igal objektil on oma OID identifikaator, mis unikaalselt defineerib hallatava objekti. Nimed on esitatud kahel kujul: numbriliselt ja inimese poolt loetavas formaadis. Mõlemal juhul on tegemist pikkade ja ebamugavate nimedega ning SNMP rakenduse arendusel on vaja arvestada, kuidas esitada nimeruumis navigeerimine kasutajatele mugavalt. Objekti ID koosneb täisarvude seeriatest, vastavalt puu hargnemisele ja on eraldatud punktidega. Inimese poolt loetav kuju on nimede seeria, mis on eraldatud punktidega. [13]

Haldusinfo andmebaas on hallatavate objektide andmebaas, mida agent jälgib. Erinevat liiki staatuse ja statistikainfo, mida NMS saab kasutada, on defineeritud MIB'is. Igal võrguseadmel on oma lokaalne MIB, kus salvestuvad seadmega seotud andmed. [14]

SNMP abil jälgimiseks on vaja esmalt konfigureerida selle protokolli agendid võrguseadmetes.

Selleks valiti järgmised SNMP sätted:

- SNMP versioon: 3
- SNMP kasutaja/kogukond: LibreNMS
- Autentimisprotokoll: SHA (vanemad seadmed ei toeta uusi Autentimine-protokolle)
- Autentimisvõti: *SigaJaLehmLaudas!*
- Privaatsusprotokoll: AES128 (AES128 oli valitud nagu privaatsusprotokoll, selle pärast, et vanad seadmed ei toeta suurem krüptimisvõti kui 128)
- Privaatsusvõti: *SigaJaLehmLaudas!*

Võrguseadmete konfiguratsiooni parameetrid on järgmised:

Cisco IOS:

snmp-server user LibreNMS LibreNMS v3 auth sha SigaJaLehmLaudas! priv aes 128 SigaJaLehmLaudas!

snmp-server group LibreNMS v3 priv read LibreNMS write LibreNMS

snmp-server view LibreNMS iso included

snmp-server community LibreNMS RW 1

Juniper JunOS:

set snmp v3 usm local-engine user LibreNMS authentication-sha authentication-key "9S3tyvWbs2JZjg4UHk.5TFn/CO1hSrMWx36WL7-

2g5QzFCtIRSv8Xyr24aZjiO1Ihev8X7-ds1RyKWLN-wYgoUj5QFt0BDiApB1yroJZji.TQnAuOaZtu1IcSaZGUjqmfT3nCs2P5TQn69ApOhSleWLNduObs2oGUHqmTn/CA0RcyOBEyKMXxNdb2JG"

set snmp v3 usm local-engine user LibreNMS privacy-aes privacy-key "9h73cevdbsoaUY2ZjikPfQFn/uORhSKvLz3vWX7sYP5TQ/CB1heM8cSs24aUDuOBReM8X7NbO1clvWx7VwYgZUP5QCp0GD9A0OcSgoaUDkf5F9tu4aCtOBEh4aJZUHqmfzF/bs.Pf5F369AuRhyrvWxNtudbsgJZjHqfFn/9p1Ecu0IclK8LxNdsoJ"

set snmp v3 vacm security-to-group security-model usm security-name LibreNMS group LibreNMS

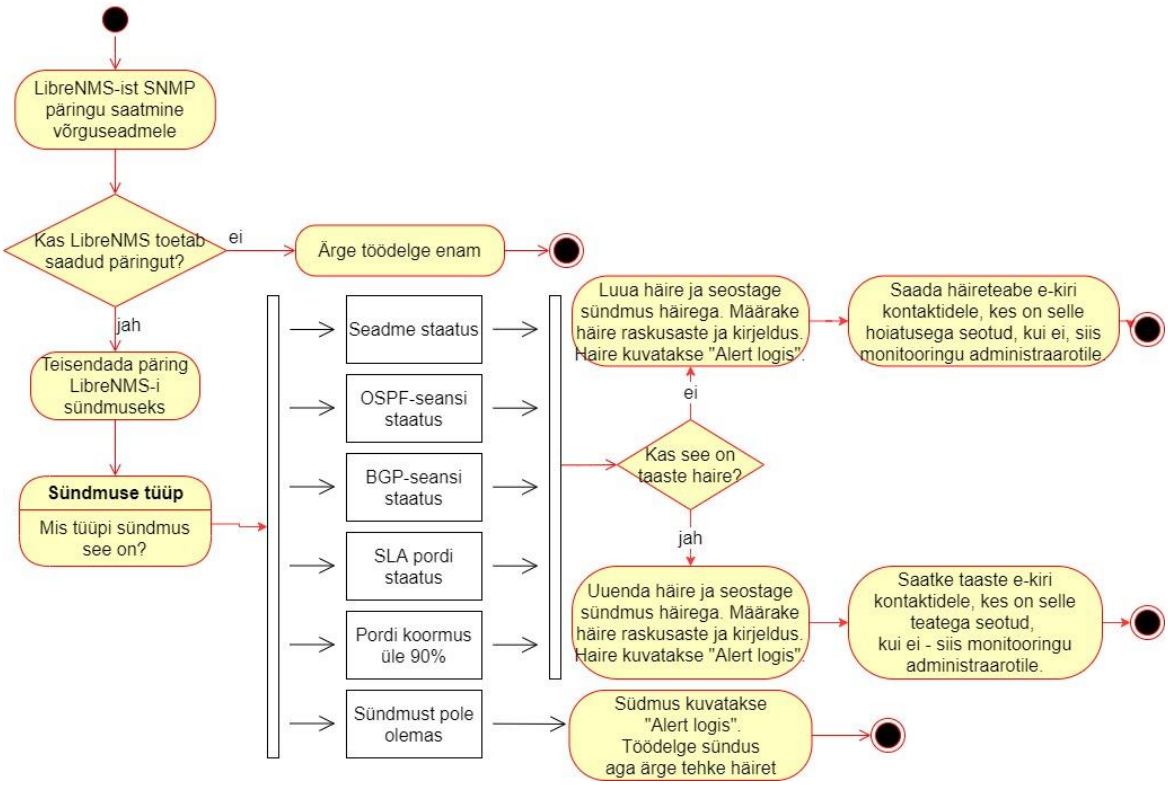
set snmp v3 vacm access group LibreNMS default-context-prefix security-model any security-level privacy read-view LibreNMS

set snmp view LibreNMS oid .1 include

set snmp community LibreNMS authorization read-only

4.6 Monitooringu protsessi kirjeldamine

Ettevõtte jaoks probleemi lahendamisel seatud tingimuste üheks peamiseks kriteeriumiks on võrgu infrastruktuuri komponendi rikke jälgimine ja sellest teatamine. Joonis 3 näitab monitooringu süsteemi LibreNMS töövoogu võrgukomponendi rikke sündmuse puhul.



Joonis 3 Monitooringu protsess

LibreNMSi monitooringu protsess töötab nii, et süsteem saadab SNMP päringuid ja võtab vastu SNMP vastuseid. Kui sündmusel põhinev vastus saadakse, määrab LibreNMS sündmuse tüübi.

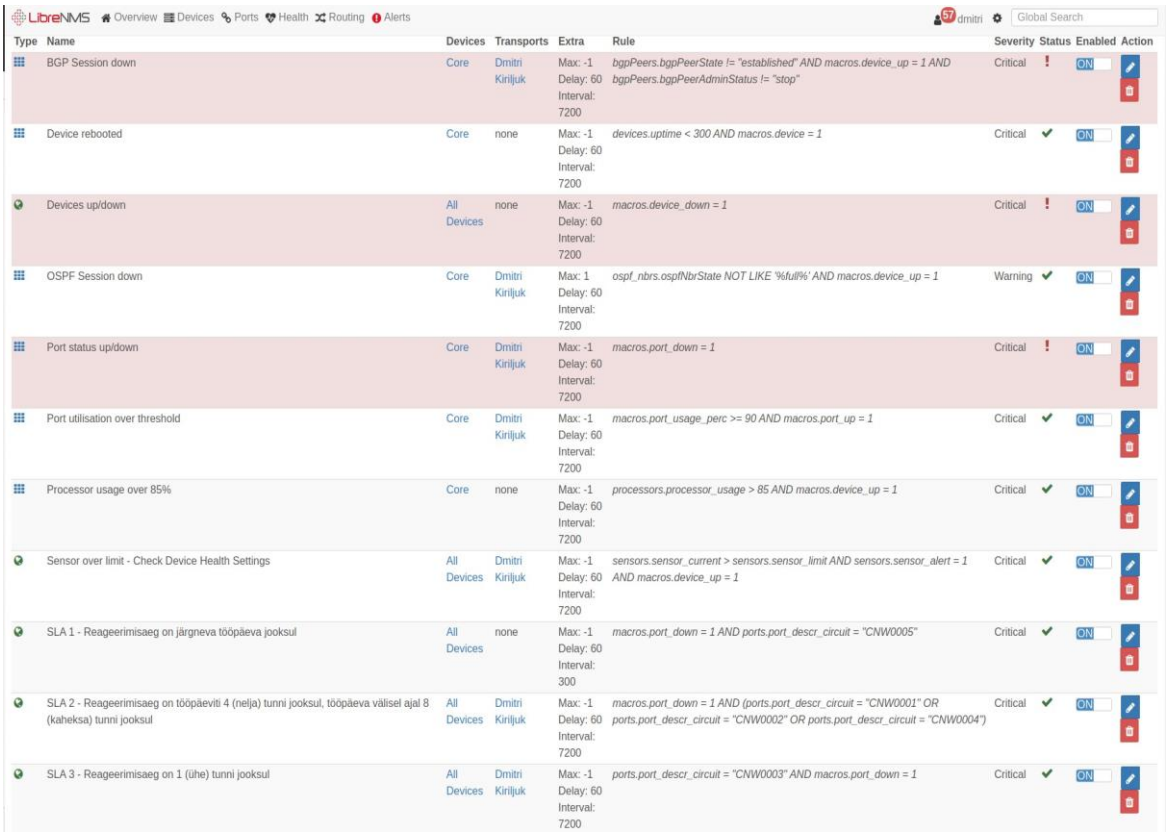
Probleemi püstitusel olid määratud sellised sündmused nagu:

- Seadme staatus
- OSPF-seansi staatus
- BGP-seansi staatus
- SLA pordi staatus
- Pordi koormus üle 90%

Sündmuse puhul kontrollitakse, kas on taastehäire. Kui ei ole, tõstatatakse häire, määratakse raskusaste ja kirjeldus, mille järel saadetakse e-kiri probleemist ja protsess lõpeb. Kui on taastehäire, värskendatakse olemasoleva häire põhjal olekut ja saadetakse

teade, et probleem on lahendatud ja protsess lõpeb. Kui sündmuse põhjal häiret ei ole seadistatud, protsess lõpeb. Monitooringu protsess kordub iga 5 minuti järel.

Joonisel 4 näeb kõiki konfigureeritud häireteateid kiireks reageerimiseks ja infrastruktuuris probleemide leidmiseks või võrgu kitsaskohtade tuvastamiseks. Põhiliste hoiatuste seadistamist kirjeldatakse järgmistes peatükkides.



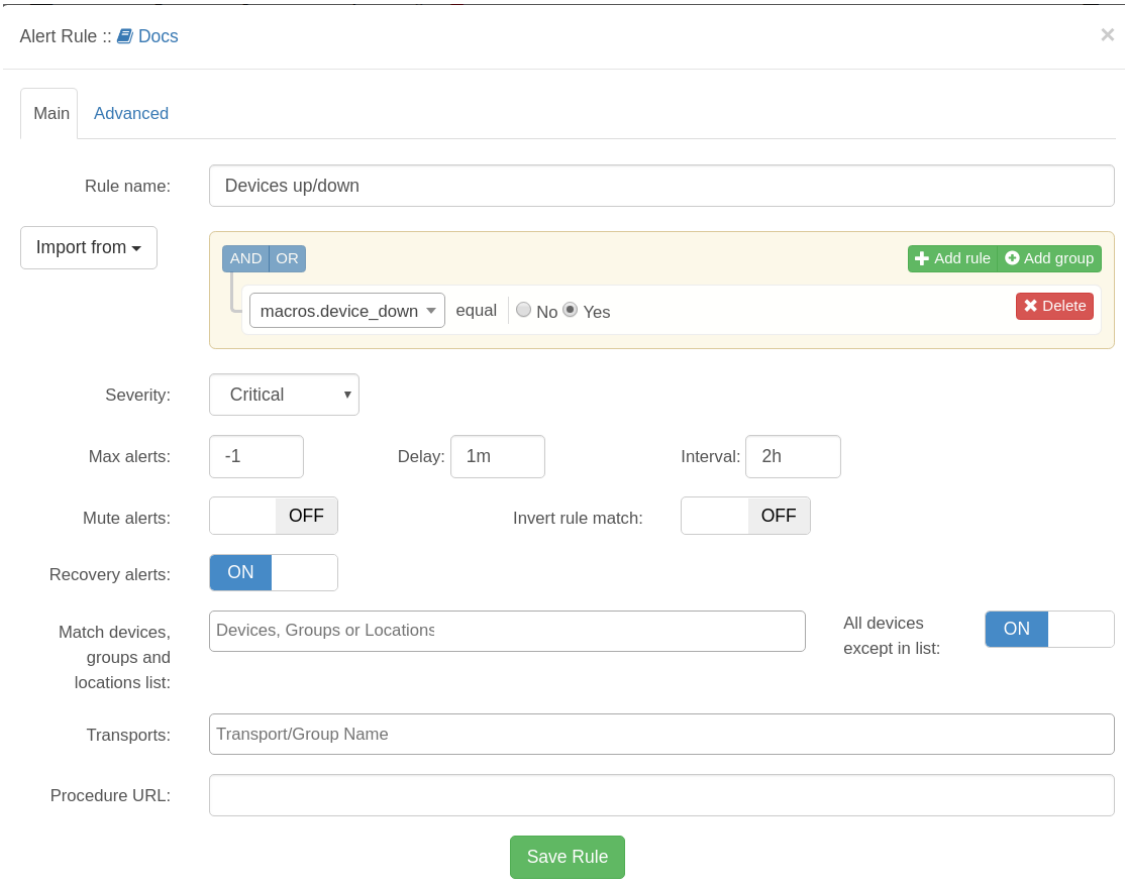
Type	Name	Devices	Transports	Extra	Rule	Severity	Status	Enabled	Action
	BGP Session down	Core	Dmitri Kiriljuk	Max: -1 Delay: 60 Interval: 7200	bgpPeers.bgpPeerState != "established" AND macros.device_up = 1 AND bgpPeers.bgpPeerAdminStatus != "stop"	Critical	!	ON	
	Device rebooted	Core	none	Max: -1 Delay: 60 Interval: 7200	devices.uptime < 300 AND macros.device = 1	Critical	✔	ON	
	Devices up/down	All Devices	none	Max: -1 Delay: 60 Interval: 7200	macros.device_down = 1	Critical	!	ON	
	OSPF Session down	Core	Dmitri Kiriljuk	Max: 1 Delay: 60 Interval: 7200	ospf_nbrs.ospfNbrState NOT LIKE '%full%' AND macros.device_up = 1	Warning	✔	ON	
	Port status up/down	Core	Dmitri Kiriljuk	Max: -1 Delay: 60 Interval: 7200	macros.port_down = 1	Critical	!	ON	
	Port utilisation over threshold	Core	Dmitri Kiriljuk	Max: -1 Delay: 60 Interval: 7200	macros.port_usage_perc >= 90 AND macros.port_up = 1	Critical	✔	ON	
	Processor usage over 85%	Core	none	Max: -1 Delay: 60 Interval: 7200	processors.processor_usage > 85 AND macros.device_up = 1	Critical	✔	ON	
	Sensor over limit - Check Device Health Settings	All Devices	Dmitri Kiriljuk	Max: -1 Delay: 60 Interval: 7200	sensors.sensor_current > sensors.sensor_limit AND sensors.sensor_alert = 1 AND macros.device_up = 1	Critical	✔	ON	
	SLA 1 - Reageerimisaeg on järgneva tööpäeva jooksul	All Devices	none	Max: -1 Delay: 60 Interval: 300	macros.port_down = 1 AND ports.port_descr_circuit = "CNW0005"	Critical	✔	ON	
	SLA 2 - Reageerimisaeg on tööpäeviti 4 (nelja) tunni jooksul, tööpäeva välisel ajal 8 (kaheksa) tunni jooksul	All Devices	Dmitri Kiriljuk	Max: -1 Delay: 60 Interval: 7200	macros.port_down = 1 AND (ports.port_descr_circuit = "CNW0001" OR ports.port_descr_circuit = "CNW0002" OR ports.port_descr_circuit = "CNW0004")	Critical	✔	ON	
	SLA 3 - Reageerimisaeg on 1 (ühe) tunni jooksul	All Devices	Dmitri Kiriljuk	Max: -1 Delay: 60 Interval: 7200	ports.port_descr_circuit = "CNW0003" AND macros.port_down = 1	Critical	✔	ON	

Joonis 4 Häireteateid

4.6.1 Seadme staatuse häireteate seadistamine

Seadme staatuse monitoorimine seadistatakse LibreNMS-is parameetri „device_down" abil. Joonis 5 näitab, kuidas häire seadistamine toimub, kui seadme staatus on DOWN.

Häireteatele seadistakse ka raskusaste, lisatakse kõik võrguseadmed ja määratakse isik keda teavitatakse.



Joonis 5 Seadme staatuse häireteate seadistamine

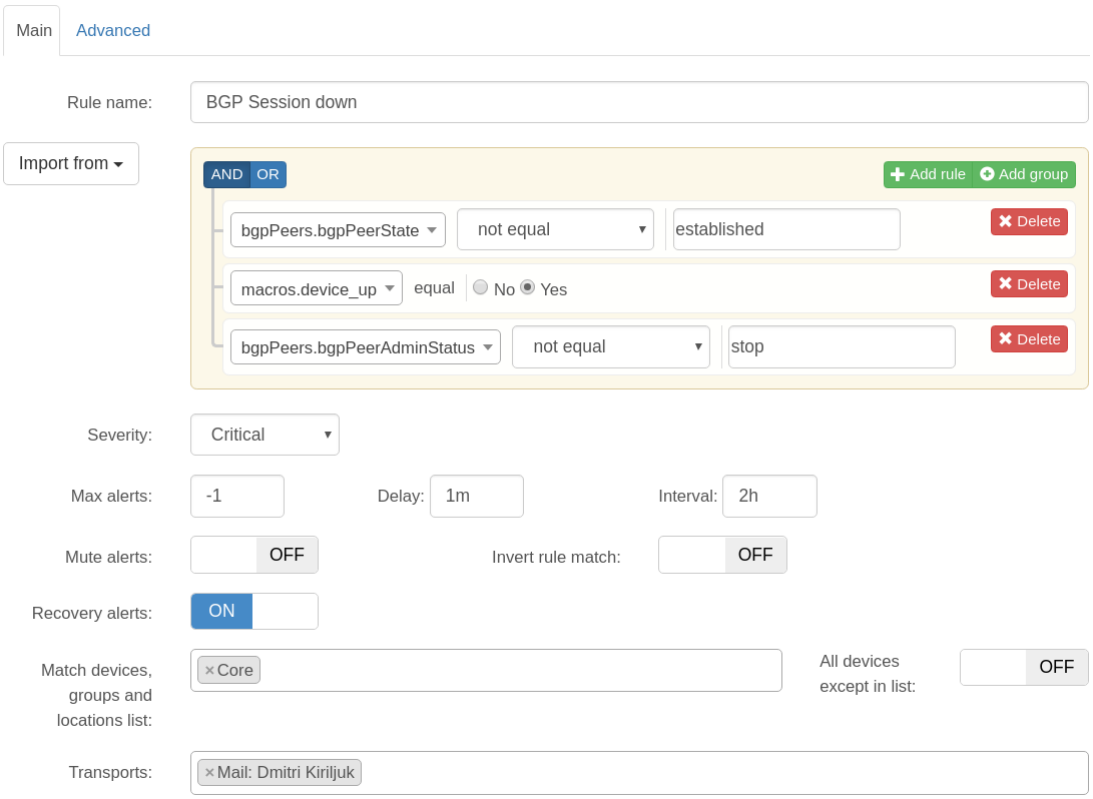
4.6.2 BGP-seansi staatuse häireteate seadistamine

BGP-seansi häire staatuse peamised parameetrid:

- „bgpPeers.bgpPeerState not equal established“ – BGP seanss ei ole väljakujunenud
- „bgpPeers.bgpPeerAdminStatus not equal stop“ - BGP seansi administratiivne olek ei ole peatatud
- „device_up equal yes“ – võrguseade on püsti

Häireteates seadistatakse ka raskusaste (Critical, Warning, OK), lisatakse võrguseadme grupp ja määratakse isik, keda teavitatakse.

Joonis 6 näitab, kuidas BGP-seansi hoiatusteade on konfigureeritud.



Joonis 6 BGP-seansi staatuse häireteate seadistamine

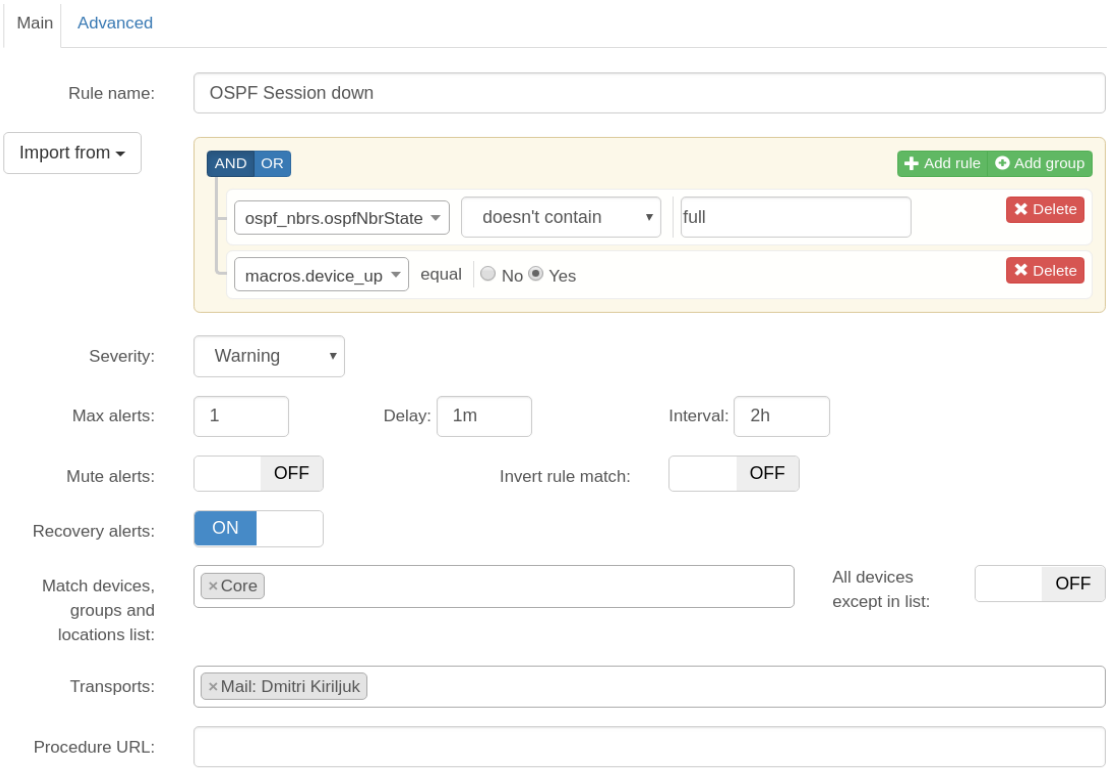
4.6.3 OSPF-seansi häireteate seadistamine

OSPF-seansi häire staatuse peamised parameetrid:

- „ospf_nbrs.ospfNbrState doesn't contain full" – OSPF naaber ei ole tabatav
- „device_up equal yes" – võrguseade on püsti

Häireteates seadistatakse raskusaste (Critical, Warning, OK), lisatakse võrguseadme grupp ja määratakse isik, keda teavitatakse.

Joonis 7 näitab, kuidas OSPF-seansi hoiatusteade on konfigureeritud.



Joonis 7 OSPF sessioonide häireteate seadistamine

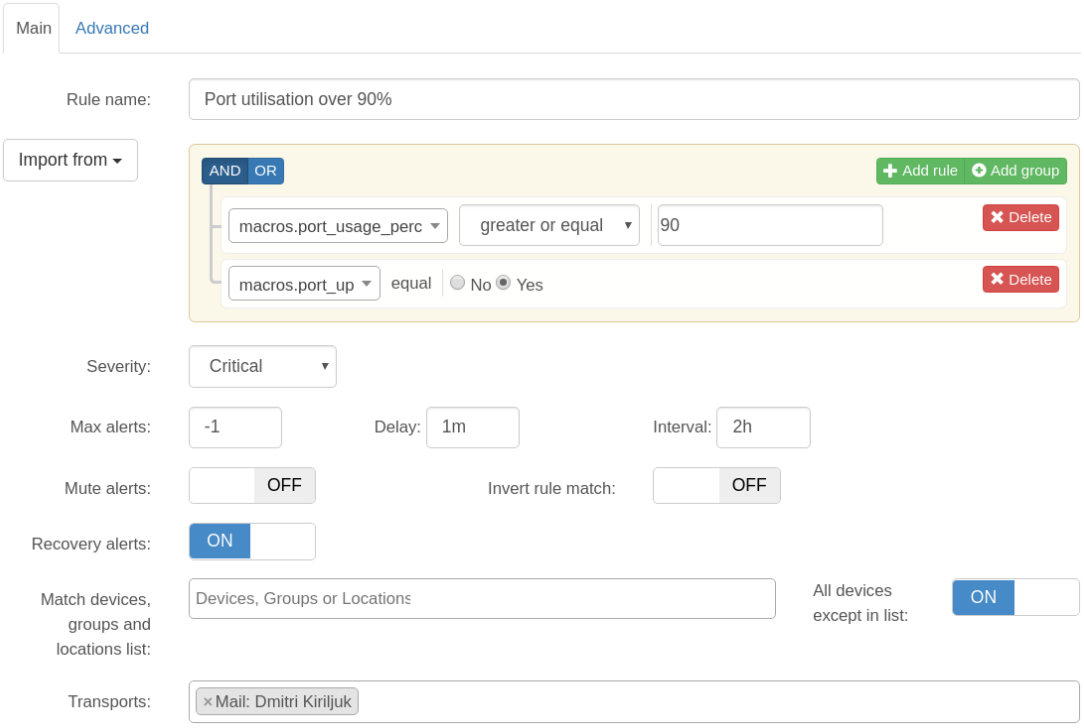
4.6.4 Võrgukanali koormuse häireteate seadistamine

Märguanded märgi ületamisest 90% ulatuses valitud kanali koormusest konfigureeritakse järgmiste parameetrite abil:

- „port_usage_percentage greater or equal 90“ – pordi kanali kasutuse protsent on suurem või võrdne 90
- „port_up equal Yes“ - võrguseade port on püsti

Häireteatele seadistatakse ka raskusaste (Critical, Warning, OK), lisatakse võrguseadme grupp ja määratakse isik, keda teavitatakse.

Joonis 8 näitab, kuidas kanali koormuse häireteade on konfigureeritud.



Joonis 8 Võrgu kanali koormuse häireteate seadistamine

4.6.5 Kliendi pordi staatuse häireteate seadistamine SLA tüübi järgi

CableNetwork AS-is on igal kliendil oma teenuse number CNWxxxx, mis vastab Interneti kasutavale teenusele.

Monitooringusüsteem LibreNMS on võimeline kirjeldama kliendi porti järgmiselt:

Cisco IOS:

descr Cust: Kliendi-Nimi [10Mbit] (T1 Telco Y CCID129031) {CNW0001}

Juniper JunOS:

set interfaces ge-0/0/0 description " Cust: Kliendi-Nimi [10Mbit] (T1 Telco Y CCID129031) {CNW0001}"

Olemasolev identifikaator määratleb teenuse tüübi, tunnustatud tüübid on:

Identifikaator:

- Cust: Klient

- Transit: Transiidi link
- Peering: Peeringi link
- Core: Infrastruktuuri link (mitte klient)
- Server: Serverilink (mitte klient)

Lisateavet saab lisada erinevate sulgude tüüpide abil:

- () - sisaldab märkust
- {} - sisaldab teenuse numbrit
- [] - sisaldab teenuse tüüpi või kiirust

Joonis 9 näitab kliendi porti koos vastava kirjeldusega.

Joonis 9 Kliendi porti, mida monitooritakse

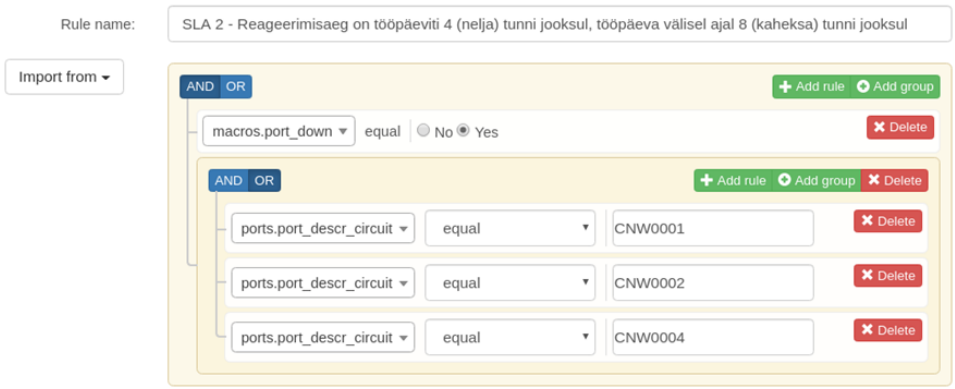
Igal teenusel on SLA tüüp:

- SLA1 – Reageerimisaeg on tööpäeva jooksul
- SLA2 – Reageerimisaeg on tööpäeviti 4 (nelja) tunni jooksul, tööpäeva välisel ajal 8 (kaheksa) tunni jooksul
- SLA3 – Reageerimisaeg on 1 (ühe) tunni jooksul

Kliendi pordi staatuse parameetrid:

- „port_down equal yes“ – võrguseadme port on maas
- „port_descr_circuit equal CNW0001“ – pordi kirjeldus võrdub CNW0001

Joonisel 10 konfigureerime SLA2 häire, sel juhul monitoorime pordi staatust ja leiame unikaalse teenusenumbriga pordi, mida lepingu alusel jälgitakse vastavalt SLA2 tüübile. SLA1 ja SLA3 on konfigureeritud samal viisil.



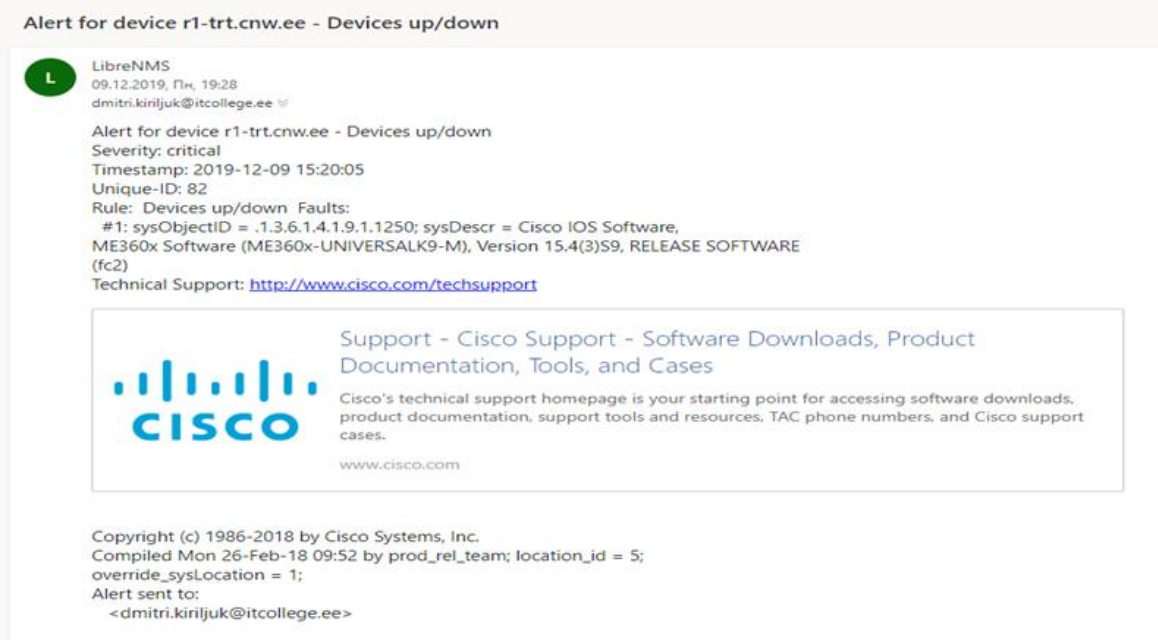
Joonis 10 Kliendi pordi staatuse seadistamine SLA tüübi järgi

4.7 NOC teavitamine probleemist e-posti teel

Võrgu monitooringu üks olulisi aspekte on võrgu katkestustest ja probleemidest õigeaegne teavitamine. Probleemi lahendamiseks kasutati LibreNMS-i funktsioonide integreerimiseks CabelNetwork AS-i, kui tõrge ilmneb, saadetakse häireteade e-postiga.

Joonis 11 näitab hoiatust, et BGP-seanss ei tööta, ja Joonis 12 näitab, et seade nimega “r1-trt.crnw.ee” ei reageeri nüüd monitooringusüsteemi päringutele.

Joonis 11 BGP-seanss ei toimi



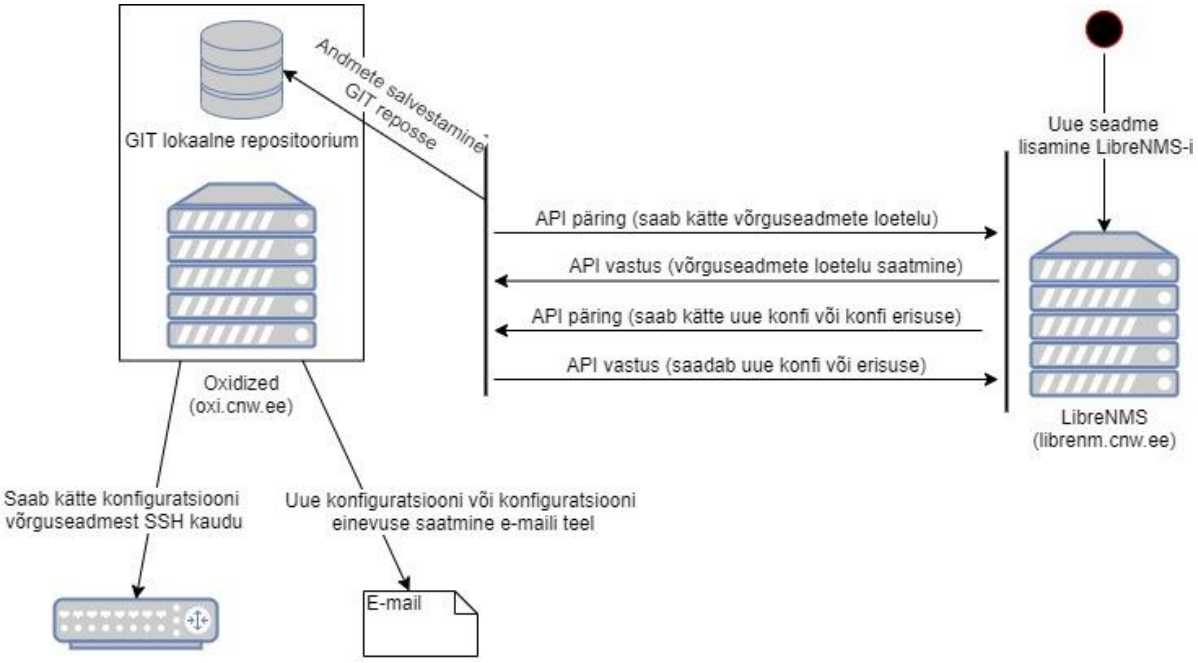
Joonis 12 Seade on häiritud/töökorras

4.8 Varundussüsteemi juurutamine

Riknenud võrguseadme kiireks asendamiseks võrguinfrastruktuuris kasutatakse varundussüsteemi.

Joonis 13 näitab konfiguratsiooni varundamise protsessi ja integreerimist monitooringusüsteemiga LibreNMS. LibreNMS ja Oxidized süsteemi integreerimise seadistamine on kirjeldatud Lisas 3.

Nagu võib näha Jooniselt 13, Oxidized ja LibreNMS suhtlevad API päringute ja vastuste abil.



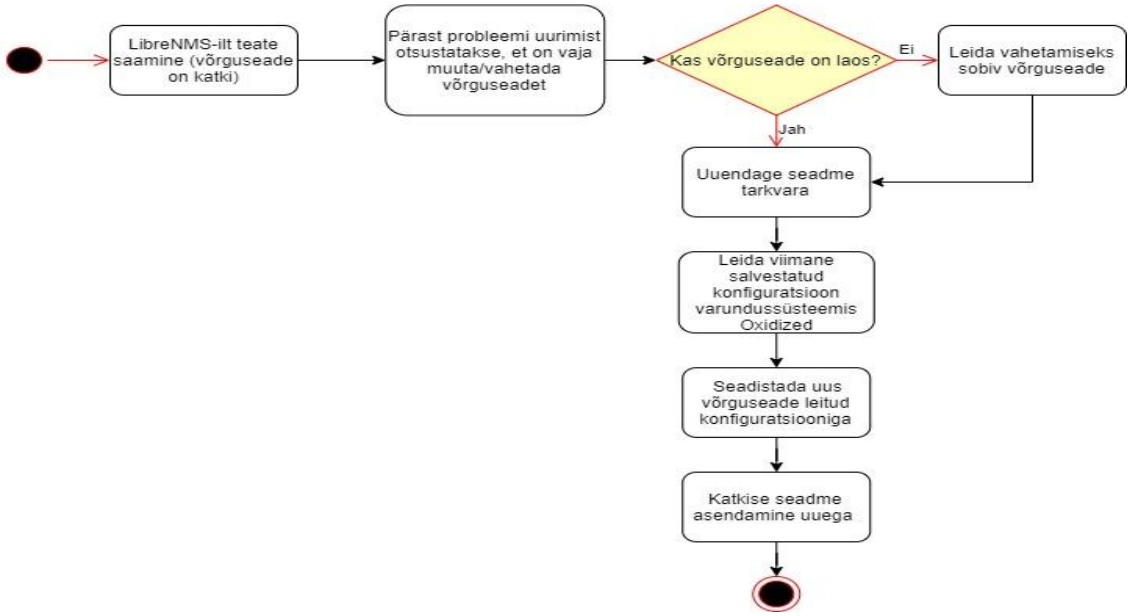
Joonis 13 Konfiguratsiooni varundamise protsess

Uue võrguseadme lisamisel saadab Oxidized LibreNMS-ile päringu kõigi seadmete kohta, kui seadme konfiguratsiooni ei hoita GIT repositooriumis, siis Oxidized logib uude seadmesse sisse Oxidized konfiguratsioonifailis kirjeldatud kasutajatunnuse abil ja salvestab konfiguratsiooni GIT repositooriumisse.

Uus konfiguratsioon saadetakse võrguadministraatorile e-posti teel. LibreNMS omakorda kuvab API kaudu olemasolevat konfiguratsiooni või muudatusi võrguseadme veebiliidese vahekaardil. Oxidized küsitleb võrguseadmeid iga 30 minuti järel, lisab muudatused GIT repositooriumisse ja saadab muudatused e-postiga.

Pärast monitooringusüsteemi ja varundussüsteemi juurutamist otsustati kirjeldada seadme asendamise protsessi, kuna enne oli see protsess kaootiline ja uutele töötajatele arusaamatu.

Joonisel 14 näete kõiki vigastatud seadmete asendamise protsessi etappe.



Joonis 14 Võrguseadme asendamise töö voog

Selle protsessi käigus toimuvad järgmised sammud:

1. LibreNMSilt teate saamine, et võrguseade ei vasta
2. Pärast probleemi uurimist otsustatakse, et on vaja muuta/vahetada võrguseade
3. Kontrollitakse, kas sarnane seade on laos, kui mitte, siis valitakse samatüüpne seade, kuna Cisco´l on palju sarnaseid võrguseadmeid, siis ei pea konfiguratsiooni muutma (sarnane tähendab, et näiteks uues seadmes on porte rohkem või näiteks mudel on erinev. Cisco Catalyst 2960-8P või Cisco Catalyst 2960-16P)
4. Tarkvara uuendamine käsitsi (Cisco iOS/JunOS)
5. Leida viimane salvestatud konfiguratsioon varundussüsteemist Oxidized
6. Seadistada uus võrguseade leitud konfiguratsiooniga
7. Katkise seadme asendamine uuega

Kahjuks on selles etapis seadme asendamise protsess väga aegunud ja seda pole mingil viisil optimeeritud. Tulevikus optimeeritakse seda protsessi nii, et seade konfigureeritakse võrguga ühendamisel iseseisvalt, kuid see ei kuulu selle töö skoopi.

5 Kokkuvõte

Käesoleva bakalaureusetöö eesmärgiks oli juurutada seadme monitooringu- ja varundussüsteem, mis võimaldab jälgida nii erinevate tootjate kommutaatoreid kui ruutereid ja anda häiret juhul, kui tekib rike, samuti seadme konfiguratsioonide viimaste muudatuste kogumist ja salvestamist kohalikku GIT-i.

Teoreetilises osas analüüsiti monitooringusüsteemide ja varundussüsteemide turgu. Turuanalüüsi põhjal võrreldi kõigi süsteemide funktsionaalsust ning SWOT-analüüsi põhjal valiti monitooringusüsteem LibreNMS ja varundussüsteem Oxidized. Need süsteemid vastavad kõigile nõuetele:

Monitooringusüsteem vastab järgmistele nõuetele:

- Vabavaraline
- Kõik kasutatavad tarkvaralised komponendid peavad olema avatud lähtekoodiga
- Süsteemi skaleeritavus ehk süsteem suudab monitoorida nii 10 seadet kui ka 3500 seadet
- Standardsed diagnostikaaruande raportid (pordi staatused, kanali koormusgraafikud jne)
- Kõigi kasutatud tarkvaratoodete üksikasjaliku dokumentatsiooni kättesaadavus
- Võime toetada erinevate tootjate võrgu seadmeid ehk monitoorib erinevate tootjate seadmeid
- SNMP jälgimine

Varundussüsteem vastab järgmistele nõuetele:

- Vabavaraline

- GIT tugi – (versioonihaldus ja konfiguratsiooni salvestamine GIT repositooriumisse)
- SSH tugi – (võrguseadme konfiguratsiooni varundamine SSH kaudu)
- Varundussüsteemi integreerimine monitooringusüsteemiga

Praktilises osas paigaldati ja konfigureeriti mõlemad süsteemid. Pärast seadistati häired käesoleva probleemi alusel kiireks rikke tuvastamiseks ettevõttevõrgus. Seadistati klientühenduse jälgimine SLA tüübi järgi. Võrgu katkestustest ja probleemidest konfigureeriti õigeaegne teavitamine e-posti teel. Seadistati ka monitooringu- ja varundussüsteemide integreerimine päringu ja vastuse API abil, kirjeldati võrguseadme konfiguratsiooni salvestamise protsessi kohalikku GIT-i. Tutvustati ja kirjeldati võrguseadme asendamise protsessi.

Tulemuseks on võrgu monitoorimiseks ja võrgu seadme konfiguratsiooni salvestamiseks terviklik lahendus.

6 Summary

The aim of this bachelor's thesis was to implement a device monitoring and backup system, which allows monitoring both switches and routers from different manufacturers and raising disturbances in case of failure, as well as collecting and saving the latest device configuration changes to the local GIT.

In the theoretical part, the market of monitoring systems and backup systems was analyzed. Based on the market analysis, the functionality of all systems was compared, and based on the SWOT analysis, the monitoring system LibreNMS and the backup system Oxidized were selected. These systems meet all the requirements:

The Monitoring System meets the following requirements:

- Free
- All software components used must be open source
- System scalability, ie the system can monitor both 10 devices and 3500 devices
- Standard diagnostic report reports (port statuses, channel load schedules, etc.)
- Availability of detailed documentation for all software products used
- Ability to support network devices from different manufacturers, ie monitors devices from different manufacturers
- SNMP monitooring

The backup system meets the following requirements:

- Free
- GIT support - (version management and saving the configuration to the GIT repository)

- SSH support - (network device configuration backup via SSH)
- Integration of the backup system with the monitoring system

In practice, both systems were installed and configured. After the alarms were configured based on this problem, the corporate network failure was quickly detected. Client connection tracking by SLA type was configured. Timely e-mail notification of network outages and problems was configured. The integration of monitoring and backup systems was also configured using the request and response API, the local GIT of the network device configuration saving process was described. The network device replacement process was introduced and described.

The result was a complete solution for monitoring the network and saving the configuration of the network device.

Kasutatud kirjandus

[1] P. Bischoff, „Top 5 open source network monitoring tools,“ 04 veebruar 2019. [Võrgumaterjal]. Available: https://opensource.com/article/19/2/network-monitoring-tools. [Kasutatud 20 aprill 2020].

[2] „Nagios Features & Capabilities,“ [Võrgumaterjal]. Available: https://www.nagios.org/about/features/. [Kasutatud 25 märts 2020].

[3] „Librenms,“ [Võrgumaterjal]. Available: https://www.librenms.org/. [Kasutatud 06 detsember 2019].

[4] „Best Free Monitoring system for Linux,“ [Võrgumaterjal]. Available: https://lintut.com/best-free-monitoring-system-for-linux/. [Kasutatud 06 detsember 2019].

[5] „Zabbix,“ [Võrgumaterjal]. Available: https://searchitoperations.techtarget.com/definition/Zabbix. [Kasutatud 20 aprill 2020].

[6] Bubnov, „Varundussüsteemid,“ 12 oktoober 2017. [Võrgumaterjal]. Available: http://www.bubnovd.net/2017/10/oxidized.html. [Kasutatud 10 detsember 2019].

[7] S. Ytti, „Oxidized,“ [Võrgumaterjal]. Available: https://github.com/ytti/oxidized. [Kasutatud 10 detsember 2019].

[8] „Rancid,“ [Võrgumaterjal]. Available: https://www.shrubbery.net/rancid/. [Kasutatud 10 detsember 2019].

[9] „Observium RANCID Integration,“ [Võrgumaterjal]. Available: https://docs.observium.org/rancid/. [Kasutatud 20 aprill 2020].

[10] „LibreNMS Docs - LibreNMS Rancid integration,“ [Võrgumaterjal]. Available: https://docs.librenms.org/Extensions/Rancid/. [Kasutatud 20 aprill 2020].

[11] „Wiki OpenNMS,“ [Võrgumaterjal]. Available: https://wiki.opennms.org/wiki/UCE2011/RANCID-Integration. [Kasutatud 20 aprill 2020].

[12] „EUCIP - SNMP teenused,“ [Võrgumaterjal]. Available: https://eopearhiiv.edu.ee/e-

kursused/eucip/haldus/622_snmp_teenused.html. [Kasutatud 10 detsember 2019].

[13] „EUCIP - Objektide nimetamine,“ [Võrgumaterjal]. Available: https://eopearhiiv.edu.ee/e-kursused/eucip/haldus/6215_objektide_nimetamine.html. [Kasutatud 20 veebruar 2020].

[14] „EUCIP - Haldusinfostruktuur ja MIB’id,“ [Võrgumaterjal]. Available: https://eopearhiiv.edu.ee/e-kursused/eucip/haldus/6214_haldusinfostruktuur_ja_mibid.html. [Kasutatud 20 veebruar 2020].

[15] „LibreNMS Docs - Installation Ubuntu18.04(Apache),“ [Võrgumaterjal]. Available: https://docs.librenms.org/Installation/Installation-Ubuntu-1804-Apache/. [Kasutatud 10 detsember 2019].

[16] A. Kili, „install-librenms-monitoring-on-ubuntu-centos,“ 25 aprill 2018. [Võrgumaterjal]. Available: https://www.tecmint.com/install-librenms-monitoring-on-ubuntu-centos/. [Kasutatud 10 detsember 2019].

[17] S. Shovon, „https://linuxhint.com/,“ 10 aprill 2020. [Võrgumaterjal]. Available: https://linuxhint.com/install_postfix_ubuntu_1804/.

[18] „Extensions Oxidized,“ [Võrgumaterjal]. Available: https://docs.librenms.org/Extensions/Oxidized/. [Kasutatud 10 detsember 2019].

Lisa 1 - LibreNMS paigaldus protsess

LibreNMS paigaldus protsess

Vaja installida järgmised paketid:

apt install software-properties-common

add-apt-repository universe

apt update

apt install curl apache2 composer fping git graphviz imagemagick libapache2-mod-php7.2 mariadb-client mariadb-server mtr-tiny nmap php7.2-cli php7.2-curl php7.2-gd php7.2-json php7.2-mbstring php7.2-mysql php7.2-snmp php7.2-xml php7.2-zip python-memcache python-mysqldb rrdtool snmp snmpd whois

Lisada LibreNMS kasutaja:

useradd librenms -d /opt/librenms -M -r

usermod -a -G librenms www-data

Laadige alla LibreNMS paketid:

cd /opt/

git clone https://github.com/librenms/librenms.git

Seadistage õigused:

chown -R librenms:librenms /opt/librenms

chmod 770 /opt/librenms

setfacl -d -m g::rwx /opt/librenms/rrd /opt/librenms/logs /opt/librenms/bootstrap/cache/ /opt/librenms/storage/

setfacl -R -m g::rwx /opt/librenms/rrd /opt/librenms/logs /opt/librenms/bootstrap/cache/ /opt/librenms/storage/

Installige PHP-sõltuvused:

su - librenms

./scripts/composer_wrapper.php install --no-dev

exit

MySQL konfigureerimine

Taaskäivita MySQL andmebaas

systemctl restart mysql

mysql -uroot -p

Palun muutke allpool olev parool “password” turvaliseks:

CREATE DATABASE librenms CHARACTER SET utf8 COLLATE utf8_unicode_ci;

CREATE USER 'librenms'@'localhost' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON librenms. TO 'librenms'@'localhost';*

FLUSH PRIVILEGES;

Exit

Vaja muuta andmebaasi konfiguratsioonifaili:

vi /etc/mysql/mariadb.conf.d/50-server.cnf

Jaotisesse [mysqld] lisage palun:

innodb_file_per_table=1

lower_case_table_names=0

Andmebaasiserveri taaskäivitamine:

systemctl restart mysql

Seadistage PHP

a2enmod php7.2

a2dismod mpm_event

a2enmod mpm_prefork

Apache seadistamine

vi /etc/apache2/sites-available/librenms.conf

Lisage järgmine konfiguratsioon, muutke *ServerName* vastavalt vajadusele:

```
<VirtualHost *:80>
  DocumentRoot /opt/librenms/html/
  ServerName  librenms.cnw.ee
  AllowEncodedSlashes NoDecode
  <Directory "/opt/librenms/html/">
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews
  </Directory>
</VirtualHost>
```

Vaja aktiveerida Apache konfiguratsiooni fail:

a2ensite librenms.conf

a2enmod rewrite

systemctl restart apache2 [15]

Cron job seadistamine:

cp /opt/librenms/librenms.nonroot.cron /etc/cron.d/librenms

***Logrotate* konfiguratsiooni kopeerimine:**

LibreNMS hoiab logisid kaustas /opt/librenms/log. Aja jooksul võivad need kasvada liiga suureks, kuid neid saab kustutada. Vanade logide üleskirjutamiseks võite kasutada kaasasolevat *logrotate* konfiguratsioonifaili:

cp /opt/librenms/misc/librenms.logrotate /etc/logrotate.d/librenms

Rakenduse paigaldamine Internetist:

Pöörduge veebilehele ja järgige ekraanil kuvatavaid juhiseid.

http://librenms.cnw.ee/install.php

Viimased sammud:

Nüüd peaks olema võimalik sisse logida http://librenms.cnw.ee/ .[16]

Postfix paigaldamine ja konfigureerimine:

Paigaldame Postfixi

sudo apt install postfix

Muudame Postfix konfiguratsiooni faili *vi /etc/postfix/main.cf* järgmiseks:

myhostname = librenms.cnw.ee # *määratakse serveri nimi-domeen*

myorigin = librenms.cnw.ee # *määratakse serveri nimi-domeen*

mydestination = $myhostname, librenms.cnw.ee, localhost.cnw.ee, localhost

relayhost = mail.cnw.ee #ettevõtte e-posti server

inet_interfaces = all

inet_protocols = all [17]

Lisa 2 - Oxidized paigaldus protsess

Oxidized paigaldus protsess

Soovitatav on kasutada versioone Debiani "Buster" või uuem ja Ubuntu 17.10 või uuem.

Ubuntul määrake kõigepealt üldhoidla (vajalik libssh2-1-dev jaoks):

add-apt-repository universe

Paigaldage vajalikud alusrakendused (sõltuvused):

apt-get install ruby ruby-dev libsqlite3-dev libssl-dev pkg-config cmake libssh2-1-dev libicu-dev zlib1g-dev g++

Lõpuks laaditakse alla Oxidized GIT kaudu:

cd /opt/

git clone https://github.com/ytti/oxidized.git

cd oxidized/

gem install bundler

rake install

Superkasutaja õigustega Oxidized käitamine pole hea mõte. Seetõttu loome kasutaja nimega oxidized, kelle õigustega varundussüsteem käivitatakse:

useradd oxidized

Ja selle kataloogi õigused anname kasutajale oxidized:

chown oxidized:oxidized -R /opt/

Selles etapis on juba võimalik süsteem käivitada ja sisestades brauserisse http://oxi.cnw.ee:8888 saab seda liidest näha. Kuid Oxidized'il on suur puudus: süsteemis pole autentimist. See tähendab, et igaüks saab brauseris avada veebiliidese ja näha kõiki teie võrguseadmete konfiguratsioone. Arendaja tegeleb ainult varundussüsteemiga ja tal pole veel plaanis sellega seotud funktsioone rakendada. [6]

Postfix paigaldamine ja konfigureerimine:

Paigaldame Postfixi

sudo apt install postfix

Muudame Postfix konfiguratsiooni faili *vi /etc/postfix/main.cf* järgmiseks:

myhostname = oxi.cnw.ee # määratakse serveri nimi-domeen

myorigin = oxi.cnw.ee # määratakse serveri nimi-domeen

mydestination = $myhostname, oxi.cnw.ee, localhost.cnw.ee, localhost

relayhost = mail.cnw.ee #ettevõtte e-posti server

inet_interfaces = all

inet_protocols = all [17]

Lisa 3 - Oxidized integreerimine LibreNMSi-ga

Oxidized edaspidine kasutamine sõltub toimivast Oxidized seadistusest, mis juba pärib seadmete konfiguratsioone.

Seadme konfiguratsioonide kuvamiseks LibreNMSi seadmete lehel on vaja ainult järgmist muudatust konfiguratsioonifailis config.php:

$config['oxidized']['enabled'] = TRUE;

$config['oxidized']['url'] = 'http://oxi.cnw.ee:8888';

LibreNMS toetab konfigureerimise versiooni, kui see on seotud Oxidized'iga. Teatavasti töötab see GIT-väljundmooduliga, sellele on vaja lisada järgmise konfiguratsiooni read:

$config['oxidized']['features']['versioning'] = true;

LibreNMS on võimeline Oxidized seadme loendit uuesti laadima. Iga kord, kui seade LibreNMSi lisatakse, on vaja lisada järgmine rida failile config.php.

$config['oxidized']['reload_nodes'] = true; [18]

Ülekirjutuste loomine:

Seadme konfiguratsioonis saab Oxidized sooritada alamvõtmega muudatusi, millele järgneb seadme leidmine ja lõpuks üle kirjutatava väärtuse määratlemine. LibreNMS ei kontrolli nende atribuutide õigsust, vaid edastab need Oxidized-le.

Seadme sobitamiseks saab kasutada *hostname*, *sysname*, *os*, *location*, *sysDescr* või *hardware*, mis sisaldab kas *'match'* võtit ja väärtust või *'regex'* võtit ja väärtust.

Sobitamise järjekord on:

- hostname
- sysname

- sysDescr
- hardware
- os
- location
- ip

Seadme OS-i ja rühmituse sobitamiseks paigutatakse LibreNMS config.php-i järgmine seadistus:

$config['oxidized']['reload_nodes'] = true;

$config['oxidized']['maps']['group']['os'][] = array('match' => 'ios', 'group' => 'CNW-CISCO');

$config['oxidized']['maps']['group']['os'][] = array('match' => 'junos', 'group' => 'CNW-JUNIPER'); [18]

Oxidized konfiguratsioon integreerimise jaoks:

Oxidized toetab seadmete sisenemist API kaudu, Oxidized tugi on LibreNMS API-le lisatud.

Oxidized konfiguratsioonis on vaja seadmete jaoks seadistada vaikimisi sertifikaadid. LibreNMS ei paku praegu kaugseadistuse sertifikaate.

Lisatakse järgmine info /opt/oxidized/.config/oxidized/config

username: username

password: password

model: cisco

resolve_dns: true

interval: 1800

use_syslog: false

debug: false

threads: 30

timeout: 20

retries: 2

prompt: !ruby/regexp /^([\w.@-]+[#>]\s?)$/

rest: 192.168.55.56:8888

next_adds_job: false

vars: {}

pid: "/opt/oxidized/.config/oxidized/pid"

crash:

directory: "/opt/oxidized/.config/oxidized/crashes"

hostnames: false

stats:

history_size: 10

input:

default: ssh, telnet

debug: false

ssh:

secure: false

ftp:

```
  passive: true
 utf8_encoded: true
# võrguseadme salvestamine GIT repositooriumisse
output:
 default: git
 git:
  user: oxidized
  email: noc@cnw.ee
  repo: "~/devices.git"
# Oxidized ja LibreNMS integreerimine API abil
source:
 default: http
 debug: flase
 http:
  url: http://librenms.cnw.ee/api/v0/oxidized
  map:
   name: hostname
   model: os
   group: group
  headers:
   X-Auth-Token: 'c9b569a9cd90b4396dec43aa7f3a1e61'
model_map:
```

```
  cisco: ios

  juniper: junos

hooks:

  export_git_to_file:

    type: exec

    events: [post_store]

    cmd: 'git archive master --remote ${OX_REPO_NAME}  ${OX_NODE_NAME} | tar -x -C /opt/oxidized/configs'

    async: true

    timeout: 300

# Konfiguratsiooni muudatus e-posti teel
 email_output:

    type: exec

    events: [post_store, node_fail]

    cmd: 'echo -e "From: ConfigDiff<oxi@cnw.ee>\nTo: 'noc@cnw.ee`\nSubject: Config diff for ${OX_NODE_NAME}\nMIME-Version: 1.0\nContent-Type: text/html; charset=utf-8\n\n" > /tmp/${OX_NODE_NAME}; /opt/oxidized/.config/oxidized/extra/oxidized-report-git-commits | tr -d \\r | colordiff | ansi2html >> /tmp/${OX_NODE_NAME}; msmtp < /tmp/${OX_NODE_NAME}; rm /tmp/${OX_NODE_NAME}'

    async: true

    timeout: 40

# Igal grupil on oma kasutajatunnus

groups:
```

CNW-CISCO:

username: getconfig

password: MajaKusOnKala!

CNW-JUNIPER:

username: getconfig

password: MajaKusOnKala!

models: {} [18]