

Hoe kan LibreNMS optimaal worden ingezet om netwerkstoringen binnen een schoolnetwerk tijdig te detecteren en automatisch alerts te versturen.

Optionele ondertitel.

Liam Dewinter.

Scriptie voorgedragen tot het bekomen van de graad van
Professionele bachelor in de toegepaste informatica

Promotor: Bert Van Vreckem

Co-promotor: Merlijn Nimmegeers

Academiejaar: 2024–2025

Eerste examenperiode

Departement IT en Digitale Innovatie .

**HO
GENT**

Woord vooraf

Tijdens mijn studie in Toegepaste Informatica heb ik altijd een sterke interesse gehad in Monitoring, en deze bachelorproef was hielp om me er verder in te verdiepen. Het onderwerp sprak me aan omdat het een actueel en relevant thema is. Het onderzoek en het schrijven van deze bachelorproef waren dan ook een leerzame en boeiende ervaring.

Dit werk had ik echter niet kunnen voltooien zonder de hulp en steun van verschillende mensen. Allereerst wil ik mijn promotor, Bert Van Vreckem, bedanken voor zijn begeleiding, waardevolle feedback en ondersteuning. Zijn inzichten en adviezen hebben me geholpen om deze bachelorproef grondig en effectief af te ronden.

Daarnaast ben ik ook mijn co-promotors, Ricky Leybaert en Merlijn Nimmegeers, dankbaar voor hun begeleiding en kritische blik. Hun advies en suggesties waren van grote meerwaarde voor het uitwerken van dit onderzoek.

Tot slot wil ik iedereen die, op welke manier dan ook, heeft bijgedragen aan dit werk, van harte bedanken. Hopelijk biedt deze bachelorproef een waardevolle bijdrage aan het vakgebied en is het voor de lezer even boeiend als het voor mij was om eraan te werken.

Samenvatting

Deze bachelorproef onderzoekt de mogelijkheden van monitoringopties met LibreNMS binnen een schoolnetwerk. Het doel is om een systeem op te zetten dat alerts genereert wanneer switches of andere netwerkapparaten uitvallen. Een goed functionerend monitoring- en waarschuwingssysteem is cruciaal binnen een schoolomgeving, waar een stabiel netwerk essentieel is voor zowel lesgeven als administratieve taken. Mogelijks zijn er dergelijke extra's die toegepast kunnen worden.

De centrale onderzoeksvraag luidt: "Hoe kan LibreNMS optimaal worden ingezet om netwerkstoringen binnen een schoolnetwerk tijdig te detecteren en automatisch alerts te versturen?" De doelstelling is om een betrouwbare en efficiënte monitoringoplossing te ontwikkelen die IT-beheerders snel op de hoogte brengt van problemen, zodat ze sneller kunnen ingrijpen en downtime wordt geminimaliseerd. Dit is op een school zeer belangrijk wegens een bijna constante vraag naar een werkend netwerk.

Om dit te onderzoeken, wordt de volgende methodologie gehanteerd:

Inventarisatie – Eerst wordt de huidige netwerkinfrastructuur in kaart gebracht en worden bestaande monitoringoplossingen geanalyseerd (indien aanwezig). Lokale testomgeving – Vervolgens wordt de LibreNMS geconfigureerd op een eigen computer om verschillende monitoring- en alertfunctionaliteiten uit te testen. Implementatie en validatie – Tot slot wordt LibreNMS op de schoolserver geïmplementeerd en wordt er getest hoe de alertfuncties werken in een realistische netwerkomgeving. Uit de eerste testresultaten blijkt dat LibreNMS uitgebreide monitoringmogelijkheden biedt, inclusief geavanceerde meldingsopties via e-mail, Slack en andere platformen. De configuratie van alerts vereist echter een grondige afstemming op de specifieke noden van het netwerk, zoals drempelwaarden voor waarschuwingen en de keuze van meldingskanalen.

De resultaten van dit onderzoek zijn relevant voor IT-beheerders in het onderwijs, omdat een goed geconfigureerd monitoring- en alertingsysteem bijdraagt aan snellere probleemdetectie en minder downtime. In de conclusie worden er aanbevelingen over de optimale instellingen voor alerts binnen een schoolomgeving geformuleerd.

Inhoudsopgave

Lijst van figuren	vii
Lijst van tabellen	viii
Lijst van codefragmenten	ix
1 Inleiding	1
1.1 Probleemstelling	1
1.2 Onderzoeksvraag	1
1.3 Onderzoeksdoelstelling	2
1.4 Opzet van deze bachelorproef	2
2 Stand van zaken	3
2.1 Hoofdstuk 1	3
2.1.1 Netwerkmonitoring in het onderwijs	3
2.1.2 Huidige softwareoplossingen voor netwerkmonitoring in scholen	3
2.1.3 Open-source monitoringtools: focus op LibreNMS	4
2.1.4 Functionaliteiten van LibreNMS	5
2.1.5 Architectuur en Begrippen	5
2.1.6 Ondersteunde protocollen	6
2.1.7 Integraties en Uitbreidbaarheid	6
2.1.8 De toestand van schoolnetwerken	7
2.1.9 Verouderde HP ProCurve-switches	7
2.1.10 Uitdagingen en Open Vragen	7
2.1.11 Verschil in onderzoek	7
2.2 Hoofdstuk 2	8
2.2.1 Inventarisatie van de school	8
2.3 Hoofdstuk 3	11
2.3.1 Benodigde Software voor een Lokale Installatie van LibreNMS	11
2.3.2 Aanmaken van de Virtuele Machine	12
2.3.3 Installatie van Ubuntu Server in de Virtuele Machine	13
2.3.4 Installatie van VirtualBox Guest Additions	15
2.3.5 Installatie van LibreNMS via Docker	15
2.3.6 Eerste apparaat toevoegen en controleren van de poller	18

2.4	Hoofdstuk 4.	21
2.4.1	Doelstellingen.	21
2.4.2	Monitoring van de infrastructuur	21
2.4.3	Gebruik van groepen en labels.	24
2.4.4	Alerting en meldingen	24
2.4.5	Logging en rapportage.	24
2.4.6	Toekomstige uitbreidingen	25
3	Methodologie	26
3.1	Literatuurstudie	26
3.2	Inventarisatie van het schoolnetwerk.	26
3.3	Lokale installatie en testfase.	27
3.4	Implementatie in het schoolnetwerk	27
4	Conclusie	28
A	Onderzoeksvoorstel	29
A.1	Inleiding	29
A.2	Literatuurstudie	30
A.2.1	Netwerkmonitoring en logging	30
A.2.2	Monitoringbehoeften in scholen.	30
A.2.3	Huidige softwareoplossingen voor netwerkmonitoring in scholen.	31
A.2.4	Uitdagingen en Open Vragen	31
A.2.5	Verschil in onderzoek	32
A.3	Methodologie	32
A.4	Verwacht resultaat, conclusie	32

Lijst van figuren

2.1	Inventarisatie	8
2.2	Inventarisatie	9
2.3	Inventarisatie	10
2.4	VM	13
2.5	Ubuntu	14
2.6	Docker installeren	17
2.7	Docker Verifiëren	18
2.8	Libre Pull	19
2.9	Add device	22
2.10	Dashboard device	23

Lijst van tabellen

Lijst van codefragmenten

1

Inleiding

1.1. Probleemstelling

In een schoolomgeving is een betrouwbaar netwerk nodig voor zowel het lesgeven als administratieve processen. Maar netwerkstoringen, zoals het onverwacht uitvallen van switches of andere netwerkapparatuur, kunnen voor aanzienlijke problemen zorgen. Momenteel ontbreekt in veel scholen een geautomatiseerd systeem dat netwerkbeheerders onmiddellijk waarschuwt bij dergelijke storingen, waardoor de hersteltijd langer is en de impact groter kan zijn.

De doelgroep van dit onderzoek bestaat uit IT-beheerders in het onderwijs, specifiek de netwerkverantwoordelijken binnen scholen die gebruikmaken van LibreNMS of op zoek zijn naar een monitoringoplossing. Dit onderzoek is ook relevant voor scholen met een groeiende IT-infrastructuur die willen investeren in een proactief netwerkbeheer.

Wegens dat de school al een LibreNMS server had om netwerkcomponenten te monitoren en dat deze ook het meest populaire is voor het monitoren van switches, ap's enzovoort, werk ik verder op de LibreNMS server die de school had. De IT-beheerders weten weinig over de LibreNMS en daarbij zal deze bachelorproef te hulp schieten.

1.2. Onderzoeksvraag

De centrale onderzoeksvraag van deze bachelorproef luidt:

"Hoe kan LibreNMS optimaal worden ingezet om netwerkkerrors binnen een schoolnetwerk tijdig te detecteren en automatisch alerts te versturen?"

Om deze onderzoeksvraag te beantwoorden, worden de volgende deelvragen onderzocht:

Welke componenten moeten worden gemonitord om kritieke storingen snel te detecteren? Welke meldingsmethoden zijn het meest geschikt binnen een schoolom-

geving? Hoe kan LibreNMS geconfigureerd worden om monitoring en alerts zo efficiënt mogelijk te maken?

1.3. Onderzoeksdoelstelling

Deze bachelorproef heeft als doel een proof-of-concept te ontwikkelen voor een effectief monitoring- en alertingssysteem met LibreNMS. De belangrijkste criteria voor succes zijn:

Een werkende configuratie van LibreNMS die netwerkcomponenten binnen een schoolomgeving monitort. Een betrouwbaar alertsysteem dat IT-beheerders tijdig waarschuwt bij storingen. Documentatie en aanbevelingen over de optimale instellingen voor netwerkmonitoring binnen scholen. Door deze doelstellingen te realiseren, draagt het onderzoek bij aan een verbeterde netwerkstabiliteit binnen scholen en een efficiënter beheer van IT-infrastructuur.

1.4. Opzet van deze bachelorproef

De rest van deze bachelorproef is als volgt opgebouwd:

In Hoofdstuk 2 wordt een overzicht gegeven van de stand van zaken binnen het onderzoeksdomein, op basis van een literatuurstudie over netwerkmonitoring, LibreNMS en relevante implementaties in scholen.

In Hoofdstuk 3 wordt de methodologie toegelicht. Hier worden de verschillende onderzoekstechnieken en stappen besproken die zijn genomen om een antwoord te formuleren op de onderzoeksvragen, waaronder de inventarisatie, lokale testomgeving en implementatie op de schoolserver.

In Hoofdstuk 4, wordt de conclusie geformuleerd en een antwoord gegeven op de onderzoeksvragen. Er worden ook aanbevelingen gedaan voor toekomstige verbeteringen en mogelijke verdere optimalisaties binnen netwerkmonitoring voor scholen.

2

Stand van zaken

Dit hoofdstuk zal de literatuurstudie beschrijven en de informatie vergaren van onderwerpen die linken met deze onderzoeksvraag.

2.1. Hoofdstuk 1

Dit hoofdstuk zal de literatuurstudie beschrijven en de informatie vergaren van onderwerpen die linken met deze onderzoeksvraag.

2.1.1. Netwerkmonitoring in het onderwijs

De nood aan een stabiele en betrouwbare netwerkverbinding binnen onderwijsinstellingen is de laatste jaren aanzienlijk toegenomen door de digitalisering van het lesgeven, administratieve processen en evaluatie-instrumenten **devriendt2022ictbeleid**. Toch blijkt uit onderzoek van De Vreese et al. (2021) dat veel Vlaamse scholen kampen met onvoldoende zichtbaarheid op de status van hun netwerkkapparatuur, wat leidt tot trage detectie van storingen en onnodige downtime **devreese2021zichtbaarheid**. Volgens De Wilde (2020) is proactieve monitoring een cruciaal aspect binnen modern netwerkbeheer, waarbij automatische waarschuwingssystemen en realtime logging netwerkbeheerders toelaten sneller op incidenten te reageren en herhaaldelijke problemen structureel aan te pakken **dewilde2020proactief**. In scholen ontbreekt echter vaak de technische kennis of tijd om complexe monitoringoplossingen te implementeren.

2.1.2. Huidige softwareoplossingen voor netwerkmonitoring in scholen

LibreNMS

LibreNMS is een netwerkanalysetool waarmee netwerkverkeer kan worden gedetecteerd en geanalyseerd. Het biedt uitgebreide functionaliteit voor netwerkmoni-

toring en is vooral geschikt voor het monitoren van virtuele netwerken. LibreNMS ondersteunt het automatisch ontdekken van netwerkapparaten, het verzamelen van prestatiegegevens en het instellen van waarschuwingen bij ongebruikelijke netwerkactiviteit. Dit maakt het een nuttige tool voor het uitvoeren van diepgaande analyses van netwerkgedrag, vooral tijdens piekmomenten waar de belasting op virtuele netwerken kan toenemen. (**LibreNMS2025**)

Prometheus + Grafana

Vaak gebruikt in combinatie voor real-time monitoring van netwerkprestaties. Prometheus verzamelt gegevens over netwerkverkeer, terwijl Grafana deze gegevens visualiseert. (**Pragathi2024**)

PRTG (Paessler Router Traffic Grapher)

PRTG is een platform voor netwerkmonitoring en data-analyse dat specifiek is ontworpen om netwerkverkeer in gedetailleerd formaat te verzamelen en te visualiseren. Het biedt tools voor het monitoren van zowel fysieke als virtuele netwerken en kan helpen bij het identificeren van verkeersopstoppingen, performanceproblemen en hardwarestoringen. PRTG biedt uitgebreide loggingmogelijkheden en kan waarschuwingen genereren bij ongebruikelijke activiteit, zoals netwerkcongestie of verhoogde latency. Dit maakt het bijzonder nuttig in virtuele netwerken, waar verkeer soms snel kan variëren en invloed kan hebben op de netwerkcapaciteit, vooral tijdens piekmomenten. (**PRTGManual2025**)

Er zijn dus verscheidene tools om aan monitoring en logging te doen in een virtueel netwerk. Er is nog weinig onderzoek gedaan naar logging en monitoring in een schoolomgeving. Maar idealiter wordt er LibreNMS gebruikt voor het monitoren van netwerkcomponenten. Het is gebruiksvriendelijk en niet complex te gebruiken.

2.1.3. Open-source monitoringtools: focus op LibreNMS

LibreNMS is een populaire open-source netwerkmonitoringtool die zich richt op SNMP-gebaseerde monitoring, autodiscovery en flexibele waarschuwingsmechanismen **librenmsdoc**. Dankzij de brede ondersteuning voor uiteenlopende netwerkapparatuur en de lage instapdrempel is het systeem uitermate geschikt voor omgevingen met beperkte IT-middelen, zoals onderwijsinstellingen **janssens2021opensource**. Pieters (2022) voerde een vergelijkende studie uit naar open-source tools zoals LibreNMS, Zabbix en Nagios. Daaruit bleek dat LibreNMS vooral uitblinkt op het vlak van gebruiksvriendelijkheid en out-of-the-box functionaliteiten **pieters2022monitoring**. De visuele weergave van apparaatstatussen, poortactiviteit en interfaceerrors helpt netwerkbeheerders om snel trends en problemen te detecteren. Daarnaast kunnen alerts per e-mail, Teams of Slack worden geconfigureerd op basis van drempelwaarden of statuswijzigingen (bijv. up/down van een switch).

2.1.4. Functionaliteiten van LibreNMS

LibreNMS is ontworpen als een gebruiksvriendelijk netwerkmonitoringsysteem dat ondersteuning biedt voor een breed scala aan protocollen en apparaten. De kernfunctionaliteiten zijn:

- **Automatische apparaatdetectie:** LibreNMS detecteert automatisch netwerkapparaten via SNMP, LLDP, CDP en andere netwerkprotocollen.
- **Visualisatie via grafieken:** De tool maakt gebruik van RRDTool voor het genereren van tijdreeksdata in grafiekvorm, waarmee trends zoals netwerkverbruik en CPU-belasting in kaart worden gebracht.
- **Waarschuwingsmeldingen (Alerting):** Er kunnen geavanceerde regels opgesteld worden die meldingen genereren bij het overschrijden van drempelwaarden.
- **REST API en integraties:** Gebruikers kunnen gegevens exporteren naar externe tools zoals Grafana, of automatiseren via de API.
- **Configuratieback-up (via Oxidized):** LibreNMS kan switchconfiguraties automatisch opslaan via integratie met Oxidized.

Volgens de officiële documentatie is het doel van LibreNMS om een eenvoudig te gebruiken maar toch krachtige monitoringtool te bieden **librenmsdocs**.

2.1.5. Architectuur en Begrippen

Poller

De poller is verantwoordelijk voor het periodiek ophalen van statistieken van gemonitorde apparaten. Dit gebeurt meestal via het SNMP-protocol. De poller leest data zoals interface-verkeer, CPU-gebruik, opslagcapaciteit en temperatuur, en slaat deze op in RRD-databases en de MySQL/MariaDB-backend **librenmsdocs**. In grootschalige omgevingen kan men gebruik maken van *distributed polling*, waarbij meerdere pollers samenwerken.

Discovery

Het *discovery*-proces detecteert nieuwe apparaten en interfaces in het netwerk, en actualiseert bestaande gegevens. Het wordt standaard dagelijks uitgevoerd en maakt gebruik van protocollen zoals CDP en LLDP om de netwerktopologie te begrijpen **meijerblommers**.

Scheduler

LibreNMS maakt gebruik van cronjobs om taken te plannen, zoals polling, discovery en housekeeping-taken. De scheduler coördineert het tijdig uitvoeren van deze processen en zorgt voor een optimale verdeling van resources.

Protocol Functie

SNMP Apparaten polleren

ICMP Ping checks voor bereikbaarheid

LLDP / CDP Topologiedetectie

Syslog Verzameling van logdata

OSPF / BGP Routinginformatie verzamelen

Alerting Engine

De alerting engine maakt gebruik van een rule-based systeem waarmee complexe logica mogelijk is. Alert-notificaties kunnen via verschillende kanalen verzonden worden zoals e-mail, Slack, Discord of webhooks. In het geval van atheneum zal dat via E-mail zijn of misschien Teams.

Device Groups

Met *Device Groups* kunnen apparaten gegroepeerd worden op basis van gemeenschappelijke kenmerken (bijv. locatie, apparaat-type). Dit maakt het eenvoudiger om specifieke alerts toe te passen of rapporten te genereren per groep. De school atheneum Dendermonde heeft een sterke vraag naar ordening ten opzichte van locatie.

2.1.6. Ondersteunde protocollen

LibreNMS ondersteunt een brede waaier aan protocollen die essentieel zijn voor netwerkdiagnostiek:

Deze protocolondersteuning maakt LibreNMS geschikt voor netwerken met apparatuur van uiteenlopende leveranciers (Cisco, HP, MikroTik, Ubiquiti, enz.).

2.1.7. Integraties en Uitbreidbaarheid

LibreNMS is uitbreidbaar via:

- **Grafana** (via InfluxDB of Prometheus)
- **Oxidized** voor configuratiebeheer
- **Weathermap-plugin** voor visuele netwerktopologie
- **Custom plugins** via de community

Deze uitbreidbaarheid maakt LibreNMS geschikt voor zowel kleine schoolnetwerken als grootschalige enterprise-omgevingen. Maar in dit geval dus een middel-grote schoolnetwerk.

2.1.8. De toestand van schoolnetwerken

De infrastructuur in veel scholen is organisch gegroeid en niet altijd ontworpen met schaalbaarheid of betrouwbaarheid in gedachten. De Vlamo-studie uit 2023 wees uit dat bijna 40% van de onderzochte scholen nog werkt met unmanaged switches of verouderde apparaten zonder centrale logging **vlamo2023netwerken**. Dit maakt troubleshooting tijdrovend en inefficiënt.

Daarnaast ontbreekt het vaak aan centrale configuratie of netwerksegmentatie, waardoor fouten in één deel van het netwerk grote gevolgen kunnen hebben voor het hele schoolgebouw. Monitoring en logging zijn in deze context essentieel om snel te kunnen reageren bij incidenten en het netwerk veerkrachtiger te maken.

2.1.9. Verouderde HP ProCurve-switches

Veel scholen gebruiken nog steeds HP ProCurve-switches uit de 2500-, 2600- of 2800-series. Deze toestellen staan bekend om hun robuustheid en lange levensduur, maar hebben beperkte ondersteuning voor moderne beheertools. Toch ondersteunen de meeste modellen wel het SNMP-protocol, waardoor basisintegratie met monitoringtools zoals LibreNMS mogelijk is **hpmanual**.

Van Looveren (2021) stelt echter dat bij oudere switches vaak belangrijke SNMP-instellingen zoals community strings of interface-namen niet correct geconfigureerd zijn, waardoor monitoring slechts gedeeltelijk werkt **vanlooveren2021switches**. Een grondige inventarisatie en configuratie van deze switches is noodzakelijk om betrouwbare monitoringdata te verkrijgen.

2.1.10. Uitdagingen en Open Vragen

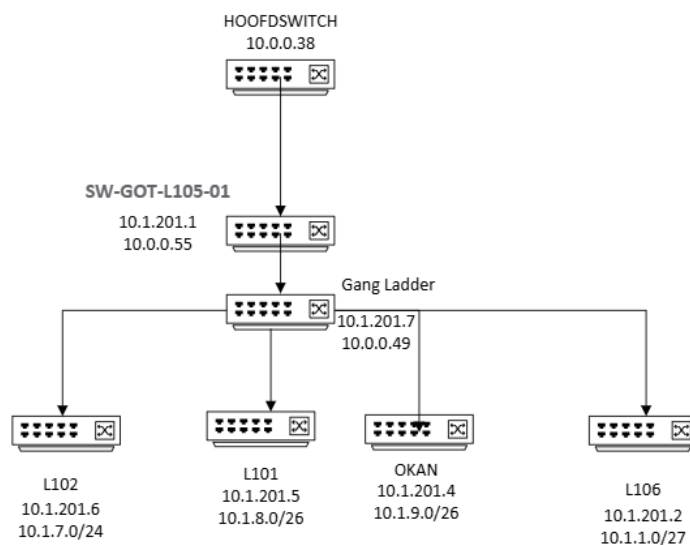
Schaalbaarheid van oplossingen: Scholen kunnen te maken krijgen met pieken in het aantal apparaten dat verbinding maakt met het netwerk, vooral tijdens het begin van schooldagen of leswissels. Is er een tool die goed inspeelt op een netwerk met Virtual SmartZone om piekmomenten te monitoren en loggen? **(BashirEtAl2022)**

Integratie met cloud-applicaties: Met de opkomst van cloudgebaseerde onderwijsplatformen, zoals Google Classroom of Microsoft Teams, wordt het moeilijker om netwerkprestaties te meten, vooral wanneer het netwerkverkeer zowel lokaal als in de cloud plaatsvindt. Hoe kunnen tools deze dynamiek effectief monitoren? **(CommScope2025)**

Kosten en middelen: Veel geavanceerde netwerkmonitoringtools, zoals PRTG, kunnen kostbaar zijn voor kleinere scholen met beperkte middelen. Is er een kosteneffectief alternatief die dezelfde mate van controle en inzicht bieden? **(Ruckus2025)**

2.1.11. Verschil in onderzoek

Op onderwijsinstellingen zijn er meestal geen monitoringopties die worden gehanteerd en is er weinig kennis. Deze bechelorproef helpt gebruiksvriendelijk de IT-beheerders van school te helpen met het opzoeken van bottlenecks in het netwerk.



Figuur 2.1: Structuur Leopoldlaan

(PeerJCS2020)

2.2. Hoofdstuk 2

Dit hoofdstuk zal de netwerkstructuur van de gebouwen weergeven in het atheneum dendermonde. Dit is gebouw west, gebouw Go-Talent, en gebouw zwijveke.

2.2.1. Inventarisatie van de school

Dit hoofdstuk geeft een overzicht van de huidige inventarisatie van de school Atheneum Dendermonde. De inventaris omvat alle fysieke en digitale switches, servers andere faciliteiten. Dit overzicht vormt de basis voor verdere analyses en optimalisaties in latere hoofdstukken.

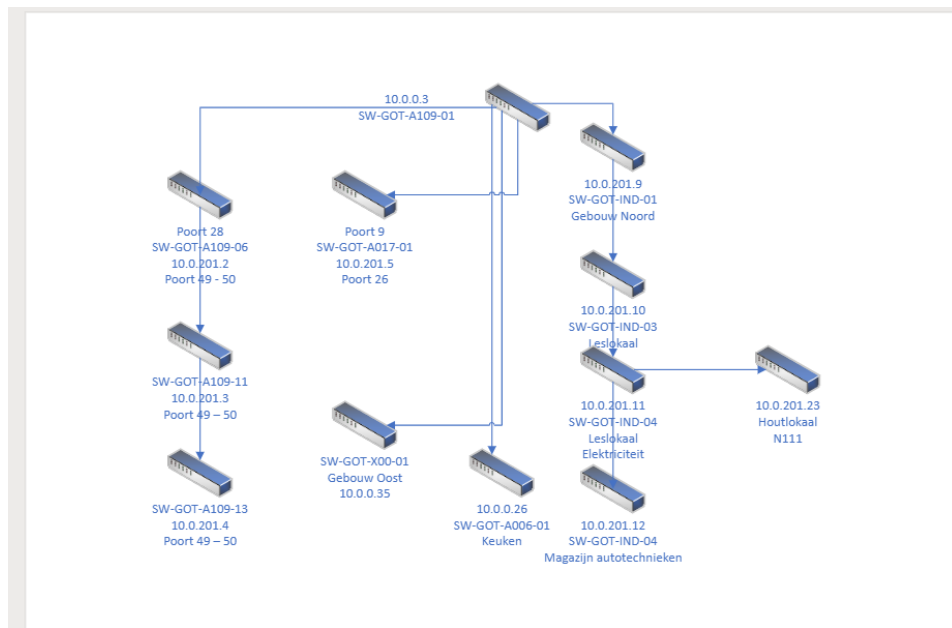
Om te beginnen wordt genoteerd dat Campus Athenea Dendermonde bestaat uit 3 plaatsen. Leopoldlaan, GO Talent en Hoofdgebouw. Elk netwerk is verbonden met de hoofdschicht en watchdog van het Hoofdgebouw. Atheneum Dendermonde krijgt wifi van The Last Mile, die een ISP is.

Leopoldlaan

Hier is een korte beschrijving van de netwerkstructuur de inventarisatie van Leopoldlaan zoals te zien in de figuur 2.1

Hoofdschicht (10.0.0.38): Dit is de centrale switch waar alle andere netwerkcomponenten op aansluiten.

Tussenschicht (SW-GOT-L105-01, 10.1.201.1/10.0.0.55): Fungeert als een backbone-switch die de hoofdverbinding beheert tussen de hoofdschicht en andere verdie-



Figuur 2.2: Structuur Go Talent

pingsswitches.

Gang Ladder Switch (10.1.221.7 / 10.0.0.49): Deze switch verdeelt de verbinding naar de verschillende subnetten of afdelingen.

Verdiepings- en kamernetwerken:

- **L102** (10.1.201.6 / 10.1.7.0/24)
- **L101** (10.1.201.3 / 10.1.80.0/26)
- **OKAN** (10.1.201.5 / 10.1.90.0/26)
- **L106** (10.1.201.2 / 10.1.10.0/27)

Dit toont een hiërarchische netwerkinfrastructuur waarin verschillende afdelingen of ruimtes hun eigen subnet hebben en via switches verbonden zijn met het hoofdnetwerk. Elk heeft natuurlijk ook zijn aantal gebruikers (PC's)

Go Talent

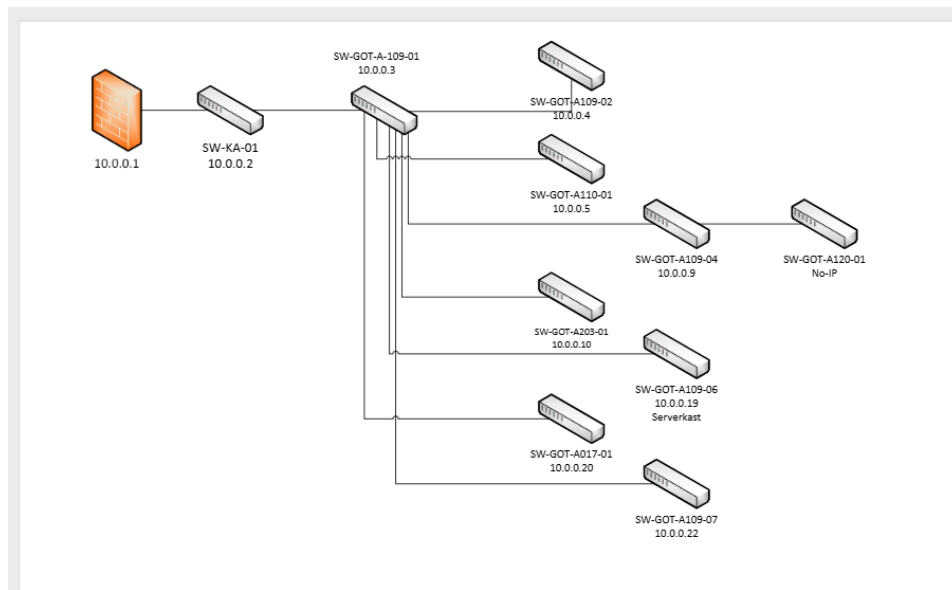
Hier is een korte beschrijving van de netwerkstructuur de inventarisatie van GoTalent zoals te zien in de figuur 2.2

Hoofdschicht (10.0.0.3): Dit is de centrale switch waar alle andere netwerkcomponenten op aansluiten.

Tussenschicht (SW-GOT-A109-01, 10.0.0.3): Fungeert als een backbone-switch die de hoofdverbinding beheert tussen de hoofdschicht en andere verdiepingsswitches.

Netwerkvertakkingen per sectie:

- **A109-netwerk**



Figuur 2.3: Structuur Hoofdgebouw

- SW-GOT-A109-06 (10.0.201.2) - Poorten 49-50
- SW-GOT-A109-11 (10.0.201.3) - Poorten 49-50
- SW-GOT-A109-13 (10.0.201.4) - Poorten 49-50

• **A017-netwerk**

- SW-GOT-A017-01 (10.0.201.5) - Poort 26

• **Oost- en keukenverbindingen**

- SW-GOT-X00-01 (10.0.0.35) - Gebouw Oost
- SW-GOT-A006-01 (10.0.0.26) - Keuken

• **Noord-netwerk en leslokalen**

- SW-GOT-IND-01 (10.0.201.9) - Gebouw Noord
- SW-GOT-IND-03 (10.0.201.10) - Leslokaal
- SW-GOT-IND-04 (10.0.201.11) - Leslokaal Elektriciteit
- SW-GOT-IND-04 (10.0.201.12) - Magazijn Autotechnieken
- Houtlokaal N111 (10.0.201.23)

Hoofdgebouw

Hier is een korte beschrijving van de netwerkstructuur de inventarisatie van Hoofdgebouw zoals te zien in de figuur 2.3

WatchGuard Firewall (10.0.0.1): De WatchGuard firewall fungeert als de beveiligingspoort voor het netwerk en regelt inkomend en uitgaand verkeer.

Hoofdschakel Hoofdgebouw (SW-KA-01, 10.0.0.2): Dit is de centrale switch in het hoofdgebouw, die het verkeer tussen de firewall en de rest van het netwerk beheert.

Hoofdschakel GoTalent (SW-GOT-A109-01, 10.0.0.3): De primaire switch van het GoTalent-netwerk, verantwoordelijk voor de verdeling van netwerkverkeer naar de onderliggende switches.

Netwerkvertakkingen per sectie:

- **A109-netwerk**
 - SW-GOT-A109-02 (10.0.0.4)
 - SW-GOT-A109-04 (10.0.0.9)
 - SW-GOT-A109-06 (10.0.0.19) - Serverkast
 - SW-GOT-A109-07 (10.0.0.22)
- **A110-netwerk**
 - SW-GOT-A110-01 (10.0.0.5)
- **A203-netwerk**
 - SW-GOT-A203-01 (10.0.0.10)
- **A017-netwerk**
 - SW-GOT-A017-01 (10.0.0.20)
- **Externe netwerkkoppeling**
 - SW-GOT-A120-01 - Geen IP toegekend

2.3. Hoofdstuk 3

Dit hoofdstuk zal beschrijven hoe LibreNMS werd opgezet op een lokale testomgeving in Oracle Virtual Box.

2.3.1. Benodigde Software voor een Lokale Installatie van LibreNMS

Voor het lokaal opzetten en testen van LibreNMS wordt een virtuele ontwikkelomgeving aanbevolen. Dit laat gebruikers toe om de volledige monitoring te simuleren zonder een productieomgeving te verstoren. Onderstaande softwarecomponenten zijn vereist:

- **Besturingssysteem (Host):** Windows 10/11. Dit systeem fungeert als basis voor de virtuele omgeving.
- **Oracle VirtualBox:** Virtualisatiesoftware die het mogelijk maakt om virtuele machines te draaien op Windows. Beschikbaar via <https://www.virtualbox.org>.

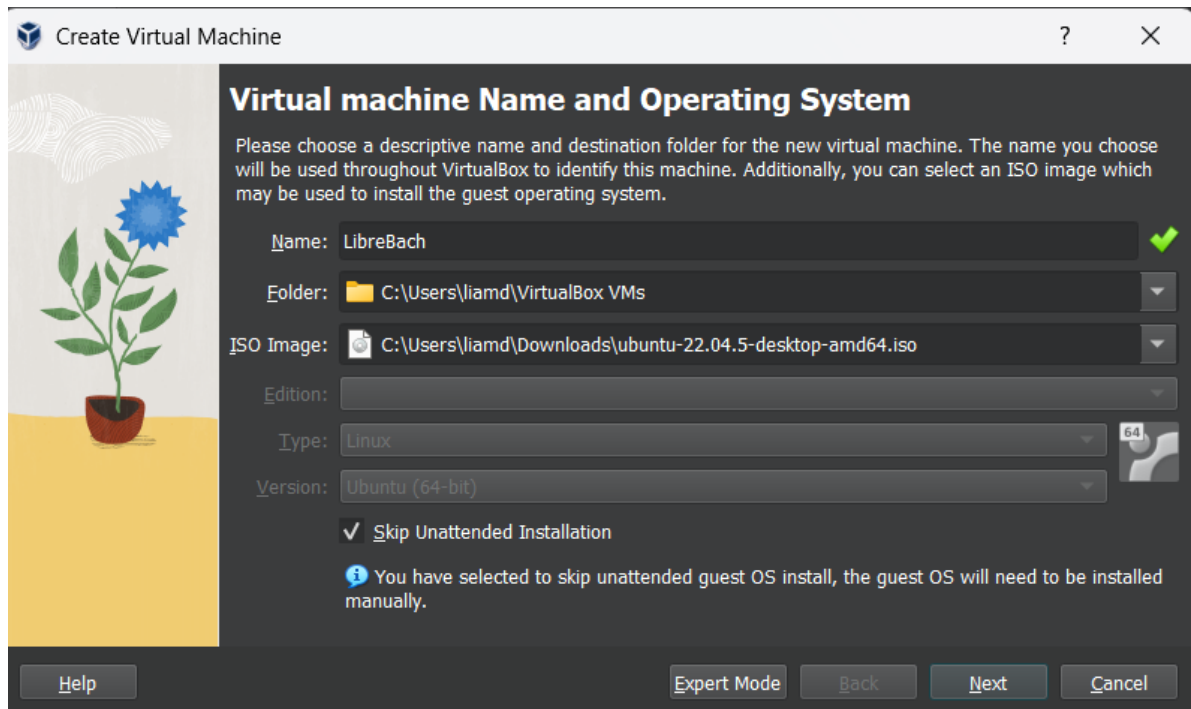
- **Ubuntu Server ISO:** Een minimale versie van Ubuntu (bijvoorbeeld Ubuntu 22.04 LTS) dient als gastbesturingssysteem voor de LibreNMS-installatie. ISO-bestanden zijn beschikbaar via <https://ubuntu.com/download/server>.
- **Docker (optioneel):** Voor gebruikers die liever een containergebaseerde installatie uitvoeren, kan Docker worden gebruikt om LibreNMS en gerelateerde services (MySQL, SNMP, etc.) in geïsoleerde containers te draaien. Docker Desktop is beschikbaar voor Windows via <https://www.docker.com/products/docker-desktop>.
- **LibreNMS Installatiebestanden:** De LibreNMS-code is beschikbaar op GitHub en kan gekloond worden via `git clone https://github.com/librenms/librenms.git`.
- **Aanvullende afhankelijkheden:** Bij installatie op Ubuntu zijn bijkomende componenten vereist zoals Apache/Nginx, PHP, MariaDB/MySQL, SNMP-tools en RRDTool. Deze worden geïnstalleerd via het pakketbeheersysteem `apt`.

Door deze tools te combineren, kan een volledige LibreNMS-omgeving lokaal worden opgezet met minimale kosten en zonder invloed op bestaande netwerkinfrastructuur.

2.3.2. Aanmaken van de Virtuele Machine

De virtuele omgeving werd opgezet via Oracle VirtualBox. Ik koos voor een Ubuntu Server 22.04 LTS ISO als basis. De VM werd aangemaakt met volgende instellingen:

- Geheugen: 4096 MB
- CPU's: 2
- Opslag: 25 GB dynamisch
- Netwerkadapter: NAT

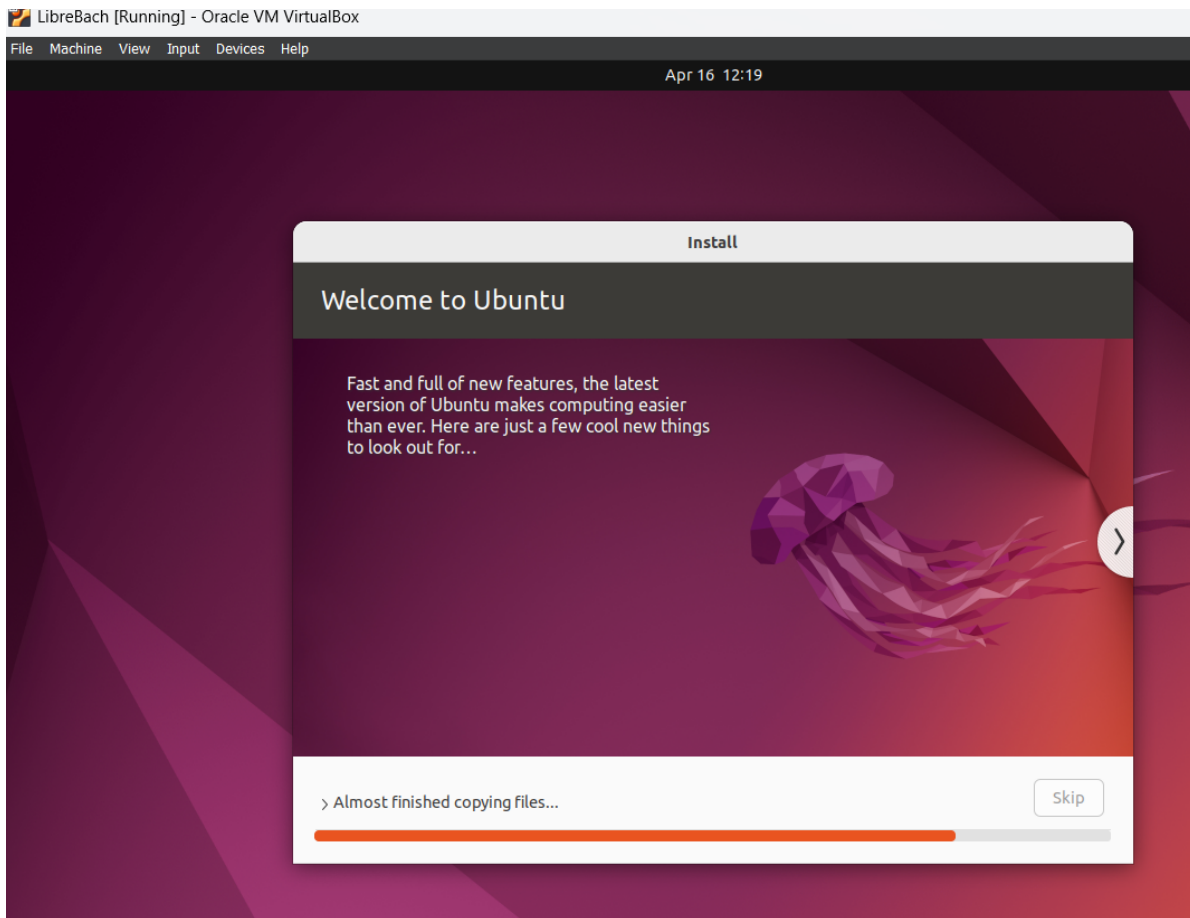


Figuur 2.4: VM Aanmaken

2.3.3. Installatie van Ubuntu Server in de Virtuele Machine

Voor de installatie van LibreNMS werd gebruikgemaakt van **Ubuntu Server 22.04 LTS Desktop Versie**, een stabiel en veelgebruikt Linux-distributie. De installatie gebeurde in een virtuele machine, aangemaakt in Oracle VirtualBox. De installatieprocedure verliep als volgt:

1. Tijdens de installatie werden volgende keuzes gemaakt:
 - Taal: Engels
 - Installatietype: Installeer ubuntu
 - Keyboard Lay-out: Belgisch (alt.)
 - Gebruiker: liam
 - Password: libre
 - Schijfindeling: Gebruik volledige schijf (zonder LVM)
2. De installatie werd voltooid en het systeem werd herstart.



Figuur 2.5: Ubuntu installeren

2.3.4. Installatie van VirtualBox Guest Additions

Om de gebruikerservaring in de virtuele Ubuntu Server-machine te verbeteren, werden de **VirtualBox Guest Additions** geïnstalleerd. Deze zorgen onder andere voor:

- Ondersteuning voor gedeelde klemborden (copy/paste tussen host en gast)
- Ondersteuning voor gedeelde mappen
- Verbeterde muisinteractie en resolutiebeheer

De installatie verliep als volgt:

Stap 1: Guest Additions ISO koppelen

In VirtualBox:

1. Ga naar Apparaat > Insert Guest Additions CD image.
2. Wacht tot de ISO gemount is op de virtuele machine.

Stap 2: Guest Additions installeren

Ga naar de bestandslocatie van Guest Additions en run the linux.run.

```
cd /media/liam/Vbox_GAs_7.0.22
sudo ./VBoxLinuxAdditions.run
```

Stap 3: Herstarten

Na installatie is een herstart aanbevolen:

```
sudo reboot
```

Na de herstart is copy/paste tussen host en gast beschikbaar. In VirtualBox zelf moet de optie Gedeeld klembord > Bidirectioneel geactiveerd zijn.

2.3.5. Installatie van LibreNMS via Docker

In plaats van een klassieke handmatige installatie werd ervoor gekozen om LibreNMS op te zetten via Docker. Deze aanpak vereenvoudigt het installatieproces, maakt het systeem beter reproduceerbaar en verlaagt de afhankelijkheden op het onderliggende besturingssysteem.

Voorbereiding

Docker en Docker Compose werden eerst geïnstalleerd op het Ubuntu Server-systeem:

```
# Docker GPG sleutel
sudo apt-get update
sudo apt-get install ca-certificates curl
```



```

sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/
sudo chmod a+r /etc/apt/keyrings/docker.asc

# Apt bronnen toevoegen
echo \
"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] h
$(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}") stable" | \
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

sudo apt-get update
#Installeer docker
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin do

#Verifieer docker
sudo docker run hello-world

```

Clonen van LibreNMS Docker-omgeving

De officiële LibreNMS Docker-omgeving werd gekloond vanaf GitHub:

```

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

```

Deze repository bevat een kant-en-klaar `docker-compose.yml`-bestand en instructies voor het opstarten van de containeromgeving.

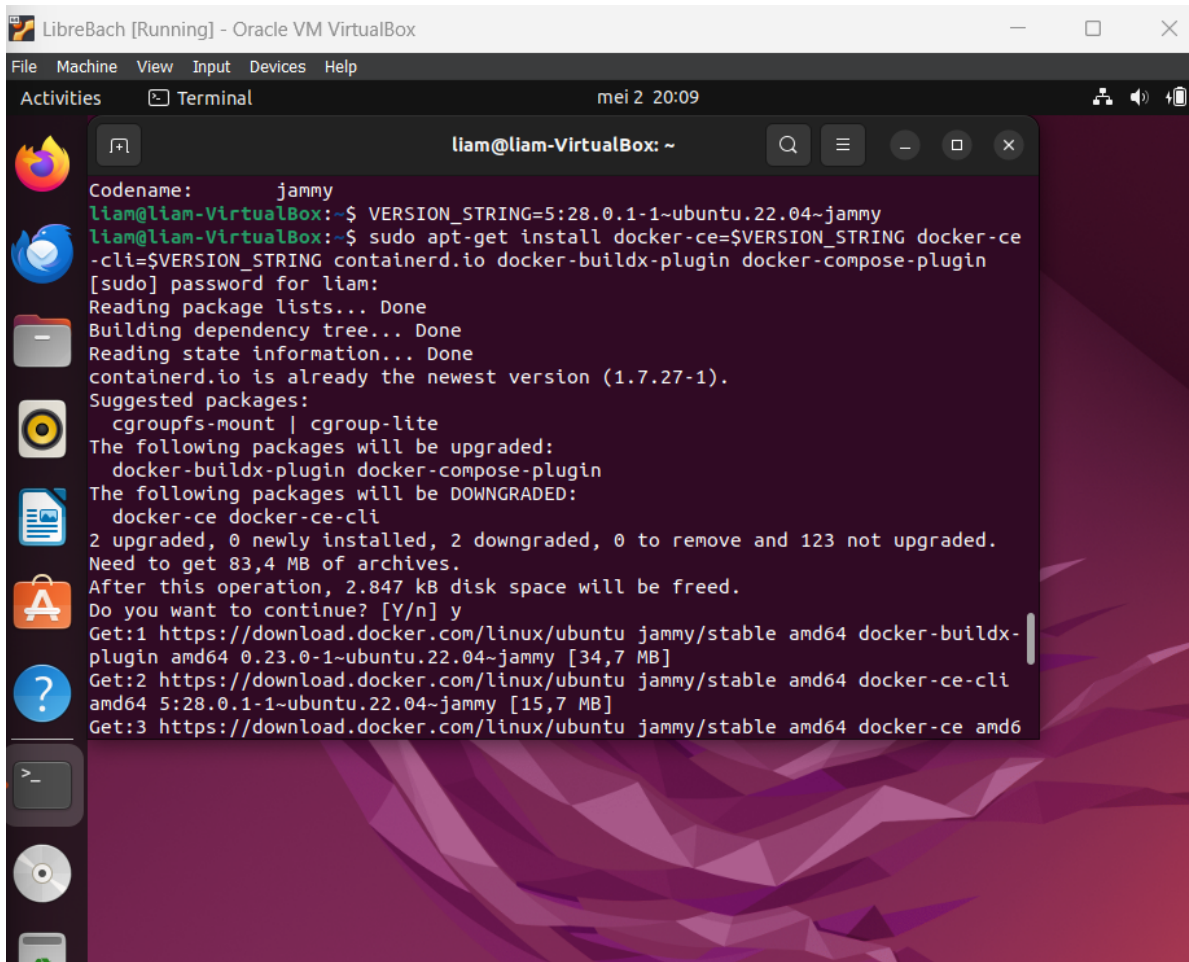
Configuratie en opstart

Na het eventueel aanpassen van instellingen in het `.env`-bestand werd het hele stack gestart via:

```
docker compose up -d
```

Hiermee worden automatisch meerdere containers opgezet:

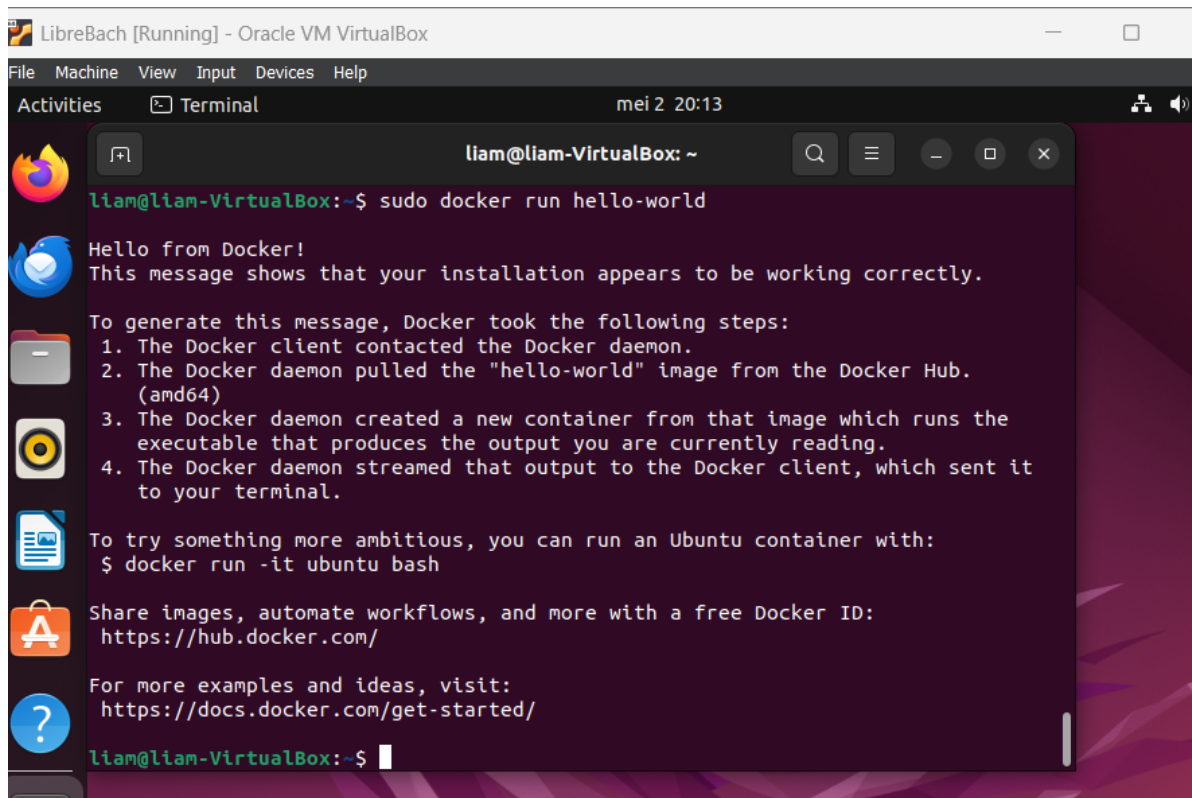
- **librenms**: De hoofdcontainer met de LibreNMS-applicatie
- **mysql**: MariaDB-database
- **memcached**: Voor caching
- **rrdcached**: Opslag van tijdreeksdata
- **syslog-ng**: Logverzameling



The screenshot shows a terminal window titled "liam@liam-VirtualBox: ~" within a LibreBach virtual machine. The user is installing Docker using the command `sudo apt-get install docker-ce=$VERSION_STRING docker-ce-cli=$VERSION_STRING containerd.io docker-buildx-plugin docker-compose-plugin`. The terminal output shows the package lists being read, the dependency tree being built, and the state information being read. It indicates that containerd.io is already the newest version. Suggested packages include cgroupfs-mount and cgroup-lite. The packages to be upgraded are docker-buildx-plugin and docker-compose-plugin, and the packages to be downgraded are docker-ce and docker-ce-cli. The total size of the archives to be downloaded is 83.4 MB, and 2.847 kB of disk space will be freed. The user is prompted to continue with the installation, and they respond with 'y'. The terminal then shows the progress of downloading the Docker packages from the Docker repository.

```
liam@liam-VirtualBox: ~  
Codename: jammy  
liam@liam-VirtualBox:~$ VERSION_STRING=5:28.0.1-1~ubuntu.22.04~jammy  
liam@liam-VirtualBox:~$ sudo apt-get install docker-ce=$VERSION_STRING docker-ce  
-cli=$VERSION_STRING containerd.io docker-buildx-plugin docker-compose-plugin  
[sudo] password for liam:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
containerd.io is already the newest version (1.7.27-1).  
Suggested packages:  
  cgroupfs-mount | cgroup-lite  
The following packages will be upgraded:  
  docker-buildx-plugin docker-compose-plugin  
The following packages will be DOWNGRADED:  
  docker-ce docker-ce-cli  
2 upgraded, 0 newly installed, 2 downgraded, 0 to remove and 123 not upgraded.  
Need to get 83,4 MB of archives.  
After this operation, 2.847 kB disk space will be freed.  
Do you want to continue? [Y/n] y  
Get:1 https://download.docker.com/linux/ubuntu jammy/stable amd64 docker-buildx-  
plugin amd64 0.23.0-1~ubuntu.22.04~jammy [34,7 MB]  
Get:2 https://download.docker.com/linux/ubuntu jammy/stable amd64 docker-ce-cli  
amd64 5:28.0.1-1~ubuntu.22.04~jammy [15,7 MB]  
Get:3 https://download.docker.com/linux/ubuntu jammy/stable amd64 docker-ce amd6
```

Figuur 2.6: Docker installeren



The screenshot shows a terminal window titled 'liam@liam-VirtualBox: ~' with a search bar and window controls. The terminal output is as follows:

```
liam@liam-VirtualBox:~$ sudo docker run hello-world
Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
   (amd64)
3. The Docker daemon created a new container from that image which runs the
   executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it
   to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/
liam@liam-VirtualBox:~$
```

Figuur 2.7: Docker Verifiëren

Toegang tot de webinterface

Na de succesvolle opstart werd LibreNMS toegankelijk via de browser op poort 8000:

<http://<ip-adres-van-de-libre>:8000>

De installatieconfiguratie werd via de webinterface verder afgerond (adminaccount, database-instellingen, enz.).

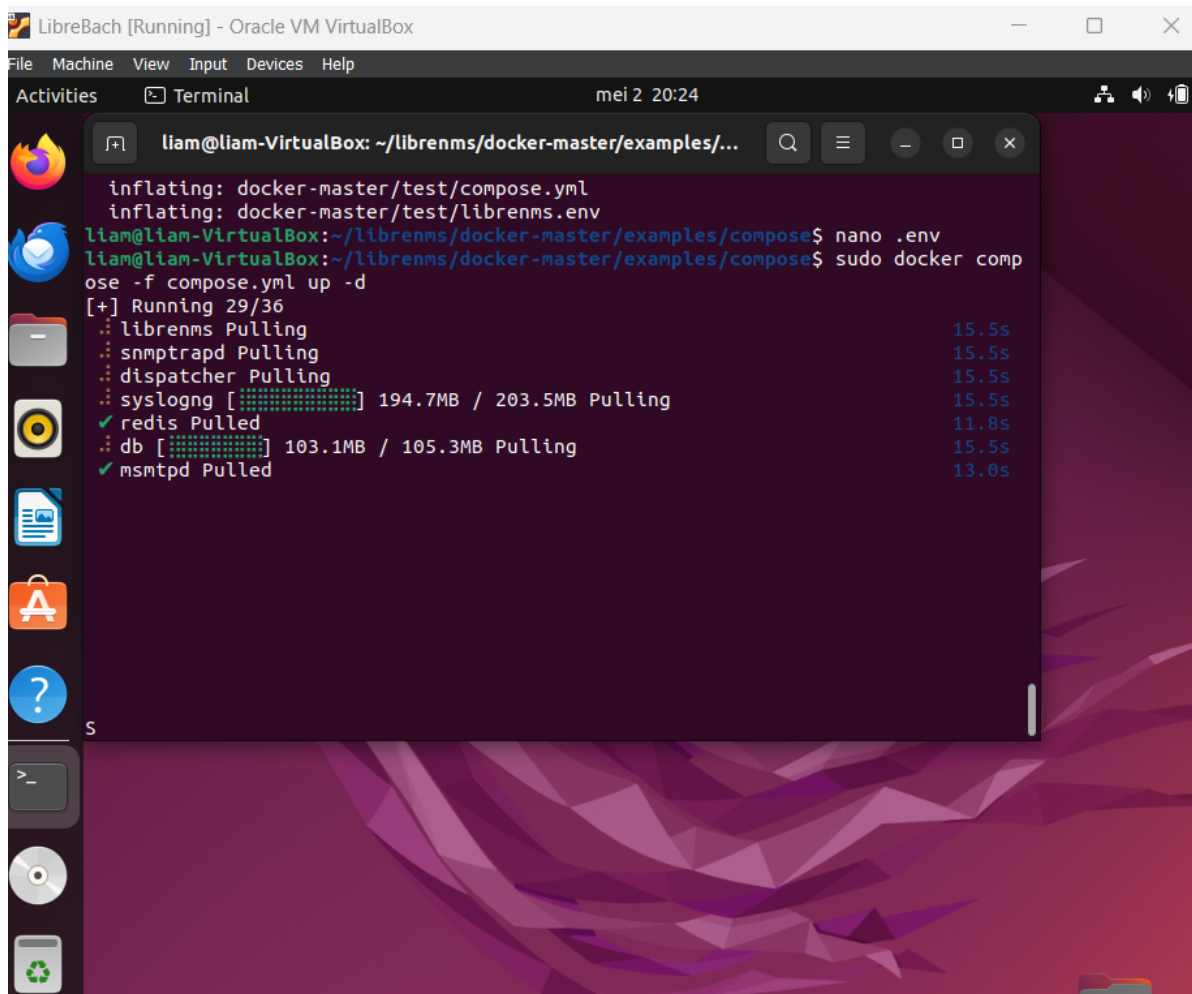
2.3.6. Eerste apparaat toevoegen en controleren van de poller

Nadat LibreNMS succesvol is geïnstalleerd en je bent ingelogd op de webinterface, kan je beginnen met het toevoegen van netwerkkapparaten die je wil monitoren. In deze stap wordt uitgelegd hoe je een apparaat toevoegt, en hoe je controleert of de poller correct functioneert.

Voorwaarden

Voor je een apparaat toevoegt, zorg ervoor dat:

- Het apparaat dat je wil monitoren SNMP geactiveerd heeft en juist geconfigureerd is.
- Het apparaat bereikbaar is vanaf de machine waarop LibreNMS draait.
- Je het IP-adres kent van het apparaat.



The screenshot shows a terminal window titled "liam@liam-VirtualBox: ~/librenms/docker-master/examples/..." with a search bar and window controls. The terminal output shows the process of pulling Docker images for a service named "librenms". The output includes the following lines:

```
inflating: docker-master/test/compose.yml
inflating: docker-master/test/librenms.env
liam@liam-VirtualBox:~/librenms/docker-master/examples/compose$ nano .env
liam@liam-VirtualBox:~/librenms/docker-master/examples/compose$ sudo docker compose -f compose.yml up -d
[+] Running 29/36
  :: librenms Pulling                                15.5s
  :: snmptrapd Pulling                                15.5s
  :: dispatcher Pulling                               15.5s
  :: syslogng [|||||] 194.7MB / 203.5MB Pulling        15.5s
  ✓ redis Pulled                                     11.8s
  :: db [|||||] 103.1MB / 105.3MB Pulling              15.5s
  ✓ msmtpd Pulled                                    13.0s
```

Figuur 2.8: Libre Pull

SNMP installeren en configureren op de host-VM

Om het lokale systeem (bijv. je Ubuntu VM) te kunnen monitoren via LibreNMS, moet SNMP correct geconfigureerd zijn. Volg onderstaande stappen om dit in te stellen:

1. Installeer de benodigde pakketten op de host-VM:

```
sudo apt update
sudo apt install snmp snmpd -y
```

2. Pas de configuratie aan van de SNMP-daemon:

```
sudo nano /etc/snmp/snmpd.conf
```

3. Gebruik deze minimale configuratie:

```
agentAddress udp:161
rocommunity public

sysLocation Host-VM
sysContact liam.dewinter@athenea.be
```

4. Sla het bestand op en herstart de SNMP-dienst:

```
sudo systemctl restart snmpd
```

5. Test of SNMP werkt vanaf de host zelf:

```
snmpwalk -v2c -c public localhost
```

6. (Optioneel) Test vanuit de LibreNMS Docker-container:

```
docker exec -it librenms bash
apt update && apt install -y snmp
snmpwalk -v2c -c public <IP-van-host>
```

Na een geslaagde test kun je het IP-adres van je host-VM gebruiken in de LibreNMS-webinterface bij het toevoegen van een nieuw apparaat. Zorg ervoor dat het IP-adres van de host correct bereikbaar is vanuit de Docker-container. Indien je bridged networking gebruikt of een host-only netwerkadapter in VirtualBox, kun je dit IP meestal vinden met het commando `ip a` op de host-VM.

Apparaat toevoegen via de GUI

1. Navigeer in de LibreNMS webinterface naar **Devices** > **Add Device**.
2. Vul de volgende velden in:
 - **Hostname / IP**: Het IP-adres van het SNMP-apparaat **10.0.2.15**.
 - **SNMP versie**: Kies **v2c**.
 - **Community**: Vul de community string in **public**.
3. Klik op **Add Device**.

LibreNMS zal nu proberen het apparaat te ontdekken via SNMP. Indien succesvol, wordt het apparaat toegevoegd en verschijnen basisgegevens zoals uptime, CPU-belasting en netwerkverkeer binnen enkele minuten.

2.4. Hoofdstuk 4

Nu LibreNMS succesvol lokaal draait, zal deze monitoringtool ingezet worden om het netwerk van de school op een gestructureerde en proactieve manier te bewaken. In dit hoofdstuk wordt uitgelegd welke concrete acties ondernomen worden, welke apparaten gemonitord zullen worden en hoe LibreNMS het beheer van het netwerk zal verbeteren.

2.4.1. Doelstellingen

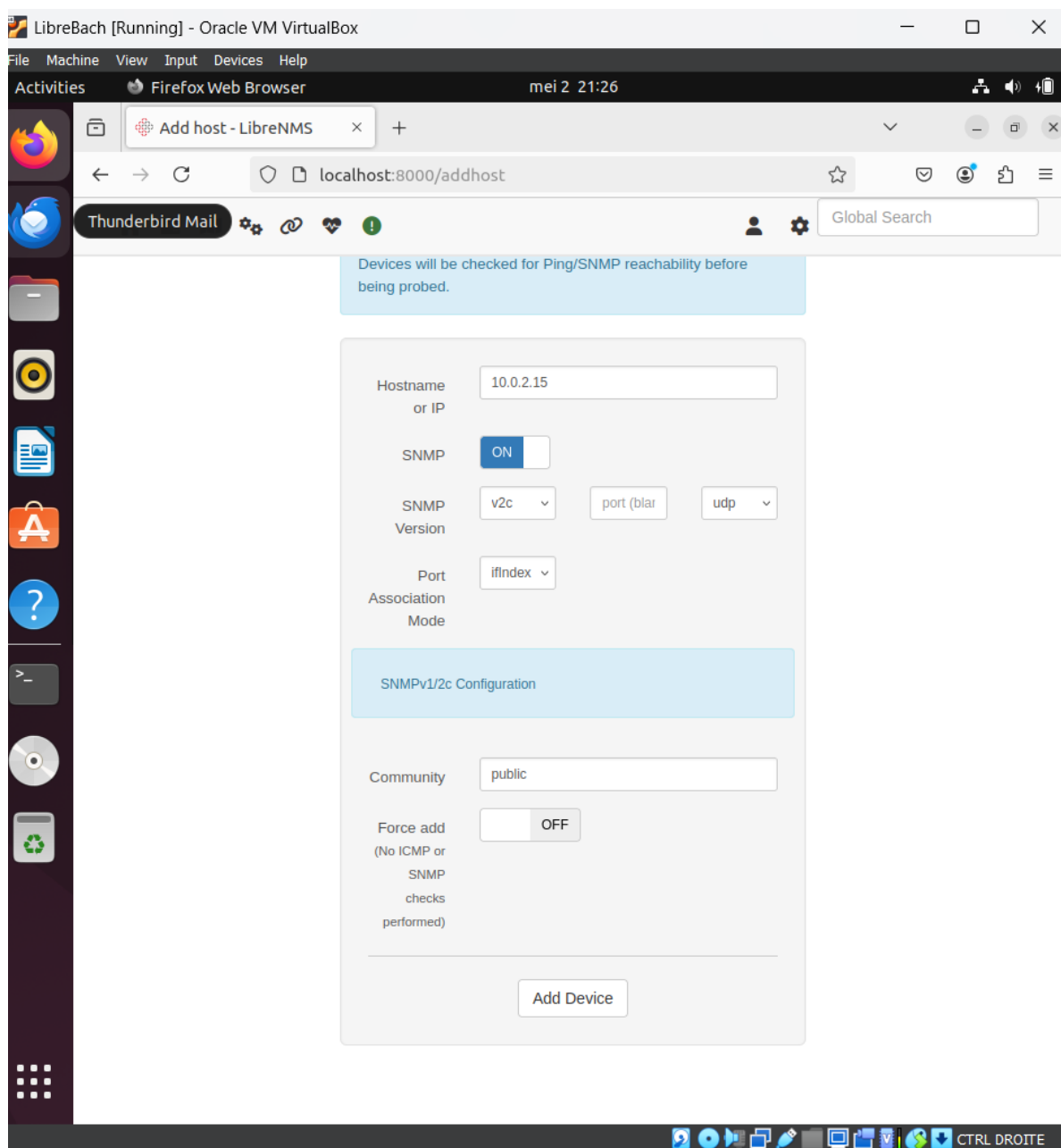
De belangrijkste doelstellingen van de monitoringoplossing zijn:

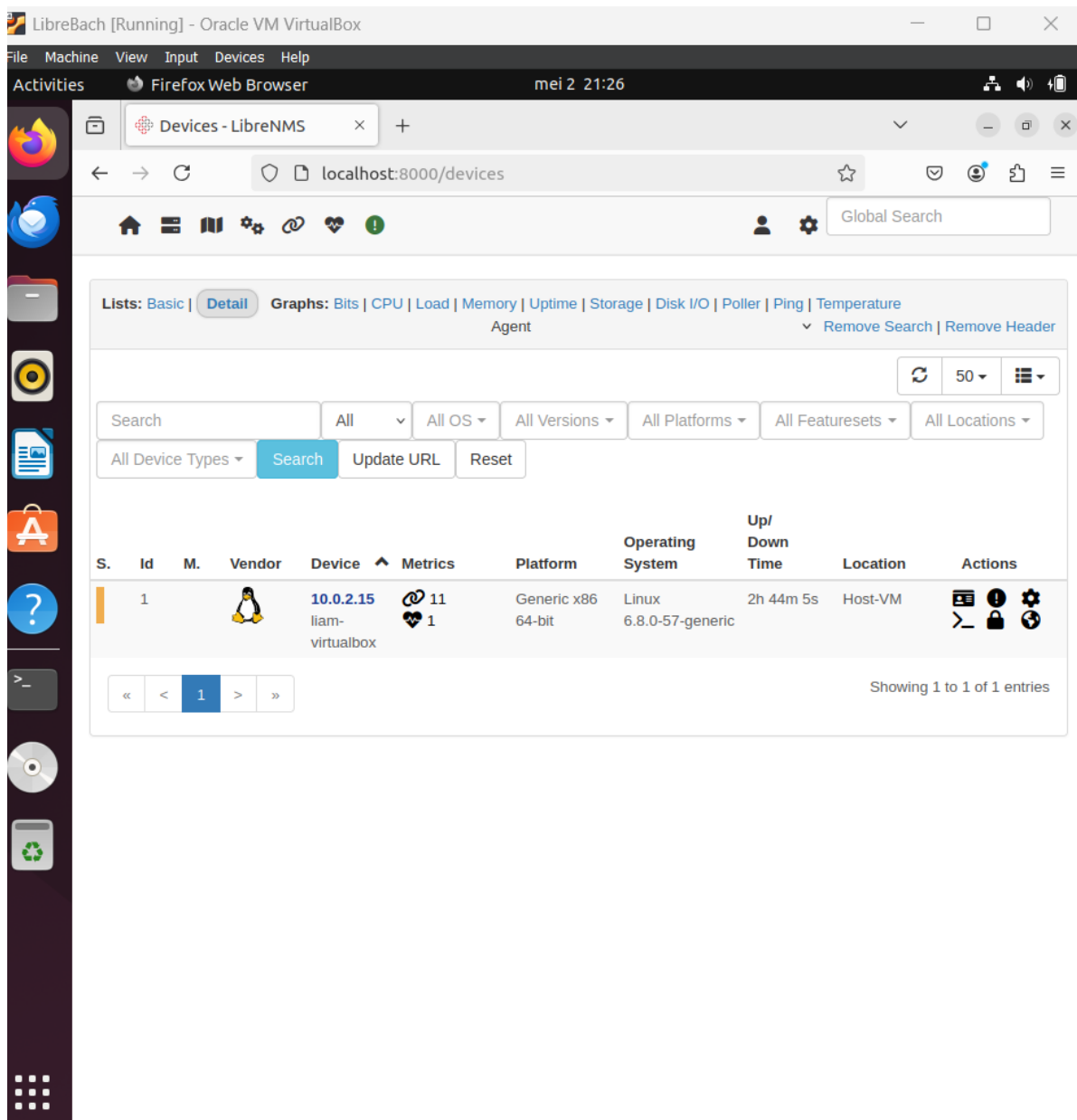
- Detectie van netwerkproblemen voordat gebruikers hiervan hinder ondervinden.
- Het verzamelen van statistieken over netwerkverkeer, CPU-belasting en beschikbaarheid van apparaten.
- Automatische waarschuwingen (alerts) bij storingen of afwijkingen.
- Inzicht krijgen in verouderde of overbelaste infrastructuur.
- Het ondersteunen van toekomstige beslissingen rond netwerkuitbreiding of vervanging.

2.4.2. Monitoring van de infrastructuur

De volgende netwerkcomponenten zullen worden toegevoegd aan LibreNMS:

- **Netwerkswitches** van oudere generaties (o.a. HP ProCurve): via SNMP kunnen de poortstatus, errors en bandbreedte geanalyseerd worden.
- **Access points**: controle van beschikbaarheid en verkeer.

**Figuur 2.9:** Libre Pull

**Figuur 2.10:** Dashboard device

- **Windows- en Linux-servers:** via SNMP, eventueel aangevuld met syslog of agents.
- **Printers:** basisinformatie zoals status en tonerpeil (indien ondersteund via SNMP).
- **Netwerkkapparatuur van Signpost** (indien aanwezig): monitoring van clients, bereikbaarheid en verkeer.

2.4.3. Gebruik van groepen en labels

Om het overzicht te bewaren in de LibreNMS-interface, zullen apparaten worden gegroepeerd op basis van:

- Locatie (bijv. Lokaal 1, Serverlokaal, Bureau administratie).
- Type (bijv. Switches, Access Points, Servers).
- Kriticiteit (bijv. Belangrijk, Niet-kritiek).

Dit maakt het mogelijk om gerichte rapporten of alerts op te stellen per groep.

2.4.4. Alerting en meldingen

De alerting-engine zal geconfigureerd worden om automatisch waarschuwingen te versturen wanneer:

- Een apparaat offline gaat.
- Een bepaalde poort op een switch overbelast raakt.
- De CPU-belasting van een server langdurig hoog is.
- Specifieke drempelwaarden overschreden worden.

Meldingen worden in eerste instantie verzonden via e-mail. Indien mogelijk kan ook integratie met Microsoft Teams of Slack onderzocht worden.

2.4.5. Logging en rapportage

Naast real-time monitoring zal LibreNMS ook gebruikt worden voor logging en historische analyse:

- Verzamelen van SNMP- en syslog-data voor foutopvolging.
- Export van grafieken en trendanalyse per week/maand.
- Inzichten in netwerkgebruik tijdens lesuren vs. pauzes.

2.4.6. Toekomstige uitbreidingen

Op termijn kan LibreNMS worden uitgebreid met:

- Integratie met Grafana voor geavanceerde dashboards.
- Weathermap-plugin voor visuele weergave van de netwerktopologie.
- Back-up van configuraties via Oxidized.
- Scripted alert-response (bv. automatisch herstarten van een AP).

Door deze stappen te volgen wordt LibreNMS een krachtige en schaalbare oplossing voor netwerkbewaking op de school, waarmee zowel technische problemen als lange termijnbeheer ondersteund worden.

3

Methodologie

Dit onderzoek volgt een systematische aanpak om de implementatie van LibreNMS in een schoolnetwerk te analyseren. De werkwijze is onderverdeeld in vier fasen: literatuurstudie, netwerkinventarisatie, lokale installatie en testfase, en ten slotte de implementatie binnen het schoolnetwerk.

3.1. Literatuurstudie

De eerste fase bestaat uit een grondige verkenning van LibreNMS en de bijbehorende functionaliteiten. Er wordt onderzocht:

- Wat LibreNMS is en hoe het zich verhoudt tot andere netwerkmonitoringtools.
- Welke protocollen en technieken LibreNMS ondersteunt (SNMP, syslog, API-integraties).
- De systeemeisen en mogelijke implementatiescenario's.
- Extra functies zoals alerts implementeren

Deze fase biedt een fundament voor de verdere stappen en helpt bij het bepalen van de geschiktheid van LibreNMS voor het schoolnetwerk.

3.2. Inventarisatie van het schoolnetwerk

Voor een succesvolle implementatie is een grondige netwerkinventarisatie noodzakelijk. Hierbij worden:

- De netwerkcomponenten en hun IP-adressen in kaart gebracht.
- De bestaande monitoringmethodes geanalyseerd.
- Toegangsrechten en beveiligingsmaatregelen in rekening gebracht.

Deze stap biedt inzicht in welke apparaten en segmenten van het netwerk geschikt zijn om te monitoren met LibreNMS.

3.3. Lokale installatie en testfase

Om de functionaliteiten van LibreNMS te verkennen, wordt een testomgeving opgezet op een lokale machine. In deze fase wordt:

- De installatieprocedure en configuratie van LibreNMS doorlopen.
- De verschillende methodes van netwerkdetectie en monitoring getest.
- Eventuele foutmeldingen en beperkingen ondervinden.

Deze testfase dient als voorbereiding op de implementatie in het schoolnetwerk en maakt het mogelijk om knelpunten vroegtijdig te identificeren.

3.4. Implementatie in het schoolnetwerk

Na de succesvolle testfase volgt de implementatie van LibreNMS in het schoolnetwerk. Dit omvat:

- Het configureren van SNMP (nodig voor LibreNMS) op de netwerkapparaten.
- Het koppelen van LibreNMS aan de relevante netwerksegmenten.
- Het instellen van meldingen en dashboards voor effectieve monitoring.
- Het uitvoeren van prestatietests en het valideren van de verzamelde data.

Door deze stapsgewijze aanpak wordt inzicht verkregen in de integratie van LibreNMS in een bestaande infrastructuur en worden optimalisaties doorgevoerd waar nodig.

Met deze methodologie wordt een gestructureerde en onderbouwde analyse van de inzetbaarheid van LibreNMS in een schoolomgeving gerealiseerd.

4

Conclusie

Deze studie had als doel de implementatie en bruikbaarheid van LibreNMS binnen het schoolnetwerk te onderzoeken. Door middel van een gestructureerde aanpak, bestaande uit literatuuronderzoek, netwerkinventarisatie en praktische experimenten, werd een diepgaand inzicht verkregen in de mogelijkheden en beperkingen van dit monitoringsysteem.

Uit het literatuuronderzoek bleek dat LibreNMS een uitgebreide en flexibele oplossing biedt voor netwerkmonitoring, met ondersteuning voor een brede schaal aan protocollen en apparatuur. Vervolgens werd een gedetailleerde inventarisatie van het schoolnetwerk gemaakt om een duidelijk beeld te krijgen van de infrastructuur en de benodigde monitoringfuncties.

Door LibreNMS lokaal te installeren en te testen, werd de functionaliteit geëvalueerd en werd inzicht verkregen in de configuratievereisten. Dit leidde tot de implementatie binnen het schoolnetwerk, waar de effectiviteit van LibreNMS in een realistische omgeving werd getest.

De resultaten tonen aan dat LibreNMS een waardevolle tool is voor netwerkbeheer, met uitgebreide visualisatie- en meldingsopties. Bepaalde beperkingen zoals de initiële configuratiecomplexiteit en mogelijke compatibiliteitsproblemen met specifieke hardware zijn er wel.

Deze studie draagt bij aan het vakgebied door een praktijkgericht perspectief te bieden op de inzet van LibreNMS in een educatieve omgeving. Het onderzoek roept tevens nieuwe vragen op, zoals de integratie met andere monitoringtools en de mogelijkheden voor verdere automatisering binnen netwerkbeheer. Verdere studies kunnen zich richten op deze aspecten om de efficiëntie van netwerkmonitoring verder te optimaliseren.



Onderzoeksvoorstel

Het onderwerp van deze bachelorproef is gebaseerd op een onderzoeksvoorstel dat vooraf werd beoordeeld door de promotor. Dat voorstel is opgenomen in deze bijlage.

A.1. Inleiding

Netwerkbeheer is een broodnodig aspect binnen IT-infrastructuren, waarbij het garanderen van een stabiele en efficiënte werking van netwerken een uitdaging vormt. Binnen scholen doen zich regelmatig prestatieproblemen voor tijdens piekmomenten. Deze piekmomenten kunnen leiden tot vertragingen, verbindingsproblemen en verminderde efficiëntie. Er ontbreekt vaak een gestructureerde methode om deze data effectief te analyseren en te gebruiken voor probleemoplossing. (**Nwakeze2023**) Dit onderzoek richt zich specifiek op IT-beheerders en netwerkadministrators die verantwoordelijk zijn voor het beheer van Virtual SmartZone-omgevingen binnen bedrijven en organisaties. Zij ondervinden moeilijkheden bij het detecteren, monitoren en analyseren van terugkerende netwerkproblemen tijdens piekmomenten en willen problemen sneller identificeren. De centrale probleemstelling is dat er onvoldoende inzicht is in de oorzaken van prestatieproblemen binnen een netwerk met een Virtual SmartZone tijdens piekmomenten, doordat logs en meldingen niet optimaal worden benut. (**CommScope2025**) Daarom is dit de centrale onderzoeksvraag van deze bachelorproef: "Hoe kunnen meldingen en logs van piekmomenten in de Virtual SmartZone effectief worden bijgehouden en geanalyseerd om veelvoorkomende problemen te identificeren en te verminderen?" De doelstelling van dit onderzoek is het ontwikkelen van een methode voor het verwerken van logs en meldingen in Virtual SmartZone, waardoor IT-beheerders beter inzicht krijgen in de oorzaken van prestatieproblemen. Om deze doelstelling te bereiken, wordt een toegepaste onderzoeksmethode ge-

bruikt. Eerst wordt een literatuurstudie uitgevoerd naar netwerkmonitoring en loganalyse. Vervolgens wordt een praktijkgerichte case study opgezet binnen het atheneum Dendermonde waar Virtual SmartZone wordt gebruikt. Hierin worden bestaande logs en meldingen geanalyseerd om problemen te identificeren. Op basis van deze analyse wordt een proof-of-concept dashboard ontwikkeld waarmee netwerkbeheerders op een efficiënte manier piekmomenten kunnen monitoren en problemen proactief kunnen aanpakken. (YinEtAl2011) Dit onderzoek biedt een meerwaarde voor IT-beheerders en organisaties die afhankelijk zijn van een goed functionerend netwerk.

A.2. Literatuurstudie

Monitoring en logging zijn cruciale aspecten van netwerkbeheer, vooral in omgevingen waar veel netwerkverkeer plaatsvindt, zoals in het onderwijs. (Aquion2018) De Virtual SmartZone, een cloud-gebaseerd platform voor netwerkbeheer, wordt vaak gebruikt voor het beheren van draadloze netwerken. Het biedt mogelijkheden voor efficiënte toegangspuntenbeheer, apparatenbeheer en het monitoren van netwerkverkeer in real-time. Bij piekmomenten, zoals begin- en eindtijden van schooldagen of tijdens drukke lessen, kunnen netwerken enorm belast worden, wat de noodzaak voor goed geconfigureerde monitoring en logging nog belangrijker maakt. (BashirEtAl2022)

A.2.1. Netwerkmonitoring en logging

Netwerkmonitoring omvat het consistent controleren van de status en prestaties van een netwerk. Het doel is om problemen te identificeren, zoals congestie, onregelmatigheden in het verkeer of netwerkstoringen. Logging is het vastleggen van netwerkgebeurtenissen en prestaties in logbestanden, zodat netwerkbeheerders patronen kunnen analyseren en storingen kunnen terugleiden naar specifieke gebeurtenissen. Monitoring- en loggingtools kunnen worden gebruikt om de prestaties te meten, toegang te controleren en waarschuwingen te genereren bij afwijkingen. (PeerJCS2020)

A.2.2. Monitoringbehoeften in scholen

Beheer van draadloze netwerken: Scholen hebben vaak draadloze netwerken die veel apparaten ondersteunen, van laptops tot tablets en smartphones van leerlingen, docenten en medewerkers. (Ruckus2025) Beveiliging: Scholen hebben te maken met gevoelige gegevens, zoals studentinformatie en onderzoeksdata, die goed moeten worden beschermd tegen inbreuken of misbruik. Gebruik van cloud-gebaseerde applicaties: Veel onderwijsinstellingen maken gebruik van cloudgebaseerde tools en platforms voor onderwijs, zoals Google Classroom, Microsoft Teams, en Office 365. Monitoring moet zich dus niet alleen richten op de lokale infrastructuur, maar ook op cloudgebaseerde toepassingen. (PeerJCS2020) Toegang tot net-

werken tijdens piekmomenten: Het netwerk moet omgaan met grote hoeveelheden gebruikers die gelijktijdig toegang willen krijgen, bijvoorbeeld bij het starten van lesuren of tijdens pauzes. (Aquion2018)

A.2.3. Huidige softwareoplossingen voor netwerkmonitoring in scholen

LibreNMS

LibreNMS is een netwerkanalysetool waarmee netwerkverkeer kan worden gedetecteerd en geanalyseerd. Het biedt uitgebreide functionaliteit voor netwerkmonitoring en is vooral geschikt voor het monitoren van virtuele netwerken. LibreNMS ondersteunt het automatisch ontdekken van netwerkapparaten, het verzamelen van prestatiegegevens en het instellen van waarschuwingen bij ongebruikelijke netwerkactiviteit. Dit maakt het een nuttige tool voor het uitvoeren van diepgaande analyses van netwerkgedrag, vooral tijdens piekmomenten waar de belasting op virtuele netwerken kan toenemen. (LibreNMS2025)

Prometheus + Grafana

Vaak gebruikt in combinatie voor real-time monitoring van netwerkprestaties. Prometheus verzamelt gegevens over netwerkverkeer, terwijl Grafana deze gegevens visualiseert. (Pragathi2024)

PRTG (Paessler Router Traffic Grapher)

PRTG is een platform voor netwerkmonitoring en data-analyse dat specifiek is ontworpen om netwerkverkeer in gedetailleerd formaat te verzamelen en te visualiseren. Het biedt tools voor het monitoren van zowel fysieke als virtuele netwerken en kan helpen bij het identificeren van verkeersopstoppen, performanceproblemen en hardwarestoringen. PRTG biedt uitgebreide loggingmogelijkheden en kan waarschuwingen genereren bij ongebruikelijke activiteit, zoals netwerkcongestie of verhoogde latency. Dit maakt het bijzonder nuttig in virtuele netwerken, waar verkeer soms snel kan variëren en invloed kan hebben op de netwerkcapaciteit, vooral tijdens piekmomenten. (PRTGManual2025)

Er zijn dus verscheidene tools om aan monitoring en logging te doen in een virtueel netwerk. Er is nog weinig onderzoek gedaan naar logging en monitoring in een schoolomgeving met Ruckus Virtual SmartZone.

A.2.4. Uitdagingen en Open Vragen

Schaalbaarheid van oplossingen: Scholen kunnen te maken krijgen met pieken in het aantal apparaten dat verbinding maakt met het netwerk, vooral tijdens het begin van schooldagen of leswissels. Is er een tool die goed inspeelt op een netwerk met Virtual SmartZone om piekmomenten te monitoren en loggen? (BashirEtAl2022)

Integratie met cloud-applicaties: Met de opkomst van cloudgebaseerde onderwijsplatformen, zoals Google Classroom of Microsoft Teams, wordt het moeilijker om

netwerkprestaties te meten, vooral wanneer het netwerkverkeer zowel lokaal als in de cloud plaatsvindt. Hoe kunnen tools deze dynamiek effectief monitoren? **(CommScope2025)**

Kosten en middelen: Veel geavanceerde netwerkmonitoringtools, zoals PRTG, kunnen kostbaar zijn voor kleinere scholen met beperkte middelen. Is er een kosteneffectief alternatief die dezelfde mate van controle en inzicht bieden? **(Ruckus2025)**

A.2.5. Verschil in onderzoek

Op onderwijsinstellingen is er overmatig gebruik gemaakt van tools die netwerken monitoren en loggen zonder een Ruckus Virtual SmartZone. Dit onderzoek implementeert dit wel. **(PeerJCS2020)**

A.3. Methodologie

Dit is een Proof of Concept (PoC) studie waarin de effectiviteit van de Ruckus Virtual SmartZone wordt getoetst in een schoolomgeving. Er zal niet alleen configuratie en werking van de hardware en software getest worden, maar ook hoe goed de Virtual SmartZone omgaat met realistische omstandigheden (zoals piekmomenten) in het netwerk van atheneum dendermonde.

Eerst wordt er een duidelijke literatuurstudie gedaan. Het doel is het begrijpen van de huidige stand van zaken in netwerkmonitoring binnen scholen, met nadruk op piekmomenten en virtuele netwerken. De literatuurstudie omvat het lezen van artikelen en whitepapers over netwerkmonitoring, tools zoals Ruckus Virtual SmartZone, en het gebruik ervan in scholen.

Dan zal testomgeving worden opgezet met de Ruckus Virtual SmartZone en mogelijks andere tools als Ruckus Virtualzone Smartzone alleen niet goed genoeg blijkt te zijn. Hardware wordt geïnstalleerd en software geconfigureerd. Daarna wordt piekbelasting gesimuleerd door gebruik te maken van de scholieren die op piekmomenten gebruik maken van het netwerk. Monitoringtools registreren het verkeer en logs.

Vervolgens zullen verzamelde logbestanden worden geanalyseerd om de effectiviteit van de tools te beoordelen.

Op basis van de resultaten wordt een eindrapport geschreven met conclusies en aanbevelingen voor scholen over netwerkmonitoringtools. Het bestaat dus uit 5 fasen waarbij fase 1, 2 en 3 het meeste tijd zal innemen.

A.4. Verwacht resultaat, conclusie

Er wordt verwacht gedetailleerde inzichten in de prestaties van netwerkmonitoringtools zoals Ruckus Virtual SmartZone, LibreNMS... tijdens piekmomenten. De belangrijkste data omvatten netwerkbelasting (Mbps), responstijd voor waarschuwingen, en de gedetailleerdheid van logs. Grafieken zullen netwerkverkeer en res-

ponstijden in real-time tonen, wat de effectiviteit van de tool bij piekbelasting laat zien.

Het onderzoek zal ervoor zorgen dat er een goede monitoring- en loggingoplossing is voor scholen voor het identificeren op basis van prestaties tijdens piekmomenten, met focus op snelheid, nauwkeurigheid van waarschuwingen en loggedetail. De Ruckus Virtual SmartZone zal goed presteren, maar andere tools kunnen mogelijk betere loganalyse bieden.

Dit onderzoek biedt school-IT-beheerders concrete aanbevelingen voor netwerkmonitoring tijdens drukke periodes, wat zorgt voor stabiele netwerken en betere prestaties in het onderwijs.