

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології моніторингу мережі на
базі рішення Nagios та обладнання Mikrotik»

Виконав: студент 2-го курсу групи КІм-24-1
спеціальності 123 «Комп'ютерна інженерія»

 Максим БУТКЕВИЧ

Керівник: доцент кафедри КІ та КБ, к.пед.н., доцент,

 Олена ГОЛОВНЯ

Рецензент: доцент кафедри КІ та КБ, к.т.н.

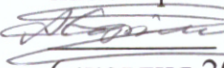
 Олексій ШЕЛУХА

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО
6 жовтня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Буткевич Максим Олександрович

Тема роботи: «Методи та технології моніторингу мережі на базі рішення Nagios та обладнання Mikrotik»

затверджена Наказом університету від 6 жовтня 2025 р. № 565/с

Термін здачі студентом закінченої роботи 16 грудня 2025 р.

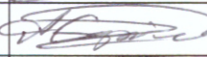
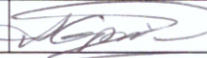
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Процес налаштування системи моніторингу Nagios.
2. Система моніторингу Nagios Core, способи моніторингу маршрутизаторів Mikrotik, методи та технології моніторингу мереж.

Обладнання та програмне забезпечення:

1. GNS3, VirtualBox.
2. Nagios Core.
3. Ubuntu 22.04 LTS, Windows 10, Lubuntu 22.04 LTS, Mikrotik CHR.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Андрій ЄФІМЕНКО	 6.10.25	 6.10.25
2	Андрій ЄФІМЕНКО	 6.10.25	 6.10.25
3	Андрій ЄФІМЕНКО	 6.10.25	 6.10.25

Студент  Максим БУТКЕВИЧ

Керівник  Олена ГОЛОВНЯ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	06.10.2025 – 08.10.2025	
2	Аналіз теоретичних відомостей про моніторинг мережі	09.10.2025 – 18.10.2025	
3	Аналіз програмних рішень для моніторингу мережі	19.10.2025 – 29.10.2025	
4	Дослідження можливостей моніторингу обладнання Mikrotik	30.10.2025 – 03.11.2025	
5	Проектування мережі	04.11.2025 – 08.11.2025	
6	Розроблення системи IP-адресації	07.11.2025 – 09.11.2025	
7	Базові налаштування мережевих пристроїв	10.11.2025 – 14.11.2025	
8	Розгортання системи моніторингу Nagios	15.11.2025 – 20.11.2025	
9	Налаштування моніторингу пристроїв мережі	21.11.2025 – 01.12.2025	
10	Проведення тестування роботи системи моніторингу	02.12.2025 – 06.12.2025	
11	Оформлення пояснювальної записки	07.12.2025 – 16.12.2025	

Студент Бу Максим БУТКЕВИЧ

Керівник Олена Олена ГОЛОВНЯ

АНОТАЦІЯ

Пояснювальна записка до випускної кваліфікаційної роботи магістра складається з переліку умовних позначень, вступу, трьох розділів, висновків, списку використаної літератури.

Метою кваліфікаційної роботи є розроблення та реалізація системи моніторингу на базі рішення Nagios та обладнання Mikrotik.

У роботі було розглянуто теоретичні аспекти моніторингу мережі, було порівняно чотири рішення для моніторингу мережі, після чого досліджено принципи роботи одного з них – Nagios. Було оглянуто можливості моніторингу маршрутизаторів Mikrotik. У другому розділі було описано процес проектування мережі та системи адресації. Третій розділ присвячений реалізації задуманих ідей. Було розгорнуто систему моніторингу Nagios та налаштовано моніторинг чотирьох хостів. Результати тестування підтвердили коректність здійснених налаштувань.

Загальний обсяг пояснювальної записки складає 62 сторінки. У роботі наведено 34 рисунки та 6 таблиць. Список використаної літератури містить 22 найменування та займає 2 сторінки.

Ключові слова: NAGIOS, MIKROTIK, МЕРЕЖЕВИЙ МОНІТОРИНГ, СИСТЕМА МОНІТОРИНГУ.

ANNOTATION

The explanatory note to the master's thesis consists of a list of conventional abbreviations, an introduction, three chapters, conclusions, a list of references.

The purpose of the qualification work is to develop and implement a monitoring system based on the Nagios solution and Mikrotik equipment.

The paper examines the theoretical aspects of network monitoring, compares four network monitoring solutions, and then investigates the operating principles of one of them – Nagios. The monitoring capabilities of Mikrotik routers were reviewed. The second chapter describes the process of network design and address planning. The third chapter is devoted to the implementation of the conceived ideas. The Nagios monitoring system was deployed and monitoring for four hosts was configured. The testing results confirmed the correctness of the applied configurations.

The total volume of the explanatory note is 62 pages. The paper contains 34 figures and 6 tables. The list of references contains 22 titles and occupies 2 pages.

Keywords: NAGIOS, MIKROTIK, NETWORK MONITORING, MONITORING SYSTEM.

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ МОНІТОРИНГУ МЕРЕЖ ЗА ДОПОМОГОЮ РІШЕННЯ NAGIOS ТА ОБЛАДНАННЯ МІКРОТІК.....	11
1.1 Загальна характеристика поняття моніторингу мереж	11
1.2 Огляд програмних рішень для моніторингу мережі.....	13
1.3 Принципи роботи та основні можливості програмного забезпечення Nagios.....	18
1.4 Можливості моніторингу обладнання MikroTik.....	22
1.5 Постановка завдання дослідження	24
РОЗДІЛ 2. ПРОЄКТУВАННЯ МЕРЕЖІ НА БАЗІ РІШЕННЯ NAGIOS ТА ОБЛАДНАННЯ МІКРОТІК	26
2.1 Опис проєктованої мережі.....	26
2.2 Розроблення схеми адресації пристроїв мережі	28
2.3 Вибір характеристик для моніторингу	30
РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ NAGIOS	34
3.1 Базове налагодження пристроїв мережі.....	34
3.2 Встановлення та налаштування система моніторингу Nagios.....	36
3.3 Налаштування моніторингу всіх вузлів мережі	40
3.4 Тестування роботи системи моніторингу Nagios.....	53
ВИСНОВКИ.....	60
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	61

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система
CHR – Cloud Hosted Router
CPU – central processing unit
DHCP – Dynamic Host Configuration Protocol
GNS3 – Graphical Network Simulator-3
HTTP – Hypertext Transfer Protocol
ICMP – Internet Control Message Protocol
IP – Internet Protocol
NCPA – Nagios Cross Platform Agent
NRPE – Nagios Remote Plugin Executor
OID – Object Identifier
PRTG – Paessler Router Traffic Grapher
RAM – random access memory
SNMP – Simple Network Management Protocol
SSH – Secure Shell Protocol

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку інформаційних технологій стабільна та безперебійна робота комп'ютерних мереж є критично важливою для функціонування організацій різного рівня. Зростання кількості мережевих пристроїв, сервісів і обсягів передавання даних ускладнює адміністрування інфраструктури та підвищує ризик виникнення збоїв. У таких умовах особливої актуальності набуває впровадження систем моніторингу, які дозволяють своєчасно виявляти проблеми, контролювати стан обладнання та забезпечувати оперативне реагування на аварійні ситуації.

Одним із найпоширеніших класів рішень для контролю мережевої інфраструктури є системи моніторингу з відкритим вихідним кодом. Вони надають широкі можливості для налаштування, інтеграції з різноманітним обладнанням та адаптації під конкретні потреби організації. Серед таких систем особливе місце займає Nagios – потужна та гнучка платформа для моніторингу мережевих пристроїв, сервісів, яка підтримує різні методи перевірки стану.

Водночас мережеве обладнання Mikrotik широко використовується в невеликих і середніх мережах завдяки своїй доступності, функціональності та можливості тонкого налаштування. Підтримка протоколу SNMP у маршрутизаторах Mikrotik дозволяє ефективно інтегрувати їх із системами моніторингу та отримувати детальну інформацію про стан ресурсів, інтерфейсів і стабільність роботи. Поєднання Nagios і Mikrotik створює універсальне рішення для побудови системи моніторингу мережевої інфраструктури.

Метою кваліфікаційної роботи є розроблення та реалізація системи моніторингу на базі рішення Nagios та обладнання Mikrotik.

Визначена мета обумовлює наступні завдання:

- проаналізувати принципи побудови систем моніторингу комп'ютерних мереж;
- здійснити огляд і порівняння сучасних систем моніторингу;
- спроектувати мережеву топологію та IP-адресний план;
- встановити та налаштувати систему моніторингу Nagios Core;

- налаштувати моніторинг хостів мережі;
- провести тестування системи моніторингу.

Об'єктом дослідження є процес налаштування системи моніторингу Nagios.

Предметом дослідження є система моніторингу Nagios Core, способи моніторингу маршрутизаторів Mikrotik, методи та технології моніторингу мереж.

У процесі виконання кваліфікаційної роботи було розроблено проект комп'ютерної мережі, у якій налаштовано систему моніторингу Nagios Core. Відбувається моніторинг чотирьох хостів: маршрутизатора Mikrotik, робочих станцій з ОС Linux та Windows, Ubuntu-сервера, на якому розгорнуто систему моніторингу.

Апробація результатів дослідження:

1. Буткевич М. О., Головня О.С. Дослідження можливостей моніторингу мережі за допомогою програмного рішення Nagios. Тези XV Міжнародної науково-технічної конференції "Інформаційно-комп'ютерні технології", 28-29 березня 2025 року. Житомир : «Житомирська політехніка», 2024. С. 115-116.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ МОНІТОРИНГУ МЕРЕЖ ЗА ДОПОМОГОЮ РІШЕННЯ NAGIOS ТА ОБЛАДНАННЯ МІКРОТІК

1.1 Загальна характеристика поняття моніторингу мереж

Мережевий моніторинг – це процес безперервного збору, аналізу та відображення даних про стан комп’ютерної мережі та її компонентів. Основною метою моніторингу є своєчасне виявлення проблем у роботі обладнання або сервісів, мінімізація простоїв і підвищення надійності всієї мережевої інфраструктури. За допомогою програмних рішень для моніторингу мережі адміністратори можуть заздалегідь виявляти недоліки, оптимізувати ефективність тощо [2].

Моніторинг може бути активним або пасивним. Активний моніторинг передбачає періодичне опитування пристроїв за допомогою мережевих протоколів (наприклад, SNMP, ICMP, HTTP) з метою перевірки їхньої доступності та отримання статистичних даних. Пасивний моніторинг базується на аналізі вже наявного трафіку або повідомлень, що надходять від пристроїв (Syslog, NetFlow), без прямого опитування.

Мережевий моніторинг має наступні переваги:

- Повна картина мережі. Завдяки моніторингу, адміністратори мають можливість бачити мережу повністю, спостерігати за тим, як дані рухаються по ній, а також швидко виявляти і виправляти проблеми.
- Автоматизація ручної роботи. Інструменти мережевого моніторингу дозволяють зменшити кількість ручної роботи для ІТ-спеціалістів. Це означає, що вони можуть перенаправити свої зусилля на інші важливі завдання.
- Здатність швидко виявляти загрози. Уся незвична активність фіксується програмою моніторингу, тому адміністратори одразу бачать проблему та можуть визначити, чи становить вона загрозу для мережі.
- Прогнозування майбутніх потреб. Однією з можливостей інструментів мережевого моніторингу є створення звіту про роботу мережі або її компонентів. Провівши аналіз звіту, адміністратори можуть передбачити, які зміни потрібно

зробити в майбутньому для покращення роботи мережі, наприклад додавання нових компонентів або оновлення наявних [4].

Є два методи збору системних даних: агентний та безагентний. Моніторинг на основі агентів передбачає використання спеціальних програмних агентів. Вони встановлюються на тій системі чи пристрої, за якими потрібно спостерігати. Агенти збирають широкий набір показників та вимірювань, які відображають поведінку та стан системи. Це можуть бути дані про використання процесора або пам'яті, використання дискового простору, пропускну здатність мережі, кількість запущених процесів, кількість користувачів у системі тощо. Таких характеристик є дуже багато. Тому адміністратори мають можливість бачити кожні деталі діяльності системи чи пристрою або налаштувати відстеження тільки тих характеристик, що відповідають актуальним потребам.

Використання агентів дозволяє здійснювати проактивний моніторинг. Для кожного показника можна встановити порогове значення, при перетинанні якого адміністраторові надходить сповіщення. Таким чином адміністратори будуть на крок попереду всіх потенційних проблем у мережі.

Основною перевагою агентного моніторингу є широкий збір даних. Але вони споживають системні ресурси, що може вплинути на продуктивність системи. Особливо, якщо система має обмежені ресурси або сам моніторинг потребує використання значної кількості ресурсів.

При безагентному моніторингу не потрібно встановлювати окремого агента, тому що тут використовуються вбудовані протоколи. До них належать SNMP, SSH, WMI, NetFlow та інші. Їхнім завданням є збір та передавання даних до системи моніторингу. Безагентний моніторинг застосовується в мережевому обладнанні, на якому неможливо встановити агент, наприклад комутатори або маршрутизатори.

Перевагою безагентного моніторингу є широке застосування. Він може застосовуватися на тих пристроях або системах, де підтримуються необхідні протоколи. Він також зменшує вплив на продуктивність системи, оскільки немає агента, який би використовував додаткові ресурси. Безагентний моніторинг

можна застосовувати в системах з обмеженим ресурсами, в застарілих системах. Але на відміну від агентного, набір показників для відстеження не такий широкий [3].

Мережевий моніторинг є невід'ємною частиною сучасного адміністрування інформаційних систем. Він дозволяє бачити стан усіх компонентів мережі, швидко реагувати на проблеми, підвищує ефективність роботи ІТ-спеціалістів, створює основу для побудови більш масштабних систем керування мережею. Якісний та ефективний моніторинг мережі залежить від програмних додатків. Сучасні програмні рішення для моніторингу мережі надають безліч корисних послуг. Контроль доступності пристроїв і сервісів, надсилання сповіщень про певну подію, візуалізація даних, формування звітів – ось декілька послуг, що роблять системи моніторингу незамінними для адміністраторів.

1.2 Огляд програмних рішень для моніторингу мережі

Кількість програмних рішень, призначених для моніторингу мережевої інфраструктури, є доволі великою. Це дозволяє обрати програмне забезпечення, що найкраще підійде для конкретної мережі. Системи моніторингу можуть відрізнятися архітектурою, функціональністю, типом ліцензування, зручністю у використанні, але вони мають спільну мету: забезпечити безперервну роботу мережі, виявляти та виправляти проблеми. Серед найбільш відомих і широко застосовуваних рішень можна виділити: Nagios, Zabbix, PRTG Network Monitor, SolarWinds Network Performance Monitor [6].

Nagios Core є одним із найстаріших і найпоширеніших рішень у сфері моніторингу. Система має модульну архітектуру та базується на принципі плагінів, які виконують перевірку стану пристроїв і сервісів. Nagios підтримує як активний, так і пасивний моніторинг, дозволяє створювати складні сценарії сповіщення та інтегрується з великою кількістю сторонніх інструментів. Основна перевага Nagios полягає у його гнучкості та можливості розширення функціоналу завдяки численним плагінам і відкритому коду. Недоліком є

складність налаштування та необхідність редагування конфігураційних файлів вручну, що може ускладнити роботу для початківців. Продукт поширюється у двох версіях: безкоштовній Nagios Core (рис. 1.1) та комерційній Nagios XI (рис. 1.2), яка має розширений веб-інтерфейс і зручні засоби адміністрування [8].

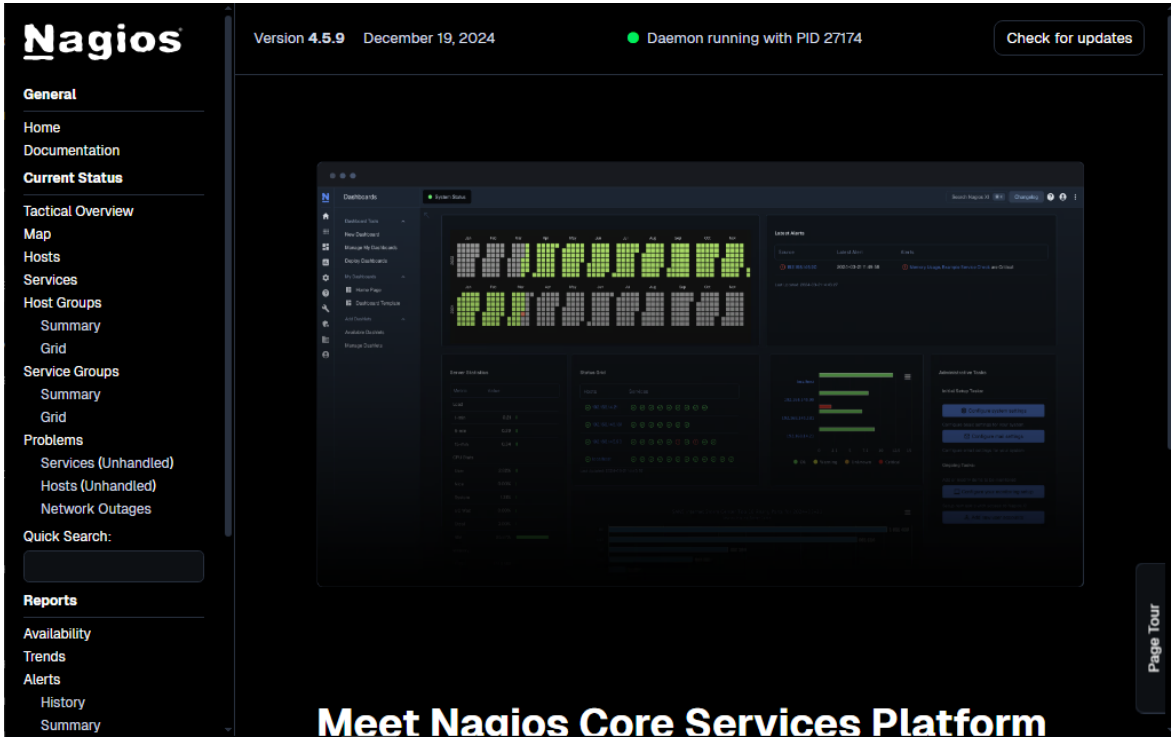


Рисунок 1.1 – Вигляд головної сторінки веб-інтерфейсу Nagios Core

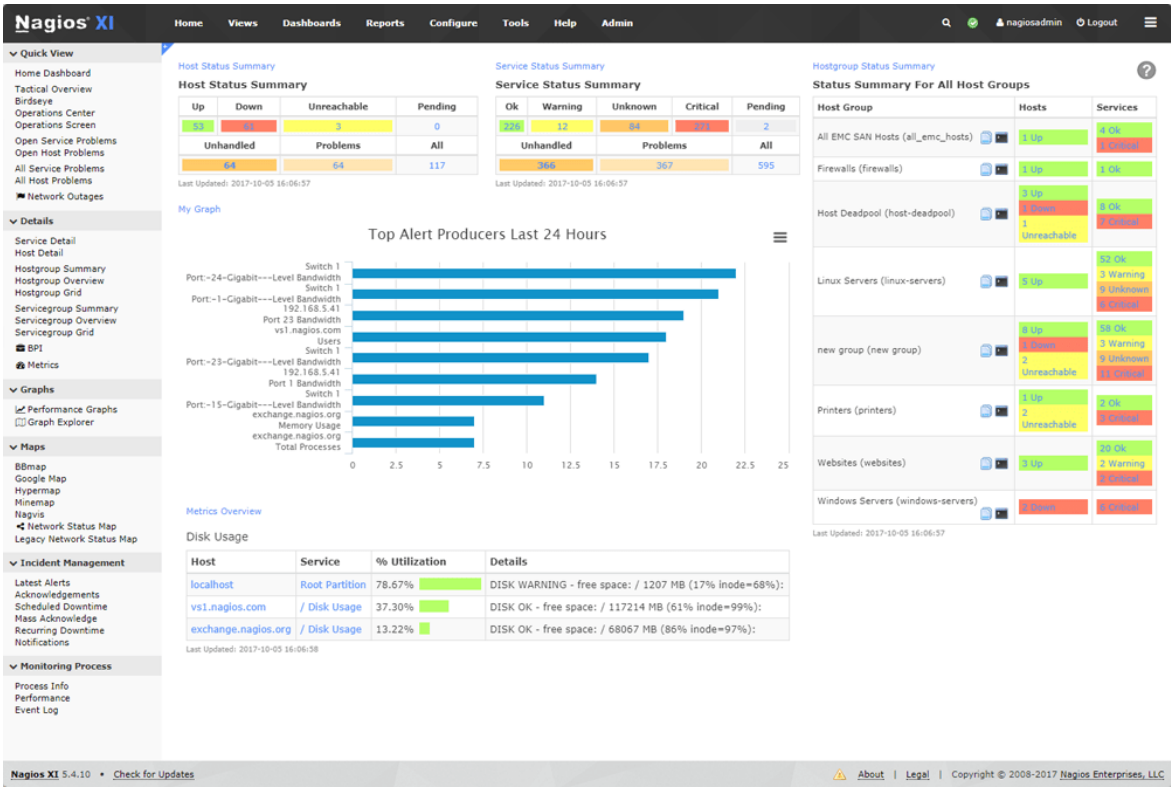


Рисунок 1.2 – Вигляд додатку Nagios XI

Іншим популярним рішенням є Zabbix [9]. Zabbix поєднує функції моніторингу, збору статистики та візуалізації даних. Він використовує централізований сервер, що приймає дані від агентів, встановлених на хостах, або отримує їх через SNMP, ICMP або інші протоколи [5]. Система має розвинений веб-інтерфейс, підтримує автоматичне виявлення пристроїв і гнучкі механізми тригерів для визначення критичних станів. Zabbix є повністю відкритим і безкоштовним рішенням, однак його продуктивність при великій кількості об'єктів може вимагати суттєвих апаратних ресурсів, а налаштування агентів на різних платформах потребує певного досвіду.

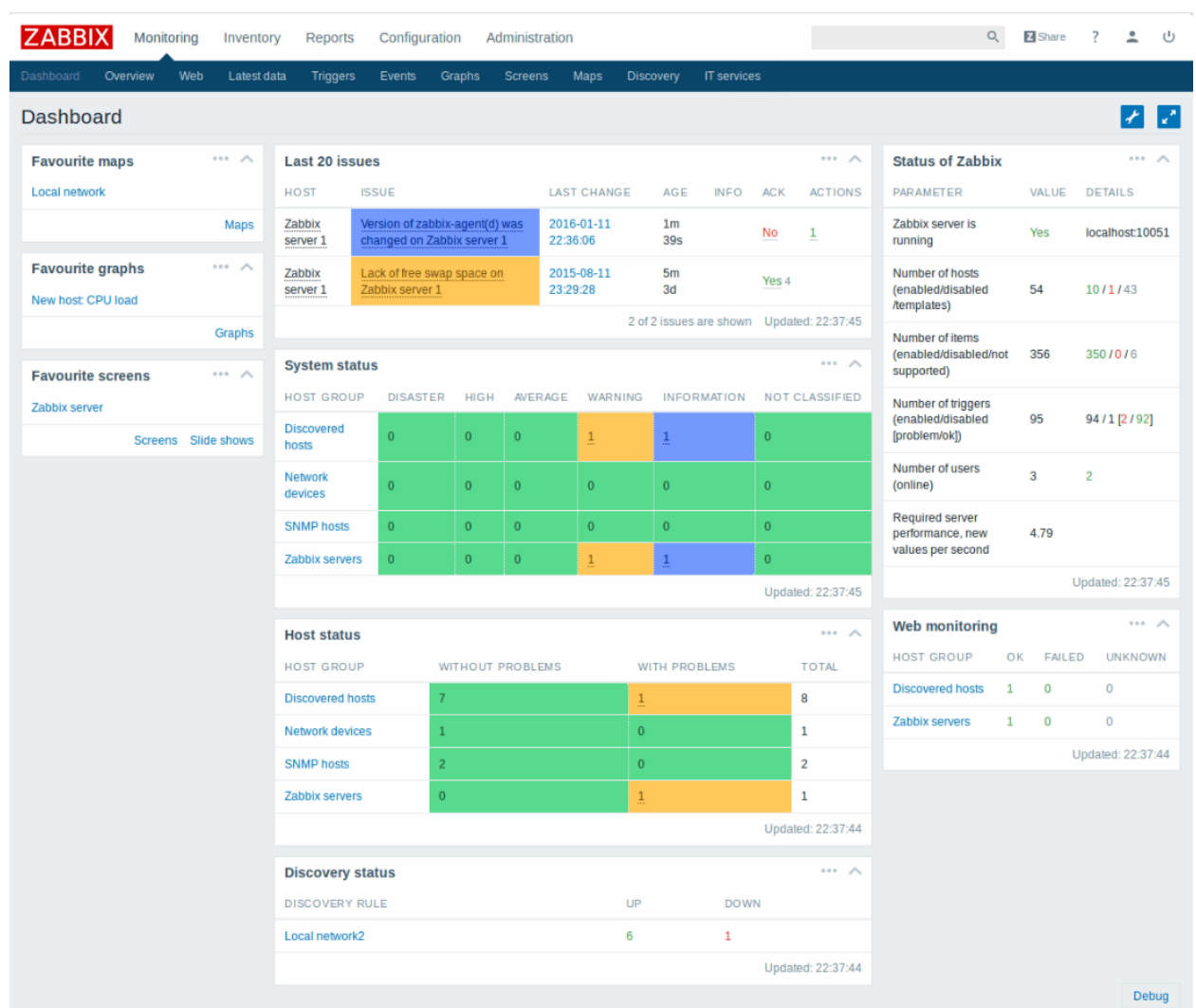


Рисунок 1.3 – Приклад роботи Zabbix

PRTG Network Monitor – це комерційне рішення від компанії Paessler, орієнтоване на середні та великі корпоративні мережі. Його ключовою особливістю є висока автоматизація процесу моніторингу: система самостійно

виявляє пристрої, налаштовує сенсори для різних протоколів (SNMP, WMI, NetFlow, HTTP) і пропонує зрозумілий графічний інтерфейс. PRTG відзначається простотою у використанні, широкими можливостями побудови графіків і звітів, однак є платною, а безкоштовна версія обмежена 100 сенсорами, що робить її менш придатною до масштабних інфраструктур [10].

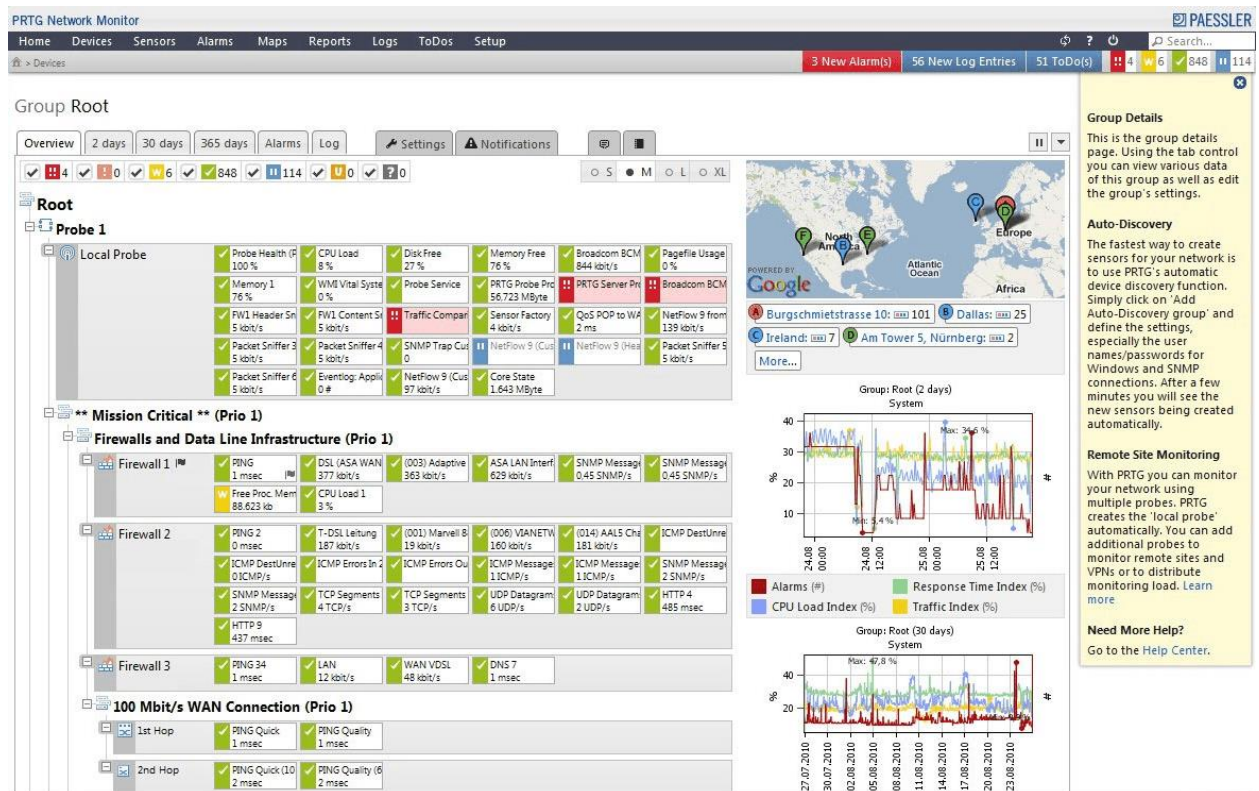


Рисунок 1.4 – Вигляд додатку PRTG Network Monitor

Ще одним потужним рішенням є SolarWinds Network Performance Monitor, яке використовується переважно у великих корпоративних та операторських мережах. Ця система має розвинену архітектуру, забезпечує глибоку аналітику трафіку, автоматичне виявлення пристроїв і детальну візуалізацію топології. SolarWinds відзначається високою точністю збору даних та інтеграцію з іншими продуктами виробника, однак її вартість є значною, а вимоги до серверного обладнання – досить високими. Унаслідок цього рішення використовується здебільшого у великих компаніях, де необхідна централізована система керування мережею [11].

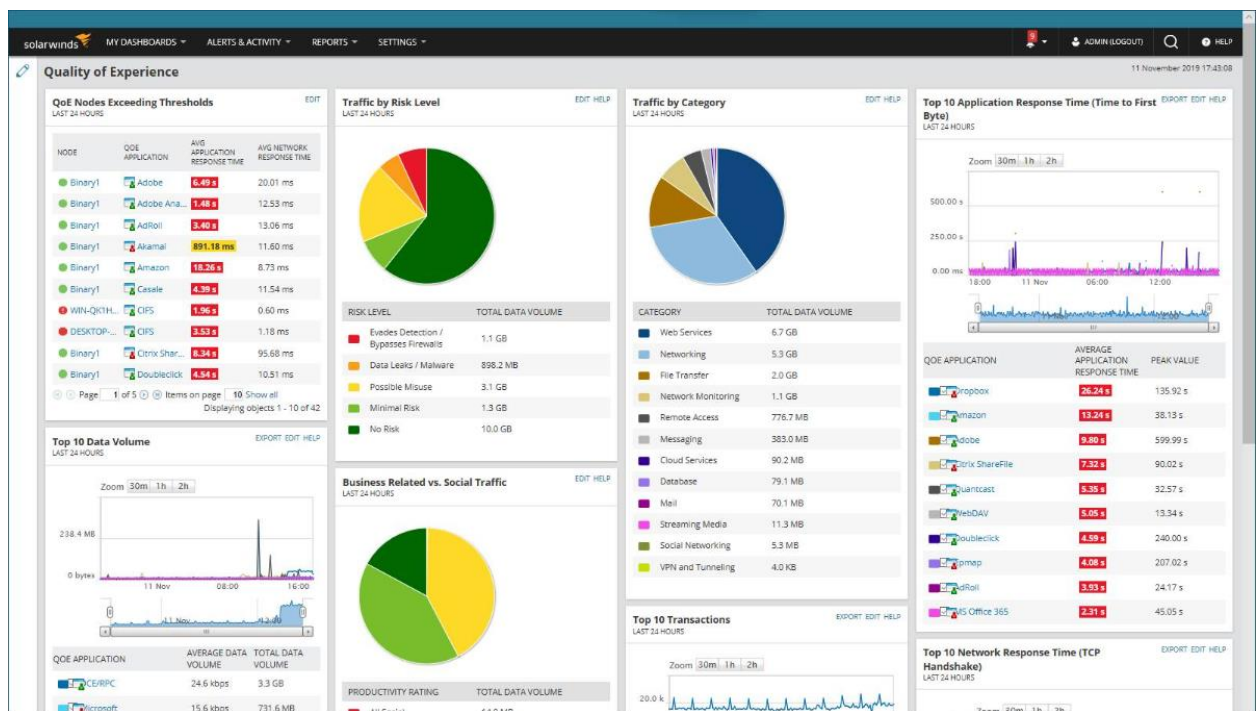


Рисунок 1.5 – Вигляд додатку SolarWinds Network Performance Monitor

У таблиці 1.1 подано порівняння розглянутих систем моніторингу.

Таблиця 1.1

Порівняльна характеристика систем моніторингу

Система	Ліцензія	Основні переваги	Недоліки
Nagios	Безкоштовна/ Комерційна	Висока гнучкість, модульність, стабільність	Складність конфігурації, старий інтерфейс
Zabbix	Безкоштовна	Візуалізація, інтеграція, централізований збір	Потребує потужного сервера
PRTG Network Monitor	Комерційна/ Безкоштовна (100 сенсорів)	Простота, автоматичне виявлення, гарний UI	Обмеження безкоштовної версії
SolarWinds NPM	Комерційна	Потужна аналітика, масштабованість	Дуже висока ціна, ресурсоємність

Проаналізувавши розглянуті рішення, можна зробити висновок, що всі вони забезпечують подібний набір базових функцій: моніторинг пристроїв, збір статистики, сповіщення про події та візуалізацію даних. Вибір конкретної системи залежить від масштабу мережі, наявних ресурсів і вимог до зручності керування[7].

Для реалізації проєкту в межах цієї кваліфікаційної роботи було обрано систему моніторингу Nagios Core, оскільки вона забезпечує оптимальне співвідношення між функціональністю, стабільністю та гнучкістю налаштування. Nagios має відкритий вихідний код, що дозволяє адаптувати систему під конкретні потреби навчального або дослідницького середовища, не обмежуючись комерційними ліцензіями.

Важливою перевагою є наявність великої спільноти користувачів, яка створює тисячі безкоштовних плагінів для моніторингу практично будь-якого пристрою чи сервісу. У контексті побудови мережі з обладнанням MikroTik це особливо корисно, адже існують готові SNMP-OID для збору даних про стан інтерфейсів, CPU, RAM та інші параметри.

Таким чином, обраний інструмент дозволяє виконати завдання кваліфікаційної роботи: встановити та налаштувати систему моніторингу, забезпечити моніторинг хостів мережі.

1.3 Принципи роботи та основні можливості програмного забезпечення Nagios

Система Nagios є одним з найстаріших і найвідоміших рішень моніторингу мережі. Мета цього програмного забезпечення – швидко інформувати адміністраторів про попереджувальні або критичні стани. Що вважається попереджувальним або критичним, визначається у конфігурації [1].

Архітектурно система складається з кількох основних компонентів, які взаємодіють між собою для забезпечення безперервного збору даних і візуалізації результатів. У центрі всієї системи розташований сервер моніторингу, який виконує роль ядра. Саме на ньому зберігаються всі

конфігураційні файли, виконується логіка перевірок і формується інформація для подальшого відображення у веб-інтерфейсі. Сервер періодично запускає перевірки стану вузлів та сервісів, використовуючи спеціальні плагіни – невеликі зовнішні програми або скрипти, що виконують конкретні дії, наприклад, перевірку доступності пристрою через ping, вимірювання часу відповіді веб-сервера, зчитування показників навантаження процесора з мережевого маршрутизатора.

Плагінна архітектура є ключовою особливістю Nagios. Вона забезпечує гнучкість і розширюваність системи. Кожен плагін виконує певну перевірку, повертаючи код завершення, який інтерпретується Nagios як один із станів: «OK», «WARNING», «CRITICAL», «UNKNOWN» тощо. Таким чином адміністратор може швидко побачити, які елементи мережі працюють стабільно, а де спостерігається відхилення. Завдяки відкритій структурі плагінів користувач може створювати власні скрипти будь-якою мовою програмування або скриптовою мовою й інтегрувати їх у систему.

Для збору детальної інформації з віддалених вузлів Nagios може використовувати агентів, зокрема NRPE (Nagios Remote Plugin Executor) і NSClient++. Ці агенти встановлюються безпосередньо на контрольовані пристрої і дозволяють виконувати локальні перевірки. Сервер Nagios надсилає запит до агента, який запускає необхідний плагін на стороні клієнта, обробляє результат і повертає відповідь назад. Такий підхід забезпечує більш точні дані про стан системи, ніж прості безагентні перевірки.

Окрім агентів, Nagios підтримує моніторинг через стандартні мережеві протоколи, серед яких найпоширенішим є SNMP. Завдяки цьому Nagios може збирати статистику з мережевого обладнання, такого як маршрутизатори MikroTik. SNMP дозволяє отримувати від пристрою показники в реальному часі. Це робить систему універсальною і придатною для моніторингу як серверної, так і мережевої інфраструктури.

Важливою частиною функціонування Nagios є система конфігураційних файлів, через яку налаштовуються всі об'єкти моніторингу. Основні параметри

зберігаються у файлі `nagios.cfg`, який визначає структуру каталогів, де розташовані інші конфігураційні файли. У цих файлах описуються хости, спостережувані служби, команди плагінів, користувачі, періоди моніторингу, способи оповіщення. Наприклад, кожен хост описується у вигляді блоку, де задаються його ім'я, IP-адреса, група, до якої він належить, та команди перевірок. Для кожного сервісу визначаються параметри, що описують, яку перевірку слід виконати, як часто її повторювати, які дії слід вжити у випадку виявлення проблеми. Конфігураційна структура дозволяє логічно групувати об'єкти за певною ознакою.

Ще одним важливим компонентом є веб-інтерфейс Nagios, який надає зручні засоби візуалізації. Через браузер адміністратор може переглядати поточний стан об'єктів, історію подій, графіки змін. Графічна оболонка, як правило, реалізується за допомогою додаткового модуля Nagios Core Web Interface або вдосконалених рішень, таких як Nagios XI.

У таблиці 1.2 подано узагальнену інформацію про компоненти системи Nagios.

Таблиця 1.2

Основні компоненти системи Nagios

Компонент	Призначення	Приклади/деталі
Nagios Core (Server)	Основне ядро системи, яке керує перевірками, збирає результати, аналізує стани та надсилає сповіщення	Виконує перевірки, обробляє події, зберігає логи
Плагіни	Невеликі програми або скрипти, що виконують конкретні перевірки	<code>check_ping</code> , <code>check_http</code> , <code>check_snmp</code>
Агенти	Дозволяють виконувати локальні перевірки на віддалених вузлах	NCPA, NSClient++
Конфігураційні файли	Описують параметри моніторингу, хости, сервіси, контакти, командні шаблони	<code>nagios.cfg</code> , <code>hosts.cfg</code> , <code>services.cfg</code> , <code>commands.cfg</code>
Веб-інтерфейс	Забезпечує графічне представлення результатів моніторингу та керування системою	Візуалізація, графіки, журнали подій, оповіщення

Умовно архітектуру системи Nagios можна зобразити у вигляді структурної схеми (рис. 1.6).

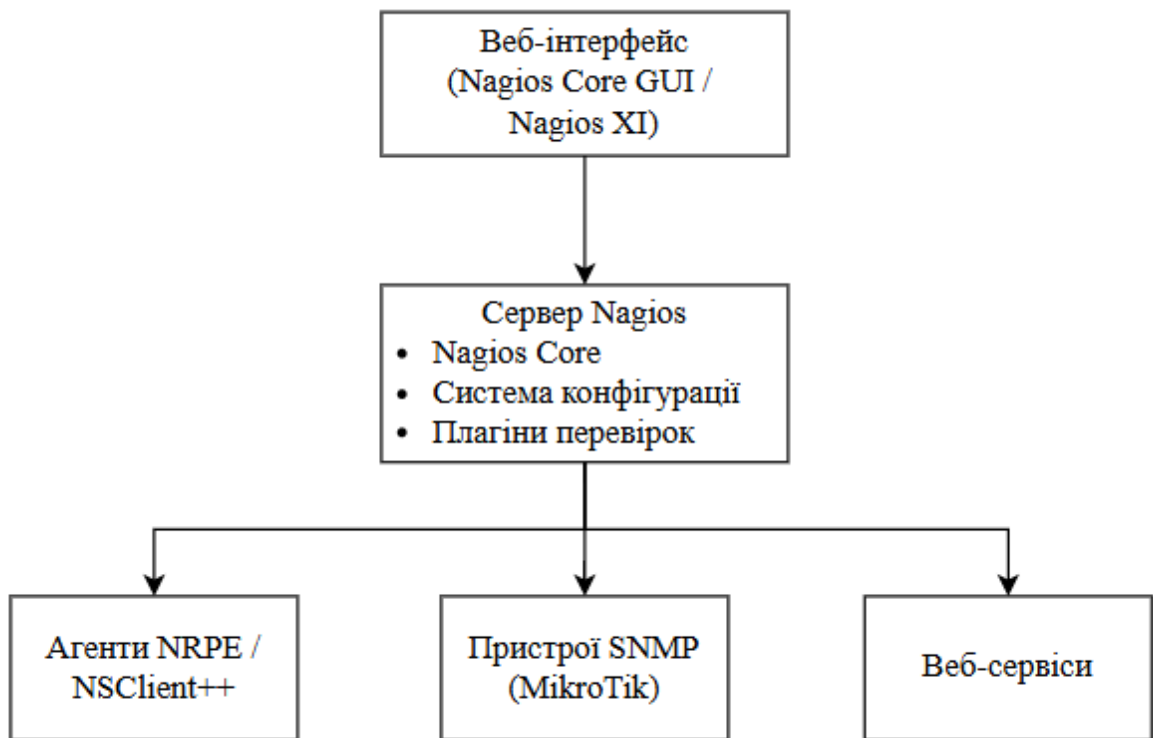


Рисунок 1.6 – Загальна архітектура системи Nagios

Nagios дозволяє здійснювати активні та пасивні перевірки. Найпоширенішими є активні перевірки. Вони ініціюються процесом Nagios та проводяться регулярно за планом. На відміну від активних, пасивні перевірки ініціюються та виконуються не Nagios, а зовнішніми програмами або процесами. До Nagios надсилаються результати цих перевірок.

Принципи роботи Nagios ґрунтуються на поєднанні модульної архітектури, використанні плагінів і агентів, стандартизованих протоколів збору даних, а також структурованої системи конфігурації. Завдяки цьому Nagios залишається одним із найгнучкіших і найефективніших інструментів моніторингу, що дозволяє забезпечити повний контроль за станом мережевої інфраструктури й оперативно реагувати на будь-які збої в роботі.

1.4 Можливості моніторингу обладнання MikroTik

Компанія MikroTik була заснована у 1996 році для розробки маршрутизаторів та систем ISP. У 1999 році було створено мережну операційну систему на базі Linux – RouterOS. Вона забезпечує широку стабільність, гнучкість для всіх видів інтерфейсу даних та маршрутизації [13].

Маршрутизатори MikroTik, що працюють під керуванням операційної системи RouterOS, є гнучким та потужним інструментом для створення і адміністрування мережевої інфраструктури. RouterOS має вбудовану підтримку протоколу SNMP, який використовується для збору статистики, діагностики та контролю за роботою пристроїв у мережі. Саме завдяки SNMP маршрутизатори MikroTik можуть інтегруватися з системами моніторингу, такими як Nagios, Zabbix, PRTG Network Monitor та іншими.

Протокол SNMP дозволяє системі моніторингу отримувати дані про стан пристрою, використовуючи спеціальні ідентифікатори – OID. Ці ідентифікатори відповідають певним параметрам, наприклад, завантаженню процесора, кількості використаної оперативної пам'яті, швидкості інтерфейсів, температурі пристрою тощо. У RouterOS реалізовано повну підтримку SNMPv1, v2c і v3, що забезпечує як базову, так і розширену безпеку обміну даними [14].

SNMP у MikroTik працює за принципом «запит-відповідь»: сервер моніторингу надсилає SNMP-запит до пристрою, а той повертає запитуване значення у вигляді OID. Для підвищення безпеки адміністратор може налаштувати SNMP-сервер так, щоб він відповідав лише на запити з певних IP-адрес, а також визначити «community string» – певний пароль для доступу до статистики. У системі Nagios SNMP-перевірки здійснюються через плагін *check_snmp*. Використовуючи це, адміністратор може контролювати стан кожного інтерфейсу, навантаження CPU, використання пам'яті або навіть кількість активних PPP-з'єднань.

Нижче наведено схему (рис. 1.7), що ілюструє взаємодію між Nagios та маршрутизатором MikroTik через SNMP.

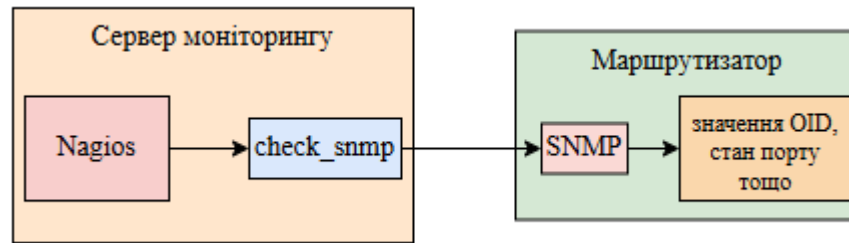


Рисунок 1.7 – Схема моніторингу MikroTik через SNMP

Для зручності моніторингу у RouterOS передбачено стандартні OID, що дозволяють знімати показники основних компонентів. Наприклад, OID .1.3.6.1.2.1.25.3.3.1.2.1 використовується для отримання показника завантаження процесора, .1.3.6.1.2.1.25.2.2.0 – для моніторингу обсягу оперативної пам’яті, а .1.3.6.1.2.1.31.1.1.1.6.2 відповідає за вхідний трафік на інтерфейсі. У системі Nagios ці параметри можуть бути додані через плагіни SNMP або спеціальні скрипти, які інтерпретують отримані значення та перетворюють їх у графіки чи оповіщення.

У таблиці 1.3 наведені приклади найпоширеніших OID, які використовуються для моніторингу пристроїв MikroTik.

Таблиця 1.3

Найпоширеніші OID для моніторингу маршрутизаторів MikroTik

Параметр	OID	Опис
Завантаження CPU	.1.3.6.1.2.1.25.3.3.1.2.1	Відсоток використання процесора пристрою
Використання RAM	.1.3.6.1.2.1.25.2.3.1.6.0	Кількість використаної оперативної пам’яті в байтах
Обсяг RAM	.1.3.6.1.2.1.25.2.2.0	Обсяг оперативної пам’яті в байтах
Вхідний трафік інтерфейсу	.1.3.6.1.2.1.31.1.1.1.6.2	Кількість байтів, отриманих інтерфейсом
Вихідний трафік інтерфейсу	.1.3.6.1.2.1.31.1.1.1.10.2	Кількість байтів, переданих інтерфейсом
Час роботи	.1.3.6.1.2.1.1.3.0	Визначає час роботи маршрутизатора

1.5 Постановка завдання дослідження

У результаті аналізу теоретичних відомостей та літературних джерел встановлено, що на сьогодні існує значна кількість систем моніторингу, які відрізняються функціональністю, складністю налаштування та вимогами до ресурсів. Комерційні продукти часто мають широкі можливості, однак їх використання обмежується ліцензійними умовами та фінансовими витратами. Натомість системи з відкритим вихідним кодом, зокрема Nagios, дозволяють створювати гнучкі та масштабовані рішення без додаткових витрат, що є особливо актуальним для навчальних середовищ і невеликих організацій.

Використання віртуального середовища дозволяє змоделювати реальну мережу, дослідити взаємодію її компонентів і перевірити ефективність системи моніторингу в контрольованих умовах. Такий підхід є доцільним як для навчальних цілей, так і для попереднього проєктування мережових рішень.

З урахуванням результатів проведеного аналізу теоретичних матеріалів та існуючих рішень метою даного дослідження є розроблення та практична реалізація системи моніторингу на базі рішення Nagios та обладнання MikroTik у віртуальному середовищі. Для досягнення поставленої мети в роботі необхідно вирішити такі основні завдання:

- розробити просту топологію локальної мережі в емуляторі GNS3;
- вибрати необхідне обладнання та програмне забезпечення для мережі;
- розробити IP-адресний план;
- налаштувати мережеве обладнання та перевірити зв'язок між пристроями у мережі;
- розгорнути систему моніторингу Nagios Core;
- налаштувати моніторинг хостів мережі, зокрема маршрутизатора MikroTik;
- провести тестування та перевірити роботу налаштованої системи моніторингу Nagios.

Висновки з розділу 1

У першому розділі кваліфікаційної роботи було розглянуто загальну характеристику мережевого моніторингу. Було визначено, що його основною метою є відстеження стану всіх компонентів мережі та швидке реагування на проблеми.

Було оглянуто чотири найпоширеніші програмні рішення для моніторингу мережі: Nagios, Zabbix, PRTG Network Monitor, SolarWinds Network Performance Monitor. Усі вони забезпечують подібні функції. Для реалізації проєкту було обрано систему Nagios, яка є безкоштовним, гнучким рішенням для моніторингу з відкритим вихідним кодом. Компонентами цієї системи є конфігураційні файли, плагіни, агенти, ядро та веб-інтерфейс. Перевірки у системі Nagios можуть бути як активними, так і пасивними.

Після цього відбулося ознайомлення з обладнанням MikroTik та можливостями моніторингу маршрутизаторів. RouterOS, що є операційною системою маршрутизаторів MikroTik, має підтримку протоколу SNMP. Саме завдяки SNMP є можливість збирати інформацію з маршрутизатора.

РОЗДІЛ 2. ПРОЄКТУВАННЯ МЕРЕЖІ НА БАЗІ РІШЕННЯ NAGIOS ТА ОБЛАДНАННЯ MIKROTIK

2.1 Опис проєктованої мережі

Мережа даної кваліфікаційної роботи має продемонструвати практичне впровадження системи моніторингу Nagios із застосуванням маршрутизатора MikroTik, серверної інфраструктури та робочих станцій. Мережа створюється як невелика корпоративна інфраструктура, що відповідає типовим умовам роботи малого офісу, де необхідно забезпечити постійний контроль за доступністю сервісів, продуктивністю обладнання та стабільністю мережевої взаємодії. Таким чином, проєкт виглядатиме наближеним до реальних умов експлуатації в організаціях.

У попередньому розділі було визначено основні кроки та завдання для побудови системи моніторингу Nagios: розроблення топології мережі, вибір обладнання та програмного забезпечення, розроблення IP-адресації, розгортання системи моніторингу Nagios, налаштування моніторингу хостів та проведення тестування. Для реалізації поставлених завдань обов'язково знадобиться Nagios-сервер та маршрутизатор MikroTik. Також потрібна робоча станція з Windows 10, на якій можна слідкувати за роботою Nagios та переглядати стан пристроїв мережі.

У центрі мережі розташований простий комутатор *Switch*, який з'єднує усі пристрої в мережі та маршрутизатор *Mikrotik-Router*, який виконує роль основного вузла маршрутизації та забезпечує взаємодію між усіма мережевими сегментами. Крім того, що він відповідає за розподіл трафіку, він також виступає об'єктом моніторингу. Дані з маршрутизатора передаються за допомогою SNMP. Це дозволяє відстежувати стан обладнання в реальному часі.

Основою серверної інфраструктури є окремий віртуальний сервер на базі Ubuntu Server, на якому розгортається Nagios Core. Сервер моніторингу виступає як центральний елемент логічної топології, приймаючи та обробляючи дані від усіх контрольованих вузлів. Через веб-інтерфейс відображаються результати

перевірок, графіки, статуси пристроїв. На цьому ж сервері можуть бути розміщені додаткові агенти або модулі, необхідні для розширення функціональності Nagios.

Клієнтські робочі станції *Win-Workstation* та *Linux-Workstation* використовуватимуться для тестування підключень, перевірки пінгів, доступу до інтерфейсу Nagios та перегляд результатів моніторингу стану пристроїв мережі. Моніторинг цих пристроїв відбуватиметься через два агенти: NSClient++ та NSCPA.

На рис. 2.1 показано схематичне зображення мережі.

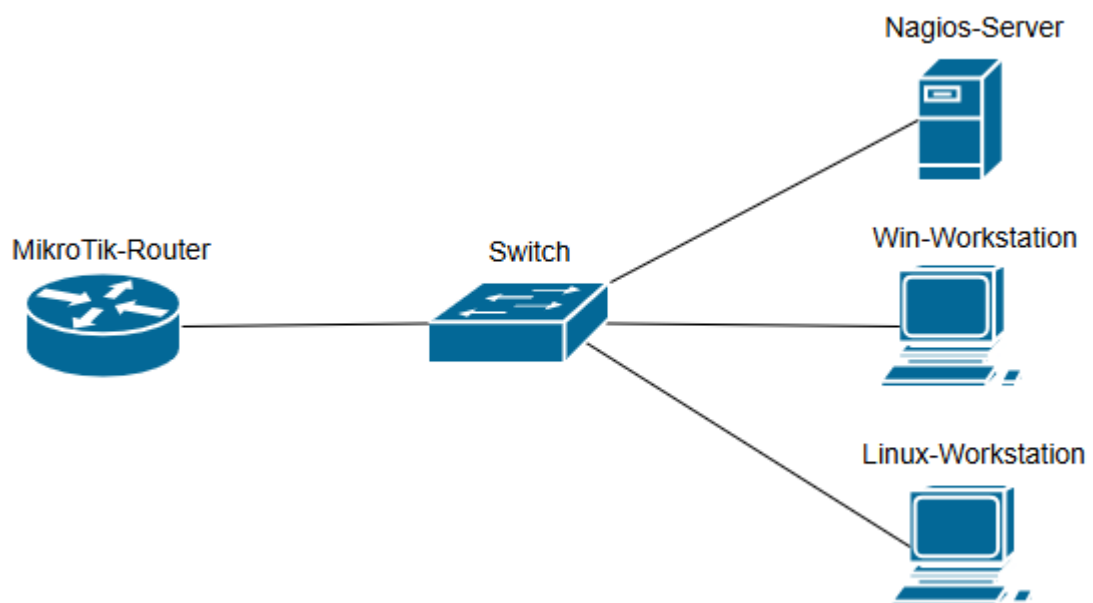


Рисунок 2.1 – Топологія мережі

У моделі також передбачена можливість масштабування. За потреби в топологію можна додати додаткові сервери, комутатори або маршрутизатори, що дозволяє адаптувати мережу до складніших сценаріїв. Це робить описану топологію не лише демонстраційною, а й універсальною платформою для подальших досліджень у галузі мережевого моніторингу та оптимізації інфраструктури.

У ролі маршрутизатора в даній мережі використовуватиметься віртуальний образ MikroTik CHR, який дозволяє легко налаштовувати

маршрутизацію, DHCP, NAT, Firewall тощо. MikroTik є популярним вибором у реальних мережах завдяки широкому функціоналу.

Комутатором є Ethernet Switch. Це базовий L2-комутатор у GNS3. Він забезпечує з'єднання всіх пристроїв у локальній мережі.

У ролі сервера використовуватиметься віртуальна машина Ubuntu Server 22.04 LTS. На цьому сервері встановлюється та налаштовується система моніторингу Nagios Core, що дозволяє здійснювати моніторинг стану інших пристроїв у мережі.

Віртуальна машина з Windows 10 виконує роль клієнтського пристрою, який підлягає моніторингу через Nagios. Віртуальна машина з ОС Linux під дистрибутивом Ubuntu 22.04 LTS, який використовує менше ресурсів, є ще одним клієнтським пристроєм.

На рис. 2.2 представлена зібрана схема мережі в емуляторі GNS3.

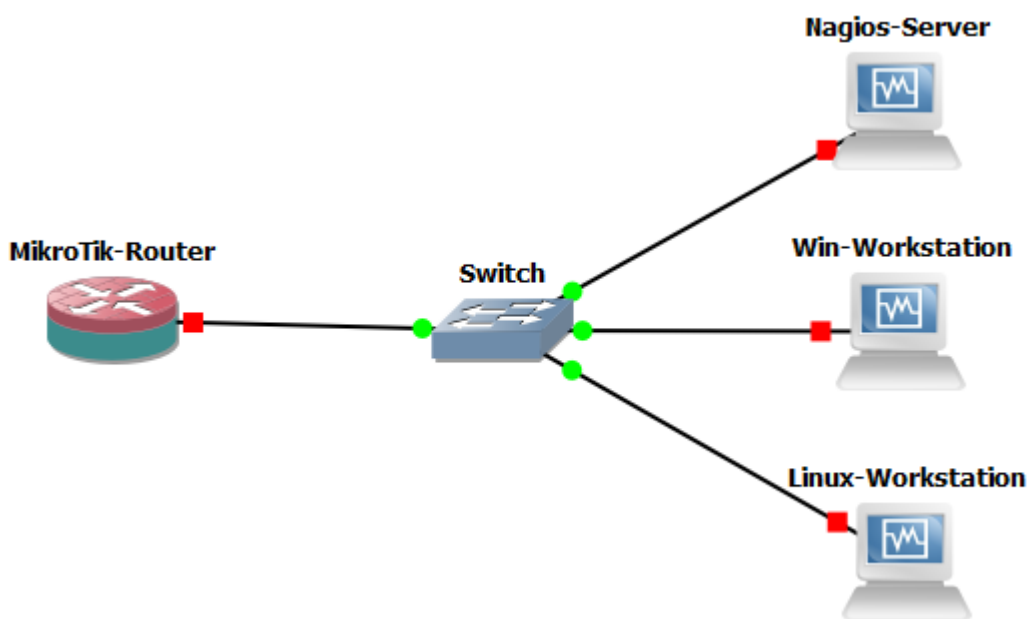


Рисунок 2.2 – Створена мережа в GNS3

2.2 Розроблення схеми адресації пристроїв мережі

На наступному кроці варто розробити систему IP-адресації мережі. Для спрощення конфігурації та уникнення конфліктів було використано статичну IP-адресацію у мережі 192.8.1.0/28. Мережа має префікс /28. Вибір такого префіксу зумовлений невеликим розміром розробленої топології. При цьому кількість

невикористаних адрес дозволяє в майбутньому додавати нові хости в дану мережу.

Таблиця 2.1

Розрахунок IP-адреси мережі

Призначення	IP-адреса
Адреса мережі	192.8.1.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	192.8.1.1
Максимальна адреса	192.8.1.14
Широкомовна адреса	192.8.1.15
Шлюз за замовчуванням	192.8.1.1
Діапазон використаних адрес	192.8.1.1 – 192.8.1.4
Діапазон невикористаних адрес	192.8.1.5 – 192.8.1.14

Маршрутизатор MikroTik-Router має IP-адресу 192.8.1.1, яка використовується як шлюз за замовчуванням для всіх внутрішніх пристроїв. Такий вибір є типовим і дозволяє уникнути конфліктів та забезпечити інтуїтивну зрозумілість конфігурації. Зрозумілість конфігурації зберігається і в подальших призначеннях IP-адрес, де кожному пристрою належить наступна по порядку IP-адреса з мережі.

Важливе значення має узгодження адресної схеми з можливостями моніторингу. Для SNMP-контролю MikroTik необхідно надати доступ до його внутрішньої IP-адреси, тому саме використання фіксованої адресації забезпечує стабільність роботи системи моніторингу та виключає можливість зміни IP-адреси маршрутизатора внаслідок DHCP або некоректної конфігурації. Сервер Nagios, який виконує роль централізованого вузла збору даних, також повинен мати статичну адресу, оскільки всі перевірки в системі налаштовуються на конкретні IP-адреси пристроїв. Статична адресація серверів і маршрутизатора створює стабільну основу для плагінів Nagios, включаючи ICMP-перевірки, SNMP-запити та виконання агентських команд через NSClient++, NCPA або NRPE.

Параметри IP-адресації мережі

Мережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска
Мережа	—	192.8.1.0	255.255.255.240
Маршрутизатор MikroTik-Router	Інтерфейс Eth0	192.8.1.1	255.255.255.240
Ubuntu-сервер Nagios-Server	Мережний адаптер	192.8.1.2	255.255.255.240
	Шлюз за замовчуванням/DNS	192.8.1.1	—
Робоча станція Win-Workstation	Мережний адаптер	192.8.1.3	255.255.255.240
	Шлюз за замовчуванням/DNS	192.8.1.1	—
Робоча станція Linux-Workstation	Мережний адаптер	192.8.1.4	255.255.255.240
	Шлюз за замовчуванням/DNS	192.8.1.1	—

Обраний IP-план дозволяє чітко структурувати мережу та однозначно ідентифікувати всі її елементи. Такий підхід мінімізує кількість можливих помилок під час налаштування Nagios, особливо при створенні конфігураційних файлів, які містять статичні записи про мережеві хости, сервіси.

2.3 Вибір характеристик для моніторингу

Ефективність системи моніторингу напряму залежить від правильного визначення параметрів, за якими відслідковується стан мережевого обладнання. У випадку маршрутизатора MikroTik ключовим завданням є вибір таких параметрів, які всебічно оцінюють працездатність пристрою та виявляють потенційні проблеми на ранніх етапах. Система Nagios підтримує широкі можливості інтеграції з MikroTik через протокол SNMP, що дозволяє отримувати різноманітні показники в реальному часі.

Умовно параметри для моніторингу можна розділити на кілька груп: моніторинг апаратних ресурсів, таких як CPU та RAM, доступність мережевих вузлів, моніторинг мережевих інтерфейсів та інші специфічні перевірки. Разом

ці показники формують достатньо повну картинну стану мережевого обладнання.

Одним із ключових параметрів є CPU. Рівень завантаження процесора безпосередньо впливає на швидкість маршрутизації, обробку пакетів і стабільність роботи системи. Високі значення CPU Load можуть свідчити про перевантаження маршрутизатора або некоректну конфігурацію трафіку. Моніторинг цього параметра дає змогу своєчасно виявляти аномальні навантаження та реагувати на них до появи більш критичних збоїв. У випадку робочих станцій та сервера Nagios контроль процесора дозволяє своєчасно запобігати ситуаціям, коли робочі служби починають працювати нестабільно або споживають надмірні ресурси. Те саме стосується і для використання оперативної пам'яті. Перевищення допустимих значень може призвести до уповільнення або нестабільності роботи системи, тому Nagios повинен відслідковувати цей показник із заданими порогоми попередження й критичного стану.

За допомогою ICMP-запитів перевіряється доступність мережевих вузлів. Перевірка ring дає змогу зафіксувати затримки, втрати пакетів або повну недоступність, що є одним із найпростіших, але дуже ефективних способів контролю стану мережевої інфраструктури. Для маршрутизатора MikroTik перевірка доступності є надзвичайно критичною, оскільки його вихід із ладу або затримки у відповідях впливають на всю інфраструктуру.

Особлива увага приділяється моніторингу мережевих інтерфейсів. Через SNMP-перевірки здійснюється оцінка вхідного та вихідного трафік, стану інтерфейсів, рівня помилок. Це дозволяє побачити момент раптового збільшення трафіку та виявити неполадки, пов'язані з фізичними або логічними мережевими з'єднаннями.

Окрему групу становлять специфічні перевірки для кожного типу пристроїв. До цієї групи можна віднести параметр Uptime – час безперервної роботи пристрою. Його відстеження дозволяє виявляти незаплановані перезавантаження пристрою і оцінити загальну стабільність роботи обладнання.

Для Ubuntu-сервера виконуються локальні скрипти, що дозволяють перевіряти статус служб, розподіл дискового простору, роботу певних протоколів, наприклад SSH.

Для забезпечення комплексного контролю роботи маршрутизатора MikroTik було обрано п'ять характеристик: завантаження процесора, використання оперативної пам'яті, доступність пристрою через ring, стан мережевих інтерфейсів та загальний час роботи. Ці показники забезпечують повноцінний огляд функціонування маршрутизатора. CPU і RAM дозволяють оцінити внутрішній ресурсний стан пристрою, інтерфейси – якість передачі даних, ring – доступність у мережі, а показник uptime – стабільність роботи.

Моніторинг характеристик на робочих станціях дещо відрізняється. Відстеження значень навантаження процесора та оперативної пам'яті, доступність пристрою визначено як основні сервіси для моніторингу, тому ці характеристики повинні відстежуватися на всіх пристроях мережі. Окрім них, було обрано моніторинг мережевих інтерфейсів, обсяг вільного простору на диску, час роботи.

На Nagios-Server при розгортанні системи моніторингу Nagios Core автоматично конфігурується файл для моніторингу сервісів. Серед них можна відзначити такі ключові характеристики, як навантаження процесора та доступність пристрою. Кілька інших метрик, що відстежуються – це моніторинг розподілу дискового розділу, роботи протоколів SSH та HTTP, перевірка числа користувачів, що увійшли в систему, та кількості запущених процесів.

Для забезпечення моніторингу кожного пристрою використовуються різні плагіни. Плагін `check_snmp` використовується для збору статистики з маршрутизатора MikroTik-Router, `check_ncpa` та `check_nt` забезпечують взаємодію з робочими станціями Linux та Windows відповідно, а на Nagios-Server виконуються локальні системні перевірки за допомогою команди `check_local`. У таблиці 2.3 подано узагальнену інформацію про те, які характеристики відслідковуються, які плагіни використовуються на кожному пристрої.

Параметри моніторингу

Пристрій	Агент/Протокол	Плагін	Показники
MikroTik-Router	SNMP	check_snmp	CPU, RAM, час роботи, інтерфейс
Nagios-Server	Локальні системні перевірки	check_local	CPU, доступність, SSH, HTTP, число користувачів та процесів, дисковий простір
Win-Workstation	NSClient++	check_nt	CPU, RAM, час роботи, доступність, інтерфейс, дисковий простір
Linux-Workstation	NCPA	check_ncpa	CPU, RAM, час роботи, доступність, інтерфейс, дисковий простір

Висновки з розділу 2

У результаті написання другого розділу було спроектовано топологію мережі. Вона складається з маршрутизатора MikroTik-Router, Nagios-Server, Switch, робочих станцій Win-Workstation та Linux-Workstation. Після цього, відповідно до топології, мережу було зібрано в емуляторі GNS3.

Було розроблено схему адресації пристроїв мережі, яка має певний простір для можливого розширення в майбутньому. Обрано статичну IP-адресацію в мережі 192.8.1.0/28.

Також було обрано, за якими показниками вестиметься спостереження на кожному хості. Базовими показниками для моніторингу є навантаження процесора, використання оперативної пам'яті, доступність пристрою, обсяг вільного дискового простору. Для моніторингу кожного пристрою використовуються різні агенти, плагіни.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ NAGIOS

3.1 Базове налагодження пристроїв мережі

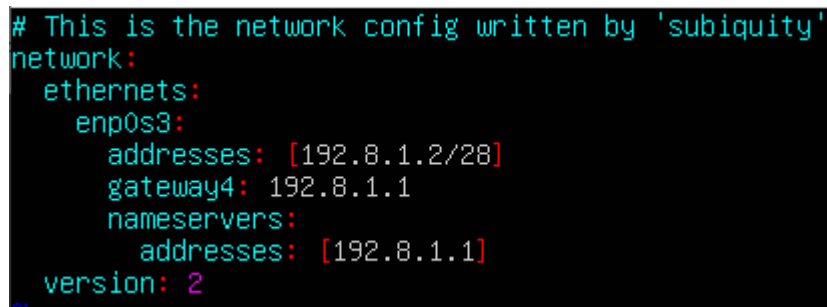
На цьому етапі відбувається іменування пристроїв мережі та налаштування IP-адресації для стабільного інформаційного обміну між ними. Для призначення IP-адреси певному інтерфейсу на маршрутизаторі MikroTik потрібно скористатися командою:

```
ip address add address=192.8.1.1/28 interface=ether1
```

Зміна імені маршрутизатора MikroTik відбувається командою:

```
system identity set name=MikroTik-Router
```

Окрім маршрутизатора, IP-адреси потрібно призначити також для Ubuntu-сервера та робочих станцій. Налаштування параметрів IP-адресації на Ubuntu-сервері відбуваються в конфігураційних файлах Netplan, що зберігаються в каталозі /etc/netplan. У даному випадку потрібно відкрити файл 00-installer-config.yaml і в цьому файлі внести дані відповідно до розробленої схеми IP-адресації (рис. 3.1).



```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses: [192.8.1.2/28]
      gateway4: 192.8.1.1
      nameservers:
        addresses: [192.8.1.1]
  version: 2
```

Рисунок 3.1 – Налаштування IP-адресації Ubuntu-сервера

Командою для перейменування сервера є:

```
sudo hostnamectl set-hostname Nagios-Server
```

Робочі станції Win-Workstation та Linux-Workstation дозволяють здійснювати налаштування засобами графічного інтерфейсу. На рис. 3.2-3.3 показано мережеве налаштування обох станцій.

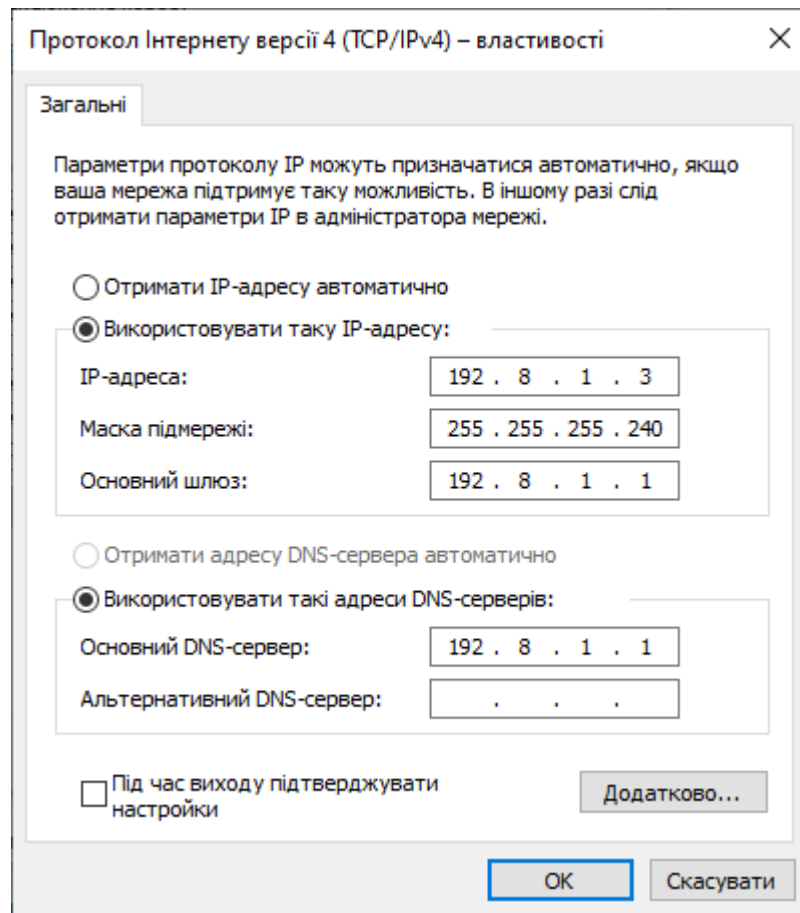


Рисунок 3.2 – Налаштування IP-адресації робочої станції Win-Workstation

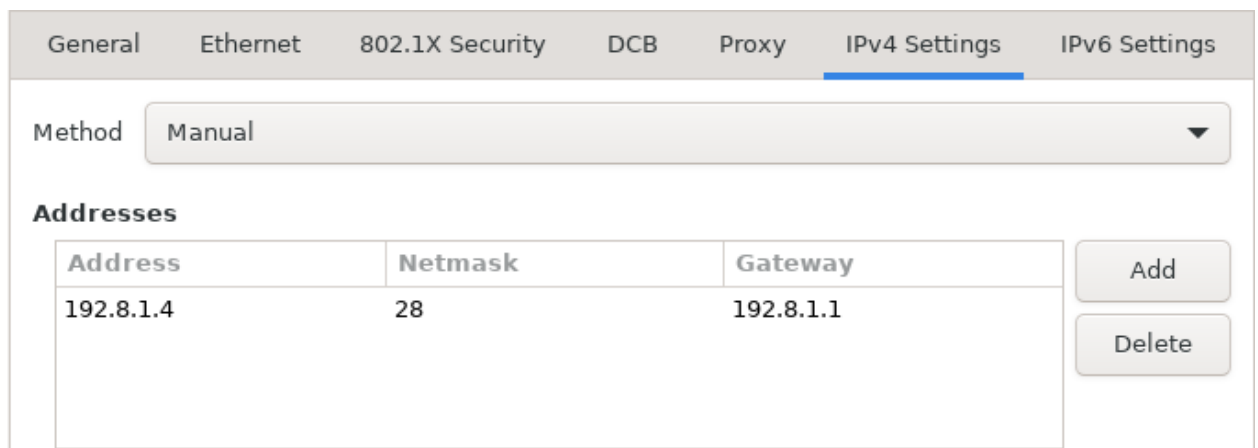


Рисунок 3.3 – Налаштування IP-адресації робочої станції Linux-Workstation

Щоб переконатися у правильності налагодження IP-адресації мережі, варто перевірити з'єднання між пристроями за допомогою службової команди ping (рис. 3.4).

```
C:\Windows\system32>ping 192.8.1.1

Pinging 192.8.1.1 with 32 bytes of data:
Reply from 192.8.1.1: bytes=32 time=8ms TTL=64
Reply from 192.8.1.1: bytes=32 time=6ms TTL=64
Reply from 192.8.1.1: bytes=32 time=18ms TTL=64
Reply from 192.8.1.1: bytes=32 time=29ms TTL=64

Ping statistics for 192.8.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 29ms, Average = 15ms

C:\Windows\system32>ping 192.8.1.2

Pinging 192.8.1.2 with 32 bytes of data:
Reply from 192.8.1.2: bytes=32 time=9ms TTL=64
Reply from 192.8.1.2: bytes=32 time=7ms TTL=64
Reply from 192.8.1.2: bytes=32 time=43ms TTL=64
Reply from 192.8.1.2: bytes=32 time=11ms TTL=64

Ping statistics for 192.8.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 43ms, Average = 17ms

C:\Windows\system32>ping 192.8.1.4

Pinging 192.8.1.4 with 32 bytes of data:
Reply from 192.8.1.4: bytes=32 time=13ms TTL=64
Reply from 192.8.1.4: bytes=32 time=7ms TTL=64
Reply from 192.8.1.4: bytes=32 time=9ms TTL=64
Reply from 192.8.1.4: bytes=32 time=40ms TTL=64

Ping statistics for 192.8.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 40ms, Average = 17ms
```

Рисунок 3.4 – Результат успішної перевірки зв'язку між робочою станцією Win-Workstation та маршрутизатором MikroTik-Router, сервером Nagios-Server, робочою станцією Linux-Workstation

3.2 Встановлення та налаштування система моніторингу Nagios

Фундаментальним завданням проєкту можна назвати розгортання системи моніторингу Nagios. Для цього буде використовуватися Ubuntu-сервер. Спочатку потрібно підготувати систему. Команди *sudo apt update* та *sudo apt upgrade* оновлюють локальну базу даних пакетів та фактично оновлюють встановлені пакети. І після цього відбувається встановлення всіх необхідних пакунків:

- wget – надає можливість завантажувати файли з Інтернету;
- build-essential – це набір інструментів для компіляції програм з вихідних кодів;
- apache2 – веб-сервер Apache2, який буде використовуватися разом з Nagios;
- php – це мовний пакет програмування PHP;
- openssl – бібліотека для реалізації протоколів шифрування;
- perl – мова програмування Perl та інші пакети, необхідні для підтримки різних функціональностей.

На момент розроблення проєкту останньою стабільною версією Nagios була 4.5.10. Завантажується архів, який треба розпакувати та після цього проводити подальші дії для встановлення Nagios.

Встановлення системи моніторингу відбувається за допомогою наступного переліку команд:

```
sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled
sudo make all
sudo make install
sudo make install-init
sudo make install-commandmode
sudo make install-config
sudo /usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-enabled/nagios.conf
```

Створено користувача Nagios та надано йому права для перегляду статусу моніторингу, графіки, журнали подій та іншу інформацію.

```
authorized_for_system_information=nagios
authorized_for_configuration_information=nagios
authorized_for_system_commands=nagios
authorized_for_all_services=nagios
authorized_for_all_hosts=nagios
authorized_for_all_service_commands=nagios
authorized_for_all_host_commands=nagios
```

Далі вмикається модуль Rewrite та CGI, перезапускається служба Apache.

```
sudo a2enmod rewrite
sudo a2enmod cgi
```

```
sudo a2enmod restart apache2  
sudo vi /etc/apache2/apache2.conf
```

У конфігураційному файлі Apache потрібно додати рядок, де вказується ім'я серверу. У даному випадку це виглядає: *ServerName 192.8.1.2*.

Також знадобляться плагіни Nagios останньої стабільної версії. Дії схожі до встановлення самого Nagios. Завантажується архів, який потрібно розпакувати. Далі подано перелік команд, за допомогою яких встановлюються плагіни Nagios:

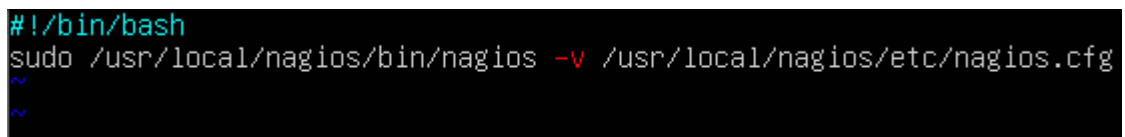
```
./configure  
sudo make  
sudo make install
```

/usr/local/nagios/etc/htpasswd.users – це файл паролів користувачів системи моніторингу. Він створюється за допомогою утиліти *htpasswd*.

```
sudo /usr/local/nagios/etc/htpasswd.users nagios
```

Основні налаштування щодо розгортання системи моніторингу Nagios на Ubuntu-сервері здійснено. Кожного разу після внесення змін у файли конфігурації системи варто здійснювати загальну перевірку. Щоб не друкувати постійно доволі громіздкий рядок, можна створити окрему просту команду з наданням їй потрібних дозволів: *checknagios* (рис. 3.5).

```
sudo vi /bin/checknagios  
sudo chmod 777 /bin/checknagios
```



```
#!/bin/bash  
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg  
~  
~
```

Рисунок 3.5 – Створення команди *checknagios*

Nagios налаштовано на Ubuntu-сервері. Отримати доступ до веб-інтерфейсу Nagios можна через робочу станцію Win-Workstation. Для цього у пошуковому рядку веб-браузера вводиться адреса сервера та додається «*/nagios*»: *192.8.1.2/nagios*.

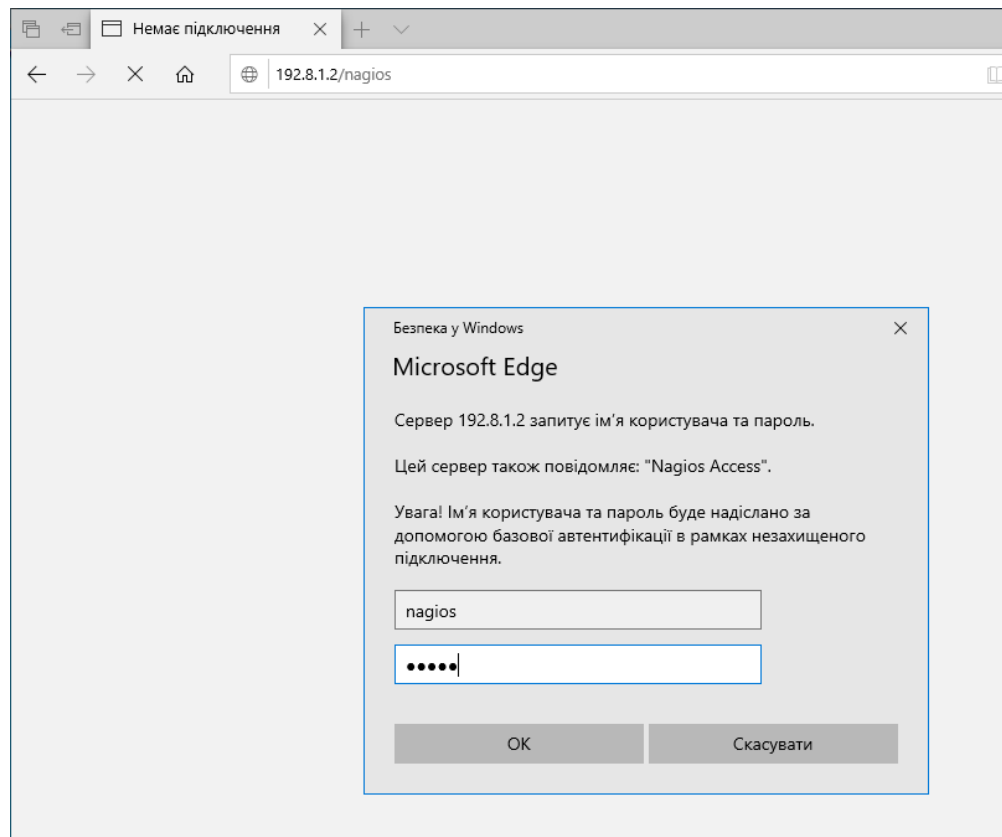


Рисунок 3.6 – Вхід до веб-інтерфейсу Nagios

Система запитає пароль та логін користувача (рис. 3.6). Після введення облікових даних раніше створеного користувача Nagios відбудеться підключення до системи моніторингу Nagios (рис. 3.7).

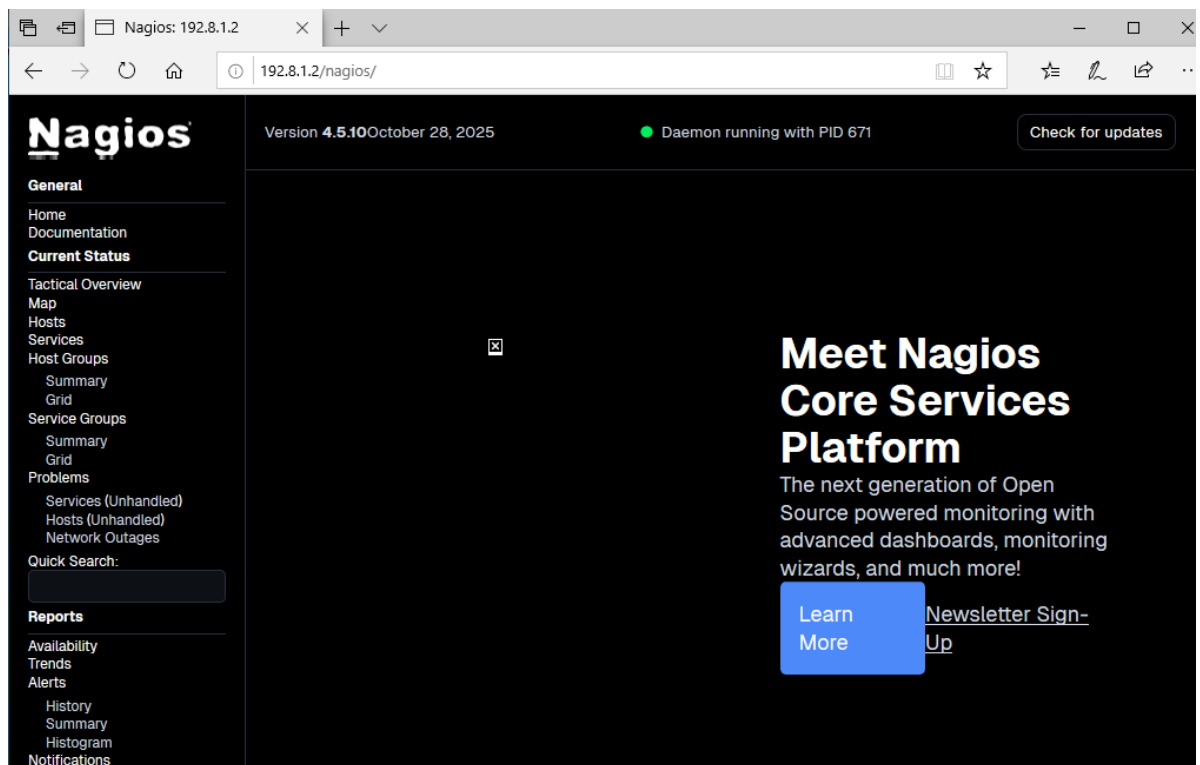


Рисунок 3.7 – Головна сторінка Nagios

3.3 Налаштування моніторингу всіх вузлів мережі

На Nagios-Server, де розгорнуто систему моніторингу, присутній каталог `/usr/local/nagios/etc/objects`. Він є одним із ключових елементів конфігураційної структури Nagios Core. Саме тут розміщуються шаблони, стандартні описи хостів і сервісів, приклади конфігурацій, які можна використати як основу для створення власної системи моніторингу. У ньому міститься кілька конфігураційних файлів:

- *commands.cfg*: файл для визначення команд, які використовуються для виконання перевірок необхідних сервісів;
- *localhost.cfg* містить уже налаштовану конфігурацію для моніторингу локального хосту. Саме цю конфігурацію видно на веб-інтерфейсі Nagios одразу після його розгортання;
- *switch.cfg*. У цьому конфігураційному файлі здійснюється налаштування моніторингу мережевого обладнання, наприклад комутаторів або маршрутизаторів;
- *timeperiods.cfg* – файл для визначення періодів часу, коли моніторинг працює або вимкнений;
- *contacts.cfg* відповідає за визначення осіб, яким прийде повідомлення про певні проблеми;
- *printer.cfg* використовується для моніторингу принтерів;
- *templates.cfg*. У цьому файлі можна визначити шаблони для спрощення конфігурації. Такі шаблони визначають властивості, які є спільними для груп хостів або сервісів;
- *windows.cfg* – файл для моніторингу Windows-серверів. Тут уже міститься зразок конфігурації.

Ці файли конфігурації включені в головний конфігураційний файл `/usr/local/nagios/etc/nagios.cfg`. При додаванні нових файлів або каталогів, у яких визначаються об'єкти моніторингу, обов'язково потрібно вказувати їх у головному конфігураційному файлі за допомогою директиви *cfg_file* або *cfg_dir*.

Для даної моделі комп'ютерної мережі доцільно буде поділити об'єкти моніторингу на машини з операційною системою Windows та Linux, а також мережеве обладнання. Тому потрібно створити окремі підкаталоги для кожної групи об'єктів моніторингу та вказати їх у головному конфігураційному файлі [16] (рис. 3.8).

```
student@Nagios-Server:~$ dir /usr/local/nagios/etc/objects
commands.cfg  hostgroups.cfg  network        switch.cfg     timeperiods.cfg
contacts.cfg  linux           printer.cfg    templates.cfg  windows
```

Рисунок 3.8 – Створено підкаталоги windows, linux та network

Директиви, які необхідно додати до nagios.cfg:

```
cfg_dir=/usr/local/nagios/etc/objects/windows
cfg_dir=/usr/local/nagios/etc/objects/linux
cfg_dir=/usr/local/nagios/etc/objects/network
```

Згідно з ідеєю проєкту, у підкаталозі linux знаходяться Nagios-Server та Linux-Workstation, у підкаталозі windows – Win-Workstation, а у network – MikroTik-Router. Саме такі групи об'єктів моніторингу в результаті мають відображатися у веб-інтерфейсі Nagios Core. Тому файл для моніторингу Nagios-Server localhost.cfg переноситься до підкаталогу, зарезервованого для групи хостів з ОС Linux. За замовчуванням цьому хосту надано ім'я localhost, яке зручніше буде змінити на реальну назву машини.

У файлі /usr/local/nagios/etc/objects/linux/localhost.cfg уже присутня конфігурація. На рис. 3.9. зображено фрагмент цієї конфігурації, де налаштовано три сервіси для моніторингу: використання команди ring, перевірка дискового простору кореневого розділу та перевірка числа користувачів, що увійшли в систему. До кожного сервісу додано пояснення у вигляді коментарів. Усі сервіси мають певні порогові значення. Наприклад, для сервісу Root Partition значення, що є меншим за 20%, але більшим за 10%, відповідає стану «WARNING». Якщо значення менше за 10%, тоді стан змінюється на «CRITICAL». Усе, що більше за 20%, вважається оптимальним та відповідає стану «OK». Як видно з рис. 3.10, вільно 39,6% дискового простору кореневого розділу, отже стан служби «OK». Окрім Root Partition, на сервері проводиться моніторинг ще семи сервісів: Current

Load, Current Users, HTTP, PING, SSH, Swap Usage, Total Processes. Наразі усі вони перебувають у нормальному стані.

```
# Define a service to "ping" the local machine

define service {

    use                local-service                ; Name of service template to use
    host_name          Nagios-Server
    service_description PING
    check_command       check_ping!100.0,20%!500.0,60%
}

# Define a service to check the disk space of the root partition
# on the local machine. Warning if < 20% free, critical if
# < 10% free space on partition.

define service {

    use                local-service                ; Name of service template to use
    host_name          Nagios-Server
    service_description Root Partition
    check_command       check_local_disk!20%!10%!/
}

# Define a service to check the number of currently logged in
# users on the local machine. Warning if > 20 users, critical
# if > 50 users.

define service {

    use                local-service                ; Name of service template to use
    host_name          Nagios-Server
    service_description Current Users
    check_command       check_local_users!20!50
}
```

Рисунок 3.9 – Фрагмент конфігурації localhost.cfg

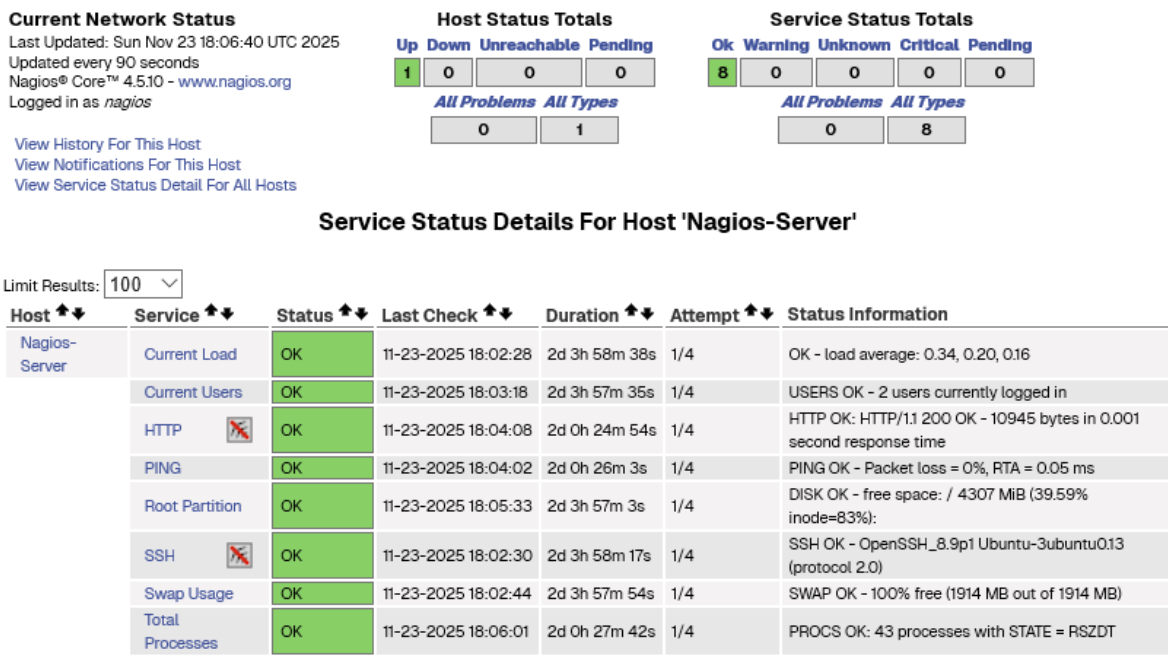


Рисунок 3.10 – Стан служб Nagios-Server

Оскільки моніторинг Ubuntu-сервера налаштовано, час переходити до налаштування моніторингу робочих станцій Win-Workstation та Linux-Workstation. Щоб ефективно моніторити віддалені хости, використовуються спеціальні агенти. У випадку Nagios існують три популярні рішення для моніторингу хостів:

1. NCPA. Цей агент може встановлюватися на операційні системи Windows, Linux/Unix, Mac OS/X. Серед його функцій є активні та пасивні перевірки, віддалене керування та локальний інтерфейс моніторингу.

2. NSClient++ – це агент моніторингу для систем Microsoft Windows. Він робить моніторинг машин Windows простим.

3. NRPE. Цей агент дозволяє віддалено запускати плагіни Nagios на інших машинах Linux/Unix. NRPE також може взаємодіяти з агентами для Windows, такими як NSClient++, тому перевірка показників на віддалених машинах Windows також можлива [15].

На робочій станції Win-Workstation використовуватиметься агент NSClient++ [21].

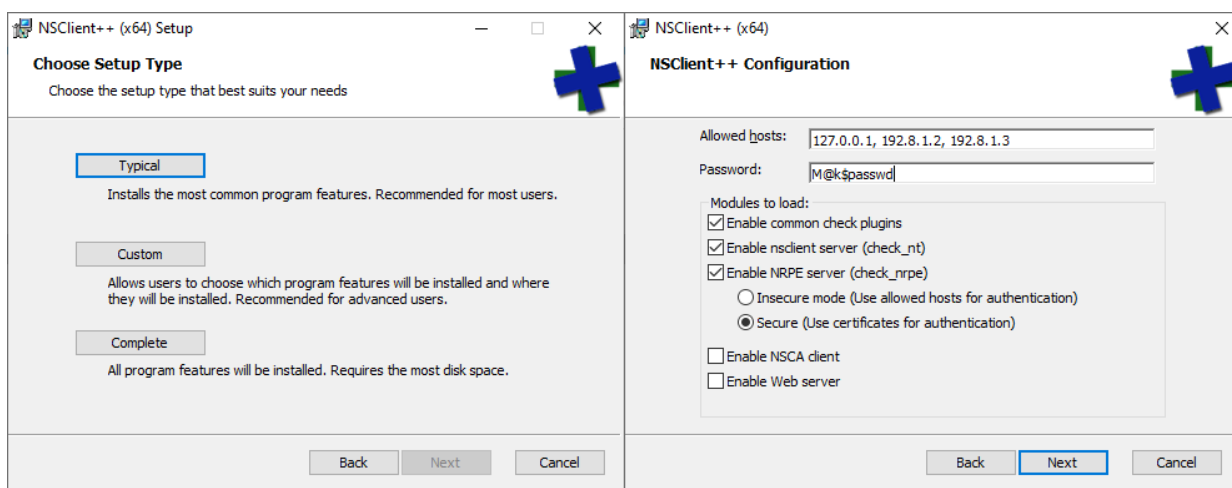


Рисунок 3.11 – Встановлення агента NSClient++

На етапі встановлення обирається типова інсталяція, вказуються адреси дозволених хостів, пароль підключення NSClient++ (рис. 3.11). У процесі встановлення автоматично конфігуруються відповідні служба та правило у Windows Firewall. У файлі C:\Program Files\NSClient++\nsclient.ini потрібно перевірити, щоб значення ключів CheckEventLog, CheckDisk, CheckSystem було

enabled. Окрім цього, у даному файлі можна змінити деякі параметри, які вказувалися під час встановлення NSClient++, наприклад пароль. Оскільки роботу агента NSClient++ на робочій станції налаштовано, можна переходити до конфігурування Nagios для взаємодії з NSClient++. Для взаємодії з NSClient++ використовується команда *check_nt*. За моніторинг робочої станції Win-Workstation відповідатиме окремий конфігураційний файл *win-workstation.cfg*, який знаходиться у відповідному каталозі */usr/local/nagios/etc/objects/windows*. Для створення цього файлу у ролі шаблону використовується файл */usr/local/nagios/etc/objects/windows.cfg*, який потім буде перейменований на *hostgroups.cfg* та відповідатиме за визначення груп хостів моніторингу. Далі показано, за допомогою яких команд визначається хост, який буде моніторитися.

```
define host {
    use                windows
    host_name          Win-Workstation
    alias              Windows Workstation
    address            192.8.1.3
    hostgroups         win-workstations
}
```

Схожим чином налаштовується моніторинг певних сервісів. Далі показано приклад таких конфігурацій, а саме перевірка навантаження процесора, використання фізичної пам'яті та пам'яті на системному диску.

```
define service {
    use                generic-service
    host_name          Win-Workstation
    service_description CPU Usage
    check_command      check_nt !CPULOAD!-s M@kspasswd -l 5,80,90
}
```

```
define service {
    use                generic-service
    host_name          Win-Workstation
    service_description Memory Usage
    check_command      check_nt!MEMUSE!-s M@kspasswd -w 80 -c 90
}
```

```
define service {
    use                generic-service
    host_name          Win-Workstation
```

```

        service_description      C:\ Drive Space
        check_command            check_nt!USEDISKSPACE!-s M@kpasswd -l c -w 80 -
с 90
    }

```

Кожен сервіс має певні межі, після яких його стан стає попереджувальним або критичним. Окрім цих трьох сервісів, було налаштовано моніторинг інших, а саме час роботи машини, версія агента NSClient++ та процесу Explorer.exe.

На робочій станції Linux-Workstation використовуватиметься агент NSCPA для DEB Linux 64-bit. Він зручно завантажується з офіційного сайту Nagios. Для безпеки та автентифікації потрібно налаштувати спеціальні таємні ключі – токени. Для цього потрібно відкрити конфігураційний файл NSCPA /usr/local/ncpa/etc/ncpa.cfg. У ньому знадобиться встановити таємний ключ для WEB API у рядку `admin_password` та для пасивних перевірок у рядку `community_string`. Токени можуть відрізнятися, але в даному випадку було введено однакову послідовність. Основні налаштування агента NSCPA на Linux-Workstation здійснено. Для взаємодії з NSCPA використовується команда *check_ncpa*. Команда не встановлюється автоматично, тому спочатку її потрібно встановити та надати файлу скрипта цієї команди дозвіл на виконання. Для моніторингу цієї робочої станції створюється новий конфігураційний файл `linux-workstation` у каталозі `/usr/local/nagios/etc/objects/linux`. Далі показано, за допомогою яких команд визначається хост:

```

define host {
    host_name      Linux-Workstation
    address        192.8.1.4
    hostgroups     linux
    check_command  check_ncpa!-t    'M@kpasswd'    -P    5693    -M
system/agent_version
    max_check_attempts  5
    check_interval      5
    retry_interval      1
    check_period        24x7
    notification_interval 60
    notification_period  24x7
    notifications_enabled 1
}

```

Приклади конфігурацій для моніторингу навантаження процесора та кількості запущених процесів:

```
define service {
    host_name          Linux-Workstation
    service_description CPU Usage
    check_command       check_ncpa!-t 'ncpasswd' -P 5693 -M cpu/percent -w 40 -
c 60 -q 'aggregate=avg'
    max_check_attempts 5
    check_interval      5
    retry_interval      1
    check_period        24x7
    notification_interval 60
    notification_period 24x7
}
```

```
define service {
    host_name          Linux-Workstation
    service_description Process Count
    check_command       check_ncpa!-t 'ncpasswd' -P 5693 -M processes -w 150 -c
200
    max_check_attempts 5
    check_interval      5
    retry_interval      1
    check_period        24x7
    notification_interval 60
    notification_period 24x7
}
```

Для перевірки навантаження процесора налаштовано межі 40%, коли стан сервісу стає «WARNING», та 60%, коли стан – «CRITICAL». Щодо кількості процесів, то стан цього сервісу зміниться на «WARNING» при 150 запущених процесів, а при 200 і більше стан буде «CRITICAL». Також для цієї робочої станції було налаштовано моніторинг використання оперативної пам'яті, обсяг вільного простору на диску, кількість прочитаних байтів на фізичному диску, кількість записаних байтів на фізичний диск, час читання фізичного диску, час запису на фізичний диск, обсяг надісланих та отриманих байтів на мережевому інтерфейсі.

Для моніторингу мережевих пристроїв, таких як маршрутизатори або комутатори, використовується протокол SNMP. Основна робота з налаштування моніторингу маршрутизатора MikroTik-Router виконується на Ubuntu-сервері, де

розгорнута система моніторингу Nagios. На самому маршрутизаторі достатньо увімкнути SNMP:

```
snmp set enabled=yes
```

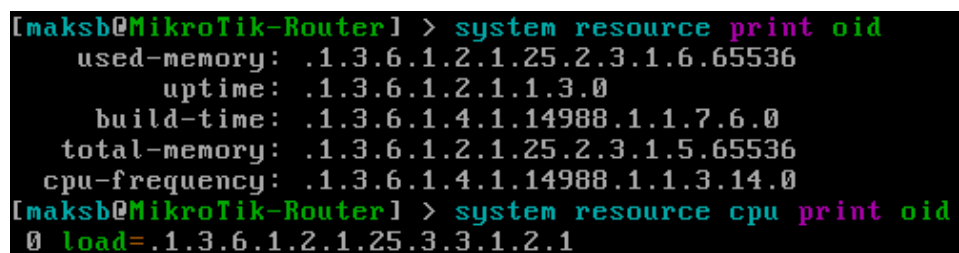
SNMP-моніторинг використовує плагін *check_snmp*. Якщо його немає в системі, то спочатку його потрібно завантажити з офіційного сайту Nagios. Команди для встановлення схожі до тих, які використовувалися для встановлення Nagios та плагінів. Готується збірка, запускається компіляція та встановлюються плагіни в системі:

```
sudo ./configure  
sudo make  
sudo make install
```

За маршрутизатор MikroTik-Router відповідає конфігураційний файл `/usr/local/nagios/etc/objects/network/mikrotik-router`. У ньому спочатку визначається хост для моніторингу [20].

```
define host {  
    use                generic-switch  
    host_name          mikrotik-router  
    alias              Mikrotik Router  
    address            192.8.1.1  
    hostgroups         network-devices  
}
```

Тепер можна переходити до налаштування сервісів, за станом яких буде вестися спостереження. Маршрутизатор MikroTik дозволяє переглянути значення OID для деяких сервісів, що стосуються системних показників (за допомогою команд *system resource print oid* та *system resource cpu print oid*) та мережевих інтерфейсів (за допомогою команди *interface print oid*) (рис. 3.12-3.13).



```
[maksb@MikroTik-Router] > system resource print oid  
used-memory: .1.3.6.1.2.1.25.2.3.1.6.65536  
uptime: .1.3.6.1.2.1.1.3.0  
build-time: .1.3.6.1.4.1.14988.1.1.7.6.0  
total-memory: .1.3.6.1.2.1.25.2.3.1.5.65536  
cpu-frequency: .1.3.6.1.4.1.14988.1.1.3.14.0  
[maksb@MikroTik-Router] > system resource cpu print oid  
0 load=.1.3.6.1.2.1.25.3.3.1.2.1
```

Рисунок 3.12 – OIDs для моніторингу системних показників

```

Flags: D - dynamic; X - disabled; I - inactive, R - running; S - slave;
P - passthrough
0   R   name=.1.3.6.1.2.1.2.2.1.2.2 actual-ntu=.1.3.6.1.2.1.2.2.1.4.2
      mac-address=.1.3.6.1.2.1.2.2.1.6.2
      admin-status=.1.3.6.1.2.1.2.2.1.7.2
      oper-status=.1.3.6.1.2.1.2.2.1.8.2
      bytes-in=.1.3.6.1.2.1.31.1.1.1.6.2
      packets-in=.1.3.6.1.2.1.31.1.1.1.7.2
      discards-in=.1.3.6.1.2.1.2.2.1.13.2
      errors-in=.1.3.6.1.2.1.2.2.1.14.2
      bytes-out=.1.3.6.1.2.1.31.1.1.1.10.2
      packets-out=.1.3.6.1.2.1.31.1.1.1.11.2
      discards-out=.1.3.6.1.2.1.2.2.1.19.2
      errors-out=.1.3.6.1.2.1.2.2.1.20.2

1   name=.1.3.6.1.2.1.2.2.1.2.3 actual-ntu=.1.3.6.1.2.1.2.2.1.4.3
      mac-address=.1.3.6.1.2.1.2.2.1.6.3
      admin-status=.1.3.6.1.2.1.2.2.1.7.3
      oper-status=.1.3.6.1.2.1.2.2.1.8.3
      bytes-in=.1.3.6.1.2.1.31.1.1.1.6.3
      packets-in=.1.3.6.1.2.1.31.1.1.1.7.3
      discards-in=.1.3.6.1.2.1.2.2.1.13.3
      errors-in=.1.3.6.1.2.1.2.2.1.14.3
      bytes-out=.1.3.6.1.2.1.31.1.1.1.10.3

```

Рисунок 3.13 – OIDs для моніторингу мережевих інтерфейсів

Оптимальним варіантом є моніторинг таких характеристик: навантаження процесора, кількість прийнятих байтів на мережевому інтерфейсі, час роботи, обсяг RAM-пам'яті, назва інтерфейсу, кількість прийнятих та переданих байтів на цьому інтерфейсі, кількість прийнятих та переданих пакетів на цьому інтерфейсі.

```

define service {
    use                generic-service
    host_name          MikroTik-Router
    service_description CPU Load
    check_command      check_snmp!-C public -o .1.3.6.1.2.1.25.3.3.1.2.1 -w 40 -c
60
}

```

```

define service {
    use                generic-service
    host_name          MikroTik-Router
    service_description Uptime
    check_command      check_snmp!-C public -o .1.3.6.1.2.1.1.3.0
}

```

```

define service {
    use                generic-service
    host_name          MikroTik-Router
    service_description Total RAM
    check_command      check_snmp!-C public -o .1.3.6.1.2.1.25.2.2.0
}

```

Як приклад, подано конфігурації для отримання кількості RAM-пам'яті, часу роботи та навантаження процесора. Кожна характеристика системи має свій унікальний OID, який вказується у команді *check_snmp*.

Важливим компонентом роботи систем моніторингу є надсилання сповіщень про проблеми в мережі. Сповіщення мають бути такими, щоб відразу захоплювали увагу адміністраторів та підштовхували до вирішення проблеми. Існує багато методів налаштування Nagios Core для надсилання сповіщень. Зазвичай вони передбачають встановлення додаткового програмного забезпечення та налаштування файлів конфігурації. До методів надсилання сповіщень належать [17]:

- електронна пошта;
- пейджер;
- телефонне SMS;
- WinPopUp повідомлення;
- звукові сповіщення;
- спеціальні методи сповіщення.

Сучасним та найпопулярнішим методом є надсилання сповіщень на електронну пошту. Проте ніщо не заважає адміністраторам налаштувати інші спеціальні методи оповіщення. Звукові сповіщення є чудовим вибором серед нетрадиційних методів. Їх можна налаштувати так, щоб вони відтворювалися на сервері моніторингу або на іншому хості. Не менш цікавим методом є сповіщення за допомогою повідомлення WinPopUp. Проте сам WinPopUp є застарілим і в сучасних ОС Windows не використовується. Служба повідомлень перестала існувати у Windows Vista та Windows Server 2008 і була замінена старим виконуваним файлом Msg [18].

З огляду на те, що в межах даної кваліфікаційної роботи був побудований невеликий стенд у GNS3, у якому досліджується система моніторингу Nagios Core, оптимальним і робочим варіантом є звукові сповіщення разом з текстовими повідомленнями у спливаючому вікні, що надходять до робочої станції Win-

Workstation. У поєднанні ці методи гарантують, що проблема, яка виникла у мережі, точно не залишиться поза увагою адміністратора.

Реалізувати задум можна за допомогою агента NRPE [22]. NRPE розроблений таким чином, що дозволяє здійснювати віддалений моніторинг системи, використовуючи скрипти, розміщені на цих системах. На робочу станцію Win-Workstation було встановлено агент NSClient++. У NSClient++ вже є вбудований модуль NRPEServer, який дозволяє приймати команди на робочій станції з ОС Windows від Nagios так само, як NRPE на Linux. Лише потрібно переконатися в тому, що у файлі nsclient.ini значення ключа NRPEServer – enabled. Окрім цього, у даному файлі в блоці [/settings/NRPE/server] мають бути прописані наступні налаштування:

```
[/settings/NRPE/server]
allow arguments = true
allow nasty characters = true
use ssl = false
port = 5666
```

Дозвіл на використання аргументів та символів додається також у блок [/settings/external scripts]. Також у блок [/settings/external scripts/scripts] потрібно вписати два скрипти, які запускатимуть текстові сповіщення у спливаючому вікні та звукові сповіщення. Перший з них це senmdsg. Він виводитиме на екран те, що надійде з Nagios-Server, за допомогою Msg.exe:

```
sendmsg = cmd /c msg.exe * "$ARG1$"
```

На Nagios-Server має бути встановлений NRPE для того, щоб можна було використовувати плагін check_nrpe. Використовуючи check_nrpe, створюються дві команди у конфігураційному файлі commands.cfg, які повідомлятимуть про збої у роботі хостів та сервісів. Вони запускатимуть скрипт на робочій станції Win-Workstation, який повідомлятиме у спливаючому вікні про те, який хост та сервіси мають проблеми. Лістинг команд notify-host-by-winpopup та notify-service-by winpopup:

```
define command {
    command_name      notify-host-by-winpopup
```

```

        command_line          /usr/local/nagios/libexec/check_nrpe -H 192.8.1.3 -c
sendmsg -n -a "$HOSTALIAS$ ($HOSTSTATE$)"
    }

define command {
    command_name      notify-service-by-winpopup
    command_line      /usr/local/nagios/libexec/check_nrpe -H 192.8.1.3 -c
sendmsg -n -a "$HOSTALIAS$: $SERVICEDESC$ - $SERVICESTATES$"
}

```

Перша команда відповідає за те, щоб повідомляти, в якому стані перебуває конкретний хост: «UP» чи «DOWN». Другою командою повідомляється про те, в якому стані перебуває певний сервіс на хості.

На наступному кроці треба налаштувати надсилання звукових сповіщень. Відповідно до задуму повідомлення про проблемний стан, у якому перебуває хост чи сервіс, має супроводжуватися певним звуком. Якщо цим станом є «CRITICAL», то відтворюється аудіо-файл critical.wav, якщо «WARNING» – warning.wav. Якщо певний хост у стані «DOWN», то відтворюється down.wav. Ці файли у минулих версіях встановлювалися разом із системою моніторингу Nagios Core. У даному випадку їх було завантажено на робочу станцію Win-Workstation. Другий скрипт для сповіщень у файлі nsclient.ini – це audio_alert:

```

audio_alert = cmd /c powershell.exe -ExecutionPolicy Bypass -File
"C:\audio\alert_type.ps1" "$ARG1$"

```

Даний скрипт запускає інший, PowerShell-скрипт, який обирає та відтворює відповідну мелодію. Лістинг скрипту alert_type.ps1:

```

param([string]$level)

switch ($level.ToUpper()) {
    "CRITICAL" { $sound = "C:\audio\critical.wav" }
    "WARNING" { $sound = "C:\audio\warning.wav" }
    "DOWN" { $sound = "C:\audio\down.wav" }
    default { return }
}

if (!(Test-Path $sound)) { return }

Add-Type -AssemblyName System.Windows.Forms
$player = New-Object System.Media.SoundPlayer $sound
$player.PlaySync()

```

Цей скрипт отримує один параметр, у якому передається стан хосту або сервісу [19]. За допомогою оператора switch визначається, який звук має відтворюватися. Звуки призначені для трьох станів: «CRITICAL», «WARNING», «DOWN». При іншому стані, наприклад «OK» або «UP», звуки відтворюватися не будуть. На Win-Workstation прийде лише текстове сповіщення без звукового супроводу. На Nagios-Server створюються дві команди аналогічні тим, які були створені для налаштування попередніх сповіщень. Ці команди викликають скрипт audio_alert та передають йому інформацію про те, в якому стані перебуває хост або сервіс. Лістинг команд notify-host-by-sound та notify-service-by-sound:

```
define command {
    command_name      notify-host-by-sound
    command_line       /usr/local/nagios/libexec/check_nrpe -H 192.8.1.3 -c
audio_alert -n -a "$HOSTSTATE$"
}

define command {
    command_name      notify-service-by-sound
    command_line       /usr/local/nagios/libexec/check_nrpe -H 192.8.1.3 -c
audio_alert -n -a "$SERVICESTATE$"
}
```

Для функціонування сповіщень потрібно налаштувати контакт, який їх отримуватиме. У файлі конфігурацій /usr/local/nagios/etc/objects/contacts.cfg створено контакт nagios та додано його до групи admins.

```
define contact {
    contact_name      nagios
    use               generic-contact
    alias             Nagios User
}

define contactgroup {
    contactgroup_name admins
    alias             Nagios Administrators
    members           nagios
}
```

Цей контакт використовує шаблон generic-contact, у якому є ширші налаштування: періоди, коли відбуваються оповіщення про стан хосту або сервісу, команди для сповіщень тощо.

```

define contact {
    name                    generic-contact
    service_notification_period 24x7
    host_notification_period 24x7
    service_notification_options w, u, c, r, f, s
    host_notification_options d, u, r, f, s
    service_notification_commands notify-service-by-sound, notify-service-by-
winpopup
    host_notification_commands notify-host-by-sound, notify-host-by-
winpopup
    register                0
}

```

Окрім цього, тут також присутні ширші налаштування для кожної групи хостів, зокрема контакти, яким надходитиме сповіщення. У даному випадку це група `admins`. Таким кроком завершується налаштування двох методів сповіщення: текстове повідомлення у спливаючому вікні, що супроводжується відповідним звуком.

3.4 Тестування роботи системи моніторингу Nagios

Моніторинг пристроїв мережі налаштовано. Робоча станція Win-Workstation відповідає за перегляд результатів моніторингу, тому що на ній можна зручно підключитися до веб-інтерфейсу системи моніторингу Nagios та дивитися, в якому стані перебувають пристрої.

Інтерфейс Nagios містить кілька вкладок, які дозволяють сформувати цілісну картину того, що відбувається у мережі. Наприклад, на вкладці Hosts (рис. 3.14) можна побачити, які пристрої призначені для моніторингу, чи вони працюють у цей момент, чи є зв'язок з цими пристроями. Отримати таку інформацію допомагає команда *ping*.

Host Status Details For All Host Groups

Limit Results:

Host 	Status 	Last Check 	Duration 	Status Information
Linux-Workstation 	UP	11-27-2025 16:37:31	0d 0h 8m 31s	OK: Agent_version was 3.21
MikroTik-Router 	UP	11-27-2025 16:41:33	0d 0h 10m 6s	PING OK - Packet loss = 0%, RTA = 16.43 ms
Nagios-Server 	UP	11-27-2025 16:38:58	6d 2h 32m 2s	PING OK - Packet loss = 0%, RTA = 0.06 ms
Win-Workstation 	UP	11-27-2025 16:40:16	0d 0h 6m 23s	PING OK - Packet loss = 0%, RTA = 25.22 ms

Рисунок 3.14 – Вкладка Hosts

Наступною важливою вкладкою є Services. На ній видно повністю всі сервіси, за якими ведеться спостереження. Сервіси чітко розподілені по хостах, яким вони належать. З рисунку 3.15 видно, що на даний момент у мережі не спостерігається жодних проблем чи аномалій. Усі сервіси перебувають у стані «OK».

Limit Results:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Linux-Workstation	CPU Usage	OK	11-27-2025 16:42:17	0d 0h 7m 31s	1/5	OK: Percent was 0.00 %
	Disk SDA. Read bytes	OK	11-27-2025 16:43:07	0d 5h 17m 15s	1/5	OK: Read_bytes was 0.01 MB/s
	Disk SDA. Read time	OK	11-27-2025 16:43:57	1d 1h 43m 37s	1/5	OK: Read_time was 0.87 ms/s
	Disk SDA. Write bytes	OK	11-27-2025 16:44:47	1d 1h 42m 47s	1/5	OK: Write_bytes was 0.18 MB/s
	Ethernet. Received bytes	OK	11-27-2025 16:40:37	1d 1h 40m 54s	1/5	OK: Bytes_rcv was 0.17 kB/s
	Ethernet. Sent bytes	OK	11-27-2025 16:41:26	1d 1h 41m 8s	1/5	OK: Bytes_sent was 0.15 kB/s
	Logical disk	OK	11-27-2025 16:42:32	0d 0h 7m 16s	1/5	OK: Free was 10.53 GB
	Logical disk used percent	OK	11-27-2025 16:44:03	0d 0h 10m 46s	1/5	OK: Used_percent was 47.50 %
	Memory Usage	OK	11-27-2025 16:42:36	0d 0h 7m 12s	1/5	OK: Memory usage was 55.20 % (Available: 0.45 GB, Total: 1.02 GB, Free: 0.06 GB, Used: 0.56 GB)
	Process Count	OK	11-27-2025 16:43:31	0d 0h 2m 18s	1/5	OK: Process count was 150
MikroTik-Router	System operation time	OK	11-27-2025 16:43:20	1d 1h 43m 10s	1/5	OK: Uptime was 11 minutes 12 seconds
	CPU Load	OK	11-27-2025 16:44:09	1d 23h 7m 45s	1/3	SNMP OK - 4
	Interface name	OK	11-27-2025 16:35:10	0d 0h 11m 38s	1/3	SNMP OK - "ether1"
	PING	OK	11-27-2025 16:40:49	1d 23h 11m 5s	1/3	PING OK - Packet loss = 0%, RTA = 23.40 ms
	SNMP: Ethernet1. Network Inbound Bytes	OK	11-27-2025 16:36:39	1d 2h 45m 59s	1/3	SNMP OK - 114451
	SNMP: Ethernet1. Network Inbound Packets	OK	11-27-2025 16:37:29	1d 23h 4m 25s	1/3	SNMP OK - 1838
	SNMP: Ethernet1. Network Outbound Bytes	OK	11-27-2025 16:38:19	1d 0h 2m 53s	1/3	SNMP OK - 222126
	SNMP: Ethernet1. Network Outbound Packets	OK	11-27-2025 16:39:08	1d 23h 12m 46s	1/3	SNMP OK - 2492
	Total RAM	OK	11-27-2025 16:42:42	1d 23h 9m 12s	1/3	SNMP OK - 1048576
	Uptime	OK	11-27-2025 16:43:32	1d 23h 8m 22s	1/3	SNMP OK - Timeticks: (76000) 0:12:40.00
Nagios-Server	Current Load	OK	11-27-2025 16:44:22	6d 2h 36m 46s	1/4	OK - load average: 0.12, 0.30, 0.26
	Current Users	OK	11-27-2025 16:40:12	6d 2h 35m 43s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	11-27-2025 16:41:02	5d 23h 3m 2s	1/4	HTTP OK: HTTP/11 200 OK - 10945 bytes in 0.003 second response time
	PING	OK	11-27-2025 16:41:47	5d 23h 4m 11s	1/4	PING OK - Packet loss = 0%, RTA = 0.21 ms
	Root Partition	OK	11-27-2025 16:41:06	6d 2h 35m 11s	1/4	DISK OK - free space: / 4288 MiB (39.42% inode=83%):
	SSH	OK	11-27-2025 16:42:04	6d 2h 36m 25s	1/4	SSH OK - OpenSSH_8.9p1 Ubuntu-3ubuntu0.13 (protocol 2.0)
	Swap Usage	OK	11-27-2025 16:42:43	6d 2h 36m 2s	1/4	SWAP OK - 100% free (1914 MB out of 1914 MB)
Win-Workstation	Total Processes	OK	11-27-2025 16:42:55	5d 23h 5m 50s	1/4	PROCS OK: 41 processes with STATE = RSZDT
	C:\ Drive Space	OK	11-27-2025 16:37:45	0d 0h 9m 3s	1/3	c: - total: 19.43 Gb - used: 11.05 Gb (57%) - free 8.38 Gb (43%)
	CPU Load	OK	11-27-2025 16:44:34	0d 0h 0m 14s	1/3	CPU Load 46% (5 min average)
	Explorer	OK	11-27-2025 16:35:24	0d 4h 51m 57s	1/3	Explorer.EXE: Running
	Memory Usage	OK	11-27-2025 16:36:14	1d 2h 41m 20s	1/3	Memory usage: total:3199.58 MB - used: 943.08 MB (29%) - free: 2256.50 MB (71%)
	NSClient++ Version	OK	11-27-2025 16:37:04	1d 2h 40m 30s	1/3	NSClient++ 0107 2025-11-09
Uptime	Uptime	OK	11-27-2025 16:37:54	1d 2h 39m 40s	1/3	System Uptime - 0 day(s) 0 hour(s) 5 minute(s)

Рисунок 3.15 – Вкладка Services

На вкладці Host Groups можна побачити, що усі хости зручно розділені по групах (рис. 3.16). Є групи для віртуальних машин з ОС Linux, маршрутизаторів та віртуальних машин з ОС Windows. При розширенні мережі нові пристрої можуть додаватися в одну з цих груп. Також можливо створити нову окрему групу, яка відповідала б доданому хосту.

Service Overview For All Host Groups

Linux Machines (linux)				Network Devices (network-devices)				Windows Machines (windows)			
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions
Linux-Workstation	UP	11 OK	  	MikroTik-Router	UP	9 OK	  	Win-Workstation	UP	6 OK	  
Nagios-Server	UP	8 OK	  								

Рисунок 3.16 – Вкладка Host Groups

Якщо значення певного сервісу перевищуватиме вказані у конфігураційному файлі для цього хоста значення, то відбудеться і зміна статусу цього сервісу. Наприклад, зараз кількість запущених процесів на робочій станції Linux-Workstation – 155 (рис. 3.17), перевищивши поріг 150. Тому стан сервісу став «WARNING».

Limit Results: 100 ▾

Host ♦♦	Service ♦♦	Status ♦♦	Last Check ♦♦	Duration ♦♦	Attempt ♦♦	Status Information
Linux-Workstation	CPU Usage	OK	12-15-2025 11:23:11	0d 0h 2m 52s	1/5	OK: Percent was 0.00 %
	Disk SDA. Read bytes	OK	12-15-2025 11:24:01	0d 0h 2m 2s	1/5	OK: Read_bytes was 0 MB/s
	Disk SDA. Read time	OK	12-15-2025 11:24:51	0d 0h 1m 12s	1/5	OK: Read_time was 0 ms/s
	Disk SDA. Write bytes	OK	12-15-2025 11:25:41	0d 0h 5m 22s	1/5	OK: Write_bytes was 0.06 MB/s
	Ethernet. Received bytes	OK	12-15-2025 11:21:31	0d 0h 4m 32s	1/5	OK: Bytes_rcv was 0 kB/s
	Ethernet. Sent bytes	OK	12-15-2025 11:22:20	0d 0h 3m 43s	1/5	OK: Bytes_sent was 0 kB/s
	Logical disk	OK	12-15-2025 11:23:15	0d 0h 2m 48s	1/5	OK: Free was 10.48 GB
	Logical disk used percent	OK	12-15-2025 11:24:52	0d 0h 1m 11s	1/5	OK: Used_percent was 47.70 %
	Memory Usage	OK	12-15-2025 11:22:15	0d 0h 3m 48s	1/5	OK: Memory usage was 59.80 % (Available: 0.41 GB, Total: 1.02 GB, Free: 0.11 GB, Used: 0.61 GB)
	Process Count	WARNING	12-15-2025 11:23:24	0d 0h 2m 39s	5/5	WARNING: Process count was 155
	System operation time	OK	12-15-2025 11:24:14	0d 0h 1m 49s	1/5	OK: Uptime was 5 minutes 15 seconds

Рисунок 3.17 – Стан сервісів на робочій станції Linux-Workstation

Оскільки стан сервісу став «WARNING», то відповідно до налаштованих сповіщень з’явилося спливаюче вікно з чіткою інформацією про те, що стан сервісу Process Count на хості Linux-Workstation – «WARNING» (рис. 3.18). Це повідомлення супроводжувалося звуком, який відповідає за такі попереджувальні сповіщення.

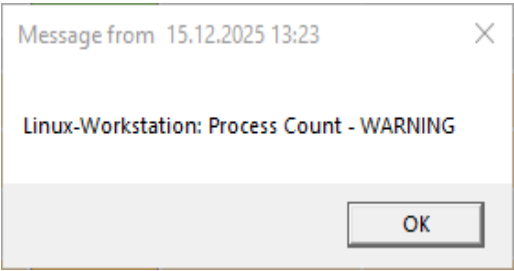


Рисунок 3.18 – Сповіщення про те, що стан сервісу Process Count – «WARNING»

На рисунку 3.19 продемонстровано, що відбувається при ситуації, коли значення переходить критичний поріг. Прийшло повідомлення про те, що на тому самому хості Linux-Workstation стан іншого сервісу, CPU Usage, став критичним.

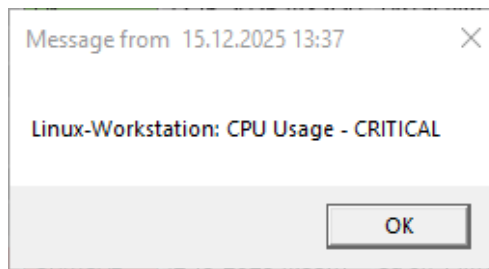


Рисунок 3.19 – Сповідження про те, що стан сервісу CPU Usage – «CRITICAL»

У даному випадку навантаження процесора перевищило поріг 60%, тому сервіс перебуває у стані «CRITICAL» (рис. 3.20).

Limit Results: 100 ▾						
Host ★★	Service ★★	Status ★★	Last Check ★★	Duration ★★	Attempt ★★	Status Information
Linux-Workstation	CPU Usage	CRITICAL	12-15-2025 11:37:15	0d 0h 1m 20s	5/5	CRITICAL: Percent was 76.50 %
	Disk SDA. Read bytes	OK	12-15-2025 11:34:01	0d 0h 14m 34s	1/5	OK: Read_bytes was 0.10 MB/s
	Disk SDA. Read time	OK	12-15-2025 11:34:51	0d 0h 13m 44s	1/5	OK: Read_time was 3.19 ms/s
	Disk SDA. Write bytes	OK	12-15-2025 11:35:41	0d 0h 17m 54s	1/5	OK: Write_bytes was 0.01 MB/s
	Ethernet. Received bytes	OK	12-15-2025 11:36:31	0d 0h 17m 4s	1/5	OK: Bytes_recv was 0.16 kB/s
	Ethernet. Sent bytes	OK	12-15-2025 11:37:20	0d 0h 16m 15s	1/5	OK: Bytes_sent was 0.18 kB/s
	Logical disk	OK	12-15-2025 11:38:15	0d 0h 15m 20s	1/5	OK: Free was 10.48 GB
	Logical disk used percent	OK	12-15-2025 11:34:52	0d 0h 13m 43s	1/5	OK: Used_percent was 47.70 %
	Memory Usage	OK	12-15-2025 11:37:15	0d 0h 16m 20s	1/5	OK: Memory usage was 57.30 % (Available: 0.43 GB, Total: 1.02 GB, Free: 0.07 GB, Used: 0.58 GB)
	Process Count	OK	12-15-2025 11:38:24	0d 0h 10m 11s	1/5	OK: Process count was 149
	System operation time	OK	12-15-2025 11:34:14	0d 0h 14m 21s	1/5	OK: Uptime was 15 minutes 15 seconds

Рисунок 3.20 – Критичний стан сервісу на хості Linux-Workstation

Також можна окремо переглянути стан сервісів на маршрутизаторі MikroTik-Router та Nagios-Server (рис. 3.21-3.22).

Service Status Details For Host 'Nagios-Server'

Limit Results: 100 ▾						
Host ★★	Service ★★	Status ★★	Last Check ★★	Duration ★★	Attempt ★★	Status Information
Nagios-Server	Current Load	OK	11-27-2025 17:14:22	6d 3h 8m 16s	1/4	OK - load average: 0.04, 0.10, 0.12
	Current Users	OK	11-27-2025 17:15:12	6d 3h 7m 13s	1/4	USERS OK - 2 users currently logged in
	HTTP	OK	11-27-2025 17:16:02	5d 23h 34m 32s	1/4	HTTP OK: HTTP/1.1 200 OK - 10945 bytes in 0.001 second response time
	PING	OK	11-27-2025 17:11:47	5d 23h 35m 41s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	Root Partition	OK	11-27-2025 17:16:06	6d 3h 6m 41s	1/4	DISK OK - free space: / 4281 MiB (39.36% inode=83%):
	SSH	OK	11-27-2025 17:12:04	6d 3h 7m 55s	1/4	SSH OK - OpenSSH_8.9p1 Ubuntu-3ubuntu0.13 (protocol 2.0)
	Swap Usage	OK	11-27-2025 17:12:43	6d 3h 7m 32s	1/4	SWAP OK - 100% free (1914 MB out of 1914 MB)
	Total Processes	OK	11-27-2025 17:12:55	5d 23h 37m 20s	1/4	PROCS OK: 42 processes with STATE = RSZDT

Рисунок 3.21 – Стан сервісів на Nagios-Server

Service Status Details For Host 'MikroTik-Router'

Limit Results: 100 ▾						
Host ★★	Service ★★	Status ★★	Last Check ★★	Duration ★★	Attempt ★★	Status Information
MikroTik-Router	CPU Load	OK	11-27-2025 17:14:09	1d 23h 40m 27s	1/3	SNMP OK - 3
	Interface name	OK	11-27-2025 17:15:10	0d 0h 44m 20s	1/3	SNMP OK - "ether1"
	PING	OK	11-27-2025 17:15:49	1d 23h 43m 47s	1/3	PING OK - Packet loss = 0%, RTA = 8.22 ms
	SNMP. Ethernet1. Network Inbound Bytes	OK	11-27-2025 17:16:39	1d 3h 18m 41s	1/3	SNMP OK - 1029680
	SNMP. Ethernet1. Network Inbound Packets	OK	11-27-2025 17:07:29	1d 23h 37m 7s	1/3	SNMP OK - 10827
	SNMP. Ethernet1. Network Outbound Bytes	OK	11-27-2025 17:08:19	1d 0h 35m 35s	1/3	SNMP OK - 1199194
	SNMP. Ethernet1. Network Outbound Packets	OK	11-27-2025 17:09:08	1d 23h 45m 28s	1/3	SNMP OK - 12227
	Total RAM	OK	11-27-2025 17:12:42	1d 23h 41m 54s	1/3	SNMP OK - 1048576
	Uptime	OK	11-27-2025 17:13:32	1d 23h 41m 4s	1/3	SNMP OK - Timeticks: (256000) 0:42:40.00

Рисунок 3.22 – Стан сервісів на MikroTik-Router

На даний момент ні на Nagios-Server, ні на MikroTik-Router проблемної поведінки не фіксується. Якщо якийсь із хостів буде вимкнений, то на робочу станцію Win-Workstation прийде сповіщення. Наприклад, на рис. 3.23 показано таке сповіщення, після того як було вимкнено маршрутизатор MikroTik.

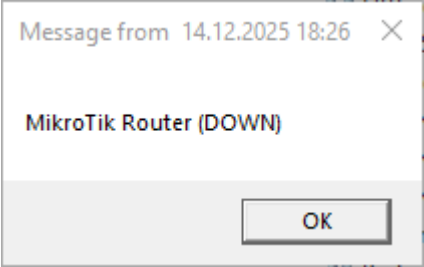


Рисунок 3.23 – Сповіщення про те, що стан хосту MikroTik-Router – «DOWN»

Не менш корисними вкладками веб-інтерфейсу Nagios Core є Trends та Availability. Вкладка Trends у Nagios Core призначена для аналізу історичних змін станів хостів і сервісів у часовому розрізі. На відміну від поточного моніторингу, який відображає лише актуальний стан об’єктів, розділ Trends дає змогу простежити, як змінювалася доступність і працездатність мережевих елементів протягом певного проміжку часу. Основою побудови графіків у розділі Trends є історичні дані, що зберігаються в журналах Nagios. Користувач може обрати конкретний хост або сервіс, а також задати часовий інтервал – від кількох годин до кількох місяців.

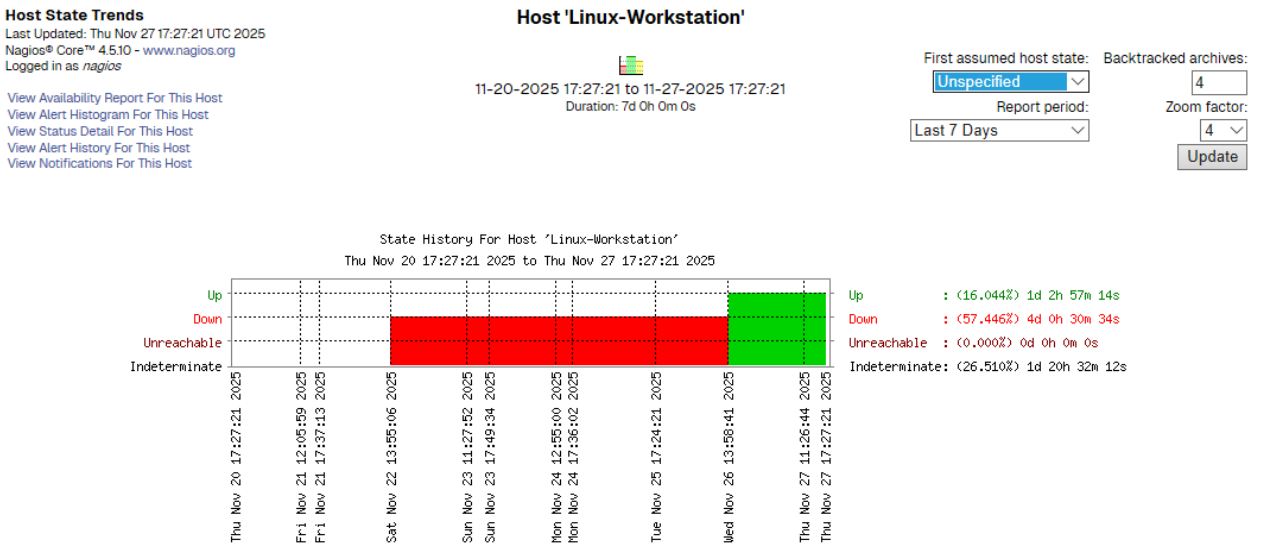


Рисунок 3.24 – Діаграма стану хосту Linux-Workstation за 7 днів

У результаті формується графічне представлення, яке показує, яку частку часу об'єкт перебував у станах «OK», «WARNING», «CRITICAL», «UNKNOWN» (для сервісів) чи «UP», «DOWN», «UNREACHABLE» (для хостів). На рис. 3.24 наведено приклад такого представлення, яке надає інформацію щодо стану хосту Linux-Workstation протягом семи днів.

Вкладка Availability призначена для формування узагальнених звітів про роботу хостів і сервісів за визначений період часу. На відміну від Trends, де основний акцент робиться на візуалізації змін станів, Availability зосереджується на кількісних показниках. У цьому розділі Nagios Core надає можливість формувати звіти про доступність хостів, груп хостів, сервісів або груп сервісів. Звіти подають інформацію у структурованому вигляді, з підрахунком тривалості кожного стану та відсотковими показниками. Користувач може задати часові межі звіту, обрати конкретний хост або сервіс і отримати таблицю з результатами. На рис. 3.25 показано звіт про доступність усіх груп хостів протягом семи днів.

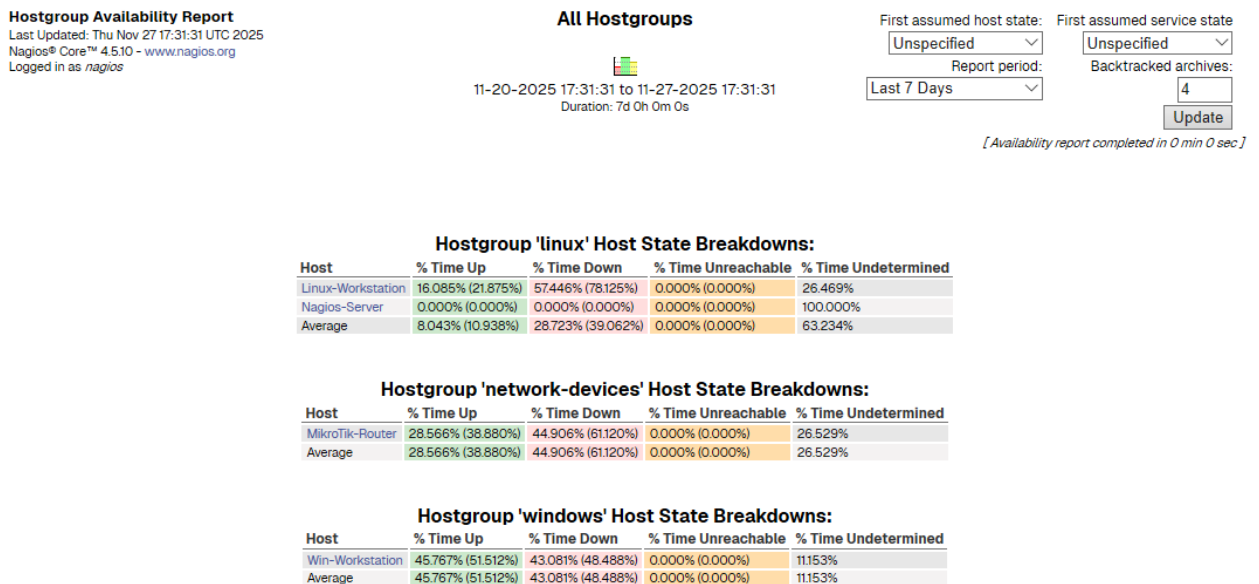


Рисунок 3.25 – Доступність усіх груп хостів за 7 днів

Розділи Trends та Availability доповнюють один одного, виконуючи різні, але взаємопов'язані функції. Trends забезпечує візуальний аналіз поведінки мережевих об'єктів, тоді як Availability надає структуровані числові показники, придатні для формування висновків.

Висновки з розділу 3

У третьому розділі кваліфікаційної роботи спочатку було налаштовано іменування пристроїв та IP-адресацію для зв'язку між ними.

Після цього на Nagios-Server було розгорнуто систему моніторингу Nagios. Було налаштовано моніторинг чотирьох хостів, які були розділені на три групи. До групи linux належать Nagios-Server та Linux-Workstation, до групи windows – Win-Workstation, а до групи network – MikroTik-Router. Моніторинг маршрутизатора MikroTik-Router здійснюється за допомогою протоколу SNMP. Для моніторингу робочих станцій Win-Workstation та Linux-Workstation було встановлено та налаштовано агенти NSClient++ та NCPA відповідно. Було налаштовано надсилання на Win-Workstation звукових сповіщень разом з текстовими у спливаючому вікні.

Щоб переконатися у правильності здійснених налаштувань, було протестовано систему моніторингу Nagios. Система повідомляла за допомогою сповіщень про те, що хост або певний сервіс на ньому мають проблеми.

ВИСНОВКИ

В результаті написання кваліфікаційної роботи магістра було налаштовано моніторинг мережі на базі системи моніторингу Nagios та обладнання Mikrotik.

У першому розділі відбулося ознайомлення з поняттям моніторингу мережі; було оглянуто сучасні програмні рішення для моніторингу мережі: Nagios, Zabbix, PRTG Network Monitor, SolarWinds Network Performance Monitor. Для реалізації проєкту було обрано систему Nagios, яка є безкоштовним, гнучким рішенням для моніторингу з відкритим вихідним кодом та великою спільнотою користувачів. Були досліджені можливості моніторингу маршрутизаторів MikroTik. Збирати інформацію з маршрутизаторів можна за допомогою протоколу SNMP.

У другому розділі було побудовано мережу, що складається з маршрутизатора MikroTik-Router, Switch, Nagios-Server, робочих станцій Win-Workstation та Linux-Workstation. Для побудованої мережі розроблено схему адресації. Обрано статичну IP-адресацію в мережі 192.8.1.0/28. Було обрано, за якими метриками відбуватиметься моніторинг.

У третьому розділі почалося налаштування пристроїв мережі. Систему моніторингу Nagios було розгорнуто на сервері Nagios-Server. Призначені для моніторингу хости були розділені на три групи: машини з ОС Windows, машини з ОС Linux та мережеве обладнання. Маршрутизатор MikroTik-Router відстежується за допомогою протоколу SNMP. Здійснювати моніторинг робочих станцій Win-Workstation та Linux-Workstation дозволяють агенти NSClient++ та NSCA. Було налаштовано два методи сповіщення, що працюють у поєднанні: текстові повідомлення у спливаючому вікні в супроводі звукових сповіщень. Після всіх налаштувань систему моніторингу було протестовано. Система повідомляла про те, що є проблеми в роботі на певному хості або що було перевищено попереджувальну чи критичну межу для певного сервісу. Надсилення сповіщень відбувалося правильно і згідно зі здійсненими налаштуваннями.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Barth W. Nagios: System and Network Monitoring. 2nd ed. San Francisco: No Starch Press, 2009. 720 p.
2. What is network monitoring? URL: <https://www.vmware.com/topics/network-monitoring>.
3. What is infrastructure monitoring? URL: <https://www.ibm.com/think/topics/infrastructure-monitoring>.
4. What is network monitoring? URL: https://www.cisco.com/c/en_uk/solutions/automation/what-is-network-monitoring.html.
5. Топ 10 програм для моніторингу мереж. URL: <https://www.softinventive.com.ua/best-network-monitoring-tools>.
6. Best Open Source and Free Network Monitoring Tools for 2025. URL: <https://uptrace.dev/tools/network-monitoring-tools>.
7. Top 11 Infrastructure Monitoring Tools & Software Solutions. URL: <https://uptrace.dev/tools/monitoring-tools-for-it>.
8. Nagios | Open Source Network Monitoring Solution. URL: <https://www.nagios.org/>.
9. Zabbix: The enterprise-class open source observability solution. URL: <https://www.zabbix.com/>.
10. PRTG Network Monitor – All-in-one network monitoring tool. URL: <https://www.paessler.com/prtg/prtg-network-monitor>.
11. Network Performance Monitor – Observability Self-Hosted. URL: <https://www.solarwinds.com/network-performance-monitor>.
12. Active and passive check in Nagios | all about. URL: <https://bobcares.com/blog/active-and-passive-check-in-nagios/>.
13. MikroTik – Company. URL: <https://mikrotik.com/aboutus/company>.
14. SNMP – RouterOS – MikroTik documentation. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/8978519/SNMP>.

15. Add-on Projects | Nagios Open Source. URL:
<https://www.nagios.org/projects/nagios-core-addons/>.

16. Main configuration file options – Nagios Core documentation. URL:
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/configmain.html>.

17. Notifications – Nagios Core documentation. URL:
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/notifications.html>.

18. Windows Messenger service – Wikipedia. URL:
https://en.wikipedia.org/wiki/Windows_Messenger_service.

19. Standard macros in Nagios – Nagios Core documentation. URL:
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/macrolist.html>.

20. Monitoring Routers and Switches – Nagios Core documentation. URL:
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/monitoring-routers.html>.

21. How to install NSClient Nagios monitoring agent on Windows system. URL:
<https://kifarunix.com/how-to-install-nsclient-nagios-monitoring-agent-on-windows-system/>.

22. Nagios Core Addons – Nagios Core documentation. URL:
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/addons.html#nrpe>.