

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
корпоративних мереж»

Виконав студент 2-го курсу групи КІм-23-1
спеціальності 123 «Комп'ютерна інженерія»



Максим СЕМЕНЧУК

Керівник Доцент кафедри КІ та КБ, к.т.н.



Олексій ШЕЛУХА

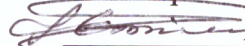
Рецензент Професор кафедри КІ та КБ, д.т.н., доцент



Володимир ВОРОТНИКОВ

Житомир – 2024

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
17 вересня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Семенчук Максим Миколайович

Тема роботи: Методи та технології моніторингу корпоративних мереж
затверджена Наказом університету від 17 вересня 2024р. № 478/с

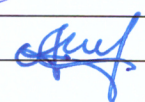
Термін здачі студентом закінченої роботи 16 грудня 2024 р.

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

1. Розроблені технічні вимоги до проєкту
2. Розроблена функціональна модель проєкту
3. Проєкт корпоративної мережі та процеси обміну даних в ньому
4. Графічний симулятор мережі GNS3
5. Система моніторингу Zabbix
6. База даних MySQL

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	І.Г. Фальковський	17.09.2024	17.09.2024
2	І.Г. Фальковський	17.09.2024	17.09.2024
3	І.Г. Фальковський	17.09.2024	17.09.2024

Студент  Максим СЕМЕНЧУК
Керівник  Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	17 вересня 2024	Виконано
2	Пошук інформації стосовно моніторингу мережі	18 вересня 2024 – 1 жовтня 2024	Виконано
3	Аналіз інструментів моніторингу	2 жовтня 2024 – 8 жовтня 2024	Виконано
4	Ознайомлення з Zabbix	9 жовтня 2024 – 22 жовтня 2024	Виконано
5	Вивчення принципів роботи Zabbix з пристроями	23 жовтня 2024– 3 листопада 2024	Виконано
6	Побудова мережі	4 листопада 2024 – 10 листопада 2024	Виконано
7	Налаштування агентів та snmp на робочих пристроях	11 листопада 2024 – 18 листопада 2024	Виконано
8	Налаштування моніторингу мережі	19 листопада 2024 – 27 листопада 2024	Виконано
9	Тестування моніторингу	28 листопада 2024– 5 грудня 2024	Виконано
10	Написання пояснювальної записки	6 грудня 2024 - 13 грудня	Виконано
11	Отримання відгуку та резенції	14 грудня 2024 - 15 грудня 2024	Виконано
12	Захист	27 грудня 2024	Виконано

Студент Сем Максим СЕМЕНЧУК

Керівник Шелуха Олексій ШЕЛУХА

АНОТАЦІЯ

Випускна кваліфікаційна робота магістра складається з проекту системи моніторингу корпоративної мережі, її реалізації та пояснювальної записки до нього. Пояснювальна записка містить 66 сторінок, 42 ілюстрацій та 1 таблицю. Список використаних джерел має 20 літературних джерел і займає 2 сторінки. Робота включає в себе 2 додатки, які розміщені на 11 сторінках

Метою роботи є аналіз методів та технологій моніторингу та реалізації проекту системи моніторингу корпоративної мережі. В рамках дослідження було побудовано мережу, налаштовано автоматизацію та додано реакцію на інциденти.

В першому розділі було проведено аналіз існуючих досліджень, методів та засобів моніторингу мережі. Було порівняно рішення моніторингу мережі та обрано Zabbix, як рішення для моніторингу.

В другому розділі було розібрано принципи роботи Zabbix та обрано рішення для симуляції мережі. Також було побудовано мережу та налаштовано зв'язок в ній.

В третьому розділі було проведено налаштування моніторингу в мережі за допомогою Zabbix, протестовано її працездатність. Також проаналізовано результати дослідження та представлені принципи для майбутніх досліджень

Ключові слова: ZABBIX, МОНІТОРИНГ, AGENT, МЕРЕЖА, SNMP, TRIGGER, MYSQL, ALERT

ANNOTATION

The qualification work consists of a corporate network monitoring system project, its implementation, and an explanatory note. The explanatory note comprises 64 pages, 36 illustrations, and 1 table. The list of references includes 20 sources and spans 2 pages.

The purpose of the work is analyze methods and technologies for monitoring and to implement a corporate network monitoring system project. As part of the study, a network was built, automation was configured, and incident response was added.

In the first chapter, an analysis of existing research, methods, and tools for network monitoring was conducted. Network monitoring solutions were compared, and Zabbix was chosen as the monitoring solution.

The second chapter examined the principles of Zabbix operation and selected a solution for network simulation. A network was built, and connectivity within it was configured.

In the third chapter, network monitoring was configured using Zabbix, and its functionality was tested. The research results were also analyzed, and principles for future studies were proposed.

Keywords: ZABBIX, МОНИТОРИНГ, AGENT, СЕТЕЖА, SNMP, TRIGGER, MYSQL, ALERT

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SNMP – Simple Network Management Protocol

IT - Інформаційні технології

WMI – Windows Management Instrumentation

MP – Management packs

SQL – Structured query language

LAN – Local Area Network

IP – Internet Protocol

DNS – Domain Name System

ЗМІСТ

ВСТУП	8
Розділ 1: Аналіз проблематики, методів та засобів моніторингу мережної інфраструктури	9
1.1 Аналіз існуючих досліджень	9
1.2 Аналіз завдань та методів моніторингу мережної інфраструктури	14
1.3 Аналіз протоколів та стандартів моніторингу мережевого трафіку	21
1.4 Порівняння рішень моніторингу	27
1.5 Постановка завдання дослідження	35
Висновки до розділу 1	36
Розділ 2: Проектування системи моніторингу корпоративної мережі	37
2.1 Вибір інструментів розробки системи моніторингу	37
2.2 Архітектура та принципи роботи Zabbix	43
2.3 Розробка схеми мережі	46
Висновки до розділу 2	48
Розділ 3: Встановлення та налаштування моніторингової мережі	49
3.1 Встановлення Zabbix	49
3.2 Тестування та перевірка роботи моніторингу	59
3.3 Аналіз результатів та пропозиції для подальших досліджень	61
Висновки до розділу 3	63
Висновки	64
Список використаних джерел	65
Додатки	67

ВСТУП

Актуальність теми: Сучасні корпорації стикаються з постійним зростанням масштабів і складності своєї мережної інфраструктури, яка охоплює сервери, мережеві пристрої, додатки та інші компоненти. Надійне функціонування цієї інфраструктури є критично важливим для безперебійної роботи бізнес-процесів. Однак складність і обсяги таких систем вимагають постійного моніторингу для вчасного виявлення потенційних проблем, запобігання аварійним ситуаціям і забезпечення швидкого реагування на інциденти. У цьому контексті розробка та впровадження ефективних систем моніторингу стають важливим завданням для сучасних організацій.

Мета дослідження: Метою роботи є дослідження методів та технологій моніторингу корпоративної мережі та реалізація проекту моніторингу мережі.

Об'єкт дослідження: процес функціонування корпоративної мережної інфраструктури.

Предмет дослідження: методи та засоби моніторингу корпоративної мережі.

Задачі дослідження: У рамках дослідження сформульовано наступні основні задачі дослідження:

1. Провести аналіз актуальних досліджень та аспектів побудови системи моніторингу мережної інфраструктури.
2. Розробити проєкт системи моніторингу корпоративної мережевої інфраструктури
3. Виконати розгортання та дослідження можливостей розробленої системи моніторингу корпоративних мереж.

Результати даної роботи будуть сприяти підвищенню ефективності моніторингу мережної інфраструктури, забезпеченню швидкого виявлення та усунення проблем, а також покращенню надійності та стабільності роботи бізнес-процесів підприємства.

Розділ 1: Аналіз проблематики, методів та засобів моніторингу мережної інфраструктури

1.1 Аналіз існуючих досліджень

Моніторинг мережі та збір даних є ключовими аспектами сучасних інформаційних систем. Дослідження в цій галузі зосереджуються на розробці інструментів, які забезпечують точність, швидкість і надійність збору даних, а також вирішують проблеми продуктивності та безпеки мережевої інфраструктури. Вивчення наявної літератури та практичних кейсів дозволяє виявити основні виклики, такі як забезпечення безперебійного функціонування систем, оптимізація витрат і дотримання стандартів захисту даних.

В даній статті^[3] розглядається забезпечення видимості в мережі. Забезпечення видимості в мережі є ключовим завданням, яке дозволяє ефективно управляти її роботою, ідентифікувати проблеми продуктивності та безпеки, а також забезпечувати надійну експлуатацію. Видимість означає повне розуміння того, що відбувається у мережі на всіх її рівнях — від фізичного рівня до прикладного.

Однією з головних проблем є складність отримання цілісного уявлення в умовах сучасних гібридних архітектур, які включають локальні мережі, хмарні сервіси і мобільні пристрої. Традиційні інструменти моніторингу часто зосереджені на певних сегментах мережі або рівнях, залишаючи поза увагою важливі взаємодії між компонентами. Це створює так звані "сліпі зони", які ускладнюють ідентифікацію проблем та аналіз причин їх виникнення.^[1]

Крім того, зростаючий обсяг мережевого трафіку ускладнює обробку даних у реальному часі. Це призводить до затримок в аналізі інформації, знижуючи ефективність реагування на потенційні інциденти. Щоб вирішити цю проблему, підприємства впроваджують аналітичні інструменти з елементами штучного інтелекту, які дозволяють виявляти аномалії та оптимізувати продуктивність.

У книзі^[2] автори досліджують традиційні методи моніторингу мереж і виявляють кілька ключових викликів, з якими стикаються адміністратори та інженери при застосуванні класичних підходів.

Традиційний моніторинг зазвичай базується на статичному зборі та обробці даних за допомогою простих інструментів, таких як SNMP (Simple Network Management Protocol) або ICMP (Internet Control Message Protocol). Хоча ці методи ефективні для базового моніторингу доступності та продуктивності пристроїв, вони мають суттєві обмеження.

Один з найбільших викликів полягає в обмеженій видимості мережі. Традиційні інструменти часто зосереджуються лише на певних аспектах мережі, таких як обсяг трафіку або стан пристроїв, не надаючи повної картини того, як працює мережа в цілому. Наприклад, вони не можуть чітко відображати складні взаємодії між різними компонентами мережі або виявляти аномалії на більш глибокому рівні, наприклад, в поведінці окремих користувачів чи служб.

Ще одним значним викликом є масштабованість. У великих, розподілених мережах традиційні інструменти можуть не справлятися з обробкою величезної кількості даних, що збираються з усіх точок мережі. Це призводить до проблем із управлінням даними, коли накопичення великої кількості метрик стає важким для зберігання та аналізу. У таких випадках мережеві адміністратори можуть упустити важливі сигнали або залишити дані неперевіреними.

Крім того, традиційні системи часто стикаються з проблемами відсутності інтеграції. Вони можуть працювати з певним набором даних, але не забезпечують достатньої інтеграції з іншими інструментами для детального аналізу або автоматизації процесів реагування на інциденти. В результаті адміністратори мереж часто змушені вручну поєднувати різні джерела даних для отримання комплексної картини.

Інші важливі проблеми включають реактивний підхід до моніторингу, коли інциденти виявляються лише після того, як вже сталася помилка або порушення. Це призводить до збільшення часу простою та втрат у продуктивності. У порівнянні з сучасними підходами, орієнтованими на

проактивне виявлення та усунення проблем у реальному часі, традиційні методи менш ефективні.

Як вирішення традиційних проблем моніторингу автор пропонує:

1. Інтеграція новітніх технологій: Автори пропонують інтегрувати сучасні методи моніторингу, такі як аналіз мережевих потоків (Network Flow Monitoring) і використання машинного навчання для виявлення аномалій. Це дозволяє системам моніторингу виявляти складні аномалії та загрози в реальному часі, на відміну від традиційних систем, які в основному фокусуються на базових показниках доступності та продуктивності.

2. Проактивний підхід: У книзі підкреслюється важливість проактивного моніторингу та виявлення проблем ще до того, як вони призведуть до серйозних збоїв. Це можна досягти за допомогою систем, які аналізують поведінку мережі на основі даних, зібраних у реальному часі, та використовують аналітику для прогнозування потенційних загроз.

3. Цілісність даних: Автори також підкреслюють важливість інтеграції різних джерел даних для створення цілісної картини мережі. Замість того, щоб працювати із окремими точками даних, система моніторингу повинна збирати інформацію з усіх аспектів інфраструктури, забезпечуючи комплексний підхід до виявлення проблем і поліпшення ефективності роботи.

4. Простота в використанні та автоматизація: Одним із ключових аспектів є полегшення процесу управління моніторингом через автоматизацію збору та обробки даних, що значно зменшує навантаження на адміністратора і допомагає швидше реагувати на виникаючі проблеми.

Ці підходи дозволяють підприємствам подолати обмеження традиційних методів моніторингу та зберегти високу ефективність і стабільність мереж у більш динамічних і складних середовищах, де традиційні інструменти не можуть забезпечити належний рівень прозорості і контролю.

Автори статті^[3] розглядають дані мережевого потоку (Network Flow Data), які є одним із найважливіших інструментів для ефективного управління мережами, безпеки та забезпечення обсервбельності. Ця інформація відображає

всі ключові характеристики потоків трафіку між пристроями в мережі: джерело і призначення IP-адрес, порти, обсяг переданих даних, протоколи, часові мітки початку і завершення з'єднання, а також інші параметри. Завдяки своїй багатофункціональності Network Flow Data надають змогу глибше розуміти поведінку мережі та знаходити критичні точки для поліпшення її ефективності.

Одним із ключових аспектів даних потоку є їх здатність швидко виявляти аномалії, які можуть свідчити про наявність загроз. Наприклад, підвищена активність із певної IP-адреси, незвичні обсяги трафіку або несанкціоновані спроби доступу легко помітити завдяки аналізу потоку даних. Ця інформація дозволяє виявляти атаки типу DDoS, сканування портів або внутрішню активність шкідливого програмного забезпечення.

Network Flow Data також є основою для платформ моніторингу продуктивності. Аналіз потоків дає змогу знаходити вузькі місця в інфраструктурі, покращувати балансування навантаження та оптимізувати використання пропускної здатності. Це дозволяє мережевим адміністраторам приймати обґрунтовані рішення щодо розширення або модернізації інфраструктури, враховуючи реальне використання мережі.

У контексті забезпечення безпеки, Network Flow Data забезпечують глибоку інтеграцію з такими системами, як SIEM (наприклад, Splunk, QRadar) або SOAR, допомагаючи у виявленні загроз та автоматизації реагування на інциденти. Ці дані також є критичними для відповідності регуляторним вимогам, наприклад, у галузях із високими стандартами захисту даних, таких як фінансовий сектор або охорона здоров'я.

Окрім того, дані потоку стають ключовим елементом для сучасних систем обсервбельності. Вони забезпечують більш глибокий огляд того, що відбувається в мережі, дозволяючи не лише моніторити її стан у реальному часі, а й проводити ретроспективний аналіз для виявлення прихованих проблем чи трендів. Це допомагає уникати простоїв, мінімізувати час відновлення та забезпечувати стабільну роботу сервісів.

Сучасні платформи для обробки Network Flow Data, такі як ElastiFlow, використовують штучний інтелект і машинне навчання для автоматизації аналізу великих обсягів даних. Це не лише скорочує час на діагностику проблем, але й забезпечує більш детальний і точний аналіз мережевих процесів, сприяючи підвищенню ефективності мереж і зменшенню операційних витрат.

Проблеми розібрані в статті^[4] розглядаються проблеми невеликих корпоративних мереж. Для невеликих корпоративних мереж основні проблеми моніторингу мережі та збору даних виникають через обмежені ресурси та зростаючу складність. Одна з поширених проблем — погана продуктивність мережі. У міру зростання бізнесу збільшується і трафік від пристроїв співробітників, IoT-пристроїв і хмарних додатків. Невеликі мережі часто не справляються з правильним управлінням всім трафіком, що призводить до утворення вузьких місць, що впливають на швидкість і надійність критичних бізнес-додатків..^[7]

Інша важлива проблема — безпека. З розширенням кількості пристроїв і підключень мережевий периметр стає менш чітким, що робить мережу вразливою до атак, таких як фішинг або DDoS. Крім того, шифрування, хоч і є необхідним для захисту чутливих даних, може ускладнити моніторинг мережі, що робить важчим виявлення та реагування на загрози в реальному часі. Малий бізнес також може мати труднощі з управлінням кількома інструментами безпеки і забезпеченням їх ефективної взаємодії.

Управління конфігурацією — ще одна проблема. Зі збільшенням кількості пристроїв стає складніше підтримувати оновлену конфігурацію мережі. Між пристроями можуть виникати конфлікти, а ручне оновлення конфігурацій збільшує ризик помилок. Без належної автоматизації або систем управління конфігураціями невеликі мережі можуть зіткнутися з непослідовними політиками мережі, що залишають їх вразливими до загроз.

Нарешті, вартість є постійною проблемою. Послуги з моніторингу мереж і рішення з безпеки часто перевищують бюджети малих компаній. Багатьом малим підприємствам доводиться робити важкий вибір щодо того, куди

розподіляти ресурси, що може призвести до недофінансування або недостатньої підтримки певних аспектів мережі. Зростаючі вимоги до пропускної здатності та високоякісних послуг, таких як VoIP і відеоконференції, лише збільшують фінансовий тягар.

Для вирішення цих проблем необхідно ретельно планувати, інвестувати в правильні інструменти та забезпечувати стратегії управління мережею, які зможуть масштабуватися разом із зростанням компанії. Важливо знайти баланс між потребою в потужному моніторингу і доступними ресурсами, щоб уникнути дорогих збоїв або порушень безпеки.

1.2 Аналіз завдань та методів моніторингу мережної інфраструктури

Моніторинг IT-інфраструктури є однією з ключових складових управління сучасними інформаційними системами в організаціях. В умовах постійно зростаючих обсягів даних і збільшення складності IT-середовища, ефективний моніторинг стає необхідним для забезпечення стабільної і безперебійної роботи мережі. Головною метою моніторингу є збір та аналіз даних про компоненти інфраструктури для виявлення можливих проблем до того, як вони призведуть до серйозних збоїв, а також для запобігання несанкціонованому доступу або зловмисним атакам на мережу.

Моніторинг допомагає організаціям оперативно реагувати на технічні несправності і збої в системах, що дозволяє значно зменшити час простою і покращити загальну ефективність роботи інфраструктури. Ключовим аспектом моніторингу є здатність швидко виявляти аномалії, такі як перевантаження ресурсів, відмови в роботі обладнання, помилки передачі даних чи збої в працездатності сервісів. Оскільки ці проблеми можуть серйозно вплинути на продуктивність і безпеку підприємства, моніторинг має на меті не тільки фіксацію таких подій, але й своєчасне їх усунення.

Важливою частиною процесу моніторингу є прогнозування можливих збоїв, що дозволяє вжити заходів до того, як ці проблеми вплинуть на кінцевих

користувачів або порушують бізнес-процеси. Завдяки такому проактивному підходу підприємства можуть значно підвищити надійність і стійкість своїх інформаційних систем. У разі виникнення інцидентів, моніторинг дає змогу швидко визначити їхні причини та вжити необхідних заходів для відновлення нормальної роботи.

ІТ-моніторинг став важливою складовою не тільки для великих організацій, але і для малого та середнього бізнесу, який також стикається з потребою підтримувати належний рівень інфраструктури. Зі зростанням популярності хмарних обчислень і збільшенням обсягу даних, моніторинг став більш комплексним і вимагає нових підходів і інструментів для інтеграції різних середовищ — як локальних, так і хмарних.

Одним із важливих аспектів моніторингу є інтеграція з іншими суміжними дисциплінами, такими як управління ІТ-операціями (ITOM), аналіз операційних інцидентів (OI), автоматизація реагування на інциденти (SOAR), а також управління інформацією та подіями безпеки (SIEM). Завдяки такій інтеграції, інструменти моніторингу можуть надавати більш глибоке розуміння стану системи та дозволяють адміністратору вчасно вжити необхідних заходів для забезпечення безпеки й ефективності.

Моніторинг є важливим інструментом для виявлення і запобігання інцидентів, а також для забезпечення стабільності та продуктивності бізнесу. Одним з головних завдань є збереження доступності критичних ресурсів і сервісів на всіх етапах роботи організації, що дозволяє забезпечити безперебійну роботу всіх бізнес-процесів.

Основні принципи моніторингу:

- **Повнота:** контроль усіх критичних компонентів ІТ-інфраструктури, таких як сервери, мережеві пристрої, додатки та бази даних.
- **Постійність:** забезпечення безперервного моніторингу 24/7 для своєчасного виявлення проблем.
- **Цільовість:** орієнтація на конкретні завдання, включаючи оптимізацію ресурсів, підвищення безпеки чи вдосконалення продуктивності.

- **Автоматизація:** використання спеціальних інструментів для автоматизованого збору та аналізу даних.

Завдання моніторингу мережної інфраструктури включають:

1. **Виявлення проблем:** швидке визначення несправностей, таких як збої в роботі обладнання, перевантаження мережі чи втрати даних.
2. **Оптимізація ресурсів:** аналіз використання мережевих ресурсів для прийняття рішень щодо їхньої оптимізації.
3. **Забезпечення безпеки:** моніторинг для виявлення аномальної активності, загроз чи атак на мережу.
4. **Вимірювання продуктивності:** збір даних про ключові метрики, такі як швидкість передачі даних або затримки, для подальшого вдосконалення.
5. **Генерація звітів і сповіщень:** створення звітів та автоматичних сповіщень про стан системи для оперативного реагування.

Таким чином, моніторинг мережної інфраструктури є необхідною умовою для забезпечення стабільності, продуктивності та безпеки роботи ІТ-систем, що підтримують бізнес-процеси.

Існують два основних підходи до моніторингу мережної інфраструктури: Agentless моніторинг і Agent based. Обидва методи мають свої переваги та недоліки.

1.2.1 Agentless monitoring

Agentless моніторинг — це метод, при якому немає необхідності встановлювати спеціальні програмні агентські програми на мережеві пристрої. Замість цього використовуються стандартні протоколи зв'язку, такі як SNMP (Simple Network Management Protocol), WMI (Windows Management Instrumentation), SSH (Secure Shell), REST API (Representational State Transfer API) для обміну даними з пристроями. Цей підхід дозволяє отримувати дані з різних типів пристроїв, включаючи маршрутизатори, комутатори, сервери, принтери та інші.

Agentless метод моніторингу дозволяє зручно контролювати загальний стан мережі та продуктивність її компонентів без необхідності встановлення додаткового програмного забезпечення. Це знижує витрати на адміністрування та обслуговування системи. Протоколи, що використовуються для збору даних, як SNMP або WMI, забезпечують широкі можливості для інтеграції з різними типами пристроїв. Однак цей метод має певні обмеження у функціональності та залежить від налаштованих протоколів зв'язку. Для тих пристроїв, які не підтримують SNMP або WMI, такий метод стає недоступним.

Agentless моніторинг також дозволяє значно скоротити витрати на управління інфраструктурою, оскільки не потрібно встановлювати і оновлювати програмні агенти на кожному пристрої. Зазвичай цей метод використовується для моніторингу мережевих пристроїв, сховищ даних, гіпервізорів та віртуальних серверів.

Програмне забезпечення, що підтримує Agentless моніторинг, може автоматично збирати показники роботи мережевих пристроїв, таких як використання пропускну здатності, завантаження процесора або мережевий трафік. Коли пристрій або програма перевищує критичний поріг, система генерує сповіщення для адміністратора, що дозволяє швидко виявити проблеми. Звітність та сповіщення можуть бути налаштовані за різними критеріями, що дає змогу гнучко реагувати на будь-які зміни.

Завдяки можливості інтеграції з різними мережевими інструментами, Agentless моніторинг здатний забезпечити комплексний аналіз стану мережі і побудову актуальних карт мережевих залежностей. Такі системи також можуть моніторити продуктивність віртуальних ресурсів через хмарні API, що робить їх універсальними для сучасних гібридних інфраструктур. Agent-based monitoring

Agent-based моніторинг — це метод, при якому на пристрої встановлюється спеціальний програмний агент для збору та передачі даних про стан системи. Агенти здійснюють моніторинг продуктивності пристроїв і збирають дані відповідно до попередньо визначених параметрів. Перевагою такого методу є значно більша гнучкість і налаштовуваність у порівнянні з

Agentless моніторингом. Агенти можуть бути налаштовані для збору конкретних даних, таких як стан пам'яті, температура процесора або наявність помилок у додатках.

Завдяки використанню Agent-based моніторингу, можна контролювати навіть ті системи, які знаходяться за межами мережі або за брандмауером, що робить цей метод корисним у середовищах з високими вимогами безпеки. Крім того, агенти можуть працювати автономно, буферизуючи дані на пристрої в разі втрати з'єднання і передаючи їх на центральну платформу моніторингу після відновлення зв'язку.

Однак Agent-based моніторинг має і певні недоліки. Наприклад, установка агентів на кожен пристрій може бути ресурсозатратною, особливо якщо мережа складається з великої кількості різноманітних пристроїв. Крім того, кожен агент потребує постійного оновлення та управління, що може стати додатковою складністю в великих мережах.

Таким чином, вибір між Agentless моніторингом і Agent-based моніторингом залежить від специфіки організації та її вимог до системи. В обох випадках важливо обрати метод, який найкраще відповідає завданням моніторингу, зокрема для різних типів пристроїв, рівня безпеки та масштабу мережі.(рис 1.1)

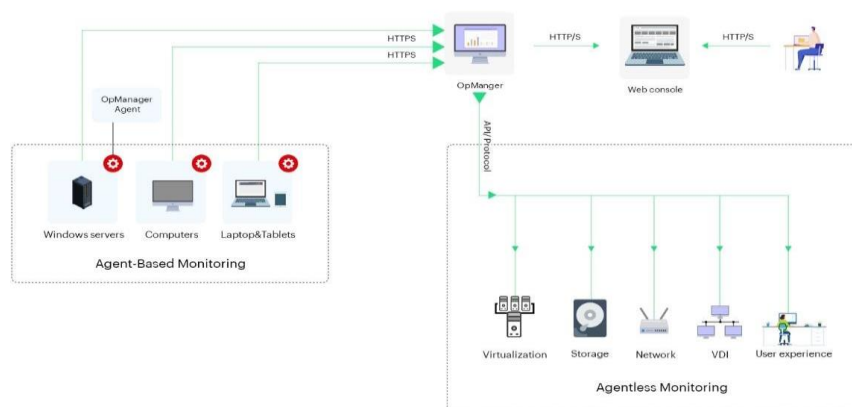


Рисунок 1.1 – Agent-Based і Agentless моніторинг

Ще одним важливим аспектом моніторингу є вибір між активним і пасивним моніторингом.

1. Активний моніторинг — це метод, при якому моніторингова система регулярно ініціює запити до мережевих пристроїв або систем для збору інформації. Наприклад, система може запитувати стан сервісів, перевіряти доступність мережевих пристроїв або вимірювати продуктивність за допомогою пінгу або інших тестів. Активний моніторинг дає змогу швидко отримувати інформацію про стан системи в реальному часі, але може створювати додаткове навантаження на мережу та пристрої через часті запити.

На відміну від пасивного, активний моніторинг додає трафік у мережу, дозволяючи збирати дані між двома кінцевими точками. Він вимірює такі параметри, як:

- доступність;
- маршрути;
- затримка та переупорядкування пакетів;
- втрати пакетів;
- пропускна здатність (ємність і доступна смуга).

Прикладами інструментів активного моніторингу є ping і traceroute. Ping відправляє ICMP-запити (ехо-пакети), які повертаються від кінцевої точки, вимірюючи затримку і втрати(рис 1.2). Traceroute, своєю чергою, визначає маршрути між точками мережі. Ще одним інструментом є iperf, який оцінює пропускну здатність TCP і UDP.

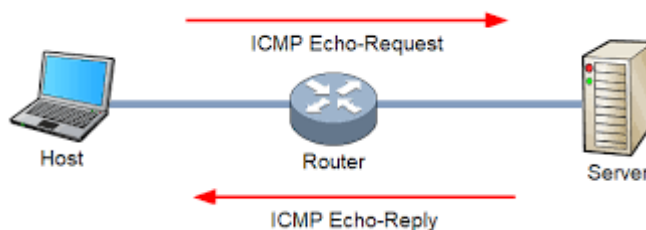


Рисунок 1.2 – Приклад команди ping

Недолік активного підходу полягає у створенні додаткового навантаження на мережу. Зонди активного моніторингу можуть оброблятися інакше, ніж звичайний трафік, що впливає на достовірність отриманих результатів. Через ці обмеження активний моніторинг рідко використовується окремо.

2. Пасивний моніторинг — це метод, при якому система моніторингу чекає на події чи зміни, що надходять від мережевих пристроїв або серверів. У цьому випадку пристрої відправляють свої дані, такі як логи або статуси, на систему моніторингу без ініціативи з її боку. Пасивний моніторинг менш ресурсоемний для мережі та пристроїв, оскільки не вимагає постійних запитів, але може мати меншу оперативність у виявленні проблем.

Цей підхід зчитує дані безпосередньо з лінії, не втручаючись у мережевий трафік. Він дозволяє отримувати інформацію про одну точку в мережі, наприклад:

- суміш протоколів і типів трафіку;
- точну швидкість передачі бітів і пакетів;
- час передачі та прибуття пакетів.

Прикладом пасивного моніторингу є системи сніфінгу пакетів, які спостерігають за трафіком у реальному часі, не впливаючи на нього. Недоліком є те, що аналіз відбувається лише в режимі офлайн, що вимагає обробки великих обсягів даних.

Хоча пасивний моніторинг мінімізує навантаження на мережу, він не дозволяє проводити вимірювання між кінцевими точками. Активний підхід дає більше даних, але може викликати перешкоди. Тому найефективнішим є комбінований метод, який об'єднує переваги обох типів моніторингу.

Процес моніторингу складається з двох основних етапів:

- Дублювання трафіку: створюється копія трафіку для аналізу. Це може здійснюватися вбудованими функціями маршрутизаторів і комутаторів у дзеркальному режимі або через окремі пристрої.
- Аналіз трафіку: обробка зібраних даних для виявлення проблем, зловмисної активності та оцінки продуктивності.

Таким чином, обидва методи мають свої сильні сторони, але їхнє поєднання забезпечує максимально точний і ефективний моніторинг мережі.

1.3 Аналіз протоколів та стандартів моніторингу мережевого трафіку

Також важливим є види протоколів збору даних.

SNMP (Simple Network Management Protocol) — це мережевий протокол, який використовується для моніторингу та керування пристроями, підключеними до мережі на основі Інтернет-протоколу. Цей протокол вбудований у багато локальних пристроїв, таких як маршрутизатори, комутатори, сервери, брандмауери та бездротові точки доступу, доступ до яких здійснюється через їхні IP-адреси. SNMP надає універсальний механізм для передачі керуючої інформації між мережевими пристроями в середовищах LAN або WAN, незалежно від виробника обладнання. Це протокол прикладного рівня, що працює в межах моделі OSI. Без використання SNMP збір даних про стан мережевих пристроїв стає неможливим.

SNMP є стандартним протоколом, призначеним для моніторингу та управління мережевими пристроями, такими як комутатори, маршрутизатори, сервери, файрволи тощо. Він забезпечує можливість отримання інформації про стан пристроїв, включаючи продуктивність, статус інтерфейсів, завантаження ресурсів, а також дозволяє надсилати команди для їхньої конфігурації та управління.

У режимі моніторингу без агентів (agentless) моніторингова система, наприклад, SCOM, здійснює взаємодію з пристроями за допомогою SNMP-запитів. Система надсилає запити через мережу, отримуючи у відповідь інформацію про такі параметри, як стан мережевих інтерфейсів, використання пам'яті, навантаження процесора чи мережевий трафік. Цей підхід дозволяє здійснювати ефективний контроль стану обладнання без необхідності встановлення додаткових програмних компонентів.

Переваги моніторингу без агентів із використанням SNMP:

- Спрощене впровадження: Відсутність потреби в установці агентів знижує витрати часу і спрощує процес моніторингу, особливо для великих мереж із численними пристроями.
- Зниження навантаження на пристрої: SNMP мінімально впливає на ресурси мережевих пристроїв, що є критично важливим для обладнання з обмеженими обчислювальними можливостями.
- Сумісність і універсальність: Оскільки SNMP підтримується більшістю сучасних мережевих пристроїв, його можна використовувати для моніторингу широкого спектру обладнання, незалежно від виробника чи операційної системи.

Agentless-моніторинг на базі SNMP дозволяє операторам мережі постійно відстежувати роботу пристроїв, аналізувати використання ресурсів, виявляти можливі проблеми та оперативно реагувати на будь-які збої. Це сприяє підвищенню ефективності управління мережею та знижує ризики простоїв. Окрім того, завдяки стандартизованому протоколу, цей підхід легко інтегрується у вже існуючі інфраструктури та може бути масштабований під потреби компанії.(рис 1.3)

SNMP Architecture

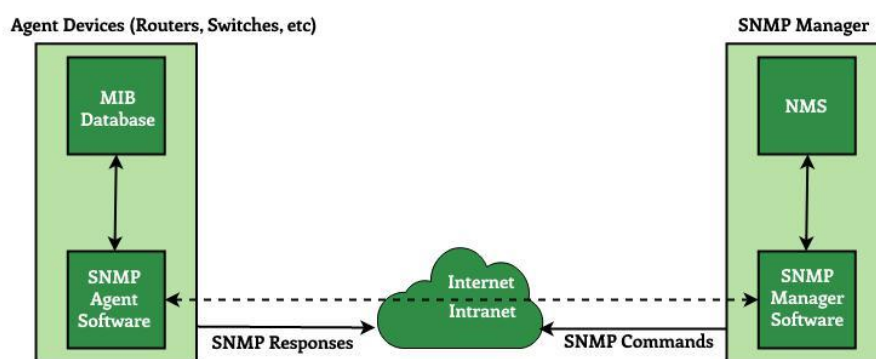


Рисунок 1.3 – Архітектура SNMP

NetFlow – це протокол для моніторингу мережі, розроблений компанією CISCO, який є частковим аналогом SNMP у контексті збору даних про мережу, але більш зосереджений, зборі статистичних даних про мережевий трафік на

пристроях, таких як маршрутизатори чи комутатори. NetFlow аналізує IP-пакети, що проходять через ці пристрої, і створює записи (відомі як "NetFlow-записи" або "потoki") з детальною інформацією про трафік. Кожен запис включає дані про джерело та призначення IP-адрес, порти, протоколи, обсяги переданих даних тощо. NetFlow дозволяє отримати більш детальну інформацію про мережевий трафік у порівнянні з SNMP.

sFlow — це ще один протокол моніторингу мережевого трафіку, який є відкритим стандартом. Відрізняється від NetFlow тим, що використовує вибіркового (sampled) підхід для збору даних про трафік, що дозволяє знижувати навантаження на мережу та пристрої. Вибірковий метод збірки полягає в тому, що пристрій регулярно вибирає лише частину пакетів для збору статистики.

Особливості sFlow:

Зниження навантаження: Завдяки вибіркового підходу sFlow знижує вимоги до пам'яті та процесора пристроїв, оскільки збирається лише частина даних.

Інтеграція: Підтримується багатьма виробниками мережевого обладнання, що забезпечує сумісність з різними системами.

Гнучкість: Може бути використаний для моніторингу не лише мережевого трафіку, але й стану пристроїв.

Обмеження sFlow:

Через вибіркового підхід sFlow не дає такої ж точної інформації про трафік, як NetFlow.

RMON (Remote Network Monitoring) — це стандарт для моніторингу мережі, який дозволяє збирати та аналізувати інформацію про мережевий трафік та стан мережевих пристроїв. Він є розширенням протоколу SNMP, що дає змогу отримувати більш детальну інформацію про мережу та її продуктивність. RMON дозволяє здійснювати моніторинг як локально, так і віддалено, що робить його ефективним для великих мереж з численними пристроями.

RMON працює через стандартний протокол SNMP і використовує ті ж самі агенти для збору та передачі статистики на центральний сервер моніторингу.

Протокол надає можливість детального збору даних про трафік, втрату пакетів, затримки, колізії, стан каналів зв'язку, а також моніторинг протоколів, таких як IP, TCP, UDP і інші. Завдяки своїй здатності здійснювати моніторинг на кількох рівнях мережі, від фізичного рівня до рівня додатків, RMON надає глибоку інформацію про мережеву інфраструктуру, що дозволяє виявляти проблеми та оптимізувати роботу мережі.

Перші версії протоколу, зокрема RMON1, забезпечують збір статистики на рівні мережевих інтерфейсів, таких як MAC-адреси, втрата пакетів, типи пакетів тощо. Пізніші версії, наприклад RMON2, розширюють функціональність, дозволяючи моніторити мережеві протоколи, такі як IP, DNS, HTTP і інші. Ці розширення дозволяють проводити глибший аналіз мережевих зв'язків і більш ефективно виявляти проблеми в мережі.

RMON підтримує можливість налаштування тригерів, що дозволяє автоматично сповіщати адміністратора або запускати певні дії, коли параметри мережі досягають критичних значень, таких як перевантаження каналів або втрата пакетів. Завдяки цьому можна своєчасно реагувати на проблеми, зменшуючи час простоїв або погіршення продуктивності мережі.

Основною перевагою RMON є його здатність здійснювати моніторинг віддалених мереж і пристроїв без необхідності безпосереднього підключення до кожного з них. Це дає змогу централізовано управляти великою кількістю пристроїв і зберігати дані для подальшого аналізу. Крім того, протокол дозволяє інтегруватися з іншими системами моніторингу та керування мережею, що робить його універсальним інструментом для управління складними мережами.

Таким чином, RMON є потужним інструментом для моніторингу мережі, який дозволяє отримувати детальну інформацію про її стан і продуктивність, а також ефективно управляти мережами, виявляючи та вирішуючи проблеми вчасно.

Аналіз лог-файлів є важливим компонентом системи моніторингу, який дозволяє відстежувати стан корпоративної мережі, діагностувати проблеми та виявляти потенційні загрози. Лог-файли містять записи про події, які

відбуваються в операційних системах, мережевих пристроях, програмах та інших компонентах інфраструктури. Ці записи надають адміністраторам цінну інформацію для розуміння роботи системи та реагування на інциденти.

Лог-файли зазвичай генеруються автоматично системами та містять дані про різні події: від помилок у роботі додатків до спроб несанкціонованого доступу. Наприклад, мережеві пристрої, такі як маршрутизатори та брандмауери, можуть записувати інформацію про підключення, відхилені запити або зміну конфігурації.

Для збору та аналізу лог-файлів у сучасних системах моніторингу застосовуються різні інструменти. Одним із популярних рішень є стек ELK (Elasticsearch, Logstash, Kibana), який дозволяє збирати, обробляти та візуалізувати дані(рис 1.4). Logstash використовується для агрегації логів із різних джерел, Elasticsearch — для їх зберігання і пошуку, а Kibana забезпечує зручний інтерфейс для аналізу. Альтернативні інструменти, такі як Splunk або Graylog, також широко використовуються в корпоративних мережах для роботи з великими обсягами даних.

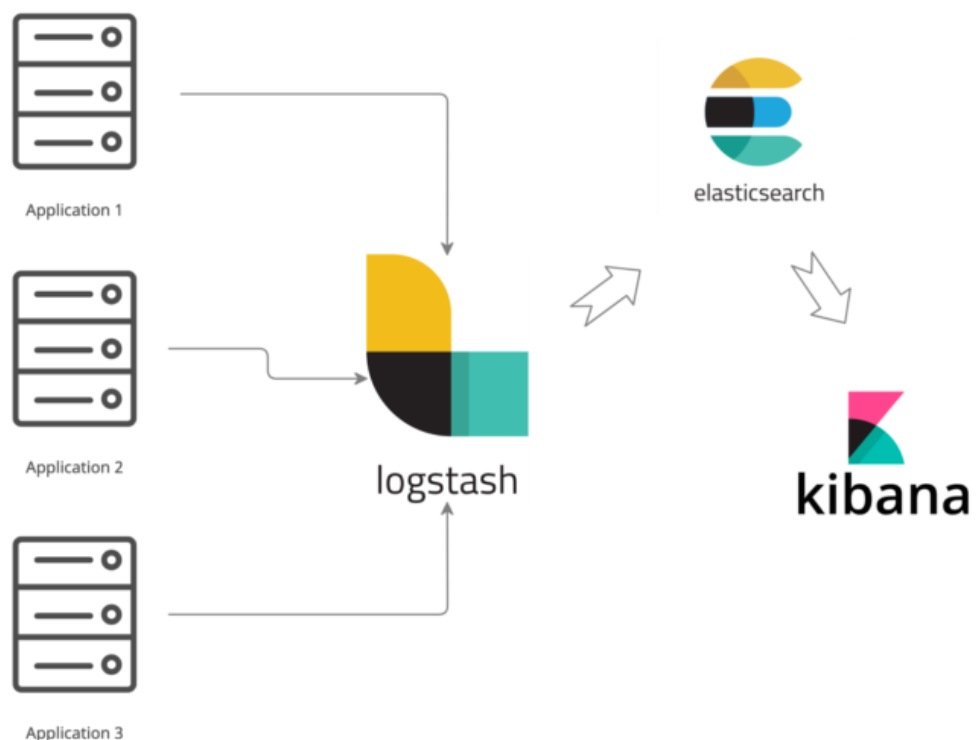


Рисунок 1.4 – Архітектура ELK Stack

Аналіз лог-файлів включає кілька основних етапів. Спершу відбувається збір логів із різних джерел. Це може бути реалізовано через централізовані системи, які отримують логи від усіх компонентів інфраструктури в реальному часі або через періодичний експорт файлів. Далі відбувається обробка зібраних даних, яка включає нормалізацію (приведення даних до єдиного формату) і видалення зайвих записів.

На етапі аналізу використовуються інструменти для виявлення ключових подій або аномалій. Це можуть бути системні помилки, спроби доступу до закритих ресурсів, незвичайна кількість запитів на певні сервери, що може свідчити про DDoS-атаку, або інші інциденти. Використання правил кореляції дозволяє поєднувати події з різних джерел і виявляти складні загрози, які неочевидні при аналізі окремих логів.

Одним із ключових завдань аналізу логів є автоматизація реагування на інциденти. Наприклад, при виявленні критичних подій система може автоматично повідомляти адміністратора через електронну пошту, SMS або месенджери. Інтеграція з інструментами, що дозволяють виконувати автоматичні дії (наприклад, блокування IP-адрес або перезавантаження сервісу), підвищує ефективність управління інцидентами.

Окрім оперативного використання, логи також можуть слугувати для довготривалого зберігання історії подій, що важливо для проведення ретроспективного аналізу або виконання аудиту безпеки. Завдяки аналізу накопичених даних можна виявляти тенденції, прогнозувати навантаження на мережу та покращувати загальну стабільність системи.

Таким чином, аналіз лог-файлів є невід'ємною частиною моніторингу корпоративних мереж, що забезпечує прозорість роботи системи та своєчасну реакцію на інциденти. Використання сучасних інструментів дозволяє ефективно обробляти великі обсяги даних, забезпечуючи високу точність і швидкість аналізу.

1.4 Порівняння рішень моніторингу

1.4.1 Microsoft SCOM

Microsoft SCOM (System Center Operations Manager) — це програмне забезпечення для моніторингу, управління та автоматизації інфраструктури ІТ-систем, яке активно спостерігає за станом мережі. У новітніх версіях Microsoft SCOM підтримує не тільки Windows-системи, а й має можливість працювати з UNIX та Linux.

Інтерфейс керування SCOM(рис 1.5) використовує кольорове кодування для візуалізації стану об'єктів: зелений вказує на нормальний стан, жовтий — на попередження, а червоний — на критичну проблему. Адміністратор може налаштувати ці рівні за потреби.

Основні можливості цього моніторингового інструменту:

- Моніторинг інфраструктури: SCOM дозволяє здійснювати моніторинг різних елементів інфраструктури, включаючи сервери, мережеві пристрої та бази даних.
- Автоматизація дій: SCOM може автоматично виконувати певні дії на основі умов та подій. Це дозволяє знизити необхідність постійного нагляду та автоматизувати процеси відновлення після виявлення проблем.
- Аналіз та звітність: SCOM дозволяє аналізувати зібрані дані про інфраструктуру та генерувати звіти щодо різних показників, таких як продуктивність, використання ресурсів, доступність систем тощо.

Основні переваги цього продукту:

Сумісність з іншими продуктами Microsoft, такими як Active Directory, Exchange Server та SharePoint.

Централізоване управління, що дозволяє здійснювати моніторинг усієї системи через єдиний інтерфейс.

Уніфікований контроль для приватних та публічних хмарних сервісів.

В загальному, Microsoft SCOM є потужним інструментом для моніторингу та управління ІТ-інфраструктурою, який особливо корисний для організацій з великою кількістю машин та мережевих пристроїв. Однак він має кілька недоліків.

Перший недолік — складність налаштування, що вимагає спеціальних знань для максимально ефективного використання. Неправильна конфігурація може призвести до збоїв, перевантаження системи та інших неполадок. Ще одним недоліком є те, що SCOM більше підходить для моніторингу загального стану системи, а не для детального огляду окремих показників та пристроїв. Також вартість SCOM є обмеженням для деяких організацій, оскільки він є платним продуктом.

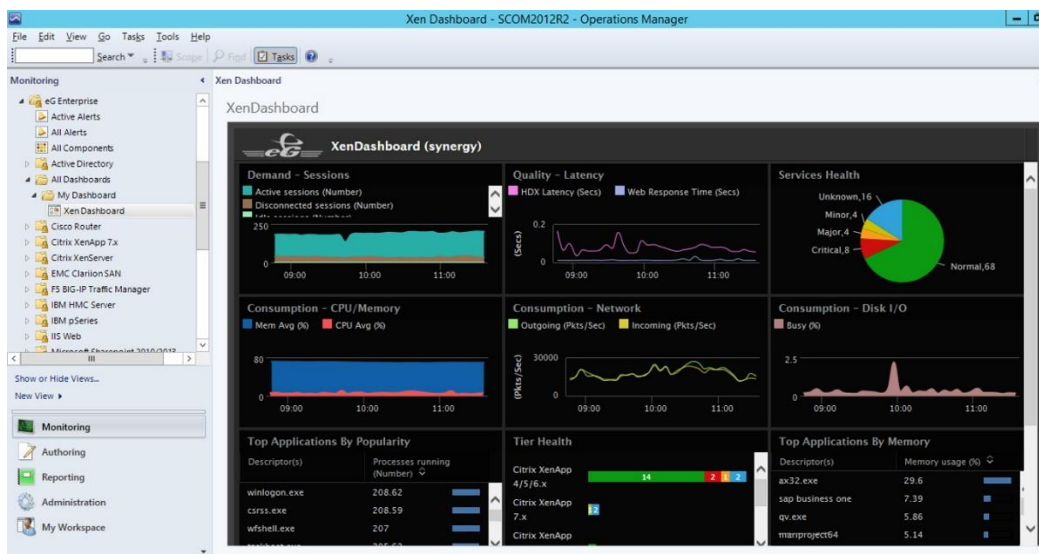


Рисунок 1.5 – Інтерфейс MS SCOM

1.4.2 Zabbix

Zabbix - це відкрите програмне забезпечення для моніторингу, тривоження та управління мережами і серверами. Він надає засоби для збору, аналізу та візуалізації даних про стан різних компонентів інфраструктури ІТ.

Zabbix є універсальною системою моніторингу, яка з успіхом:

- відстежує тенденції в роботі серверів і мережевої техніки;
- оперативно реагує на різні процеси;
- передупреждає про потенційні проблеми з навантаженням;
- збирає статистичні дані в певній робочій середі;
- діє в конкретних ситуаціях за заданим алгоритмом.

Zabbix має веб-інтерфейс, який може відображати всю зібрану інформацію з баз даних, віртуальних машин, мережних пристроїв у вигляді графіків, діаграм

та звітів, що дозволяє зручно аналізувати інформацію та виявляти аномалії.(рис 1.6)

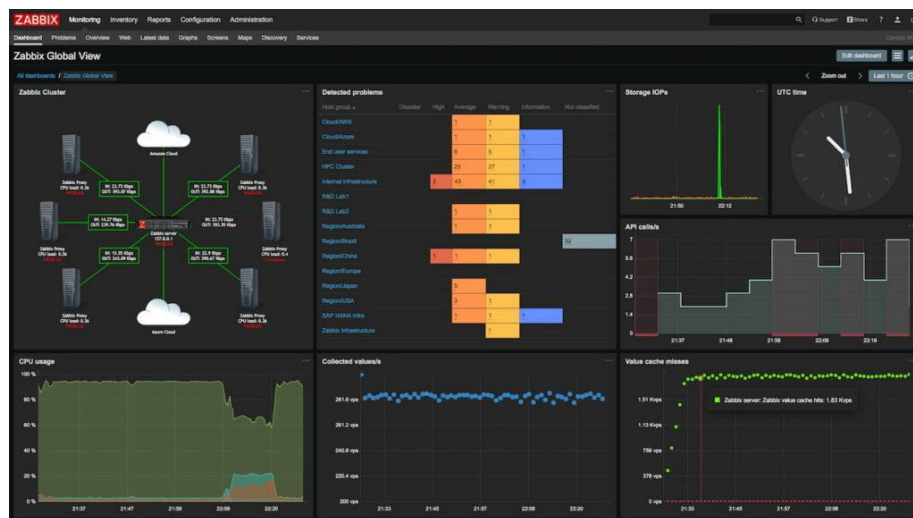


Рисунок 1.6 – Веб-інтерфейс Zabbix

Zabbix в процесі своєї роботи аналізує різну інформацію починаючи від навантаження на ЦП, закінчуючи моніторингом веб-серверів, NTP, та значенням пінгу.

При аваріях чи неполадках зазвичай спрацьовують налаштовані завчасно тригери, які відправляють інформацію адміністратору, або навіть самостійно піднімають сервіс, який вийшов з ладу.

Окрім цього Zabbix є програмою з відкритим кодом, що дозволяє вільно використовувати його при необхідності.

До недоліків Zabbix можна віднести доволі складне налаштування та громіздкість сервісу. Він потребує доволі високих вимог до ресурсів і підходить для пристроїв з високими характеристиками. Також Zabbix потребує встановлення агентів на всіх машинах у мережі.

1.4.3 Nagios

Nagios — це одна з найпопулярніших систем моніторингу з відкритим кодом, яка застосовується для нагляду за інфраструктурою ІТ-систем, такими як сервери, мережеві пристрої, програмне забезпечення та інші компоненти. Основна функція Nagios полягає в безперервному моніторингу різних параметрів системи та сповіщенні адміністратора про виникнення проблем або збоїв, що дозволяє вчасно реагувати на них (як показано на рисунку 1.7).

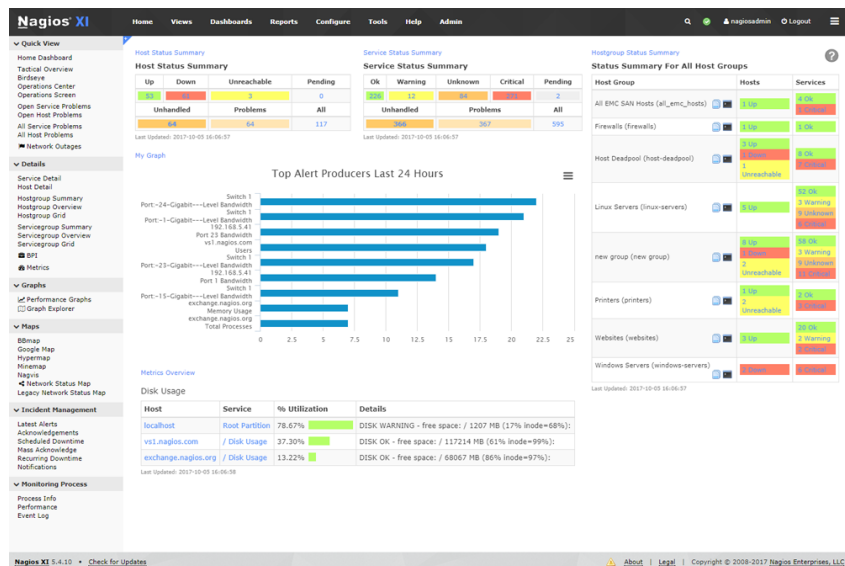


Рисунок 1.7 – Моніторинг мережі в Nagios

Nagios підтримує два способи керування: через командний рядок та веб-інтерфейс, що дає користувачам можливість вибору найбільш зручного варіанту. Однією з ключових особливостей є підтримка плагінів — доповнень, які дозволяють користувачам налаштовувати моніторинг різних об'єктів і параметрів. Плагіни дають можливість перевіряти стан пристроїв, наприклад, відстежувати час відгуку при пінгуванні або моніторити температуру та вологість через сенсори, що робить систему гнучкою та здатною працювати з різними типами пристроїв

Також Nagios підтримує використання шаблонів, що дозволяє швидко налаштувати подібні один до одного пристрої, і дає можливість швидкого налаштування мережі.

Також Nagios підтримує шаблони, що дозволяє швидко налаштувати пристрої, схожі між собою, і спрощує процес конфігурації мережі. Однак, попри свої переваги, Nagios має й недоліки. Одним із них є низька сумісність з операційними системами Windows. Оскільки система здебільшого орієнтована на Linux, підтримка Windows не є пріоритетом, що інколи призводить до проблем.

Іншим недоліком Nagios є те, що він може не бути достатньо ефективним для великих або складних інфраструктур. Якщо кількість моніторингових

об'єктів або частота перевірок надзвичайно велика, Nagios може зіткнутися з затримками або збоями. Крім того, система більше орієнтована на моніторинг мережі.

В цілому, Nagios є потужним інструментом для моніторингу систем, який пропонує гнучкість у налаштуванні та виявленні проблем. Проте, перед його впровадженням варто врахувати, що він може не підходити для великих мереж або працювати з Windows-сервісами з певними обмеженнями.

1.4.4 PRTG Network Monitor

PRTG Network Monitor — це потужний інструмент для моніторингу та управління мережами, розроблений компанією Paessler AG. Цей програмний продукт дозволяє організаціям здійснювати контроль за їхньою мережевою інфраструктурою, виявляти потенційні проблеми та забезпечувати безперервну роботу систем.

PRTG базується на агент-базованій архітектурі, де основний компонент, званий «ядро PRTG», розміщується на центральному сервері або комп'ютері, що виконує роль сервера моніторингу. Ядро відповідає за збір даних, їх обробку, зберігання і візуалізацію стану мережі.

Крім моніторингу різних пристроїв, Paessler PRTG також дозволяє контролювати ресурси, пов'язані з цими пристроями. Наприклад, можна стежити за використанням процесора, пам'яті, простору на диску та іншими показниками. Це дозволяє отримати повну картину продуктивності пристроїв і швидко виявити потенційні проблеми.

Інтерфейс користувача PRTG дуже інтерактивний, що дозволяє легко налаштовувати пристрої і датчики, переглядати реальні дані та налаштовувати сповіщення в одному місці. Веб-інтерфейс працює як односторінкова програма, що забезпечує високу швидкість, зручність і чуйність. (рис 1.8)

Додатково, Paessler PRTG пропонує альтернативний інтерфейс для підключення до локальної інсталяції, що є зручним у випадках, коли доступ до Інтернету обмежений.

PRTG також включає вбудовану функцію створення звітів, що дозволяє генерувати детальні звіти про мережеву активність. Ці звіти можна налаштовувати, включаючи лише необхідну інформацію, що робить їх незамінними для виявлення несправностей та планування потужностей.

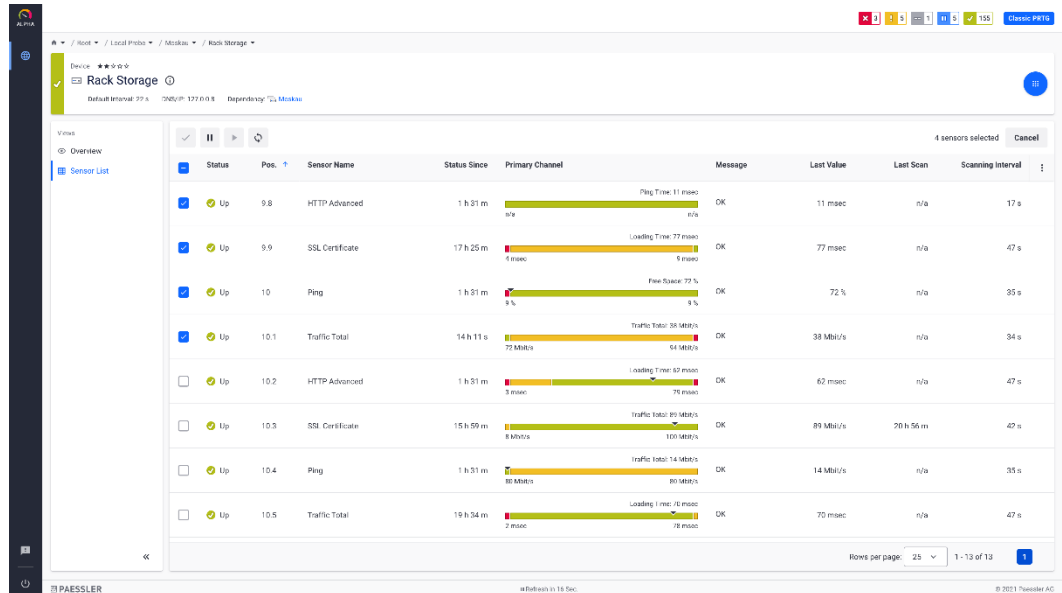


Рисунок 1.8 – Інтерфейс PRTG

Paessler PRTG Network Monitor має широкі можливості інтеграції з іншими програмами, що робить його дуже гнучким інструментом управління мережею. Серед найбільш популярних програм, які можна інтегрувати з Paessler PRTG Network Monitor, можна виділити Microsoft Azure, Amazon Web Services, Slack, ServiceNow, Zabbix, Nagios та багато інших.

Але окрім всіх плюсів, PRTG має і недоліки. Основним недоліком є його вартість. Він коштує доволі багато, і не всі компанії мають бюджет для його підтримки.

Окрім цього він вимагає постійного підключення до мережі і не працює в автономному режимі.

1.4.5 Cacti

Cacti — це безкоштовний та відкритий інструмент для моніторингу, який використовується для збору даних і візуалізації їх у вигляді графіків за допомогою інструмента RRD. Cacti дозволяє контролювати роботу різних пристроїв і систем, таких як маршрутизатори, комутатори, сервери, бази даних,

додатки та інше обладнання. Для збору інформації використовується SNMP (Simple Network Management Protocol).

Cacti надає веб-інтерфейс для управління користувачами, пристроями та графіками, що спрощує настройку моніторингу. Збір даних здійснюється за допомогою RRDTool, який зберігає інформацію в базі даних і використовує циклічні архіви (RRA) для забезпечення тривалого зберігання даних, при цьому не збільшуючи розмір файлів.

Переваги Cacti:

- Швидкість налаштування;
- Можливість налаштування графіків, як на рис 1.8, з не обмеженою кількістю елементів;

- Легка організація управління через користувачів та графіки.

Недоліки:

- Обмежений моніторинг для пристроїв, що не належать до мережі;
- Відсутність оновлень і підтримки, що обмежує додавання нових функцій.

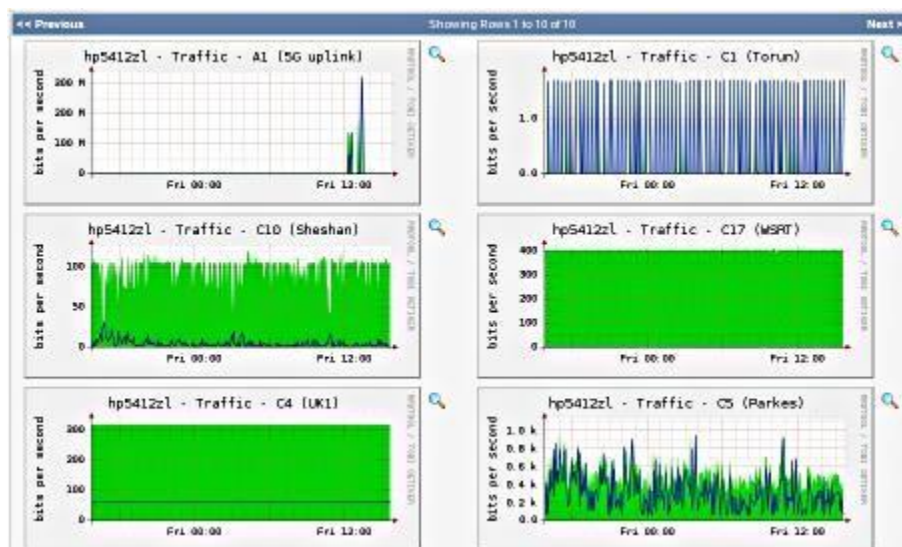


Рисунок 1.9 – Графіки Cacti

1.4.6 SolarWinds Network Performance Monitor

SolarWinds Network Performance Monitor (NPM) — це потужне програмне забезпечення для моніторингу і управління комп'ютерними мережами,

розроблене компанією SolarWinds. Його основна мета — забезпечити адміністраторів мережі інструментами для виявлення, аналізу та усунення проблем у мережі, забезпечуючи безперебійне функціонування мережевих ресурсів.

NPM дозволяє отримати цілісну картину про стан мережі, включаючи моніторинг серверів, комутаторів, маршрутизаторів, віртуальних і фізичних машин, а також інші ресурси. Програма використовує стандартні протоколи моніторингу, такі як SNMP, і збирає дані про продуктивність, використання ресурсів, пропускну здатність та інші важливі параметри.

Особливості SolarWinds NPM:

- Цілісний огляд мережевих ресурсів, включаючи фізичні та віртуальні пристрої;
- Моніторинг через SNMP та інші протоколи;
- Сповіщення про проблеми через налаштовані тригери(рис 1.10), що можуть автоматично відновлювати збої.

Недоліки:

Висока вартість, що може бути обмеженням для деяких компаній;

Не працює в автономному режимі і вимагає постійного підключення до мережі.



Alert name	Object that triggered this alert	Active time	Trigger time
High packet loss	R1	1h 14m	1/5/2017 3:51 PM
Alert me when an application goes into warning or critical state	MSSQLSERVER on vman-2008R2-SQL	1h 19m	1/5/2017 3:46 PM
High response time	dev-brn-mkun-01	1h 49m	1/5/2017 3:16 PM
High response time	R1	2h 11m	1/5/2017 2:54 PM
High response time	R9	2h 16m	1/5/2017 2:49 PM
Alert me when an application goes down	Microsoft IIS on adf-web-21.tul.solarwinds.net	14h 14m	1/5/2017 2:51 AM
High Transmit Percent Utilization	Ethernet1 -WAN (NetFlow) on Internet Gateway 3725	16h 58m	1/5/2017 12:07 AM
Alert me when a transaction step goes into warning or critical state	Sign in to Office 365	1d 8h 58m	1/4/2017 8:07 AM
Alert me when a transaction step goes into warning or critical state	Office 365 from Austin	1d 8h 58m	1/4/2017 8:07 AM
Alert me when an application goes down	Microsoft IIS on ADF-WEB-03	1d 12h 56m	1/4/2017 4:09 AM
Alert me when a transaction step goes down	Microsoft Dynamics CRM Online	1d 13h 44m	1/4/2017 3:21 AM
Alert me when a transaction step goes down	Log out from Office 365	1d 14h 24m	1/4/2017 2:41 AM
Host memory utilization	LAB-DEM-HYV on lab-dem-hyv.demo.lab	1d 15h 25m	1/4/2017 1:39 AM
Host CPU utilization	SYD-HYV-02 on 10.199.5.109	1d 15h 25m	1/4/2017 1:39 AM
Host CPU utilization	bas-esx-02.lab.tex	1d 15h 25m	1/4/2017 1:39 AM
Host CPU utilization	tok-esx-02.lab.tex	1d 15h 25m	1/4/2017 1:39 AM
Alert me when a transaction step goes down	Navigate to email section	1d 16h 14m	1/4/2017 12:51 AM
NTA: CBQoS Drops	QoS-Ethernet-Shaper\class-default\QoS-WAN-EthernetWeb	1d 16h 42m	1/4/2017 12:23 AM
Alert me when a component goes into warning or critical state	Top Indexes for Database (dnm) on LAB-DEM-SQL-02	1d 21h 23m	1/3/2017 7:42 PM
NTA: CBQoS Drops	QoS-Ethernet-Shaper\class-default (Drops)	1d 21h 42m	1/3/2017 7:23 PM
Page me when a Node goes down(2)	Lab/ Samsung	1d 22h 37m	1/3/2017 6:28 PM

Рисунок 1.10 – Генерація повідомлень у SolarWinds

1.4.4 Порівняльний аналіз моніторингових систем

Кожен із інструментів моніторингу має свої плюси та мінуси, підходить для різних типів мережі та використовується по своєму. Для пошуку оптимальної системи управління проведемо порівняння систем моніторингу за параметрами наведеними в табл. 1.1.

Таблиця 1.1

Функція	SCOM	Nagios	Zabbix	PRTG	Cacti	Solarwinds
Моніторинг мережних пристроїв	+	+	+	+	+	+
Оповіщення	+	+	+	+	+	+
Моніторинг продуктивності	+	+	+	+	-	+
Підтримка SNMP	+	+	+	+	+	+
Безкоштовне використання	-	+	+	-	+	-
Хмарний моніторинг	+	-	+	-	-	-
Моніторинг в реальному часі	+	-	+	-	+	+
APM	+	-	+	-	-	-
Аналіз топології мережі	+	-	-	+	+	-

Zabbix має всі потрібні нам функції, є безплатним рішенням і ідеально підходить для корпоративної мережі, тому в майбутньому буде використано Zabbix

1.5 Постановка завдання дослідження

Проаналізувавши інформацію, можна сказати, що система моніторингу повинна здійснювати постійний збір інформації про стан мережних компонентів, включаючи сервери, маршрутизатори, комутатори, принтери та інші пристрої. Це включає моніторинг параметрів, таких як навантаження процесора, використання пам'яті, доступність сервісів та інші метрики, які відображають стан компонентів.

Також система моніторингу повинна забезпечувати зручну візуалізацію стану мережних компонентів та подій. Це може включати графіки, діаграми, таблиці та інші елементи візуалізації для зручного сприйняття і аналізу даних.

Крім того, система повинна надавати можливість створення звітів зі зібраних даних, які допомагають у вирішенні проблем та прийнятті рішень.

Важливою складовою є проєктування масштабованої моделі системи, яка враховує особливості корпоративної мережі, та її подальша інтеграція з використанням сучасних протоколів, таких як SNMP чи NetFlow.

Важливою частиною системи моніторингу є автоматичне реагування на інциденти. Моніторингова система повинна швидко реагувати на інциденти в мережі та сповіщати адміністратора, про всі можливі загрози, які можуть бути в мережі.

Реалізація системи буде доповнена тестуванням, виявленням вузьких місць та оптимізацією для підвищення ефективності. Очікується, що впровадження цієї системи дозволить мінімізувати ризики інцидентів у мережі, підвищити її продуктивність і забезпечити надійний контроль над ключовими процесами в організації.

Висновки до розділу 1

В цьому розділі було проаналізовано завдання та методи моніторингу, розглянуто функції, які повинна виконувати моніторингова система, розглянуто та порівняно різні моніторингові системи, і вирішено, що Zabbix найбільш підходить для нашого типу мережі. Також було поставлено завдання для дослідження.

Розділ 2: Проектування системи моніторингу корпоративної мережі

2.1 Вибір інструментів розробки системи моніторингу

Корпоративна мережа — це сукупність апаратних і програмних засобів, що забезпечують з'єднання і взаємодію інформаційних систем, пристроїв та користувачів в межах однієї організації. Вона створюється для підтримки бізнес-процесів компанії, сприяння ефективній комунікації між співробітниками та забезпечення доступу до корпоративних ресурсів, таких як бази даних, файлові сховища чи програмні платформи.

Висока складність корпоративних мереж вимагає надійного моніторингу для забезпечення їх стабільної роботи, виявлення проблем та зменшення часу простою. Тут нам і потрібні системи моніторингу типу Zabbix

Zabbix є ідеальним рішенням для моніторингу корпоративної мережі завдяки своїй універсальності, масштабованості та широкому функціоналу. Ця система підтримує моніторинг різноманітних компонентів мережі, таких як сервери, маршрутизатори, комутатори, бази даних та кінцеві пристрої, що робить її придатною для організацій будь-якого масштабу

Важливою перевагою Zabbix є його безкоштовна open-source ліцензія, яка зменшує витрати на впровадження та обслуговування. Це зменшить витрати нашого проекту і дозволить вільно користуватися всіма перевагами моніторингової системи. Система також забезпечує створення тригерів, що допоможе нам автоматично реагувати на відхилення від нормальних показників, що дозволить швидко виявляти й усувати проблеми, зменшуючи негативний вплив на бізнес-процеси.

Zabbix підтримує популярні протоколи моніторингу, включаючи SNMP, ICMP, IPMI та інші, що забезпечує сумісність із сучасними мережевими пристроями. Гнучкість налаштувань дозволить нам створювати користувацькі шаблони для моніторингу специфічних елементів інфраструктури, а автоматизація процесів зменшить час впровадження та знизить ризик помилок. Потужна система сповіщень Zabbix підтримує різні канали зв'язку, такі як

електронна пошта, SMS, месенджери та вебхуки, що дозволить нашій системі реагувати на проблеми.

Інструменти візуалізації, які включають графіки, дашборди та звіти, допоможуть нам аналізувати стан мережі й дозволять швидко виявляти її слабкі місця.

Zabbix як система моніторингу корпоративних мереж потребує надійного способу зберігання великих обсягів даних, і в якості бази даних буде використано MySQL. У базі даних зберігається вся інформація про конфігурацію системи, метрики моніторингу, події, тригери, історичні дані, а також інформація, необхідна для побудови звітів і графіків. Завдяки цьому MySQL стане для нашого проекту фундаментом, який забезпечить ефективну обробку та доступ до даних, необхідних для повноцінної роботи Zabbix.

MySQL було обрано для Zabbix завдяки поєднанню високої продуктивності, надійності та доступності. Висока швидкість виконання запитів дозволить Zabbix обробляти тисячі записів щосекунди, що є надзвичайно важливим у корпоративній мережі. Ця продуктивність забезпечить можливість миттєвої обробки даних, швидкого доступу до метрик і своєчасного реагування на події у корпоративній мережі. MySQL також відома своєю надійністю, яка реалізується через механізми захисту даних, транзакційність, можливість реплікації та створення резервних копій, що буде гарантувати стабільність роботи навіть у разі збоїв чи високих навантажень на систему.

Однією з ключових переваг MySQL є її простота у налаштуванні та інтеграції з Zabbix. У процесі розгортання ми зможемо швидко підключити MySQL, використовуючи доступні інструкції та приклади з офіційної документації. Це дозволяє мінімізувати час на налаштування та розпочати моніторинг у найкоротші терміни. Додатковою перевагою є відкритий вихідний код MySQL, що робить її безкоштовною для використання, і в поєднанні з Zabbix значно понижає наші витрати на проєкт.

Варто відзначити, що MySQL має активну спільноту користувачів і розробників, яка постійно працює над її вдосконаленням. Це забезпечує доступ

до великої кількості ресурсів для навчання, технічної підтримки та готових рішень для оптимізації роботи бази даних. Завдяки цьому, MySQL може бути швидко освоєний будь-яким адміністратором в мережі

Таким чином, MySQL є ідеальним вибором для Zabbix завдяки поєднанню продуктивності, надійності, простоти у використанні та економічності. Вона забезпечить стабільну основу для зберігання та обробки даних, дозволяючи Zabbix виконувати свої завдання з максимальною ефективністю та мінімальними витратами.

В зв'язку з необхідністю отримання оповіщень з системи в будь-який час про стан мережі та ключових вузлів було вирішено реалізувати та інтегрувати програмний модуль, який би дозволяв отримувати актуальні дані про важливі події в мережі та графіки з інформацією про стан вузлів та мережі.

Для забезпечення оперативного інформування про стан корпоративної мережі та виявлені проблеми в системі моніторингу Zabbix обрано два основних інструменти для сповіщень — Telegram і Email. Кожен із них має свої особливості, які роблять їх ідеальними для використання в цьому контексті.

Telegram є сучасним месенджером, що надає можливість миттєвих сповіщень у реальному часі. Його інтеграція з Zabbix дозволить налаштувати автоматичну відправку повідомлень про критичні події або відхилення в роботі мережі. Однією з головних переваг Telegram є його мобільність: адміністратори зможуть отримати доступ до сповіщень незалежно від свого місця знаходження через смартфон, планшет чи ПК. Крім того, Telegram підтримує функцію ботів, що дасть змогу створити спеціалізовані канали або чати для команди, де агрегуються всі повідомлення. Додатковою перевагою є шифрування повідомлень і висока швидкість доставки, що гарантує безпеку та своєчасність сповіщень та нашої мережі.

Для розгортання віртуальних машин, які будуть використовуватись у процесі налаштування та тестування системи моніторингу Zabbix, обираються два популярних рішення: VirtualBox і VMware. Обидва інструменти мають свої особливості, що робить їх придатними для різних завдань.

VirtualBox — це безкоштовна система для віртуалізації з відкритим вихідним кодом, розроблена компанією Oracle. Вона має широку підтримку операційних систем, включаючи Windows, Linux і macOS. VirtualBox вирізняється простотою у використанні, що робить її ідеальним вибором для тих, хто лише починає працювати з віртуальними машинами. Крім того, її відкрите програмне забезпечення дозволить розширювати функціонал за допомогою плагінів і модулів. VirtualBox підтримує функції моментальних знімків (snapshots), спільних папок і налаштування мережевих адаптерів, що полегшує тестування складних середовищ, таких як корпоративні мережі.

VMware є професійним і добре зарекомендованим рішенням для віртуалізації, яке пропонує потужні функції для створення високопродуктивних віртуальних середовищ. Основною перевагою VMware є її продуктивність: віртуальні машини, створені за допомогою цього інструмента, зазвичай працюють швидше завдяки оптимізації використання апаратного забезпечення. VMware також забезпечує більш гнучке управління ресурсами, включаючи підтримку графічних процесорів і складніших мережевих конфігурацій. Інструмент підтримує широкий спектр функцій, таких як висока доступність, клонування машин і інтеграція з хмарними рішеннями.

Обидва інструменти мають свої переваги залежно від контексту використання. VirtualBox підходить для невеликих проєктів, освітніх завдань і тестування завдяки своїй доступності та простоті. Це економічний варіант без втрати функціональності, і буде оптимальним варіантом для тестування мережі

Для проектування та тестування корпоративної мережі в рамках роботи використовується GNS3 (Graphical Network Simulator 3). Це популярний інструмент, який дозволяє створювати складні мережеві топології у віртуальному середовищі. GNS3 забезпечує високий рівень симуляції, підтримуючи не лише програмні маршрутизатори та комутатори, але й інтеграцію з реальним обладнанням, що робить його ідеальним вибором для практичної роботи з нашою мережею.

Побудова ефективної та стабільної корпоративної мережі неможлива без правильного вибору ключових компонентів інфраструктури, таких як комутатори та маршрутизатори. Ці пристрої виконують різні, але взаємопов'язані функції, що дозволяють забезпечити швидкість, надійність та безпеку обміну даними в межах мережі та між різними підмережами.

Комутатори є основою для побудови локальної мережі (LAN), забезпечуючи зв'язок між комп'ютерами, серверами, принтерами та іншими пристроями. Основним завданням комутатора є передача даних між кінцевими точками мережі. Сучасні комутатори здатні не лише виконувати базову функцію передачі пакетів даних, а й здійснювати налаштування VLAN (Virtual Local Area Network), що дозволяє сегментувати мережу на кілька логічних підмереж для зручності керування трафіком і підвищення безпеки. Вибір комутатора залежить від таких факторів, як кількість портів, швидкість з'єднання, підтримка стандартів QoS (Quality of Service) та можливості керування.

Для нашого проекту ідеальним варіантом є комутатори, які підтримують 24 або 48 портів Ethernet та надають можливості для розділення мережі на VLAN, пріоритезації трафіку та моніторингу її стану. Вони дозволяють організувати ефективну маршрутизацію трафіку між різними підмережами та контролювати використання ресурсів мережі.

В якості комутатора буде використано Cisco Catalyst Switch WS-C2960-48TC-L(рис 2.1).



Рисунок 2.1 – Cisco Catalyst Switch WS-C2960-48TC-L.

Маршрутизатори є основними пристроями, які забезпечують передачу даних між різними мережами. Їх основне завдання полягає в маршрутизації трафіку між локальною мережею (LAN) і зовнішніми мережами, такими як Інтернет, або між різними підмережами в межах організації. Крім цього, маршрутизатори виконують роль фільтрації трафіку для підвищення безпеки, а також можуть реалізовувати функції, пов'язані з контролем доступу, обмеженням пропускної здатності і балансуванням навантаження.

Ключовими характеристиками для нашого маршрутизатора є продуктивність, гнучкість у налаштуваннях і можливості для безпеки.

Маршрутизатори зазвичай працюють на рівні 3 моделі OSI і здатні здійснювати маршрутизацію між різними підмережами, що дозволить наам розподілити трафік оптимальним шляхом.

Крім того, маршрутизатори часто підтримують функції безпеки, зокрема міжмережеві екрани (firewall) для захисту від зовнішніх атак, інші функції включаючи шифрування даних для захисту конфіденційної інформації, моніторинг і аналіз трафіку для виявлення аномалій і потенційних загроз допоможе нам забезпечити нам безпечне з'єднання

Вибір маршрутизатора для нашої мережі залежить від багатьох факторів, таких як масштаби мережі, вимоги до продуктивності, типи з'єднань (наприклад, широкосмугові чи волоконно-оптичні лінії), а також наявність специфічних функцій, таких як підтримка IPv6, VoIP, або QoS для оптимізації голосових і відео-зв'язків. Для нашого проєкту важливими є такі параметри, як зручність налаштування, підтримка базових функцій безпеки і доступність технічної підтримки.

Для тестування буде використано Cisco ISR (Integrated Services Routers) 4400 Series(рис 2.2



Рисунок 2.2 – Маршрутизатор Cisco ISR (Integrated Services Routers) 4400 Series

2.2 Архітектура та принципи роботи Zabbix

Структура Zabbix складається з кількох основних компонентів, які взаємодіють для збору, обробки та відображення даних про стан мережі, серверів і інших систем. Ось основні компоненти, які формують архітектуру Zabbix викладені нижче та приведені на рис 2.3.



Рисунок 2.3 – Основні компоненти системи Zabbix

Основним компонентом є Zabbix Server, який відповідає за обробку і збереження всієї інформації, що надходить від агентів або проксі-серверів. Він займається збором даних, обчисленням метрик, створенням сповіщень про події та інциденти, а також зберігає історичні дані в базі даних. Zabbix Server також відповідає за виконання команд, наприклад, запуск скриптів або відновлення

стану служби після збою. Крім того, сервер може генерувати графіки, звіти, а також надає доступ до всіх зібраних даних через веб-інтерфейс.

Zabbix Database відіграє важливу роль у зберіганні даних, які зібрані з моніторингованих систем. База даних містить всю інформацію, пов'язану з налаштуваннями системи, даними про події та статуси хостів, а також історичні дані про моніторинг. Це дозволить здійснювати аналіз та відстеження продуктивності з часом, що є важливим для виявлення тенденцій і запобігання потенційним проблемам. База даних також забезпечує швидкий доступ до потрібних даних, що дозволить нам оперативно реагувати на зміни в стані системи.

Zabbix Agent – це програмне забезпечення, яке встановлюється на хостах, що моніторяться. Агент відповідає за збір інформації про стан системи, наприклад, використання процесора, пам'яті, простору на диску, а також за передавання цих даних на сервер. Агент може здійснювати моніторинг як на запит сервера, так і в режимі активного збору даних, що дозволяє гнучко налаштовувати моніторинг для різних умов.

Zabbix Proxy є необов'язковим компонентом, який використовується для моніторингу віддалених хостів або мереж, де неможливо або неефективно підключати агент безпосередньо до сервера Zabbix. Проксі виступає як посередник між сервером і віддаленими пристроями, збираючи дані від агентів і передаючи їх на сервер, що дозволить знижувати навантаження на сервер і забезпечувати безперебійний моніторинг в умовах обмеженого або нестабільного з'єднання.

Zabbix Web Interface надає нам доступ до інтерфейсу для налаштування, перегляду даних і управління моніторингом. Він дозволить додавати нові хости, налаштовувати параметри моніторингу, переглядати історію подій, створювати графіки та отримувати сповіщення. Веб-інтерфейс є основним інструментом для взаємодії з системою і дозволяє нам використовувати Zabbix через зручний графічний інтерфейс.

Zabbix API забезпечує можливість інтеграції Zabbix з іншими системами. API дозволяє автоматизувати процеси, додавати або змінювати хости, налаштовувати параметри моніторингу, а також взаємодіяти з іншими інструментами моніторингу та управління інфраструктурою. Це дає можливість збудувати автоматизовані рішення для моніторингу та забезпечити швидке реагування на зміни в інфраструктурі.

. Моніторинг пристроїв та метрик буде здійснюватися в Zabbix з через елементи моніторингу (items), які збирають дані з різних джерел. Це будуть системні метрики, такі як використання процесора або пам'яті, або специфічні показники з додатків або мережевих пристроїв. Ці метрики допоможуть адекватно оцінити стан інфраструктури і визначити потенційні проблеми.

Zabbix використовує ряд потужних інструментів для автоматизації моніторингу, які дозволяють точно і ефективно виявляти проблеми в інфраструктурі. Одним із важливих компонентів є тригери, які визначають умови, за яких повинні бути активовані сповіщення або вжиті інші дії. Тригери працюють на основі змін у значеннях моніторингових елементів (items), таких як використання процесора, пам'яті, доступність мережевих інтерфейсів або стан сервісів. Якщо значення метрики перевищує певний поріг або відповідає іншим умовам, тригер буде активуватися і генерувати подію, яка може бути оброблена за допомогою сповіщень або автоматичних дій.

Шаблони в Zabbix є набором налаштувань, які можна застосовувати до групи хостів для спрощення управління моніторингом. Використання шаблонів допоможе нам значно знизити час на налаштування та забезпечити узгодженість в конфігураціях. Наприклад, шаблон для моніторингу серверів Linux буде включати стандартні елементи моніторингу для цих хостів, такі як використання процесора, пам'яті, стан диска, а також тригери для виявлення аномалій у роботі.

Хости є одиничними елементами інфраструктури, які моніторяться. Хост може бути фізичним або віртуальним сервером, пристроєм мережі, додатком чи іншою частиною інфраструктури, що потребує моніторингу. Хости можуть бути налаштовані для використання одного або кількох шаблонів, що спрощує процес

додавання нових хостів до системи. Кожен хост має свої елементи моніторингу, які збирають відповідні метрики.

Управління цими елементами здійснюється через **графіки та звіти**, які допомагають нам візуалізувати зібрані дані та спостерігати за їх динамікою. Графіки відображають тренди для конкретних елементів моніторингу, що дозволяє нашій мережі виявляти потенційні проблеми на ранніх стадіях і вживати необхідні заходи. Також буде створено звіти для збору статистики по всій інфраструктурі, що дозволяє здійснювати аналіз за певний період.

Дії в Zabbix відповідають за виконання автоматичних операцій, таких як надсилання сповіщень або запуск скриптів у разі активації тригера. В Zabbix налаштовано дії для різних типів інцидентів, що дозволяє нашій системі оперативно реагувати на проблеми, без необхідності втручання адміністратора. Сповіщення можуть бути відправлені через різні канали, включаючи email, SMS, Telegram, або через інші інтеграції, що забезпечує зручність і оперативність.

Таким чином, Zabbix дозволяє ефективно організувати моніторинг нашої мережі за допомогою шаблонів, тригерів, елементів моніторингу, графіків та автоматичних дій, що дозволяє не лише збирати та аналізувати дані, а й оперативно реагувати на проблеми в інфраструктурі. Це робить Zabbix потужним інструментом для забезпечення безперебійної роботи корпоративної мережі

2.3 Розробка схеми мережі

Макет Віртуальної мережі складається з: 4 маршрутизаторів, 4 комутаторів, 12 ПК, Ubuntu сервера, та адміністративного ПК

Адміністративний відділ включає в себе сам Zabbix сервер, комп'ютер адміністратора, та маршрутизатор для зв'язку з мережею Інтернет і зображений на рис 2.4

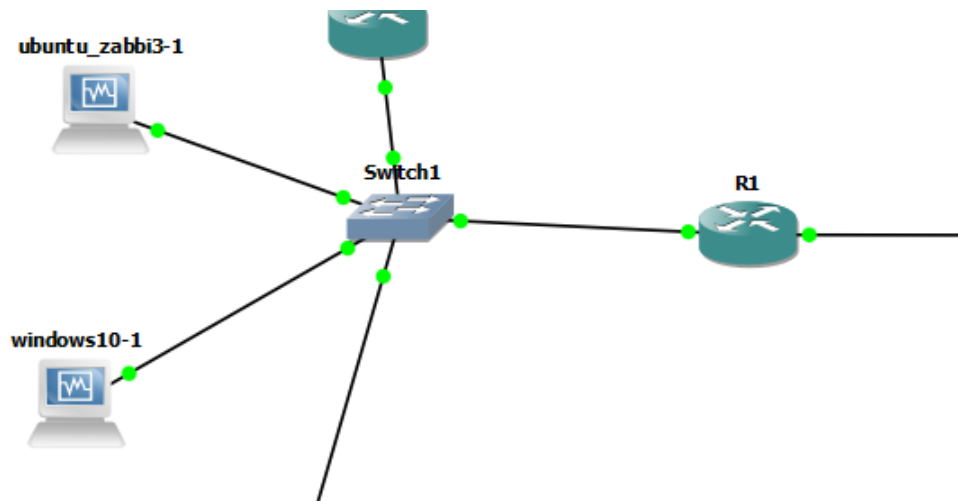


Рисунок 2.4 – Адміністративний відділ

На Zabbix сервері раніше налаштовано фаїрволл та введено статичну ір адресу:

```
ufw allow 80,443,10050,10051/tcp
```

```
ufw allow 10050,10051/udp
```

Де:

- 80 (порт для http запитів (веб-інтерфейс));
- 443 (для https запитів (веб інтерфейс));
- 10050 (порти для отримання інформації від zabbix агентів).

На всіх маршрутизаторах налаштовано DHCP, протокол маршрутизації, SNMP для зв'язку з Zabbix сервером, та на головному роутері налаштовано NAT.

Приклад налаштування:

SNMP:

```
R1(config)#snmp-server community public RO
```

```
R1(config)#snmp-server community private RW
```

DHCP:

```
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

!

```
R1(config)#ip dhcp pool MYPOOL
```

```
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
```

```
R1(dhcp-config)#default-router 192.168.1.1
```

```
R1(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
```

Маршрутизація:

```
R1(config)#router rip
```

```
R1(config-router)#version 2
```

```
R1(config-router)#network 192.168.1.0
```

```
R1(config-router)#no auto-summary
```

NAT:

```
R1(config)#ip nat inside source list 1 interface FastEthernet0/0 overload
```

Для зв'язку з адміністративним ПК на ньому буде налаштовано Zabbix Agent

Відділ 1 має 2 маршрутизатори та 10 віндос та лінукс машинта зображений на рис. 2.5. Відділ 2 аналогічно, кожен з них має свого адміністратора Zabbix. Маршрутизатори налаштовані аналогічно

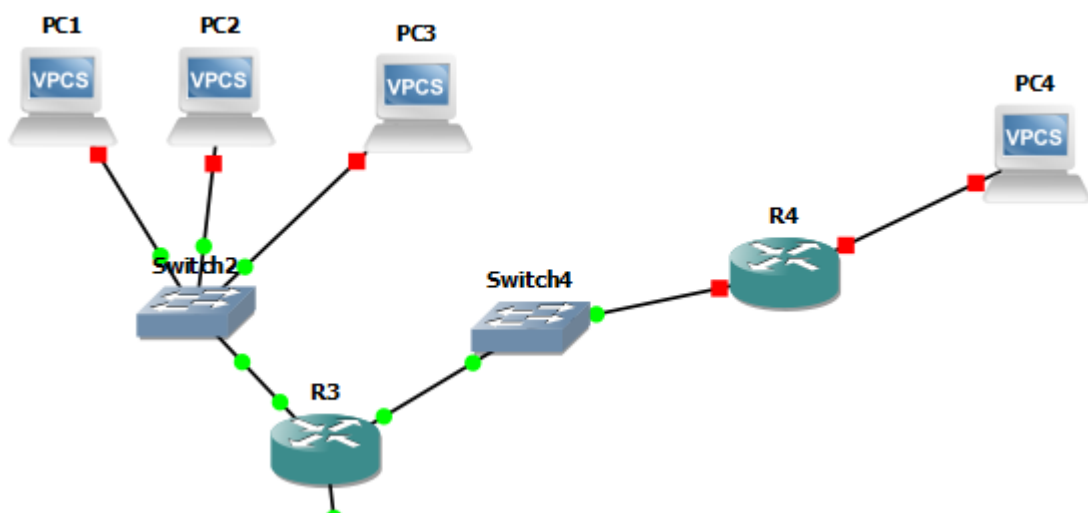


Рисунок 2.5 – Приклад мережі відділу мережі

Висновки до розділу 2

В цьому розділі було вибрано інструментарій для майбутнього проекту, розглянуто принципи роботи Zabbix та методи його реалізації в нашій мережі. Проаналізовано вибір найбільш ефективного графічного симулятора та платформу віртуалізації. Створено макет корпоративної мережі та налаштовано зв'язок між відділами.

Розділ 3: Встановлення та налаштування моніторингової мережі

3.1 Встановлення Zabbix

Спочатку оновимо apt та встановимо базу даних:

```
semenchuk@semenchuk:~$ sudo apt update
```

```
semenchuk@semenchuk:~$ sudo apt upgrade -y
```

Встановлення і налаштування бази даних:

```
semenchuk@semenchuk:~$ sudo apt install mysql-server -y
```

```
semenchuk@semenchuk:~$ sudo mysql_secure_installation
```

```
semenchuk@semenchuk:~$ sudo mysql -u root -p
```

```
CREATE DATABASE zabbix character set utf8mb4 collate utf8mb4_bin;
```

```
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'zabbix_password';
```

```
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
```

```
FLUSH PRIVILEGES;
```

```
EXIT;
```

Встановлення Zabbix

```
semenchuk@semenchuk:~$
```

wget

```
https://repo.zabbix.com/zabbix/6.0/ubuntu/debian/pool/main/z/zabbix-release/zabbix-  
release_6.0-1%2Bbionic_all.deb
```

```
semenchuk@semenchuk:~$ sudo dpkg -i zabbix-release_6.0-1+bionic_all.deb
```

```
semenchuk@semenchuk:~$ sudo apt update
```

Встановлення серверу, веб-інтерфейсу, агента:

```
semenchuk@semenchuk:~$ sudo apt install zabbix-server-mysql zabbix-  
frontend-php zabbix-agent -y
```

Встановлення веб сервера та PHP для роботи з інтерфейсом:

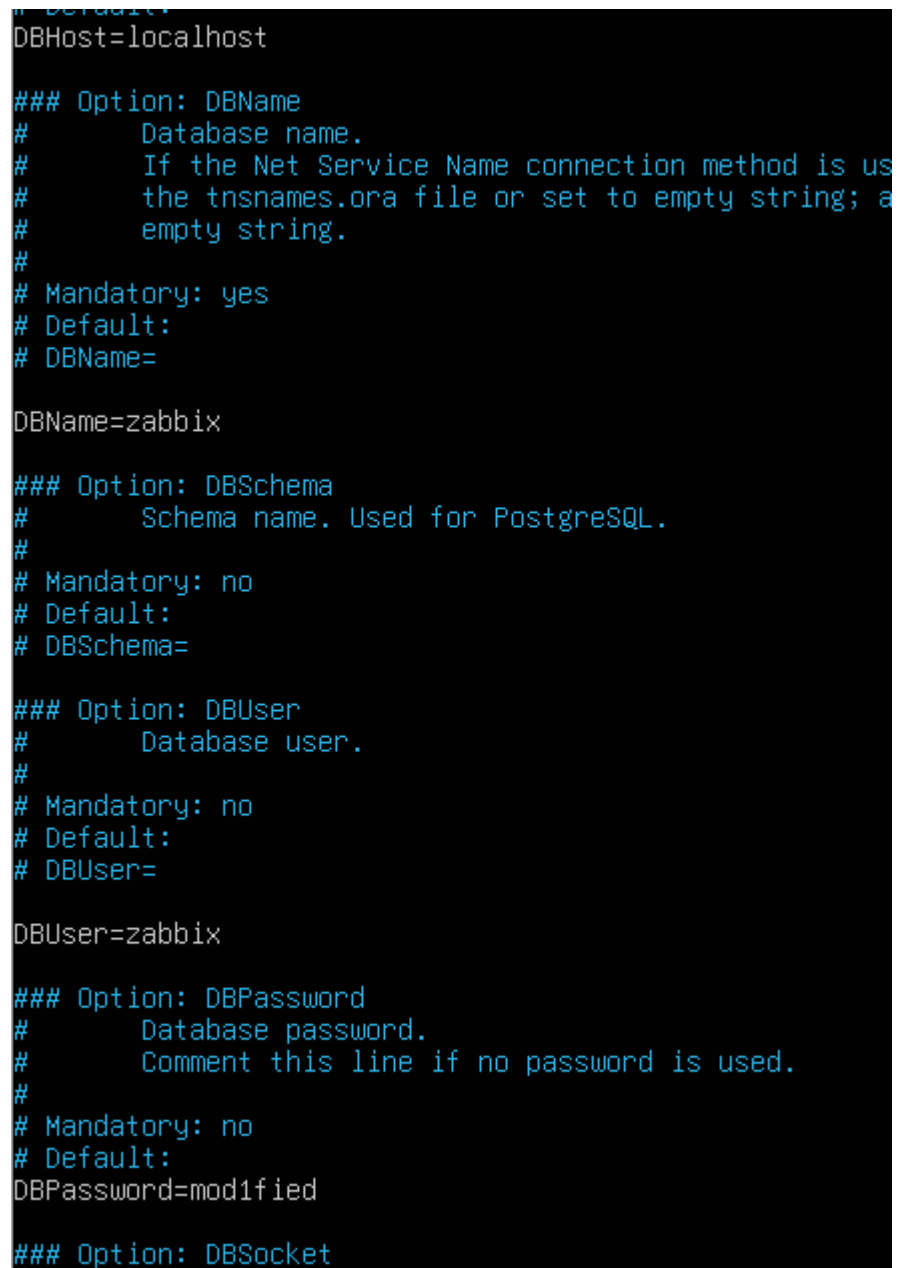
```
semenchuk@semenchuk:~$ sudo apt install apache2 libapache2-mod-php php-  
mbstring php-gd php-xml php-bcmath php-ldap php-mysql php-json php-fpm -y
```

Імпортування бази даних:

```
semenchuk@semenchuk:~$ sudo zcat /usr/share/doc/zabbix-server-  
mysql*/create.sql.gz | mysql -u zabbix -p zabbix
```

Змінимо конфігураційний файл(рис 3.1):

semenchuk@semenchuk:~\$ sudo nano /etc/zabbix/zabbix_server.conf

A screenshot of a terminal window showing the nano text editor editing the file /etc/zabbix/zabbix_server.conf. The file content is as follows:

```
# Database configuration
DBHost=localhost

### Option: DBName
# Database name.
# If the Net Service Name connection method is used,
# the tnsnames.ora file or set to empty string; a
# empty string.
#
# Mandatory: yes
# Default:
# DBName=

DBName=zabbix

### Option: DBSchema
# Schema name. Used for PostgreSQL.
#
# Mandatory: no
# Default:
# DBSchema=

### Option: DBUser
# Database user.
#
# Mandatory: no
# Default:
# DBUser=

DBUser=zabbix

### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=modified

### Option: DBSocket
```

Рисунок 3.1 – Конфігураційний файл zabbix-server.conf

Після всіх цих дій можемо перейти до веб-інтерфейсу(рис 3.2):

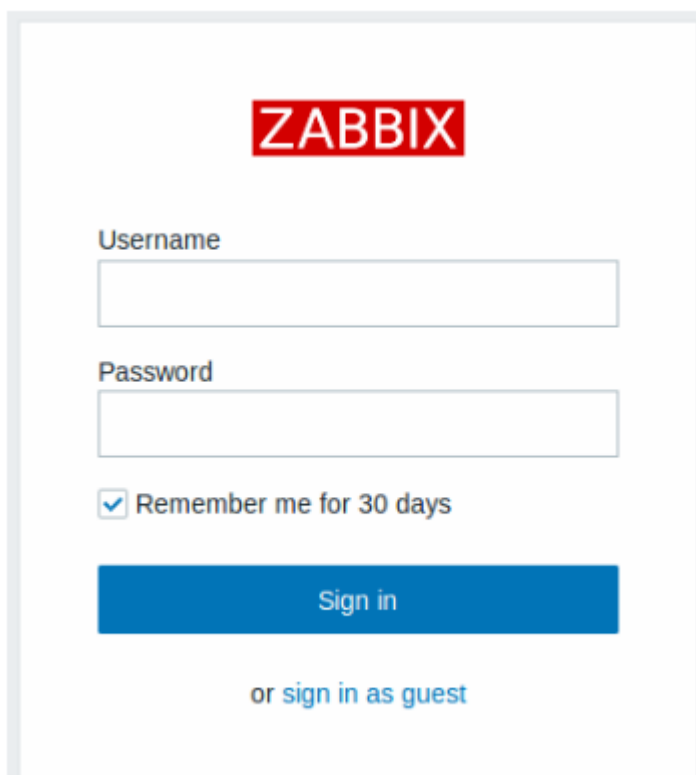


Рисунок 3.2 – Окно входу в Zabbix

Після всіх цих дій нарешті можна перейти до веб інтерфейсу Zabbix(рис 3.3), і почати налаштування самого моніторингу в мережі

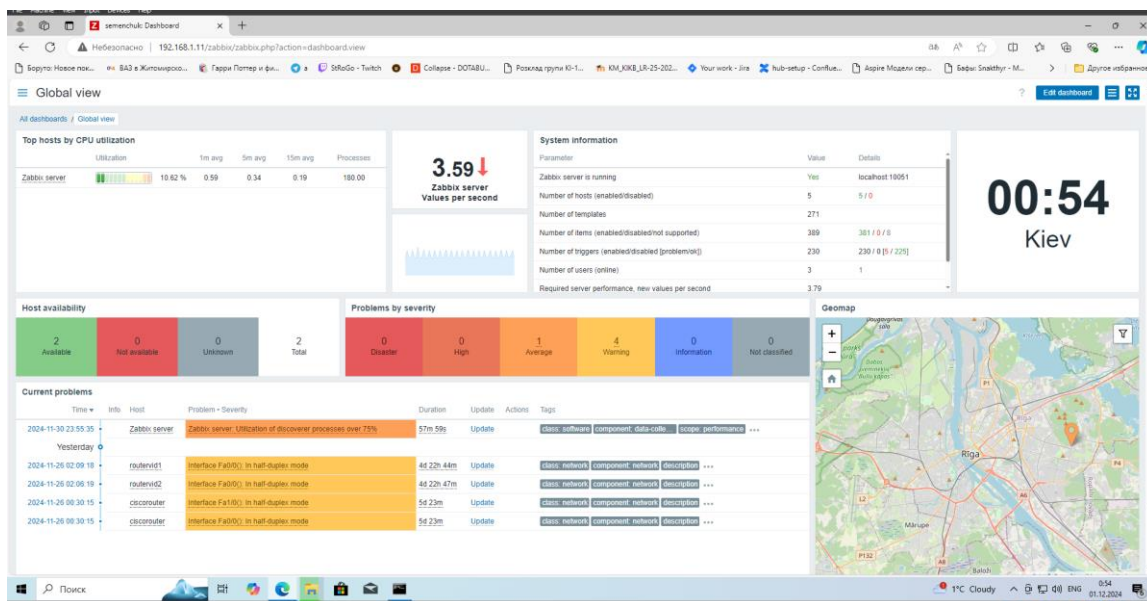


Рисунок 3.3 – Начальне вікно Zabbix

Почнемо з додавання мережових пристроїв в моніторингову систему. Завдяки SNMP добавляємо комутатори та маршрутизатори в мережу. Як приклад приведемо маршрутизатор 1 відділення на рис 3.4 і його успішне відображення на рис 3.5.

Host ? X

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name:

Visible name:

Templates

Name	Action
Cisco IOS by SNMP	Unlink Unlink and clear

* Host groups:

Interfaces

Type	IP address	DNS name	Connect to	Port	Default
SNMP	192.168.1.4		IP DNS	161	☒ Remove

[Add](#)

Description:

Monitored by proxy:

Enabled: ☒

Рисунок 3.4 – Додавання мережового хоста

routervid1	192.168.1.4:161	Enabled	Latest data (5)	10	Graphs: 7	Dashboards: 1	Time
routervid2	192.168.1.5:161	Enabled	Latest data (5)	1	Graphs: 7	Dashboards: 1	Time

Рис 3.5 – Успішне додавання хоста

Далі перейдемо до підключення пристроїв за допомогою агентів. Як приклад будемо використовувати машину Windows 10 на рис 3.6-8.

Zabbix Agent (64-bit) v6.4.20 Setup X

Zabbix Agent service configuration

Please enter the information for configure Zabbix Agent

ZABBIX

Host name:

Zabbix server IP/DNS:

Agent listen port:

Server or Proxy for active checks:

☐ Enable PSK

☐ Add agent location to the PATH

Рисунок 3.6 – Встановлення Zabbix-Agent на Windows

Рисунок 3.7 – Додавання хоста Windows в Zabbix

Рисунок 3.8 – Перевірка додавання хоста

Після цих базових налаштувань ми вже можемо побачити початкові результати роботи моніторингової системи, моменти навантаження на мережевий трафік, або навантаження на фізичні параметри пристроїв, як приклад рисунки 3.9-10:

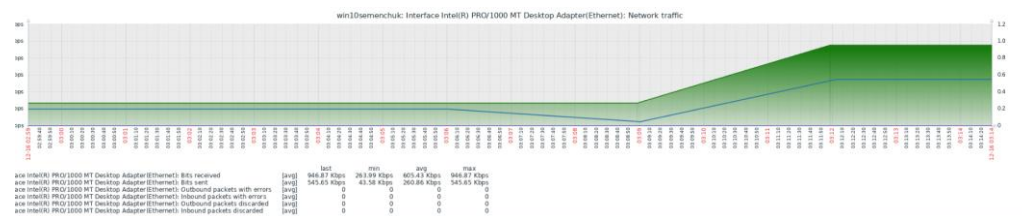


Рисунок 3.9 – Графік мережного трафіка

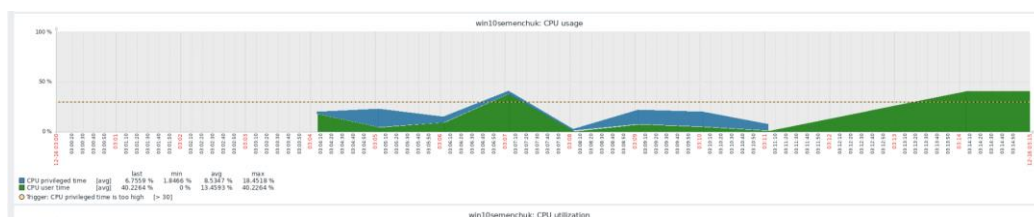


Рисунок 3.10 – Графік навантаження CPU

Налаштування системи сповіщень також має вагомий вклад в роботу системи. Сповіщення допомагають адміністратору швидко реагувати на інциденти, навіть коли він знаходиться не в процесі моніторингу мережі. Для цього налаштуємо розсилку за допомогою telegram і email. Процес

налаштування системи сповіщень показаний на рисунках 3.11-16. Тестування продукту було проведено в наступному розділі

Створимо телеграм бота та отримаємо токен:

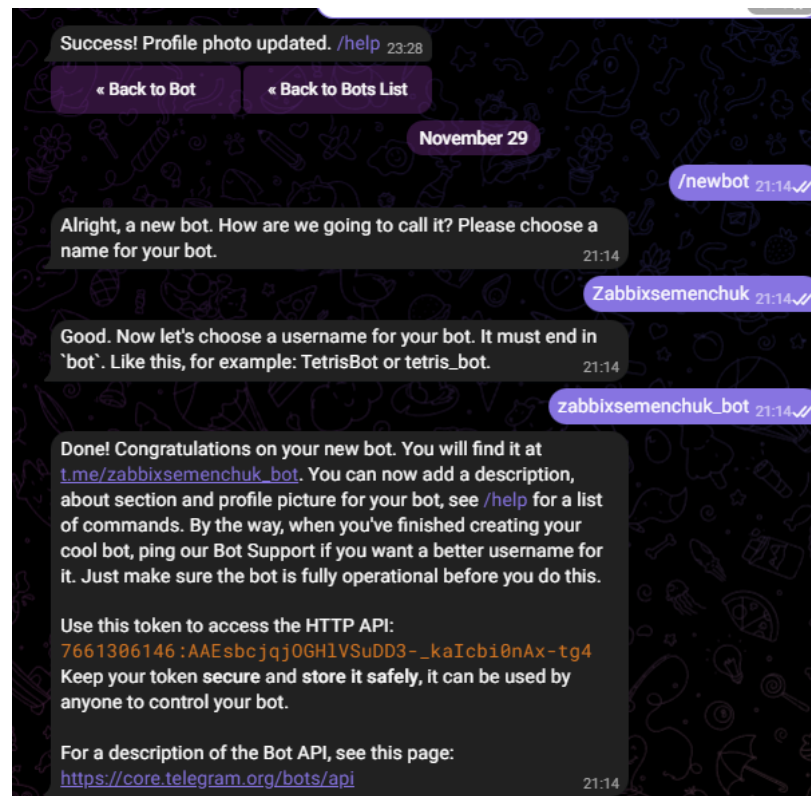


Рисунок 3.11 – Створення токена

Створимо телеграм медіа алерт:

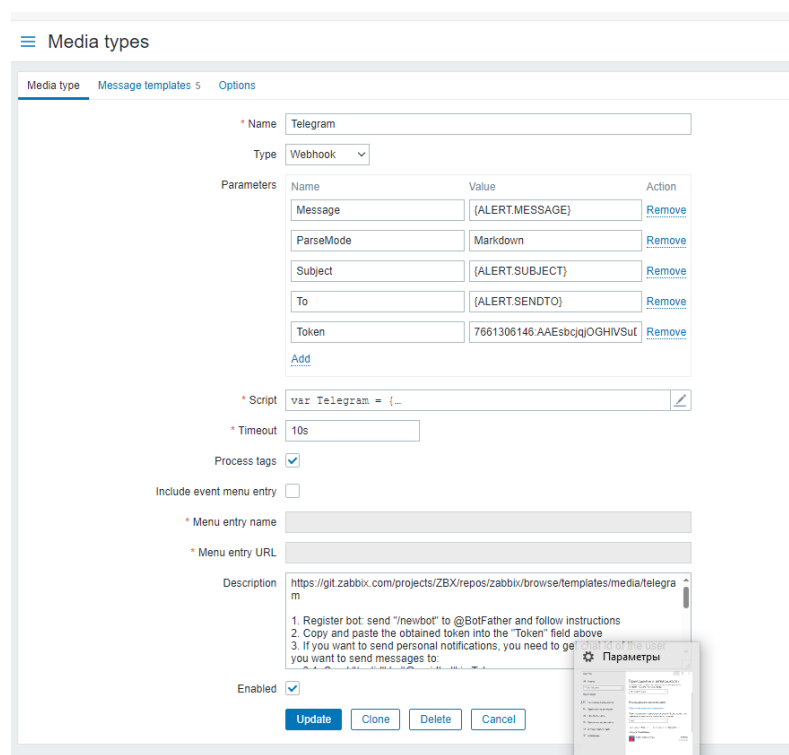


Рисунок 3.12 – Створення медіа алерт telegram

Також створимо alert для роботи з email. Для коректної автентифікації в гугл аккаунті було створено пароль для додатку Zabbix:

The screenshot shows the 'Media types' configuration page in Zabbix. The 'Media type' tab is selected. The configuration fields are as follows:

- Name: email
- Type: Email
- Email provider: Generic SMTP
- SMTP server: smtp.gmail.com
- SMTP server port: 465
- Email: semencukmaksym639@gmail.com
- SMTP helo: gmail.com
- Connection security: None, STARTTLS, SSL/TLS (selected)
- SSL verify peer: ☐
- SSL verify host: ☐
- Authentication: None, Username and password (selected)
- Username: semencukmaksym639@g
- Password: [Change password button]
- Message format: HTML, Plain text (selected)
- Description: [Empty text area]
- Enabled: ☒

Buttons at the bottom: Update, Clone, Delete, Cancel.

Рисунок 3.13 – Створення медіа алерт email

Тепер створимо двох адмінів для кожного відділу та присвоємо їм дані:

The screenshot shows the 'Users' page in Zabbix. The 'Media' tab is selected. It displays a table of media permissions for two users:

Media	Type	Send to	When active	Use if severity	Status	Action
email	email	kim231_smm@student.ztu.edu.ua	1-7,00:00-24:00	N I W A H D	Enabled	Edit Remove
Telegram	Telegram	497750216	1-7,00:00-24:00	N I W A H D	Enabled	Edit Remove

Buttons at the bottom: Update, Delete, Cancel.

Рисунок 3.14 – Створення адмінстратора

Створимо тестовий трігер для сповіщення адміністратора при недоступності ICMP ping на роутері:

Action

Action

Operations 3

* Name

alert_routervid1

Conditions

Label	Name	Action
A	Trigger equals routervid1: Unavailable by ICMP ping	Remove
Add		

Enabled

☒

* At least one operation must exist.

Update

Clone

Delete

Cancel

Рисунок 3.15 – Налаштування дії на перевірку пінга

Action

Action

Operations 3

* Default operation step duration

1m

Operations

Steps	Details	Start in	Duration	Action
1	Send message to users: adminvid1 (Maksym Semenchuk) via email Send message to user groups: Zabbix administrators via email	Immediately	Default	Edit Remove
1	Send message to users: adminvid1 (Maksym Semenchuk) via telegram Send message to user groups: Zabbix administrators via telegram	Immediately	Default	Edit Remove
1	Send message to users: adminvid1 (Maksym Semenchuk) via Telegram Send message to user groups: Zabbix administrators via Telegram	Immediately	Default	Edit Remove
Add				

Recovery operations

Details	Action
Add	

Update operations

Details	Action
Add	

Pause operations for symptom problems

☒

Pause operations for suppressed problems

☒

Notify about canceled escalations

☒

* At least one operation must exist.

Update

Clone

Delete

Cancel

Рисунок 3.16 – Налаштування дії на відправлення повідомлення

Постійне додавання хостів вручну на нові прилади не зовсім зручне для великої мережі, тому важливо додати автоматичне додавання хостів, щоб спростити процес налаштування мережі та зменшити кількість сліпих зон в мережі. Створення автоматичної системи перегляду мережі та автоматичне додавання хостів показано на рис. 3.17-20

Discovery rules

*** Name**

Discovery by proxy

*** IP range**

*** Update interval**

*** Checks**

Type	Actions
ICMP ping	Edit Remove
SNMPv2 agent "iso.3.6.1.2.1.1.1.0"	Edit Remove
Zabbix agent "system.uname"	Edit Remove
Add	

Device uniqueness criteria

☒ IP address

☐ SNMPv2 agent "iso.3.6.1.2.1.1.1.0"

☐ Zabbix agent "system.uname"

Host name

☒ DNS name

☐ IP address

☐ SNMPv2 agent "iso.3.6.1.2.1.1.1.0"

☐ Zabbix agent "system.uname"

Visible name

☒ Host name

☐ DNS name

☐ IP address

☐ SNMPv2 agent "iso.3.6.1.2.1.1.1.0"

☐ Zabbix agent "system.uname"

Enabled ☒

[Update](#) [Clone](#) [Delete](#) [Cancel](#)

Рисунок 3.17 – Налаштування автоматичного знаходження пристроїв

Добавимо дію, яка автоматично додає хост:

Action ? ×

Name

Type of calculation A and B and C and D

Conditions

Label	Name	Action
A	Received value equals Windows	Remove
B	Uptime/Downtime is greater than or equals 3600	Remove
C	Discovery status equals Up	Remove
D	Service type equals Zabbix agent	Remove
Add		

Enabled ☒

* At least one operation must exist.

[Update](#) [Clone](#) [Delete](#) [Cancel](#)

Рисунок 3.18 – Перевірка Action на Windows agent

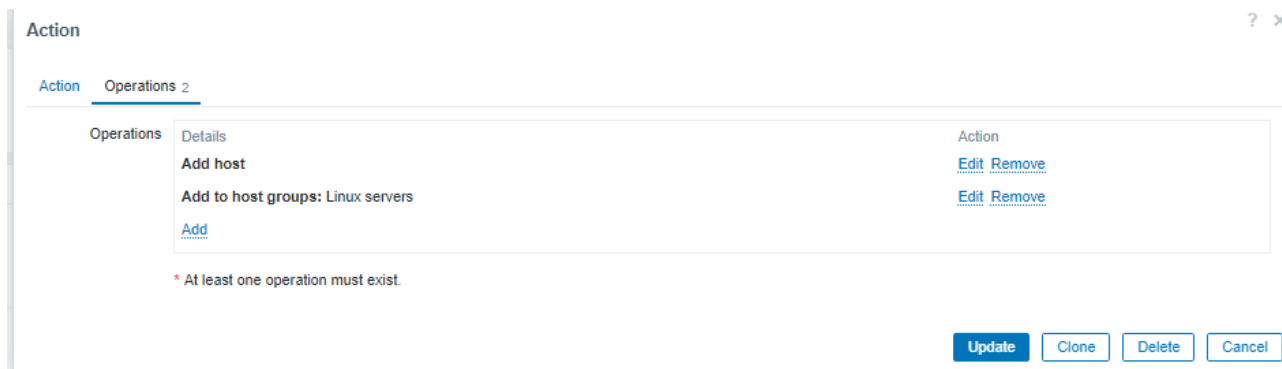


Рисунок 3.19 – Автоматичне додавання хоста

Результат:

Discovered device	Monitored host	Uptime/Down time	SNMP ping	Zabbix agent	Zabbix agent (unreachable)
localnetwork2 (1 device)					
192.168.3.1		02:01:02		2h 1m 2s	
localnetwork2 (5 devices)					
192.168.1.11 (semenchuk)		00:45:14	45m 14s		
192.168.1.5	routerid2	00:48:27	48m 27s	46m 27s	
192.168.1.4	routerid1	00:48:29	48m 29s	46m 29s	
192.168.1.2	vs10semenchuk	00:48:54	48m 54s		46m 54s
192.168.1.1 (gateway)	ciscorouter	00:48:56	48m 56s	46m 56s	

Рисунок 3.20 – Список пристроїв в мережі

Для реагування на інциденти безпеки в Zabbix використовується SNMP trap. На відмінну від звичайних дій Zabbix, які опитують пристрої для отримання даних, трапи надсилаються автоматично і відразу самим пристроєм.

На комутаторах було налаштовано базові налаштування безпеки, включаючи Port Security.

На Zabbix сервері встановимо snmptrap:

```
semenchuk@semenchuk:~$sudo apt update
```

```
semenchuk@semenchuk:~$sudo apt install snmptrapd snmptt
```

Змінемо конфігураційний файл /etc/snmp/snmptrapd.conf, і добавимо функцію отримання трап:

```
authCommunity log,execute,net public
```

```
traphandle default /usr/lib/zabbix/alertscripts/zabbix_trap_receiver.pl
```

Добавимо тригер на реакцію(рис 3.20):

Triggers

All hosts / Switch1 / Enabled / **SNMP** / Items 170 / Triggers 78 / Graphs 17 / Discovery rules 8 / Web scenarios

Trigger Tags Dependencies

* Name: Port Security Violation Detected

Event name: Port Security Violation Detected

Operational data:

Severity: Not classified Information Warning Average High Disaster

* Expression: last (/Switch1/cpsIfPortSecurityStatus,#5)=3 Add

Expression constructor

OK event generation: Expression Recovery expression None

PROBLEM event generation mode: Single Multiple

OK event closes: All problems All problems if tag values match

Allow manual close: ☐

Menu entry name: Trigger URL

Menu entry URL:

Description:

Enabled: ☒

Update Clone Delete Cancel

Рисунок 3.20 – Налаштування реакції на порушення Port Security

При порушенні політик Port Security, система реагує відключенням порта та відправленням повідомлення адміністратору, як і показано на рис 3.21:

	Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Ta
☐	03:28:25	High				Switch1	Port Security Violation Detected	11s	Update		

Рис 3.21 Реакція на порушення Port Security

3.2 Тестування та перевірка роботи моніторингу

В цьому розділі буде протестовано реагування на інциденти в мережі. Як приклад створимо ситуацію, де CPU windows10 PC перегрузилось до 90+%. Zabbix повинен відреагувати на це, та сповістити адміністратора, про загрозу. Результат графіків наведений на рис. 3.22-23.

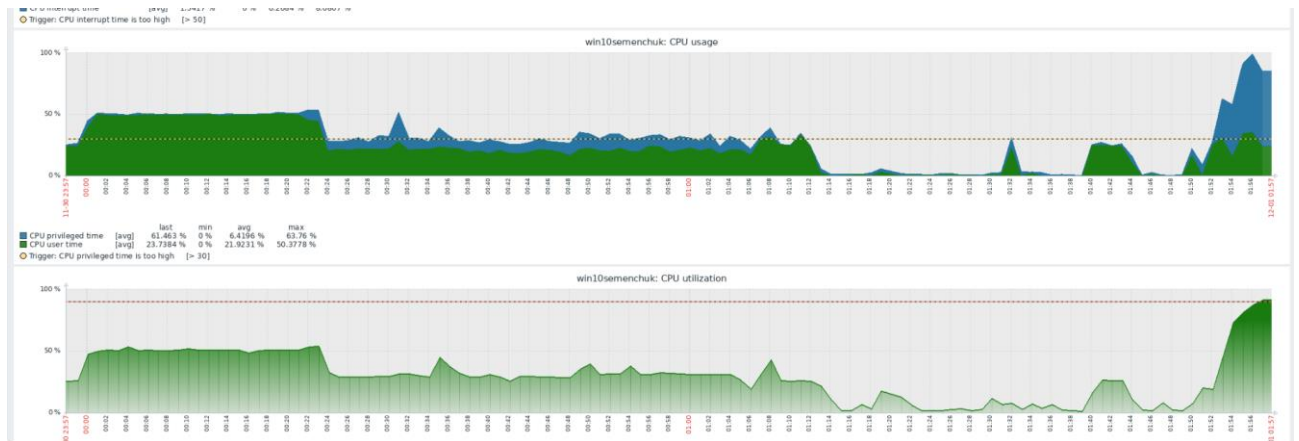


Рисунок 3.22 – Графіки навантаження

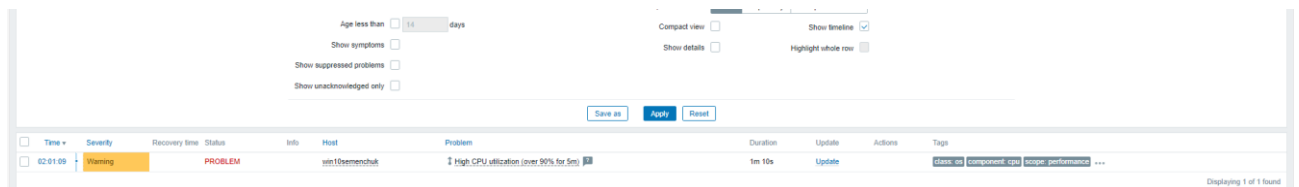


Рисунок 3.23 – Попередження про CPU usage >90%

Тепер спрокуємо ситуацію, де маршрутизатор втратив зв'язок. В цьому система повинна автоматично повідомити адміністратора в самому веб-інтерфейсі Zabbix та відправити повідомлення на пошту та в telegram.(рис 3.24-27)

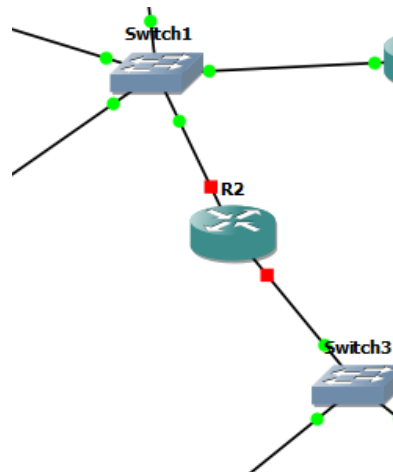


Рисунок 3.24 – відключення маршрутизатора

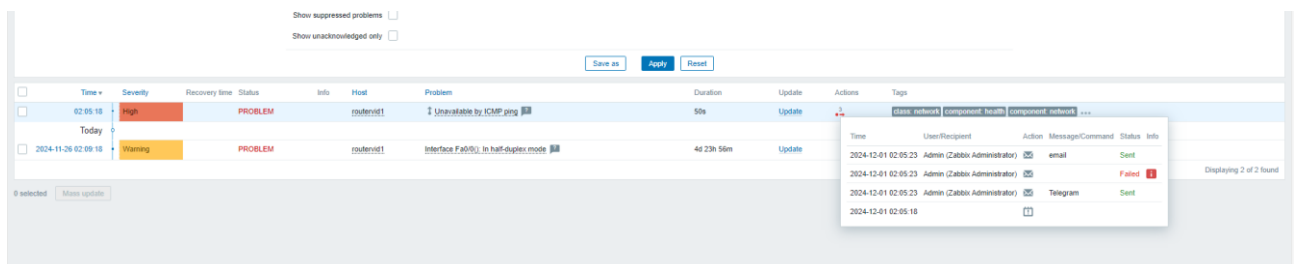


Рис 3.25 – Сповіщення в веб-інтерфейсі

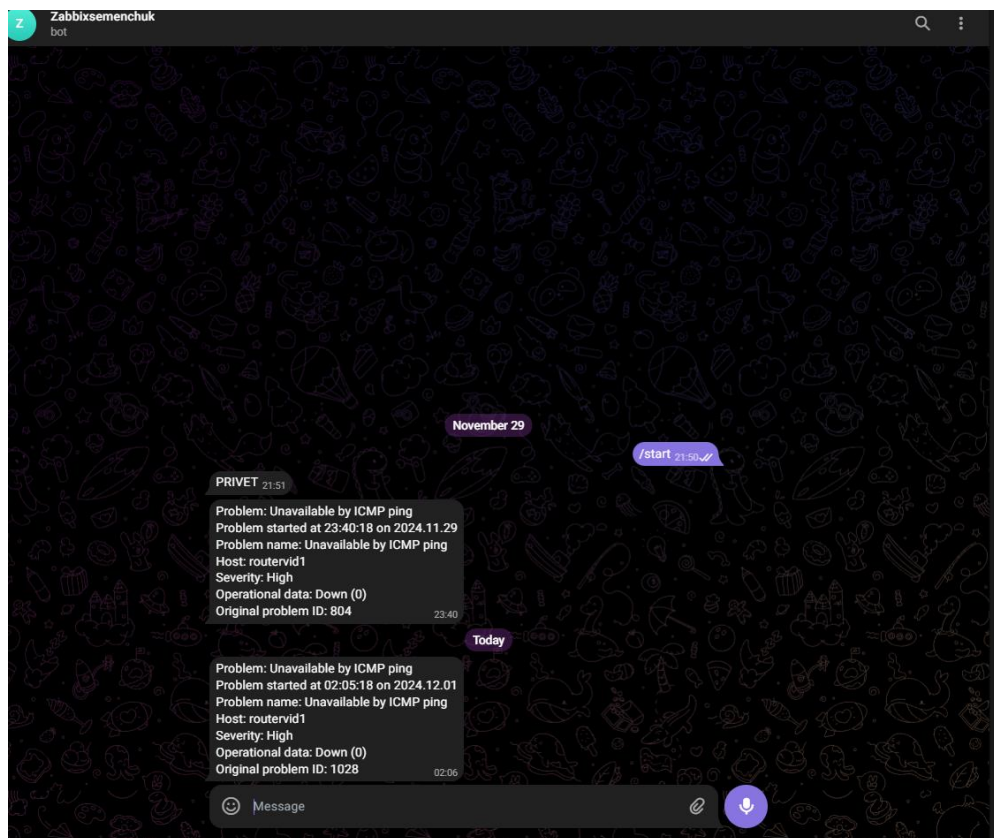


Рисунок. 3.26 – Сповіщення в Telegram

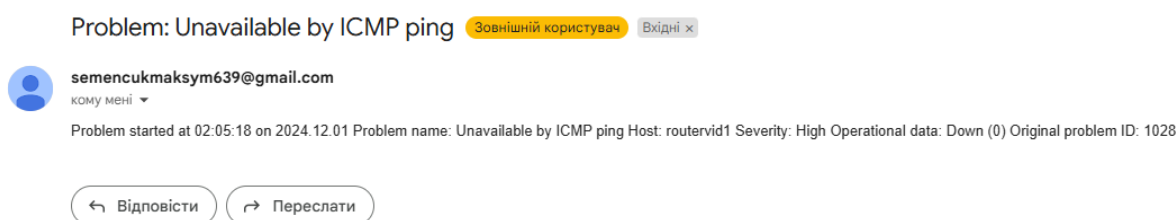


Рисунок 3.27 – Сповіщення в email

3.3 Аналіз результатів та пропозиції для подальших досліджень.

Розроблена моніторингова система мережі, яка включає моніторинг пристроїв, мережевого трафіку та автоматичне реагування на інциденти, досягла поставлених цілей. Система здатна відслідковувати мережевий трафік, виявляти аномалії, що можуть вказувати на потенційні загрози чи несправності, та моніторити стан пристроїв в реальному часі. Вона також може автоматично реагувати на інциденти безпеки, наприклад, блокуючи підозрілі IP-адреси або відправляючи сповіщення адміністратору, що значно знижує час реагування. Додатково система має можливість автоматично додавати нові хости, що робить її гнучкою і масштабованою, здатною адаптуватися до змін у мережі без

втручання адміністраторів. Отримані результати свідчать про високу ефективність розробленої системи в забезпеченні моніторингу та безпеки мережі.

Основні функціональні можливості, що були реалізовані:

Моніторинг мережевого трафіку: Система здатна відслідковувати потоки даних в мережі, виявляти аномалії, що можуть вказувати на потенційні загрози або несправності. Це дозволяє своєчасно реагувати на навантаження або несанкціоновані спроби доступу до мережевих ресурсів.

Моніторинг стану пристроїв: Використовуючи різні технології, система відстежує стан фізичних та віртуальних пристроїв у реальному часі. Це включає в себе перевірку доступності пристроїв, використання їх ресурсів, а також моніторинг працездатності окремих компонентів.

Автоматичне реагування на інциденти: У разі виявлення аномалій чи загроз, система автоматично активує реакцію (наприклад, блокування підозрілих IP-адрес, або відправка сповіщень адміністратору). Це дозволяє значно зменшити час реагування на інциденти і автоматизувати процес усунення неполадок.

Автоматичне додавання хостів: Система здатна самостійно додавати нові пристрої до моніторингової мережі, що забезпечує її масштабованість і дозволяє безперервно адаптуватися до змін у мережевій інфраструктурі без втручання адміністратора.

Незважаючи на досягнуті результати, є кілька напрямків, які можуть бути досліджені і впроваджені в майбутньому для покращення системи та забезпечення більшої ефективності. Для подальшого вдосконалення та розширення функціональних можливостей, можна впровадити інтеграцію з новими технологіями. Зокрема, інтеграція з ELK Stack дозволить покращити аналіз логів та прогнозування інцидентів, оскільки Elasticsearch забезпечить ефективне зберігання та аналіз великих обсягів даних, а Kibana надасть потужні інструменти для візуалізації цих даних. Це дозволить адміністраторам швидше і точніше виявляти загрози та аномалії в мережі.

Інтеграція з SIEM системами, такими як Splunk, також може суттєво покращити безпеку мережі. Splunk має розширені можливості для кореляції подій безпеки та виявлення аномалій у реальному часі. Така інтеграція дозволить підвищити рівень безпеки за рахунок більш глибокого аналізу інцидентів та швидкого реагування на них. Вдосконалення системи з використанням машинного навчання дозволить автоматично виявляти нові типи загроз і аномалій без необхідності вручну налаштовувати пороги та правила. Це дозволить системі адаптуватися до нових типів атак і покращити ефективність виявлення загроз.

Висновки до розділу 3

В цьому розділі налаштовано систему моніторингу мережі та її автоматизацію. Протестовано її працездатність та проаналізовано, які б ще функції та інтеграції могли б покращити систему.

Висновки

У цій роботі було розглянуто методи та технології моніторингу корпоративних мереж. Досліджено різні аспекти моніторингу, включаючи типи моніторингу, методи дослідження та інші релевантні питання. Побудовано мережу та налаштовано моніторинг в ній

У розділі 1 було проведено огляд теми дипломної роботи, було розглянуто дослідження по моніторингу та проведено аналіз, як вони можуть допомогти. Було проаналізовано методи та технології моніторингу, вибрано платформу для моніторингу, та поставлена ціль дипломної роботи

У розділі 2 було обрано інструменти моніторингу. Було розглянуто структура Zabbix, як він зв'язується з робочими пристроями та розібрано його архітектуру. Також було побудовано загальну схему мережі та налаштовано базові протоколи

У розділі 3 налаштовано моніторинг пристроїв на Zabbix та додано необхідні функції. Було протестовано мережу та проведено аналіз, що можна додати в існуючу систему

Загальним висновком дослідження є те, що моніторинг є важливим в структурі мережі, та допомагає уникнути можливих проблем, або швидко зреагувати на існуючі. Zabbix в свою чергу надає широкі можливості збору, аналізу та візуалізації даних, а також має інтеграцію з іншими продуктами, що забезпечує повний огляд стану мережі та ефективне управління мережею.

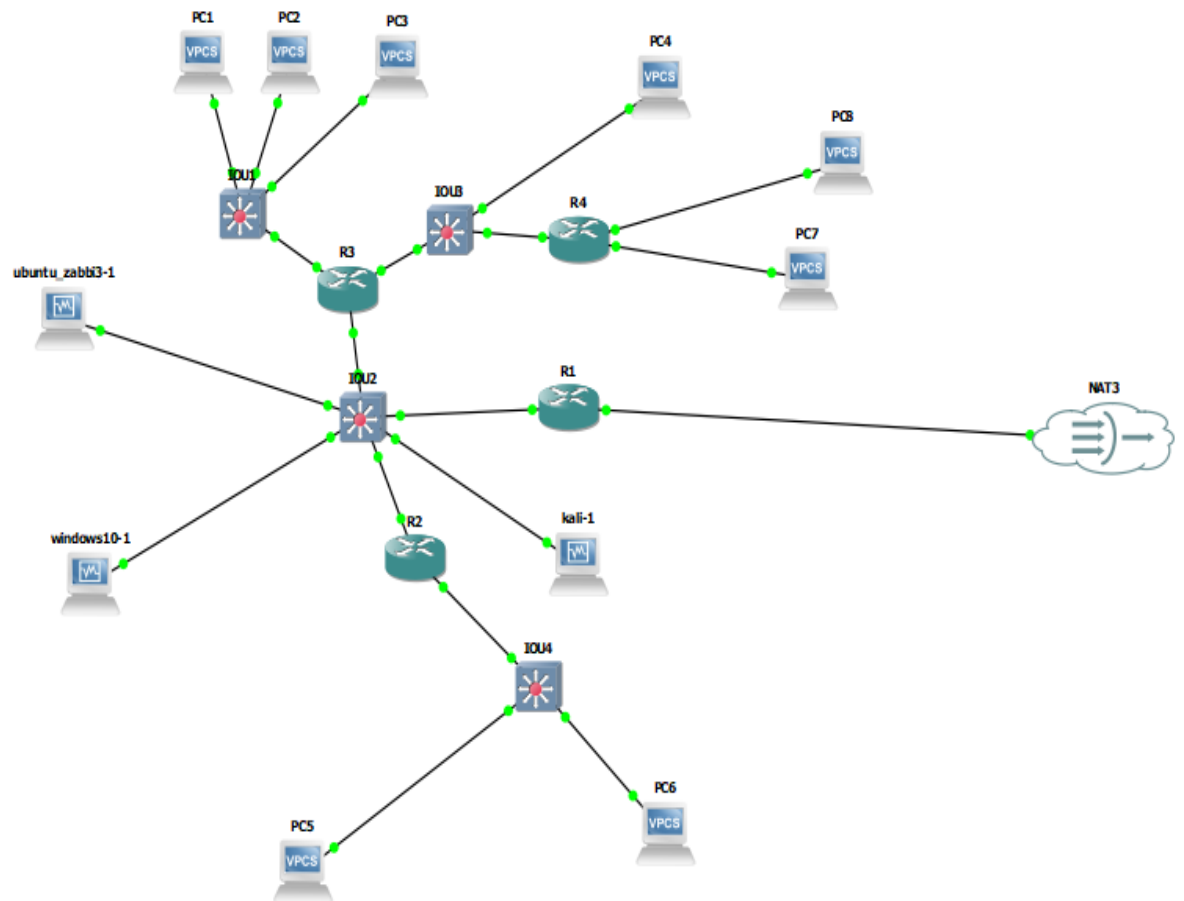
Список використаних джерел

1. Olivie B. Computer Networking : Principles, Protocols and Practice. — Saylor Foundation, 2011. — 282 p.
2. Flores D. Modern Network Observability.— Packt Publishing, 2024. — 506 с.
3. Explaining Network Flow Data - the Foundation of Network Observability. [Електронний ресурс]. — Режим доступу до ресурсу:
<https://www.elastiflow.com/blog/posts/explaining-network-flow-data-the-foundation-of-network-observability>.
4. SentryMSP. How to troubleshoot common network issues in small businesses [Електронний ресурс]. — Режим доступу до ресурсу:
5. William S. Snmp, Snmpv2, Snmpv3, and Rmon 1 and 2. — Addison-Wesley Professional, 1999. — 619 с.
6. Slawek L. Effective Monitoring and Alerting. — O'Reilly Media, 2012, 164 с.
7. Turnbull J., The Art of Monitoring. — 2016. — 769 с.
<https://sentrymsp.com/blog/how-to-troubleshoot-common-network-issues-in-small-businesses/>
8. Ed W. Network Monitoring and Analysis: A Protocol Approach to Troubleshooting. — Prentice Hall, 2000. — 359 с
9. Brian B. Prometheus: Up & Running: Infrastructure and Application Performance Monitoring. — O'Reilly Media 2018. — 368 с.
10. What is network monitoring? [Електронний ресурс]. — Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitorin>
11. Zabbix Documentation. [Електронний ресурс]. — Режим доступу до ресурсу: <https://www.zabbix.com/documentation/7.0/en/manual/introduction>.
12. Dalle Vacche A., Zabbix: Enterprise Network Montioring Made Easy./ Dalle Vacche A., Uytterhoeven P. — Packt Publishing 2017. — 1327 p.
13. Олексюк В. П. Організація комп'ютерної локальної мережі: Посіб. / В. П.Олексюк, Н. Р. Балик, А. В. Балик. — Т. : Підруч. і посіб., 2006. — 80 с.

14. Using Zabbix for Risk Management [Електронний ресурс]: — Режим доступу: <https://blog.zabbix.com/usingzabbix-for-risk-management/6570/> (дата звернення: 15.11.2022).
15. Технологія виявлення мережових загроз з використанням програмного забезпечення Zabbix [Електронний ресурс]: — Режим доступу до ресурсу: <https://journals.dut.edu.ua/index.php/dataprotect/article/view/2762?>
16. Моніторинг обладнання [Електронний ресурс]: — Режим доступу: <https://hs.whitehat.one/ukua/blog/monitorynh-pratsezdatnosti-vashoho-obladnannya>
17. Anggi M. Mobile-based Network Monitoring System Using Zabbix and Telegram. [Електронний ресурс]: — Режим доступу до ресурсу: <https://ieeexplore.ieee.org/document/9274582>.
18. Моніторинг Cisco SNMP Zabbix. [Електронний ресурс]: — Режим доступу до ресурсу: <https://ozt.com.ua/2023/02/02/monitoring-cisco-snmp-zabbix/>
19. Server monitoring with zabbix. . [Електронний ресурс]: — Режим доступу до ресурсу: https://www.zabbix.com/network_monitoring.
20. Liefting N. Zabbix 7 IT Infrastructure Monitoring Cookbook. — Packt Publishing 2024. —540 p.

Додатки

Схема мережі



Налаштування мережових пристроїв

Конфігурація маршрутизатора R-1

Building configuration...

Current configuration : 1622 bytes

!

upgrade fpd auto

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

logging message-counter syslog

!

no aaa new-model

ip source-route

no ip icmp rate-limit unreachable

ip cef

!

!

ip dhcp excluded-address 192.168.1.1 192.168.1.10

!

ip dhcp pool MYPOOL

network 192.168.1.0 255.255.255.0


```
!  
!  
ip tcp synwait-time 5  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
  ip address dhcp  
  ip nat outside  
  ip virtual-reassembly  
  duplex half  
!  
interface FastEthernet1/0  
  ip address 192.168.1.1 255.255.255.0  
  ip nat inside  
  ip virtual-reassembly  
  duplex half  
!  
interface FastEthernet2/0  
  ip address 192.169.1.1 255.255.255.0  
  duplex auto  
  speed auto  
!  
interface FastEthernet2/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!
```

```
router rip
version 2
network 192.168.1.0
no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat inside source list 1 interface FastEthernet0/0 overload
!
access-list 1 permit 192.168.1.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
!
!
snmp-server community public RO
snmp-server community private RW
!
control-plane
!
!
!
!
!
!
!
```

```
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
End
```

Конфігурація маршрутизатора SW-1
Building configuration...

Current configuration : 2022 bytes

```
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname IOU2
```

```
!  
boot-start-marker  
boot-end-marker  
!  
!  
logging discriminator EXCESS severity drops 6 msg-body drops  
EXCESSCOLL  
logging buffered 50000  
logging console discriminator EXCESS  
!  
no aaa new-model  
no ip icmp rate-limit unreachable  
!  
no ip cef  
!  
!  
no ip domain-lookup  
no ipv6 cef  
ipv6 multicast rpf use-bgp  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
!  
!  
!  
!  
!  
vlan internal allocation policy ascending  
!  
ip tcp synwait-time 5
```

```
!  
!  
!  
!  
interface Ethernet0/0  
  switchport mode access  
  switchport port-security maximum 2  
  switchport port-security  
  switchport port-security violation restrict  
  duplex auto  
!  
interface Ethernet0/1  
  switchport mode access  
  switchport port-security maximum 2  
  switchport port-security  
  switchport port-security violation restrict  
  duplex auto  
!  
interface Ethernet0/2  
  switchport mode access  
  switchport port-security maximum 2  
  switchport port-security  
  switchport port-security violation restrict  
  duplex auto  
!  
interface Ethernet0/3  
  switchport mode access  
  switchport port-security maximum 2  
  switchport port-security  
  switchport port-security violation restrict
```

```
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
```

```
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
ip address 192.168.1.7 255.255.255.0
!
ip default-gateway 192.168.1.1
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
```

```
line vty 0 4
login
!
end
```