ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Архітектура системи моніторингу комп'ютерних систем та мереж з використанням штучних нейронних мереж»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерна інженерія
освітньо-професійної програми «Комп'ютерні системи та мережі»

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Владислав Дідовець
(підпис)

Виконав: здобувач вищої освіти групи КСДМ-61
Владислав Дідовець

Керівник: Наталія ЛАЩЕВСЬКА
к.т.н., доцент

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерна інженерія
Ступінь вищої освіти Магістр
Спеціальність 123 Комп'ютерна інженерія
Освітньо-професійна програма «Комп'ютерні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
«_____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дідовцю Владиславу Максимовичу

1. Тема кваліфікаційної роботи: «Архітектура системи моніторингу комп'ютерних систем та мереж з використанням штучних нейронних мереж»

керівник кваліфікаційної роботи Наталія ЛАЩЕВСЬКА, к.т.н.,доцент,

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 р. № _____.

2. Строк подання кваліфікаційної роботи «17» листопада 2025 р.

3. Вихідні дані до кваліфікаційної роботи: системи моніторингу та спостережуваності, документація систем моніторингу, архітектура систем моніторингу, хмарні технології: IaaS, SaaS, PaaS, віртуалізація, методи побудови корпоративних комп'ютерних мереж.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз сучасних систем моніторингу комп'ютерних мереж, їх можливостей та обмежень.
2. Аналіз спостережуваності мережевої інфраструктури.
3. Розробка архітектури інтелектуальної системи моніторингу на основі нейронної мережі.

4. Розробка моделі в Cisco Packet Tracer для отримання системних повідомлень та моделювання умовних ситуацій.
5. Оцінка перспектив розвитку інтелектуальної системи моніторингу.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання«01» вересня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз існуючих систем моніторингу та спостережуваності	01.09-01.10.2025	Виконано
2	Аналіз документації та літератури про системи моніторингу	01.09-01.10.2025	Виконано
3	Моделювання корпоративної мережі у Cisco Packet Tracer	01.09-30.09.2025	Виконано
4	Розробка архітектури інтелектуальної системи моніторингу	01.10-15.11.2025	Виконано
5	Опис модулів інтелектуальної системи моніторингу	01.10-15.11.2025	Виконано
6	Демонстрація роботи IMC на згенерованих інцидентах	01.10-15.11.2025	Виконано
7	Оформлення роботи: вступ, висновки, реферат	15.12-17.12.2025	Виконано
8	Розробка демонстраційних матеріалів	04.12-11.12.2025	Виконано
9	Попередній захист роботи	15.12-17.12.2025	Виконано
	Здача в деканат		

Здобувач вищої освіти _____ Владислав ДІДОВЕЦЬ
(підпис)

Керівник
кваліфікаційної роботи _____ Наталія ЛАЩЕВСЬКА
(підпис)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 73 стор., 46 рис., 8 табл., 26 джерел.

Мета роботи – підвищення ефективності роботи систем моніторингу комп'ютерних систем та мереж, шляхом розробки архітектури інтелектуальної системи моніторингу, що використовує штучні нейронні мережі для автоматичного виявлення інцидентів, аналізу системних подій, і прогнозування можливих збоїв в мережі.

Об'єкт дослідження – система моніторингу комп'ютерних мереж та систем.

Предмет дослідження – методи виявлення інцидентів та аномалій у процесі моніторингу мереж та системи моніторингу комп'ютерних мереж та систем.

Короткий зміст роботи: Сучасні корпоративні комп'ютерні мережі стають дедалі різноманітнішими через активний розвиток технологій. Вони починають більше використовувати хмарні технології, віртуалізацію, розосередження інфраструктури, розміщаючи частину в дата-центрах. Це ставить нові виклики та задачі для існуючих систем моніторингу комп'ютерних систем та мереж. Розподіленість інфраструктури ускладнює моніторинг і знижує рівень спостережуваності та моніторингу мережі. Обмежений моніторинг та спостережуваність підвищує ризики збоїв, збільшення кількості інцидентів, погіршення надійності та відмовостійкості мережі. Запропоновано архітектуру інтелектуальної системи моніторингу комп'ютерних систем та мереж з використанням моделі обробки даних, що здатна класифікувати типи інцидентів, аналізувати їх причини та формувати рекомендації щодо усунення. Такий функціонал забезпечить інтелектуальна система моніторингу, застосовуючи нейронну мережу як інтелектуальний модуль. Використовуючи системні повідомлення отримані з моделі корпоративної комп'ютерної мережі та синтетичних повідомлень, що були згенеровані на основі реальних повідомлень продемонстровано приклади того, як має працювати дана система.

На основі проведеного дослідження було з'ясовано доцільність використання штучних нейронних мереж у системах моніторингу для підвищення точності діагностики, швидкості реагування, автоматизації, модернізації та контролю.

КЛЮЧОВІ СЛОВА: МОНІТОРИНГ МЕРЕЖ, ІНЦИДЕНТ, ШТУЧНІ НЕЙРОННІ МЕРЕЖІ ВИЯВЛЕННЯ АНОМАЛІЙ, СИСТЕМНІ ПОВІДОМЛЕННЯ, ІНТЕЛЕКТУАЛЬНА СИСТЕМА, АГЕНТНИЙ МЕТОД, , IAAS, SAAS, PAAS.

ABSTRACT

Text part of the master's qualification work: 73 pages., 46 pictures., 8 table.,26 sources.

The purpose of the work is to improve the efficiency of computer system and network monitoring by developing an architecture of an intelligent monitoring system that uses artificial neural networks for automatic incident detection, analysis of system events, and forecasting of possible network failures.

Object of research – monitoring systems of computer networks and systems.

Subject of research – methods for detecting incidents and anomalies in the monitoring process using artificial neural networks.

Summary of the work: Modern corporate networks are becoming increasingly complex due to the expansion of cloud services, virtualization, and distributed infrastructures, including the relocation of components to data centers. This complexity creates new challenges for monitoring tools, especially regarding visibility and reliable detection of failures. Limited observability leads to an increased risk of undetected malfunctions, higher incident rates, and reduced reliability and fault tolerance of network infrastructure. The work introduces an architecture of an intelligent monitoring system that incorporates a data-processing module based on an artificial neural network. This module is capable of classifying incident types, analyzing their causes, and generating recommendations for mitigation. The functionality of the intelligent module is demonstrated using real-like system messages obtained from a simulated corporate network and synthetically generated logs that reflect typical operational events.

Based on the results, the feasibility of implementing neural networks in monitoring systems has been confirmed to enhance diagnostic accuracy, reduce response time, and improve automation and efficiency in network administration.

KEYWORDS: network monitoring, incident, artificial neural networks, anomaly detection, system messages, intelligent system, IAAS, SAAS, PAAS.

ЗМІСТ

ВСТУП…… 10
…….
РОЗДІЛ 1. ПОНЯТТЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ, ЇЇ СКЛАДОВІ, ВИДИ, ТИПИ ТА АРХІТЕРКТУРА……... 12

1.1 Поняття про корпоративну комп'ютерну мережу……. 12

1.2 Види та типи комп'ютерних мереж……. 14

1.3 Топології мереж та трирівнева модель……... 20

1.4 Роль та використання віртуалізації, хмарних технологій та хмарних обчислень……. 24

РОЗДІЛ 2. СИСТЕМИ МОНІТОРНГУ КОМП'ЮТЕРНИХ МЕРЕЖ, ЇХ МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ……. 32

2.1 Що таке система моніторингу комп'ютерної мережі?..... 32

2.2 Принципи роботи систем моніторингу комп'ютерних мереж…… 34

2.3 Огляд наявних систем моніторингу, переваги та недоліки……... 36

РОЗДІЛ 3. ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ МОНІТОРНГУ КОМП'ЮТЕРНИХ МЕРЕЖ, ЇХ ФУНКЦІЇ, ПРИНЦИПИ ТА АРХІТЕКТУРА…… 56

3.1 Перспективи розвитку систем моніторинг комп'ютерних мереж…… 56

3.2 Концепція та архітектура системи моніторингу з використанням нейронної мережі або штучного інтелекту…… 57

3.3 Архітектура системи моніторингу комп'ютерної мережі з використанням штучного інтелекту або нейронних мереж…… 60

3.4 Приклад застосування інтелектуальної системи моніторингу……... 69

3.5 Проблеми використання інтелектуальної системи моніторингу комп'ютерної мережі та перспективи розвитку…… 75

ВИСНОВКИ……. 81

ПЕРЕЛІК ПОСИЛАНЬ……... 83
ДОДАТОК А. Відображення статусу комутатора та портів в Prometheus з Grafana…….. 86
ДОДАТОК Б. Інформаційна панель про помилки в Prometheus…….. 87

ДОДАТОК В. Інформаційна панель метрик комп’ютерної мережі з Observium 88
ДОДАТОК Г. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (*Презентація*)……. 89

ВСТУП

Швидкий розвиток інформаційних технологій тісно пов’язаний з трансформацією суспільного життя. Технології покликані зробити наш спосіб життя зручнішим, безпечнішим та продуктивнішим. Це у свою чергу, створює нові виклики для компаній, які мають задовольняти попит на різноманітні сервіси та товари. Для ІТ-сектору це означає постійне зростання обсягів даних, збільшення навантаження на мережі та обчислювальні системи, а також нові загрози у сфері інформаційної безпеки.

Комп’ютерні мережі стали невід’ємною складовою нашого життя. Вони представлені як у вигляді простих домашніх мереж з комп’ютерами, мобільними пристроями й IoT-пристроями, так і у вигляді складних корпоративних інфраструктур, що об’єднують сотні або тисячі різноманітних пристроїв. Якщо для пересічного користувача потрібно лише стабільне підключення до інтернету то для компаній критично важливими є надійність, безперервність і відмовостійкість мереж та сервісів.

Проте сама наявність потужного обладнання не гарантує безпеки та стабільності. Зі зростанням кількості користувачів і сервісів виникає потреба в розширенні мережі та інфраструктури. Використання віртуалізації та хмарних сервісів дозволяє гнучкіше керувати ресурсами, але водночас створює нові ризики та потенційні точки відмови. Для контролю за системами, мережами та сервісами використовуються системи моніторингу та спостережуваності, що дозволяють відстежувати стан мережевого обладнання, мережі та сервісів. Однак в умовах зростаючої кількості даних класичні методи аналізу поступово втрачатимуть ефективність. Оскільки постійний моніторинг та аналіз вимагає правильного налаштування тригерів та правил, а помилки в налаштуванні можуть призвести до надмірної кількості спрацювань і втрати якості аналізу. У свою чергу це ускладнює роботу й знижує ефективність роботи.

У таких умовах більшої актуальності набуває використання нейронних мереж, як інструменту в системах моніторингу. Їх інтеграція дозволить здійснювати цілодобовий моніторинг та аналіз, автоматично обробляти великі обсяги інформації, виявляти помилки, аномалії, попереджати про можливі інциденти та шукати можливості модернізації мережі. Нейронні мережі спиратимуться не тільки на початкову навчальну базу а й вчитимуться в процесі роботи на реальних даних та випадках поступово підвищуючи точність та ефективність. Вони зможуть надавати детальні звіти та рекомендації, що значно спрощує та підвищує ефективність управління інфраструктурою та підвищує її надійність.

РОЗДІЛ 1. ПОНЯТТЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ, ЇЇ СКЛАДОВІ, ВИДИ, ТИПИ ТА АРХІТЕРКТУРА

1.1 Поняття про корпоративну комп'ютерну мережу

Комп'ютерна мережа – це сукупність з двох чи більше взаємопов'язаних пристроїв(комп'ютери, сервери, мережеве обладнання, периферійні пристрої тощо), що можуть здійснювати обмін інформацією та спільно використовувати ресурси через канали зв'язку [1].

Корпоративна комп'ютерна мережа – це мережа, що функціонує на підприємствах або компаніях й об'єднує різноманітні пристрої та системи(див. рис. 1.1-2)[9]. Такими пристроями та системами є сервери, робочі станції, мережеве обладнання, периферійне обладнання, системи контролю доступу(СКД), системи вентиляції, пожежної безпеки тощо. Корпоративна комп'ютерна мережа може охоплювати як одну будівлю так і складатися з розосереджених географічно офісів, підприємств, об'єктів. Прикладами де використовуються такі мережі є банківські установи, навчальні заклади та наукові центри, центри обробки та зберігання даних, ігрові компанії, державні установи тощо. Кожна з цих компаній має власні потреби та вимоги до корпоративної комп'ютерної мережі в залежності від її сфери діяльності. З цього виходить, що підхід у проєктуванні та побудові корпоративних комп'ютерних мереж буде різний з використанням різноманітних технологій та архітектури.

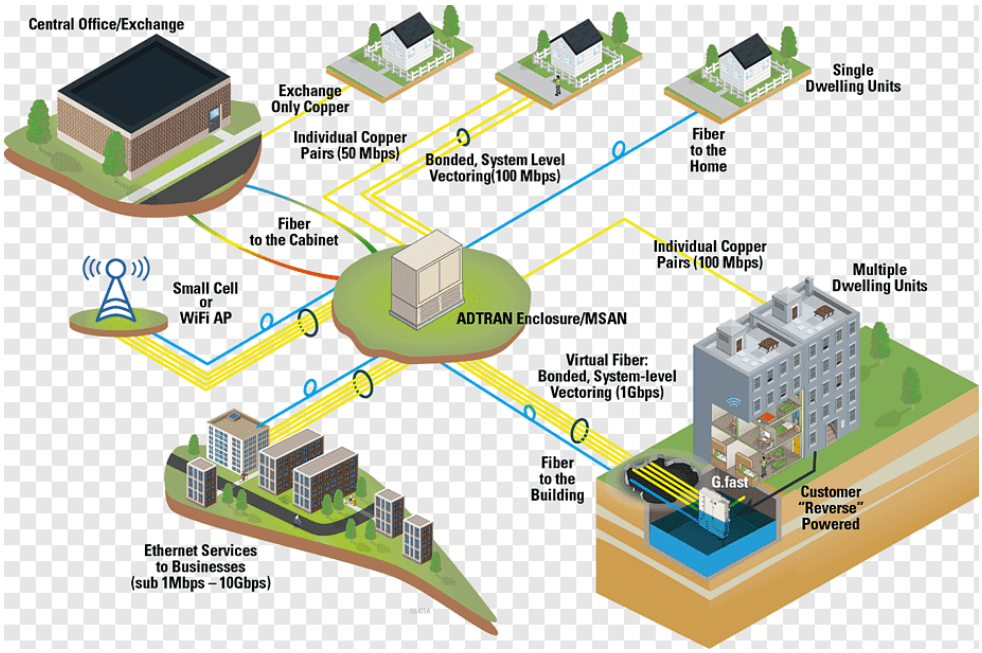


Рисунок 1.1 – Приклад корпоративної комп'ютерної мережі

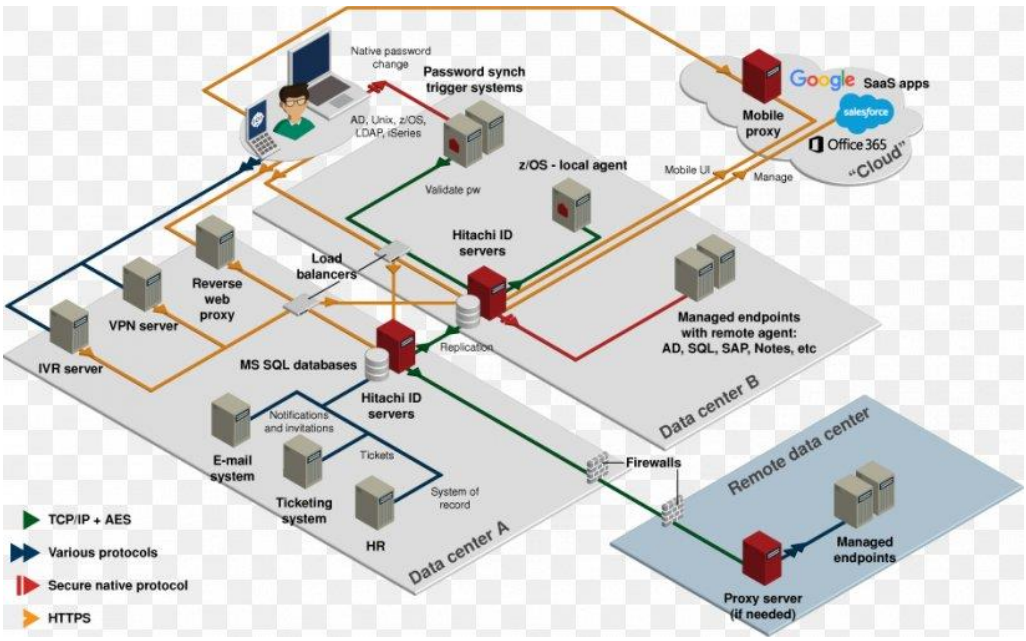


Рисунок 1.2 – Приклад корпоративної комп'ютерної мережі

Хоча конкретні вимоги до кожної мережі залежать від сфери діяльності компанії та будуть відрізнятися, проте базові вимоги залишаються однаковими[2]:

1. достатня пропускна здатність – це кількісна характеристика будь-якої мережі, яка визначає кількість даних, які мережа може передати за одиницю часу(біт/с, Мбіт/с, Гбіт/с). Це важливо аби забезпечити у корпоративній комп'ютерній мережі якісне обслуговування без затримок. Вона завжди має розраховуватися з запасом на пікове навантаження мережі.

2. надійність мережі – це здатність функціонувати безперервно з мінімальними збоями у випадках відмови частини обладнання або ліній. Надійність мережі досягається через дублювання або створення резервних каналів, резервного обладнання, резервних копій конфігурації обладнання тощо.
3. безпека мережі – це комплекс заходів, які спрямовані на захист мережі від внутрішнього та зовнішнього впливу, обмежений доступ(СКД), наявність шифрування, фаєрволів, антивірусного програмного забезпечення тощо. Обмежений доступ за допомогою СКД включатиме розмежування прав на пересування за допомогою карток доступу й створення спеціальних серверних, комутаційних кімнат та обмеженого доступу до IT відділу.
4. керованість – це наявність централізованих засобів та способів керування інфраструктурою, що включають в себе програми для моніторингу, оновлення та аналізу. Також до керованості входить наявність детальної документації, що надає розуміння інфраструктури.
5. резервування важливих даних – це комплекс заходів спрямованих на створення резервних копій документації, конфігурації обладнання, копії даних, налаштування віртуальних машин для швидкого розгортання у випадку збоїв.
6. підтримка периферійного обладнання – це можливість підключати до різноманітного обладнання в мережі такі пристрої: принтери, сканери, відео/аудіо системи, проєктори, камери, IoT пристрої тощо.

1.2 Види та типи комп’ютерних мереж

Усі комп’ютерні мережі можна класифікувати за видом та типом. Під видом комп’ютерної мережі мається на увазі класифікація за масштабом покриття та функціональним призначенням. Це дозволяє відрізняти мережі за територіальним охопленням, кількістю вузлів та використанням(див. рис. 1.3)[4,6,7].

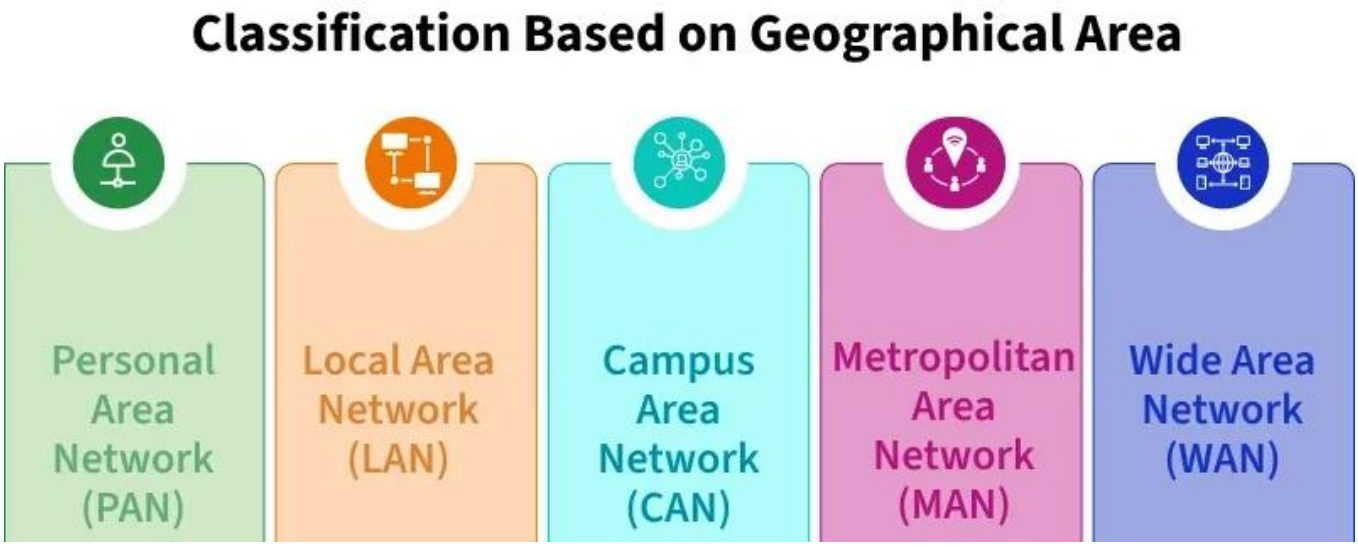


Рисунок 1.3 – Класифікація видів комп’ютерних мереж

Види комп’ютерних мереж за географічним охопленням:

1. PAN(Personal Area Network) – це персональна мережа, що має межу охоплення в декілька метрів. Використовується дана мережа для об’єднання пристроїв одної людини(смартфон, планшет, навушники, годинник, ноутбук). Для цього використовується технологія Bluetooth та радіоканал.
2. LAN(Local Area Network) – це локальна мережа в межах офісу, будинку, чи кампусу. Цей вид мережі об’єднує мінімум декілька комп’ютерів, смартфонів та периферійних пристроїв через дротове з’єднання Ethernet або Wi-Fi.
3. CAN(Campus Area Network) – це мережа, що охоплює декілька будівель, корпусів в межах університетського кампусу. Використовується у навчальних закладах та дозволяє ділитися ресурсами через дротове з’єднання Ethernet або Wi-Fi.
4. MAN(Metropolitan Area Network) – це мережа в масштабах міста, що охоплює місто або великий чіткий район. Поєднує в собі різноманітні LAN та CAN.
5. WAN – Глобальна мережа, що охоплює великі географічні території, такі як великі міста чи країни для забезпечення обміну даними між LAN на великих відстанях.

6. Intranet – це приватна мережа компанії, яка використовується для надання співробітникам безпечного доступу до внутрішніх ресурсів, сервісів та даних. За розмірами обмежена територією офісів або офісу.

Типи мереж – це класифікація за способом організації та архітектурою взаємодії вузлів. Основні типи мереж за архітектурою:

1. Однорангова(P2P)
2. Клієнт-серверна

Однорангова мережа (Peer-to-peer, P2P) – це мережа в якій кожен вузол(учасник) одночасно є клієнтом та сервером одночасно(див. рис. 1.4)[3].

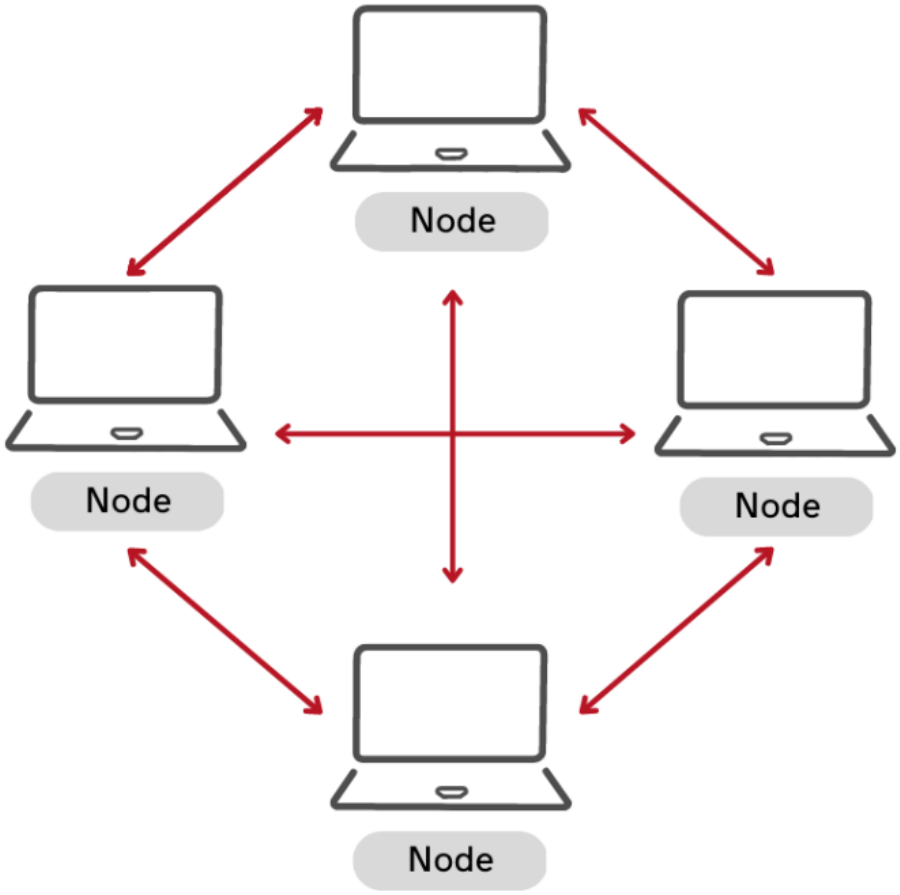


Рисунок 1.4 – Однорангова мережа (Peer-to-peer, P2P)

У такій мережі кожен вузол одночасно є отримує та надає ресурси іншим вузлам не використовуючи централізований сервер. Такий підхід забезпечує децентралізований обмін даними, що підвищує відмовостійкість оскільки немає

єдиної точки відмови. Цей тип мережі характерний для систем спільного доступу до файлів, навчальних закладів чи при проведенні досліджень.

Переваги однорангової мережі[4]:

1. Економія коштів. P2P-мережі дозволяють ефективно використовувати наявні ресурси завдяки розподіленню навантаження між усіма вузлами. Вузли надають власні ресурси, такі як пропускна здатність, сховище даних, обчислювальна потужність.
2. Відмовостійкість. P2P-мережі завдяки децентралізації уникають єдиної точки відмови. Це дозволяє підвищити стійкість та надійність мережі.
3. Спільний доступ до ресурсів. P2P-мережі забезпечують простий та швидкий доступ до мережі оскільки не потребують наявності посередників або централізованого сервера. Це означає, що зберігання даних відбувається на кожному комп’ютері та за потреби ці дані можуть бути надані іншим комп’ютерам або взяті з іншого комп’ютера.
4. Безпека. P2P-мережі можуть підвищити рівень безпеки та конфіденційності завдяки шифруванню зв’язку між ними, що у свою чергу забезпечує конфіденційність даних. До того ж відсутність центрального сервера знижує вразливість до точкових атак роблячи такі мережі більш стійкими

Недоліки однорангової мережі:

1. Відсутність централізованого керування. Відсутність централізованого керування в P2P-мережі здатне призвести до серйозних проблем в керуванні такою мережею, дотриманні встановлених політик або цілісності даних. Оскільки кожен є клієнтом та сервером одночасно то існує ризик внутрішньої диверсії або атаки, яка у свою чергу здатна призвести до пошкодження, спотворення, втрати чи витоку даних.
2. Складність управління. Оскільки вузли мають однакові ролі та обов’язки це може призвести до проблем з адресацією, безпекою чи оптимізацією продуктивності.
3. Залежність від доступності вузлів. Доступність ресурсів та сервісів в P2P-мережі залежить від активної участі кожного з вузлів. У разі виходу з ладу

великої кількості вузлів може серйозно вплинути на загальну продуктивність та доступність ресурсів та сервісів.

4. Порушення авторських прав. Даний тип мережі пов’язують також з можливим ризиком порушення авторських прав. Це може виникнути через рівні права кожного з учасників та призвести до несанкціонованого поширення контенту, захищеним авторським правом. Тож в такому випадку захист покладається тільки на самого користувача.

Клієнт-серверна мережа (client server network) – це мережа, яка забезпечує доступ до ресурсів користувачам за допомогою виділеного або виділених серверів з різними правами доступу(див. рис. 1.5)[5].

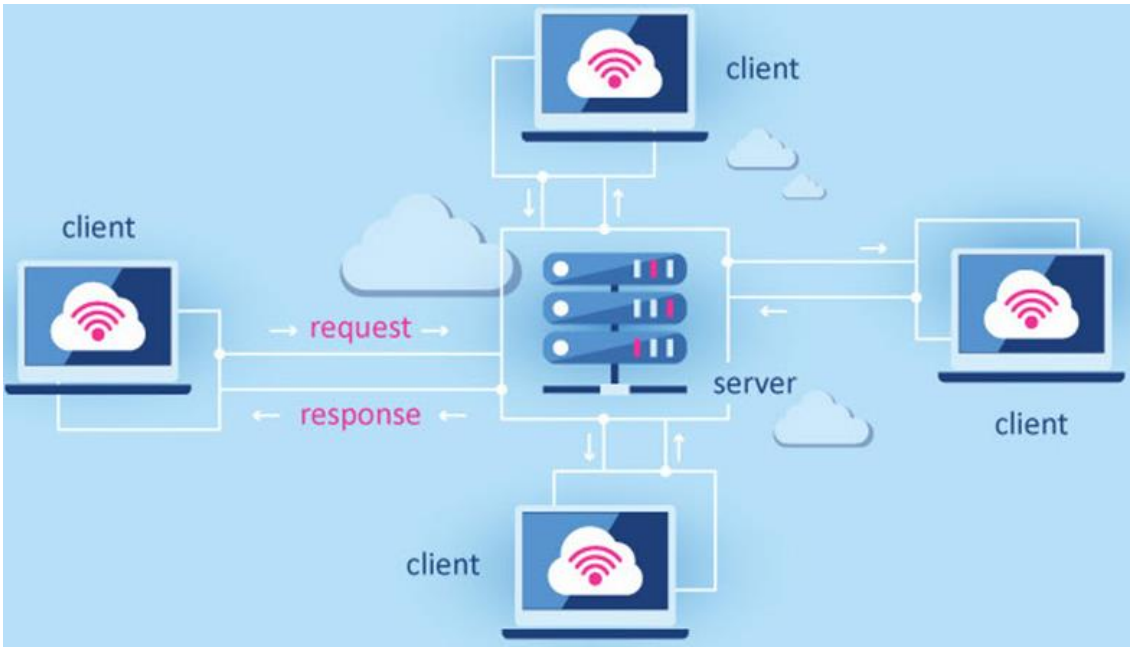


Рисунок 1.5 – Клієнт-серверна мережа (client server network)

Тобто клієнтський комп’ютер запитує доступ до певного сервісу чи пошти надаючи їм відповідну інформацію, а сервер після аналізу запиту надає або відхиляє його. Вона активно використовується веб-сайтами, поштовими серверами або платформах хмарного доступу. В цій мережі учасники поділяються на два ролі:

1. Клієнт – це будь-який пристрій або програмне забезпечення(ПЗ), яке ініціює зв’язок, запитуючи дані або послуги від сервера.

2. Сервер – це потужна обчислювальна система на якій розгортаються сервіси та зберігаються дані. Вони обробляють великий обсяг запитів одночасно дозволяючи користувачам отримати інформацію або послуги.

Переваги клієнт-серверної мережі[6]:

1. Централізоване управління даними. Завдяки визначеним ролям в мережі є пристрій до якого усі звертаються за послугами чи даними. Також оскільки ресурси зосереджуються на одному або на декількох серверах, що дозволяє простіше керувати цими ресурсами.
2. Безпека. Завдяки централізованим політикам безпеки та процедурі автентифікації на одному сервері забезпечується захист від несанкціонованого доступу мережі та її ресурсів.
3. Відновлення даних. Оскільки дані зосереджуються на одному або декількох серверах це спрощує систему резервування даних.
4. Економічна доцільність. Через зосередження основних обчислювальних потужностей на серверах користувачам необхідно менш потужна техніка для роботи.

Недоліки клієнт серверної мережі:

1. Вразливість користувачів. Якщо сервер буде заражено шкідливим ПЗ то існує ризик зараження користувачів в цій мережі.
2. Серверна інфраструктура, як ціль. В таких мережах сервери є головною ціллю різноманітних атак й їх захист потребує додаткових зусиль та ресурсів.
3. Вартість. Клієнт-серверні мережі можуть бути дорогими при впровадженні та експлуатації.

За технологією передачі даних мережі розрізняють на 3 типи:

1. Дротові мережі
2. Бездротові мережі
3. Гібридні мережі

Дротові мережі – це мережі, що використовують лише фізичні канали зв’язку(мідні кабелі, оптоволоконні лінії). Це з’єднання забезпечує високу пропускну здатність але потребує коштів на прокладання кабелів.

Бездротові мережі – це мережі, що використовують радіотехнології. До таких технологій належать: Wi-Fi, LTE, 5G, Bluetooth та інші. Вони забезпечують мобільність та більше зручності для користувачів. Однак такі мережі є вразливими до природних перешкод, накладання радіохвиль або навмисному глушінню сигналу засобами РЕБ.

1.3 Топології мереж та трирівнева модель

Корпоративні комп'ютерні мережі різняться не тільки за масштабом, типом з'єднання або типом мережі, а й за типом побудови, що визначає взаємодію компонентів всередині мережі та політики безпеки, доступу. Тож важливими її складовими є топологія мережі та трирівнева модель, які закладають основу логічної та фізичної структури. Розуміння цих аспектів надає змогу IT-спеціалістам правильно проєктувати мережу й підтримувати. У контексті системи моніторингу це є важливими даними, оскільки без розуміння топології та моделі мережі IT-спеціалісти не матимуть змоги правильно інтерпретувати та налаштовувати моніторинг.

Топологія мережі – це структурна схема мережі, що представлена у вигляді фізичної та логічної топологій[7]. Вона визначає місце розташування обладнання та логічні зв'язки між ними.

Логічна топологія – це схема, що описує логіку з'єднань між різними вузлами в мережі не акцентуючи увагу на їх безпосередньому розташуванні(див. рис. 1.6).

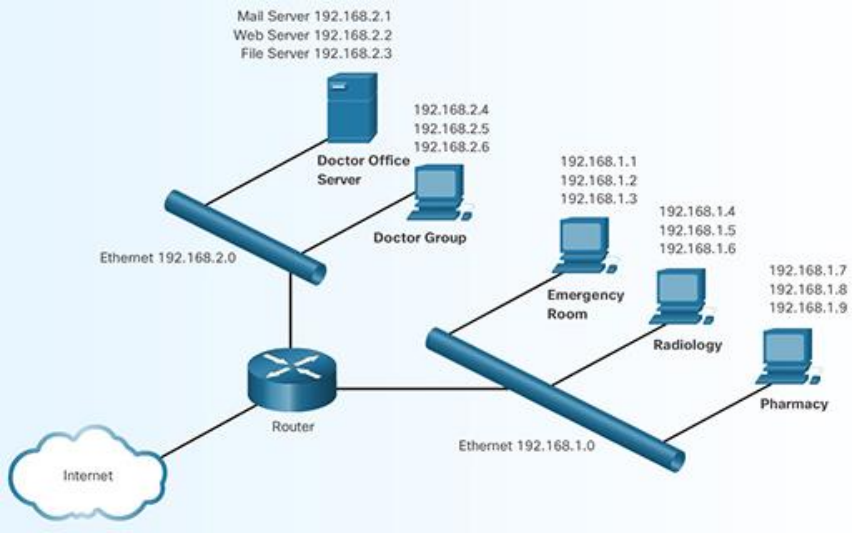


Рисунок 1.6 – Логічна топологія мережі

Фізична топологія – це схема, що описує розташування кожного вузла та компоненту мережі додаючи також інформацію про їх підключення(див. рис. 1.7).

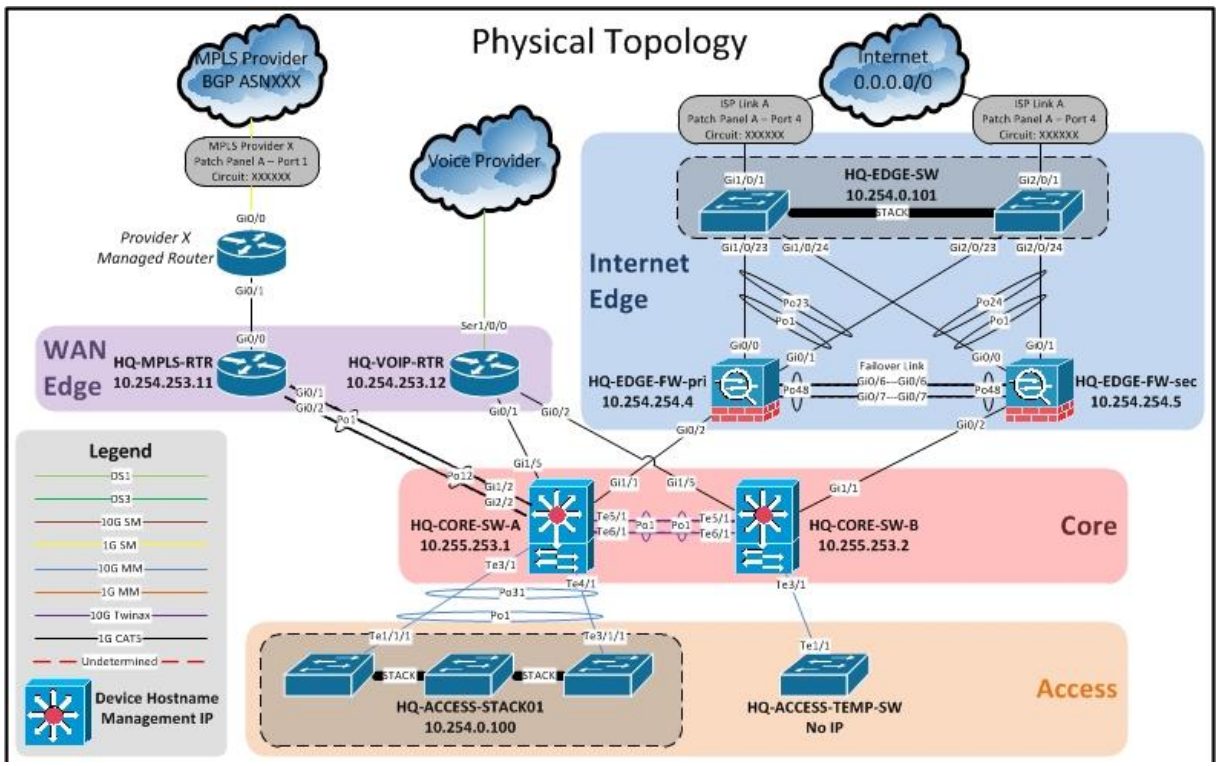


Рисунок 1.7 – Логічна топологія мережі

Дана топологія показує, як той чи інший пристрій в мережі взаємодіє та які канали використовує. На ній відображаються пропускні спроможності кожного каналу, порти, що задіяні в транспортуванні даних, агрегація, стеки, тощо.

Окрім представлення мережі через її топологію використовують трирівневу ієрархічну модель, яка чітко розділяє ролі та використовується при проєктуванні мережі та її побудови. Дана трирівнева ієрархічна модель має в собі три рівні (див. рис. 1.8)[8]:

1. Рівень доступу(Access layer).
2. Рівень розподілу(Distribution layer).
3. Рівень ядра(Core layer).

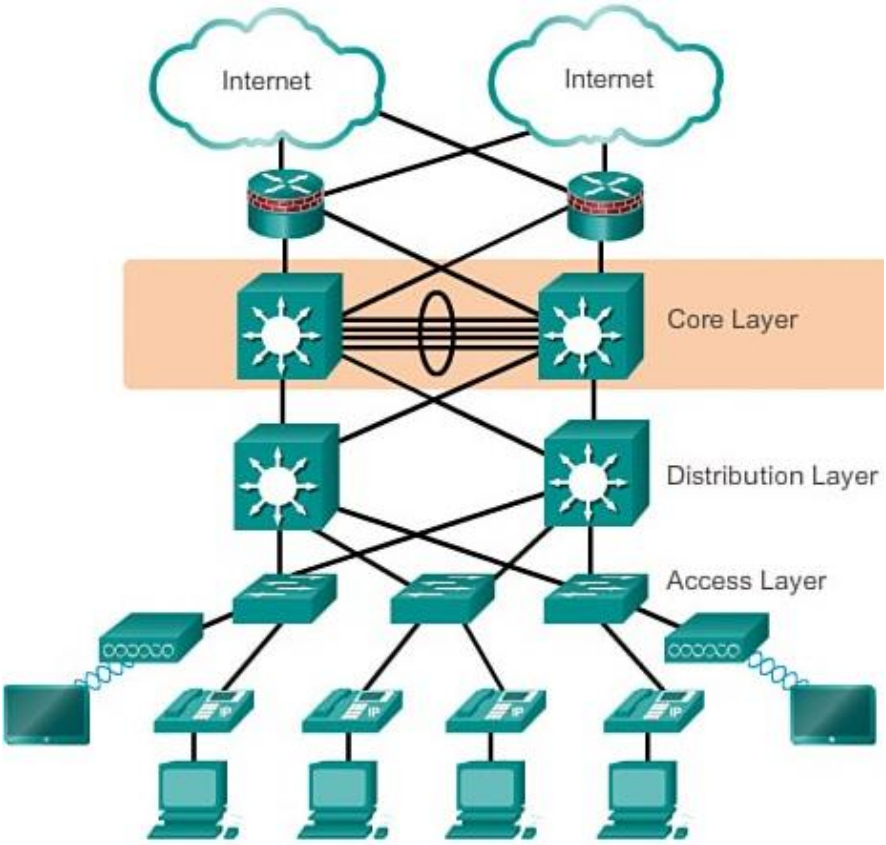


Рисунок 1.8 – Трирівнева ієрархічна модель мережі

Рівень доступу (Access layer)(див. рис. 1.9). забезпечує початкове підключення кінцевих пристроїв до мережі. На цьому рівні розташовані комутатори доступу, які забезпечують комутацію на 2 рівні та налаштовуються різні служби з політиками безпеки. Основні функції рівня доступу:

1. Підключення різних типів кінцевих пристроїв до локальної мережі.
2. Забезпечення комутації другого рівня та впровадження різних послуг комутації другого рівня, таких як Spanning Tree, віртуальний контроль доступу, QoS, PoE та ARP.
3. Запобігання підключенню неавторизованих пристроїв до локальної мережі шляхом застосування різних політик безпеки, таких як безпека портів, відстеження DHCP та конфігурація статичної MAC-адреси.

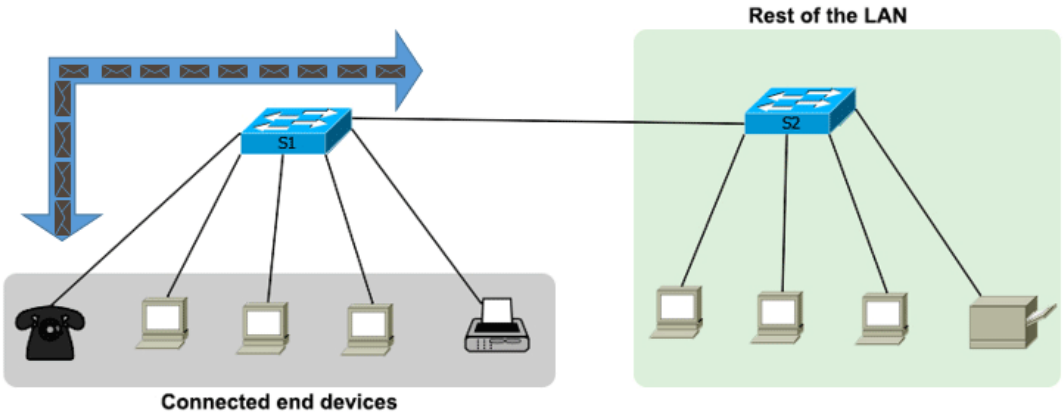


Рисунок 1.9 – Рівень доступу (Access layer)

Рівень розподілу (Distribution layer) (див. рис. 1.10) забезпечують з'єднання між комутаторами доступу та рівнем ядра. Основні функції комутаторів розподільчого рівня:

1. Забезпечення зв'язку між комутаторами доступу та рівнем ядра.
2. Контроль та фільтрація трафіку шляхом впровадження ACL.
3. Забезпечення балансування навантаження та резервування.
4. Надання послуг маршрутизації між різними VLAN.

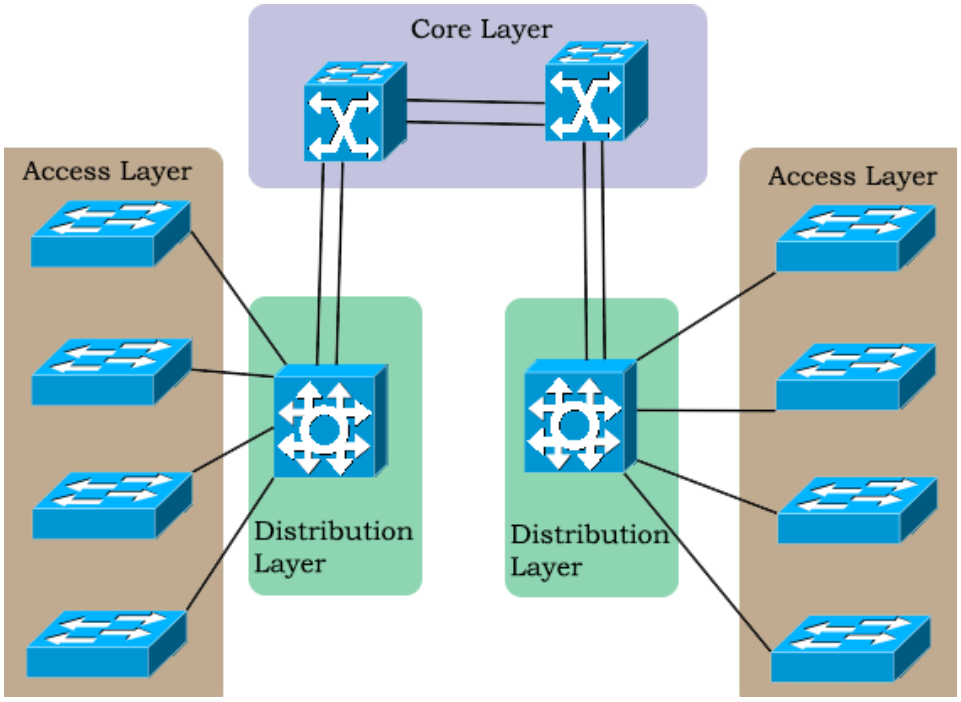


Рисунок 1.10 – Рівень розподілу(Distribution layer)

Рівень ядра (Core layer) (див. рис. 1.11) представляє собою високо швидкісний магістральний рівень, який з'єднує між собою комутатори розподілу.

У складних та великих мережах комутатори ядра зменшують потреби в кабелях та перемикають порти дозволяючи всім пристроям надсилати дані всім іншим пристроям у локальній мережі та забезпечуючи вихід в інтернет.

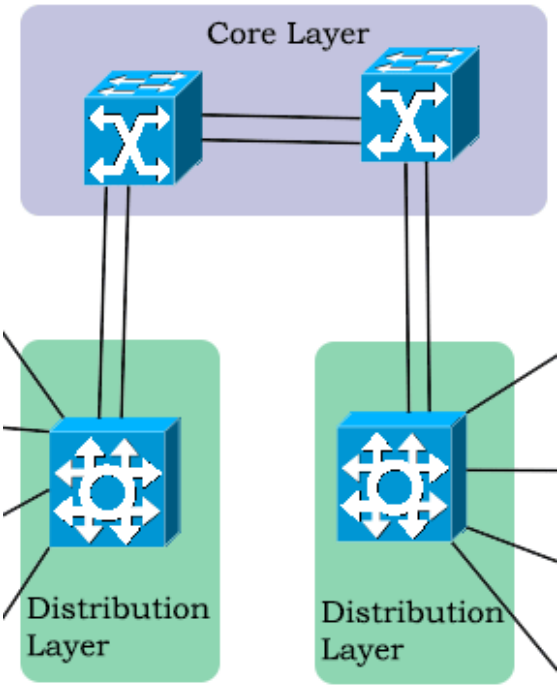


Рисунок 1.11 – Рівень ядра(Core layer).

1.4 Роль та використання віртуалізації, хмарних технологій та хмарних обчислень

Віртуалізація – це технологія, яка дає змогу одночасно запускати декілька віртуальних машин використовуючи лише один фізичний комп’ютер чи сервер[9]. Це дозволяє ефективніше використовувати обчислювальні ресурси та забезпечувати одночасну роботу декількох різних операційних систем(ОС) на одному пристрої. Сьогодні віртуалізація широко використовується різноманітними компаніями, закладами освіти та користувачами для забезпечення роботи різних відділів, тестування, розробки програмного забезпечення, навчання чи експериментів(див. рис. 1.12).

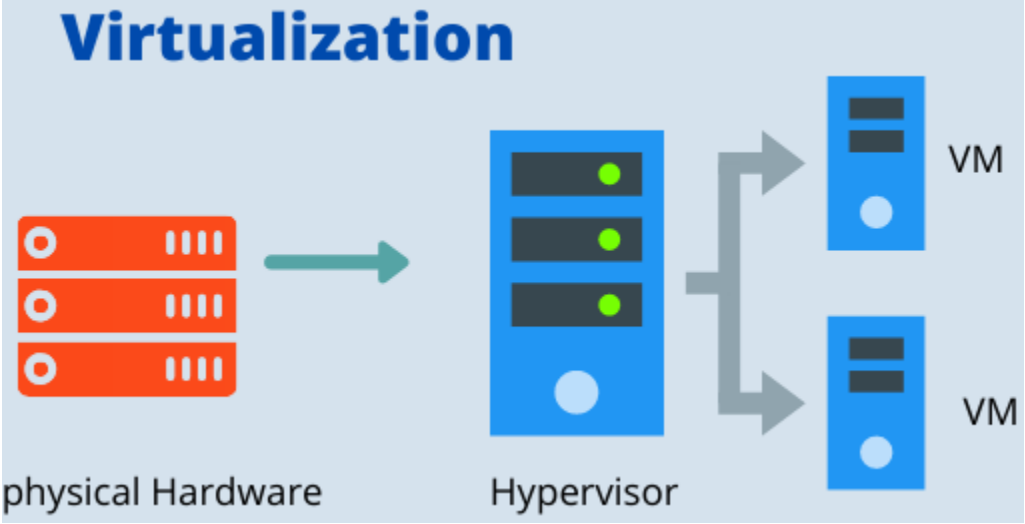


Рисунок 1.12 – Приклад віртуалізації

Сьогодні віртуалізація широко використовується різноманітними компаніями, закладами освіти та користувачами для забезпечення роботи різних відділів, тестування, розробки програмного забезпечення, навчання чи експериментів. Віртуальна машина – це програмне забезпечення, яке здатне імітувати роботу реального комп'ютера, дозволяючи запускати різні операційні системи та програми ізольовано від хоста. Вона виконує функції справжнього комп'ютера та використовує процесор, диск, мережу, хоча фізично вони не існують. Програмами, що дозволяють створювати та використовувати віртуальні машини називаються гіпервізорами та поділяються на 2 типи.

Гіпервізор (Virtual Machine Monitor) – це програмне забезпечення за допомогою якого створюються, запускаються та керуються віртуальні машини[10]. Він дозволяє одному головному комп'ютеру підтримувати декілька гостьових віртуальних машин(ВМ), що розгорнуті на ньому, виділяючи їм конкретні обчислювальні потужності або забезпечуючи динамічне виділення ресурсів у разі потреби. Тобто, якщо ВМ1 не використовує повністю в даний момент часу виділені їй ресурси то ВМ2 може використати їх для себе. Це дозволяє забезпечити максимальну ефективність віртуальній машині та уникнути простою ресурсів. Розглянемо тепер типи гіпервізорів (див. рис. 1.13).

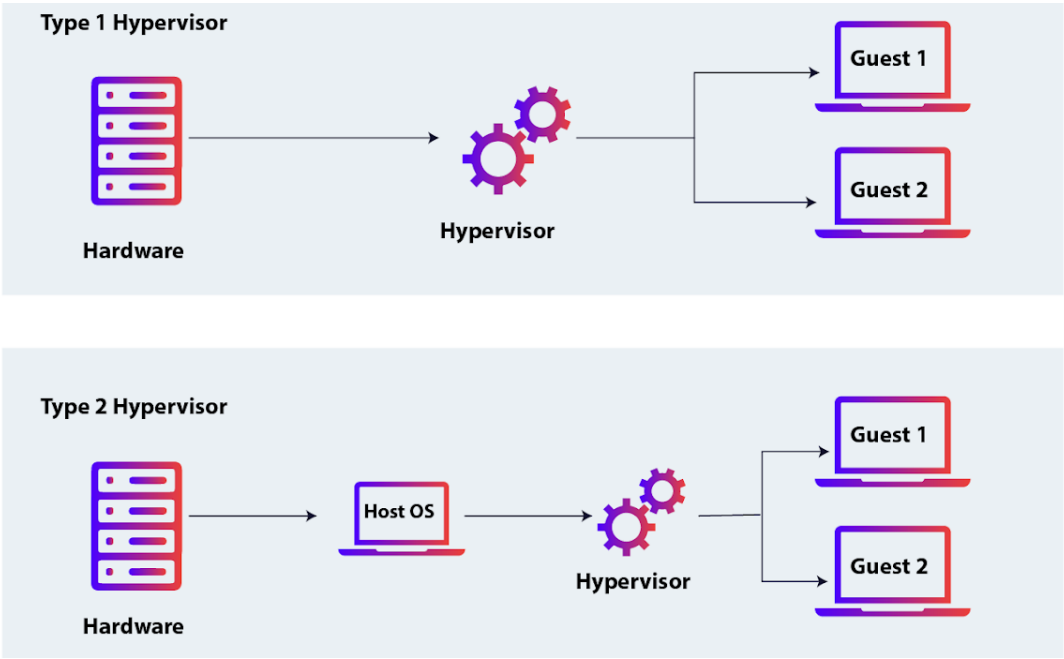


Рисунок 1.13 – Типи гіпервізора

Гіпервізор першого типу – це програмне забезпечення, що встановлюється на комп'ютер чи сервер замість операційної системи, надає більшу продуктивність та контроль над ресурсами за рахунок наявності одної операційної системи на комп'ютері чи сервері[11]. Він використовується для центрів обробки даних, хмарних провайдерів, ферм з віртуальних машин, або за потреби розгортати декілька віртуальних серверів на одному фізичному сервері. Прикладами таких гіпервізорів є: VMware ESXi, Microsoft Hyper-V та KVM.

Переваги гіпервізора першого типу:

1. Висока продуктивність. Мають прямий доступ до фізичного обладнання.
2. Підвищена безпека. Відсутність проміжного шару операційної системи, що робить її менш уразливими до атак.
3. Гнучкість. Відокремлення операційної системи від фізичного обладнання, що робить їх більш гнучкими та дозволяє мігрувати віртуальні машини між різними серверами.

Недоліки гіпервізора першого типу:

1. Потреба в окремому засобі управління. Для керування може знадобитися окремий сервер та програмне забезпечення.

2. Складність налаштування. На початковому етапі налаштувавання може бути складнішим ніж в порівняні з гіпервізорами другого типу.

Гіпервізор другого типу – це програмне забезпечення, що встановлюється на наявну операційну систему[12]. Цей тип гіпервізора зазвичай використовується для віртуалізації робочих столів, розробки чи тестування де користувачу потрібно використовувати декілька ОС на своєму персональному або лабораторному комп'ютері. Також цей тип гіпервізора можна використовувати в якості навчальних цілей в лабораторіях або дослідженнях. Продуктивність буде нижчою через використання частини ресурсів базовою операційною системою, що знаходиться між апаратною складовою та гіпервізором проте достатньою для навчальних цілей. Прикладами гіпервізорів другого типу є: Oracle VM VirtualBox, VMware Workstation та Parallels Desktop.

Переваги гіпервізора другого типу:

1. Легко встановлюється та використовується.
2. Корисно для розробки, тестування та аналізу шкідливих програм.
3. Забезпечує хороші функції інтеграції хост-гість.

Недоліки гіпервізора другого типу:

1. Повільніша продуктивність. Гіпервізор другого типу не має прямого доступу до обладнання та частина апаратних ресурсів зайнята операційною системою.
2. Безпека. Безпека віртуальних машин залежить від безпеки базової операційної системи. Компрометація хоста може вплинути на гостьові системи.

Також варто додати, що віртуалізація не обмежується лише створенням віртуальних серверів чи персональних робочих місць на сервері або комп'ютері. Для роботи мережі також використовують мережеву віртуалізацію де можна розгорнути віртуальні маршрутизатори або комутатори[13]. Також існує віртуалізація сховищ, яка досягається за рахунок об'єднання фізичних носіїв в однин віртуальний пул, що дозволяє оптимізувати місце, гнучко розподіляти ресурси та забезпечувати відмовостійкість й резервування даних.

Окрім того в архітектурі мережі та її побудові застосовуються хмарні технології. Хмарні технології – це модель надання обчислювальних ресурсів через глобальну мережу інтернет з оплатою лише за фактичне використання (див. рис. 1.14).



Рисунок 1.14 – Хмарні технології

Основна ідея полягає у тому, що компанія чи користувач не має потреби купувати та обслуговувати серверне обладнання, а орендує ці ресурси в хмарного провайдера за встановленою платою. Замість них це робить хмарний провайдер, який займається підтримкою та розширенням цієї інфраструктури, щоб надавати її в користування іншим компаніям. Це дозволяє бізнесу та звичайним користувачам економити кошти на дороге обладнання та спеціалістів для забезпечення його роботи. Такий підхід дозволяє отримати доступ компанії або користувачу доступ до ресурсів з будь-якої точки світу маючи інтернет. Хмарні технології поділяються на три моделі в залежності від рівня послуг та сервісу, що необхідно надати. Такими моделями є: IaaS, PaaS, SaaS[14]. Кожна з моделей має різний рівень контролю та управління, що надається користувачам (див. рис. 1.15).

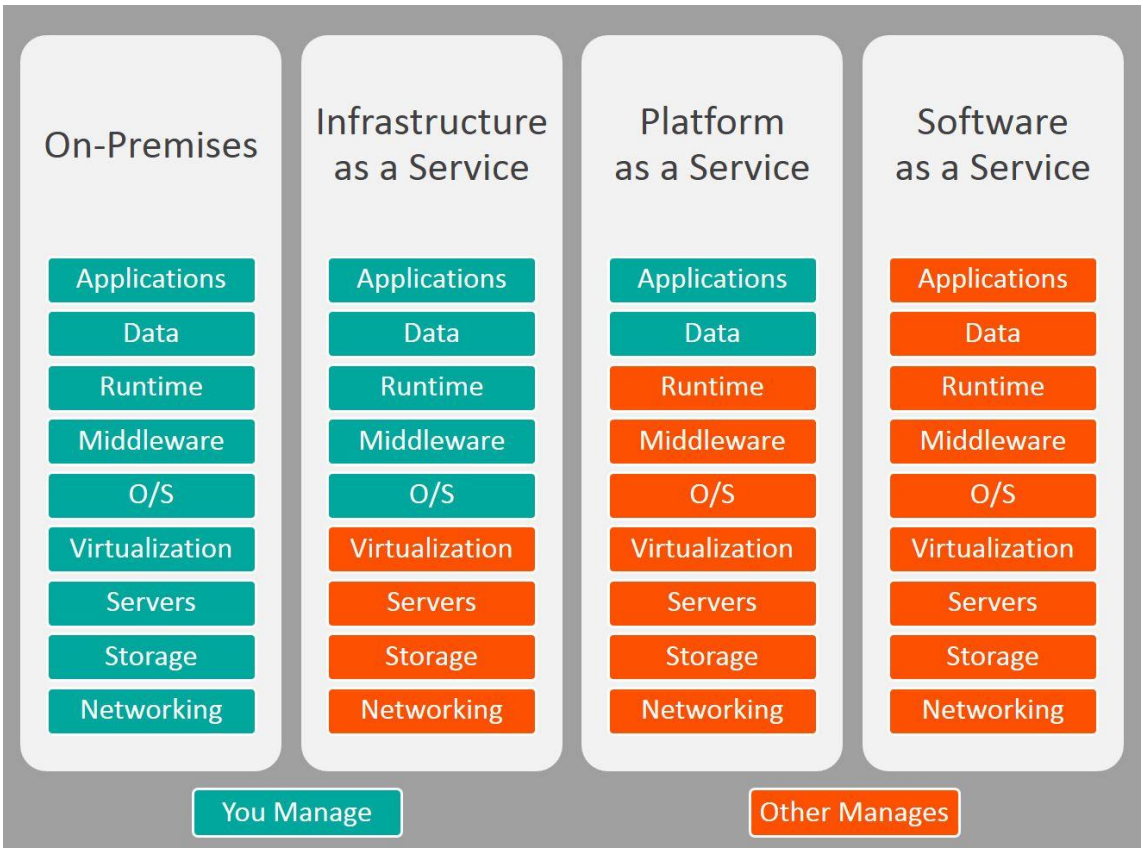


Рисунок 1.15 – Хмарні технології PaaS, SaaS, IaaS

IaaS (Infrastructure as a Service) – це модель надання провайдером користувачу обчислювальних ресурсів для його потреб. В ці ресурси входять: віртуальні сервери, мережі та сховища даних для розгортання користувачем власного програмного забезпечення. В цій моделі апаратною складовою займається провайдер. Він займається встановленням програмного забезпечення(ПЗ) для створення віртуальних машин але не займається установкою та підтримкою програмного забезпечення користувача. Компанії, що надають такі послуги: IBM Softlayer, Hetzner Cloud, Microsoft Azure, Amazon EC2, GigaCloud. Дана модель підходить для розміщення веб-сайтів, корпоративних застосунків, баз даних, навчальних або тестових середовищ, резервного копіювання або аварійного відновлення.

Переваги IaaS:

1. Можливість швидко розгорнути сервіси бізнесу.
2. Економія коштів на розгортання та підтримку власної інфраструктури.
3. Відповідальність за стабільну роботу інфраструктури несе провайдер.

4. Гнучкість при навантаженні, оскільки потрібно тільки доплатити за додаткову потужність без витрачення часу на її розгортання.

Недоліки IaaS:

1. Обмежені можливості керування інфраструктурою клієнту, оскільки він не має доступу ні до апаратної частини ні до гіпервізору.
2. Немає повноти вибору обладнання з специфічними характеристиками.

SaaS (Software as a Service) – це модель надання провайдером користувачу програмного забезпечення як сервісу. Програми та сервіси розробляються та обслуговується провайдером, що розміщує їх в хмарі та надає користувачу через програму або браузер. В цій моделі користувач вносить лише абонплату за користування сервісом. Прикладами таких сервісів є: Dropbox, Google Doc, Microsoft Office 365, Zoom тощо.

Переваги SaaS:

1. SaaS є простою та зручною для кінцевого користувача моделлю хмарних полслуг.
2. Забезпечення працездатності хмарного сервісу лежить повність на провайдері.
3. Підгодить для малого та середнього бізнесу, який у 99% випадків має вирішувати типові IT-завдання.
4. Економія на оплаті за послуги розробників, мережевих інженерів та системних адміністраторів.

Недоліки SaaS:

1. Обмежені можливості для кастомізації та інтеграції з стороннім програмним забезпеченням.
2. Доступний лише перелік функцій, що закладені розробником.
3. Відповідальність за безпеку покладається на провайдера.

PaaS (Platform as a Service) – це модель надання провайдером користувачу доступу да операційних систем, засобів розробки, тестування, систем управління базами даних. В цій моделі провайдер контролює не тільки сервери, системи зберігання даних і обчислювальні потужності. Користувач зосереджується тільки

на розробці та керуванні даними й додатками але не турбується про інфраструктуру. Приклади PaaS: Google App Engine, IBM Bluemix, Microsoft Azure, VMWare Cloud Foundry. Здебільшого PaaS використовують розробники.

Переваги PaaS:

1. За розробку, оновлення, виправлення та підтримку працездатності інструментів на платформі відповідальний провайдер.
2. Клієнт заощаджує на розробці та конфігуруванні програмного забезпечення та може швидко почати використовувати необхідні інструменти.
3. Доступні на платформі засоби для розробників легко комбінуються в залежності від потреб клієнта.

Недоліки PaaS:

1. Клієнт не може масштабувати свою IT-інфраструктуру у разі потреби.
2. Клієнт не має глобального впливу на конфігурацію виділених у хмарі ресурсів.

Віртуалізація та хмарні технології є невід'ємною складовою сучасних корпоративних комп'ютерних мереж. Використання гіпервізорів дозволяє розгортати віртуальні середовища, оптимізуючи використання апаратних ресурсів. Моделі IaaS, PaaS, SaaS надають організаціям та користувачам можливості орендувати середовище розробки, інфраструктури чи вже готовий продукт для власних потреб економлячи кошти й час на розгортанні власної інфраструктури та сервісів.

РОЗДІЛ 2. СИСТЕМИ МОНІТОРНГУ КОМП'ЮТЕРНИХ МЕРЕЖ, ЇХ МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

2.1 Що таке система моніторингу комп'ютерної мережі?

У сучасних корпоративних мережах безперервне спостереження за станом та продуктивністю є критично важливим. Забезпечуються це системами моніторингу для комп'ютерних мереж, що забезпечують моніторинг та спостережуваність.

Моніторинг мережі – це використання програмно апаратного забезпечення для цілодобового контролю стану та надійності комп'ютерної мережі[15].

Спостережуваність (observability) – це здатність системи аналізувати внутрішній стан та надання контексту подій, що дозволяє зробити висновки та знайти в чому першопричина.

Система моніторингу комп'ютерної мережі – це програмне або програмно-апаратне рішення, що безперервно відстежує стан, продуктивність, завантаженість та безпеку комп'ютерної мережі. Головним завданням системи моніторингу комп'ютерної мережі, є допомога системним адміністраторам слідкувати за станом мережі, виявляти проблеми, аномалії, та потенційні загрози для забезпечення безперебійної роботи мережевої інфраструктури й вчасного виявлення помилок чи збоїв. Системи моніторингу здатні забезпечити зручний вивід зібраних та проаналізованих даних у вигляді діаграм, таблиць повідомлень тощо. Вона забезпечує контроль за інфраструктурою незалежно від того, чи вся інфраструктура знаходиться у компанії локально, чи вони знаходяться в центрах обробки даних(ЦОД), чи використовується хмарними провайдерами, що надають ресурси в оренду, або використовується гібридна інфраструктура коли частина ресурсів знаходиться в компанії, а частина ресурсів в ЦОД, хмарного провайдера або в іншому місті. Система моніторингу комп'ютерної мережі збирає дані в режимі реального часу, аналізують потік трафіку, вимірюють продуктивність та стан вузьких місць в мережі відповідно до налаштованих порогових значень. Коли виникає аномальна поведінка, наближення до порогових значень або їх перевищення система сповіщає про проблему чи помилку через систему миттєвих сповіщень та підсвічує на графічному екрані куди виведені усі необхідні показники.

Моніторинг та спостережуваність мережі є необхідними компонентами для обслуговування інфраструктури компанії, оскільки дозволяють підтримувати та забезпечувати стабільну роботу комп'ютерної мережі компанії. Відсутність цих

компонентів призвела б до проблем та збоїв в роботі мережі, погіршення якості обслуговування, відмови обслуговування, втрати репутації та клієнтів.

Основні задачі моніторингу мережі:

1. Збір та обробка інформації. Система постійно опитує пристрої або отримує від них повідомлення, зберігає метрики в базі даних та відфільтровує некоректні значення.
2. Моніторинг та контроль продуктивності й стану обладнання. Вимірюються завантаження процесора, використання пам’яті, пропускна здатність, затримки, втрати пакетів, наявність переривань чи помилок.
3. Виявлення відмов та аномалій. За допомогою порогових значень та статистичних моделей система визначає, коли певний показник вийшов за межі норми, і оповіщає адміністратора.

Основні компоненти спостережуваності:

1. Логи. Це текстові записи подій, які мають детальний опис та фіксують деталі роботи систем та можуть містити корисну інформацію для діагностики.
2. Метрики. Це числові показники, що характеризують та відображають стан або продуктивність системи (наприклад, CPU util, пропускна здатність, кількість з’єднань)
3. Трасування. Це відстеження шляху виконання запитів через різні компоненти системи. Це особливо важливо у мікросервісних архітектурах та розподілених системах, де без трасування неможливо визначити, де саме виникло «вузьке місце».

Вузьке місце (Bottle neck) – це найслабше та вразливе місце в системі. Наприклад в комп’ютері, якщо комп’ютеру не вистачає оперативної пам’яті для роботи, то його продуктивність падає або він перестає працювати. Тобто нестача оперативної пам’яті є слабким місцем у комп’ютера. В мережі це може виражатися в недостатній пропускній здатності каналу через що не весь об’єм трафіку виходить пропустити та це призводить до затримок та перевантаження каналу (див. рис. 2.1).

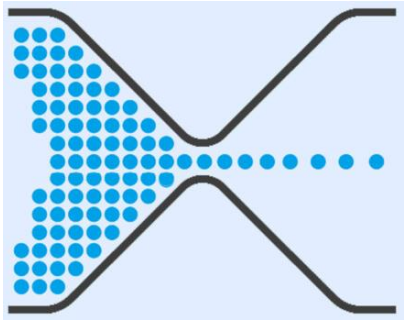


Рисунок 2.1 – Вузьке місце(Bottle neck) в пропускній здатності каналу

Сьогодні існує багато різноманітних рішень для моніторингу та спостережуваності комп'ютерних мереж. Ці рішення відрізняються своїм функціоналом, вартістю, підтримкою та складністю налаштування. Вони поділяються на open–source рішення та комерційні пропозиції. До open–source рішень відносяться: Nagios Core, Zabbix, Icinga, Cacti, Prometheus, а до комерційних пропозицій відносяться SolarWinds Network Performance Monitor, PRTG Network Monitor, Datadog, LogicMonitor та ManageEngine OpManager. Варто зазначити, що деякі open-source рішення є безкоштовними лише у базовій версії й подальша їх підтримка та розширений функціонал будуть потребувати купівлі ліцензії.

2.2 Принципи роботи систем моніторингу комп'ютерних мереж.

Для отримання інформації про стан обладнання системи моніторингу використовують різні способи збору даних. Найбільш популярною в системах є модель менеджер-агент. Агент – це програма чи модуль, який збирає дані з керованого обладнання (маршрутизаторів, комутаторів, точок доступу, віртуальних машин тощо) і передають їх менеджеру. Менеджер – це сервер, який приймає та обробляє дані від агентів. Також для збору інформації використовуються протоколи інтернет-протоколи для отримання даних про доступність або навантаження обладнання. Метрики – це числові показники, що відображають стан або продуктивність мережі. Основні метрики, що збираються системами моніторингу:

1. **Продуктивність пристроїв**. Збираються дані про завантаженість CPU та GPU, температури, завантаженість оперативної пам'яті, робота накопичувачів, пропускна здатність інтерфейсів, кількість та типи помилок тощо.
2. **Статус обладнання**. Збираються дані про доступність обладнання, активні інтерфейси.
3. **Мережевий трафік та якість обслуговування**. Кількість вхідних та вихідних пакетів даних, затримки, втрата пакетів, рівень використання каналів зв'язку.
4. **Апаратні датчики**. Дані про температури CPU, GPU, жорстких дисків або SSD, продуктивність роботи системи охолодження тощо. Це дозволяє відстежувати стан обладнання.
5. **Інтернет-протоколи**. Крім згаданого SNMP, поширені WMI (Windows Management Instrumentation) для систем Windows, SSH/CLI для Unix-пристроїв, IPMI (для апаратних сенсорів серверів) та HTTP(S)/REST–API для сервісів і хмарних платформ. Деякі системи використовують NetFlow/sFlow для аналізу потоків трафіку, а Syslog для збору журналів подій. Нові

технології, такі як streaming telemetry, транслюють дані безпосередньо із пристроїв у реальному часі, зменшуючи затримки та обсяг опитувань.

Агентний та без агентний методи

Вибір способу збору даних залежить від конкретних вимог організації до системи моніторингу та специфіки обладнання, що використовується. Моніторинг за допомогою агента передбачає інсталювання програми–агента на кожен керований вузол. Це забезпечує доступ до розширених метрик (детальна інформація про процеси, локальні логи, дані про пристрій тощо) та стійкість до тимчасових мережевих відмов, оскільки агент здатен кешувати дані і передати й пізніше. Недоліком є необхідність встановлення та оновлення агентів на всіх пристроях. Що на початковому етапі може ускладнювати налаштування та споживає певну кількість ресурсів. Без агентний метод моніторингу передбачає використання стандартних інтернет-протоколів (SNMP, WMI, HTTP/S, ICMP, IPMI), не потребуючи встановлення додаткового ПЗ на пристроях. Перевага такого підходу в розгортанні та сумісності із великою кількістю пристроїв, що є в мережі. Однак недоліком такого підходу є доступність лише тих метрик, які дозволені протоколами й ці протоколи не є забороненими всередині системи, проте це потребує постійного мережевого з’єднання.

Сенсори та тригери

Деякі системи можуть використовувати спеціальні сенсори (датчики) для специфічних завдань. Наприклад, для VPN–моніторингу SNMP–сенсори збирають дані про кількість користувачів, активні тунелі, обсяг трафіку і можуть попереджати про перевищення порогу. Аналогічно, датчики температури чи напруги дозволяють відстежувати апаратні параметри серверів.

Тригери — це автоматизована дія, що має логічні умови, при спрацьовуванні яких система створює події (alerts) та сповіщає використовуючи систему оповіщення. Для кожної метрики встановлюються порогові значення, щоб тригери коректно відпрацьовували. Наприклад коли показник завантаження або температури досягає граничного рівня CPU busy > 80 % або температура > 70 °C, активується тригер, і система надсилає сповіщення адміністраторам попереджаючи про потенційну проблему або сповіщаючи про проблему, що виникла. Ці показники можуть братися за різний проміжок часу та виводитися на монітори за допомогою діаграм, графіків, системних повідомлень тощо.

Візуалізація та аналітика даних

Зібрані дані системи за допомогою описаних методів зберігаються у базі даних про систему та відображаються у вигляді графіків, таблиць і інтерактивних панелей або системних повідомлень. Це допомагає відстежувати тенденції, шукати кореляції, знаходити слабкі місця й усувати їх та планувати розширення або модернізацію

мережі. Багато рішень для систем моніторингу такі як: Zabbix, Prometheus, Grafana підтримують можливість будувати інформаційні панелі, щоб відображати в режимі реального часу стан інфраструктури. Деякі системи починають інтегрувати алгоритми машинного навчання для автоматичного виявлення аномалій, прогнозування перевантажень і оптимізації ресурсів тощо.

2.3 Огляд наявних систем моніторингу, переваги та недоліки

Сьогодні для моніторингу комп'ютерної мережі існує багато різноманітних рішень, що відрізняються за спектром надаваних послуг, підтримкою та рівнем підписки. Можна знайти як open-source рішення, так і комерційні продукти. Уніфікованого рішення на ринку немає, проте перелік доступних варіантів здатен забезпечити різноманітні потреби для різного бізнесу. Серед популярних рішень, які сьогодні активно використовуються Zabbix, Nagios Core, Prometheus, Grafana, Observium, SolarWinds Network Performance Monitor (NPM), PRTG Network Monitor, Datadog, LogicMonitor (див. рис. 2.2).



Рисунок 2.2 – Приклад загальної інформаційної панелі в Zabbix, що поєднує дані про використання CPU, карту мережі та виявленні проблеми.

Zabbix – це система моніторингу служб з відкритим кодом, що дозволяє відстежувати стан комп'ютерних мереж, серверів, хмарних сервісів та додатків[16].

Вона збирає метрики, дані про стан апаратної частини, виявляє проблеми, дозволяє візуалізувати інформацію графічно у вигляді інформаційних панелей та графіків й сповіщати системних адміністраторів про спрацювання тригерів чи помилок для своєчасного реагування на помилки та інциденти й забезпечення безперебійної роботи мережі (див. рис. 2.3).



Рисунок 2.3 – Приклад налаштованої інформаційної панелі в Zabbix

У базовій версії Zabbix йде безкоштовним програмним забезпеченням. Проте з часом коли ваша мережа потребує розширення та додаткових послуг й обслуговування вам надається додаткові послуги, які вже є платними. Для моніторингу комп'ютерної мережі Zabbix використовує два основні підходи: агентний та без агентний.

Агентний моніторинг передбачає встановлення агента безпосередньо на обладнання. Агент – це легкий застосунок, який встановлюється на обладнання для збору локальних даних. Агенти здатні збирати локальні дані, такі як стан апаратних компонентів та показники температури, навантаження тощо та надсилають їх на центральний сервер Zabbix для подальшої обробки (див. рис. 2.4).



Рисунок 2.4 – Відображення стану обладнання в Zabbix

Без агентний метод моніторингу використовуються у випадках коли встановлення агента неможливе або недоцільне (табл. 2.1). Цей підхід ґрунтується на використанні стандартних мережевих протоколів та технологій, які забезпечують отримання даних безпосередньо від обладнання чи сервісів. Цей метод спрощує розгортання та обслуговування систем, хоч може надавати менший обсяг інформації в порівнянні з агентним способом.

Таблиця 2.1

Без агентний метод роботи Zabbix

Протокол або технологія	Опис
SNMP(Simple Network Management Protocol)	Стандартний мережевий протокол, що використовується для керування та моніторингу мережевих пристроїв. Цей протокол дозволяє збирати інформацію про стан мережевих пристроїв, налаштовувати конфігурацію та отримувати сповіщення про помилки чи події.
SSH(Secure Shell)	Це мережевий протокол, який забезпечує безпечне віддалене підключення та керування пристроями й передачу даних через незахищені сегменти мережі.

Продовження таблиці 2.1

Без агентний метод роботи Zabbix

Протокол або технологія	Опис
IPMI (Intelligent Platform Manegment Interface)	Інтерфейс для автономного моніторингу та керування системою, що працює незалежно від операційної системи чи сервера. Він надає можливість керувати пристроями віддалено та отримувати з них дані про стан компонентів ПК чи сервера.
JMX (Java Management Extensions)	Технологія Java, що забезпечує контроль та керування системними застосунками, об’єктами та комп’ютерними мережами.
HTTP/HTTPS	Мережеві протоколи, що визначають правила обміну даними між клієнтом та сервером в інтернеті й забезпечують передавання даних.
API (Application Programing Interface)	Це набір правил та інструкцій, який дозволяє різним програмним додаткам взаємодіяти та обмінюватися даними між собою. Це визначає, як один додаток може запитувати інформацію чи функціонал іншого.

Завдяки поєднанню цих протоколів та технологій Zabbix здатен забезпечити комплексну картину стану інфраструктури мережі незалежно від її розташування (див. рис. 2.5).

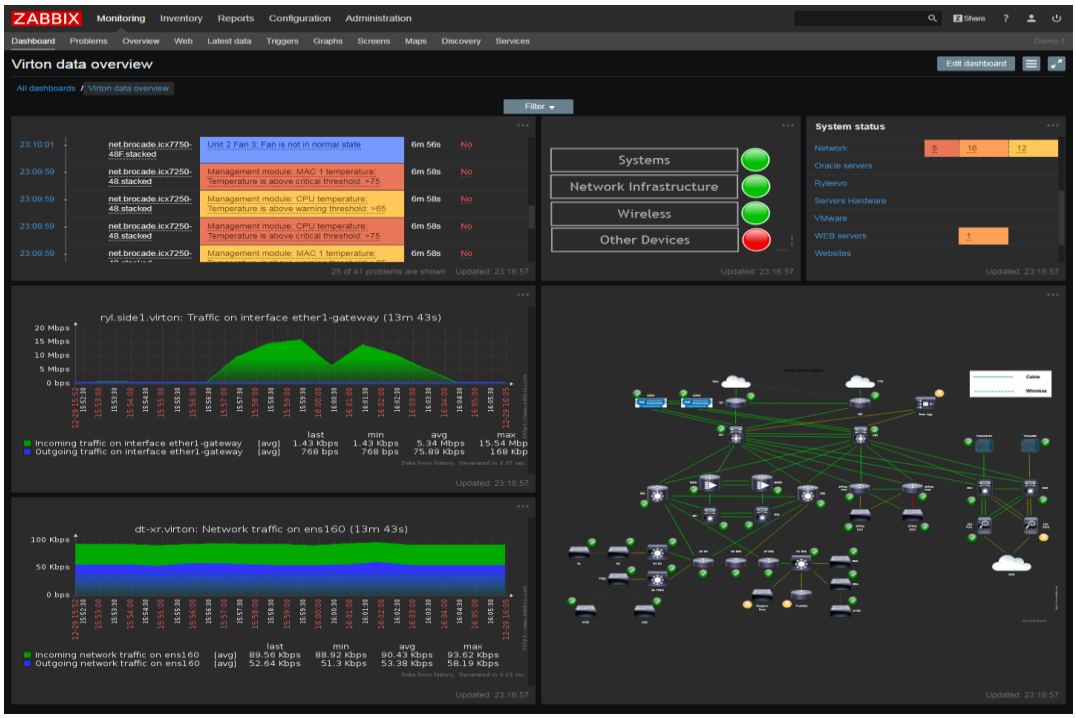


Рисунок 2.5 – Інформаційна панель Zabbix, яка показує сповіщення про стан системи, мережевий трафік з часом та детальну мапу мережі.

Це дозволяє забезпечувати її стабільну роботу та допомагає системним адміністраторам в адмініструванні мережі. Переваги та недоліки використання Zabbix розглянуто в таблиці 2.2 Переваги та недоліки Zabbix.

Таблиця 2.2

Переваги та недоліки Zabbix

Переваги	Недоліки
Безкоштовний та відкритий вихідний код (Open-Souce). Zabbix є безкоштовним програмним забезпеченням, що є вигідним для будь-якого бізнесу.	Складність початкового налаштування. Базове встановлення Zabbix не є складним, проте тонке та більш точне налаштування потребує знань та зусиль.
Універсальність та комплексність. Zabbix здатен виконувати моніторинг, як комп'ютерів, серверів, мережевого обладнання, додатків та хмарних сервісів. Це забезпечується його гнучким підходом до моніторингу використовуючи агентний метод та без агентний метод.	Навантаження на базу даних. При моніторингу великої кількості обладнання, сервісів та великої мережі Zabbix генерує значне навантаження на свою базу даних (MySQL, PostgreSQL, Oracle), що вимагає регулярного обслуговування, оптимізації та достатніх ресурсів. Це своєю чергою може викликати додаткові витрати.

Продовження таблиці 2.2

Переваги та недоліки Zabbix

Переваги	Недоліки
Система сповіщень. Zabbix має розвинуту систему оповіщень, яка дозволяє налаштувати сповіщення використовуючи різні месенджери(Webex, Slack, Telegram, email тощо.	Відсутність безкоштовної підтримки. Будучи безкоштовним продуктом Zabbix не має безкоштовної підтримки й у разі виникнення проблем доведеться покладатися на спільноту або купувати платну підписку.
Масштабованість. Zabbix здатен працювати, як у великих офісах, масштабних корпоративних середовищах з тисячами пристроїв так і в невеликих компаніях. Це робить його дуже зручним у використанні.	Залежність від продуктивності сервера. Ефективність роботи Zabbix залежить від потужностей сервера на якому він розгорнутий та його база даних.
Актуальна документація та активна спільнота. Zabbix має багато документації та постійно актуалізує її. До того ж активна спільнота користувачів Zabbix дозволяє знайти багато необхідного роблячи підтримку та використання продукту простішим та зручнішим.	

Zabbix переважно використовують для моніторингу великих корпоративних мереж і дата–центрів, де потрібно поєднати традиційні мережеві пристрої з хмарними сервісами й сервісами SaaS. Наприклад, провайдер може збирати метрики з комутаторів та маршрутизаторів через SNMP і одночасно стежити за станом віртуальних машин і баз даних через агенти або API. За допомогою шаблонів користувачі можуть швидко масово додавати однотипне обладнання (Cisco, Juniper, Huawei) та отримувати готові інформаційні панелі. Проте він також може застосовуватися і в невеликих компаніях яким потрібен моніторинг та спостережуваність.

Nagios Core – це безкоштовне програмне забезпечення для моніторингу та спостереження за комп’ютерними системами, мережами та інфраструктурою[17]. Вона контролює стан служб і ресурсів, оповіщає системних адміністраторів про збої та відновлення роботи сервісів, обладнання тощо(див. рис. 2.6)



Рисунок 2.6 – Відображення стану мережі в Nagios Core.

Для своєї роботи Nagios Core використовує агентний та без агентний режим. В без агентному режимі використовуються протоколи: SMTP, POP3, HTTP, NNTP, FTP, SSH, ICMP, SNMP тощо. Також для детального та глибокого моніторингу використовується режим агента. В цьому режимі використовуються невеликі демони або служби, що встановлюються на віддалених хостах. Для перевірки вузлів використовуються NRPE та NCPA.

NRPE (Nagios Core Remote Plugin Executor) – це агент, що дозволяє серверу Nagios Core віддалено виконувати плагіни, які знаходяться на відстежуваному хості. Сервер Nagios Core надсилає запит агенту NRPE на віддаленому хості. Агент NRPE отримує запит, запускає вказаний локальний плагін (наприклад, check disk для перевірки диска).Плагін виконує перевірку і повертає результат (код стану та дані) агенту. Агент NRPE пересилає цей результат назад на сервер Nagios Core.

NCPA (Nagios Core Cross-Platform Agent) – це сучасніший агент розроблений як кросплатформене рішення для Windows, Linux та macOS. Він забезпечує легке розгортання та уніфікований підхід до моніторингу різних операційних систем. NCPA працює як API-сервер. Замість того, щоб просто виконувати команди, він надає доступ до широкого спектру метрик через веб-інтерфейс (JSON API). Сервер Nagios Core може "запитувати" метрики (pull-модель) безпосередньо через API. Або ж агент NCPA може "надсилати" результати перевірок на Nagios Core-сервер (push-модель).

Також Nagios Core контролює ресурси хостів мережі, такі, як: навантаження CPU,GPU, використання дисків, RAM тощо (див. рис. 2.7).



Рисунок 2.7 – Інформаційна панель, що відображає стану системи в Nagios Core.

Він працює за принципом постійних перевірок регулярно запускаючи спеціальні плагіни для перевірки статусів. У випадку зміни статусу чи відхилення система генерує про це сповіщення. Nagios Core можна масштабувати оскільки він підтримує розподілений моніторинг, високодоступні конфігурації та механізми failover для серверів і плагінів. Веб–інтерфейс дозволяє переглядати поточні та історичні статуси, розклад перевірок і надає базові графіки. Сильним боком Nagios Core є розгалужена екосистема плагінів, існують тисячі готових модулів для різноманітних пристроїв, сервісів та додатків, що спрощує та робить зручніше роботу з ним. Це дозволяє адаптувати систему до майже будь–якого середовища (табл. 2.3).

Таблиця 2.3

Переваги та недоліки Nagios Core.

Переваги	Недоліки
Відкритий код та розвинута спільнота користувачів. Nagios Core має розвинену спільноту користувачів, що може полегшити процес виправлення помилок або налаштування та є безкоштовним продуктом у базових версіях, що дозволяє знизити витрати.	Інтерфейс користувача є застарілим в порівнянні з іншими системами, що може бути незручно.

Продовження таблиці 2.3

Переваги та недоліки Nagios Core.

Переваги	Недоліки
Гнучка архітектура з великою кількістю різноманітних плагінів. Завдяки наявності великої кількості плагінів, як від спільноти так і офіційних можливо налаштовувати та моніторити майже будь-який пристрій.	Початкове налаштування та подальші зміни в конфігурації можуть бути складними. Налаштування здійснюються через файли конфігурації через відсутність веб інтерфейсу для цього та при потребі внесення змін доводиться змінювати цілі файли.
Проста інтеграція інструментами візуалізації. Nagios Core здатний інтегруватися з такими інструментами візуалізації, як: RRDTool, Graphite та Grafana для розширеного та зручного відображення метрик та аналітики.	Відсутність достатньої підтримки при використанні базових версій.
Зручна система оповіщень. Nagios Core дозволяє надсилати сповіщення у вигляді повідомлень на email, веб інтерфейс та за допомогою API надсилати сповіщення в месенджери.	

Nagios Core часто використовують у компаніях середнього масштабу для базового моніторингу серверів, мережевих пристроїв, сервісів (веб–серверів, баз даних). Завдяки розподіленій архітектурі система здатна масштабуватись на великі мережі, але для нормального відображення метрик у вигляді графіків часто потребує інтеграції з окремими компонентами (RRDTool, Grafana).

Prometheus – це набір інструментів для моніторингу та оповіщення з відкритим кодом, що дозволяє контролювати стан інфраструктури та застосунків в хмарному середовищі[18]. Prometheus збирає дані у форматі часових рядів, тобто інформація про метрики зберігається з позначкою часу, коли вона була записана. Для отримання метрик він використовує модель pull. В цій моделі центральний сервер (Prometheus server) опитує цілі (хости, застосунки тощо) та експортує метрики в форматі HTTP/HTTPS. Для моніторингу фізичних пристроїв і ОС використовуються експортери (Node Exporter, SNMP Exporter, Blackbox Exporter)(див. рис. 2.8) Запити виконуються мовою PromQL, що дозволяє будувати складні аналітичні запити.

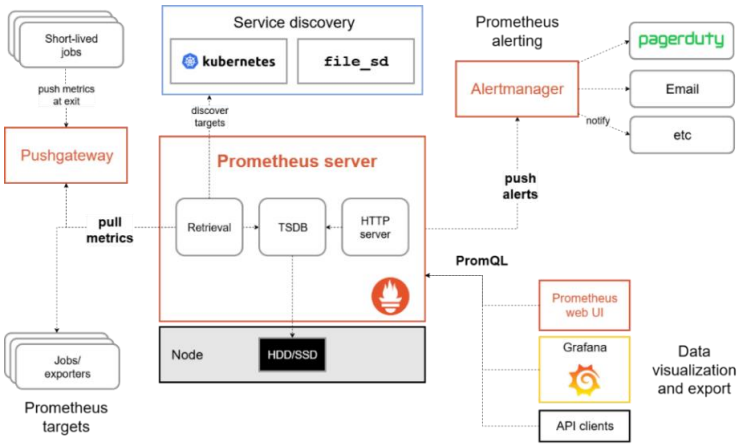


Рисунок 2.8 – Архітектура роботи Prometheus

Для візуалізації метрик використовується Grafana. Grafana — це мультиплатформенний веб-додаток для аналітики та інтерактивної візуалізації з відкритим кодом. Він може створювати діаграми, графіки та сповіщення у вигляді інформаційних повідомлень (табл. 2.4)(див. рис. 2.9). Додаткові приклади наведено в додатках А, Б.



Рисунок 2.9 – Відображення статусу та завантаженості обладнання Prometheus з Grafana

Таблиця 2.4

Переваги та недоліки Prometheus.

Переваги	Недоліки
Гнучкий механізм збору даних за допомогою експортерів.	Обмеження по довгостроковому зберіганню даних. Дані можна зберігати від 15 до 90 днів після чого вони видаляються. Тож для довгострокового зберігання необхідно використовувати інші сервіси.

Продовження таблиці 2.4

Переваги та недоліки Prometheus.

Переваги	Недоліки
Потужна та гнучка мова PromQL розроблена спеціально для вибору та агрегування даних часових рядів у системі моніторингу Prometheus.	Має складну архітектуру та може вимагати значних зусиль для налаштування особливо у випадку великих комп'ютерних мереж.
Інтеграція з Grafana для зручного відображення метрик.	

Prometheus з Grafana широко застосовують у DevOps та хмарних середовищах: моніторинг контейнерів (Kubernetes), мікросервісів, баз даних PostgreSQL/MySQL, брокерів Kafka та серверних додатках. Завдяки експортеру Node Exporter система може контролювати CPU, пам'ять, мережевий трафік, систему файлів; а Exporter SNMP дозволяє інтегрувати мережеві пристрої.

Observium – це система моніторингу мережевої інфраструктури, яка працює використовуючи протокол SNMP та дозволяє оцінювати стан мережі різного масштабу й аналізувати її продуктивність[19]. Observium має безкоштовну версію, професійну та для великих компаній. Ця система інтегрується обладнанням від виробників Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp, що забезпечує зручність у використанні(див. рис. 2.10-11).



Рисунок 2.10 – Інформаційна панель трафіку мережі з Observium.

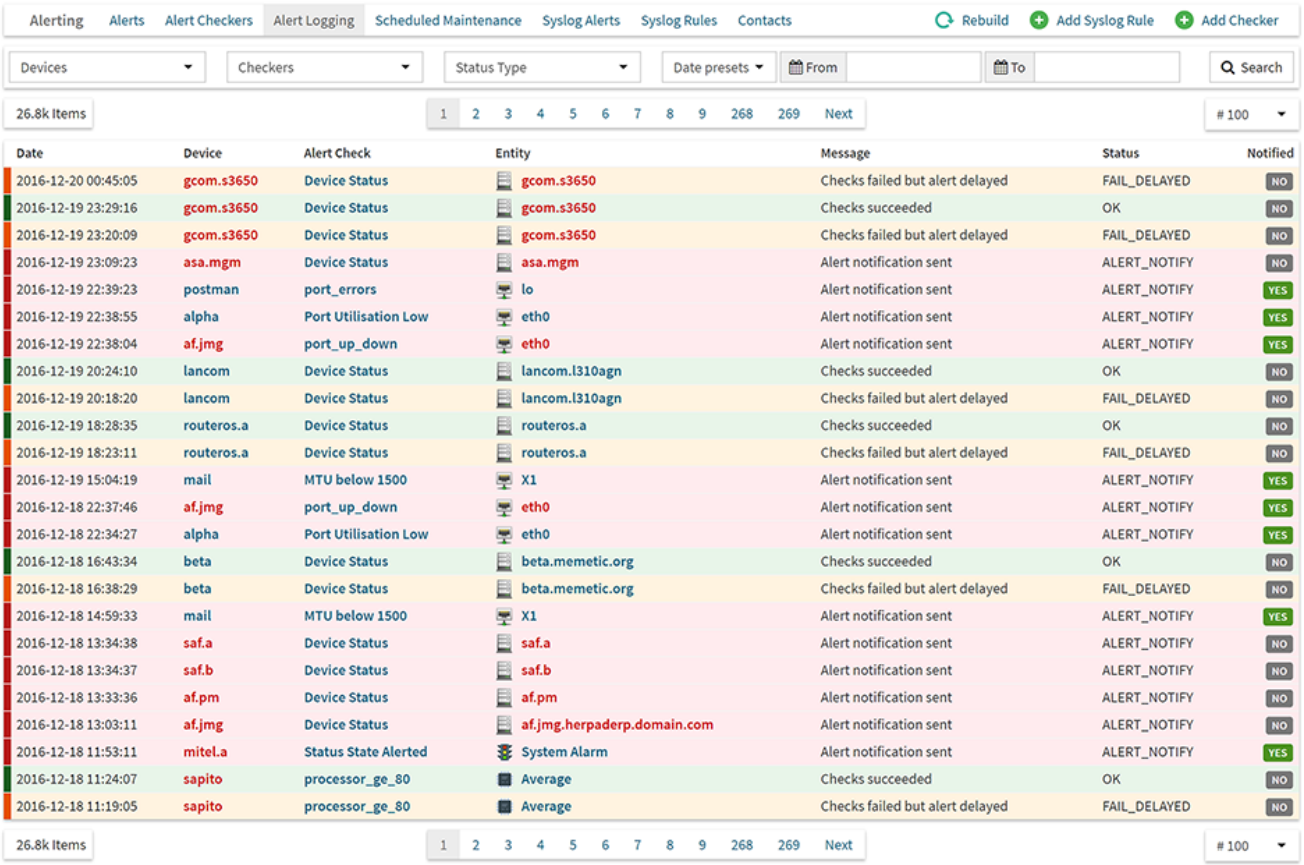


Рисунок 2.11 – Вкладка помилок та тривоги в Observium.

Observium доступний у трьох основних редакціях, які відрізняються частотою оновлень, набором функцій та моделлю ліцензування: Community, Professional та Enterprise. Observium доступний у трьох основних редакціях, які відрізняються частотою оновлень, набором функцій та моделлю ліцензування: Community, Professional та Enterprise.

Observium Community є безкоштовною версією з відкритим кодом. Вона надає повний функціонал моніторингу, включаючи автоматичне виявлення пристроїв, створення графіків, підтримку SNMP та широкої бази обладнання. Ключове обмеження цієї версії полягає у затримці оновлень (шість місяців) та відсутності доступу до деяких розширених модулів і комерційної підтримки. Вона є ідеальною для невеликих і тестових середовищ.

Observium Professional — це платна комерційна версія, яка пропонує миттєвий доступ до всіх оновлень (щодня). На додаток до базового функціоналу Community-версії, Professional надає розширені можливості, критичні для робочих середовищ: автоматичне управління конфігурацією (Config management), розширені дайджести сповіщень електронною поштою, докладніші звіти та функціонал мережевої інвентаризації. Вона рекомендована для середніх компаній та операторів, яким потрібна стабільність та доступ до новітніх функцій.

Observium Enterprise — найповніша платна версія, призначена для великих корпорацій та організацій з критично важливою інфраструктурою. Вона включає усі функції Professional (щоденні оновлення, Config Management, звіти), але також пропонує додаткові інструменти для масштабування, високої доступності (High Availability) та розширену комерційну підтримку (SLA). Ця версія забезпечує найбільшу надійність та здатність працювати у складних, багатокомпонентних мережевих архітектурах (табл. 2.5).

Таблиця 2.5

Переваги та недоліки Observium

Переваги	Недоліки
Для початкового використання доступна безкоштовна версія.	Обмеженість безкоштовної версії та висока вартість ліцензій
Observium здатен автоматично виявляти нові пристрої в мережі.	Вимогливість до ресурсів. Для повноцінної роботи може знадобитися окремо виділений потужний сервер
Широка інтеграція з виробниками мережевого обладнання	Складність в подальшому обслуговуванні та кастомізації. При подальшому розростанні мережі можуть виникати труднощі в налаштуваннях системи моніторингу
Забезпечення глибокого аналізу та збору метрик про мережу	
Гарна візуалізація даних за рахунок продуманих інформаційних панелей	

Observium широко використовують інтернет–провайдери та оператори дата–центрів для моніторингу стану каналів, трафіку й температури комутаторів. Система підходить для мереж, де основну інформацію можна отримати через SNMP(див. рис. 2.12)(Додаток В).

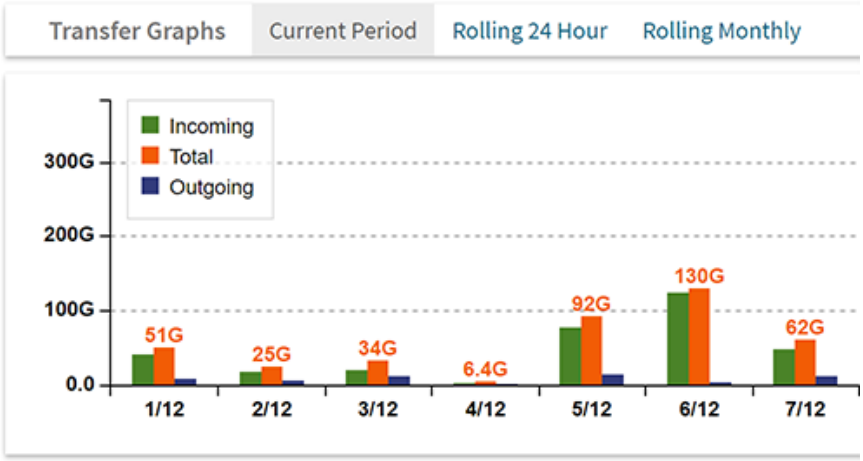


Рисунок 2.12 – Аналіз трафіку в Observium.

SolarWinds NPM – це комерційна платформа призначена для моніторингу мереж та дата-центрів[20]. Система збирає дані за допомогою SNMP, WMI, NetFlow, sFlow, IPFIX і Syslog та виконує автоматичне сканування мережі для виявлення нових пристроїв та надає кореневий аналіз причин. SolarWinds Observability Self-Hosted відстежує кожен сервер і компонент застосунку для забезпечення високої доступності та швидкого усунення несправностей. Завдяки постійному моніторингу сервера застосунків, він допомагає виявляти проблеми та підтримувати оптимальну продуктивність у всіх середовищах. Також SolarWinds NPM дозволяє контролювати використання фізичних ресурсів обладнання (див. рис.2.13).

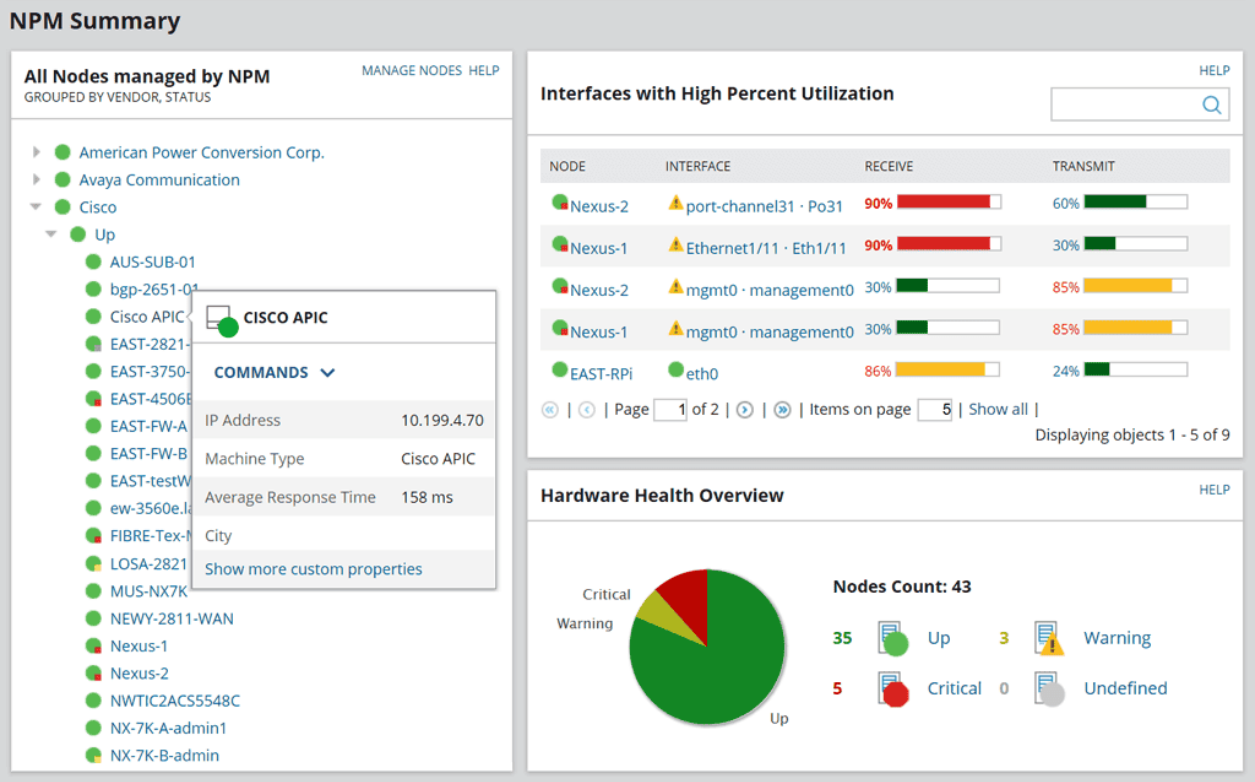


Рисунок 2.13 – Відображення пристроїв та статусу інтерфейсів в SolarWinds.

Однією з ключових переваг SolarWinds є модульна архітектура, яка дозволяє розширювати функціональність системи відповідно до потреб організації. Базова платформа Orion може доповнюватися спеціалізованими модулями, що забезпечують глибший рівень моніторингу окремих компонентів інфраструктури (див. рис. 2.14-15).



Рисунок 2.14 – Інформаційна панель SolarWinds.

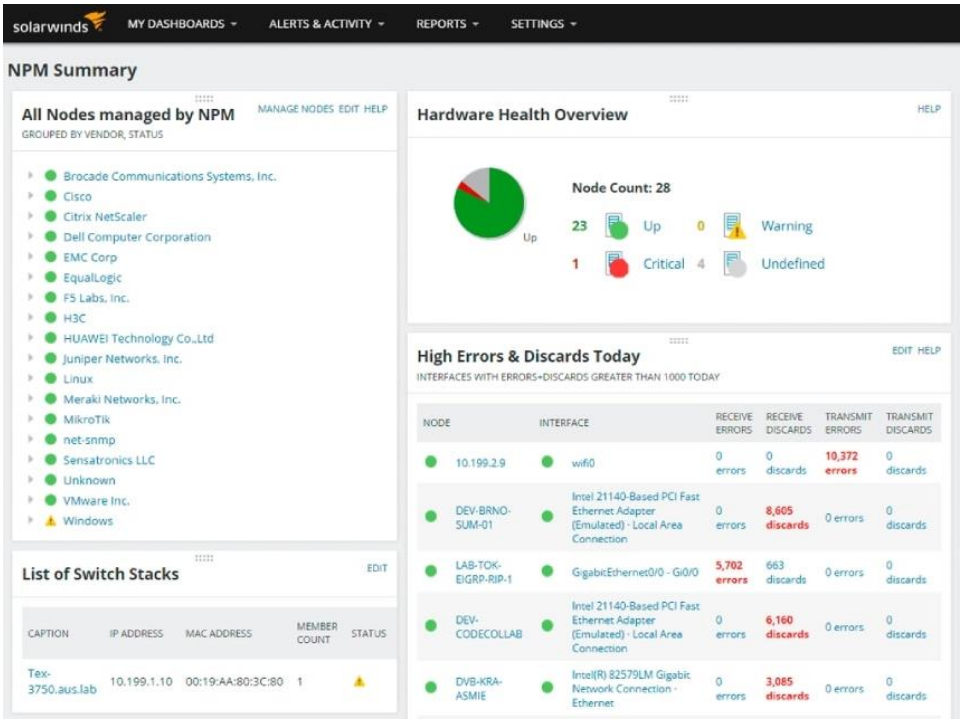


Рисунок 2.15 – Відображення помилок в SolarWinds.

Найпоширенішими модулями є: Network Performance Monitor (NPM), Server Application Monitor (SAM), NetFlow Traffic Analyzer (NTA), Database Performance Analyzer (DPA) та Security Event Manager (SEM) (табл. 2.6).

- Network Performance Monitor (NPM) – основний модуль для моніторингу мережевої інфраструктури, що забезпечує аналіз продуктивності мережі, виявлення збоїв, побудову топології та контроль стану мережевих пристроїв.
- Server Application Monitor (SAM) – призначений для контролю продуктивності серверів та додатків, включаючи моніторинг процесів, сервісів, стану обладнання, а також підтримку Windows, Linux, VMware та інших платформ.
- NetFlow Traffic Analyzer (NTA) – модуль аналізу мережевого трафіку, що дає змогу відстежувати джерела навантажень, типи трафіку, виявляти аномалії та здійснювати capacity planning.
- Database Performance Analyzer (DPA) – забезпечує детальний моніторинг та діагностику продуктивності баз даних (Oracle, MySQL, SQL Server, PostgreSQL тощо), дозволяючи виявляти "вузькі місця" у роботі СУБД.
- Security Event Manager (SEM) – модуль для аналізу подій безпеки та журналів, який забезпечує виявлення загроз, кореляцію подій, реагування на інциденти та відповідність стандартам безпеки.

Таблиця 2.6

Переваги та недоліки SolarWinds.

SolarWinds має широкий спектр функцій, щоб забезпечити моніторинг комп’ютерної мережі, серверів, додатків та баз даних.	Висока вартість підписки, оскільки це комерційна платформа.
Автоматичне виявлення нових пристроїв в мережі.	Складність початкового налаштування та подальшої підтримки. Ця платформа вимагає певного рівня знань про неї перед впровадженням.
Інтеграція з популярними виробниками обладнання, такими, як Cisco, Juniper, HP, Dell, MikroTik, VMware.	Залежність від вендора. Хоч система й має інтеграцію з різними виробниками, але розбудова інфраструктури та подальше розширення з зміною вендора обладнання може викликати труднощі.
Наявна власна екосистема модулів, що дозволяють організувати краще моніторинг комп’ютерної мережі.	Вимогливість до ресурсів. Для повноцінної роботи SolarWinds вимагає достатньо потужного обладнання, що може вимагати виділення окремого серверу або додаткових витрат на покращення існуючого.

SolarWinds NPM часто використовують у корпоративних мережах і великих дата–центрах: система дозволяє адміністраторам виявляти вузькі місця у пропускній здатності, відстежувати SLA, виконувати динамічне балансування навантаження й корелювати події між різними компонентами (маршрутизаторами, комутаторами, firewall). Платформа інтегрується з іншими продуктами SolarWinds (Server Application Monitor, NetFlow Traffic Analyzer).

Datadog – це SaaS платформа, яка поєднує в собі функції моніторингу інфраструктури, безпеки хмарних застосунків, додатків та системних записів syslog[21]. Datadog підтримує агентний та без агентний підходи, збирає інформацію з серверів, контейнерів Docker, Kubernetes), баз даних, хмарних сервісів (AWS, Azure, Google Cloud), додатків (APM) та має інтеграцію з більш ніж 1000 технологій та сервісів (табл. 2.7)(див. рис. 2.7).

Таблиця 2.7

Переваги та недоліки Datadog.

Переваги	Недоліки
Datadog має інтеграцію з хмарними платформами та підтримує більш ніж 1000 технологій та сервісів включаючи великих хмарних провайдерів, бази даних тощо.	Високі ціни на підписку. Витрати на Datadog ставатимуть більшими в міру використання додаткових функцій та розширення інфраструктури. Оскільки базова версія не може забезпечити всі потреби для великих компаній.
Моніторинг продуктивності застосунків(APM). Аналіз продуктивності програм за допомогою розподіленого трасування. Розподілене трасування — це метод моніторингу та діагностики програм, особливо в мікросервісних архітектурах. Це дозволяє відстежувати шлях запиту через різні служби, щоб зрозуміти продуктивність, виявити затримки та вузькі місця на шляху.	Залежність від підключення до хмарного середовища. Якщо відсутнє підключення до мережі інтернет то зв’язок з Datadog буде втрачено. Тож варто врахувати наявність запасного провайдера.
Зручні інформаційні панелі. Datadog дозволяє створювати персоналізовані панелі для візуалізації важливих показників продуктивності та налаштовувати окремі сповіщення про виявленні аномалії, спрацювання критичних тригерів та збоїв.	Складність при масштабуванні: Хоча початкове налаштування може бути простим, з розширенням інфраструктури використання Datadog стає все більш складним і дорогим, що вимагає більших зусиль.

Продовження таблиці 2.7

Переваги та недоліки Datadog.

Переваги	Недоліки
Висока швидкість і аналітика в реальному часі: Платформа здатна надавати дані в режимі реального часу, що є критично важливим для швидкої діагностики та усунення несправностей. Це дозволяє оперативно реагувати на інциденти й вирішувати їх.	Обмеження на зберігання даних: За замовчуванням Datadog може мати обмежені терміни зберігання логів. Щоб збільшити цей термін, потрібно додатково купувати місце для зберігання.
Інтеграція штучного інтелекту у вигляді модуля (Watchdog): Watchdog автоматично виявляє аномалії та допомагає з аналізом першопричин, що значно прискорює пошук і усунення проблем.	Залежність від вендора: Високий рівень інтеграції з Datadog може ускладнити перехід на інше рішення в майбутньому, оскільки вивчення нової системи потребуватиме достатньо часу, а міграція може бути складною. Й потрібно одразу враховувати можливі проблеми при міграції або відсутність частини функцій.

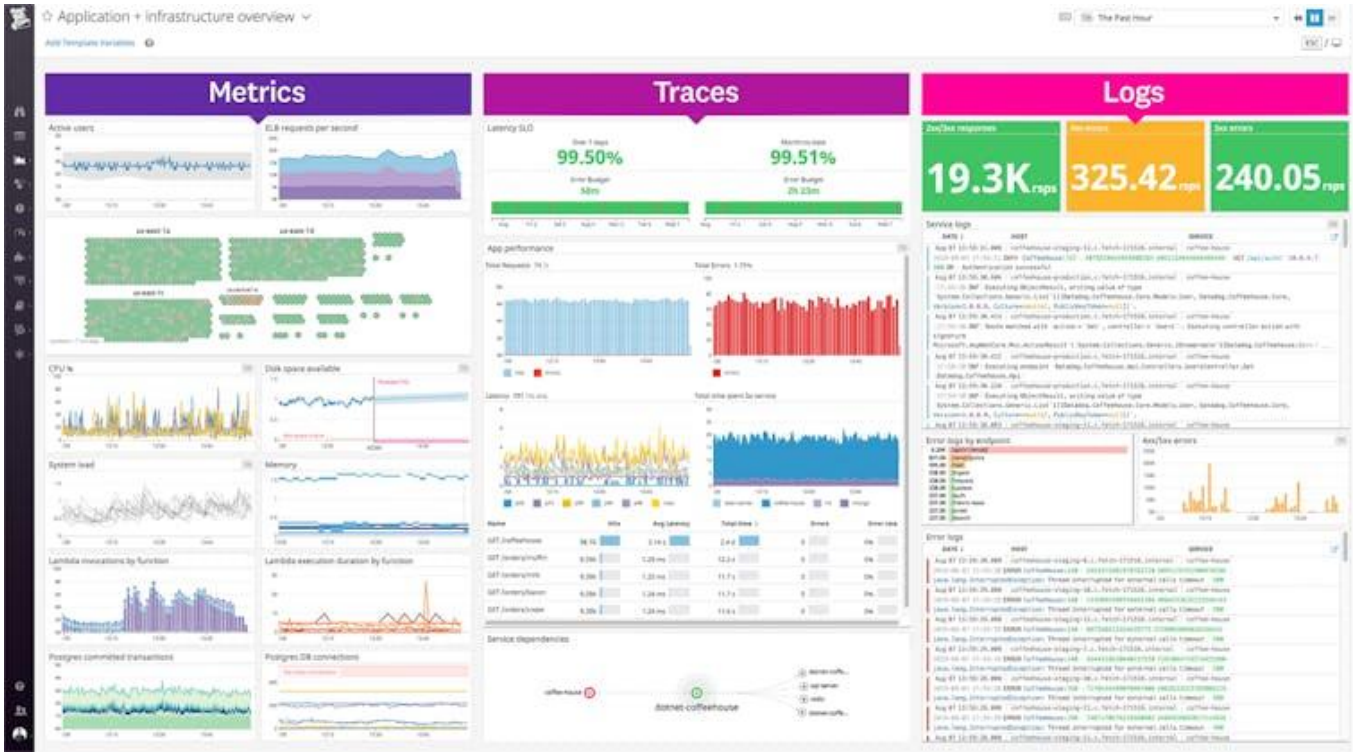


Рисунок 2.16 – Відображення метрик, traces та logs в Datadog.

Ключовою особливістю Datadog є наявність модуль Watchdog, що представляє собою інтегрований штучний інтелект. Цей інтегрований штучний інтелект дозволяє аналізувати великі масиви даних, виявляти аномалії, виконувати кореляцію подій та знаходити першопричини помилок та збоїв до можливого впливу на користувачів (див. рис. 2.17).

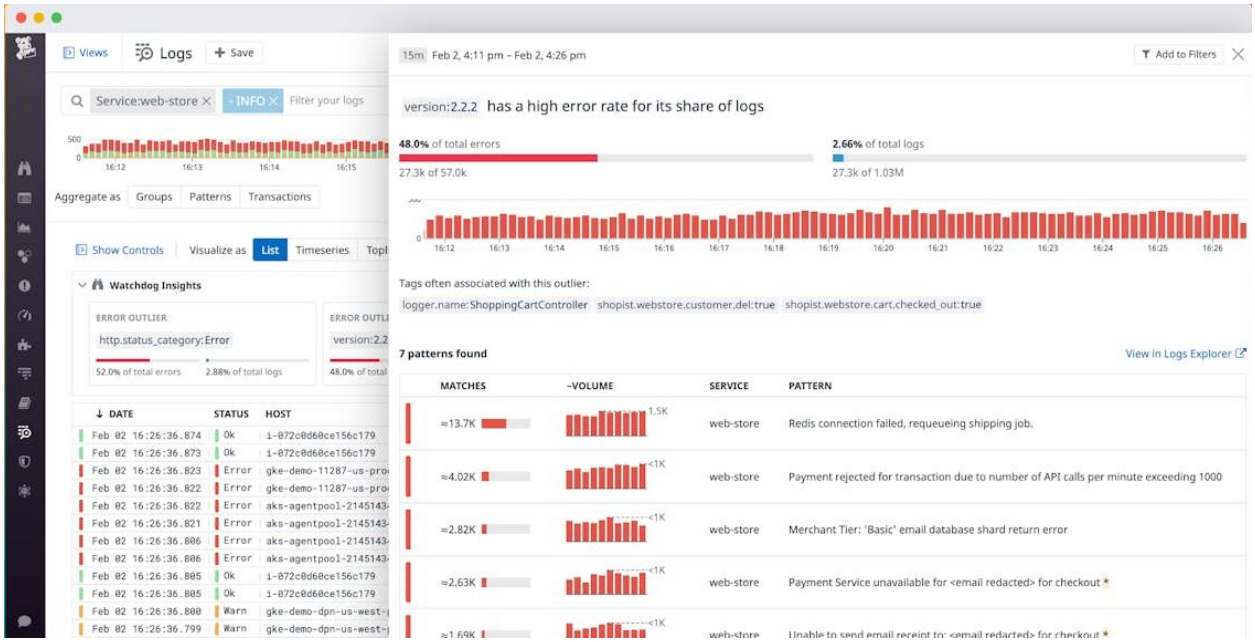


Рисунок 2.17 – Відображення роботи модулю Watchdog в Datadog.

Datadog застосовують в DevOps-командах великих компаній для моніторингу мікросервісних додатків, хмарних середовищ та безсерверних функцій. Наприклад, команда може відстежувати Kubernetes–кластер, бази даних PostgreSQL, черги RabbitMQ і веб–додатки на Node.js, отримуючи повну видимість і аналіз продуктивності.

З проведеного огляду популярних систем моніторингу можна зазначити, що немає єдиного універсального рішення, яке могло підійти будь-якому користувачу. Вибір системи моніторингу визначається конкретними вимогами до самої мережі, її інфраструктурою, масштабом, розгорнутими сервісами в компанії, командою та бюджетом.

Open-source системи такі як: Zabbix, Nagios Core, Prometheus, Observium надають базові та гнучкі інструменти для моніторингу та спостережуваності й за рахунок використання безкоштовних версій дозволяють знизити витрати на підписку чи ліцензію. Водночас ці системи мають обмеження не дивлячись на те,

що це open-source продукт. З розширенням компанії буде необхідно переходити на інше рішення або докупляти додаткові модулі чи підписки. Також open-source продукти можуть мати гіршу офіційну підтримку й пошук відповідей та рішення може зайняти багато часу оскільки доведеться шукати потрібну інформацію на форумах. Такі системи можуть підходити для команд розробників, невеликих чи середніх компаній залежно від потреб.

Комерційні рішення такі як: SolarWinds та Datadog мають ширший функціонал у базовій версії, інтеграції з різними сервісами й технологіями, готові шаблони, кращу сервісну підтримку, але й коштують дорожче залежно від вендора обладнання та підписок. Такі моделі є виправданими в великих компаніях, які хочуть мати стабільність, глибокий та якісний моніторинг зі спостережуваністю та ефективне реагування на проблеми в мережі. Проте для малих та середніх компаній це може бути надмірним та невиправданим.

За принципами роботи більшість рішень працює за моделями “агент-сервер” та без агентний підхід. Агент або в деяких системах експортер, збирає метрики на вузлах в мережі та передає для аналізу на центральний сервер. Без агентний підхід включає використання стандартних технологій та інтернет-протоколів. Частіше за все можна зустріти використання протоколів: SNMP, IPMI, HTTP/HTTPS, SSH, REST-API, WMI, NetFlow та syslog для отримання системних записів (логів). Системи моніторингу також підтримують можливість налаштування власної системи оповіщення, тригерів, інтеграцію з месенджерами, такі як: Slack, Webex або через email та спеціальні інструменти для візуалізації даних такі як Grafana.

Тенденцією останніх років є перехід від класичного моніторингу зі спостережуваністю до інтеграції штучного інтелекту чи нейронних мереж у системи моніторингу. Головною метою є автоматизація систем моніторингу, реагування на випередження, оптимізація мережевої інфраструктури, скорочення часу реагування на інциденти та підвищення доступності сервісів. Інтеграція штучного інтелекту чи нейронних мереж в системи моніторингу дозволить створити гібридний підхід до моніторингу та спостережуваності, що в перспективі дозволить отримати оптимальну інфраструктуру в компанії прибравши вузькі місця та надлишки й підвищивши роботу мережі та сервісів.

РОЗДІЛ 3. ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ МОНІТОРНГУ КОМП'ЮТЕРНИХ МЕРЕЖ, ЇХ ФУНКЦІЇ, ПРИНЦИПИ ТА АРХІТЕКТУРА

3.1 Перспективи розвитку систем моніторинг комп'ютерних мереж

Розвиток технологій, корпоративних комп'ютерних мереж, зростання кількості пристроїв у користувачів та нові вимоги до сервісів з послугами створює нові виклики для мережевої інфраструктури компаній [22]. Адаптуючись до нових вимог та тенденцій, додатки та сервіси починають змінюватися та генерувати більші об'єми даних. Віртуалізація, хмарні сервіси та контейнеризація починають все більше застосовуватися в інфраструктурі комп'ютерних мереж компаній через їх зручність, що призводить до розосередження корпоративної комп'ютерної мережі компанії та зростання рівня її складності. Разом з цим, комп'ютерна мережа отримує більше навантаження, яке потрібно контролювати та відстежувати її стан. Бо у випадку перевантаження чи відмови мережі, компанія може втратити репутацію, клієнтів та гроші. Отже, постає питання, як модернізувати теперішні системи моніторингу під сучасні та майбутні потреби, оскільки підходи, зо в них застосовуються до моніторингу та спостережуваності побудовані здебільшого на статичних правилах, які не пристосовані для динамічних умов.

Згідно зі звітами Cisco Annual Internet Report (2018–2023) та Digital 2024: Global Overview Report однією з ключових тенденцій розвитку корпоративних мереж є різке збільшення обсягів даних, що пересилаються між сервісами, пристроями та обчислювальними ресурсами[23]. Щорічне зростання обсягу трафіку в корпоративному середовищі перевищує 25%, а у сфері критичної інфраструктури близько 40%. Дана тенденція спричиняє зростання навантаження на корпоративні комп'ютерні мережі, що впливає на показники продуктивності та обсяги обробленої інформації. Це своєю чергою навантажує системи моніторингу, які можуть або видавати хибні спрацювання або не справлятися з новими обсягами інформації.

З огляду на зазначене можна зробити висновок, що необхідно адаптувати та модернізувати системи моніторингу до зростаючого навантаження. Можливим розв'язком цього питання може бути інтеграція та використання штучного інтелекту та нейронних мереж в сучасних системах моніторингу. У звіті "Network Performance Monitoring Trends Report 2024" від LiveAction описується застосування та вплив штучного інтелекту на час виявлення інцидентів, зменшення часу простоїв та зазначається перспектива покращення спостережуваності та моніторингу.

Також варто зазначити, що додатковим чинником, що впливає на потребу в модернізації систем моніторингу є також фактор інформаційної безпеки. Кіберзагрози набуваючи дедалі складнішого характеру та змінюючи підходи для ураження систем, викрадення даних, видалення даних тощо. Разом з розвитком кібератак розвивається й протидія атакам та захист систем. Чим краще система безпеки тим складніше вона є та вимагає більше ресурсів. Це також своєю чергою створює додаткове навантаження на комп'ютерні мережі компаній. Оскільки нові системи безпеки можуть вимагати не лише фіксації подій а й додаткової кореляції та відстеження її шляху. Звіт Global Cybersecurity Outlook 2024[24] наводить інформацію, що понад 60 відсотків інцидентів у корпоративних мережах могли бути виявленні, ще на початкових етапах за наявності систем аналітичного моніторингу з автоматизованим пошуком аномалій[25]. Таким чином перспективним напрямком розвитку систем моніторингу мережі є впровадження аналітичних функцій та дослідження аномальної поведінки чи порушень безпеки штучним інтелектом або нейронними мережами. Тож головним напрямком розвитку систем моніторингу комп'ютерної мережі є використання штучного інтелекту або нейронних мереж у якості аналітичного інструменту з функціоналом систем моніторингу. Такі системи будуть здатні будувати причинно-наслідкові зв'язки для розуміння природи виникнення проблеми чи збоїв та проводити діагностику системи для пошуку вразливостей та надмірної надлишковості.

3.2 Концепція та архітектура системи моніторингу з використанням нейронної мережі або штучного інтелекту

Концепція використання системи моніторингу комп'ютерної мережі з використанням нейронної мережі або штучного інтелекту полягає у використанні нейронної мережі або штучного інтелекту в якості інтелектуального інструменту для моніторингу, спостережуваності та аналітики. Тобто нейронна мережа або штучний інтелект буде інтегровано в систему моніторингу комп'ютерної мережі в якості окремого інтелектуального модуля, що матиме наступні функції: моніторинг та аналіз метрик, пошук аномальної поведінки, виявлення вузьких місць та надмірної надлишковості, сповіщення, надання звітів та оперативне реагування.

Моніторинг та аналіз метрик. Інтегрований інтелектуальний модуль виконуватиме аналіз метрик, які збираються системою моніторингу комп'ютерної мережі використовуючи агентний або без агентний метод. Аналіз метрик передбачає розуміння характеристик цих метрик, для чого вони збираються, які їх порогові значення, чи є хибні спрацювання, як часто це відбувається та причина цих спрацювань. Прикладом неправильно налаштованих метрик можуть бути: встановлені статичні порогові значення, встановлення низьких порогових значень,

вимірювання ізольованих метрик без контексту або прив’язки до інших подій. Наприклад, при встановленні порогового значення для рівня завантаженості сервера або процесора сервера у 80% здатне призводити до хибного спрацювання, якщо не врахована специфіка цього сервера. Цей сервер може працювати 24/7 при середньому навантаженні в межах від 60% до 85% відсотків. Таке навантаження може бути звичайним робочим навантаженням для серверу, що обробляє платежі. В даному випадку падіння навантаження може свідчити про проблеми з обробкою платіжних операцій або при різкому зростанні та утримання високого рівня завантаження протягом тривалого періоду про збільшення кількості операцій або спроби атаки на сервер. Встановлення низьких порогів навантаження здатне призвести до значної кількості хибних спрацювань, через що ці сповіщення можуть бути проігноровані, як спам, що в майбутньому здатне призвести до пропущення серйозної проблеми.

Пошук аномальної поведінки передбачає виявлення нетипового трафіку чи запиту в мережі, проблеми з доступністю серверів чи сервісів або нетипові показники апаратного забезпечення. В цьому випадку йде збір необхідних метрик та фіксуються проміжки часу й обставини при, яких виникла ця нетипова поведінка.

Сценарій 1: Сервер бази даних, що зазвичай генерував невелике або стабільний рівень навантаження починає отримувати велику кількість запитів. Цей сервер займався обробкою запитів від веб серверів, які запитували інформацію з баз даних. Система моніторингу починає фіксувати раптовий стрибок вихідного трафіку, який триває більше декількох хвилин чи пів години. При тому вхідний трафік залишається в межах норми або має незначне зростання. Система моніторингу виявляє цю аномалію за допомогою налаштованої метрики про вхідний та вихідний мережевий трафік. Спрацьовує тригер про перевищення порогових значень з відповідним рівнем критичності. В цей момент підключається інтегрований інтелектуальний модуль з нейронною мережею та починає проводити аналіз, що відбувалося до цієї аномалії, які запити були від веб серверів, за яким маршрутом вони курсували, які сповіщення були від системи безпеки тощо. Після чого цей модуль надає детальну звітність про виявлену аномальну поведінку та можливі її причини.

Сценарій 2: Система фіксує поступове збільшення робочої температури або її різке зростання. Під час роботи сервера бази даних спрацював тригер про різке збільшення температури процесора. Типова температура процесора сягала 45-60 градусів за Цельсієм. Зараз метрики фіксують температуру 75 градусів за Цельсієм й вона різко зростає до 95 градусів за Цельсієм. Відбувається це впродовж 30 хвилин або 1 години й температура не падає. Збір цієї інформації відбувається за допомогою IPMI або інструментів операційної системи. Дана аномалія може вказувати на проблему з системою охолодження, яка може виражатися у

несправності вентилятора, водяного охолодження, висихання термопасти або нетісний контакт процесора з радіатором, збій системи кондиціонування або засмічення пилом. Модуль з нейронною мережею починає зчитувати метрики системою моніторингу та досліджувати можливі передумови, стан системи охолодження та навколишні умови. Проаналізувавши та зібравши дані він надає детальний звіт про ситуацію дозволяючи спеціалістам оперативно зреагувати до відмови сервера та знайти причину такої поведінки.

Виявлення вузьких місць передбачає аналіз мережевого трафіку, пропускної здатності каналів та завантаженості й ефективності обробки інформації серверами. Наприклад між рівнем доступу та рівнем ядра в мережі виникають затримки в обробці та надсиланні пакетів з інформацією. Проводиться аналіз рівня завантаженості в різні періоди дня, тижня чи місяця та визначається, чи є це сезонним явищем чи це на постійній основі. Після цього відбувається визначення пропускної здатності каналу, можливість його покращення та потреби. Модуль з нейронною мережею зібравши необхідну інформацію формує звіт про цю ситуацію та вказує чи може це бути потенційною проблемою в майбутньому. Аналогічно відбувається з пошуком надлишковості. Модуль аналізує канали, які задіяні мінімально й не використовують усю пропускну здатність, переглядає історію використання цього каналу та формує висновок, щодо доцільності надлишковості цього каналу.

У випадку з апаратною складовою проводиться аналіз рівня її використання, продуктивності сервера та сервісів розгорнутих на ньому. Після чого формується висновок про потребу модернізації компонентів сервера, якщо це потрібно.

Система сповіщень та звітів модуля зі штучним інтелектом або нейронною мережею полягає у надсиланні цим модулем сповіщення про виявлену проблему, ризи чи вразливість та прикріпленні звіту про пророблений аналіз даної проблеми. Головною ідеєю оповіщень від цього модулю є здатність аналізувати великі обсяги даних за певні періоди часу та надавати звітність до 5 або 10 хв після виникнення проблеми.

Оперативне втручання відбувається при фіксації підозрілої активності чи спрацюванні критичних тригерів. Це передбачає використання інтелектуальним модулем інструкцій, які були створені системними адміністраторами, мережевими інженерами або фахівця з кібербезпеки. Це інструкції, які передбачають використання підготовлених скриптів, що мають на меті в екстреному порядку ізолювати ділянку або вимкнути обладнання, порти чи сервіси.

Таким чином ідея інтеграції в системи моніторингу інтелектуального модуля з нейронною мережею полягає в автоматизації та впровадженні інтелектуальної системи в саму систему моніторингу комп’ютерної мережі. На модуль будуть покладатися задачі аналізу мережі в режимі 24/7, передбачення проблем, виявлення

аномалій оптимізація інфраструктури та в майбутньому можливість діяти на випередження за допомогою встановлених інструкцій та використання скриптів для оперативного реагування в критичних ситуаціях.

Враховуючи покладені на інтелектуальну систему моніторингу задачі, вона має відповідати переліку вимог, дотримання яких забезпечить її ефективну роботу в корпоративних комп'ютерних мережах:

1. Автоматичне виявлення інцидентів. Інтелектуальна система моніторингу повинна самостійно аномалії, помилки конфігурації, деградацію обладнання, атаки на мережу тощо.
2. Класифікація подій. На основі бази знань інтелектуальна система моніторингу повинна визначити тип та критичність події для подальшого аналізу та реагування.
3. Кореляція логів та метрик. Провівши аналіз даних система повинна вибудовувати причинно-наслідкові зв'язки між подіями в мережі, об'єднуючи їх загальну картину інциденту.
4. Формування рекомендацій. Після проведеного аналізу система має сформувати звіт де будуть вказані рекомендації по усуненню проблеми або запобігання подібному в майбутньому.
5. Автоматичне реагування на інциденти. Маючи достатньо інформації та інструкцій система повинна автоматично реагувати на інциденти використовуючи підготовленні скрипти та інструкції для зменшення можливого впливу на мережу.

3.3 Архітектура системи моніторингу комп'ютерної мережі з використанням штучного інтелекту або нейронних мереж.

Архітектура інтелектуальної системи моніторингу комп'ютерної мережі з використанням штучного інтелекту або нейронної мережі передбачає багаторівневу модульну систему з розподілом функцій між різними вузлами, площинами, рівнями обробки та центральним аналітичним ядром на основі нейронної мережі. Такий підхід здатен забезпечити масштабованість, відмовостійкість, обробку великих обсягів даних в режимі майже реального часу(квазіреальний час) та знизить в майбутньому навантаження на центральну систему за рахунок виконання частини операцій з нормалізації та агрегації даних на периферійному рівні. Нормалізація даних – це процес упорядкування даних за відношеннями для зменшення надлишковості та уникнення аномалій даних. Агрегація даних – це процес узагальнення даних з різних джерел в єдину форму подачі у вигляді звіту, структурованої таблиці тощо.

В даній моделі, архітектура розглядається за допомогою використання двох площин: площина даних та площина керування, що дозволяє відокремлювати транспортування та обробку даних, механізми конфігурації, контроль версій моделей та оркестрацію процесів реагування[26]. Такий поділ відповідає концепції SOAR відокремивши збір та обробку даних від процесу керування, налаштування та навчання моделі (див. рис. 3.1).



Рисунок 3.1 – Модель SOAR

SOAR (Security Orchestration Automation and Response) – це набір служб та інструментів, що використовуються для забезпечення автоматизованого підходу до запобігання кібератакам, та реагуванням на них. Цей підхід складається з оркестрації, автоматизації, безпеки та реагування на інциденти. В контексті систем моніторингу комп'ютерних мереж метод SOAR відображає, яким має бути підхід та вектор розвитку системи моніторингу для її ефективної роботи. Оркестрація – це поєднання внутрішніх та зовнішніх інструментів для отримання доступу до цих інструментів з одного централізованого розташування. Це дозволяє консолідувати дані, спростити процеси та підготувати підґрунтя для автоматизації.

Площина даних – це рівень, що відповідає за збір, обробку, зберігання та аналіз даних. Ця площина забезпечує взаємодію з інфраструктурою, пристроями, сервісами та службами для збору даних. Функції площини даних полягають у зборі даних, нормалізації та обробці даних. Основні модулі площини даних (див. рис. 3.2):

1. Модуль збору даних. Це модуль, що відповідає за збір даних про комп'ютерну мережу використовуючи для цього агентний та без агентний методи.

2. Модуль попередньої обробки. Це модуль, що відповідає за нормалізацію даних та перевірку на ознаки та наявність спрацювань критичних тригерів.
3. Модуль операційного сховища даних. Цей модуль є місцем для зберігання даних, що були зібрані та нормалізовані на попередніх рівнях. Використовується дане сховище для короткострокового зберігання даних для забезпечення аналітики в режимі реального часу. Дані в цьому сховищі постійно перезаписуються на нові вхідні дані.
4. Модуль обробки та візуалізації даних. Цей модуль обробляє отриману інформацію, що знаходиться в операційному сховищі виводить необхідні дані на монітори за допомогою інформаційних панелей.
5. Інтелектуальний модуль системи (ІМС). Це модуль, що є інтегрованим штучним інтелектом або нейронною мережею та є мозком системи де відбувається обробка даних та навчання. Цей модуль аналізує отримані метрики відповідно до бази знань та правил й повертає звіт про пророблений аналіз з висновками, які можуть містити попередження, рекомендації або сповіщення про проблеми.
6. Модуль оперативного реагування. Це модуль, який використовує готові скрипти для запобігання поширенню проблеми або проведення негайних дій при виявленні проблеми. Використання скриптів виконується при роботі модуля попередньої обробки у разі спрацювання критичних тригерів або на етапі обробки даних та підготовки до графічного виводу. Відповідають за створення скриптів системні адміністратори, мережеві інженери та фахівці з кібербезпеки.
7. Модуль оцінки ефективності. Цей модуль відповідає за оцінювання роботи ІМС, яка складається з точності та правильності звітів, коректних спрацювань модулю швидкого реагування тощо.
8. Модуль сховища даних. Це модуль, який відповідає за подальше зберігання даних, що були оброблені в операційному сховищі даних. Тут зберігаються усі логи та метрики, що були отримані системою моніторингу відповідно до встановленого терміну. Термін зберігання залежить від розміру сховища та політики зберігання даних, які встановлюються кожною компанією індивідуально.

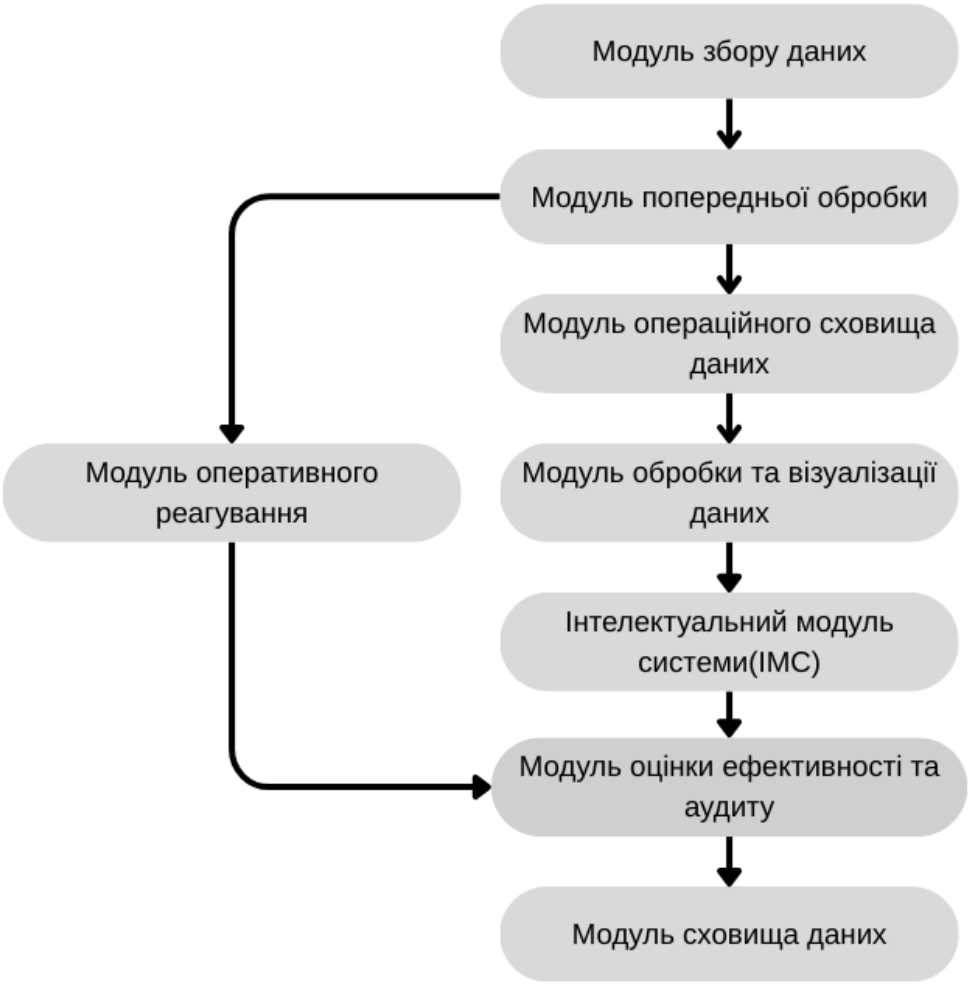


Рисунок 3.2 – Взаємодія модулів площини даних.

Також в інтелектуальній системі моніторингу комп’ютерних мереж важливо забезпечити розмежування оперативного реагування та поглибленого аналізу, який проводить інтелектуальний модуль системи. Оперативне реагування використовує мінімум інформації для спрацювання, оскільки орієнтується лише на критичне спрацювання та використовує підготовлені шаблони дій. Поглиблений аналіз навпаки, передбачає детальне вивчення ситуації, включно з аналізом оперативного реагування для забезпечення детального звіту з встановленими причинно-наслідковими зв’язками. Обидва підходи є важливими, оскільки перший скорочує час на реагування, а другий підвищує якість діагностики та запобігає повторним інцидентам в майбутньому.

Відобразити роботу цих модулів можна наступним чином: Під час пікового навантаження на сервер спостерігається недоступність частини сервісів через що згодом починають приходити скарги від користувачів. Тригери, які знаходяться в модулі збору даних спрацьовують та починають передавати інформацію про недоступність сервісів. В модулі попередньої обробки відбувається нормалізація

даних та аналіз на наявність критичного спрацювання. У випадку виявлення спрацювання критичного тригера залучається модуль швидкого реагування, який застосовує відповідний скрипт та одразу відправляється сповіщення на інформаційну панель. Якщо такого спрацювання не було виявлено, то дані передаються до модуля операційного сховища де обробляються модулем обробки та візуалізації даних. На цьому етапі відбувається аналіз даних їх передумов та їх візуалізація за допомогою інформаційних панелей. Потім підключається модуль оцінювання ефективності та дані відправляються до сховища даних.

Площина керування – це рівень системи де відбувається керування інтелектуальним модулем системи (ІМС) та системою моніторингу за допомогою відповідних модулів. Ця площина не відповідає безпосередньо зав обробку даних, формує політику доступу, координує роботу модулів, визначає правила взаємодії тощо. Основними її елементами є (див. рис. 3.3):

1. Конфігураційний модуль. Цей модуль відповідає за налаштування системи, порогові значення, види тригерів, методи збору інформації та систему сповіщень.
2. Модуль керування та політик доступу. В даному модулі визначаються права доступу, взаємодія між компонентами системи, рівні доступу.
3. Модуль оркестрації даних. Цей модуль відповідає за поєднання даних та інструментів для запуску дій по реакції чи усунення інцидентів.
4. Модуль керування модулем ІМС. Цей модуль відповідає за контроль актуальності та точності моделі ІМС, якістю роботи модулю та навчання.
5. Модуль аудиту та безпеки. Модуль аудиту та безпеки відповідає за фіксацію дій та рішень ІМС. Це важливо для забезпечення контролю за діями нейронної мережі, використанням даних, можливих змін, що були внесені в системі модулем ІМС та аналізу ефективності системи. Також це дозволяє забезпечити можливість відстеження інциденту від початку до кінця.
6. Модуль бази знань. База знань для інтелектуального модуля системи (ІМС) представлятиме збірник з довідника кодів подій та помилок мережі, опису конфігурації мережі та каталогу типових інцидентів. Що має забезпечити коректну роботу даної системи моніторингу.



Рисунок 3.3 – Взаємодія модулів площини керування.

Це важливо при ситуаціях, коли модуль ІМС помилково спрацював класифікувавши повідомлення тригера, як критичний інцидент та ввів в дію один зі скриптів тим самим ізолювавши ядро мережі. Через це всі сервіси та комунікація стали недоступними. Модуль аудиту зареєстрував цю подію та відправив на аналіз. ІТ спеціалісти компанії отримали звітність про цей інцидент та проаналізували його виявивши помилкове спрацювання. Було усунуто неправильну конфігурацію та покращено інструкцію реагування для ІМС. В модуль аудиту та безпеки внесено необхідну інформацію й ініційовано до навчання ІМС для уникнення подібних інцидентів в майбутньому.

Центральне ядро системи – це аналітичне ядро, що побудоване на основі штучних нейронних мереж та виконує роль головного мозкового центру системи. В даній архітектурі воно представлене інтелектуальним модулем системи (ІМС). Його головним завданням є обробка даних відповідно до їх змісту та бази знань системи моніторингу комп’ютерної мережі. Цей модуль взаємодіє разом з модулем оцінки ефективності та модулем аудиту та безпеки для самонавчання на поточних даних, використовуватиме базу знань, доповнюватиме її та проводитиме оцінку

якості. Це забезпечить коректну роботу системи оскільки звіти будуть ґрунтуватися на реальних даних.

Модуль бази знань – це збірка кодів, подій та помилок, опис конфігурації мережі та каталогу інцидентів, що складаються з документації виробників мережевого обладнання, документації системи моніторингу, стандартів RFC та мережевих протоколів, топології мережі та конфігурацій обладнання (див. рис. 3.4-5).

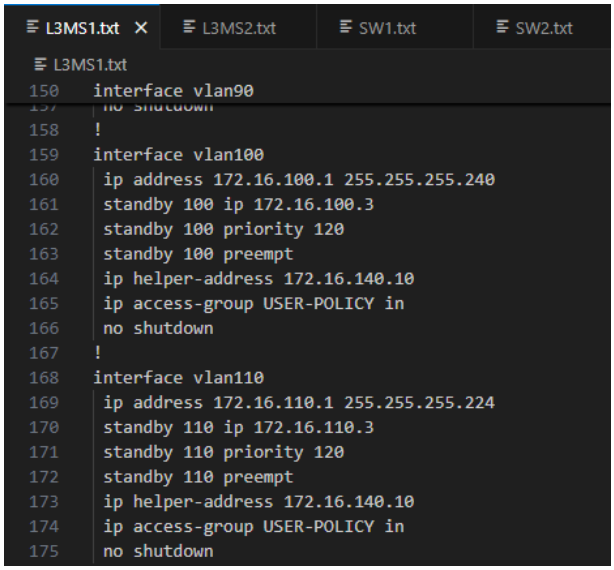


Рисунок 3.4 – Частина конфігурації комутатора 3 рівня в мережі

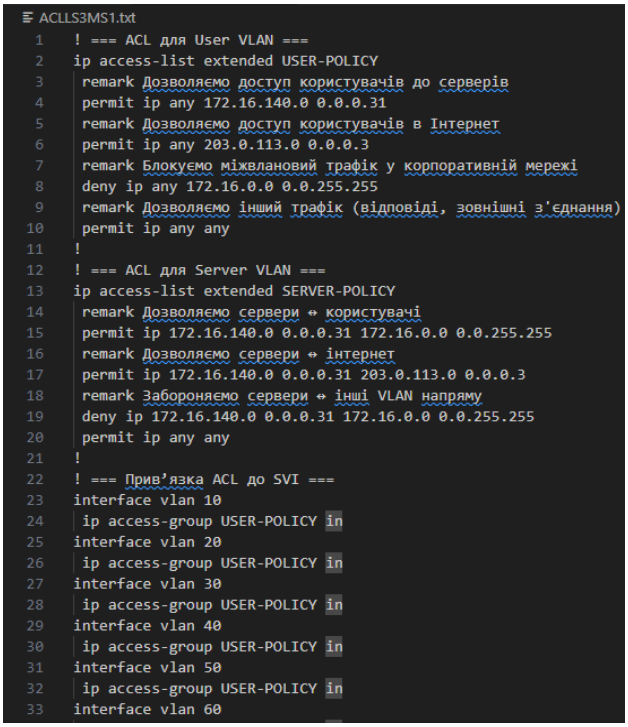


Рисунок 3.5 – Частина конфігурації списків доступу на комутаторі 3 рівня в мережі

Наприклад обладнання Cisco має систему кодів, що показує критичність системних повідомлень, як були зафіксовані пристроєм й мають різні рівні критичності(див. рис. 3.6):

1. Рівні 0-2 сигналізують про критичні стани, що можуть призвести до відмови обладнання або недоступності системи.
2. Рівні 3-4 вказують на помилки та попередження, які можуть вплинути на роботу, але зупиняють систему одразу.
3. Рівні 5-6 повідомляють про нормальні системні повідомлення та події як не потребують втручання.
4. Рівень 7 сигналізує про діагностику та налагодження при запуску debug-команди.

Level	Description
0 – emergency	System unusable
1 – alert	Immediate action needed
2 – critical	Critical condition
3 – error	Error condition
4 – warning	Warning condition
5 – notification	Normal but significant condition
6 – informational	Informational message only
7 – debugging	Appears during debugging only

Рисунок 3.6 – Розшифровка кодів серйозності системних повідомлень Cisco

Протокол ICMP, який також використовується в роботі систем має систему кодів з статусами (табл. 3.1). Ці статуси дають зрозуміти ймовірну причину та дають розуміння де потрібно виправити помилку. ICMP – це мережевий протокол, який використовується для передачі повідомлень про помилки та службову інформацію між мережевими пристроями.

Таблиця 3.1

Значення кодів протоколу ICMP

ICMP code	Message	Значення
0	Echo reply	Echo відповідь на ping
3	Destination unreachable	Пункт призначення недоступний
4	Source quench	Переповнення буферу
5	Redirect	Перенаправлення
8	Echo	Запит Echo
9	Router advertisement	Оголошення маршрутизатора
10	Router selection	Вибір маршрутизатора
11	Time exceeded	Перевищено час життя пакету(TTL)
12	Parameter problem	Проблема параметрів IP-заголовка
13	Timestamp	Запит часової позначки
14	Timestamp reply	Відповідь на запит часової позначки
15	Information request	Запит інформації
16	Information reply	Відповідь на запит інформації
17	Address mask request	Запит маски мережевої адреси
18	Address mask reply	Відповідь маски мережевої адреси
30	Traceroute	Повідомлення traceroute

Надійність та безпека даної архітектури має бути забезпечена за допомогою багаторівневої моделі. Площина даних передбачає перевірку цілісності отриманих даних, відповідність формату даних, перевірку на аномалії в даних та відсіювання зайвого. Площина керування відповідає за реплікацію операційних та архівних сховищ, розмежування доступу до даних згідно встановлених політик доступу, шифрування даних, аудит змін, логування дій та доступність даних, що є важливим для будь-якої компанії. Застосування такої моделі має забезпечити доступність, цілісність та конфіденційність інформації. Також використання механізмів для кореляції подій дозволяє поєднувати аномалії, що виявленні в різних ділянках

мережі та спрацювання тригерів формуючи цілісну картину та уявлення про інцидент вказуючи на його можливу першопричину. Такий комплексний підхід створює адаптивне середовище безпеки, у якому система здатна автоматично реагувати на загрози та підтримувати стабільність роботи корпоративної комп'ютерної мережі компанії.

3.4 Приклад застосування інтелектуальної системи моніторингу.

Для прикладу застосування інтелектуальної системи моніторингу візьмемо за приклад компанію "Interactive Games". Interactive Games – це компанія, що займається розробкою ААА-ігор та забезпечує можливість грати онлайн у свої проєкти. Також ця компанія займається розробкою сервісів та програм для створення модифікацій, різної атрибутики для ігор та навчальних ресурсів. Мережева інфраструктура компанії складається з декількох регіональних офісів серед яких головний офіс, дата-центр та резервний дата-центр для відновлення важливої інформації. Також активно використовуються хмарні технології. Сама мережа в будь-якому з офісів чи дата-центрі складається з трьох рівнів: рівень доступу, рівень розподілу та рівень ядра. Така мережа використовує кореневі комутатори, роутери, комутатори розподілу та доступу, фаєрволи та інші безпекові пристрої. Така архітектура дозволяє забезпечити масштабованість, відмовостійкість та надійність (див. рис. 3.7).

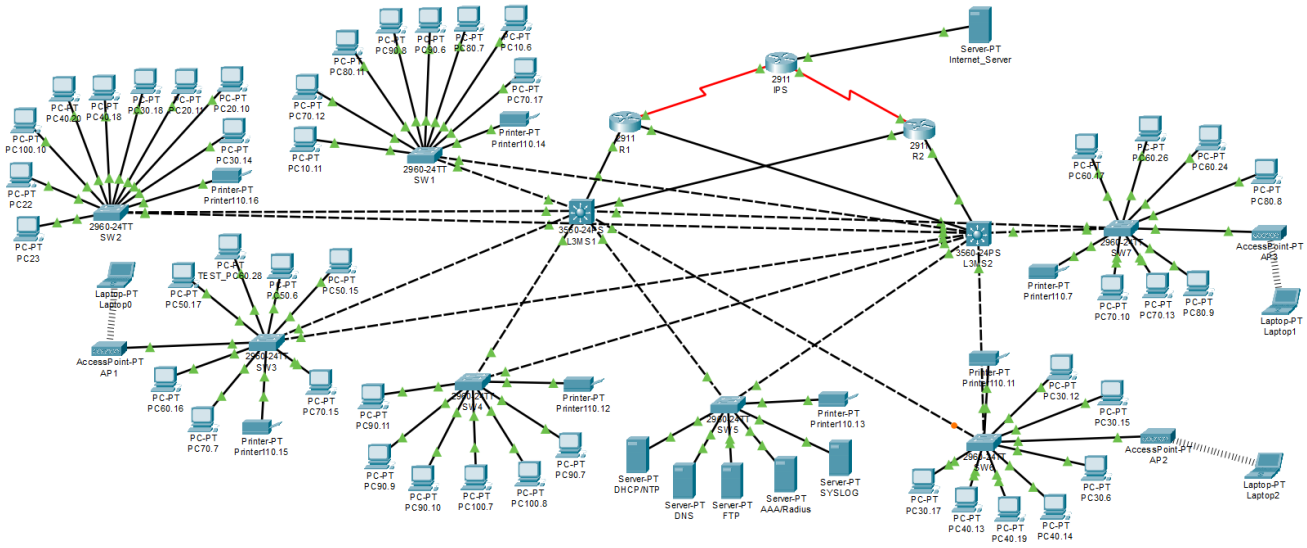


Рисунок 3.7 – Модель мережі одного з офісів компанії

Проте з огляду на її складність та масштаб компанії в цій мережі генерується великий обсяг трафіку й даних. З розвитком компанії та більшим попитом на її продукт зростає потреба в кращій та більш автоматизованій системі, яка здатна швидко реагувати та виявляти інциденти надаючи рекомендації з покращення та може працювати в умовах необхідності оперативних дій. Описана інтелектуальна система моніторингу здатна вирішити наступні речі:

1. Скорочення часу виявлення інцидентів (MTTD) – впровадження автоматичного аналізу повідомлень, що дозволить виявляти проблеми в реальному часі та на початкових стадіях.
2. Зменшення часу реагування (MTTR) – використання написаних скриптів та протоколів дій у разі виявлення критичних несправностей або проблем та формування рекомендацій з покращення. Це дозволить швидше усувати несправності та проблеми, які потребуватимуть втручання спеціалістів.
3. Прогнозування можливих несправностей чи збоїв на основі знань про мережу.
4. Розвантаження служби підтримки, що дозволить більше зосередитися на важливих аспектах роботи.

Таким чином застосування інтелектуальної системи моніторингу дозволить підвищити ефективність роботи мережі компанії, вивільнить ресурси співробітників для складніших та нагальних задач, зменшить час та кількість простоїв та покращить якість обслуговування.

Для демонстрації, як може працювати інтелектуальна система моніторингу проведемо симуляцію за допомогою Cisco Packet Tracer та згенеруємо штучно необхідні системні сповіщення, що будуть схожі на реальну ситуацію. Під час роботи мережі приходить повідомлення від системи про падіння порту на комутаторі третього рівня, втрату сусідства за протоколом OSPF з іншим комутатором, надмірне завантаження CPU та виявлення петлі STP (див. рис. 3.8).

```
%LINK-3-UPDOWN: Interface Gi1/0/24, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Gi1/0/24, changed state to down
%OSPF-5-ADJCHG: Process 1, Nbr 172.16.205.4 on Vlan205 from FULL to DOWN, Neighbor Down
%CPU-4-HIGHCPU: CPU utilization reached 92% for 60 seconds
%SPANTREE-2-LOOPGUARD: Loop detected on interface Gi1/0/2
```

Рисунок 3.8 – Приклад повідомлення системи про проблеми

Ці події відповідають сценарію коли в годину пікового використання ресурсів компанії користувачі помічають затримки та розриви з’єднання. Маючи системні повідомлення можна проаналізувати та зрозуміти де саме несправність. Користувачі помічали затримки та розриви з’єднання через час, що необхідний аби перевести трафік на інші канали. Проте навантаження на резервні канали тепер

зросло. Розглянемо поведінку інтелектуального модуля в інтелектуальній системі моніторингу.

Ситуація №1: В площині даних модуль збору даних отримує системне повідомлення про проблему в мережі та спрацювання тригера завантаженості процесора. Отримана інформація відправляється в модуль операційного сховища для обробки попередньо пройшовши нормалізацію в модулі попередньої обробки. Далі відбувається обробка даних модулем обробки та візуалізації разом з обробкою даних інтелектуальним модулем системи (ІМС). Оброблені дані виводяться на інформаційну панель та модуль ІМС генерує звіт про подію після чого дані відправляються в сховище даних для зберігання та відбувається оцінка й аудит дій ІМС. Інтелектуальний модуль системи обробляючи дані проводить наступні дії:

1. Класифікація подій. ІМС обробляє кожне повідомлення та визначає до якої категорії воно відноситься, наприклад: апаратна помилка, проблеми з каналами зв’язку, зміна конфігурації, можлива або потенційна атака тощо. Для цього переглядаються ознаки даних які отримані при нормалізації даних.
2. Виявлення можливої причини. На основі бази даних та розуміння, що відбувалося до цього система оцінює ймовірні причини та включає їх у звіт, наприклад: протягом 1 години відбувалися перебої з живленням, порт комутатора час від часу вимикався, процесор працював з підвищеним навантаженням, відбувалися помилки маршрутизації тощо.
3. Прогнозування можливого впливу. Модуль виконує аналіз залежності між проблемною ділянкою та іншими сегментами мережі й формує повідомлення у звіт про можливий вплив на сервіси чи мережу.
4. Формування звіту з рекомендаціями. Після завершення аналізу та усунення або не усунення інциденту формується звіт з детальною інформацією про проблему, можливий вплив, рішення та рекомендації на майбутнє.

В площині керування відбувається керування процесами в площині даних, перевірка відповідності політикам, аудит та контроль безпеки, наповнення бази знань та навчання ІМС за потреби.

На прикладі наведеного системного повідомлення система згенерує звіт про цей інцидент (див. рис. 3.9). Такий формат звіту дозволяє спростити пошук несправності, розуміння проблеми та можливого впливу на систему. Дані про налаштування мережі, топологію та назви беруться з її конфігурації, яка завантажена в систему у вигляді конфігураційних даних.

Звіт про інцидент № 24578 від 14:03

- **Обладнання:** L3MS1 (ядро мережі)
- **Подія:** падіння інтерфейсу Gi1/0/24 і втрата сусідства OSPF з R1 на VLAN205
- **Критичність:** висока
- **Опис:** Обладнання зафіксувало зміну стану інтерфейсу на down. OSPF-сусідство перейшло до стану DOWN. Рівень завантаження CPU на L3MS1 сягнув 92 %, а протокол STP виявив петлю на сусідньому комутаторі.
- **Ймовірні причини:** фізичне відключення кабелю; збій живлення; петля STP, що спричинила Broadcast Storm; перевантаження процесора через аномальний трафік.
- **Прогнозований вплив:** зростання затримки і втрати пакетів для клієнтів; можливе відключення серверів у VLAN 140 та 150; ризик недоступності авторизаційного сервісу.
- **Рекомендації:**
  1. Перевірити фізичний стан порту Gi1/0/24 на комутаторі SW1.
  2. Аналізувати журнали живлення для Power Supply 1, щоб усунути відмову.
  3. Переглянути STP-топологію, ізолювати сегмент із петлею та усунути її.
  4. Перевірити процеси на маршрутизаторі L3MS1, що спричинили високе завантаження CPU, і оптимізувати конфігурацію.
- **Прогноз:** ймовірність повторної відмови протягом 15 хвилин — 78 %.

Рисунок 3.9 – Приклад згенерованого звіту на Ситуацію №1

Ситуація №2: Під час роботи користувачів з внутрішнім веб-сайтом було помічено втрату доступу. На інформаційну панель надійшли сповіщення про недоступність веб-сайту та порушення політик доступу. Згодом почали надходити скарги від користувачів про блокування їх роботи через недоступність веб-сервісу (див. рис. 3.10-11).

```
%ACL-4-DENY: Inbound TCP connection denied from 172.16.20.14 to 172.16.140.10 on port 80
%ACL-4-DENY: Inbound TCP connection denied from 172.16.70.45 to 172.16.140.10 on port 443
%HTTP-3-ACCESS: Web service unreachable (172.16.140.10)
%SYS-5-CONFIG_I: ACL USER-POLICY modified by admin
```

Рисунок 3.10 – Приклад системного повідомлення про зміни та помилки



Рисунок 3.11 – Приклад системного повідомлення про помилки

Модуль IMC починає обробку даних відповідно до алгоритму роботи площини даних та площини керування. Для початку він фіксує велику кількість deny-подій, які свідчать про відхилення доступу до ресурсу. Після нормалізації даних модуль класифікує тип події та починає аналізувати конфігурацію доступу (ACL, Access Control List) та чи проводилися зміна конфігурації. Після аналізу IMC визначає, що були внесені зміни в конфігурацію, що й спричинило недоступність веб-сайту. Після проведеної роботи генерується звіт в якому детально зазначається, що сталося, причина, вплив та рекомендації з вирішенням (див. рис. 3.12).

Звіт про інцидент № 58373 від 11:26

Обладнання: L3MS1 (ядро мережі)

Подія: блокування трафіку користувачів VLAN20, VLAN70 і VLAN80 до серверного сегмента VLAN140 через зміну ACL USER-POLICY

Критичність: середньо-висока

Опис:
Система зафіксувала різке збільшення кількості відхилених з'єднань (ACL-DENY) при зверненні користувачів до серверів у VLAN140. Логи показали, що одразу перед появою помилок відбулася зміна конфігурації (CONFIG_I). Аналіз виявив, що у списку контролю доступу USER-POLICY правило **deny ip any 172.16.0.0/16** було розташоване вище за дозволяючі правила доступу до серверного сегмента. У результаті весь міжвлановий трафік, включно з раніше дозволеними потоками, був заблокований.

Ймовірні причини: неправильне впорядкування правил ACL; помилка адміністратора під час модифікації USER-POLICY; відсутність внутрішньої перевірки конфігурації перед застосуванням; некоректне тестування політик доступу.

Прогнозований вплив:

- повна недоступність веб-сервісів у VLAN140 для користувачів VLAN20, VLAN70 та VLAN80;
- порушення бізнес-процесів відділів продажів, маркетингу та підтримки;
- помилки авторизації і неможливість підключення до внутрішніх інформаційних систем;
- можливі скарги зовнішніх клієнтів у разі залежності сервісів.

Рекомендації:

- Переглянути структуру ACL USER-POLICY та повернути дозволяючі правила у верхню частину списку.
- Відновити попередню версію ACL із системи контролю конфігурацій (Git/Backup).
- Упровадити контроль зміни правил доступу через інтелектуальний модуль моніторингу.
- Виконувати тестування ACL у спеціальному середовищі перед внесенням у продуктивну мережу.

Прогноз: ймовірність повторної помилки конфігурації протягом 30 хвилин за відсутності змін — **56 %**.

Рисунок 3.12 – Приклад згенерованого звіту на Ситуацію №2

Ситуація №3: Під час роботи користувачів з внутрішніми сервісами компанії було помічено тимчасову недоступність сервісів, втрата доступу до 1 хв, а потім повну недоступність сервісів компанії. На інформаційну панель почали надходити сповіщення про недоступність сервісу, порушення політик доступу та кількість сповіщень про порушення політик доступу тільки зростала (див. рис. 3.13).

```
%SW-4-EXCESSIVEARP: Interface Fa0/12 exceeded ARP rate threshold
%STORM-2-TRAFFIC: Broadcast storm detected on VLAN130
%PORTSEC-3-INVALIDSRC: Security violation detected on port Fa0/12
%CPU-4-HIGHCPU: CPU utilization reached 98% for 30 seconds
%ACL-4-DENY: Inbound connection denied from 172.16.130.52 to 172.16.140.10
%HTTP-3-ACCESS: Internal web service is unreachable (172.16.140.10)
```

Рисунок 3.13 – Приклад системного повідомлення про проблеми

Модуль IMC отримавши дані почав одразу діяти застосувавши модуль оперативного реагування, оскільки було зафіксовано спрацювання критичного тригера та аномальну активність. В ході аналізу цього інциденту було виявлено, що в гостьовій Wi-Fi мережі (Vlan130) почався ARP-флуд та розсилка широкомовного трафіку, що викликав навантаження на обладнання та перевантаження комутаторів. Разом з тим були спроби отримати доступ до кожної частини мережі через сканування портів мережі. Система безпеки почала фіксувати велику кількість порушення політик безпеки на портах. Оперативно відреагувавши на інцидент модуль IMC почав аналіз цього інциденту та складання звіту (див. рис. 3.14).

Звіт про інцидент № 60166 від 15:22

Обладнання: SW1 (комутатор доступу)

Подія: ARP-флуд і broadcast-шторм у VLAN130, що спричинили перевантаження комутатора та деградацію сусідніх VLAN

Критичність: Висока

Опис:
Система зафіксувала різке зростання кількості ARP-запитів та широкомовного трафіку у VLAN130. На порту Fa0/12 зареєстровано порушення політики port-security. Завантаження процесора SW1 сягнуло 98 %, що призвело до затримок обробки трафіку та часткової деградації VLAN120 і серверного сегмента VLAN140. ACL-політики заблокували спроби доступу до корпоративних ресурсів, проте сам обсяг трафіку спричинив порушення роботи внутрішнього веб-сайту.

Ймовірні причини:
аномальна активність або DoS-атака з боку пристрою користувача; зараження пристрою шкідливим ПЗ; ARP-spoofing; некоректна робота WiFi-клієнта; traffic-generator у гостьовій мережі.

Прогнозований вплив:

- тимчасова недоступність внутрішнього веб-сайту;
- зростання затримки у VLAN120 і VLAN130;
- ризик подальшого перевантаження SW1;
- можливість виникнення STP-аномалій при ускладненні флуду.

Рекомендації:

- Вимкнути порт Fa0/12 та ідентифікувати пристрій, що генерує аномальний трафік.
- Активувати контроль широкомовного трафіку (storm-control) у VLAN130.
- Переглянути політики безпеки на гостьових SSID та посилити фільтрацію.
- Провести аудит логів точок доступу та перевірити пристрої, що працюють у WiFi Guest.

Прогноз: ймовірність повторного ARP-шторму протягом 1 години — 78 %.

Рисунок 3.14 – Приклад згенерованого звіту на Ситуацію №3

Наведені приклади можливих інцидентів демонструють ключові переваги використання інтелектуальної системи моніторингу замість класичної системи моніторингу у великих корпоративних мережах. Запропонована система з інтелектуальним модулем не тільки фіксує події, але й аналізує їх у контексті інфраструктури, вивчає передумови, визначає причини інцидентів, оперативно реагує на критичні спрацювання та надає рекомендації з усуненню формуючи детальний звіт про проблему. Використання такої системи здатне зменшити час виявлення проблем, зменшити час на їх реагування, виявити помилки конфігурації чи слабкі місця, виправляти частину помилок або проблем в режимі реального часу, запобігання або зменшення шкоди від атак на мережу, допомога та підвищення ефективності роботи IT-відділу компанії: системні адміністратори, мережеві інженери, програмісти, фахівці з кібербезпеки.

Проведене моделювання демонструє, що інтелектуальна система моніторингу здатна забезпечити значно вищий рівень аналізу та реагування на збої чи інциденти в мережі порівняно з традиційними системами моніторингу. Інтелектуальний модуль не тільки фіксує інциденти, а й розглядає їх в контексті мережевої конфігурації, взаємозв'язків між сервісами та аномаліями. Це дає змогу швидко встановлювати причини відмов, прогнозувати можливі ризики та формувати рекомендації для їх усунення або попередження подібних проблем у майбутньому. Згенеровані тестові сценарії показують принцип та приклад реагування інтелектуального модуля. Таким чином інтеграція інтелектуального модуля здатна підвищити ефективність моніторингу, спостережуваності, скоротити час простоїв та мінімізувати наслідки потенційних інцидентів у корпоративних мережах.

3.5 Проблеми використання інтелектуальної системи моніторингу комп'ютерної мережі та перспективи розвитку.

Враховуючи всі можливі переваги та перспективи розвитку наведеної інтелектуальної системи моніторингу необхідно зазначити її недоліки та проблеми експлуатації. Дана система моніторингу матиме наступні проблеми експлуатації та недоліки:

1. Вимогливість до ресурсів.
2. Складний процес налаштування.
3. Підходить лише для великих комп'ютерних мереж.
4. Безпека даних.
5. Висока ціна підписки та плата за додаткові можливості.
6. Великий час провадження та навчання.

Вимогливість до ресурсів полягає у потребі виділення окремого сервера в мережі для повноцінної роботи інтелектуального модуля та зберігання даних. Для ефективної роботи такої системи необхідно виділити ресурси для її роботи та навчання. Найкращим шляхом буде розгортання модуля ІМС на окремо виділеному сервері для уникнення проблем з роботою інших сервісів компанії, якби вона була розгорнута на одному сервері з іншими сервісами. Виділення окремого серверу є дорого вартісною задачею та збільшує затрати на експлуатацію. У випадку, якщо розгортати на віддаленому сервері використовуючи хмарні технології є ризики затримки реагування або непрацездатності ІМС у випадку атаки на мережу, оскільки дані про помилки та команди для реагування не зможуть дійти. Також постає ризик засвітити дані про мережу в глобальній мережі інтернет, що є великим мінусом.

Складний процес налаштування такої системи полягає в її модульності, тонкощах налаштування роботи інтелектуального модуля системи, надані прав, інструкцій, спеціально підготовлених скриптів для реагування, навчальної бази та навчання. Для початку автономної роботи інтелектуального модуля повинно пройти його навчання на реальній мережі, вивчення конфігурації та обладнання, вивчення навчальної бази, відпрацювання тестових та навчальних сценаріїв й контроль за його роботою. Це є складним та тривалим процесом перш ніж буде досягнуто бажаного ефекту.

Дана система моніторингу підходить лише для великих компаній де є потреба в автоматизації, стабільності роботи, відмовостійкості, зменшення витрат на обслуговування та підвищення її ефективності. Оскільки дана система потребуватиме значних витрат, досягнути максимального рівня ефективності вона зможе саме у великій компанії.

Безпека даних. Питання безпеки даних є ключовим фактором у використанні інтелектуальної системи моніторингу. Система оперує великою кількістю внутрішніх даних серед яких відомості про топологію, конфігурацію, поточний стан мережі, що робить її потенційно привабливою ціллю для зловмисників. Важливо враховувати, на яких даних відбувається навчання інтелектуального модуля. Будуть використовуватися локально зібрані дані, дані тестової мережі або мереж розробника або агреговані дані інших клієнтів. Це створює ризики несанкціонованої передачі частини або всієї внутрішньої інформації, що здатне серйозно вплинути на конфіденційність та роботу корпоративної мережі компанії. Крім того, у випадках використання хмарних сервісів в інфраструктурі корпоративної мережі можливе виникнення затримок у реагуванні під час інцидентів або навіть часткова недоступність ІМС у разі мережевих атак. Отже будь-які перебої у з’єднанні між локальною інфраструктурою та хмарною інфраструктурою можуть унеможливити роботу ІМС, що може призвести до зменшення рівня захисту та швидкості реагування. Водночас впровадження

жорстких політик безпеки та обмеження свободи системи підвищують захищеність, але водночас зменшують ефективність алгоритмів навчанні та роботи.

Висока вартість підписки та додаткових можливостей. Використання інтелектуальної системи моніторингу передбачає комплекс витрат, що включають в себе: вартість самої системи, технічної підтримки, придбання оновлень, активація ліцензій, закупівля додаткових функцій та модулів. Чим більша інтеграція з різними сервісами, модернізація або розширення мережі тим більша вартість обслуговування. До цих витрат також варто врахувати витрати на оренду або закупівлю додаткового обладнання для функціонування ІМС, що збільшує витрати на експлуатацію. Для великих компаній даний рівень витрат може бути прийнятним, проте для малих або середніх компаній це є бар'єром для впровадження.

Великий час впровадження та навчання. Тривалий час впровадження даної системи зумовлений необхідністю детального налаштування мережі, систематизації документів про мережу, підготовку конфігурацій обладнання, написання інструкцій або скриптів та проведення початкового навчання ІМС. Для досягнення стабільної та коректної роботи ІМС потрібно виконати наступні етапи:

1. Збір та аналіз даних про мережу.
2. Формування навчальної бази.
3. Тестування системи на контрольних сценаріях.
4. Поступове впровадження в реальне середовище.
5. Навчання персоналу роботі та підтримці інтелектуальної системи моніторингу.

Окрім цього, протягом перших місяців використання цієї системи необхідний постійний моніторинг роботи ІМС, коригування та виправлення помилок в роботі. Такий підхід забезпечить високу якість роботи але потребує значних ресурсів.

Перспективи розвитку інтелектуальної системи комп'ютерної мережі:

1. Оптимізація інфраструктури.
2. Розвантаження та підвищення ефективності роботи ІТ-відділу компанії.
3. Підвищення рівня відмовостійкості, надійності мережі та роботи компанії.
4. Економія коштів в майбутньому.
5. Інтеграція в систему захисту мережі від кіберзагроз.

Оптимізація інфраструктури полягає у знаходженні слабких місць, надмірної надлишковості або вузьких місць під час вивчення конфігурації мережі, топології, файлів конфігурації обладнання та роботи інтелектуального модуля з мережею. Обробивши ці дані інтелектуальний модуль Здатний згенерувати рекомендації щодо оптимізації маршрутизації, зменшення надмірної надлишковості, покращення конфігурації обладнання вказавши на недоліки, перерозподіл

навантаження та модернізації критичних елементів. Таким чином, інтелектуальна система моніторингу сприятиме побудові оптимальної та збалансованої інфраструктури.

Розвантаження та підвищення ефективності ІТ-відділу компанії буде досягнуто за рахунок автоматизації рутинних процесів, які уповільнюють та відволікають від основної роботи та важливих задач. Такими процесами є:

1. Збір та систематизація даних.
2. Первинний аналіз інцидентів.
3. Генерація звітів.
4. Виконання стандартних сценаріїв оперативного реагування.
5. Виявлення повторюваних помилок та аномалій.

Це дозволить зосередитися на складніших та стратегічних задачах з модернізації та покращення інфраструктури й забезпечення надійності та ефективності роботи корпоративної мережі.

Підвищення рівня відмовостійкості та надійності мережі. Це досягається шляхом покращеної спостережуваності, моніторингу, оперативного реагування на інциденти та збої, аналізу та встановлення першопричин та оптимізацією інфраструктури. Це дозволяє краще налаштувати роботу, зменшити затримки, досягнути більшого рівня ефективності при наявній інфраструктурі та зробити більш точну модернізацію інфраструктури. Доступність та стабільність роботи продуктів та сервісів компанії буде вище за рахунок підвищення рівня відмовостійкості та надійності мережі зумовлених роботою ІМС.

Економія коштів. Економія коштів полягає у рентабельності витрат на інфраструктуру, які будуть потенційно меншими шляхом оптимізації інфраструктури, правильному розподіленню навантаження та підвищення ефективності роботи мережі.

Інтеграція в систему захисту мережі від кіберзагроз. Інтелектуальний модуль може бути інтегрований в системи кіберзахисту або на його основі буде розроблено спеціалізований модуль для виявлення та попередження атак. Таких підхід здатен забезпечити виявлення аномальної активності, яка є характерною для мережевих атак, виявляти ознаки сканування мережі, виявляти нетипові зміни конфігурації, попереджати про виявлені вразливості та пом’якшувати вплив та можливі наслідки атаки на мережу.

Було детально розглянуто концепцію застосування нейронних мереж в системах моніторингу комп’ютерної мережі, архітектуру побудови та роботи, практичні аспекти застосування, переваги та недоліки. Практичний аспект був продемонстрований на прикладі згенерованих системних повідомлень, які були оброблені системою моніторингу з нейронною мережею у якості інтелектуального

модуля та представлені приклади звітів про інциденти та покращення від цього модулю. Отримані дані та розглянута концепція демонструє можливості покращити рівень моніторингу, спостережуваності, надійності, відмовостійкості та ефективності роботи мережі.

Передусім було розглянуто сучасні тенденції розвитку корпоративних мереж для яких характерне стрімке зростання обсягів даних, розосередження інфраструктури, використання хмарних технологій та підвищення рівня складності. За таких умов класична система моніторингу не здатна в повному обсязі надати моніторинг та спостереження, оскільки ґрунтуються на статичних правилах та ручному втручанні. Це знижує ефективність їх використання в майбутньому та здатність реагувати на нові виклики.

Запропонована в роботі архітектура інтелектуальної системи моніторингу спроможна усунути ці недоліки шляхом впровадження дворівневого підходу за допомогою площини даних та площини керування з інтеграцією інтелектуального модуля зробленого з використанням нейронної мережі. Такий підхід дозволяє виконувати нормалізацію даних, багаторівневий збір інформації, оперативне реагування, аналіз причин, наслідків та встановлення причинно-наслідкового зв’язку, завдяки якому система здатна визначити першопричину проблеми та надати детальний звіт з рекомендаціями замість простої реєстрації симптомів. Ця система матиме модуль аудиту та оцінки ефективності, що дозволить контролювати дії інтелектуального модуля, оцінювати ефективність спрацювання та навчати за потреби для покращення роботи модуля IMC.

Наведені демонстраційні приклади були зроблені за допомогою мережі, що побудована в Cisco Packet Tracer та згенеровані на основі справжніх повідомлень Cisco IOS. Вони демонструють результати аналізу та звітності інтелектуального модуля та результатів його роботи. Це дозволяє показати переваги впровадження нейронної мережі в систему моніторингу Продемонстровані приклади показують можливі реальні ситуації з падінням інтерфейсів, втрати зв’язку між комутаторами, помилок в ACL-політиках, DoS-активністю у мережі, велике завантаження обладнання тощо.

Також важливим компонентом є здатність системи до оперативного реагування у критичних ситуаціях використовуючи написані спеціалістами скрипти для дій, що дозволяє зменшити потенційний вплив від атаки або критичних збоїв, здатність системи до аналізу мережі, знаходження вразливостей або надлишковості, що дозволяє оптимізувати та підвищити надійність мережі.

Таким чином можна стверджувати, що застосування нейронної мережі у якості інтелектуального модулю в системі моніторингу є ефективним та перспективним інструментом для сучасних корпоративних мереж, де класичні системи можуть не справлятися з обсягом навантаження та масштабом через що, старі системи можуть

працювати неефективно. Також це здатне підвищити стабільність роботи, надійність та відмовостійкість в критичних ситуаціях.

Висновки

Будь-яка корпоративна комп’ютерна мережа потребує належного рівня обслуговування, підтримки та контролю. Цей контроль та підтримка забезпечуються за допомогою спостережуваності та моніторингу мережі. Зі зростанням масштабів мережі, кількості сервісів, користувачів та розосередженості інфраструктури завдяки використанню хмарних технологій зростає складність самої мережі через що традиційні системи моніторингу можуть не справлятися з навантаженням. Традиційні системи моніторингу покладаються на статичні правила та не можуть забезпечити належний рівень контролю під зростаючі вимоги. При таких умовах виникає потреба у впровадженні інтелектуальних систем моніторингу здатних проводити аналіз подій, встановлювати причино-наслідкові зв’язки, реагувати на критичні ситуації, прогнозувати вплив та пропонувати рішення з покращенню мережі.

У процесі виконання магістерської роботи було дослідженні сучасні тенденції розвитку систем моніторингу, комп’ютерних мереж, підходи до їх експлуатації. Розглянуто архітектури систем моніторингу, методи збору інформації та інтеграцій. Описано інтелектуальну систему моніторингу, її архітектуру, складові, взаємодію функціональних елементів (модулів). Описано архітектуру інтелектуальної системи моніторингу мережі з інтелектуальним модулем та спроєктовано модель мережі для симуляції помилок й отримання системних повідомлень, що було використано для створення сценаріїв збоїв в мережі та демонстрації роботи інтелектуального модуля системи моніторингу мережі. Описані результати та використання такого підходу дозволяє знизити час виявлення інцидентів (MTTD), час реагування та підвищити рівень діагностики та контролю. Важливим аспектом є те, що інтелектуальний модуль здатен працювати не тільки з подіями, а й з конфігураціями обладнання, документацією мережі, що дозволяє виявляти та усувати проблемні місця раніше чим вони стануть проблемою та покращувати ефективність роботи. На основі цього було продемонстровано приклад формування звіту та аналізу збоїв, інцидентів тощо.

Проведене дослідження показує, що використання інтелектуальних систем моніторингу є актуальним та перспективним напрямком розвитку. Це відповідає сучасним тенденціям та прогнозам розвитку. Попри наявність труднощів на етапах реалізації пов’язаних з вимогою до ресурсів, кваліфікації персоналу та безпековому факторі, вплив такої системи на стабільність, продуктивність та безпеку є суттєвим.

Інвестиції в розвиток подібних інтелектуальних систем або модернізацію існуючих систем моніторингу, розширенням можливостей, самонавчання та глибшу

кореляцію подій є необхідним кроком, який сприятиме покращенню й фінансовій рентабельності внесених інвестицій в комп’ютерну мережу.

Результати цієї роботи підтверджують доцільність використання інтелектуальних систем моніторингу у корпоративних мережах, демонструють їх можливу ефективність у практичних сценаріях та підкреслюють важливість подальшого розвитку цього напрямку.

Список використаних джерел

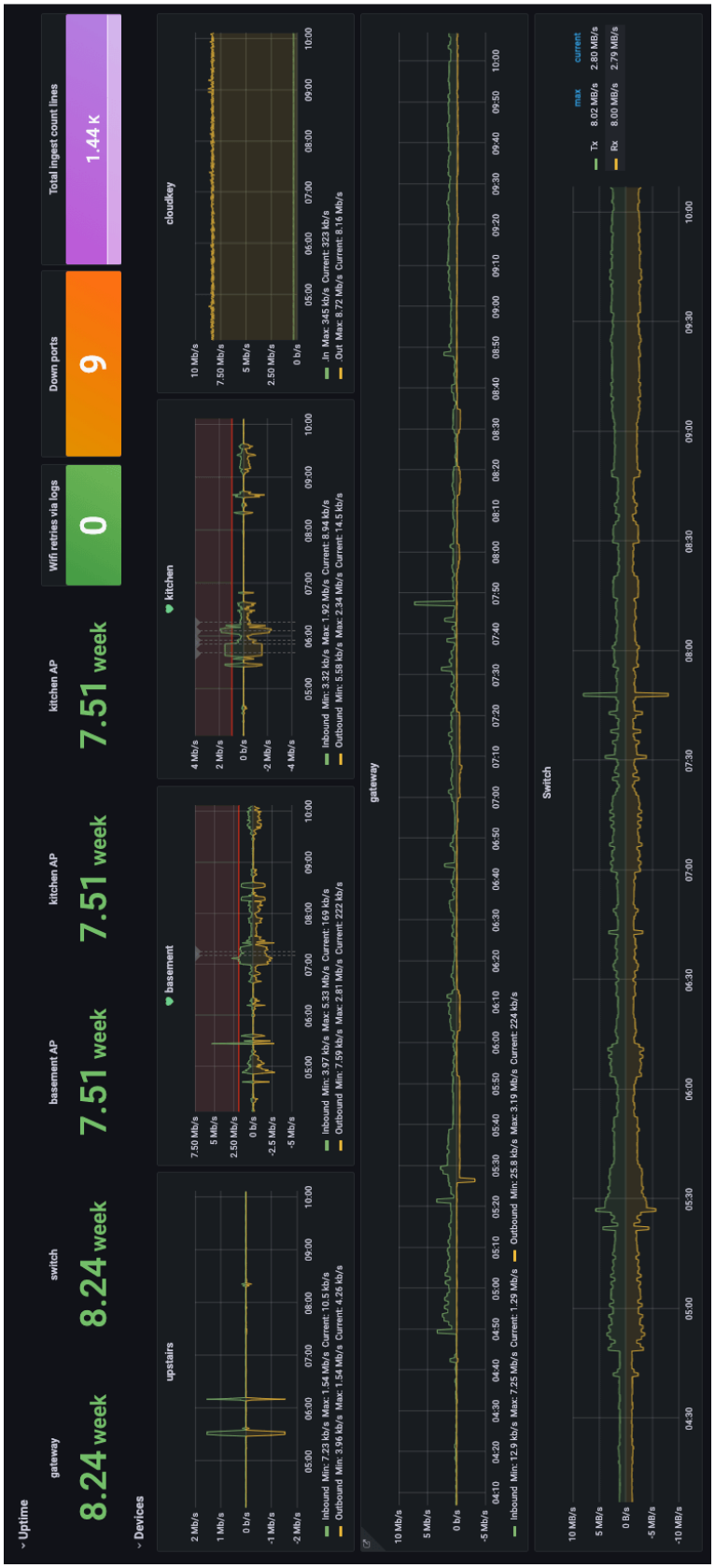
1. IBM. What Is Computer Networking? | IBM. IBM. URL: https://www.ibm.com/think/topics/networking (дата звернення: 02.09.2025).
2. IBM Power System E1080 Server (9080-HEX). IBM. URL: https://www.ibm.com/docs/en/power10/9080-HEX?topic=adapters-network-requirements (дата звернення: 02.09.2025).
3. Peer-To-Peer Networks: Features, Pros, and Cons - Spiceworks. Spiceworks Inc. URL: https://www.spiceworks.com/networking/what-is-peer-to-peer/ (дата звернення: 02.09.2025).
4. GeeksforGeeks. What is P2P (Peer-to-Peer Process)? - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/computer-networks/what-is-p2p-peer-to-peer-process/ (дата звернення: 02.09.2025).
5. Client-Server Network: Understanding, Functions, and Services. FS.com. URL: https://www.fs.com/blog/a-guide-to-understanding-clientserver-network-6976.html (дата звернення: 02.09.2025).
6. Zenarmor. What is Client-Server Network? Definition, Advantages, and Disadvantages - zenarmor.com. Zenarmor - Agile Service Edge Security. URL: https://www.zenarmor.com/docs/network-basics/what-is-client-server-network (дата звернення: 02.09.2025).
7. Logical vs. Physical Network Diagrams - DNSstuff. Software Reviews, Opinions, and Tips - DNSstuff. URL: https://www.dnsstuff.com/physical-logical-network-diagram (дата звернення: 02.09.2025).
8. AI Infrastructure, Secure Networking, and Software Solutions - Cisco. URL: https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Small_Enterprise_Design_Profile/chap2sba.pdf (дата звернення: 12.09.2025).
9. Susnjara S., Smalley I. What Is Virtualization? | IBM. IBM. URL: https://www.ibm.com/think/topics/virtualization (дата звернення: 12.09.2025).
10. What is a Hypervisor?. VMware by Broadcom - Cloud Computing for the Enterprise. URL: https://www.vmware.com/topics/hypervisor (дата звернення: 12.09.2025).
11. What Is a Hypervisor? Definition, Types, and Capacities - GigaCloud. GigaCloud. URL: https://gigacloud.ua/en/articles/shho-take-gipervizor-vyznachennya-typy-ta-mozhlyvosti/ (дата звернення: 12.09.2025).
12. GeeksforGeeks. Hypervisor - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/system-design/hypervisor/ (дата звернення: 12.09.2025).
13. z/VM. IBM. URL: https://www.ibm.com/docs/en/zvm/7.2.0?topic=options-virtual-switch (дата звернення: 12.09.2025).

14. China C. R., Goodwin M. Iaas, Paas, Saas: What's the difference? | IBM. IBM. URL: https://www.ibm.com/think/topics/iaas-paas-saas (дата звернення: 12.09.2025).
15. IBM. What is Network Monitoring? | IBM. IBM. URL: https://www.ibm.com/think/topics/network-monitoring (дата звернення: 12.09.2025).
16. Zabbix: The enterprise-class open source observability solution. Zabbix: The enterprise-class open source observability solution. URL: https://www.zabbix.com/ (дата звернення: 12.09.2025).
17. Nagios: Free Open Source IT Monitoring Tools. Nagios Open Source. URL: https://www.nagios.org/ (дата звернення: 12.09.2025).
18. Prometheus - Monitoring system & time series database. Prometheus - Monitoring system & time series database. URL: https://prometheus.io/ (дата звернення: 12.09.2025).
19. Observium. Observium. URL: https://www.observium.org/ (дата звернення: 12.09.2025).
20. Network Performance Monitor - Observability Self-Hosted. Observability, Database, and IT Service Management | SolarWinds. URL: https://www.solarwinds.com/network-performance-monitor (дата звернення: 12.09.2025).
21. What is Datadog?. Uptrace. URL: https://uptrace.dev/glossary/what-is-datadog (дата звернення: 12.09.2025).
22. Digital 2024: Global Overview Report – DataReportal – Global Digital Insights. DataReportal – Global Digital Insights. URL: https://datareportal.com/reports/digital-2024-global-overview-report?rq=Global%20Overview%20Report%202024 (дата звернення: 19.09.2025).
23. Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper. Cisco. URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (дата звернення: 12.09.2025).
24. Global Cybersecurity Outlook 2024. World Economic Forum. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2024/ (дата звернення: 19.09.2025).
25. AI Network Monitoring 2025: Transform Enterprise Operations with Intelligent Automation. Communications & Payment Systems Management Solutions | IR. URL: https://www.ir.com/guides/ai-network-monitoring-2025-transform-enterprise-operations-with-intelligent-automation#:~:text= (дата звернення: 19.09.2025).
26. Що таке SOAR? Технології та рішення | Захисний комплекс Microsoft. Microsoft – AI, Cloud, Produktivität, Computing, Gaming und Apps. URL:

https://www.microsoft.com/uk-ua/security/business/security-101/what-is-soar (дата звернення: 19.09.2025).

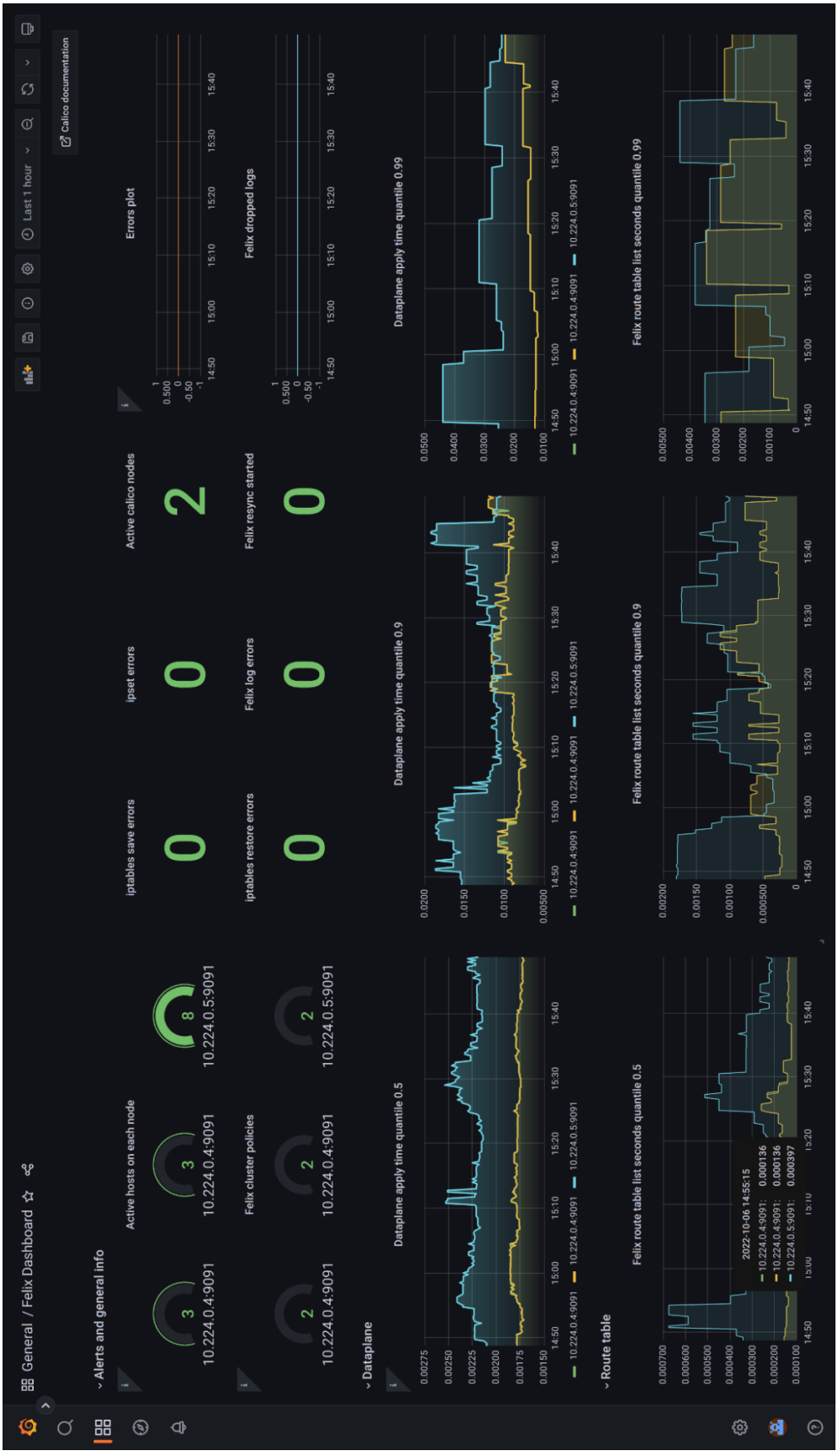
Додаток А

Відображення статусу комутатора та портів в Prometheus з Grafana



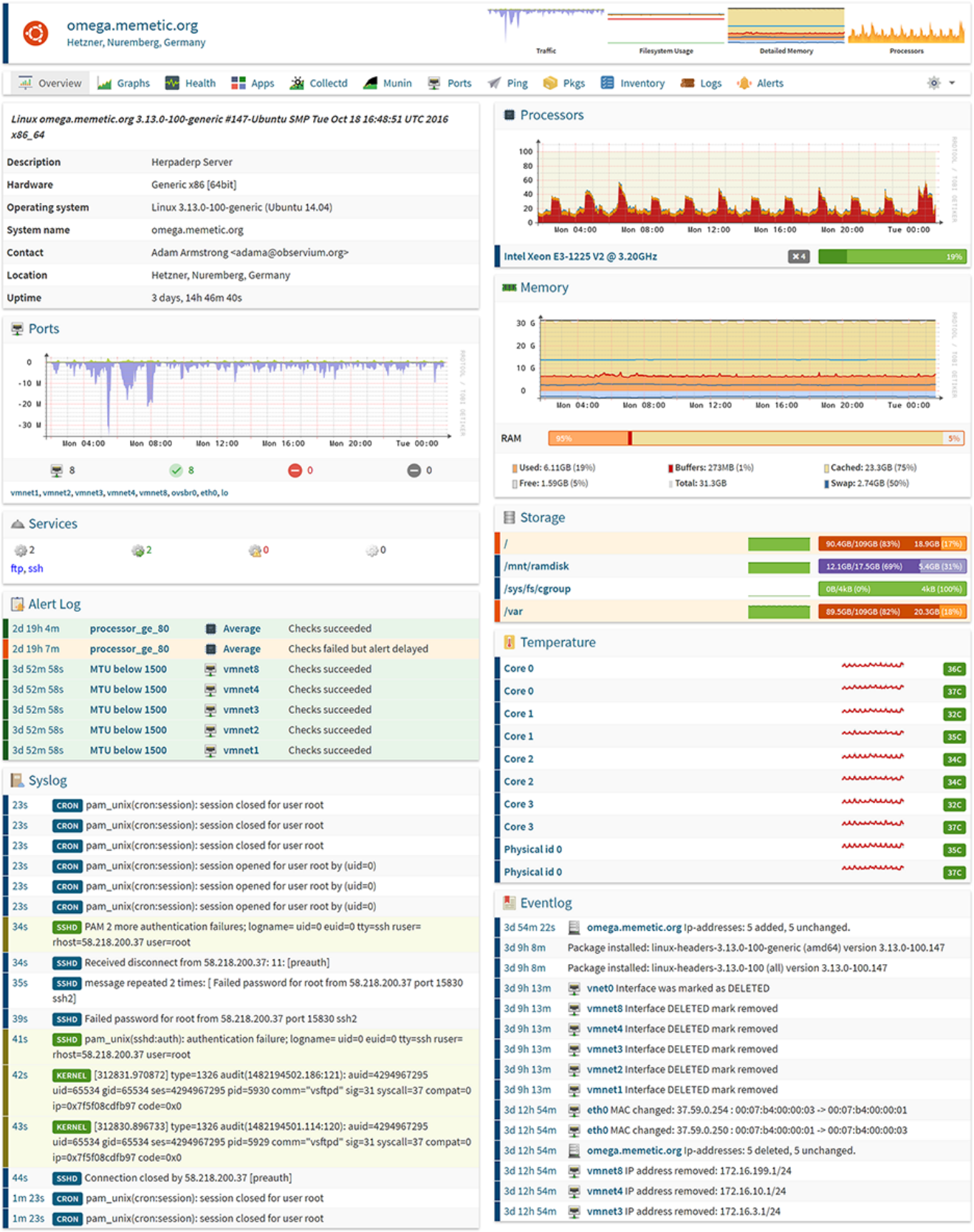
Додаток Б

Інформаційна панель про помилки в Prometheus



Додаток В

Інформаційна панель метрик комп’ютерної мережі з Observium



Додаток Г

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

на тему: «Архітектура системи моніторингу комп'ютерних систем та мереж з використанням штучних нейронних мереж»

Виконав студент групи КСДМ-61
Дідовець Владислав Максимович

Керівник кваліфікаційної роботи:
Лащщевська Наталія
Олександрівна,
завідувач кафедри КІ, к.т.н., доцент

Київ – 2025

Мета роботи – підвищення ефективності роботи систем моніторингу комп'ютерних систем та мереж, шляхом розробки архітектури інтелектуальної системи моніторингу

Об`єкт дослідження – система моніторингу комп'ютерних мережі та систем

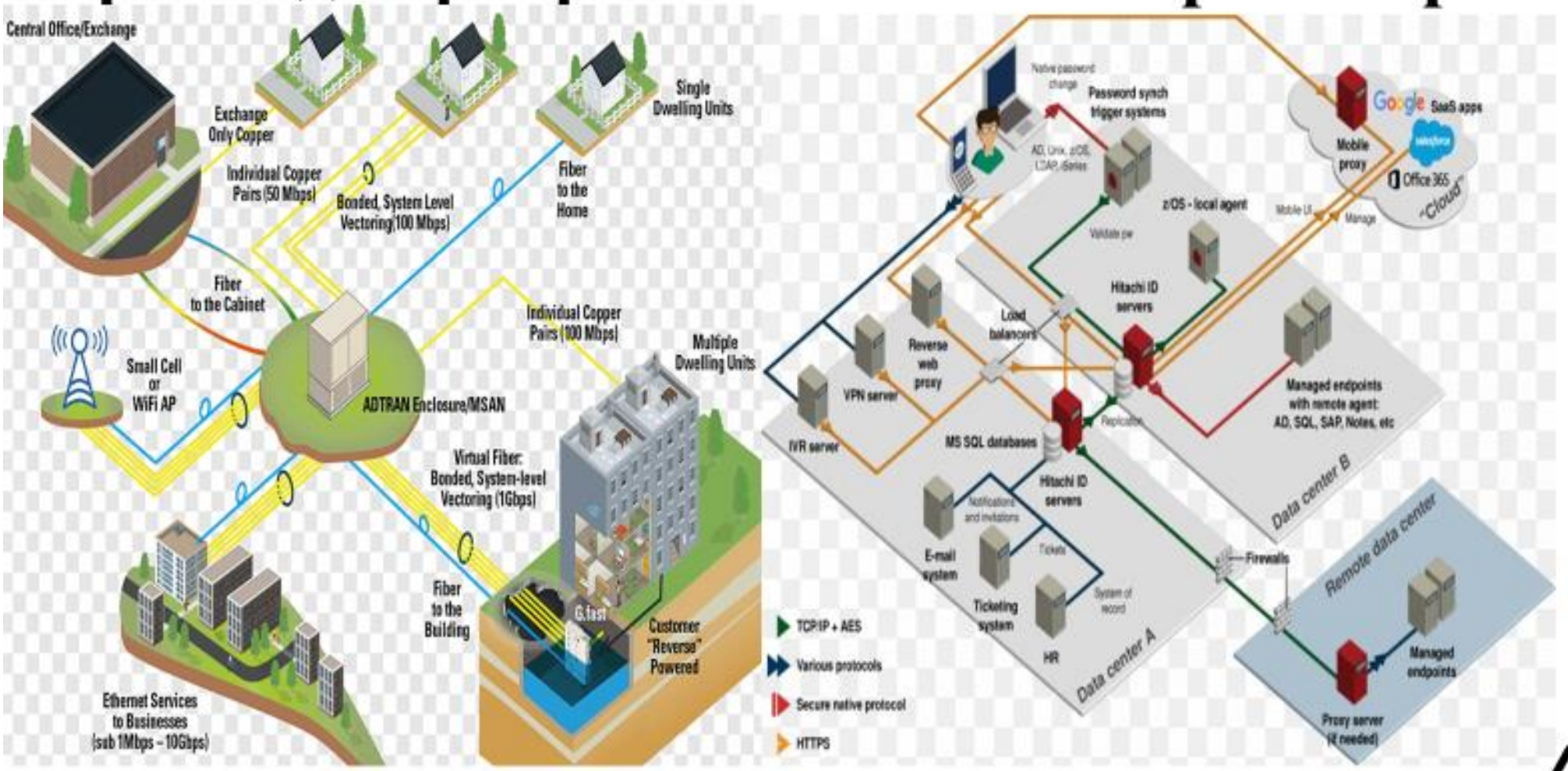
Предмет дослідження – методи виявлення інцидентів та аномалій у процесі моніторингу мереж з використанням штучних нейронних мереж та моделей інтелектуального аналізу даних.

2

Актуальність обраної теми

В наш час комп'ютерні мережі є важливою основою для роботи будь-якого бізнесу, установи та компанії. Вони забезпечують функціонування безлічі послуг та сервісів, якими користуються люди кожного дня. Це можуть бути платіжні операції, месенджери, хмарні сховища зберігання даних, сервіси для створення фото, відео тощо. Зростання навантаження, обсягів даних та вимог створюють додаткове навантаження та ускладнюють роботу мережі. За таких умов важливо забезпечити, якісний рівень моніторингу та спостережуваності комп'ютерної мережі, для стабільної роботи компанії та бізнесу. Використання штучних нейронних мереж дозволить підвищити ефективність роботи мережі, скоротити час реагування на інциденти та підвищити надійність мережевої інфраструктури.

Приклад корпоративної комп'ютерної мережі



Приклад корпоративної комп'ютерної мережі

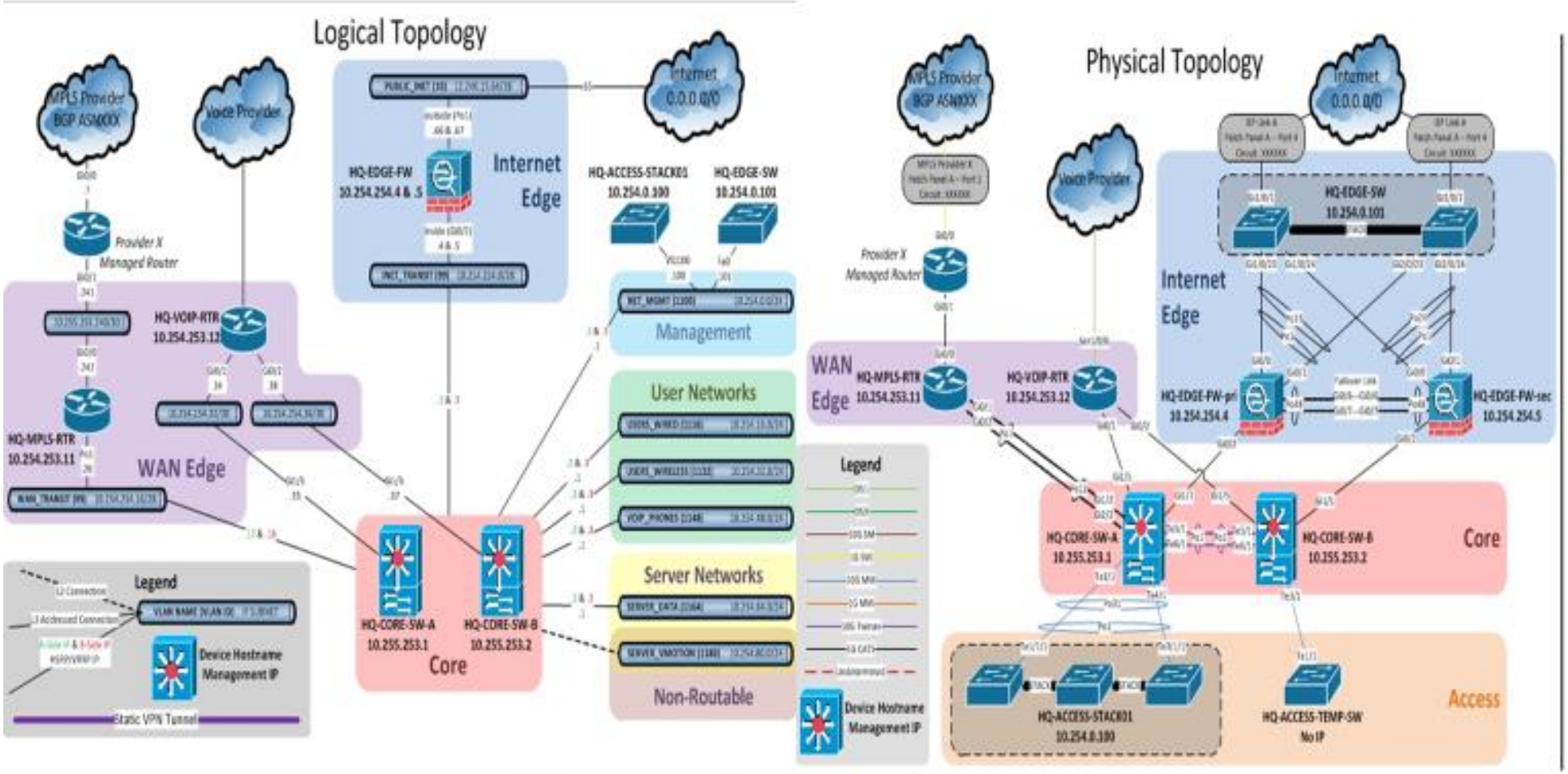
4

Основні вимоги до корпоративної комп'ютерної мережі:

1. достатня пропускна здатність;
2. надійність мережі;
3. безпека мережі;
4. керованість;
5. резервування важливих даних;
6. підтримка периферійного обладнання.

5

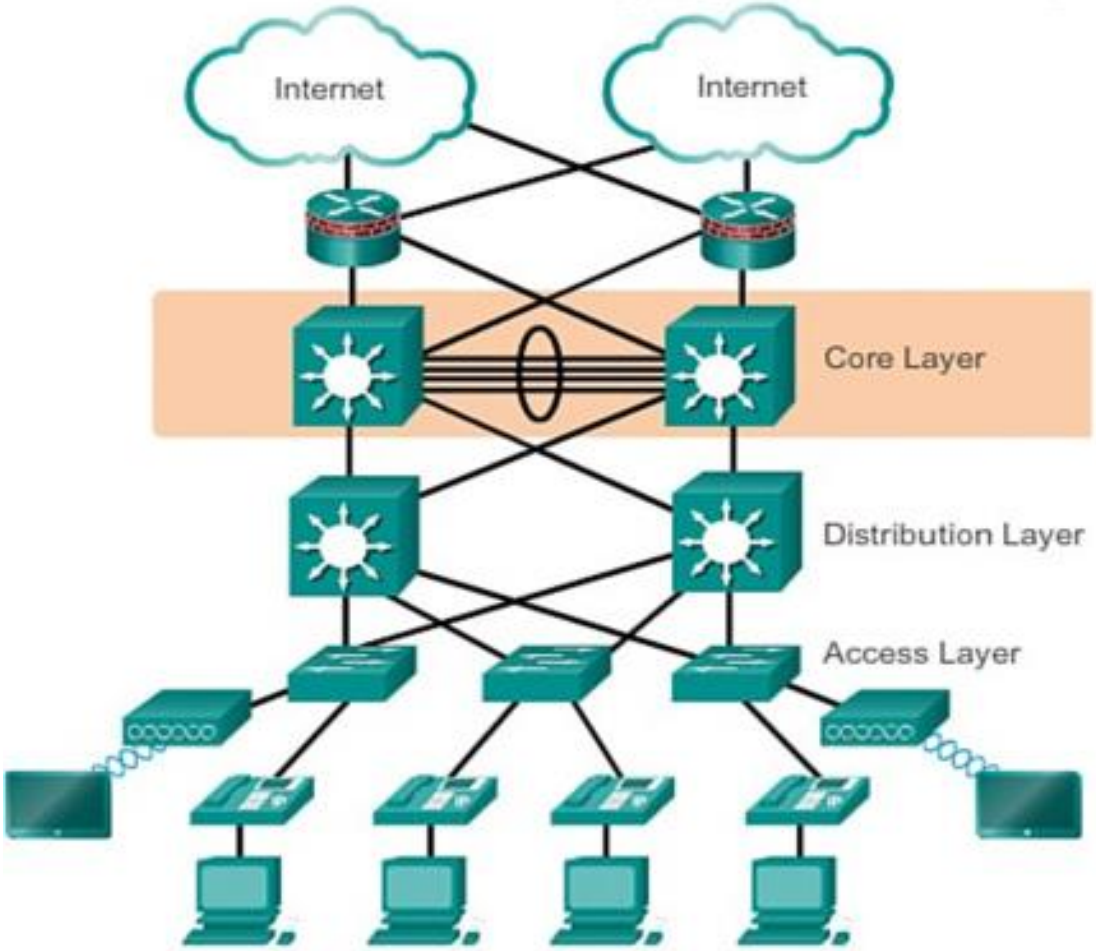
Топології



Фізична та логічна топологія мережі

6

Трирівнева ієрархічна модель



Трирівнева ієрархічна модель Cisco

Рівень доступу (Access layer) забезпечує початкове підключення кінцевих пристроїв до мережі.
Рівень розподілу (Distribution layer) забезпечують з'єднання між комутаторами доступу та рівнем ядра.
Рівень ядра (Core layer) представляє собою високо швидкісний магістральний рівень, який з'єднує між собою комутатори розподілу.

Система моніторингу мережі

Система моніторингу комп'ютерної мережі – це програмне або програмно-апаратне рішення, що безперервно відстежує стан, продуктивність, завантаженість та безпеку комп'ютерної мережі.

Моніторинг мережі – це використання програмно апаратного забезпечення для цілодобового контролю стану та надійності комп'ютерної мережі.

Спостережуваність (observability) – це здатність системи аналізувати внутрішній стан та надання контексту подій, що дозволяє зробити висновки та знайти в чому першопричина.

8

Принципи роботи систем моніторингу та збір даних

Модель роботи систем моніторингу

- агентний;
- безагентний метод;

Способи збору інформації

- агенти на мережевих пристроях і серверах;
- стандартні протоколи: SNMP, WMI, SSH/CLI, IPMI, HTTP(S), NetFlow/sFlow, Syslog;
- streaming telemetry для збору даних у реальному часі.

Типи зібраних даних

- продуктивність (CPU, пам'ять, інтерфейси, трафік);
- статус і доступність обладнання;
- дані апаратних сенсорів (температура, живлення, охолодження);
- журнали подій та мережеві потоки.

Аналіз і реагування

- сенсори фіксують значення метрик;
- тригери спрацьовують при перевищенні порогів;
- автоматичне створення сповіщень та подій.

Візуалізація та аналітика

- графіки, таблиці, інформаційні панелі;
- аналіз тенденцій і аномалій;
- використання нейронних мереж для прогнозування та оптимізації.

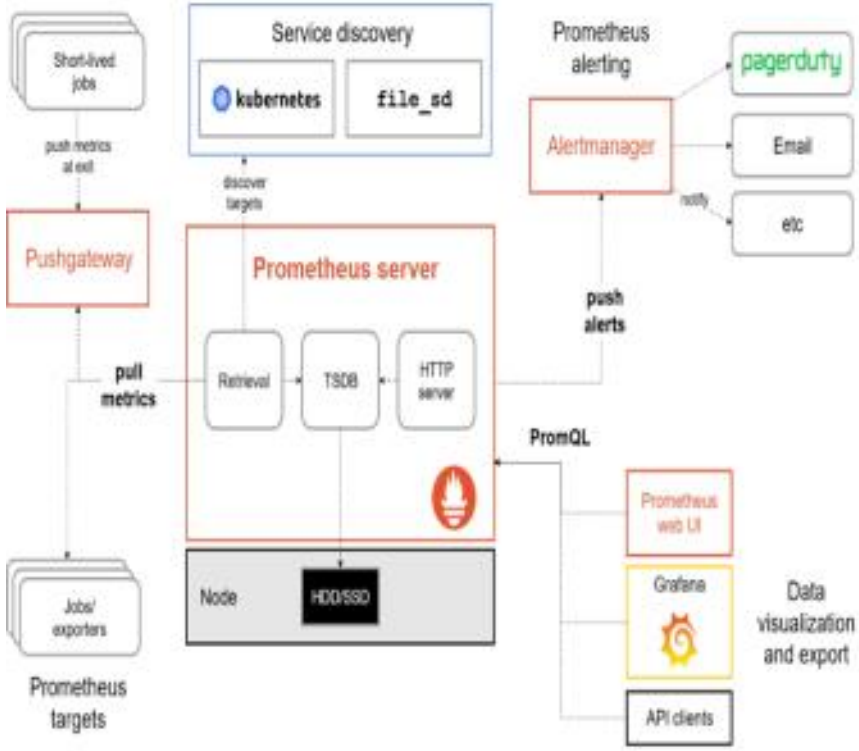
Системи моніторингу комп’ютерних мереж



Інформаційна панель Zabbix, яка показує сповіщення про стан системи, мережевий трафік з часом та детальну мапу мережі.

10

Системи моніторингу комп’ютерних мереж

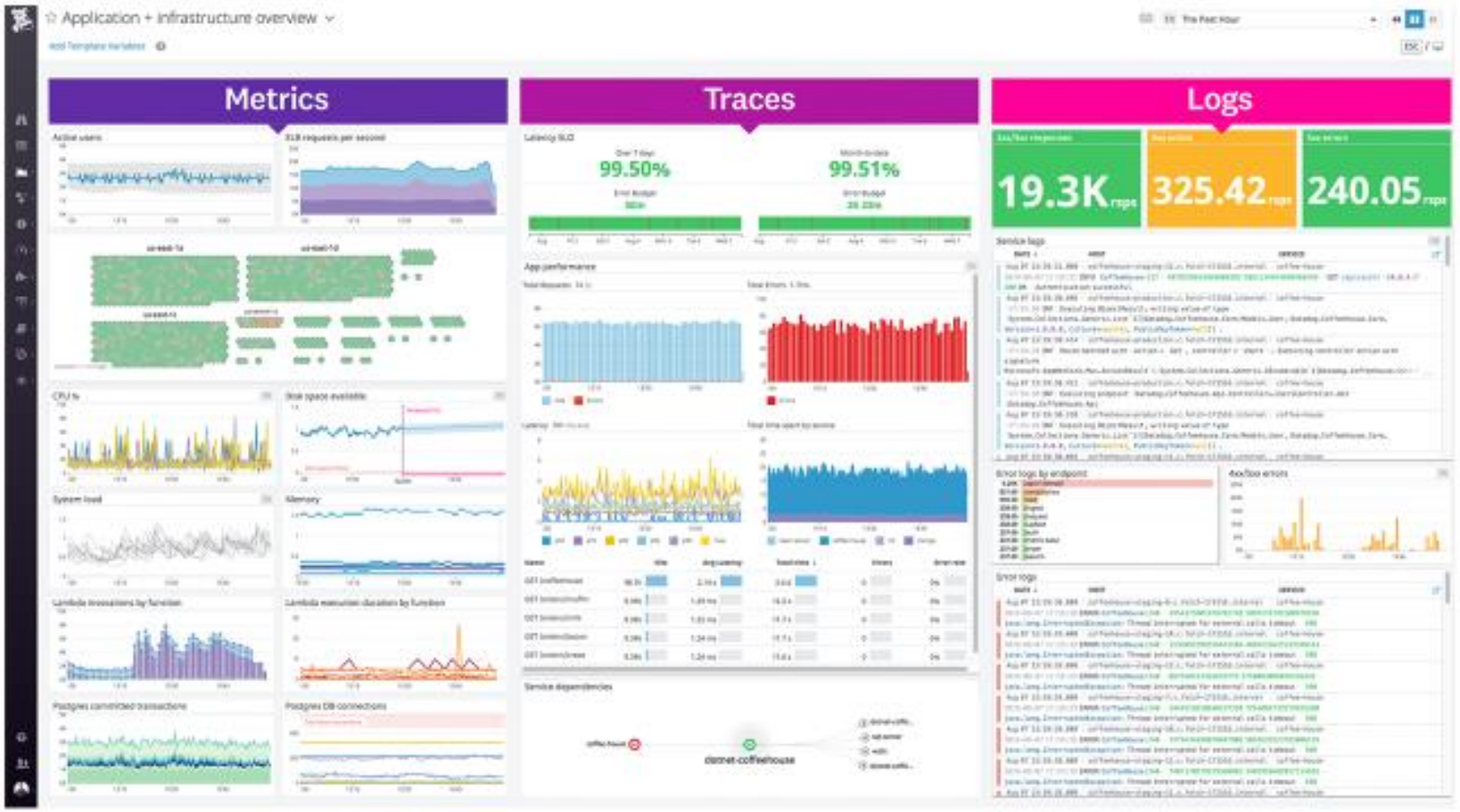


Архітектура роботи Prometheus



Відображення статусу та завантаженості обладнання Prometheus з Grafana

Системи моніторингу комп’ютерних мереж

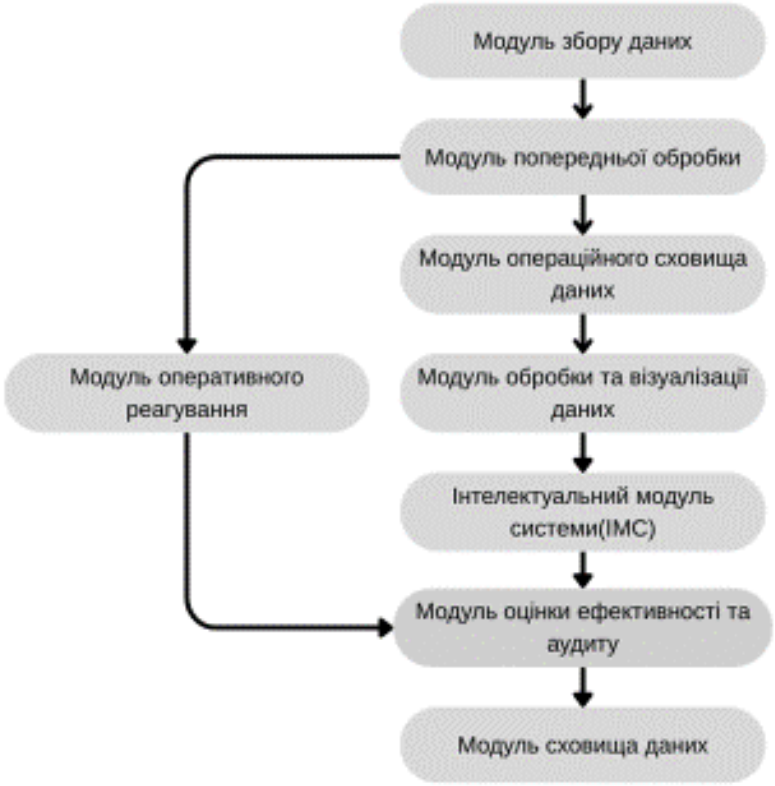


Відображення метрик, traces та logs в Datadog

Вимоги до інтелектуальної системи моніторингу

1. **Автоматичне виявлення інцидентів.** Інтелектуальна система моніторингу повинна самостійно аномалії, помилки конфігурації, деградацію обладнання, атаки на мережу тощо.
2. **Класифікація подій.** На основі бази знань інтелектуальна система моніторингу повинна визначити тип та критичність події для подальшого аналізу та реагування.
3. **Кореляція логів та метрик.** Провівши аналіз даних система повинна вибудовувати причинно-наслідкові зв'язки між подіями в мережі, об'єднуючи їх загальну картину інциденту.
4. **Формування рекомендацій.** Після проведеного аналізу система має сформувати звіт де будуть вказані рекомендації по усуненню проблеми або запобігання подібному в майбутньому.
5. **Автоматичне реагування на інциденти.** Маючи достатньо інформації та інструкцій система повинна автоматично реагувати на інциденти використовуючи підготовленні скрипти та інструкції для зменшення можливого впливу на мережу.

Взаємодія модулів площини даних



Взаємодія модулів площини даних

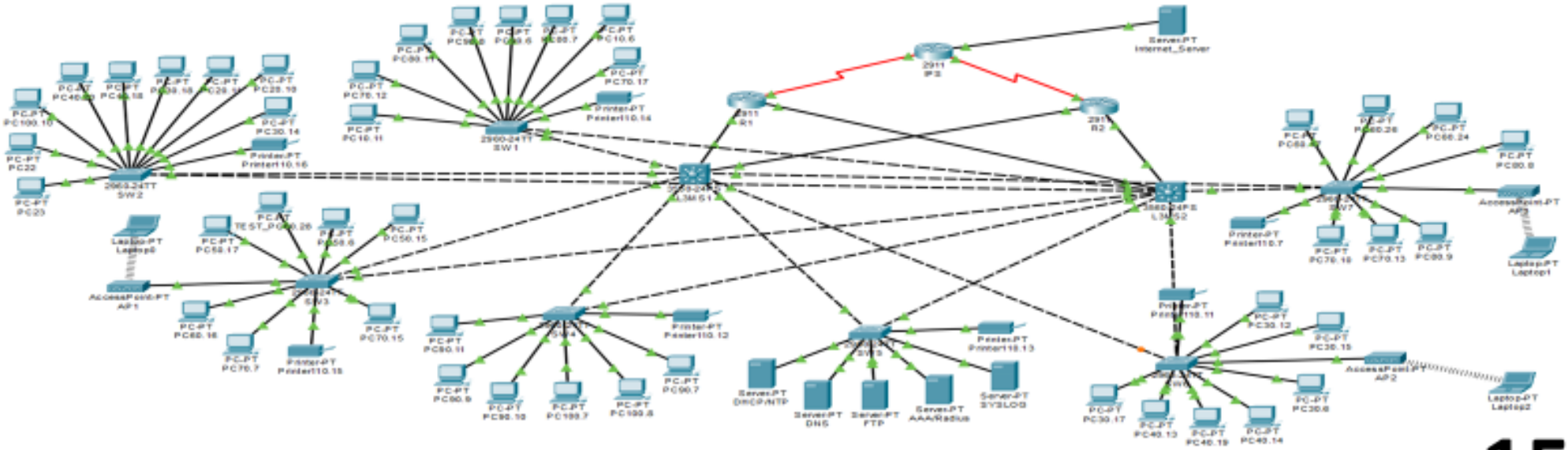
Взаємодія модулів площини керування



Взаємодія модулів площини керування

Демонстраційна модель корпоративної мережі компанії «Interactive Games»

Для прикладу застосування інтелектуальної системи моніторингу візьмемо за приклад компанію “Interactive Games”. Interactive Games – це компанія, що займається розробкою AAA-ігор та забезпечує можливість грати онлайн у свої проєкти. Також ця компанія займається розробкою сервісів та програм для створення модифікацій, різної атрибутики для ігор та навчальних ресурсів. Мережева інфраструктура компанії складається з декількох регіональних офісів серед яких головний офіс, дата-центр та резервний дата-центр для відновлення важливої інформації. Також активно використовуються хмарні технології. Сама мережа в будь-якому з офісів чи дата-центрі складається з трьох рівнів: рівень доступу, рівень розподілу та рівень ядра. Така мережа використовує кореневі комутатори, роутери, комутатори розподілу та доступу, фаєрволи та інші безпекові пристрої. Така архітектура дозволяє забезпечити масштабованість, відмовостійкість та надійність.



Модель комп’ютерної корпоративної мережі

Приклад звітності інтелектуальної системи моніторингу

Звіт про інцидент № 58373 від 11:26

Обладнання: L3MS1 (ядро мережі)

Подія: блокування трафіку користувачів VLAN20, VLAN70 і VLAN80 до серверного сегмента VLAN140 через зміну ACL USER-POLICY

Критичність: середньо-висока

Опис:
Система зафіксувала різке збільшення кількості відхилених з'єднань (ACL-DENY) при зверненні користувачів до серверів у VLAN140. Логи показали, що одразу перед появою помилок відбулася зміна конфігурації (CONFIG_I). Аналіз виявив, що у списку контролю доступу USER-POLICY правило **deny ip any 172.16.0.0/16** було розташоване вище за дозволяючі правила доступу до серверного сегмента. У результаті весь міжвлановий трафік, включно з раніше дозволеними потоками, був заблокований.

Ймовірні причини: неправильне впорядкування правил ACL; помилка адміністратора під час модифікації USER-POLICY; відсутність внутрішньої перевірки конфігурації перед застосуванням; некоректне тестування політик доступу.

Прогнозований вплив:

- повна недоступність веб-сервісів у VLAN140 для користувачів VLAN20, VLAN70 та VLAN80;
- порушення бізнес-процесів відділів продажів, маркетингу та підтримки;
- помилки авторизації і неможливість підключення до внутрішніх інформаційних систем;
- можливі скарги зовнішніх клієнтів у разі залежності сервісів.

Рекомендації:

- Переглянути структуру ACL USER-POLICY та повернути дозволяючі правила у верхню частину списку.
- Відновити попередню версію ACL із системи контролю конфігурацій (Git/Backup).
- Упровадити контроль зміни правил доступу через інтелектуальний модуль моніторингу.
- Виконувати тестування ACL у спеціальному середовищі перед внесенням у продуктивну мережу.

Прогноз: ймовірність повторної помилки конфігурації протягом 30 хвилин за відсутності змін — **56 %**.

Приклад згенерованого звіту

Можлива ситуація в мережі: Під час роботи користувачів з внутрішнім веб-сайтом було помічено втрату доступу. На інформаційну панель надійшли сповіщення про недоступність веб-сайту та порушення політик доступу. Згодом почали надходити скарги від користувачів про блокування їх роботи через недоступність веб-сервісу

```
%ACL-4-DENY: Inbound TCP connection denied from 172.16.20.14 to 172.16.140.10 on port 80
%ACL-4-DENY: Inbound TCP connection denied from 172.16.70.45 to 172.16.140.10 on port 443
%HTTP-3-ACCESS: Web service unreachable (172.16.140.10)
%SYS-5-CONFIG_I: ACL USER-POLICY modified by admin
```

Приклад системного повідомлення про зміни та помилки

Переваги використання інтелектуальної системи моніторингу

1. **Автоматизація моніторингу та аналізу інцидентів.** Зменшення ручної роботи за рахунок автоматичного збору даних, аналізу подій і генерації звітів.
2. **Підвищення надійності та відмовостійкості мережі.** Краще виявлення інцидентів, встановлення першопричин та оперативне реагування.
3. **Оптимізація мережевої інфраструктури.** Виявлення слабких місць, вузьких місць та надмірної надлишковості в конфігураціях і топології.
4. **Розвантаження ІТ-відділу.** Автоматизація рутинних задач: первинний аналіз інцидентів, генерація звітів, стандартні сценарії реагування.
5. **Економія коштів у довгостроковій перспективі.** Оптимізація ресурсів, зменшення простоїв та ефективніша модернізація інфраструктури.
6. **Інтеграція з системами кібербезпеки.** Виявлення аномальної активності, ознак атак та нетипових змін конфігурації.

Недоліки та ризики використання інтелектуальної системи моніторингу

1. **Вимогливість до ресурсів.** Потреба у виділеному сервері або хмарних ресурсах для роботи та навчання інтелектуального модуля.
2. **Складний і тривалий процес налаштування.** Необхідність підготовки навчальної бази, конфігурацій, сценаріїв реагування та навчання системи.
3. **Великий час впровадження та навчання.** Поетапне розгортання, тестування та постійний контроль на початкових етапах.
4. **Підходить переважно для великих мереж.** Висока ефективність досягається лише у великих компаніях з масштабною інфраструктурою.
5. **Ризики безпеки даних.** Обробка чутливої інформації про топологію, конфігурації та стан мережі.
6. **Висока вартість впровадження та експлуатації.** Ліцензії, підписки, додаткові модулі, технічна підтримка та обладнання.

ВИСНОВКИ

У процесі виконання магістерської роботи було досліджені сучасні тенденції розвитку систем моніторингу, комп'ютерних мереж, підходи до їх експлуатації. Розглянуто архітектури систем моніторингу, методи збору інформації та інтеграцій. Описано інтелектуальну систему моніторингу, її архітектуру, складові, взаємодію функціональних елементів (модулів). Описано архітектуру інтелектуальної системи моніторингу мережі з інтелектуальним модулем та спроєктовано модель мережі для симуляції помилок й отримання системних повідомлень, що було використано для створення сценаріїв збоїв в мережі та демонстрації роботи інтелектуального модуля системи моніторингу мережі. Описані результати та використання такого підходу дозволяє знизити час виявлення інцидентів (MTTD), час реагування та підвищити рівень діагностики та контролю.

Важливим аспектом є те, що інтелектуальний модуль здатен працювати не тільки з подіями, а й з конфігураціями обладнання, документацією мережі, що дозволяє виявляти та усувати проблемні місця раніше чим вони стануть проблемою та покращувати ефективність роботи. На основі цього було продемонстровано приклад формування звіту та аналізу збоїв, інцидентів тощо.

ПРОДОВЖЕННЯ ВИСНОВКІВ

Проведене дослідження показує, що використання інтелектуальних систем моніторингу є актуальним та перспективним напрямком розвитку. Це відповідає сучасним тенденціям та прогнозам розвитку. Попри наявність труднощів на етапах реалізації пов'язаних з вимогою до ресурсів, кваліфікації персоналу та безпековому факторі, вплив такої системи на стабільність, продуктивність та безпеку є суттєвим.

Інвестиції в розвиток подібних інтелектуальних систем або модернізацію існуючих систем моніторингу, розширенням можливостей, самонавчання та глибшу кореляцію подій є необхідним кроком, який сприятиме покращенню й фінансовій рентабельності внесених інвестицій в комп'ютерну мережу.

Результати цієї роботи підтверджують доцільність використання інтелектуальних систем моніторингу у корпоративних мережах, демонструють їх можливу ефективність у практичних сценаріях та підкреслюють важливість подальшого розвитку цього напрямку.

ПУБЛІКАЦІЇ ТА АПРОБАЦІЯ РОБОТИ

Тези доповідей:

1. Дідовець В. М. Застосування штучного інтелекту для систем моніторингу мережевої інфраструктури для середнього та великого бізнесу. «Проблеми комп'ютерної інженерії» : V науково-практ. конф., м. Київ, 3 груд. 2024 р. С. 85–88. URL: https://duikt.edu.ua/uploads/p_2661_71874682.pdf

Статті:

1. Дідовець В. М. Тенденції розвитку систем моніторингу комп'ютерних мереж в сучасному світі. Телекомунікаційні та інформаційні технології.(*Подано до друку*)