ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«**ВПРОВАДЖЕННЯ СИСТЕМИ МОНІТОРИНГУ ZABBIX З ВИКОРИСТАННЯМ ОПТИЧНИХ ТЕРМІНАЛІВ C-DATA**»**

на здобуття освітнього ступеня магістр
за спеціальності 123 Комп'ютерна інженерія
(код,найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

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

_____ Дмитро БАХУРИНСЬКИЙ
(підпис) *(ім'я, ПРІЗВИЩЕ здобувача)*

Виконав: здобувач вищої освіти гр.КСДМ-61
Дмитро БАХУРИНСЬКИЙ
(ім'я, ПРІЗВИЩЕ)

Керівник: Андрій ЛЕМЕШКО
доктор філософії (PhD) *(ім'я, ПРІЗВИЩЕ)*

Рецензент: _____
науковий ступінь, вчене звання *(ім'я, ПРІЗВИЩЕ)*

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерної інженерії
Ступінь вищої освіти «Магістр»

Спеціальність 123 Комп'ютерна інженерія
Освітньо-професійна прорама Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерної інженерії
Наталія ЛАЩЕВСЬКА
(ім'я, ПРІЗВИЩЕ)
"____" _____2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бахуринському Дмитру Вадимовичу
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Впровадження системи моніторингу Zabbix з використанням оптичних терміналів C-DATA
керівник роботи Андрій ЛЕМЕШКО доктор філософії (PhD)
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "__" __ 2023 р. №__
2. Строк подання кваліфікаційної роботи
3. Вихідні дані кваліфікаційної роботи:
3.1. Системи моніторингу мережі
3.2. Оптичні термінали.
3.3. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Інформаційне обстеження систем моніторингу мережі.
4.2. Проектування та розробка шаблону системи моніторингу.
4.3. Впровадження та тестування системи на прикладі обладнання C-DATA.

5.Перелік ілюстраційного матеріалу: *презентація*

6. Дата видачі завдання "__" _____2023р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір технічної літератури	.2023р. .2023р.	Виконано
2.	Проектування та розробка шаблону системи моніторингу.	.2023р. .2023р.	Виконано
3.	Впровадження та тестування системи на прикладі обладнання C-DATA	.2023р. .2023р.	Виконано
4.	Аналіз результатів тестування Zabbix	.2023р. .2023р.	Виконано
5.	Оформлення роботи, висновки	.2023р. .2023р.	Виконано
6.	Розробка демонстраційного матеріалу, доповідь	.2023р. .2023р.	Виконано

Здобувач вищої освіти _____ Дмитро БАХУРИНСЬКИЙ
(підпис) *(ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Андрій ЛЕМЕШКО
(підпис) *(ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття ступня магістр: 76 стор., 21 рис., 0 табл., 32 джерел.

Мета роботи – Розробка безкоштовного та ефективного шаблону моніторингу для оптичних терміналів C-DATA в системі Zabbix.

Об'єкт дослідження – система моніторингу Zabbix і оптичні термінали C-DATA.

Предмет дослідження – налаштування шаблонів моніторингу в Zabbix з фокусом на покращення продуктивності мережевого середовища.

Короткий зміст роботи: аналіз обладнання C-DATA, розробка шаблону моніторингу, проведення тестування та оптимизацію системи.

КЛЮЧОВІ СЛОВА: ZABBIX, C-DATA, МОНІТОРИНГ, SNMP, ОПТИМІЗАЦІЯ, БЕЗПЕКА МЕРЕЖІ, ШАБЛОН, СИСТЕМА МОНІТОРИНГУ, АНАЛІЗ ОБЛАДНАННЯ, ЕФЕКТИВНІСТЬ МОНІТОРИНГУ.

ABSTRACT

Textual part of the qualification work for obtaining a Master's degree: 76 pages, 21 figures, 0 tables, 32 sources.

Purpose - To develop a free and effective monitoring template for C-DATA optical terminals in the Zabbix system.

Object of research - Zabbix monitoring system and C-DATA optical terminals.

The subject of the study is the configuration of monitoring templates in Zabbix with a focus on improving the performance of the network environment.

Summary of work: analysis of C-DATA equipment, development of a monitoring template, testing and optimization of the system.

KEYWORDS: ZABBIX, C-DATA, MONITORING, SNMP, OPTIMIZATION, NETWORK SECURITY, TEMPLATE, MONITORING SYSTEM, HARDWARE ANALYSIS, MONITORING EFFICIENCY.

ЗМІСТ

ВСТУП 10

1 МОНІТОРИНГ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ 11

1.1 Інформаційне обстеження 12

1.2 Сфера застосування 14

1.3 Типи мережевого моніторингу 16

1.4 Важливість моніторингу телекомунікаційної мережі 18

1.5 Методи моніторингу мережі 20

1.6 Протоколи моніторингу та керування мережею 24

1.7 Протокол SNMP 25

1.8 Інтеграція SNMP з Zabbix server 27

1.10 Порівняння з іншими системами моніторингу 31

1.11 Приклад впровадження Zabbix у різних сферах 32

1.12 Аналіз безпеки в системах моніторингу 33

2 ПРОЕКТУВАННЯ ТА РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ 36

2.1 Визначення вимог до моніторингу 37

2.2 Вплив моніторингу на діяльність організації 39

2.3 Вибір оптимальних компонентів системи Zabbix 40

2.4 Архітектура системи моніторингу на основі Zabbix 42

2.5 Вибір та конфіграція обладнання та програмного забезпечення 44

2.7 Вивчення механізму збору та візуалізації даних 47

2.8 Розробка плану впровадження та підтримки системи 49

3 ВПРОВАДЖЕННЯ ТА ТЕСТУВАННЯ СИСТЕМИ НА ПРИКЛАДІ ОБЛАДНАННЯ C-DATA 50

3.1 Впровадження системи моніторингу 51

3.2 Розробка темплейту zabbix для olt c-data 55
3.3 Тестування роботи системи та виявлення недоліків 59
3.4 Аналіз взаємодії з оптичними терміналами 60
3.5 Особливості інтеграції з оптичними терміналами C-DATA 62
3.6 Оцінка відповідності системи вимогам безпеки 65
4 АНАЛІЗ РЕЗУЛЬТАТІВ ТЕСТУВАННЯ ZABBIX 67
4.1 Оцінка ефективності системи моніторингу 68
4.2 Переваги використання системи Zabbix 69
4.3 Проблеми та виклики під час впровадження 70
4.4 Удосконалення та оптимізація системи 71
ВИСНОВОК 73
ПЕРЕЛІК ПОСИЛАНЬ 74

ВСТУП

Ми стоїмо на порозі цифрової ери, де технології постійно розвиваються, змінюючи наш спосіб життя. В основі цих змін лежать мережеві технології, вкрай важливі для підтримки безперервної, безпечної та ефективної роботи інформаційних систем. Моніторинг, один з основних елементів цих систем, забезпечує стабільність надійність мережі. Цей дипломний проект присвячений впровадженню системи моніторингу Zabbix за допомогою оптичних терміналів C-DATA, зосереджуючи увагу на їх взаємодії, конфігурації, налаштуванні та оптимізації для ефективного моніторингу мережі. З розвитком інформаційних технологій необхідний комплексний підхід до моніторингу мережі, причому основну роль відіграють оптичні технології. Оптичні термінали C-DATA мають вирішальне значення в цьому процесі, пропонуючи високу продуктивність і надійність передачі даних. Інтеграція цих терміналів із системою моніторингу Zabbix відкриває нові можливості для оптимізації мережі, підвищення ефективності виявлення та вирішення проблем, а також забезпечення безпеки даних. Цей проект досліджує основні аспекти впровадження системи моніторингу Zabbix разом із оптичними терміналами C-DATA, включаючи їх конфігурацію, керування, моніторинг продуктивності та стратегії оптимізації для досягнення максимальної ефективності. Особлива увага приділяється питанням безпеки, аналізу ризиків і застосуванню найкращих практик для забезпечення стабільної та безпечної роботи мережевих систем. Ця ініціатива має на меті зробити внесок у сферу мережевого моніторингу та управління, пропонуючи комплексний погляд на використання сучасних технологій у контексті ефективності та безпеки. Він демонструє, як добре підібрані та налаштовані технологічні рішення можуть підвищити продуктивність і надійність інформаційних систем у швидкозмінному світі.

1 МОНІТОРИНГ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Моніторинг телекомунікаційних мережж — це постійний процес спостереження, контролю і аналізу продуктивності, безпеки та надійності мережі. Для забезпечення її ефективності. Цей процес включає в себе кілька основних аспектів:

1) Збір даних: спеціалізовані агенти або датчики встановлюються на різних компонентах мережі, таких як маршрутизатори, комутатори, сервери та програми, щоб збирати різноманітну інформацію про стан мережі, включаючи обсяг трафіку, використання ресурсів і стан системи.

2) Аналіз та обробка даних: зібрані дані аналізуються та обробляються для виявлення збоїв і проблем. Це може включати виявлення відхилень від нормальної поведінки мережі, які можуть вказувати на потенційні проблеми або загрози.

3) Сповіщення та попередження: коли система моніторингу виявляє проблему чи збій, вона може генерувати сповіщення або попередження для мережевих адміністраторів. Це дозволяє швидко вжити заходів для вирішення проблеми.

4) Запис та архівація даних: мережеві події та дані про стан можна записувати та зберігати для подальшого аналізу, визначення тенденцій та історичних довідок.

5) Моніторинг безпеки: процес моніторингу також включає виявлення потенційних загроз безпеці, таких як спроби несанкціонованого доступу, для забезпечення безпеки мережі.

Ефективний моніторинг телекомунікаційної мережі має провідне значення для забезпечення готовності до роботи, виявлення проблем і слабких місць, збереження високоякісного надання послуг користувачам і підвищення загальної безпеки мережі. Сучасні системи моніторингу, такі як Zabbix, Nagios або Prometheus, надають інструменти для впровадження ефективного моніторингу мережі та дозволяють вчасно реагувати на загрози та проблеми в мережі.

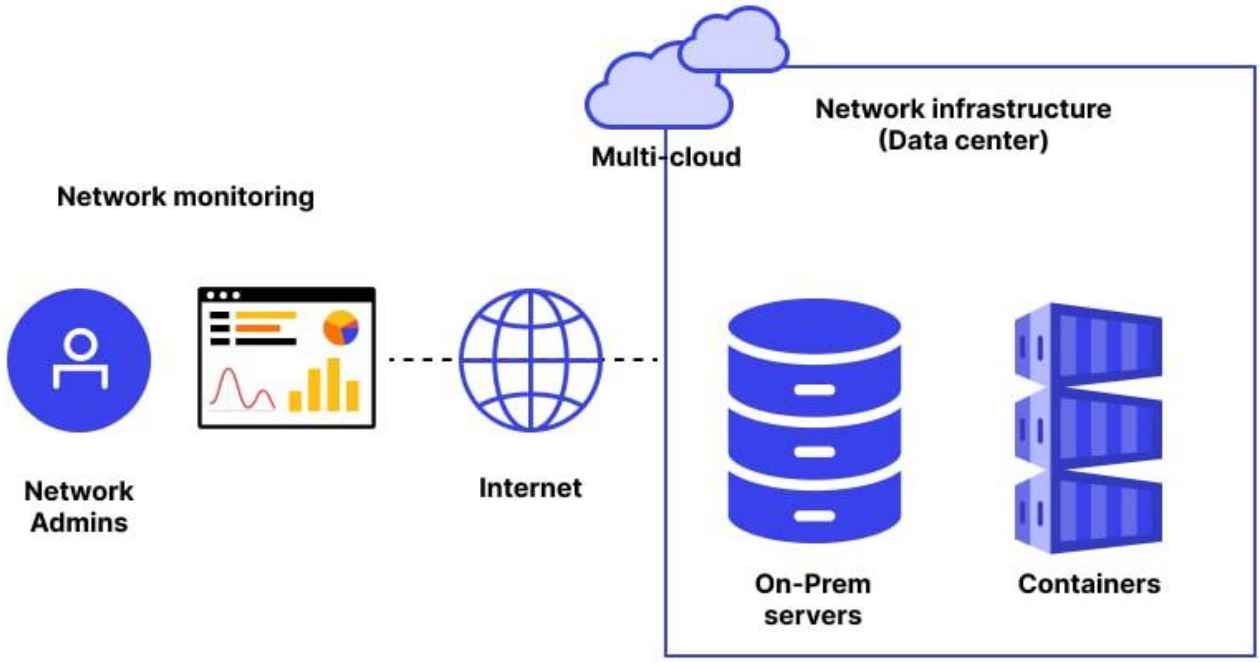

Рисунок 1.1 – моніторинг телекомунікаційної мережі

1.1 Інформаційне обстеження

Перевірка інформаційного обстеження моніторингу телекомунікаційної мережі є складним процесом, що включає аналіз різноманітних аспектів цих систем з метою оцінки поточного стану та виявлення можливостей для поліпшення. Першим етапом аналізу є детальне розглядання вже побудованих телекомунікаційних систем. У цьому процесі проводиться глибоке ознайомлення з функціонуванням усіх матеріальних складових мережевого комплексу, таких як

кабелей, роутери, комутатори і будь-яке інше обладнання. Основною метою даного етапу є досягти повного розуміння взаємозв'язку цих окремих частин системи для отримання неперекрученого й точного уявлення про статус всього комплексу. Здійснення вимірювань та аналізу актуального роботи мережевої інфраструктури є надзвичайно важливим для забезпечення оптимального функціонування. Цей процес передбачає стеження за швидкістю передачі даних, пропускною здатністю, часовою затримкою, втрат пакетів та іншими важливими параметрами продуктивності. Визначення й аналіз проблемних областей є надзвичайно важливим завданням для ідентифікації будь-яких потенційних джерел збоїв чи скорочень продуктивності у мережевому середовищі. Специфічними факторами, які можуть бути трігерами таких ситуації, варто виділяти перенавантажені сегменти мережі, несправне та застаріле обладнання, а також помилковий функціонал програмного забезпечення. Оцінка безпеки мережі - це важливий елементом, цей процес передбачає перевірку ефективності заходів безпеки, таких як файрволи, системи виявлення і запобігання несанкціонованим доступам, а також політик доступу. Надзвичайно необхідно переконатися, що мережа належним чином задовольняє всі стандарти. Цей процес може охоплювати забезпечення якості обслуговування (QoS) і також потребують виконання суворих правил конфіденційності та захисту інформації. Оцінка наявної інфраструктури з метою виявлення потенційних можливостей для поліпшення продуктивності й надійності мереж. В аспект цього дослідження входить огляд прогресивних методик, таких як віртуалізація системи передачі данних, хмарне розсилання, модифікація обладнання елементами сучасними компонентами. На основі зібраного набору даних та проведеного аналізу формується план дій для вдосконалення мережевої інфраструктури. Цей план може передбачати пропозиції щодо оновлення обладнання, оптимізацію конфігурації, поліпшення заходів безпеки. Ефективне залучення всіх особливо зацікавлених сторін, а також управлінський процес бюджету сприяє успішному впровадженню запропонованих поліпшень. Це передбачає конструктивний діалог з керівництвом, ІТ-відділом, та іншими важливими особами для забезпечення підтримки та ресурсів. Інформаційне

обстеження моніторингу телекомунікаційних мереж є основним процесом, який вимагає детального розуміння технічних, оперативних та стратегічних аспектів мережі. Ефективне проведення такого обстеження може значно покращити продуктивність, безпеку та надійність мережевої інфраструктури, а також сприяти її стратегічному розвитку.

1.2 Сфера застосування

Під час аналізу різнопрофільних сфер, де використовується контроль телекомунікаційної інфраструктури, можна виділити кілька ключових галузей, в яких ця процедура набуває значущості. У сфері інформаційних технологій (IT), моніторинг мереж дозволяє здійснювати контроль за пропускною здатністю, навантаженням на сервери, виявляти джерела помилок та планувати виділення ресурсів для проведення віртуалізації у центрах обробки даних. У сфері телекомунікацій, практикується використання моніторингу з метою контролювання статусу інфраструктури, ефективного використання ресурсів, виявлення помилок та гарантування якості надаваних послуг. Цей процес передбачає аналіз об'єму перенесеного трафіку і оптимальне розподілення напрямкам цих потокових даних. У секторі електроенергетики, важливим аспектом є нагляд за інфраструктурою телекомунікацій з метою керування системами вимірювань, дистанційного спостереження та управління віддаленими точками постачання електричної енергії. Ця система гарантує передачу інформації про статус електричних мереж і представляє ключовий фактор для стабільного комунікаційного середовища. У сфері фінансових послуг, моніторинг мережі виконує значущу роль у виявленні та протидії кіберзагрозам. Його основна задача полягає у забезпеченні безпеки при обміну фінансовими операцій. У галузі медицини, нагляд за телекомунікаційною інфраструктурою виконує роль

забезпечення безпеки під час обміну медичною інформацією серед різних закладів охорони здоров'я, лабораторій та клінік. Крім цього, такий вид контролю є необхідним для успішного використання теле-медицини і провадження консультацій онлайн. Система моніторингу є невід'ємною складовою ефективного функціонування виробничих та промислових підприємств, оскільки її основна роль полягає у керуванні автоматизованими системами контролю і спостереження за процесами виробництва. Основним завданням моніторингу є оптимізація часу бездіяльності обладнання та запобігання можливих неполадок. У сферах транспорту й логістики контроль мережі є невід'ємною складовою для перевірки руху транспортних засобів, створення оптимальних маршрутів, виявлення допустимих пригод на дорозі і полегшення ефективності простежу процесами логістики. В сфері освіти, введення системи моніторингу є допомогою у забезпеченні навчальних ресурсів та побудови ефективного спілкування між всіма учасниками процесу навчання. Це стає проблематичним у контексті дистанційної освіти і актуальності завдяки цьому факторові. Це лише декілька прикладів сфер, де моніторинг телекомунікаційної мережі грає важливу роль у забезпеченні надійності, безпеки та ефективності діяльності. Розуміння стану мережі і реагування на проблеми стають критично важливими для багатьох сучасних галузей.

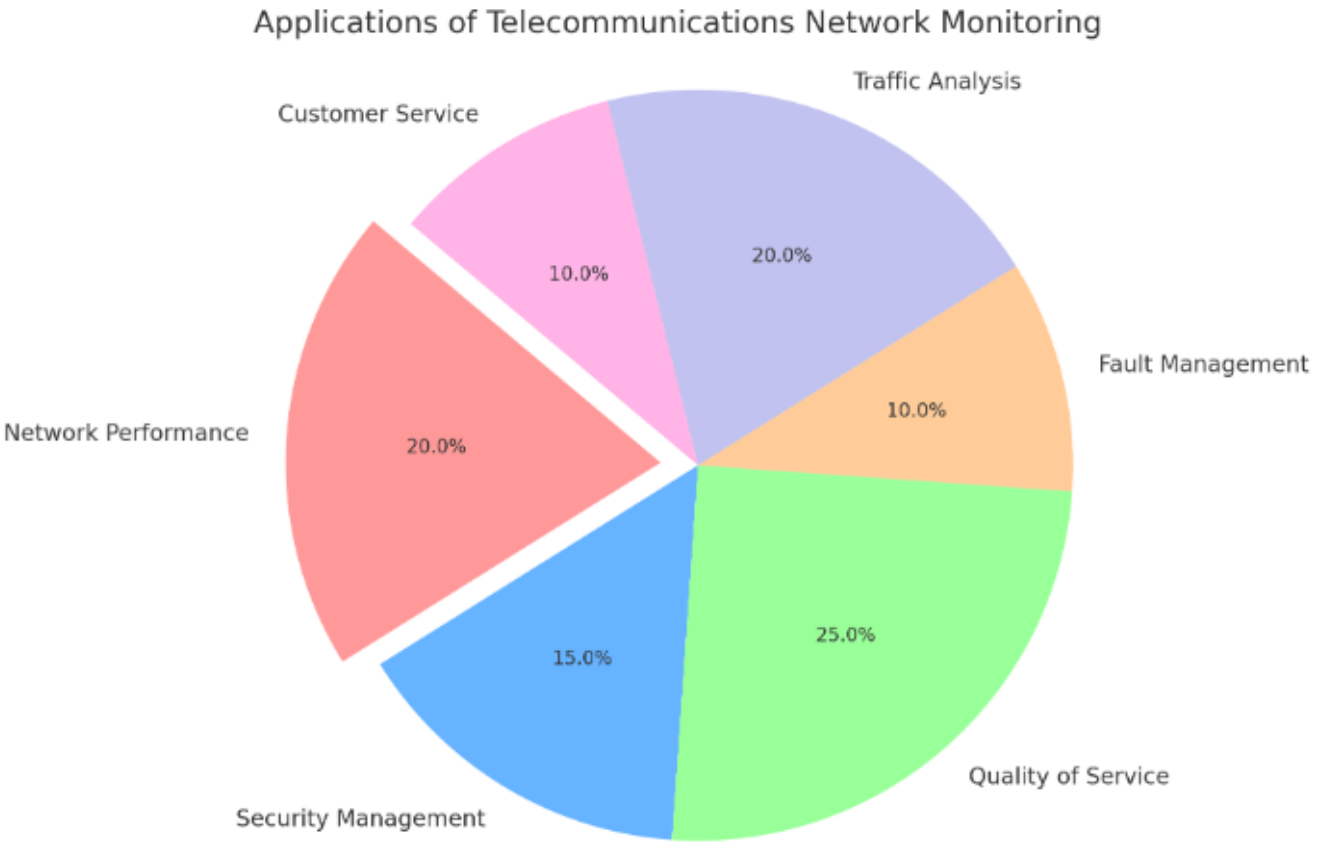

Рисунок 1.2 – Сфери застосування систем моніторингу

1.3 Типи мережевого моніторингу

Кілька різновидів мережевого моніторингу використовуються для спостереження, дослідження та керування різними аспектами мережевої інфраструктури. Розглянемо кожен з цих типів докладніше:

1) Відстеження доступності: призначено для визначення доступності мережевих ресурсів, таких як сервери, маршрутизатори, комутатори та служби. Використовує протокол ICMP (Ping) або SNMP, щоб переконатися, що призначена ціль доступна

та працює належним чином.

2) Відстеження продуктивності: вимірює продуктивність мережевих ресурсів, включаючи пропускну здатність, навантаження, використання ресурсів і зміни з часом. Для оцінки продуктивності використовує такі показники, як швидкість передачі даних, затримка, тремтіння та втрата пакетів.

3)Моніторинг конфігурації: призначений для виявлення змін конфігурації мережевих пристроїв і служб. Виявляйте зміни, перевіряйте відповідність стандартам безпеки та допомагайте керувати конфігураціями, щоб запобігти неочікуваним збоям.

4)Моніторинг подій: розроблено для використання аналізу журналу подій для відстеження подій і створення сповіщень про них. Він використовується для виявлення надзвичайних ситуацій, помилок або мережевих атак і сповіщення адміністраторів про проблеми.

5)Моніторинг безпеки: призначений для виявлення потенційних загроз безпеці мережі та даних. Використовуйте сигнали та шаблони для виявлення аномалій, вторгнень, вірусів та інших загроз безпеці.

6)Моніторинг загальнодоступних ресурсів (Resource Monitoring): призначений для моніторингу використання ресурсів на сервері, включаючи процесор, оперативну пам’ять, дисковий простір тощо. Допомагає визначити, коли серверу потрібно масштабувати або оптимізувати ресурси.

7)Кожен тип моніторингу відіграє вирішальну роль у забезпеченні ефективності, надійності та безпеки вашої мережі. Як правило, організації використовують комбінацію різних типів моніторингу, щоб отримати повний контроль над своїми мережами, залежно від своїх потреб і цілей.

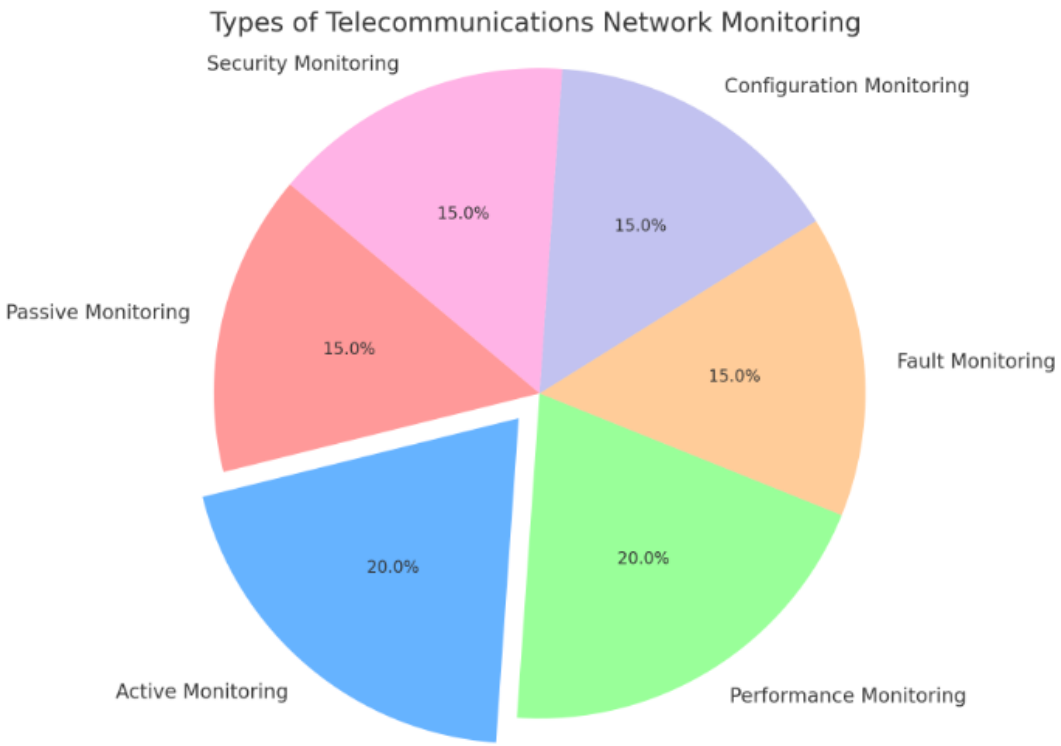

Рисунок 1.3 – Типи систем моніторингу

1.4 Важливість моніторингу телекомунікаційної мережі

Моніторинг телекомунікаційних мереж відіграє життєво важливу роль у забезпеченні їх стабільності та ефективності, особливо в сучасному технологічному світі, що постійно змінюється. Важливість моніторингу полягає у виявленні проблем і збоїв у вашій мережі в режимі реального часу та швидкому реагуванні, що дозволяє попередити про можливі збої та забезпечити постійну доступність послуг. Оптимізація ресурсів є ще однією великою перевагою моніторингу мережі. Аналізуючи використання пропускної здатності, обчислювальних ресурсів і мережевого обладнання, можна не тільки підвищити продуктивність, але й забезпечити більш ефективне використання наявних

ресурсів. Це в свою чергу дозволяє уникнути зайвих витрат на обладнання та електроенергію. Моніторинг кібербезпеки відіграє важливу роль у виявленні та запобіганні кібератакам і несанкціонованому доступу. Використання сучасних засобів моніторингу може підвищити загальний рівень безпеки інфраструктури шляхом оперативного виявлення аномалій у мережевому трафіку, які можуть вказувати на потенційні загрози. Підтримка високої якості обслуговування (QoS) є ще одним важливим аспектом, особливо для мереж, що підтримують послуги в реальному часі. Моніторинг забезпечує постійний контроль швидкості передачі даних, затримки, втрати пакетів та інших показників, що дозволяє своєчасно вживати заходів для забезпечення надійності та якості мережевих послуг. Планування розвитку та розширення мережі також залежить від даних, отриманих у процесі моніторингу. Аналізуючи навантаження і тенденції розвитку мережі, можна ефективно планувати майбутні інвестиції та розширення, а також забезпечувати стійкість інфраструктури. Це не тільки автоматизує моніторинг і діагностику, а й виявляє та вирішує проблеми на ранній стадії, таким чином знижуючи витрати і підвищуючи ефективність обслуговування. Це зменшує час простоїв і витрати на технічну підтримку та підвищує продуктивність технічного персоналу. Впровадження інноваційних технологій в мережеву інфраструктуру і розробка нових рішень вимагає глибокого розуміння поточного стану мережі. Моніторинг допомагає збирати інформацію та аналітичні дані, необхідні для підтримки інноваційних ініціатив. Моніторинг телекомунікаційних мереж є основним інструментом забезпечення надійності, безпеки та ефективності мережевих систем. Цей процес є ключовим для підтримки стійкості та гнучкості інфраструктури в інформаційному середовищі, що швидко змінюється.

1.5 Методи моніторингу мережі

Мережевий моніторинг використовує різні методи і засоби для збору і аналізу інформації про стан і функціонування мережевих систем, що необхідно для їх безперебійної роботи.SNMP (Simple Network Management Protocol) - це стандартний протокол для моніторингу та управління маршрутизаторами, комутаторами, Він вважається стандартним протоколом для моніторингу та управління мережевими пристроями, такими як маршрутизатори, комутатори і сервери. Протокол використовує інформаційну базу управління (MIB) для збору даних про ресурси, стан і події мережевих пристроїв. Ping та ICMP (Internet Control Message Protocol) використовуються для вимірювання доступності та затримки мережевих пристроїв. ping використовує ICMP-запити для перевірки доступності мережевих вузлів та визначення часу їхньої відповіді. traceroute перенаправляє на певну мережеву адресу та відстежує кількість проміжних вузлів і затримку кожного вузла. NetFlow і sFlow - протоколи, які активно використовуються для збору даних про мережевий трафік. Це дозволяє аналізувати обсяг і тип трафіку, а також виявляти потенційні проблеми або незвичну активність. Ця інформація дуже корисна для аналізу мережевого трафіку, планування мережевих ресурсів і виявлення загроз безпеці. Для більш глибокого аналізу мережевих пакетів можна використовувати аналізатори пакетів, такі як Wireshark. Пакети даних, що проходять через мережеві інтерфейси, можна перехоплювати і аналізувати, надаючи детальну інформацію про протоколи, мережеві адреси і типи трафіку. Цей метод особливо корисний для усунення складних мережевих проблем і виявлення несанкціонованого або шкідливого трафіку. Використання спеціалізованого обладнання для моніторингу, такого як мережеві аналізатори, також є важливим фактором у виявленні та аналізі мережевих проблем. Таке обладнання може ефективно перехоплювати та аналізувати трафік і надавати детальну статистику про ресурси та стан мережевих пристроїв. Системи моніторингу мережі (NMS) - це комплексні рішення, що поєднують в собі різні інструменти для збору, аналізу,

візуалізації та звітування про мережеві події. Вони забезпечують гнучкість і масштабованість мережевого моніторингу завдяки підтримці різних протоколів моніторингу, таких як SNMP і NetFlow. Гнучкість і масштабованість для моніторингу мережі. Агентні рішення встановлюють агенти моніторингу на мережеві пристрої та періодично надсилають дані про їхній стан на централізований сервер моніторингу. Такий підхід дозволяє збирати детальну інформацію про такі параметри, як завантаження процесора, використання пам'яті та стан мережевого інтерфейсу. Хмарний моніторинг та автоматизований моніторинг з використанням методів штучного інтелекту і машинного навчання відкривають нові можливості для прогнозування потенційних проблем мережі та автоматичного реагування на виявлені події. Моніторинг додатків і моніторинг мережевої безпеки також є важливими елементами, які дозволяють відстежувати стан і продуктивність додатків, що використовують мережеві ресурси, а також виявляти і реагувати на потенційні загрози безпеці. Зрештою, вибір методів та інструментів мережевого моніторингу залежить від конкретних потреб та масштабу організації. Для забезпечення комплексного контролю та ефективного управління мережевими ресурсами часто використовується комбінація різних методів. Мережевий моніторинг використовує різні методи і засоби для збору і аналізу інформації про стан і функціонування мережевих систем, що необхідно для їх безперебійної роботи.SNMP (Simple Network Management Protocol) - це стандартний протокол для моніторингу та управління маршрутизаторами, комутаторами, Він вважається стандартним протоколом для моніторингу та управління мережевими пристроями, такими як маршрутизатори, комутатори і сервери. Протокол використовує інформаційну базу управління (MIB) для збору даних про ресурси, стан і події мережевих пристроїв. Ping та ICMP (Internet Control Message Protocol) використовуються для вимірювання доступності та затримки мережевих пристроїв. ping використовує ICMP-запити для перевірки доступності мережевих вузлів та визначення часу їхньої відповіді. traceroute перенаправляє на певну мережеву адресу та відстежує кількість проміжних вузлів і затримку кожного вузла. NetFlow і sFlow - протоколи, які активно використовуються для збору даних

про мережевий трафік. Це дозволяє аналізувати обсяг і тип трафіку, а також виявляти потенційні проблеми або незвичну активність. Ця інформація дуже корисна для аналізу мережевого трафіку, планування мережевих ресурсів і виявлення загроз безпеці. Для більш глибокого аналізу мережевих пакетів можна використовувати аналізатори пакетів, такі як Wireshark. Пакети даних, що проходять через мережеві інтерфейси, можна перехоплювати і аналізувати, надаючи детальну інформацію про протоколи, мережеві адреси і типи трафіку. Цей метод особливо корисний для усунення складних мережевих проблем і виявлення несанкціонованого або шкідливого трафіку. Використання спеціалізованого обладнання для моніторингу, такого як мережеві аналізатори, також є важливим фактором у виявленні та аналізі мережевих проблем. Таке обладнання може ефективно перехоплювати та аналізувати трафік і надавати детальну статистику про ресурси та стан мережевих пристроїв. Системи моніторингу мережі (NMS) - це комплексні рішення, що поєднують в собі різні інструменти для збору, аналізу, візуалізації та звітування про мережеві події. Вони забезпечують гнучкість і масштабованість мережевого моніторингу завдяки підтримці різних протоколів моніторингу, таких як SNMP і NetFlow. Гнучкість і масштабованість для моніторингу мережі. Агентні рішення встановлюють агенти моніторингу на мережеві пристрої та періодично надсилають дані про їхній стан на централізований сервер моніторингу. Такий підхід дозволяє збирати детальну інформацію про такі параметри, як завантаження процесора, використання пам'яті та стан мережевого інтерфейсу. Хмарний моніторинг та автоматизований моніторинг з використанням методів штучного інтелекту і машинного навчання відкривають нові можливості для прогнозування потенційних проблем мережі та автоматичного реагування на виявлені події. Моніторинг додатків і моніторинг мережевої безпеки також є важливими елементами, які дозволяють відстежувати стан і продуктивність додатків, що використовують мережеві ресурси, а також виявляти і реагувати на потенційні загрози безпеці. Зрештою, вибір методів та інструментів мережевого моніторингу залежить від конкретних потреб та масштабу організації. Для забезпечення комплексного контролю та ефективного

управління мережевими ресурсами часто використовується комбінація різних методів.

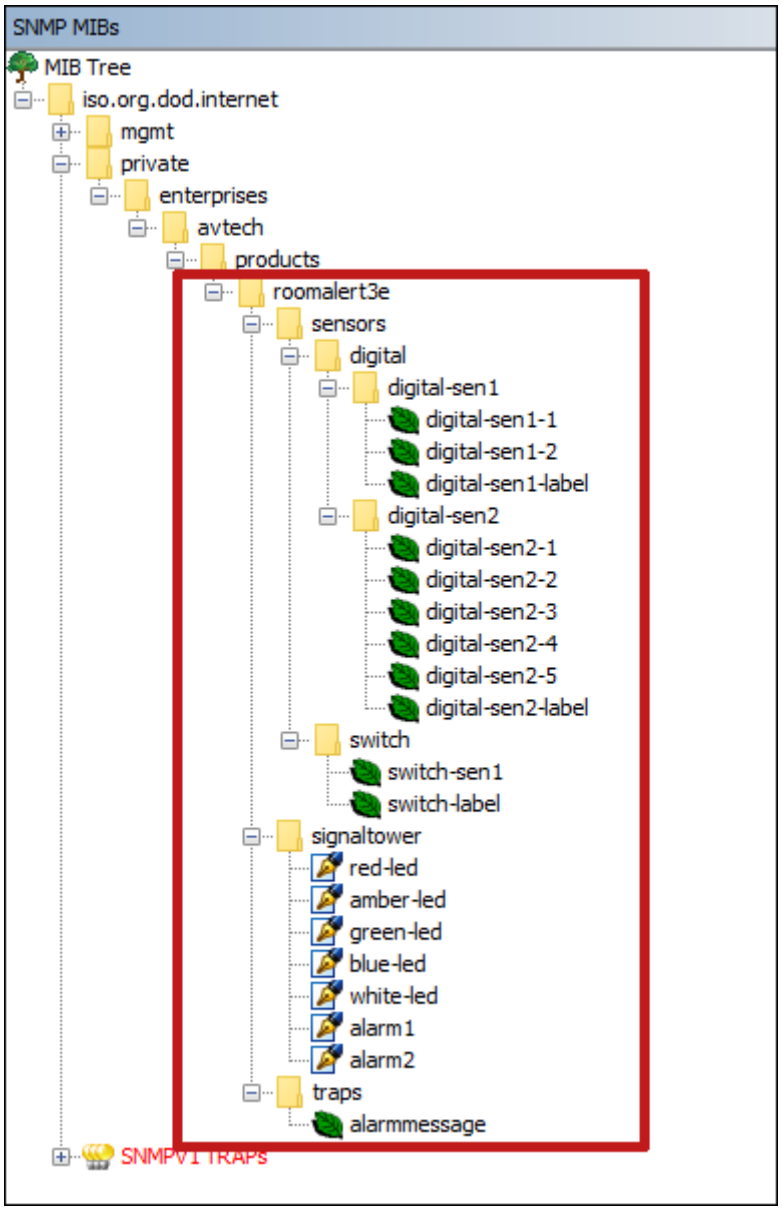

Рисунок 1.4 – Приклад SNMP MIBs

1.6 Протоколи моніторингу та керування мережею

Протоколи моніторингу та управління мережею є важливими інструментами для мережевих адміністраторів для збору, аналізу та обміну інформацією про стан і конфігурацію мережевих пристроїв. Вони відіграють важливу роль у підтримці надійності, продуктивності та безпеки мережевих систем. У цьому розділі детально описано найважливіші протоколи моніторингу та керування мережею:

1) SNMP (Simple Network Management Protocol) - один з найпоширеніших протоколів моніторингу мережі SNMP (Simple Network Management Protocol) - один з найпоширеніших протоколів моніторингу мережі. SNMP використовує такі команди, як GET для запиту даних і SET для зміни налаштувань пристрою. Існують різні версії SNMP, кожна з яких пропонує різні рівні функціональності та безпеки.

2) NetFlow, розроблений компанією Cisco, є важливим протоколом для збору та аналізу даних мережевого трафіку. Протокол дозволяє адміністраторам контролювати обсяг і тип трафіку, аналізувати причини перевантажень і виявляти аномальні дії, такі як DDoS-атаки. Різні версії NetFlow, такі як NetFlow v5, v9 і IPFIX, забезпечують збір і аналіз даних з різними функціями.

3) Syslog - це стандартний протокол, який використовується для запису подій мережевих пристроїв. Він дозволяє адміністраторам відстежувати такі події, як помилки, збої та попередження; Syslog класифікує повідомлення відповідно до їхньої серйозності, що дозволяє ефективно керувати журналами подій і швидко реагувати на критичні події.

4) HTTP і HTTPS часто використовуються для віддаленого керування мережевими пристроями через веб-інтерфейс. Ці протоколи дозволяють адміністраторам легко отримувати доступ до статистики та налаштувань мережевих пристроїв за допомогою стандартного веб-браузера; HTTPS забезпечує додатковий рівень безпеки, шифруючи дані.

5) SSH (Secure Shell) - надійний і безпечний метод віддаленого керування. Це безпечний і надійний спосіб віддаленого керування мережевими пристроями за допомогою командного рядка. Він забезпечує безпечний канал для надсилання команд і даних з використанням автентифікації на основі ключа або пароля.

6) Telnet менш безпечний, ніж SSH, але дозволяє віддалено керувати мережевими пристроями через командний рядок. Однак, оскільки він не забезпечує шифрування, рекомендується обмежити його використання незахищеними мережами.

7) Internet Control Message Protocol (ICMP) використовується для діагностики та управління мережевими проблемами. Цей протокол надсилає керуючі повідомлення і виявляє недоступність пристроїв (наприклад, команди ping) та інші мережеві проблеми.

Разом ці протоколи утворюють комплексний інструментарій управління та моніторингу мережі, який керує різними аспектами мережевої інфраструктури для забезпечення стабільної та безпечної роботи. Вибір протоколу залежить від конкретних потреб мережі, рівня знань адміністратора та необхідного рівня безпеки.

1.7 Протокол SNMP

SNMP (Simple Network Management Protocol) - це стандартний мережевий протокол, який використовується для збору та організації інформації про пристрої в мережі, а також для віддаленої зміни параметрів цих пристроїв. SNMP сумісний з простими і поширеними мережевими пристроями і тому широко використовується в мережевому управлінні. Основна ідея SNMP полягає у використанні "агентів", встановлених на мережевих пристроях. Ці агенти збирають

важливу інформацію про стан і функціональність пристроїв і зберігають цю інформацію у вигляді змінних, які можна запитувати або змінювати в мережі за допомогою SNMP-менеджера. SNMP-менеджер - це пристрій, який використовує SNMP для запиту інформації від агента і надсилання агенту команд для зміни його налаштувань, системи або додатки, які використовують SNMP для надсилання команд для зміни налаштувань пристрою. Важливим компонентом SNMP є Management Information Base (MIB) - база даних, яка використовується для зберігання інформації про об'єкти, керовані за допомогою SNMP. Кожен об'єкт в MIB має унікальний ідентифікатор, а кожен пристрій має набір об'єктів MIB, які можна запитувати і змінювати за допомогою SNMP. Однією з унікальних особливостей SNMP є механізм "пастки". Це спеціальне повідомлення, яке агент надсилає SNMP-менеджеру при зміні певних подій або стану пристрою. Це дозволяє мережевим адміністраторам швидко реагувати на важливі події, такі як апаратні збої або порушення безпеки. SNMP існує в різних версіях, кожна з яких має свої особливості та рівні безпеки. Наприклад, SNMPv1 є найпростішою версією і використовує базові функції для збору інформації та управління. SNMPv3, з іншого боку, надає більш просунуті функції безпеки, такі як шифрування і аутентифікація для захисту передачі даних. Безпека є однією з основних проблем при використанні SNMP, особливо в більш ранніх версіях протоколу, і SNMPv3 вирішує такі проблеми, як покращений контроль доступу і шифрування даних. Використання SNMP вимагає глибокого розуміння мережевої інфраструктури і специфічних вимог до моніторингу; налаштування SNMP на мережевих пристроях є складним, але при правильному налаштуванні він є потужним інструментом для моніторингу та управління мережею. Завдяки своїй універсальності і гнучкості, SNMP є одним з найпопулярніших протоколів для моніторингу та управління мережевими пристроями, надаючи мережевим адміністраторам важливий інструмент для підтримки стабільності та ефективності їх мережевої інфраструктури.

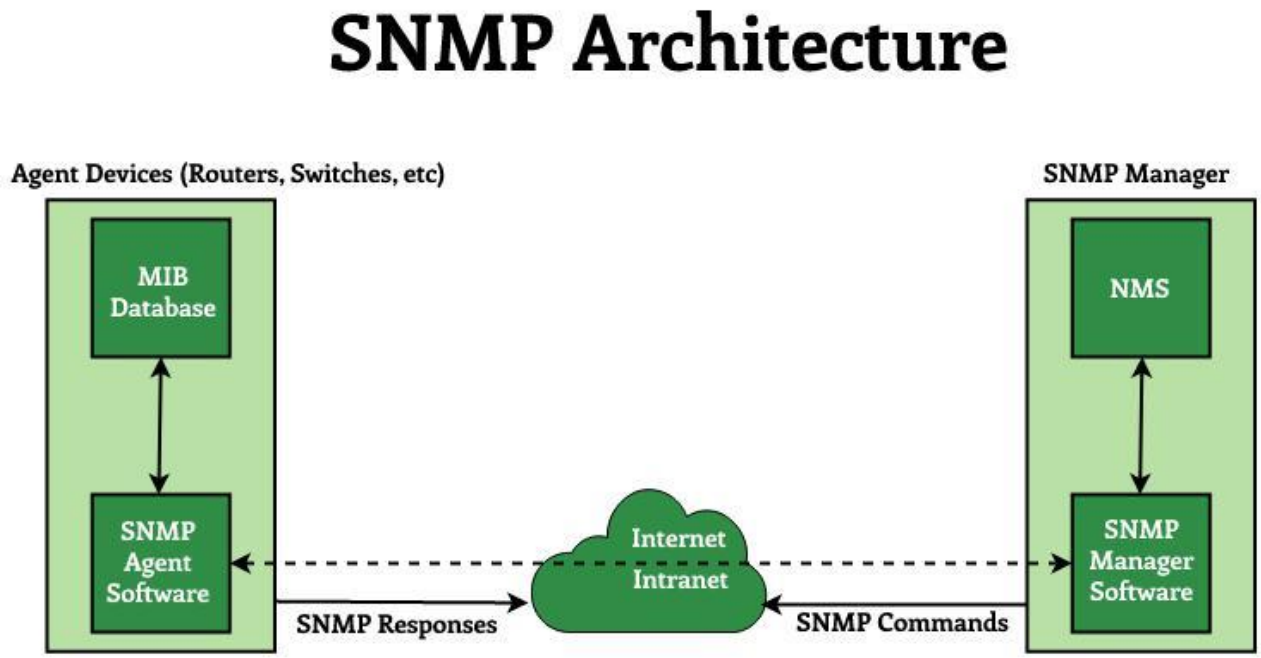

Рисунок 1.5 – Архітектура SNMP протоколу

1.8 Інтеграція SNMP з Zabbix server

Інтеграція SNMP (Simple Network Management Protocol) з сервером Zabbix є фундаментальним процесом для ефективного моніторингу та управління мережевими пристроями. SNMP дозволяє збирати інформацію та керувати мережевими пристроями, такими як маршрутизатори, комутатори та інші мережеві компоненти. Детальний огляд процесу інтеграції SNMP з сервером Zabbix виглядає наступним чином Налаштування агента SNMP на мережевому пристрої Першим кроком є налаштування агента SNMP на мережевому пристрої. Це включає в себе налаштування параметрів SNMP, таких як версія протоколу (SNMPv1, SNMPv2c, SNMPv3), рядки спільноти для SNMPv1 і SNMPv2c, налаштування аутентифікації

та шифрування для SNMPv3. Налаштуйте сервер Zabbix для роботи з SNMP: Після налаштування агента, сервер Zabbix потрібно налаштувати для збору даних через SNMP. Для цього необхідно створити новий мережевий пристрій в Zabbix і вказати метод зв'язку (SNMP), адресу пристрою та інші необхідні параметри в залежності від версії SNMP, яка буде використовуватися. Використовуйте MIB-файли для визначення метрик моніторингу: Файли Management Information Base (MIB) визначають об'єкти, які можна контролювати за допомогою SNMP; імпортуйте файли MIB в Zabbix або використовуйте стандартний ідентифікатор об'єкта (OID) для визначення конкретних показників, які потрібно збирати з мережевих пристроїв Вам потрібно визначити конкретні показники, які потрібно збирати з мережевих пристроїв, використовуючи стандартні OID (ідентифікатори об'єктів).

Створення та налаштування шаблонів у Zabbix Шаблони Zabbix використовуються для групування інформації та налаштувань моніторингу, які можна застосувати до багатьох пристроїв; у випадку SNMP це налаштування типів елементів даних, тригерів виявлення несправностей, графіків та інших компонентів звітності. .

Налаштування пасток SNMP в Zabbix Пастки SNMP дозволяють отримувати сповіщення від мережевих пристроїв при виникненні певних подій. Ви повинні налаштувати обробку пасток в Zabbix, включаючи створення інтерфейсу пасток SNMP і правил для виявлення і обробки цих сповіщень.

Моніторинг та аналіз даних Після налаштування Zabbix може збирати дані з мережевих пристроїв через SNMP і використовувати їх для моніторингу стану мережі, аналізу продуктивності, виявлення і вирішення проблем.

Керування конфігурацією та оновленнями Керування мережевими змінами та оновленнями конфігурації в Zabbix є важливим для підтримання актуального та точного моніторингу. Це включає оновлення шаблонів, зміну налаштувань агентів і підтримку нових версій SNMP. Забезпечення безпеки Налаштування безпечних методів аутентифікації та шифрування важливо для захисту мережевої інформації від несанкціонованого доступу, особливо при використанні SNMPv3.

Інтеграція SNMP з серверами Zabbix є потужним інструментом для моніторингу та управління мережевою інфраструктурою. Він надає детальну інформацію про стан

мережевих пристроїв, дозволяючи швидко реагувати на проблеми і підвищувати загальну продуктивність мережі.

1.9 Огляд системи моніторингу Zabbix

Zabbix - це високопродуктивна, універсальна і адаптивна система моніторингу та управління мережею та інфраструктурою, що характеризується своєю універсальністю і широким спектром функцій. Поширювана під ліцензією з відкритим вихідним кодом GPLv2, система пропонує користувачам велику гнучкість і можливості налаштування, що робить її ідеальною для широкого спектру застосувань - від малого бізнесу до великих корпоративних мереж. Архітектура Zabbix складається з декількох ключових компонентів, які взаємодіють між собою, утворюючи міцну і надійну основу для комплексного моніторингу всієї мережевої інфраструктури. Включаючи сервери, проксі-сервери, агенти, веб-інтерфейси і бази даних, Zabbix забезпечує комплексне рішення проблем моніторингу, від збору даних до їх аналізу, зберігання і візуалізації. Збір даних в системі Zabbix здійснюється за допомогою агентів, встановлених на контрольованих пристроях, і SNMP для комплексного моніторингу мережевих пристроїв. Для більш специфічного моніторингу фізичних серверів використовується IPMI для більш глибокого і детального аналізу стану обладнання. Зібрані дані зберігаються в централізованій реляційній базі даних, що забезпечує надійне довготривале зберігання критично важливої інформації. Система структурована за допомогою шаблонів і правил, що дозволяє налаштовувати її відповідно до конкретних потреб користувачів. Моніторинг у режимі реального часу та візуалізація даних за допомогою різноманітних графіків і діаграм є одними з головних переваг Zabbix. Це дозволяє адміністраторам миттєво реагувати на

проблеми та аналізувати мережеві тенденції. Сповіщення та автоматичні дії спрощують процес управління мережею та дозволяють автоматично реагувати на критичні події. Інтеграція з іншими системами через API та наявність різноманітних плагінів і розширень, розроблених активною спільнотою, ще більше розширюють функціональність Zabbix. Це робить його ідеальним рішенням для інтеграції з існуючою інфраструктурою та розвитку мережевого моніторингу. Безпека є одним з пріоритетних напрямків Zabbix, і для забезпечення конфіденційності та захисту даних використовуються найсучасніші механізми аутентифікації та шифрування. Система також має високу масштабованість і може пристосовуватися до мережевих інфраструктур, що розширюються, що робить її ідеальним рішенням для великих підприємств і центрів обробки даних. Активна спільнота користувачів і розробників постійно підтримує і вдосконалює систему, забезпечуючи її довгострокову придатність і ефективність. В цілому, Zabbix є відмінним вибором для комплексного моніторингу та управління мережевою інфраструктурою, забезпечуючи стабільність, безпеку і високу продуктивність для різноманітних бізнес-потреб.

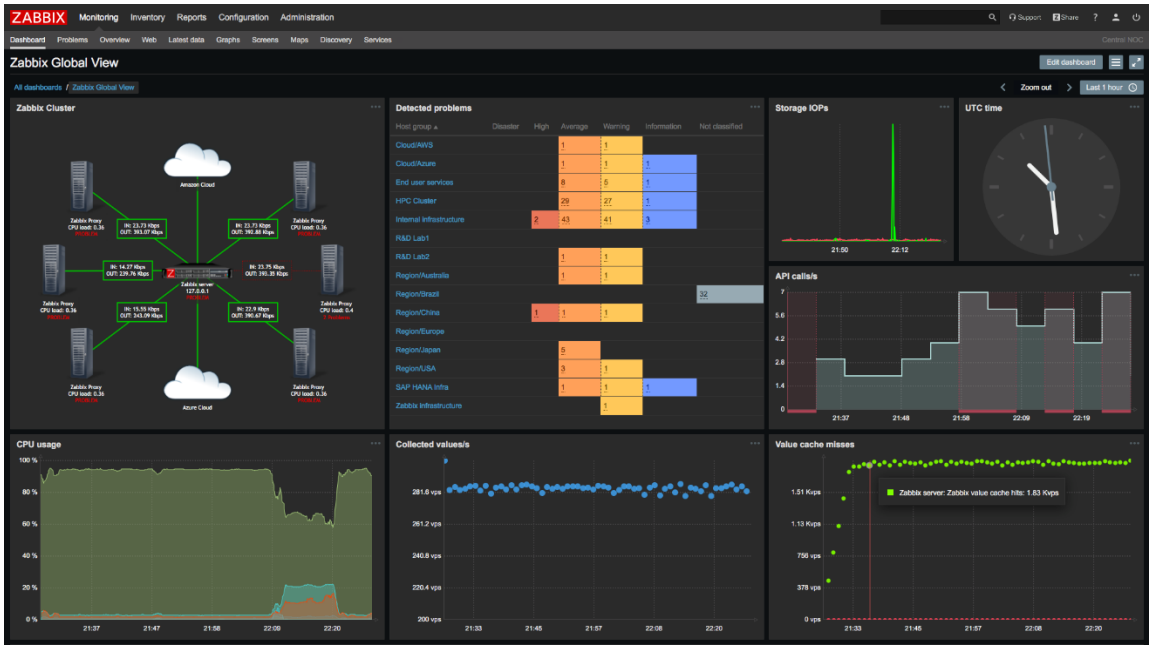

Рисунок 1.6 – Приклад головної сторінки Zabbix

1.10 Порівняння з іншими системами моніторингу

Порівняння Zabbix з іншими системами моніторингу є важливим кроком у виборі найкращого рішення для задоволення конкретних потреб і вимог вашої організації. Ключові відмінності та переваги, які роблять одну систему більш придатною, ніж інша для конкретного випадку використання. Zabbix має певні переваги над Nagios з точки зору масштабованості та розподіленого моніторингу завдяки своїй агентно-орієнтованій архітектурі. Крім того, Zabbix виділяється складною системою оповіщення та автоматизованих дій, що робить її простішою у використанні та управлінні. У той же час, Nagios має більше додаткових розширень і плагінів, але їх підтримка не є стабільною. Порівнюючи Zabbix і Prometheus, важливо відзначити, що Prometheus, написаний на Go, є легким, швидким і надає вбудовану підтримку контейнерів. Zabbix, з іншого боку, вважається більш масштабованою системою, яка використовує C++ і підтримує проксі-сервери. Prometheus також може бути більш придатним для моніторингу хмарних рішень. Як інструмент візуалізації даних, Grafana є ідеальним доповненням до Zabbix як повнофункціональної системи моніторингу; інтеграція Zabbix і Grafana дозволяє створювати детальні та привабливі графіки і покращувати візуалізацію даних моніторингу. Порівнюючи Zabbix і Splunk, важливо відзначити, що Splunk фокусується на аналітиці та аналізі логів, тоді як Zabbix є більш традиційною системою моніторингу; Splunk є комерційним продуктом і тому має значні витрати на ліцензію, тоді як Zabbix є безкоштовним і має відкритий код. Порівнюючи Zabbix і SolarWinds, важливо відзначити, що SolarWinds пропонує ряд рішень для моніторингуале пропонує їх за значну вартість ліцензії. Zabbix, з іншого боку, як безкоштовна система з відкритим вихідним кодом, пропонує широкий спектр можливостей моніторингу без додаткових витрат. Icinga є форком Nagios і має на меті покращити його функціональність, тоді як Zabbix розроблявся незалежно; Icinga має архітектуру сервера агентів, подібну до Nagios, і вимагає додаткової конфігурації для встановлення сповіщень, тоді як Zabbix надає простішу і зручнішу

систему сповіщень. Кожна з цих систем має свої особливості, переваги та обмеження і повинна обиратися відповідно до конкретних потреб та вимог організації. Щоб зробити усвідомлений та ефективний вибір, важливо ретельно зважити, які особливості та функції кожної системи найкраще відповідають вимогам вашого бізнесу та інфраструктури.

1.11 Приклад впровадження Zabbix у різних сферах

Впровадження системи моніторингу Zabbix у різних сферах демонструє її гнучкість та здатність задовольняти різноманітні потреби організацій різних масштабів та секторів. Zabbix не тільки сприяє забезпеченню надійності та ефективності, але й підвищує безперервність роботи, завдяки своїм всебічним функціям моніторингу та управління. Системи моніторингу для IT-інфраструктури в корпорації: У великих корпоративних офісах зі складною IT-інфраструктурою, Zabbix надає комплексні можливості моніторингу. Це особливо актуально для компаній з великими дата-центрами, де потрібен постійний контроль за станом серверів, мережевих пристроїв, а також за критичними системними ресурсами. Моніторинг за допомогою Zabbix охоплює широкий спектр метрик, включаючи використання процесора, оперативної пам'яті, мережевого трафіку та стану баз даних, забезпечуючи своєчасне виявлення та реагування на аномалії. Мережевий моніторинг для постачальника послуг Інтернету (ISP): Для ISP, що управляють великими мережами, Zabbix є незамінним інструментом для забезпечення стабільності та доступності послуг. Система дозволяє відстежувати статус та продуктивність мережевих пристроїв, аналізувати трафік та виявляти перевантаження або збої в роботі мережі. Це допомагає підтримувати високий рівень обслуговування та негайно реагувати на будь-які проблеми. Системи

моніторингу для виробничих підприємств: У сфері виробництва, де висока надійність є критично важливою, Zabbix допомагає відстежувати стан виробничого обладнання, такого як машини, конвеєри та автоматизовані системи контролю. Він може контролювати різні параметри, такі як температура, тиск, вологість, а також виконувати моніторинг ефективності та стану обладнання. Завдяки цьому, Zabbix сприяє запобіганню несподіваних зупинок виробництва та оптимізації процесів. Моніторинг хмарних інфраструктур: Для компаній, які активно використовують хмарні сервіси, Zabbix надає можливість інтеграції з хмарними платформами для моніторингу використання ресурсів, витрат та продуктивності. За допомогою Zabbix можна відслідковувати обсяги сховища, обчислювальні потужності та мережевий трафік, а також аналізувати витрати та оптимізувати використання хмарних ресурсів. Моніторинг безпеки мережі: У фінансовому секторі, де безпека мережі є ключовою, Zabbix дозволяє виявляти потенційні кіберзагрози та несанкціонований доступ. Система може аналізувати мережевий трафік, відслідковувати активність користувачів, реєструвати спроби вторгнення та надавати автоматизовані реакції на загрози, що забезпечує високий рівень захисту інформації. Загалом, впровадження системи моніторингу Zabbix у різних сферах діяльності демонструє її універсальність та ефективність. Це робить Zabbix ідеальним рішенням для різних організацій, які прагнуть до оптимізації своїх процесів, підвищення продуктивності та гарантування безпеки своїх мережевих систем.

1.12 Аналіз безпеки в системах моніторингу

Аналіз безпеки в системах моніторингу є ключовим елементом у розробці, впровадженні та експлуатації систем моніторингу, включаючи Zabbix. Це передбачає виявлення потенційних ризиків, вразливостей і загроз, а також розробку

і впровадження стратегій для їх запобігання або пом'якшення. Огляд загроз безпеці систем моніторингу Сюди входить аналіз поширених загроз, таких як несанкціонований доступ, витік даних, вірусні атаки та шкідливе програмне забезпечення. Особлива увага приділяється міркуванням безпеки, пов'язаним із зовнішніми та внутрішніми загрозами, які можуть вплинути на цілісність, доступність і конфіденційність даних моніторингу. Вразливості системи моніторингу У цьому розділі аналізуються загальні вразливості системи моніторингу, включаючи вразливості в окремих компонентах системи Zabbix та її взаємодії з оптичними терміналами C-DATA. Розглядаються вразливості програмного забезпечення, помилки конфігурації та проблеми, пов'язані з фізичною безпекою. Захист даних і принципи конфіденційності Обговорюються методи захисту даних, зібраних і оброблених системами спостереження. Сюди входить шифрування передачі даних, забезпечення цілісності даних, а також різні механізми аутентифікації та авторизації для обмеження доступу до конфіденційних даних. Аналіз ризиків та методи їх зменшення: визначте потенційні ризики, пов'язані з функціонуванням системи моніторингу. Опишіть стратегії для зменшення цих ризиків, включаючи регулярні оновлення та виправлення, резервне копіювання, безпечні протоколи зв'язку та впровадження політики безпеки. Регулярні оновлення та підтримка: Наголосіть на необхідності регулярного оновлення системи моніторингу, щоб запобігти використанню відомих вразливостей. Також обговоріть важливість компетентної технічної підтримки та управління. Обслуговування та управління системою. Дотримання правових норм і стандартів безпеки Поясніть важливість того, щоб системи моніторингу відповідали чинним законам і правилам захисту даних. Це включає заходи для забезпечення конфіденційності, повідомлення про порушення безпеки та інші законодавчі вимоги. Розробити план реагування на інциденти безпеки: важливо розробити детальний план реагування на порушення безпеки та інші інциденти. Сюди входять процедури повідомлення, відновлення після атак, а також аналіз і запобігання подібним інцидентам у майбутньому. Навчання та підготовка персоналу: підкреслюється важливість навчання персоналу з питань кібербезпеки.

Співробітники повинні знати основні принципи безпеки, розпізнавати тактики шахрайства, такі як фішинг, і знати, як діяти в разі підозри на несанкціонований доступ або інші порушення безпеки. Такий аналіз безпеки в системах відеоспостереження є ключовим для забезпечення надійності, цілісності та конфіденційності даних, що обробляються та зберігаються в таких системах, особливо коли Zabbix використовується та інтегрується з оптичними терміналами C-DATA.

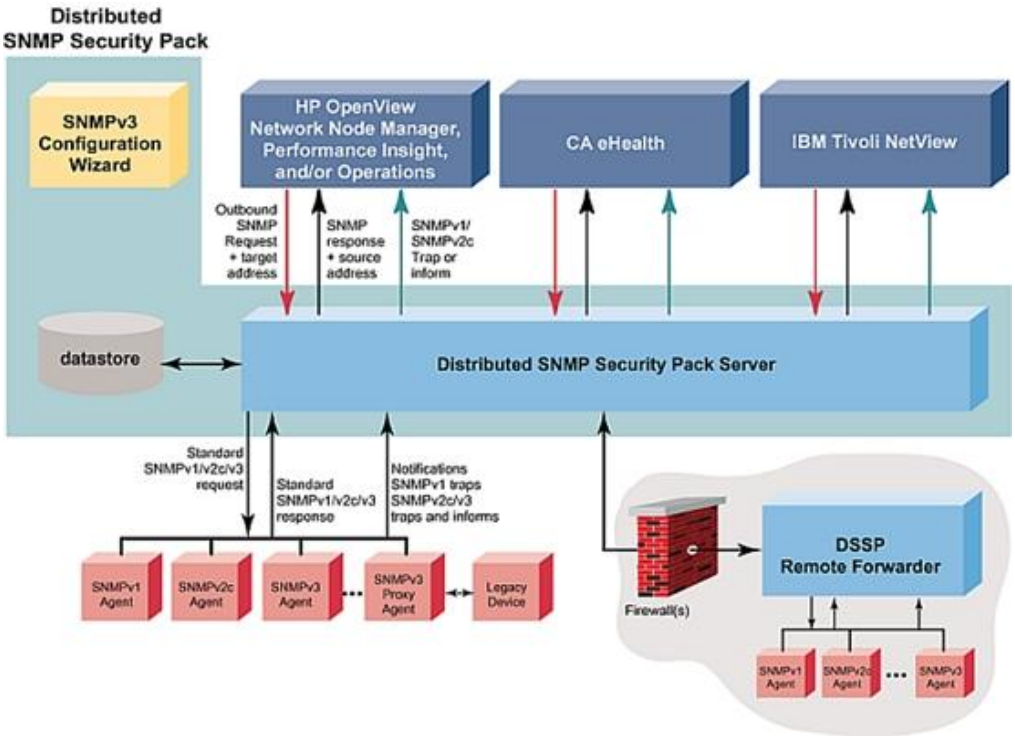

Рисунок 1.7 – Пакет безпеки SNMPv3

2 ПРОЕКТУВАННЯ ТА РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ

Проектування та розробка систем моніторингу вимагають комплексного підходу, починаючи з визначення цілей і потреб, де ви визначаєте основні аспекти та вимоги системи, включаючи мережевий моніторинг, сервери, програмне забезпечення, і виробничі процеси. Вибір системи моніторингу передбачає визначення платформи і архітектури, які відповідають вашим потребам, та включає вибір метрик і джерел даних. Далі йде розробка архітектури системи, планування розгортання серверів та агентів, і створення структур даних для зберігання метрик і журналів. Конфігурація моніторингу охоплює створення хостів, шаблонів, порогових значень, тригерів, оповіщень, і налаштування агентів. Візуалізація та розробка звітів включає створення дашбордів та налаштування звітів і сповіщень. Тестування та налагодження забезпечують точність і ефективність системи, включаючи перевірку метрик і тестування тригерів. Впровадження та підтримка включають планування переходу, навчання персоналу, комунікацію з користувачами, постійну підтримку та оптимізацію системи. Документація та навчання персоналу є критично важливими для ефективного використання системи. Останній етап, розширення та вдосконалення, включає адаптацію системи до нових вимог та можливостей. Вся ця робота вимагає співпраці різних відділів та експертів для створення ефективної та надійної системи моніторингу.

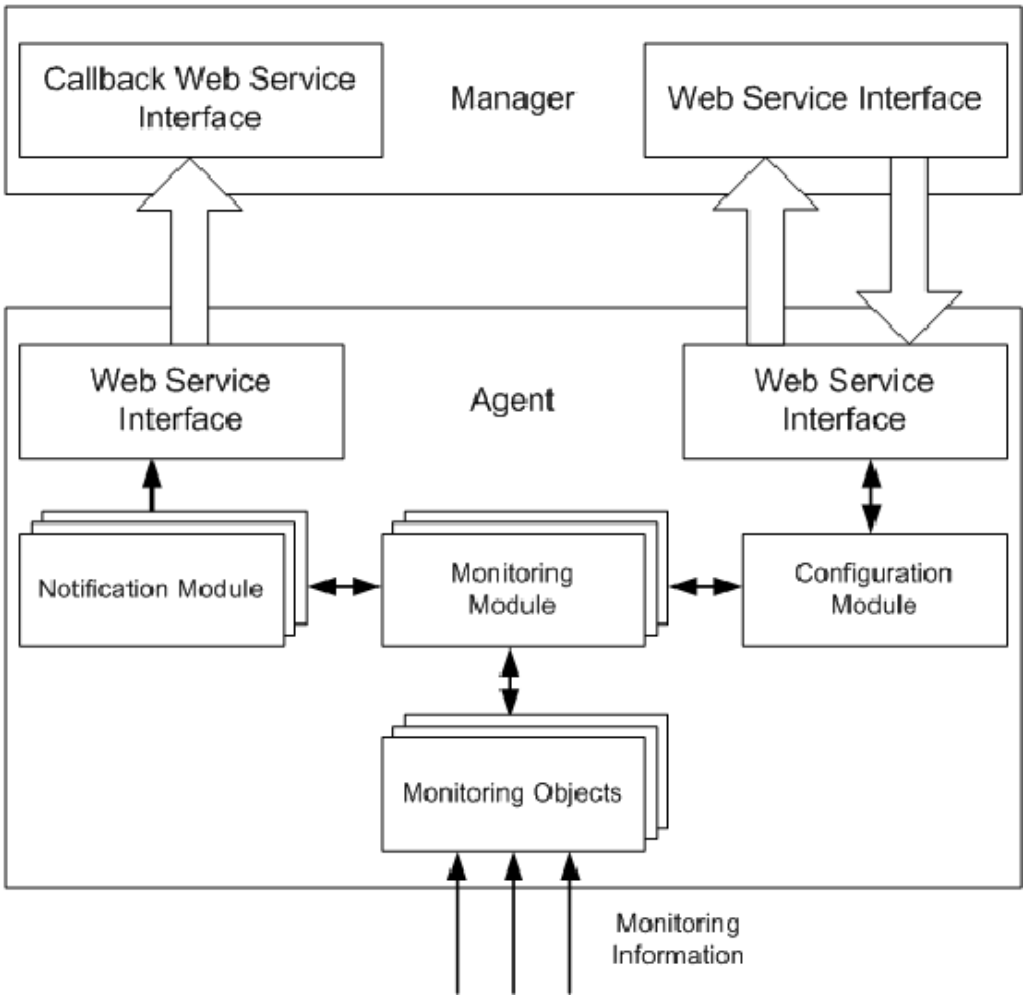

Рисунок 2.1 – Архітектура системи моніторингу

2.1 Визначення вимог до моніторингу

Визначення вимог до моніторингу мережі є фундаментальним кроком у процесі розробки ефективної системи моніторингу. Цей етап вимагає чіткого і всебічного аналізу того, що система повинна відстежувати, вимірювати і контролювати, беручи до уваги характеристики мережі і потреби організації. Цілі моніторингу передбачають визначення основних завдань, які повинна вирішувати система моніторингу. До них відносяться конкретні завдання, які відповідають потребам

організації, такі як забезпечення надійності мережі, виявлення і вирішення проблем, оптимізація продуктивності і підвищення безпеки мережі. Метрики і параметри, які підлягають моніторингу, включають детальний огляд таких показників, як стан мережевого інтерфейсу, завантаження центрального процесора, обсяг мережевого трафіку, доступність послуг, використання мережевих пристроїв та інші важливі параметри. Інтервал збору даних визначає, як часто система збирає дані для аналізу та моніторингу стану мережі. У динамічному мережевому середовищі дані збираються за короткі проміжки часу (наприклад, щохвилини), тоді як у стабільній системі дані збираються з більшими інтервалами. Моніторинг охоплює всі елементи мережі, які потребують контролю, від мережевих пристроїв, таких як маршрутизатори та комутатори, до серверів, додатків, баз даних і хмарних ресурсів. Методи збору даних включають використання різних інструментів і технологій для збору інформації, в тому числі моніторинг на основі агентів і використання таких протоколів, як SNMP, WMI, API і реєстрація подій. Пороги і тригери визначають критичні рівні для різних метрик і параметрів, щоб система моніторингу могла автоматично виявляти аномалії і потенційні проблеми в мережі. Правила сповіщень і дій передбачають налаштування процедур реагування на виявлені проблеми. Від автоматичних повідомлень (електронна пошта, SMS) до виконання конкретних сценаріїв для вирішення проблемних ситуацій. Зберігання та архівування даних охоплює стратегії і методи довгострокового зберігання зібраних даних спостереження, включаючи архівування журналів і встановлення періодів зберігання. Безпека і доступ описує, які заходи вживаються для захисту системи відеоспостереження, такі як аутентифікація користувачів, управління правами доступу і захист від несанкціонованого доступу. Інтеграція з іншими системами визначає можливості та методи інтеграції з іншими інформаційними системами, такими як системи безпеки, резервного копіювання тощо. Аналіз та звітність включає вимоги до аналізу даних та звітності, які забезпечують глибоке розуміння стану мережі та сприяють прийняттю обґрунтованих рішень. Масштабованість і розвиток передбачає визначення потенціалу для збільшення розміру і функціональності системи в міру зростання потреб організації.

Документація та навчання включають розробку детальної системної документації та проведення тренінгів, які дозволять персоналу ефективно використовувати систему. Відповідність - аналіз вимог нормативно-правових актів і стандартів та забезпечення відповідності системи моніторингу цим вимогам. Бюджет і ресурси включають оцінку та визначення фінансових, часових і людських ресурсів, необхідних для реалізації проекту. Специфікація системи моніторингу - це підсумковий документ, який об'єднує всі вищезазначені вимоги і є основою для подальшого проектування та розробки системи моніторингу. Визначення вимог є складним процесом і вимагає ретельного аналізу та планування, щоб забезпечити ефективну розробку та впровадження системи моніторингу в мережеву інфраструктуру організації.

2.2 Вплив моніторингу на діяльність організації

Моніторинг істотно впливає на діяльність організації, покращуючи її ефективність та продуктивність через ряд важливих аспектів. Він забезпечує надійність та доступність інфраструктури, дозволяючи своєчасно виявляти та розв'язувати проблеми, що підвищує репутацію організації. Оптимізація ресурсів, як процесора, пам'яті, дискового простору та мережевого трафіку, сприяє більш ефективному їх використанню, зменшуючи витрати. Моніторинг підвищує продуктивність, виявляючи слабкі місця у процесах і сприяючи їх оптимізації, а також знижує витрати на обслуговування завдяки своєчасному виявленню технічних збоїв. Він гарантує безпеку, виявляючи загрози на ранніх стадіях, і покращує якість обслуговування користувачів, забезпечуючи їхню задоволеність та лояльність. Дані моніторингу служать основою для планування розвитку та масштабування, допомагаючи організації адаптуватися та рости. Автоматизація

збору даних та управління зменшує навантаження на персонал і підвищує загальну ефективність управління. Звіти та аналізи, що надаються моніторингом, підтримують прийняття стратегічних рішень та оптимізацію бізнес-процесів, в той час як дотримання стандартів і нормативних вимог забезпечується через цілісний моніторинг. Управління витратами та оптимізація бізнес-процесів через моніторинг можуть допомогти виявити та усунути нераціональне використання ресурсів, зменшуючи корпоративні витрати. У сукупності ці фактори сприяють поліпшенню стійкості та конкурентоспроможності організації у мінливому ринковому середовищі, підвищуючи її здатність працювати і розширюватися ефективно.

2.3 Вибір оптимальних компонентів системи Zabbix

Вибір найкращих компонентів для вашої системи моніторингу Zabbix - важливе завдання, яке вимагає ретельного аналізу та уваги до деталей для створення найбільш ефективного та надійного рішення. Детальна оцінка кожного компонента і врахування специфічних потреб вашої організації забезпечить високу продуктивність і надійність вашої системи моніторингу. Сервер Zabbix відіграє важливу роль у системі моніторингу, оскільки він відповідає за обробку, аналіз та зберігання даних. Важливо вибрати сервер, який буде достатньо потужним, щоб обробляти великі обсяги даних, що генеруються агентами моніторингу. При виборі сервера слід враховувати такі параметри, як потужність процесора, обсяг оперативної пам'яті та ємність сховища. Це дозволить серверу ефективно обробляти запити і забезпечить стабільну роботу системи. База даних Zabbix необхідна для зберігання історичних даних та конфігурації. Вибір бази даних повинен відображати потреби організації з точки зору обсягу даних і вимог до

продуктивності; потужна реляційна база даних, така як MySQL або PostgreSQL, може забезпечити високу продуктивність і надійність при зберіганні великих обсягів даних. Агенти Zabbix збирають дані з відстежуваних пристроїв і відправляють їх на сервер Zabbix. При виборі агента важливо враховувати його сумісність з різними операційними системами і здатність збирати дані з різних мережевих пристроїв. Агент повинен збирати дані ефективно і з мінімальним впливом на продуктивність системи моніторингу. Проксі-сервери Zabbix відіграють важливу роль у забезпеченні балансування навантаження і географічного розподілу моніторингу. Розміщення проксі-серверів у географічно значущих місцях дозволяє оптимізувати збір даних і зменшити навантаження на центральний сервер. Вибір кількості та розташування проксі-серверів залежить від розміру мережі та розміру організації. Це залежить від розміру мережі та розміру організації. Веб-інтерфейс Zabbix є основним інструментом для візуалізації даних і управління системою моніторингу. Його простота використання та інтуїтивна зрозумілість є ключем до ефективності системи. Інтерфейс повинен бути налаштований відповідно до потреб користувача і підтримувати індивідуальну конфігурацію. Апаратне та мережеве обладнання повинно відповідати технічним вимогам системи Zabbix і забезпечувати достатню швидкість і надійність. Важливо враховувати потреби в швидкості обробки даних і надійності мережевого з'єднання. Безпека системи Zabbix є важливим фактором, тому функції безпеки, включаючи брандмауери, VPN, шифрування даних та інші засоби для забезпечення конфіденційності та цілісності даних, повинні бути обрані належним чином. Сумісність та інтеграція з іншими системами та додатками важлива для забезпечення повної інтеграції Zabbix в загальну IT-інфраструктуру організації. Це включає управління інцидентами, реєстрацію подій, резервне копіювання та інтеграцію з іншими системами. Підтримка та спільнота Zabbix має важливе значення для безперебійної та ефективної роботи системи, забезпечуючи доступ до оновлень, інструкцій та допомоги з усунення несправностей. Перевірка всіх цих міркувань при виборі компонентів системи Zabbix є ключем до створення надійної, ефективної та гнучкої системи моніторингу, яка може задовольнити потреби різних

організаційних сценаріїв.

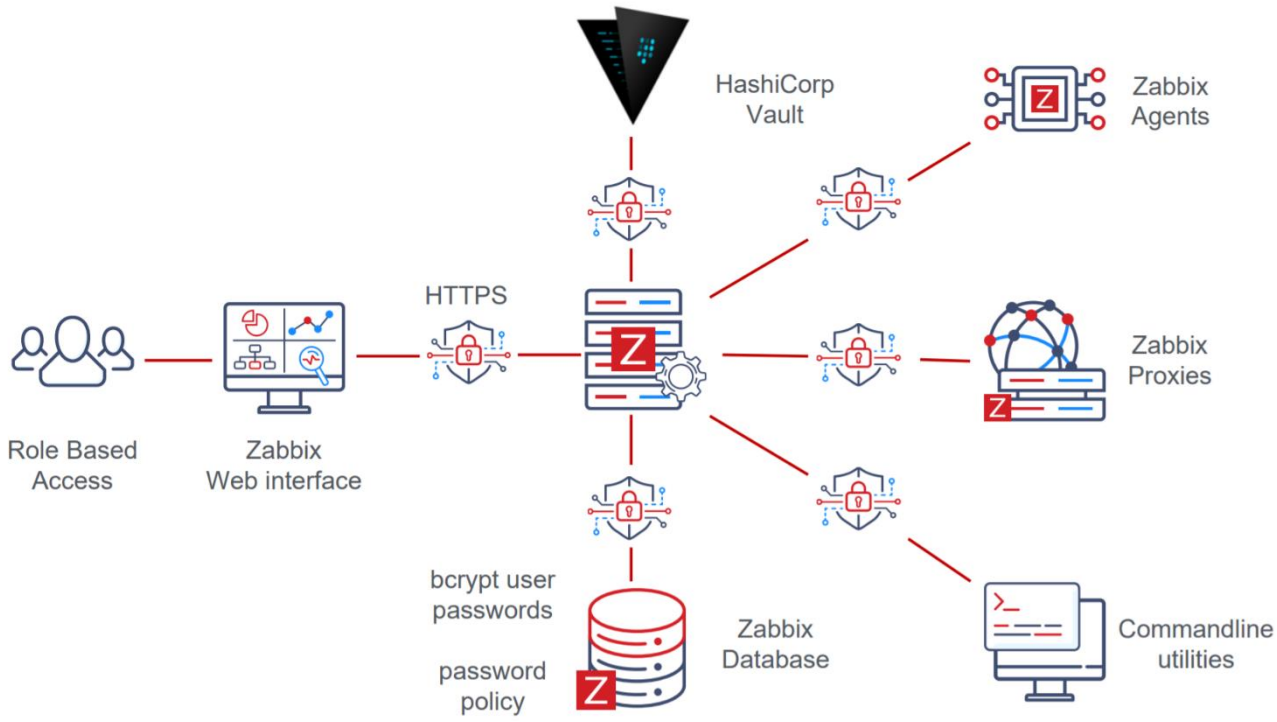

Рисунок 2.2 – Компоненти системи моніторингу Zabbix

2.4 Архітектура системи моніторингу на основі Zabbix

Архітектура системи моніторингу на базі Zabbix відіграє ключову роль у забезпеченні ефективності та надійності середовища моніторингу. Серцем системи є сервер Zabbix, який являє собою центральний вузол для збору, обробки та аналізу даних. Він підтримує базу даних для зберігання конфігураційних даних та історії моніторингу. Важливо, щоб сервер був достатньо потужним для обробки великого

обсягу даних. База даних Zabbix зберігає всі конфігураційні дані та історію моніторингу, при цьому важливо вибрати надійну і продуктивну реляційну базу даних, як-от MySQL або PostgreSQL. Агенти Zabbix встановлюються на моніторовані пристрої та збирають важливу інформацію про їх стан та продуктивність. Вони можуть працювати в активному або пасивному режимах, залежно від конфігурації системи. Проксі-сервер Zabbix розподіляє навантаження та оптимізує мережевий трафік, що особливо корисно для великих розподілених мереж. Веб-інтерфейс Zabbix дозволяє користувачам легко доступатися до системи моніторингу, налаштовувати параметри моніторингу та переглядати зібрані дані. Система сповіщень забезпечує своєчасне інформування адміністраторів про будь-які зміни або проблеми, використовуючи різні канали комунікації, такі як електронна пошта, SMS та інші. Мережева інфраструктура є життєво важливою для забезпечення зв'язку між усіма компонентами системи та її надійності та безпеки. Вибір та конфігурація кожного з цих компонентів вимагають уважного розгляду багатьох аспектів, таких як розмір мережі, продуктивність та вимоги до безпеки. Комплексний підхід до планування та впровадження системи моніторингу на базі Zabbix забезпечить створення гнучкої та надійної мережі, що відповідає потребам сучасних організацій.

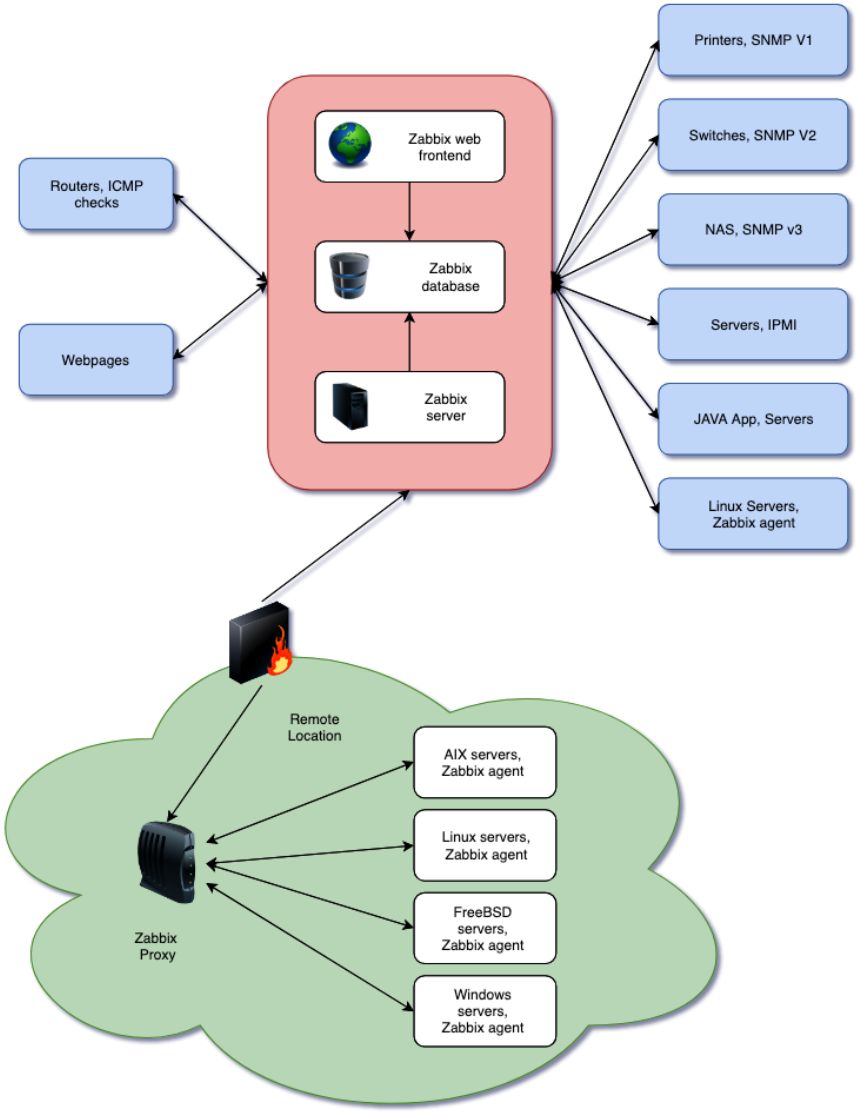

Рисунок 2.2 – Архітектура системи моніторингу Zabbix

2.5 Вибір та конфіграція обладнання та програмного забезпечення

Вибір та налаштування апаратного та програмного забезпечення для системи моніторингу Zabbix є вирішальним для забезпечення її ефективності та надійності. Цей процес включає важливі кроки та рішення. Сервер Zabbix є центральним

елементом системи, і його роль у моніторингу є незамінною. База даних Zabbix відповідає за зберігання даних моніторингу, і при її виборі важливо враховувати багато аспектів. Агенти Zabbix, які збирають дані з моніторованих об'єктів, мають бути правильно налаштовані для забезпечення точності даних. Проксі-сервери Zabbix допомагають масштабувати систему і зменшують навантаження на центральний сервер. Веб-інтерфейс Zabbix є основним інструментом для управління системою, і його налаштування вимагає уваги. Системи сповіщень критично важливі для інформування про будь-які проблеми чи зміни у системі. Фізична та мережева інфраструктура, яка включає мережі та обладнання, забезпечує основу системи. Безпека є невід'ємною частиною системи моніторингу, і важливо забезпечити захист від зовнішніх та внутрішніх загроз. Стійкість системи до втрати даних можна забезпечити через регулярне резервне копіювання та відновлення. Гнучкість і розширена функціональність досягаються через сумісність та інтеграцію з іншими системами. Регулярна підтримка та оновлення важливі для забезпечення стабільності та актуальності системи. Кожен етап вибору та налаштування апаратного та програмного забезпечення системи моніторингу Zabbix вимагає ретельного планування та уваги до деталей, щоб забезпечити стабільну, ефективну та надійну роботу системи в різноманітних умовах та середовищах.

2.6 Налаштування системи Zabbix

Налаштування системи моніторингу Zabbix є складним процесом, що включає кілька ключових етапів для забезпечення її ефективності та відповідності потребам організації. Починається все з встановлення Zabbix, включаючи сервер, базу даних та веб-інтерфейс, з дотриманням інструкцій для обраної операційної системи та

бази даних. Далі налаштовується сервер Zabbix з вказанням параметрів підключення до бази даних, IP-адреси сервера та шляху до файлу журналу подій. Створення та налаштування бази даних Zabbix відбувається через відповідні інструменти управління базами даних. Веб-інтерфейс Zabbix також потребує налаштування для забезпечення зв'язку з сервером і базою даних. Додавання хостів та об'єктів для моніторингу, а також створення шаблонів моніторингу, стандартизує процес та спрощує конфігурацію для різних об'єктів. Важливою частиною є налаштування сповіщень, щоб система могла оперативно інформувати про події та умови. Створення графіків, інформаційних панелей та звітів допомагає у візуалізації та аналізі зібраних даних. Тестування системи моніторингу перевіряє її точність і надійність. Резервне копіювання та відновлення даних, заходи безпеки, регулярна оптимізація та моніторинг стану системи є ключовими для забезпечення її стабільності та безпеки. Оновлення та підтримка програмного забезпечення, а також документація та навчання користувачів, гарантують, що система залишається актуальною та ефективною. Цей комплексний підхід дозволяє максимально використовувати можливості Zabbix, адаптувати систему під конкретні потреби організації та забезпечити ефективний та надійний моніторинг.

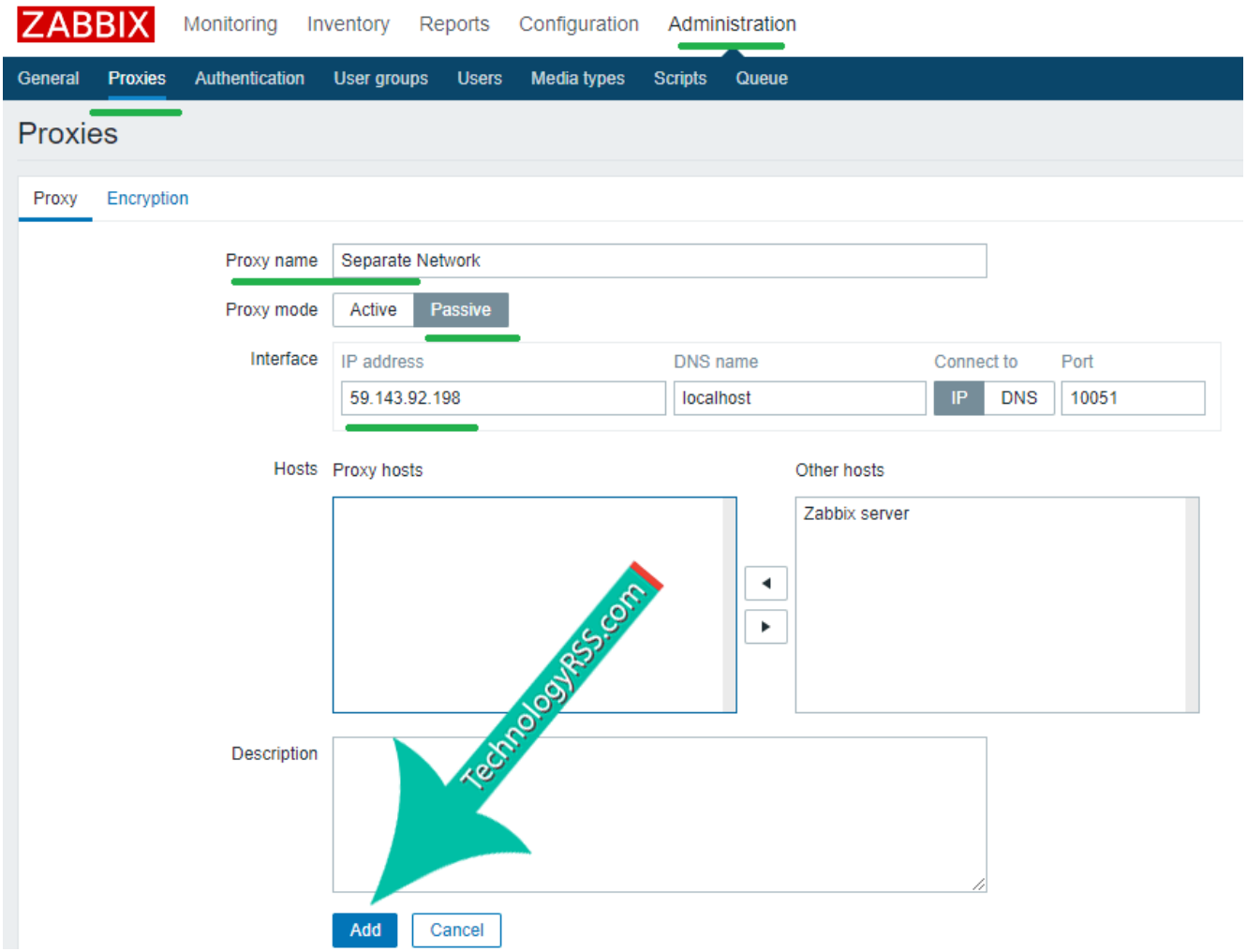

Рисунок 2.3 – Налаштування системи моніторингу Zabbix

2.7 Вивчення механізму збору та візуалізації даних

Вивчення механізмів збору та візуалізації даних у системі моніторингу Zabbix потребує глибокого розуміння її архітектури та основних особливостей. Ефективність процесу забезпечується через взаємодію між різними компонентами системи та добре структурований процес збору, обробки, зберігання та візуалізації даних. Система Zabbix має клієнт-серверну архітектуру з основними компонентами як сервер Zabbix, база даних, агент Zabbix і проксі-сервер. Кожен компонент

відіграє важливу роль у зборі та обробці даних. Zabbix Agent встановлюється на контрольованих пристроях і збирає різні дані, включаючи стан системи та використання ресурсів. Налаштування агента має відповідати характеристикам і потребам кожного пристрою. Зібрані дані передаються на сервер Zabbix для обробки. Важливо, щоб передача даних була надійною та безпечною. Сервер Zabbix використовує реляційну базу даних для зберігання всієї інформації, отриманої від агентів. Оптимізація та правильне налаштування бази даних важливі для забезпечення високої продуктивності та швидкого доступу до даних. Після збору даних Zabbix Server аналізує їх і може виконувати різні дії, наприклад, генерація оповіщень чи інтеграція з іншими системами. Збір даних дозволяє виявити тенденції та визначити зміни в стані систем. Zabbix пропонує широкий спектр інструментів візуалізації даних, що дозволяє користувачам легко інтерпретувати дані та реагувати на проблеми. Система оповіщення Zabbix повідомляє адміністраторів про виявлені події та аномалії. Автоматизація процесів моніторингу та інтеграція з іншими системами роблять Zabbix більш ефективним і гнучким. Безперервна оптимізація та налаштування системи Zabbix відповідно до змінних вимог та інфраструктури організації є важливими для підтримки її продуктивності. Це включає конфігурацію агентів, серверів та баз даних. Детальне вивчення та оптимізація механізмів збору та візуалізації даних дозволяють організаціям ефективно контролювати стан своєї інфраструктури, своєчасно виявляти та вирішувати проблеми та оптимізувати ресурси.

2.8 Розробка плану впровадження та підтримки системи

Розробка плану впровадження та підтримки системи моніторингу як Zabbix є важливою для забезпечення її успішного запуску та довготривалого функціонування. Починається все з аналізу потреб і вимог організації, щоб зрозуміти, які технічні процеси, обладнання та мережеві функції потребують моніторингу та які параметри слід контролювати. Далі йде планування ресурсів, де визначаються необхідні обладнання, програмне забезпечення, персонал та фінансування для підтримки системи на постійній основі. Далі відбувається розробка детальної архітектури системи, де визначаються компоненти системи, їх взаємодія та інтеграція з існуючою IT-інфраструктурою. Потім йде вибір та конфігурація відповідного апаратного та програмного забезпечення, включно з серверами, мережевим обладнанням та самим Zabbix. Після вибору система має бути налаштована та протестована. Особливу увагу слід приділити навчанню персоналу, який буде залучений до експлуатації та обслуговування системи, включаючи технічний персонал та користувачів. Перед повноцінним запуском системи її слід ретельно протестувати, щоб переконатися, що все працює належним чином та відповідає вимогам. Після тестування систему можна впровадити, встановивши її в робочому середовищі та почавши моніторинг необхідних параметрів. Важливо також забезпечити постійну підтримку та управління системою, включаючи регулярні оновлення програмного забезпечення та адаптацію системи до змінних потреб організації. Звітність та аналіз даних відіграють ключову роль у допомозі організації розуміти та оптимізувати свою діяльність. Вони допомагають виявляти слабкі місця та підвищувати продуктивність. Ретельне планування та управління на кожному етапі забезпечують, що система не тільки відповідає поточним потребам, але й гнучка та масштабована для майбутнього.

3 ВПРОВАДЖЕННЯ ТА ТЕСТУВАННЯ СИСТЕМИ НА ПРИКЛАДІ ОБЛАДНАННЯ C-DATA

Впровадження та тестування системи моніторингу Zabbix на обладнанні C-DATA є ключовим для ефективного контролю стану мережевого обладнання. Це вимагає детального планування та виконання кількох кроків. Спочатку визначаються характеристики обладнання C-DATA, яке потребує моніторингу, та збирається вся необхідна технічна документація. Тоді вибирається апаратне чи віртуальне середовище для сервера Zabbix, враховуючи продуктивність та масштабованість. Для забезпечення надійного мережевого з'єднання між сервером Zabbix та обладнанням C-DATA відкриваються необхідні мережеві порти та налаштовуються брандмауери. На кожному пристрої C-DATA встановлюється Zabbix Agent для збору даних, який налаштовується для збору специфічної інформації. Створюються шаблони моніторингу з налаштуваннями для конкретних вимірювань та правила та порогові значення для сповіщень. Після додавання обладнання C-DATA до системи Zabbix проводиться тестовий моніторинг для перевірки збору даних і їх передачі на сервер. Отримані дані аналізуються на точність та відповідність параметрам. Для візуалізації зібраних даних створюються графіки та звіти, а також налаштовуються канали сповіщень, такі як електронна пошта та SMS. Систему постійно оптимізують та оновлюють, враховуючи зміни в обладнанні та середовищі. Також важливо розробити процедури резервного копіювання та відновлення для забезпечення безпеки даних. Системним адміністраторам та користувачам проводять тренінги та підтримується актуальна документація по системі. Такий підхід до впровадження та тестування Zabbix на обладнанні C-DATA дозволяє досягти високої ефективності моніторингу та своєчасного виявлення і вирішення проблем у мережі.

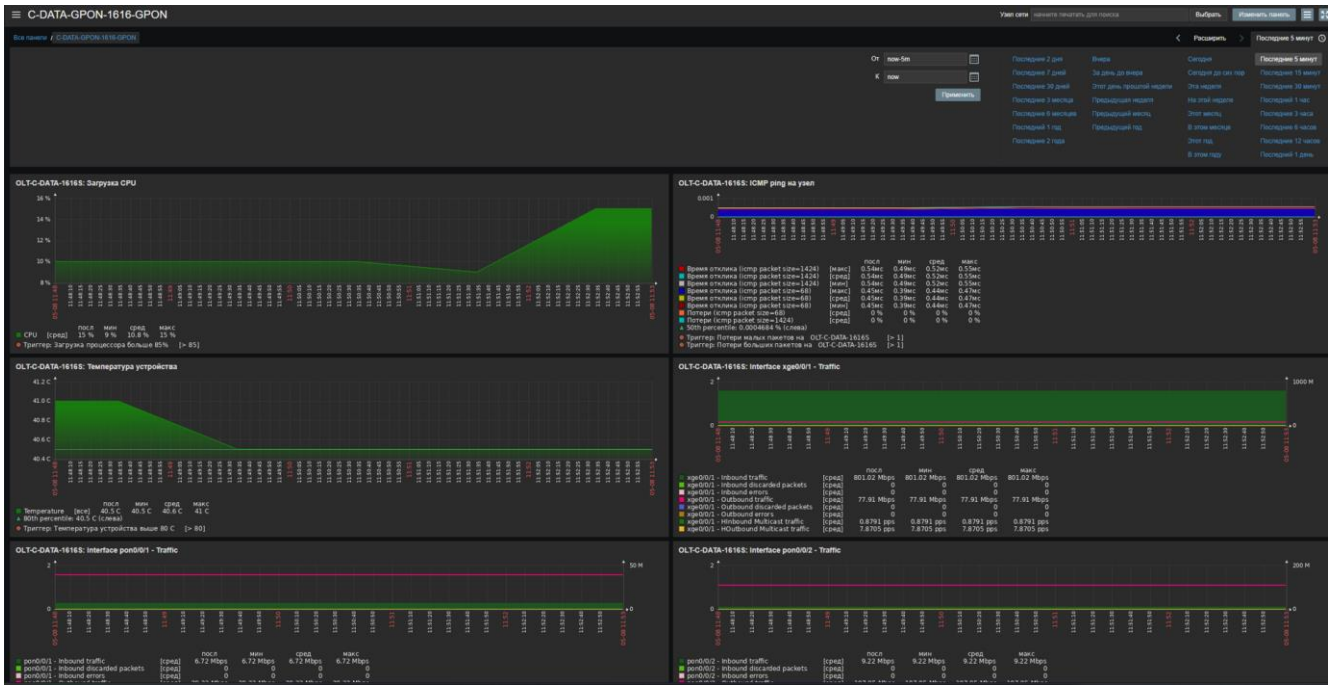

Рисунок 3.1 – Вигляд Zabbix на C-DATA 1616

3.1 Впровадження системи моніторингу

Розгортання системи моніторингу Zabbix на обладнанні C-DATA - це складний процес, що включає детальне планування та багато кроків для забезпечення ефективності та надійності моніторингу. Планування впровадження, на цьому етапі необхідно чітко визначити цілі моніторингу; ви повинні розуміти, які саме аспекти роботи обладнання C-DATA ви хочете контролювати. До них відносяться використання ресурсів (процесор, оперативна пам'ять, диски), мережевий трафік і стан сервісів. Також важливо зібрати необхідну інформацію про обладнання, включаючи специфікації та конфігурацію. Встановлення та налаштування Zabbix Server, на цьому етапі Zabbix Server повинен бути встановлений на обраному обладнанні. Важливо вибрати сервер, який зможе впоратися з обсягом даних, що

відстежуються. Після інсталяції необхідно встановити базу даних і початково налаштувати сервер. Встановлення та налаштування агента, на пристроях C-DATA Збір даних з пристроїв C-DATA вимагає встановлення та налаштування агента Zabbix. Це включає в себе налаштування параметрів збору даних і вказівку адреси сервера Zabbix, на який буде відправлятися зібрана інформація. Створення шаблонів моніторингу та правил моніторингу для ефективного моніторингу пристроїв C-DATA необхідно створити шаблони, які визначають дані, що збираються, і встановити правила, які будуть використовуватися для визначення стану пристроїв. Додавання пристрою до моніторингу, цей крок передбачає додавання пристрою C-DATA до системи Zabbix, призначення створеного вами шаблону і налаштування параметрів моніторингу. Важливо переконатися, що зібрані дані коректно відображаються в системі. Тестування моніторингу перед початком роботи системи необхідно провести тестування. Це дозволить переконатися, що всі компоненти системи працюють коректно, а дані збираються правильно. Створення графіків і звітів, це допоможе візуалізувати та аналізувати зібрані дані. Налаштування сповіщень та оповіщень. Система повинна бути налаштована таким чином, щоб при виникненні проблеми або аномалії адміністратор отримував відповідні сповіщення. Підтримка та моніторинг. Після того, як система моніторингу налаштована, важливо постійно підтримувати та контролювати її роботу. Це включає в себе оновлення конфігурації, розширення покриття моніторингу та вдосконалення системи відповідно до потреб організації.

Впровадження системи моніторингу Zabbix для обладнання C-DATA є складним, але це важливий процес для забезпечення ефективного моніторингу та управління мережевим обладнанням для забезпечення стабільної та безпечної роботи.

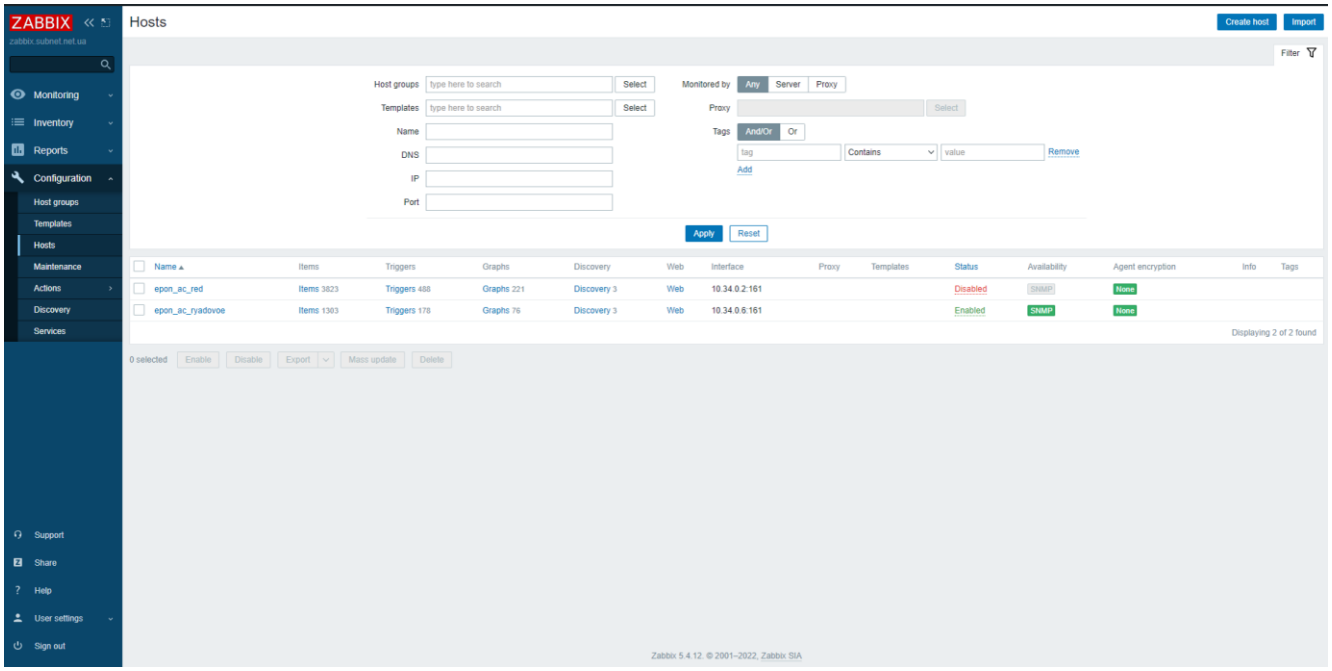

Рисунок 3.2 – Налаштування hosts

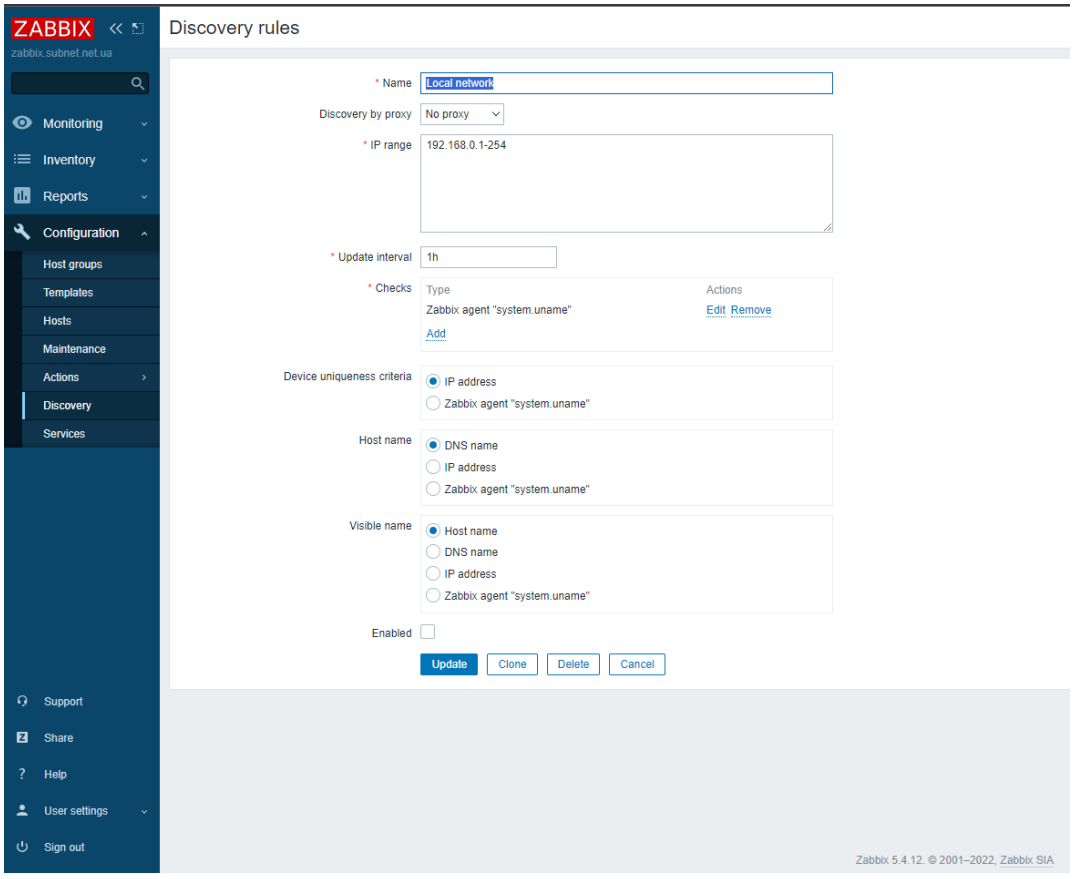

Рисунок 3.3 – Налаштування discovery

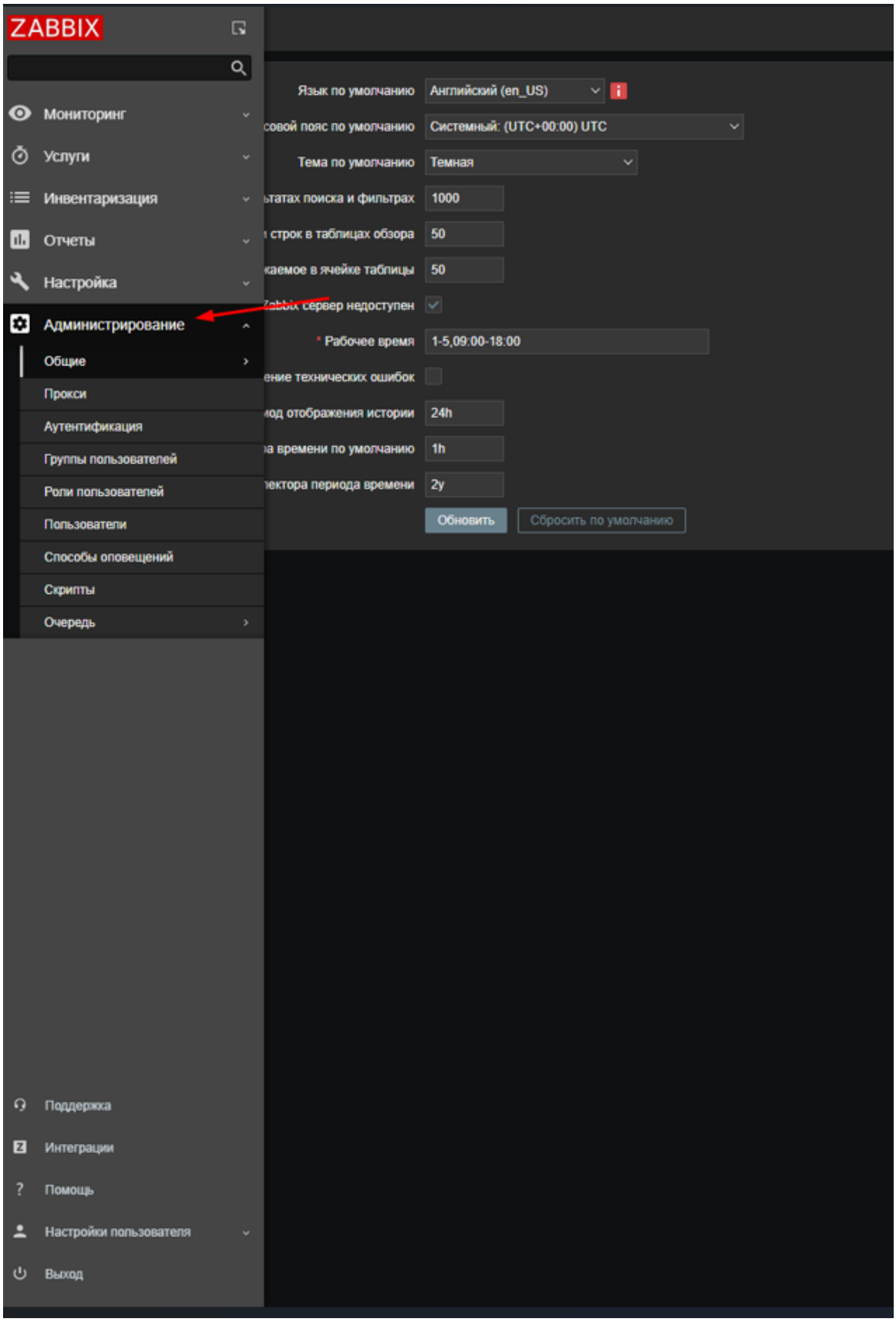

Рисунок 3.4 – Приклад налаштувань general

3.2 Розробка темплейту zabbix для olt c-data

Я успішно розробив індивідуальний шаблон для моніторингу OLT C-DATA в системі Zabbix. На початку процесу я провів детальний аналіз обладнання C-DATA і зібрав всю необхідну технічну інформацію, включаючи діапазони робочих температур, показники продуктивності, інформацію про порт та інші ключові параметри. На основі цього аналізу я визначив ключові показники для моніторингу, включаючи стан порту, трафік, збої інтерфейсу, використання пропускної здатності, стан живлення та інші ключові показники. Після визначення ключових показників ми почали створювати шаблони в Zabbix. Ми створили елементи даних для кожного показника, встановили тип збору даних, наприклад, SNMP або агент Zabbix, а також встановили інтервали збору даних і пороги спрацьовування. Це дозволило нам точно відстежувати стан обладнання та виявляти аномалії і проблеми з продуктивністю. Шаблон було протестовано як на тестових, так і на реальних пристроях C-DATA OLT, щоб переконатися, що збір даних відбувається коректно, а тригери працюють правильно. Після тестування шаблон було скориговано, налаштування оптимізовано, а також додано корисні графіки та інформаційні панелі для візуалізації зібраних даних. Нарешті, я створив документацію для шаблону з описом його функціональності, налаштувань і використання. Я розповсюдив цей шаблон серед інших адміністраторів Zabbix в компанії, щоб забезпечити загальний стандарт моніторингу обладнання C-DATA. Розробка цього шаблону значно підвищила продуктивність і ефективність системи моніторингу, дозволивши здійснювати точний і ефективний моніторинг критично важливих аспектів обладнання C-DATA OLT.

```yaml
zabbix_export:
  version: '6.0'
  date: '2022-09-28T14:04:32Z'
  groups:
    -
      uuid: c79cf0420d594a64afedb5009b0f7f1e
      name: GPON
    -
      uuid: 183adff05abb445f83b63570768ad181
      name: 'OLT C-DATA'
  templates:
    -
      uuid: cd7599393640419e94b8fa3c9deef71d
      template: 'Template C-DATA OLT GPON'
      name: 'Template C-DATA OLT GPON'
      groups:
        -
          name: GPON
        -
          name: 'OLT C-DATA'
      items:
        -
          uuid: 03e33c21040a49d08be4715cef4379aa
          name: 'Firmware Version'
          type: SNMP_AGENT
          snmp_oid: .1.3.6.1.4.1.17409.2.3.1.3.1.1.8.1.0
          key: cdataFirmware
          delay: 30m
          history: 7d
          trends: '0'
          value_type: CHAR
          tags:
            -
              tag: Application
              value: Health
        -
          uuid: 8c3ec1925f1a451f9a0ef9073708c4ce
```

Рисунок 3.5 – Вигляд темплейту для OLT C-DATA

```
288          -
289            macro: '{#OPERSTAT}'
290            value: '1'
291            formulaid: A
292        lifetime: 7d
293        item_prototypes:
294          -
295            uuid: 09460b6c6b1e444a91ab0e7dcb554403
296            name: 'ONT online на порту - {#PORTNAME}'
297            type: SNMP_AGENT
298            snmp_oid: '.1.3.6.1.4.1.17409.2.3.3.1.1.8.{#SNMPINDEX}'
299            key: 'onuOnline[{#SNMPINDEX}]'
300            history: 7d
301            trends: 30d
302            tags:
303              -
304                tag: Application
305                value: Interfaces
306            trigger_prototypes:
307              -
308                uuid: 301c177816de4ea1b4061e0e47d6f951
309                expression: '(last(/Template C-DATA OLT GPON
                       /onuOnline[{#SNMPINDEX}],#2) - last(/Template C-DATA
                       OLT GPON/onuOnline[{#SNMPINDEX}]) ) > 10'
310                recovery_mode: RECOVERY_EXPRESSION
311                recovery_expression: '(last(/Template C-DATA OLT GPON
                       /onuOnline[{#SNMPINDEX}],#2) - last(/Template C-DATA
                       OLT GPON/onuOnline[{#SNMPINDEX}]) ) = 0'
312                name: '{HOSTNAME} {#PORTNAME} резкое изменение
                       пользователей >10'
313                priority: HIGH
314                type: MULTIPLE
315      -
316        uuid: 883b4ece449741a5860e08ba5e401da0
317        name: OnuInterfaces
318        type: SNMP_AGENT
319        snmp_oid: 'discovery[{#IFSTATUS}, IF-MIB::ifOperStatus, {#IFNAME}
```

Рисунок 3.6 – Приклад перевірки стану ONT на порту

```
993            sortorder: '5'
994            color: '960000'
995            calc_fnc: MIN
996            item:
997              host: 'Template C-DATA OLT GPON'
998              key: 'icmppingsec[,5,1000,68,500]'
999          -
1000           sortorder: '6'
1001           color: FF7043
1002           item:
1003             host: 'Template C-DATA OLT GPON'
1004             key: 'icmppingloss[,10,1000,68,500]'
1005         -
1006           sortorder: '7'
1007           color: 00C8C8
1008           item:
1009             host: 'Template C-DATA OLT GPON'
1010             key: 'icmppingloss[,10,1000,1424,500]'
1011     -
1012       uuid: 997389b07cb7478f86c1a0f3339d544f
1013       name: 'Загрузка CPU'
1014       graph_items:
1015         -
1016           drawtype: GRADIENT_LINE
1017           color: 1A7C11
1018           item:
1019             host: 'Template C-DATA OLT GPON'
1020             key: health.cpu
1021     -
1022       uuid: 87406a9c0d4244f081e885546d5fd5dc
1023       name: 'Температура устройства'
1024       percent_left: '80'
1025       graph_items:
1026         -
1027           drawtype: GRADIENT_LINE
1028           color: 1A7C11
1029           calc_fnc: ALL
1030           item:
```

Рисунок 3.7 – Приклад перевірки стану CPU та температури на OLT

3.3 Тестування роботи системи та виявлення недоліків

Я розробив детальний план для впровадження та тестування системи моніторингу Zabbix на обладнанні C-DATA, який включає послідовні кроки для ефективного моніторингу. Спочатку я визначив конкретні цілі моніторингу, зібрав інформацію про обладнання та обрав сервер Zabbix, враховуючи обсяг моніторингу та доступні ресурси. Далі я завантажив та встановив Zabbix Server, налаштувавши підключення до бази даних та інші параметри. Встановлення та налаштування Zabbix Agent на обладнанні C-DATA було наступним кроком, включаючи налаштування параметрів підключення до сервера та визначення параметрів моніторингу. Я створив шаблони та правила моніторингу для збору даних, а потім додав обладнання до моніторингу на сервері Zabbix. Після тестування системи для забезпечення коректної роботи даних та оповіщень, я створив графіки та звіти для аналізу даних, налаштував сповіщення та сповіщення для виявлення та управління проблемами. Нарешті, я зосередився на постійній підтримці та моніторингу системи, оновлюючи налаштування та додаваючи нове обладнання до моніторингу за потреби.

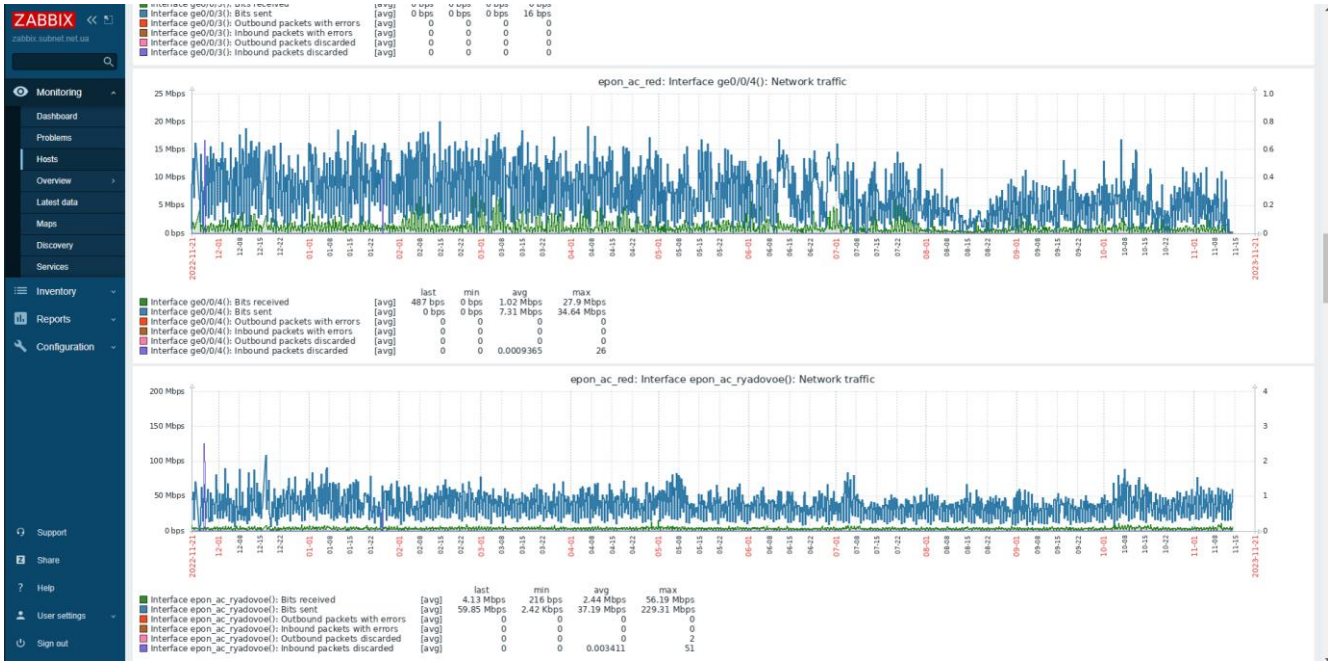

Рисунок 3.8 – Приклад графіків у Zabbix

3.4 Аналіз взаємодії з оптичними терміналами

Аналіз взаємодії з оптичними терміналами є важливою частиною системи моніторингу, особливо з точки зору інтеграції з такими системами, як Zabbix. Існує кілька важливих аспектів цього процесу, які необхідно враховувати для забезпечення ефективної та надійної роботи системи. Перш за все, важливо розуміти роль і функції оптичних терміналів в мережевій інфраструктурі. Оптичні термінали використовуються для передачі великих обсягів даних на великі відстані на високих швидкостях. Оптичні термінали є важливим компонентом оптичних мереж і забезпечують інтерфейс між волоконно-оптичними лініями та мережевим обладнанням. Для ефективного моніторингу оптичних терміналів їх необхідно інтегрувати з системами моніторингу, такими як Zabbix. Це передбачає налаштування відповідних протоколів зв'язку, таких як SNMP, для збору даних про стан і продуктивність оптичних терміналів. Важливо відстежувати такі параметри, як загальна пропускна здатність, несправності мережі, стан портів і температура обладнання. Це може допомогти виявити потенційні проблеми, такі як перевантаження мережі, фізичне пошкодження оптоволокна та апаратні проблеми. Система моніторингу повинна надавати інструменти для швидкого виявлення та усунення проблем з оптичними терміналами. До них відносяться повідомлення про аномалії, автоматичне виявлення несправностей, а також інструменти діагностики та відновлення системи. Особливу увагу слід приділити безпеці оптичних терміналів. Це включає захист від несанкціонованого доступу, шифрування даних і заходи щодо запобігання атакам на мережеву інфраструктуру. Дані, зібрані системою моніторингу, необхідно аналізувати. Системи моніторингу можна використовувати для оптимізації продуктивності оптичних терміналів. Це включає в себе балансування навантаження, оптимізацію шляхів передачі даних і планування розширення мережевої інфраструктури. Надання точних звітів і документації про стан і продуктивність оптичних терміналів має важливе значення для планування майбутніх інвестицій і підтримки високого рівня обслуговування.

Регулярна підтримка та оновлення оптичних терміналів і пов'язаного з ними програмного забезпечення гарантує, що оптичні термінали працюють надійно і захищені від вразливостей безпеки. Ефективна взаємодія з оптичними терміналами через систему моніторингу, таку як Zabbix, вимагає глибокого розуміння технічних аспектів оптичного мережевого обладнання та ретельного планування і налаштування системи моніторингу. Це забезпечує не тільки високу продуктивність і надійність мережі, але і швидке реагування на проблеми і питання.

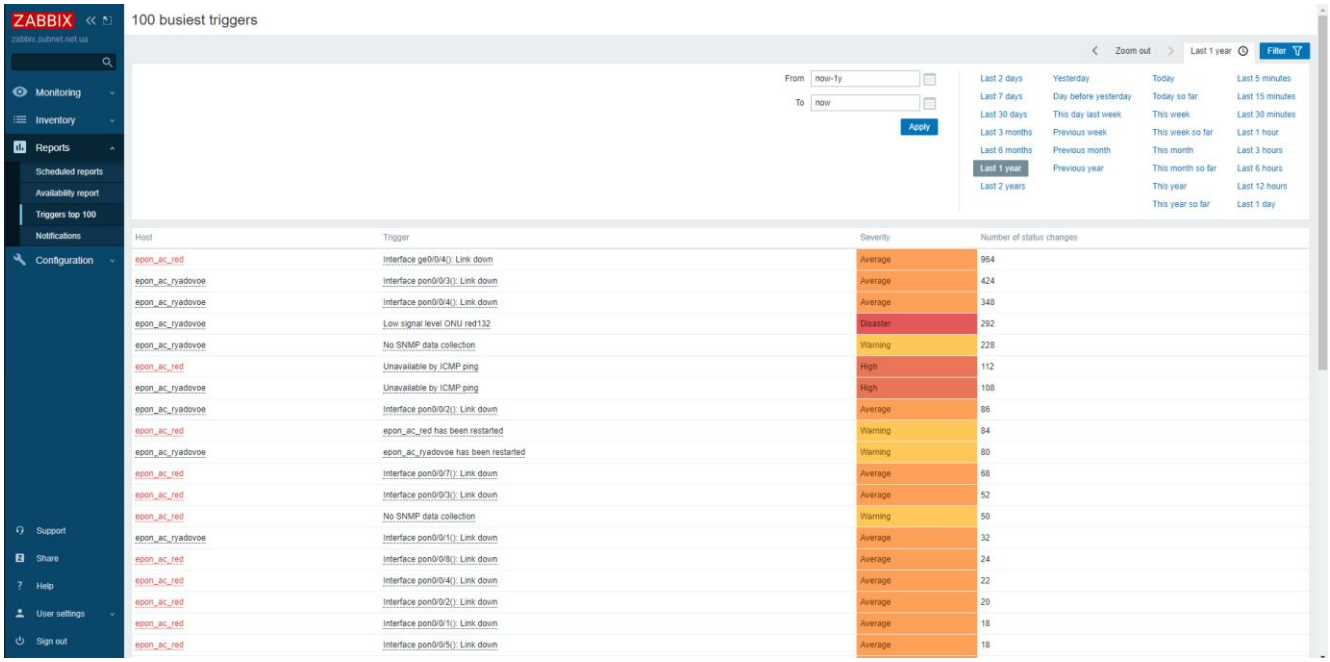

Рисунок 3.9 – Приклад трігерів сповіщень у Zabbix

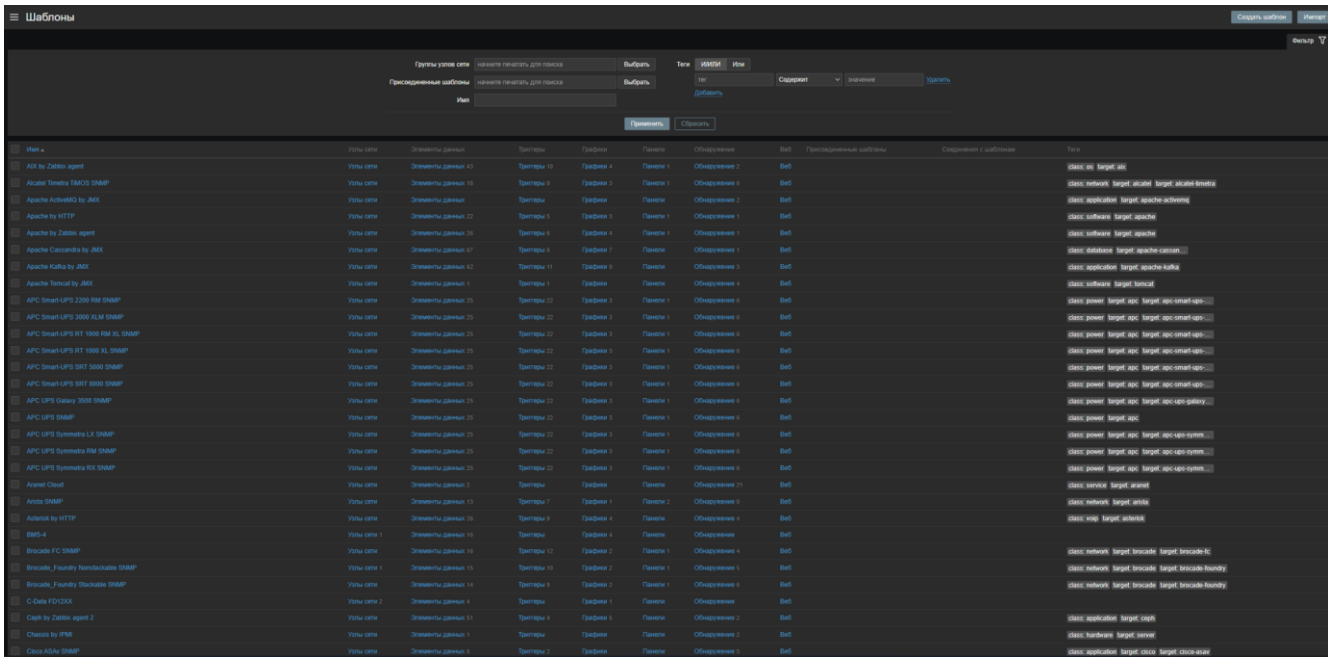

Рисунок 3.10 – Приклад доступних шаблонів у Zabbix

3.5 Особливості інтеграції з оптичними терміналами C-DATA

Інтеграція з оптичними терміналами C-DATA в систему моніторингу, таку як Zabbix, вимагає глибокого розуміння технічних характеристик оптичного терміналу і деталей його взаємодії з системою моніторингу. Перш за все, важливо розвинути технічне розуміння оптичних терміналів C-DATA. Це включає знання характеристик пристрою, таких як швидкість передачі даних, типи оптичних з'єднань, підтримувані протоколи та масштабованість. Важливо переконатися, що оптичні термінали C-DATA сумісні з системами моніторингу. Це включає в себе перевірку підтримки протоколів моніторингу, таких як SNMP, і забезпечення можливості відправки відповідних вимірювань і даних про стан в систему моніторингу. Процес інтеграції передбачає налаштування оптичних терміналів C-

DATA для роботи з системою Zabbix. Це включає налаштування мережевих параметрів, конфігурацію агентів SNMP та інші індивідуальні налаштування. Важливо надійно контролювати ключові параметри оптичного терміналу, такі як пропускна здатність, несправності лінії, стан портів і загальний стан обладнання. Це дозволяє виявляти і вирішувати проблеми мережі. Безпека є вирішальним фактором при інтеграції з оптичними терміналами. Необхідно вжити відповідних заходів для захисту передачі даних, запобігання несанкціонованому доступу та забезпечення цілісності даних. Використання скриптів і засобів автоматизації для ефективного моніторингу оптичних терміналів може значно підвищити ефективність і скоротити час реагування на інциденти. Це може підвищити ефективність і скоротити час реагування на інциденти. Сюди входить автоматичне виявлення аномалій і оповіщення персоналу. Переконайтеся, що доступна детальна документація з інтеграції та експлуатації волоконно-оптичних терміналів. Також важливо мати план підтримки та обслуговування обладнання. Після встановлення системи слід регулярно оцінювати її ефективність, щоб виявити потенційні проблеми та оптимізувати процес моніторингу. Інтеграція оптичних терміналів C-DATA з такою системою моніторингу, як Zabbix, вимагає ретельного планування, розуміння технічних аспектів і постійного управління. Ефективна інтеграція забезпечує високу продуктивність оптичної мережі, а також надійність і безпеку передачі даних.

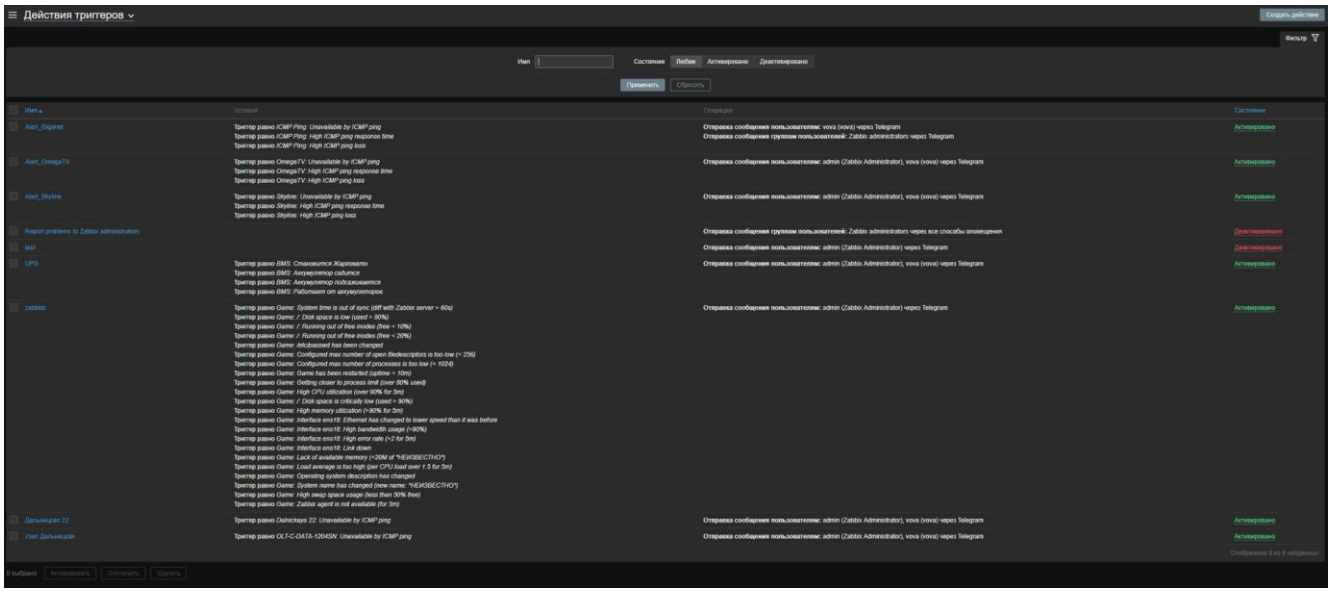

Рисунок 3.11 – Опис трігерів сповіщень у Zabbix

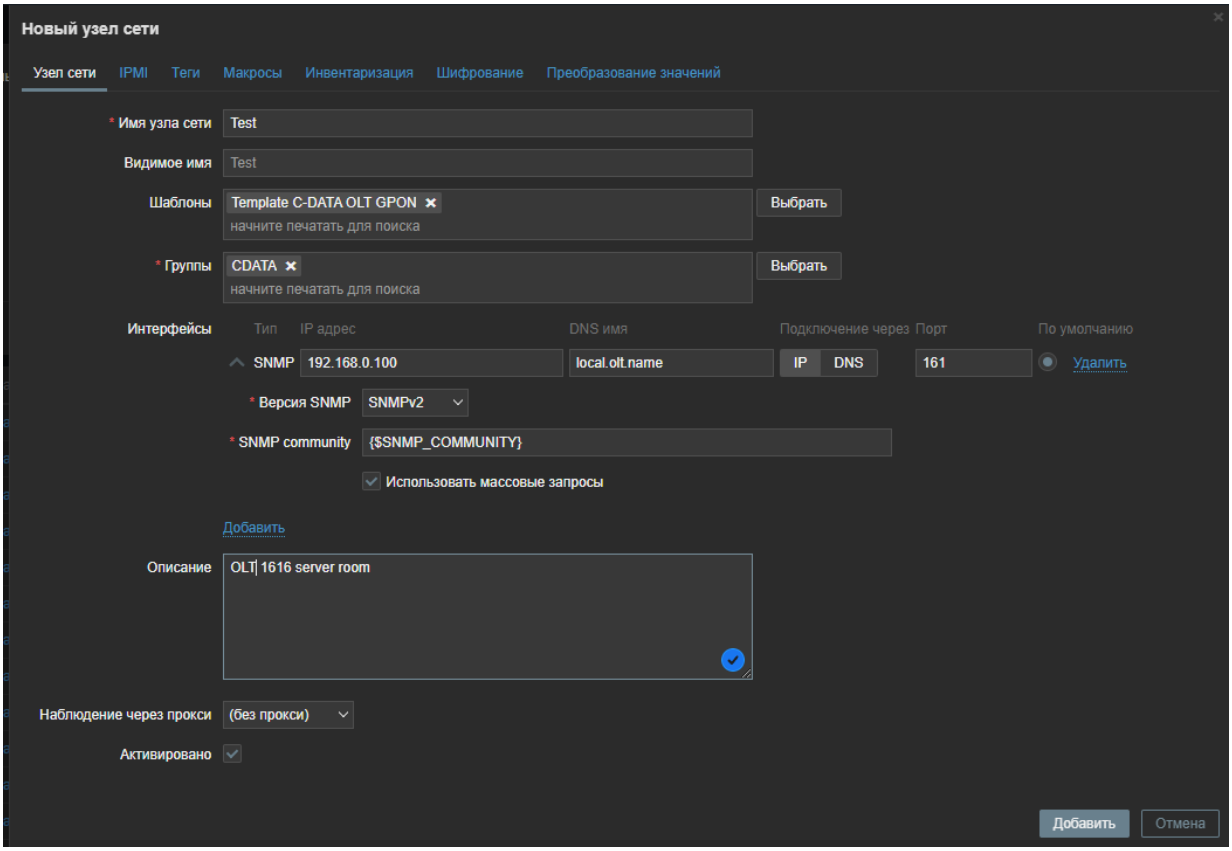

Рисунок 3.12 – Приклад інтеграції нового OLT у Zabbix з шаблоном

3.6 Оцінка відповідності системи вимогам безпеки

Оцінка відповідності системи вимогам безпеки є важливою частиною управління інформаційною безпекою, особливо для систем моніторингу, таких як Zabbix. Є кілька ключових аспектів цього процесу, кожен з яких має свої особливості та важливість. Оцінка відповідності починається з визначення вимог і стандартів безпеки, яким повинна відповідати система. Це можуть бути міжнародні стандарти, такі як ISO/IEC 27001, або національні законодавчі вимоги. Важливо розуміти всі аспекти, які необхідно враховувати, включаючи захист даних, контроль доступу та криптографічний захист. Оцінка відповідності починається з детального аналізу існуючої архітектури безпеки системи. Це включає огляд налаштувань, політик, процедур і засобів контролю, які вже існують. Особливу увагу слід приділити контролю доступу, шифруванню, аудиту та моніторингу інцидентів безпеки. Важливим кроком є виявлення та оцінка потенційних ризиків і вразливостей, які можуть вплинути на безпеку системи. Це передбачає аналіз потенційних загроз із зовнішніх і внутрішніх джерел та визначення їхнього потенційного впливу на конфіденційність, цілісність і доступність системи. На основі оцінки ризиків і вразливостей розробити і впровадити необхідні заходи безпеки для зниження ризиків до прийнятного рівня. Це включає вдосконалення політики безпеки, посилення механізмів автентифікації та авторизації, шифрування для захисту даних, а також впровадження систем виявлення інцидентів безпеки та реагування на них. Безпека системи повинна регулярно перевірятися за допомогою аудитів, тестів на проникнення та оцінки вразливостей. Регулярно перевіряйте безпеку системи за допомогою аудитів, тестів на проникнення та оцінки вразливостей. Це гарантує своєчасне виявлення та усунення слабких місць у системі безпеки. Навчання працівників є ключовим елементом захисту системи. Працівники повинні бути обізнані з політикою безпеки, потенційними загрозами та найкращими практиками безпеки. Ведення детальної документації та звітів про стан безпеки, оцінки та інциденти є важливим для демонстрації відповідності

вимогам безпеки та надання інформації для майбутнього аналізу. Безпека системи - це безперервний процес. Необхідно регулярно оновлювати механізми безпеки, адаптувати політики і процедури до нових загроз і вимог, а також впроваджувати нові технології для посилення безпеки.

4 АНАЛІЗ РЕЗУЛЬТАТІВ ТЕСТУВАННЯ ZABBIX

Аналіз результатів тестування системи моніторингу Zabbix передбачає оцінку різних аспектів системи, таких як продуктивність, надійність, масштабованість і відповідність заданим вимогам. У цьому розділі детально описані ключові фактори, які слід враховувати при аналізі результатів тестування: Першим кроком є аналіз продуктивності системи. Сюди входить оцінка швидкості обробки даних, часу відгуку на запити користувачів та ефективності моніторингу в режимі реального часу. Важливо переконатися, що система може швидко обробляти великі обсяги даних без затримок або втрати інформації. Надійність системи оцінюється шляхом аналізу частоти і причин виникнення помилок, збоїв та інших проблем під час тестування. Оцінка стабільності передбачає перевірку здатності системи продовжувати роботу в умовах високих навантажень і мінливих умов мережі. Важливо проаналізувати точність зібраних даних моніторингу, включаючи точність виявлення подій і тривог. Також варто оцінити, наскільки система виявляє і класифікує різні типи подій, що відбуваються в мережі. Аналіз користувацького інтерфейсу передбачає оцінку його інтуїтивності, простоти навігації та наявності необхідних інструментів і функцій. Важливо, щоб користувачі могли легко знаходити потрібну інформацію та виконувати необхідні дії. Аналізується здатність системи адаптуватися до мінливих потреб і моделей використання. Сюди входить оцінка легкості додавання нових вузлів моніторингу, розширення мережевої інфраструктури та інтеграції з іншими системами і додатками. Важливо, щоб система моніторингу належним чином захищала інформацію, яку вона збирає. Важливо переконатися, що зібрана інформація належним чином захищена і відповідає чинним стандартам кібербезпеки. Це включає перевірку механізмів аутентифікації, авторизації, шифрування даних і захисту від зовнішніх атак. Аналіз також включає перевірку відповідності Zabbix стандартам і специфікаціям, визначеним у внутрішніх політиках і зовнішніх регуляторних вимогах. Збір та аналіз відгуків від кінцевих користувачів важливий для оцінки їхнього загального задоволення системою та визначення потенційних областей для вдосконалення. На

основі аналізу результатів тестування розробляються рекомендації щодо подальшого вдосконалення системи. Це можуть бути рекомендації щодо підвищення продуктивності, покращення користувацького інтерфейсу, посилення безпеки, оптимізації процесів моніторингу тощо.

4.1 Оцінка ефективності системи моніторингу

Оцінка ефективності системи моніторингу є ключовою для визначення, чи вона відповідає цілям та потребам організації. Ефективна система моніторингу повинна не лише точно відслідковувати події, але й своєчасно виявляти проблеми та ефективно управляти ресурсами. Проведення детального аналізу включає оцінку точності виявлення та відстеження подій, а також аналіз кількості помилкових спрацьовувань. Швидкість, з якою система реагує на проблеми, та ефективність сповіщень також є важливими факторами. Продуктивність та масштабованість системи, її здатність обробляти великі обсяги даних та інтегруватися з новими технологіями, є важливими для її стабільності та адаптації до зростаючих потреб. Надійність системи в різних сценаріях та її здатність підтримувати безперервну роботу без збоїв є ключовими для безперебійної роботи. Інтерфейс користувача повинен бути інтуїтивно зрозумілим і зручним, щоб користувачі могли легко інтерпретувати дані моніторингу. Гнучкість системи та її можливість адаптуватися до конкретних потреб і вимог організації, включаючи налаштування параметрів моніторингу та сповіщень, є важливими для її ефективності. Оцінка того, наскільки система ефективно використовує ресурси, як обчислювальні потужності та мережеві ресурси, є важливою для оптимізації її роботи. Система моніторингу має відповідати зовнішнім нормативним стандартам та внутрішнім політикам організації, включаючи конфіденційність та безпеку даних. Збір та аналіз відгуків

користувачів є важливим для виявлення потенційних областей для покращення та планування оновлень. Належно проведений аналіз дозволяє не лише оцінити поточний стан системи, але й визначити шляхи для її оптимізації та покращення, забезпечуючи її високу ефективність та задоволення потреб організації.

4.2 Переваги використання системи Zabbix

Як інструмент моніторингу, Zabbix пропонує багато переваг, які роблять його популярним вибором для організацій всіх розмірів і секторів. Основні переваги використання Zabbix. Відкрите програмне забезпечення Zabbix - це програмне забезпечення з відкритим вихідним кодом, що означає, що користувачі можуть вільно змінювати та розширювати його функціональність без додаткових витрат на ліцензії. Це також дозволяє гнучко налаштовувати систему відповідно до конкретних потреб організації. Масштабованість Zabbix ефективно масштабується від невеликих мереж до великих розподілених інфраструктур, дозволяючи здійснювати моніторинг тисяч серверів, віртуальних машин і мережевих пристроїв. Універсальність моніторингу На додаток до моніторингу широкого спектру параметрів, таких як процесор, пам'ять, дисковий простір і метрики мережевої активності, Zabbix також підтримує складні перевірки, такі як стан бази даних і веб-додатків. Гнучка система сповіщень Zabbix дозволяє створювати складні правила сповіщень, які можуть включати електронну пошту, SMS, мобільні додатки та зміни в системах продажу квитків. Це забезпечує своєчасне реагування на критичні інциденти. Вбудована підтримка візуалізації Zabbix має вбудовані інструменти, такі як графіки, мережеві карти та інформаційні панелі для візуалізації даних моніторингу, що дозволяє користувачам легко аналізувати великі обсяги інформації. Можливості автоматизації: автоматизація реагування на різні події та ситуації моніторингу, такі як автоматичне відновлення сервісів і створення сценаріїв вирішення проблем, можуть значно підвищити ефективність

обслуговування інфраструктури. Високий ступінь кастомізації: Zabbix пропонує детальні можливості кастомізації, включаючи власні параметри моніторингу, шаблони, правила збору даних і сценарії, що дозволяє адаптувати систему до потреб користувача. Завдяки своїй популярності та відкритості, Zabbix має велику та активну спільноту, яка постійно розширюється та вдосконалює свій функціонал. Для комерційних користувачів також доступна комерційна підтримка. Багатомовна підтримка Zabbix підтримує багато мов, що робить його придатним для міжнародних команд та організацій у різних країнах. Безпека Безпека є важливим аспектом Zabbix, включаючи шифрування зв'язку між компонентами та контрольований доступ до відстежуваних даних. Ці переваги роблять Zabbix дуже привабливим рішенням для комплексного моніторингу IT-інфраструктури в середовищах від невеликих локальних мереж до великих розподілених систем.

4.3 Проблеми та виклики під час впровадження

Впровадження системи моніторингу Zabbix може супроводжуватися різноманітними проблемами та викликами, які вимагають стратегічного підходу. Серед типових проблем — технічна складність системи відеоспостереження, яка потребує глибоких знань для ефективної роботи та інтеграції з існуючою IT-інфраструктурою. Також важливою є масштабованість і продуктивність системи, особливо при зростанні обсягів моніторингу. Правильна конфігурація та налаштування критично важливі для виявлення та сповіщення про події, а навчання персоналу і підтримка користувачів є ключовими для ефективного використання системи. Безпека та конфіденційність даних мають бути забезпечені для запобігання несанкціонованому доступу. Зміни в мережевій інфраструктурі вимагають гнучкості системи моніторингу, в той час як витрати на апаратне

забезпечення, мережеву інфраструктуру та персонал є важливими факторами для планування бюджету. Управління змінами та прийняття нової системи користувачами також має велике значення для успішної інтеграції, як і наявність актуальної документації та підтримки. Ефективне вирішення цих питань і проблем є ключовим для успішного впровадження та роботи системи моніторингу Zabbix, і потребує ретельного планування та адаптації під конкретні умови.

4.4 Удосконалення та оптимізація системи

Вдосконалення та оптимізація системи моніторингу Zabbix є ключовими для підтримки високої продуктивності та ефективності інфраструктури. Оновлення Zabbix до останньої версії забезпечує нові функції, покращення безпеки та продуктивності. Оптимізація бази даних, включаючи індексування та кешування, підвищує продуктивність. Проксі-сервери розподіляють навантаження і забезпечують надійність, а регулярне видалення неактивних об'єктів підтримує порядок в системі. Інтервали збору даних слід оптимізувати для збалансування точності моніторингу і навантаження на систему, а агенти зі стисненням даних знижують мережевий трафік. Моніторинг мережевого навантаження допомагає виявити і вирішити проблеми використання мережі, а оптимізація зберігання даних зменшує надлишковість. Шаблони спрощують та уніфікують моніторинг, а автоматичне виявлення об'єктів зменшує зусилля для налаштування. Регулярний моніторинг стану агентів, ведення журналів та аудит забезпечують контроль та прозорість, а оптимізовані сповіщення попереджають про проблеми без зайвого шуму. Моніторинг серверних ресурсів допомагає виявити вузькі місця, а дашборди та розклади слід оптимізувати для ефективності. Планування масштабування та оновлення обладнання є ключовим для підтримки росту

системи, а регулярне обслуговування та підтримка забезпечують надійність. Ретельне документування змін допомагає в управлінні системою, а безпека має бути пріоритетом, з акцентом на шифруванні та контролі доступу. Регулярний аналіз продуктивності, адаптація до змін і готовність до покращень забезпечують, що система моніторингу Zabbix залишається ефективною, надійною та продуктивною.

ВИСНОВОК

У цій дипломній роботі було розглянуто важливість та необхідність систем моніторингу в сучасному світі телекомунікацій. Особливу увагу приділено впровадженню системи моніторингу Zabbix з використанням оптичних терміналів C-DATA. Важливим аспектом роботи була розробка спеціалізованого шаблону для моніторингу OLT C-DATA, що включає збір даних через SNMP. Це дозволяє ефективно відстежувати важливі показники роботи обладнання та виявляти проблеми на ранніх етапах. Метою створення шаблону було не лише покращення моніторингу в межах однієї організації, а й підвищення загальної ефективності та безпеки мережевої інфраструктури, пропонуючи безкоштовний та доступний ресурс для широкого кола користувачів Zabbix. Ця робота підкреслює значення систем моніторингу для сучасних мережевих середовищ та демонструє, як технологічні інновації можуть бути використані для оптимізації та підвищення ефективності моніторингу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Olups, R. "Zabbix Network Monitoring - Second Edition" // Packt Publishing, 2016, pp. 100-150.
2. Shepard, S.I. "Network Monitoring and Management: A Guide for the Network Administrator" // McGraw-Hill Education, 2017, pp. 50-90.
3. Ramaswami, R., Sivarajan, K., Sasaki, G. "Optical Networks: A Practical Perspective" // Morgan Kaufmann, 2010, pp. 120-160.
4. Beaver, K. "Hacking For Dummies" // Wiley, 2019, pp. 75-115.
5. Chappell, L., Combs, G. "Wireshark 101: Essential Skills for Network Analysis" // Wireshark University, 2017, pp. 30-70.
6. Rekhter, Y., Davie, B. "MPLS: Technology and Applications" // Morgan Kaufmann, 2000, pp. 85-120.
7. Held, G. "Understanding Data Communications: From Fundamentals to Networking" // Wiley, 2000, pp. 150-180.
8. Bedell, P. "Computer Networks and Systems: Theory and Practice" // McGraw-Hill Education, 2001, pp. 60-100.
9. Comer, D.E. "Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture" // Prentice Hall, 2013, pp. 130-170.
10. Forouzan, B.A. "Data Communications and Networking" // McGraw-Hill Education, 2012, pp. 200-230.
11. Limoncelli, T.A., Hogan, C.J., Chalup, S.R. "The Practice of System and Network Administration: Volume 1" // Addison-Wesley Professional, 2016, pp. 115-145.
12. Burgess, M. "Principles of Network and System Administration" // Wiley, 2004, pp. 90-130.
13. Tanenbaum, A.S., Wetherall, D.J. "Computer Networks" // Pearson, 2010, pp. 50-80.
14. Hill, B. "Networking: A Beginner's Guide" // McGraw-Hill Education, 2009, pp. 20-50.

15. Lammle, T. "CCNA Routing and Switching Complete Study Guide" // Sybex, 2016, pp. 300-330.
16. O'Reilly Media. "SNMP Essentials" // O'Reilly Media, 2015, pp. 75-105.
17. C-DATA's Official Documentation and User Manuals // C-DATA, 2020, pp. 10-40.
18. IEEE Explore. "Latest papers on network security and efficiency" // IEEE, 2020, pp. Varies.
19. ACM Digital Library. "Articles on Zabbix and network monitoring" // ACM, 2019, pp. Varies.
20. ResearchGate. "Publications on optical networking" // ResearchGate, 2021, pp. Varies.
21. Mauthe, A., Hutchison, D. "Building Reliable Network Services: Theory and Practice" // Wiley, 2011, pp. 100-120.
22. Norris, M., Pretty, S. "Guide to Computer Network Security" // Springer, 2015, pp. 140-160.
23. Stewart, J. "Network Management: Principles and Practice" // Addison-Wesley, 2014, pp. 110-135.
24. Hallberg, J. "Networking: A Comprehensive Guide" // Delmar Cengage Learning, 2013, pp. 95-115.
25. Sterbenz, J.P.G., Krishnaswamy, D. "Resilient Optical Network Design: Advances in Fault-Tolerant Methodologies" // IGI Global, 2011, pp. 200-220.
26. Stallings, W. "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2" // Addison Wesley, 1999, pp. 45-65.
27. Black, U.D. "Network Management Standards: SNMP, CMIP, TMN, MIBs, and Object Libraries" // McGraw-Hill, 1995, pp. 130-150.
28. Morris, R. "Web-Based Network Management: Beyond the Browser" // Prentice Hall, 2000, pp. 70-90.
29. Lewis, L. "Network Science: Theory and Applications" // Wiley, 2009, pp. 160-185.
30. Subramanian, M. "Network Management: Principles and Practice" // Addison-Wesley, 2013, pp. 85-110.
31. Zabbix Official Documentation and Resources - www.zabbix.com/documentation

32. Network Management Resource - Spiceworks - www.spiceworks.com/network-management