ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОВЕДЕННЯ МОНІТОРИНГУ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ ZABBIX»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Аяйі Ф.О.
(прізвище та ініціали)

Керівник Гайдур Г.І.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Аяйі Френсісу Одіжі
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи:
«Дослідження шляхів та розробка рекомендацій щодо проведення моніторингу інфраструктури організації на базі рішення Zabbix»
керівник бакалаврської роботи Гайдур Галина Іванівна, д.т.н., проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від « 24 » лютого 2023 року № __.

2. Строк подання студентом бакалаврської роботи _____р.

3. Вихідні дані до бакалаврської роботи
1. Програмні діагностичні утиліти;
2. Експериментальне програмне забезпечення
3. Кінцеві точки користувачів;
4. Наукова та технічна література, експлуатаційна документація

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми моніторингу інфраструктури організації.
2. Актуальність проблеми моніторингу інфраструктури організації
3. Методи та засоби моніторингу інфраструктури організації.
4. Рекомендації щодо застосування методів та засобів моніторигу мереж та сервісів.

5. Перелік графічного матеріалу

1. Тема, мета, актуальність та предмет бакалаврської роботи.
2. Аналіз програмного забезпечення для здійснення моніторингу.
3. Роль програмного забезпечення для моніторингу в інфраструктурі організації.
4. Рекомендації щодо застосування методів та засобів моніторингу інфраструктури організації.
5. Висновки за результатами роботи.

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Визначення актуальності проблеми моніторингу інфраструктури.	24.02.2023 р.	
2.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	22.03.2023 р.	
3.	Аналіз методів та засобів збору даних в мережі.	27.03.2023 р.	
4.	Розроблення рекомендацій щодо застосування методів та засобів моніторингу інфраструктури організації	17.04.2023 р.	
5.	Оформлення результатів дослідження.	11.05.2023 р.	
6.	Підготовка доповіді до захисту.	28.05.2023 р.	

Студент Аяйі Ф.О.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи Гайдур Г.І.
(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина бакалаврської роботи: 70 сторінок, 27 рисунки 14 джерел за посиланням.

Об'єкт дослідження — процес моніторингу інфраструктури організації.

Предмет дослідження – методи та засоби моніторингу інфраструктури організації на базі програмного забезпечення Zabbix.

Мета роботи – розробити рекомендації щодо моніторингу інфраструктури організації на базі програмного забезпечення Zabbix.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів, розробка рекомендацій та проведення експериментів.

В роботі проведено аналіз роботи SNMP:v1, v2 і v3, досліджено найпоширеніші системи моніторингу IT ресурсів: Zabbix, Dude, Nagios, а також практичну реалізацію протоколу SNMP, що дозволило значно підвищити ефективність і досвід взаємодії з системами моніторингу мережі.

СИСТЕМА МОНІТОРИНГУ, ZABBIX, MIB, ICMP, SNMP, CDP, TTL, IP, POP3, HTTP, URL, UDP, FTP, IPX, NNTP, SQL, LDAP, VPN, IPX, SPX, VTP.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MIB - Management Information Base

ICMP - Internet Control Message Protocol

SNMP - Simple Network Management Protocol

CDP - Cisco Discovery Protocol

TTL - Time to live

IP - Internet Protocol

POP3 - Post Office Protocol

HTTP – HyperText Transfer Protocol

URL - Uniform Resource Locator

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

FTP - File Transfer Protocol

IoT - internet of things

IPX - Internetwork Packet Exchange

NNTP - Network News Transfer Protocol

SQL - Structured query language

VPN - Virtual private network

LDAP - Lightweight Directory Access Protocol

IPX - Internetwork Packet Exchange

SPX - Sequence Packet Exchange

VTP - VLAN Trunking Protocol

ВСТУП

Актуальність теми. Будь-які комп'ютерні мережі, включаючи маленькі, вимагають цілодобового нагляду. Якою б відмовостійкою вона не була б спроектована, наскільки б надійне і дороге обладнання та техніка не була встановлена - не варто покладатися на пильність лиш одного мережевого фахівця. Моніторинг мережі програмного забезпечення стає необхідною системою контроля та сповіщення про можливі неполадки.

Системи моніторингу дозволяють оперативно виявляти та реагувати на збої в роботі обладнання та програмного забезпечення. Це дозволяє швидко виявляти проблеми та усувати їх до того, як вони почнуть суттєво впливати на продуктивність роботи обладнання або призведуть до його повної відмови.

Крім того, моніторинг дозволяє оптимізувати використання ресурсів та підвищити безпеку організації. За допомогою моніторингу можна виявити вузькі місця в роботі мереж та оптимізувати процеси передачі даних, а також виявити загрози безпеці та вжити заходів щодо їх запобігання.

Таким чином, тема моніторингу мережі за допомогою Zabbix є актуальною та затребуваною у сучасному бізнесі та виробництві, оскільки допомагає знизити ризики виникнення неполадок та покращити продуктивність та безпеку мережі.

Метою дипломної роботи є аналізі технологій, що пропонуються компанією Zabbix, яка дозволить ефективно відстежувати роботу мережевого обладнання та програмного забезпечення, виявляти та усувати неполадки та підвищувати продуктивність та безпеку корпоративних ресурсів.

Об’єкт дослідження: підвищення ефективності сучасних методів моніторингу на базі програмного забезпечення Zabbix.

Предмет дослідження – методи та засоби моніторингу мереж та програмного забезпечення.

Наукова новизна одержаних результатів. Новими науково-обґрунтованими результатами, які отримані в роботі, є опрацювання новітніх технологій в галузі моніторингу.

Практичне значення одержаних результатів. Отримані результати та рекомендації, що ґрунтуються на аналізі даних моніторингу мережі за допомогою Zabbix, мають практичне значення для організацій, які використовують мережну інфраструктуру у своїй діяльності.

1 ЗАГАЛЬНИЙ АНАЛІЗ МОНІТОРИНГУ МЕРЕЖІ ТА ПРОТОКОЛІВ МОНІТОРИНГУ

1.1. Моніторинг в мережі

Моніторинг мережі — це процес постійного моніторингу комп'ютерної мережі на наявність таких проблем, як повільний трафік або збій компонентів. Інструменти моніторингу мережі постійно сканують мережу та призначені для автоматичного сповіщення мережевих адміністраторів за допомогою текстових повідомлень, електронної пошти або інших програм, таких як Slack, про виникнення проблеми.

Системи моніторингу продуктивності мережі (NPM) зазвичай генерують топологічні карти та корисну інформацію на основі зібраних і проаналізованих даних про продуктивність. Завдяки цьому відображенню мережі IT-команди отримують повну видимість мережевих компонентів, моніторингу продуктивності додатків і відповідної IT-інфраструктури, що дозволяє їм відстежувати загальний стан мережі, виявляти червоні прапорці та оптимізувати потік даних. Незалежно від того, чи є мережеві ресурси локальними, у центрі обробки даних, розміщені постачальником хмарних послуг або частиною гібридної екосистеми, система моніторингу мережі стежить за несправними мережевими пристроями та перевантаженими ресурсами.

Програмне забезпечення для моніторингу мережі відрізняється від систем мережевої безпеки чи систем виявлення вторгнень тим, що мережевий моніторинг зосереджений на проблемах внутрішньої мережі, таких як перевантажені маршрутизатори, збої сервера або проблеми з мережевим з'єднанням, які можуть вплинути на інші пристрої.

Рішення для моніторингу мережі також можуть ініціювати зміну налаштувань після відмови, щоб усунути проблемні пристрої або схеми з роботи, доки не буде виконано усунення проблеми. В ідеалі проактивне рішення для

моніторингу мережі запобігатиме простоям або збоям до їх виникнення, визначаючи аномалії, які можуть призвести до збою, якщо їх не перевірити.

Постійний моніторинг має вирішальне значення для підтримки цілісності мережі. Найкращі інструменти моніторингу мережі забезпечують візуалізацію або інформаційну панель, яка надає миттєвий огляд стану мережевих компонентів, що контролюються, із зазначенням будь-яких параметрів, що виходять за межі норми, що потребують подальшої перевірки, або таких компонентів, як комутатори, маршрутизатори, брандмауери, сервери та програмні служби. , програми або URL-адреси, які можуть бути джерелом збоїв у мережі. Для досягнення максимальної ефективності система моніторингу мережі повинна включати компоненти високої доступності, щоб апаратний або програмний збій систем, на яких працює інструмент керування мережею, міг бути автоматично виправлений шляхом переключення на іншу установку моніторингу мережі.

Моніторинг мережі повинен забезпечити:

– Повну візуалізацію IT та мережевої інфраструктури організації;

– Моніторинг, усунення несправностей і усунення проблем продуктивності мережі;

– Інструменти аналізу першопричини, коли виникають проблеми;

– Інформаційна панель із чіткими інструментами візуалізації та звітамиs;

Збої в мережі які можуть вплинути на загальну продуктивність IT і спричинити проблеми з доступністю в усій організації. Моніторинг мережі має кілька важливих переваг для організації, оскільки дозволяє раннє виявлення проблем, зокрема:

– Економія коштів завдяки скороченню часу простою та прискоренню усунення за рахунок допомоги в аналізі першопричини або відображення елементів мережі, які використовуються надмірно або недостатньо. Мережеві ресурси можуть зосередитися на продуктивних завданнях замість постійного пошуку проблем.

– Проблеми з продуктивністю можна виявити до того, як вони вплинуть на бізнес-операції або призведуть до погіршення взаємодії з клієнтами.

– Підвищення безпеки мережі можна реалізувати шляхом виявлення неочікуваного трафіку або невідомих пристроїв, які підключаються до мережі. Це можуть бути перші ознаки кібератак або спроб програм-вимагачів.

– Сплески використання, такі як штормові входи в систему або сезонні стрибки трафіку, можна визначити на ранній стадії, що дає змогу мережевим адміністраторам вживати заходів для виправлення ситуації, щоб гарантувати, що це не вплине на використання.

– Використання несанкціонованого додатка може бути виявлено. Кожен бізнес-підрозділ може мати групу додатків, які вони хочуть відстежувати, і моніторинг мережі може визначити, якими додатками користуються працівники та що роблять у мережі.

Організації часто здійснюють мережевий моніторинг у центрі мережевих операцій (NOC), який відстежує мережеві пристрої та з’єднання між усіма залежностями, не знаючи кінцевих користувачів, що NOC працює за лаштунками.

1.2. Аналіз протоколів моніторингу мережі

Протоколи для моніторингу мережі - це набори правил та стандартів, які використовуються для передачі інформації про стан мережевих пристроїв та служб між системами моніторингу та мережевими пристроями. Протоколи для моніторингу мережі дозволяють системам моніторингу отримувати інформацію про стан мережних пристроїв, як-от статуси пристроїв, завантаження мережі, використання ресурсів, продуктивність та інші параметри.

Існує велика кількість протоколів мережевого моніторингу, розроблених і розповсюджених різними постачальниками, деякі з яких об’єднують унікальні функції різних протоколів в одному. Загалом, основні функції всіх протоколів можна узагальнити в п’яти діях: виявлення, відображення, моніторинг, сповіщення та звіт.

1.2.1. Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) - це протокол прикладного рівня для моніторингу та керування мережевими пристроями в локальній мережі (LAN) або глобальній мережі (WAN), який використовує номер порту UDP 161/162. SNMP дозволяє керувати пристроями та отримувати інформацію про їх стан, таку як статуси пристроїв, завантаження мережі, використання ресурсів, продуктивність та інші параметри.

Є чотири основні компоненти мережі, керованої SNMP.

1. Агент SNMP

Програмне забезпечення агента працює на апаратному забезпеченні чи службі, що контролюється, збираючи дані про дисковий простір, використання пропускної здатності та інші важливі показники продуктивності мережі. Коли менеджер SNMP отримує запит, агент надсилає запитувану інформацію назад до системи керування. Агент також може заздалегідь повідомити NMS про помилку. Більшість пристроїв постачається з попередньо встановленим агентом SNMP, але зазвичай його потрібно ввімкнути та налаштувати.

2. Вузли мережі, керовані SNMP

Це мережеві пристрої та служби, на яких працюють агенти.

3. Менеджер SNMP

NMS — це програмна платформа, яка функціонує як централізована консоль, на яку агенти передають інформацію. NMS активно вимагатиме від агентів надсилати оновлення через регулярні проміжки часу. Те, що мережевий менеджер може зробити з цією інформацією, значною мірою залежить від того, наскільки багатофункціональна NMS.

Існує кілька безкоштовних менеджерів SNMP, але вони зазвичай обмежені своїми можливостями або кількістю вузлів, які вони можуть підтримувати. З іншого боку, платформи корпоративного рівня пропонують розширені функції для більш складних мереж, при цьому деякі продукти підтримують до десятків тисяч мережевих вузлів.

4. Інформаційна база управління

Ця база даних MIB є текстовим файлом (.mib), який перераховує та описує всі об’єкти на певному пристрої, які можна запитувати або керувати за допомогою SNMP. Кожному елементу MIB присвоюється ідентифікатор об’єкта (OID).SNMP настільки популярний, що більшість мережевих пристроїв уже постачаються з агентами SNMP. Однак, щоб використовувати протокол, мережеві адміністратори повинні спочатку змінити параметри конфігурації за замовчуванням своїх мережевих пристроїв, щоб агенти SNMP могли спілкуватися з системою керування мережею.

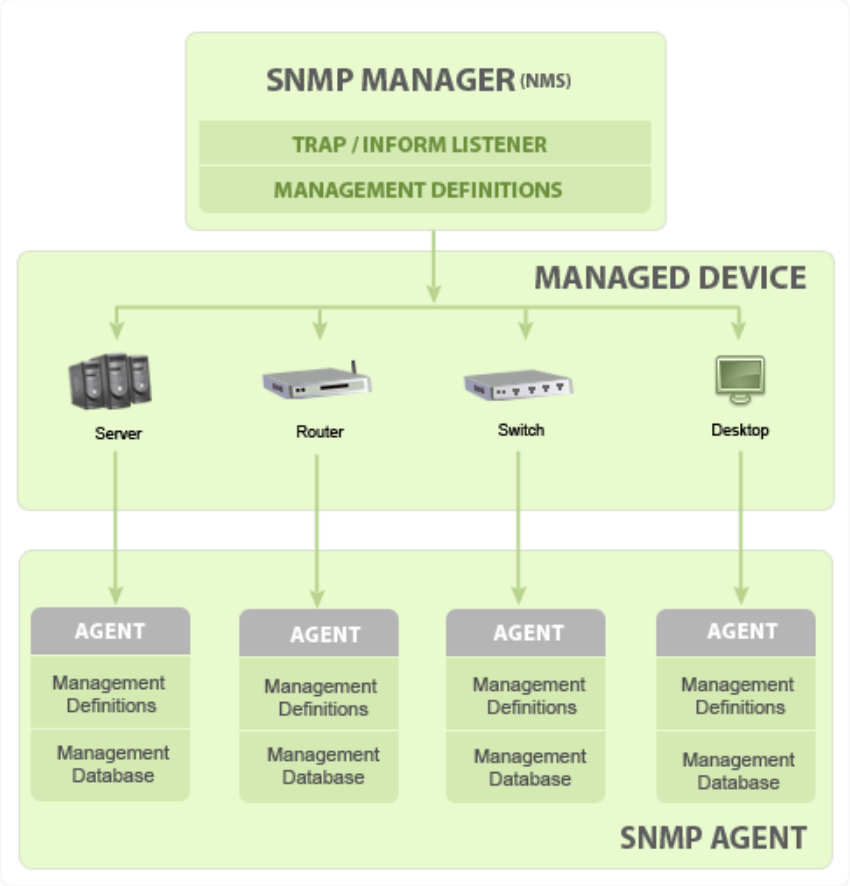


Рис.1.1. Базова схема зв’язку SNMP

SNMP є частиною оригінального набору протоколів Інтернету (IP), як визначено Інженерною групою Інтернету (IETF). Існує кілька версій протоколу SNMP.

Існує 3 версії SNMP:

– SNMPv1 – він використовує community strings для автентифікації та використовує лише UDP.

– SNMPv2c – він використовує community strings для автентифікації. Він використовує UDP, але його можна налаштувати на використання TCP.

– SNMPv3 – він використовує MAC на основі хешу з MD5 або SHA для автентифікації та DES-56 для конфіденційності. Ця версія використовує TCP.

Рівнень безпеки SNMP – визначається типом алгоритму захисту, що виконується для пакетів SNMP. Вони використовуються лише в SNMPv3. Існує 3 рівні безпеки, а саме:

– noAuthNoPriv – цей (без автентифікації, без конфіденційності) рівень безпеки використовує рядок спільноти для автентифікації та без шифрування для конфіденційності.

– authNopriv – цей рівень безпеки (автентифікація, без конфіденційності) використовує HMAC з Md5 для автентифікації та не використовує шифрування для конфіденційності.

– authPriv – цей рівень безпеки (автентифікація, конфіденційність) використовує HMAC з Md5 або SHA для автентифікації, а шифрування використовує алгоритм DES-56.

Таким чином, можна зробити висновок: чим вища версія SNMP, тим безпечнішою вона буде.

Повідомлення SNMP (Simple Network Management Protocol) - це формат, який використовується для передачі інформації між керуючою станцією та пристроєм, яким керується. Повідомлення SNMP представляють собою набір даних, які містять інформацію про запит або повідомлення, а також про відповідь на запит.

Повідомлення SNMP складаються із заголовка повідомлень і тіла повідомлень. Заголовок повідомлення містить інформацію про тип повідомлення, номер версії SNMP, номер повідомлення, ідентифікатор спільноти та інші параметри. Тело повідомлення містить сам запит або повідомлення.

Існує кілька типів повідомлень SNMP, які використовуються для різних цілей. Деякі з найбільш поширених типів повідомлень включають себе:

– GetRequest: використовується для запиту інформації про змінну або змінну.

– GetNextRequest: використовується для запиту інформації про наступну змінну в дереві змінних.

– SetRequest: використовується для зміни значення змінної.

– Відповідь: використовується для відповіді на запит GetRequest, GetNextRequest або SetRequest.

– Пастка: використовується для передачі повідомлення про помилку або події на керуючу станцію.

Повідомлення SNMP відіграють важливу роль в управлінні сетією, оскільки адміністратори мережі можуть отримувати інформацію про стан пристроїв і змінювати їх конфігурацію. Вони також використовуються для передачі відомостей про помилки або інших подій у мережі.

SNMP дозволяє моніторити стан мережевих пристроїв, виявляти проблеми з продуктивністю, контролювати завантаження мережі, керувати налаштуваннями пристроїв та вирішувати інші завдання керування мережею. Він є одним з найпопулярніших протоколів для моніторингу мережі та широко використовується в різних організаціях, підприємствах та провайдерах послуг.

1.2.2. Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) - це протокол мережного рівня, який використовується для обміну повідомленнями про помилки та контролю стану мережі в мережевих системах, що працюють на базі протоколу IP.

ICMP призначено передачі інформації про помилки, що виникають під час передачі даних між вузлами мережі. Це може бути, наприклад, повідомлення про

те, що пакет не може бути доставлений до призначення, що вузол недоступний або мережа перевантажена.

Зазвичай використовувані термінальні утиліти traceroute і ping обидві працюють за допомогою ICMP. Утиліта traceroute використовується для відображення шляху маршрутизації між двома Інтернет-пристроями. Шлях маршрутизації — це фактичний фізичний шлях підключених маршрутизаторів, який має пройти запит, перш ніж він досягне пункту призначення. Подорож між одним маршрутизатором та іншим відома як «стрибок», і traceroute також повідомляє час, необхідний для кожного переходу на шляху. Це може бути корисним для визначення джерел затримки мережі.

ICMP є невід'ємною частиною протоколу IP і використовується в багатьох мережних додатках та утилітах для діагностики та моніторингу стану мережі. Він дозволяє адміністраторам мереж швидко визначити проблеми з мережею та усувати їх, що підвищує доступність та надійність мережевих систем.

На відміну від Інтернет-протоколу (IP), ICMP не пов’язаний з протоколом транспортного рівня, таким як TCP або UDP. Це робить ICMP протоколом без з’єднання: одному пристрою не потрібно відкривати з’єднання з іншим пристроєм перед надсиланням повідомлення ICMP. Звичайний IP-трафік надсилається за допомогою TCP, що означає, що будь-які два пристрої, які обмінюються даними, спочатку виконають протокол TCP, щоб переконатися, що обидва пристрої готові приймати дані. ICMP не відкриває з’єднання таким чином. Протокол ICMP також не дозволяє націлюватися на певний порт пристрою. На жаль, мережеві атаки можуть використовувати цей процес, створюючи засоби зриву, такі як атака ICMP flood і атака ping of death.

Пакети ICMP передаються у формі дейтаграм, які містять IP-заголовок із даними ICMP. Дейтаграма ICMP схожа на пакет, який є незалежною сутністю даних. Формат пакета ICMP Заголовок ICMP стоїть після заголовка пакета IPv4 та IPv6.

У форматі пакета ICMP перші 32 біти пакета містять три поля:

	Bit 0-7	Bit 8-15	Bit 16-23	Bit 24-31
0	Тип	Код	Контрольна сума	
32	Інформація про заголовок			

Таблиця 1.1. Формат пакета ICMPv4

Тип (8-бітний): початкові 8-бітний пакет призначений для типу повідомлення, він надає короткий опис повідомлення, щоб мережа-одержувач могла знати, яке повідомлення вона отримує та як на нього відповісти. Ось деякі поширені типи повідомлень:

- Тип 0 – Exo відповідь
- Тип 3 – пункт призначення недоступний
- Тип 5 – повідомлення перенаправлення
- Тип 8 – exo-запит
- Тип 11 – Перевищення часу
- Тип 12 – проблема з параметрами

Код (8-бітний): код — це наступні 8 бітів формату пакета ICMP, це поле містить додаткову інформацію про повідомлення про помилку та тип.

Контрольна сума (16 біт): останні 16 біт призначені для поля контрольної суми в заголовку пакета ICMP. Контрольна сума використовується для перевірки кількості бітів у повному повідомленні та ввімкнення інструменту ICMP для забезпечення доставки повних даних.

Наступні 32 біти заголовка ICMP є розширеним заголовком, який вказує на проблему в IP-повідомленні. Розташування байтів визначається вказівником, який викликає повідомлення про проблему, і приймаючий пристрій шукає тут, щоб вказати на проблему.

Останньою частиною пакета ICMP є дані або корисне навантаження змінної довжини. Байти, включені в IPv4, становлять 576 байт, а в IPv6 – 1280 байт.

Типи повідомлень ICMP:

ICMP тип	ICMPv6 тип	Назва типу	Код	Опис
3	129	Ехо-Відповідь		Перевіряє наявність, відповівши на мережевий пінг
	1	Пункт Призначення Недоступний	0–15	Повідомлення ICMP, що інформує про недоступність певних компонентів (мережа, протокол, порт, хост) в поле "код" через проблеми з маршрутизацією або блокування брандмауером.
5	137	Перенаправити Повідомлення	0–3	Повідомлення про перенаправлення пакета для зазначеної мережі (0), зазначеної служби та мережі (2) або зазначеної служби та хоста (3).
8	128	Повторний запит		Мережевий пінг
9	134	Оголошення маршруту		Використовується маршрутизаторами для зв'язку з різними мережевими клієнтами.
11	3	Час Перевищено	0 або 1	Звіти про стан, які або повідомляють про тривалість життя (час життя, TTL) пакета (0), або про час очікування, поки не закінчиться збірка фрагментованих пакетів (1).
13	13	Позначка часу		Це забезпечує відповідний IP-пакет тимчасовою міткою, яка відповідає часу відправки і служить для синхронізації двох комп'ютерів.
14	-	Відповідь з відміткою часу		Відповідне повідомлення-тимчасова мітка ICMP, яку адресат відправляє після його отримання.
30	-	Трасування маршруту		Застарілий тип повідомлень ICMP, який використовується для відстеження шляху пакета даних в мережі.

Таблиця 1.2 – Типи повідомлень ICMP

1.2.3. Internet Control Message Protocol (ICMP)

NetFlow - це технологія, розроблена компанією Cisco Systems, яка використовується для збору, аналізу та відображення даних про трафік у мережі. NetFlow надає інформацію про те, як використовуються ресурси мережі, які

програми та протоколи використовують найбільше трафіку, хто і куди надсилає дані, а також допомагає виявити потенційні проблеми з продуктивністю мережі.

Кеш NetFlow — це база даних згорнутої інформації, де дані NetFlow зберігаються після перевірки пакетів.

Інтерфейс командного рядка (CLI) є одним із двох методів підключення NetFlow для доступу до даних NetFlow. Він забезпечує миттєве уявлення про ваш мережевий трафік і корисний для усунення несправностей.

Другим варіантом доступу до даних NetFlow є експорт даних до колектора NetFlow. Колектор NetFlow — це сервер звітів, який збирає й обробляє трафік і експортовані дані, щоб їх було легко аналізувати. Ці колектори NetFlow поділяються на дві категорії: апаратні колектори та програмні колектори, причому програмні рішення є більш поширеними, ніж апаратні пристрої.

NetFlow працює на рівні маршрутизаторів та комутаторів та дозволяє збирати інформацію про трафік, який проходить через ці пристрої. Дані про трафік збираються на основі інформації, яку надають пакети через маршрутизатор або комутатор. Ці дані можуть включати інформацію про джерело та призначення, протоколи, порти, обсяг трафіку та інші характеристики.

Зібрані дані NetFlow можуть бути використані для багатьох цілей, включаючи:

– Моніторинг використання пропускної спроможності: NetFlow дозволяє визначити, які програми або протоколи використовують найбільше пропускну здатність мережі, і допомагає виявити вузькі місця в мережі.

– Визначення джерел атак та загроз безпеки: NetFlow дозволяє виявляти підозрілий трафік у мережі, який може бути пов'язаний з атаками або іншими загрозами безпеці.

– Планування ємності мережі: дані NetFlow можуть бути використані для прогнозування майбутнього використання пропускної спроможності мережі та планування її ємності.

– Оптимізація налаштувань мережі: дані NetFlow можуть допомогти оптимізувати налаштування мережних пристроїв і покращити продуктивність мережі.

Недоліки NetFlow

Хоча NetFlow забезпечує покращену видимість мережевого трафіку, планування та аналіз безпеки, він має певні недоліки.

Враховуючи високі вимоги до доступної смуги пропускання, NetFlow має вплив на продуктивність пристроїв, на яких він реалізований. Щоб зменшити цей вплив на продуктивність, мережеві пристрої часто покладаються на вибірку пакетів (подібно до sFlow) для створення статистики NetFlow. На жаль, низькі частоти дискретизації — іноді лише один на 1000 пакетів — різко знижують видимість мережі та можуть перешкодити командам виявити критичні загрози безпеці або проблеми з продуктивністю.

Крім того, записи NetFlow можна пересилати лише певній кількості збирачів або інструментів моніторингу. Часто це число може бути набагато меншим, ніж потрібно для належного керування мережею та її усунення. Оскільки компанії стикаються зі зростаючим обсягом як даних, так і загроз безпеці, бачення лише частини того, що відбувається в мережі, ризикує мати недостатньо інформації для боротьби із загрозами безпеці.

NetFlow і Gigamon

Gigamon усуває ризики, пов’язані із вибіркою даних, запускаючи статистику NetFlow паралельно з необробленими потоками пакетів. Завдяки цим можливостям обробки користувачі Gigamon можуть генерувати статистику NetFlow або з набагато вищою частотою дискретизації, або навіть зі швидкістю рядка.

Генерація NetFlow зазвичай виконується маршрутизаторами та комутаторами як частиною робочої мережі. Однак, як згадувалося вище, NetFlow дійсно впливає на продуктивність пристроїв, на яких він реалізований. Не відставати від зростаючого обсягу даних і швидкості мережі стає все більшою проблемою для більшості підприємств, які намагаються мати достатньо обчислювальних ресурсів для задоволення зростаючого попиту.

1.2.4. Remote Monitoring (RMON)

Remote Monitoring (RMON) - це технологія, яка дозволяє віддалено моніторити та аналізувати трафік у мережі на рівні комутаторів та маршрутизаторів. RMON був розроблений для забезпечення ефективного моніторингу та управління мережею, дозволяючи адміністраторам мережі збирати та аналізувати дані про трафік у режимі реального часу.

RMON дозволяє збирати велику кількість інформації про мережевий трафік, включаючи кількість переданих пакетів, швидкість передачі даних, час затримки, помилки та багато іншого. Для збору даних RMON використовує власний протокол, який дозволяє збирати інформацію про трафік на різних рівнях OSI.

Одним із недоліків цієї системи є те, що віддалені пристрої несуть більший тягар керування та вимагають для цього набагато більше ресурсів. Деякі підприємства намагаються «зрівноважити терези», впровадивши підмножину RMON. Мінімальний агент RMON може підтримувати лише кілька функцій керування.

Ключовою перевагою RMON є порогові значення продуктивності та автоматичні сповіщення при перевищенні порогових значень. Це дозволяє підтримувати проактивну стратегію керування мережею.

Основними перевагами RMON є:

– Можливість збирати дані про трафік на рівні комутаторів та маршрутизаторів. Це дозволяє отримувати докладнішу інформацію про те, як використовується мережа.

– Здатність працювати у режимі реального часу, що дозволяє оперативно реагувати на зміни у мережі.

– Можливість аналізувати трафік на різних рівнях моделі OSI, що дозволяє отримувати докладнішу інформацію про характеристики трафіку.

– Можливість використовувати алерти та сповіщення для швидкого виявлення та усунення проблем у мережі.

– Можливість налаштування RMON для збору лише необхідної інформації, що дозволяє знизити навантаження на мережу та покращити її продуктивність.

RMON зазвичай реалізується лише на одному пристрої чи інтерфейсі на підмережу. Програмне забезпечення агента працює на порту маршрутизатора, який відстежує та збирає статистику мережі Ethernet для підключеної підмережі. Ці статистичні дані стосуються фізичного рівня та рівня каналу даних еталонної моделі взаємозв’язку відкритих систем для мереж. Консоль керування SNMP зв’язується з агентом RMON, коли їй потрібно зібрати статистику, щоб допомогти технікам проаналізувати тенденції мережевого трафіку.

1.2.5. Jitter

Jitter - це параметр, який характеризує мінливість затримки (delay variation) при передачі даних через мережу. Він вимірюється в мілісекундах і показує, наскільки розрізняються часові інтервали між надходженням пакетів на приймальній стороні.

Jitter впливає на якість голосового та відеозв'язку, а також на продуктивність програм, які використовують передачу даних у режимі реального часу. Якщо затримка при передачі даних змінюється сильно і не передбачувано, це може призвести до ефекту "розгублених кадрів" у відео, втрати якості звуку та інших проблем.

Для вимірювання Jitter використовується спеціальний тест, який відправляє серію пакетів даних через мережу та аналізує часові інтервали між їх надходженням на приймальну сторону. Результати тесту показують, як швидко змінюється затримка передачі даних і наскільки вона передбачувана.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ МОНІТОРИНГУ ЛОКАЛЬНИХ МЕРЕЖ

Система моніторингу включає в себе функціональну частину програмного забезпечення, що збирає інформацію з кількох джерел і проводить аналіз цих даних для відображення складних графіків і візуалізації даних. Ці дані можуть бути зібрані з будь-якого компонента мережі, використовуючи стандартні методи, такі як SNMP, або з використанням API через агентний підхід для контрольованих пристроїв. Агенти забезпечують збір інформації з пристроїв і взаємодію з системою моніторингу з використанням звичайного протоколу. Дані, що були зібрані, піддаються аналізу з використанням налаштованих правил. Система моніторингу перевіряє, чи перевищує значення порогу, і вживає відповідних заходів для реагування на події. Графіки, що побудовані на основі даних, показують їх інформативність та дозволяють відстежувати історію метрики.

2.1. Огляд різних рішень для мережевого моніторингу

Після дослідження ринку програмного забезпечення для систем моніторингу, стало зрозуміло, що існує велика кількість таких систем. Оскільки їх значення та корисність дуже важко переоцінити, особливо якщо системний адміністратор управляє складним серверним та мережевим обладнанням. Кожна з цих систем має свої переваги та недоліки, тому часто необхідно витрачати багато часу на ефективне настроювання та адаптацію під конкретне завдання. Більшість цих систем надають базовий набір функцій, таких як:

- моніторинг мережі;
- угруповання пристроїв;
- автоматичне виявлення;
- гнучке конфігурування;
- візуалізація даних та доступ через веб-інтерфейс;
- події та реакція на них у вигляді оповіщень та виконання команд;

– можливість розширення функціональності через плагіни;

– зберігання конфігурації та історії моніторингу в базі даних;

– створення карт мережі та керування доступом.

У даній роботі розглянуто найбільш поширені та рекомендовані на ринку системи моніторингу, не описуючи все їх розмаїття, але дозволяючи коротко описати особливості та специфіку роботи основних з них.

2.2. Nagios

Nagios — це безкоштовне програмне забезпечення з відкритим кодом для комп'ютерних систем. Використовується для моніторингу систем, мереж та інфраструктури. Це програмне забезпечення в основному надає послуги моніторингу та попередження для комутаторів, програм і серверів у культурі DevOps. Він дозволяє моніторити сервери, додатки, комутатори та інші мережеві сервіси та надсилати попередження користувачам про виявлені проблеми.

Nagios розроблено для операційних систем Linux та UNIX і має три основні компоненти: веб-інтерфейс, демон та плагіни. Він дозволяє відстежувати різні типи мережевих служб, таких як SMTP, HTTP, POP 2, SNMP, NNTP, SSH та FTP, а також ресурси хоста, такі як завантаження процесора, системний журнал та використання диска. Nagios підтримує різні типи операційних систем, включаючи Windows та Linux, та може використовуватися для віддаленого моніторингу за допомогою зашифрованих тунелів SSL та SSH. Надійний веб-інтерфейс дозволяє переглядати повідомлення, стан мережі, файлів журналів та історії проблем.

Інструмент моніторингу Nagios володіє багатьма функціями. Деякі з них згадуються нижче:

– цим інструментом легко керувати, щоб знаходити проблеми, що існують в мережі, забезпечувати безпеку і масштабованість мережі;

– інструмент також допомагає керувати журналами та системами баз даних;

– інструмент моніторингу Nagios надає інформативний веб-інтерфейс і простий у використанні користувацький інтерфейс, що надає змогу легко контролювати мережу;

– коли виникають будь-які неполадки з мережею, інструмент надсилає негайні попередження. Коли який-небудь сервер виходить з ладу, користувачеві відправляється повідомлення для інформування про проблеми, щоб можна було зробити негайні дії щодо проблем;

– вузькі місця в продуктивності можна виявити за допомогою інструменту моніторингу Nagios;

– інструмент здатний автоматично усувати проблеми, оскільки інструмент пропонує опції безперервного моніторингу;

– інструмент пропонує кілька типів моніторингу мережевих служб, таких як SMTP, HTTP, FTP, POP, SNMP, SSH і багато інших мережеві служби;

– інструмент забезпечує гнучкість для одночасного багатокористувацького доступу, що надає змогу здійснювати моніторинг мережевих компонентів;

– однією з найсильніших функцій є можливість переходу на інший ресурс і безперервний моніторинг, що дозволяє виявляти вузькі місця продуктивності в мережі;

Інструмент моніторингу Nagios — це клієнт-серверна архітектура, де сервер Nagios працює на хості, а плагіни інструменту запускаються на віддаленому хості, щоб контролювати його на наявність будь-яких проблем або загроз. Інструмент моніторингу Nagios надає різні плагіни для забезпечення доступності інтелектуальних даних для мережі, яка може розміщуватися в ядрі Nagios. Для виконання цих плагінів використовується ядро Nagios. Інструмент моніторингу Nagios підключається до бази даних для відстеження файлу журналу. Інструмент також пропонує інтерактивний веб-інтерфейс, який дозволяє створювати веб-сторінки. Він сповіщає користувача про будь-які проблеми в мережі та надсилає сповіщення адміністратору мережі, коли виникає попередження.

Так само як і в системах-конкурентах основною логічною одиницею є вузли в мережі (тобто хости), які відображаються у веб-інтерфейсі так, як показано на

рисунку 2.2. Веб-сервіс Nagios досить інформативний, є можливість подивитися список хостів, сервісів, журнал виниклих проблем і повідомлень про них.

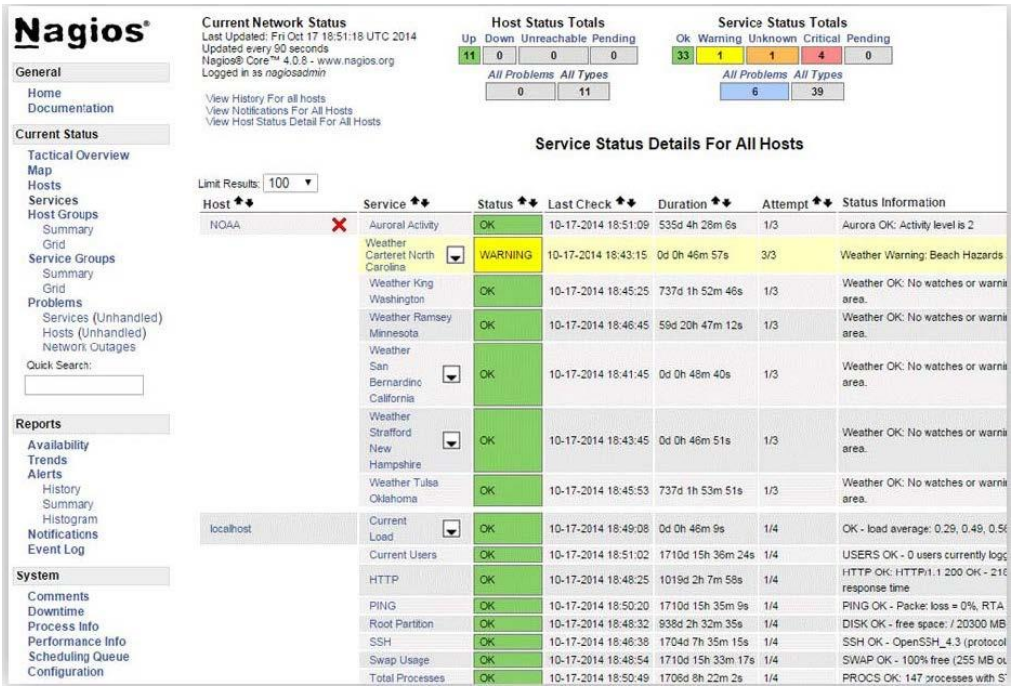


Рис.2.2. Веб інтерфейс Nagios

Можливість додавати власні методи моніторингу та обробники подій завдяки простоті структури плагінів, а також принципу "батьківських" вузлів, який дозволяє знаходити залежності між хостами, дозволяє системі Nagios відрізняти вузли в аварійній ситуації від недоступних системі моніторингу. Завдяки великому спектру візуального відображення зібраних даних, таких як візуальні карти мережі, комплексні звіти, різні графіки спостережуваних параметрів, численні діаграми і багато іншого, система Nagios конкурує з іншими системами моніторингу.

Хоча установка та налаштування системи Nagios не є складним завданням, налаштування має дуже багато параметрів. Всі налаштування проходять шляхом редагування файлів конфігурації і вказівки даних про хости і їх групи. Особливості Nagios полягають у тому, що налаштування зберігаються в файлах конфігурації, моніторинг характеристик проводиться з використанням плагінів, які можна гнучко налаштувати під потрібне завдання, і ці ж плагіни знаходяться в основі архітектури системи.

Серед переваг Nagios можна виділити простий формат файлу, що дозволяє легко конфігурувати систему, використовуючи будь-які створені утиліти, стабільність роботи та простоту управління системою. Також є можливість створення своїх обробників подій, які будуть виконуватися в разі появи подій, ініційованих перевірками сервісів або серверів. Відкритий вихідний код Nagios в поєднанні з модульним характером й розширені можливості налаштування роблять його потужним інструментом для моніторингу мережі та серверів. Нагіос може бути налаштований для моніторингу різних метрик, таких як доступність веб-сайту, використання ресурсів сервера, стан служб та процесів, що запущені на сервері, і багато іншого.

Крім того, Nagios дозволяє створювати свої власні скрипти моніторингу та плагіни, які можна використовувати для моніторингу метрик, що не входять до стандартного набору. Інші корисні функції Nagios включають інтеграцію з різними системами сповіщення (наприклад, електронною поштою, SMS-повідомленнями, Slack тощо), можливість налаштовувати залежності між моніторингом, що дозволяє пріоритезувати проблеми та автоматично відключати моніторинг для взаємозалежних систем.

Загалом, Nagios є дуже потужним інструментом для моніторингу мережі та серверів, який може бути легко налаштований та розширений за допомогою різних плагінів і налаштувань. Він дозволяє забезпечити високу доступність та продуктивність мережі та серверів, а також зменшити час, потрібний для виявлення та вирішення проблем.

Проте, Nagios має й деякі недоліки. Наприклад, відсутність можливості конфігурації через графічний інтерфейс та складність налаштування для користувачів з недостатнім рівнем програмування. При великій кількості хостів та перевірок, стандартних вбудованих плагінів може бракувати.

2.2. The Dude

Серед існуючих систем моніторингу Dude позиціонується як найкращий за співвідношенням ціна/якість продукт. Це слушно, через те що він розповсюджується безкоштовно. Однак, незважаючи на безкоштовність, він не поступається, а часто перевершує комерційні продукти. Розглянувши багато прикладів успішного використання цього програмного продукту, починаючи від комерційних банків та інтернет-провайдерів до державних структур.

Функціонал Dude дозволяє моніторити окремі сервери, а також мережі та мережеві послуги будь-якого ступеня складності. У більшості випадків, можливості даного програмного забезпечення не використовуються максимально. Це пов'язано насамперед із відсутністю якісної документації. Навіть досвідченому системному або мережному адміністратору необхідно кілька тижнів на те, щоб коректно налаштувати моніторинг системи, якщо він починає це робити з нуля.

Після першого запуску dude network monitor, програмне забезпечення автоматично виявляє всі існуючі підмережі і починає їх сканування. Потім виявлені пристрої перевіряються, щоб визначити, які з більш ніж десятка служб на основі IP вони підтримують (наприклад, NetBIOS, HTTP, FTP та інші), Але є можливість додати свої власні тести для будь-яких служб, які ще не налаштовані заздалегідь.

Після завершення процесу виявлення пристроїв, результати будуть відображені на мережевій карті у вигляді значків. Наведення курсору миші на значок пристрою викличе спливаюче діалогове вікно, яке містить багато корисної інформації, включаючи інформацію про стан служб пристрою та графік, який показує мережеву активність за останню годину.

Мережеві карти Dude дуже прості у налаштуванні, тому легко можна змінювати їх розташування та орієнтацію пристроїв. Якщо у вас є миша з колесиком, ви можете використовувати його для збільшення або зменшення масштабу карти. Для багатокомпонентних мереж сусідній вид з висоти пташиного польоту дозволяє швидко переміщуватися по великих картах та переходити до певного розділу.

Клацання правою кнопкою миші на пристрої на карті викликає меню інструментів, яке дозволяє встановити зв'язок з пристроєм декількома способами, включаючи ping, FTP або telnet. Для пристроїв, що працюють під управлінням RouterOS (фірмова мережева операційна система MikroTik), ви також можете виконувати дії, такі як перевірка пропускної здатності або моніторинг трафіку в режимі реального часу.

Коли пристрій, який відстежується, переходить в автономний режим, значок його мережевої карти стає червоним, і Dude може повідомити про це, але за замовчуванням він не робить цього, окрім публікації записів в журналі подій. Для повідомлення про перехід в автономний режим підтримуються інші способи, такі як відправка електронної пошти, відтворення звуків або відображення спливаючих попереджень (але немає підтримки SMS). Крім того, опція повідомлення має бути включена та налаштована індивідуально для кожного пристрою.

Dude Network Monitor надає можливість налаштування безлічі параметрів конфігурації, але користувальницький інтерфейс додатка не є особливо зрозумілим та привабливим. Інтерфейс складається з двох панелей, який дозволяє вибрати елемент конфігурації зі списку ліворуч і переглянути його праворуч, що зображено на рисунку 2.3. Деякі користувачі можуть знайти інтерфейс додатка заплутаним.

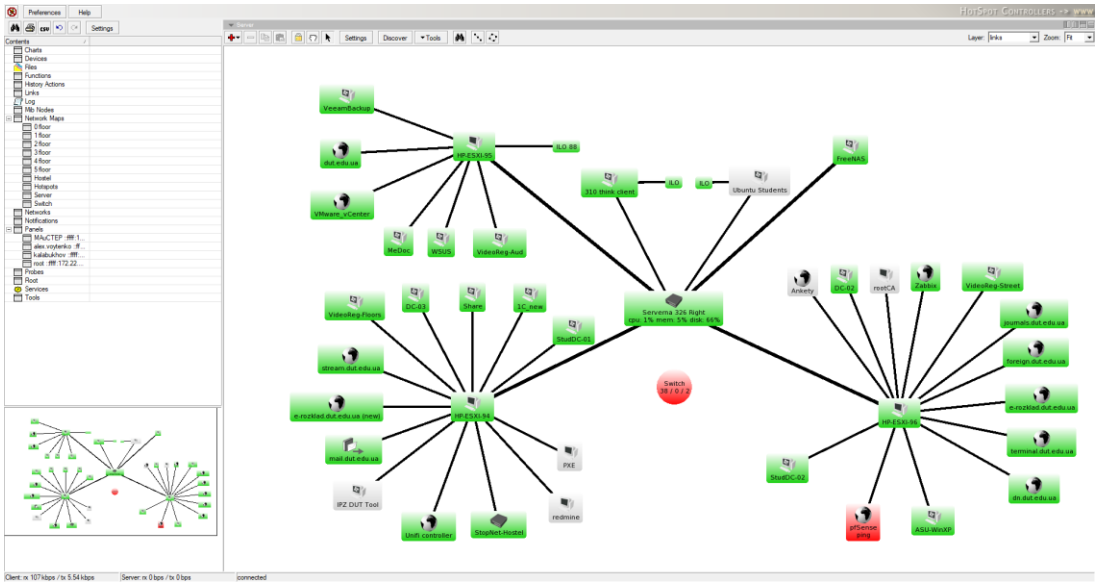


Рис.2.3. Ітерфейс The Dude

Також плюсом є той факт, що макет вікна Dude зберігається на сервері, а не на клієнті, тому, як тільки ви налаштуєте все так, як вам подобається, Ви зможете переглядати його однаково з декількох клієнтів.

Деякі з його особливостей:

– автоматичне виявлення та компонування мережі;

– виявляє будь-який тип або марку пристрою;

– моніторинг пристроїв, посилань і повідомлень;

– включає значки SVG для пристроїв і підтримує користувальницькі значки та фони;

– простота установки і використання;

– дозволяє малювати власні карти та додавати власні пристрої;

– підтримує моніторинг SNMP, ICMP, DNS і TCP для пристроїв, які його підтримують;

– моніторинг та графіки використання окремих посилань;

– прямий доступ до інструментів дистанційного керування для керування пристроями;

– підтримує віддалений веб-сервер і локальний клієнт;

– працює в середовищі Linux Wine, Mac OS і Windows.

2.2. Zabbix

Zabbix — це програмне забезпечення з відкритим кодом для моніторингу різноманітних IT-компонентів, включаючи мережі, сервери, віртуальні машини (ВМ) і хмарні служби. Zabbix надає метрики моніторингу, такі як використання мережі, завантаження процесора та використання дискового простору. Програмне забезпечення відстежує роботу в Linux, Hewlett Packard Unix (HP-UX), Mac OS X, Solaris та інших операційних системах (ОС); однак моніторинг Windows можливий лише через агентів.

Zabbix можна розгорнути для моніторингу на основі та без агентів. На IT-компоненти встановлюються агенти для перевірки продуктивності та збору даних.

Потім агент звітує на централізований сервер керування Zabbix. Ця інформація включається у звіти або представлена візуально в графічному інтерфейсі користувача (GUI) Zabbix. Якщо виникнуть проблеми щодо того, що відстежується, Zabbix надішле сповіщення або сповіщення користувачеві. Моніторинг без агентів виконує той самий тип моніторингу за допомогою наявних ресурсів у системі чи пристрої для емуляції агента.

Веб-інтерфейс Zabbix дозволяє користувачам переглядати своє IT-середовище за допомогою настроюваних інформаційних панелей на основі віджетів, графіків, мережевих карт, слайд-шоу та звітів. Наприклад, користувач може налаштувати звіт, щоб відображати показники, пов’язані як з угодами про рівень обслуговування (SLA), так і з ключовими показниками продуктивності (KPI) щодо навантаження на ЦП.

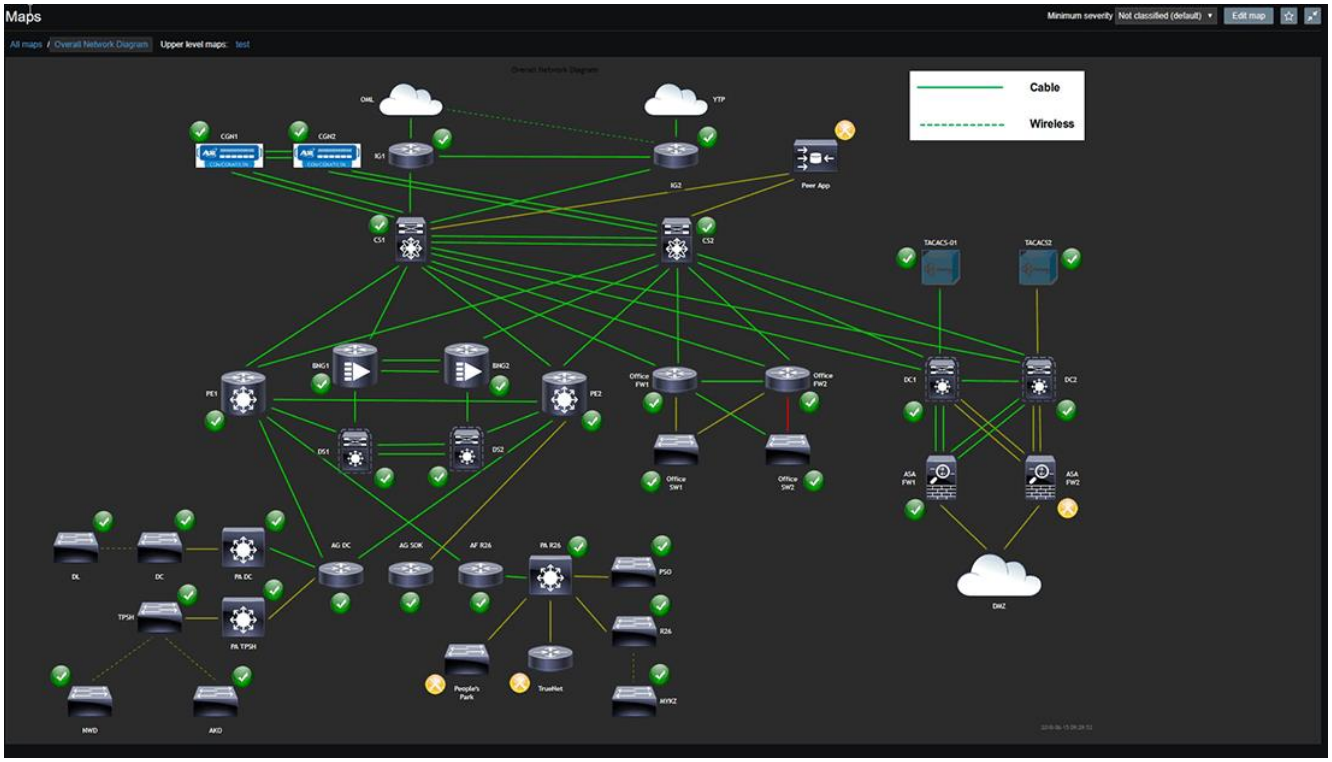


Рис.2.4. Приклад карти мережі в Zabbix

Zabbix працює через три варіанти режиму виявлення:

– Функція виявлення мережі періодично сканує IT-середовище та записує тип пристрою, IP-адресу, стан, час роботи та простою.

– Низькорівневе виявлення автоматично створює елементи, тригери та графіки на основі виявленого пристрою. Низькорівневе виявлення може створювати метрики з ідентифікаторів об’єктів простого протоколу керування мережею (SNMP), служб Windows, запитів на мові структурованих запитів (SQL) Open Database Connectivity (ODBC), мережевих інтерфейсів тощо.

– Автоматичне виявлення автоматично починає моніторинг будь-якого виявленого пристрою за допомогою агента Zabbix.

За допомогою розподіленого моніторингу Zabbix віддалено запущені сценарії збирають дані з кількох пристроїв у розподілених місцях і об’єднують ці дані на одній інформаційній панелі чи звіті, наприклад доступність серверів по всій країні.

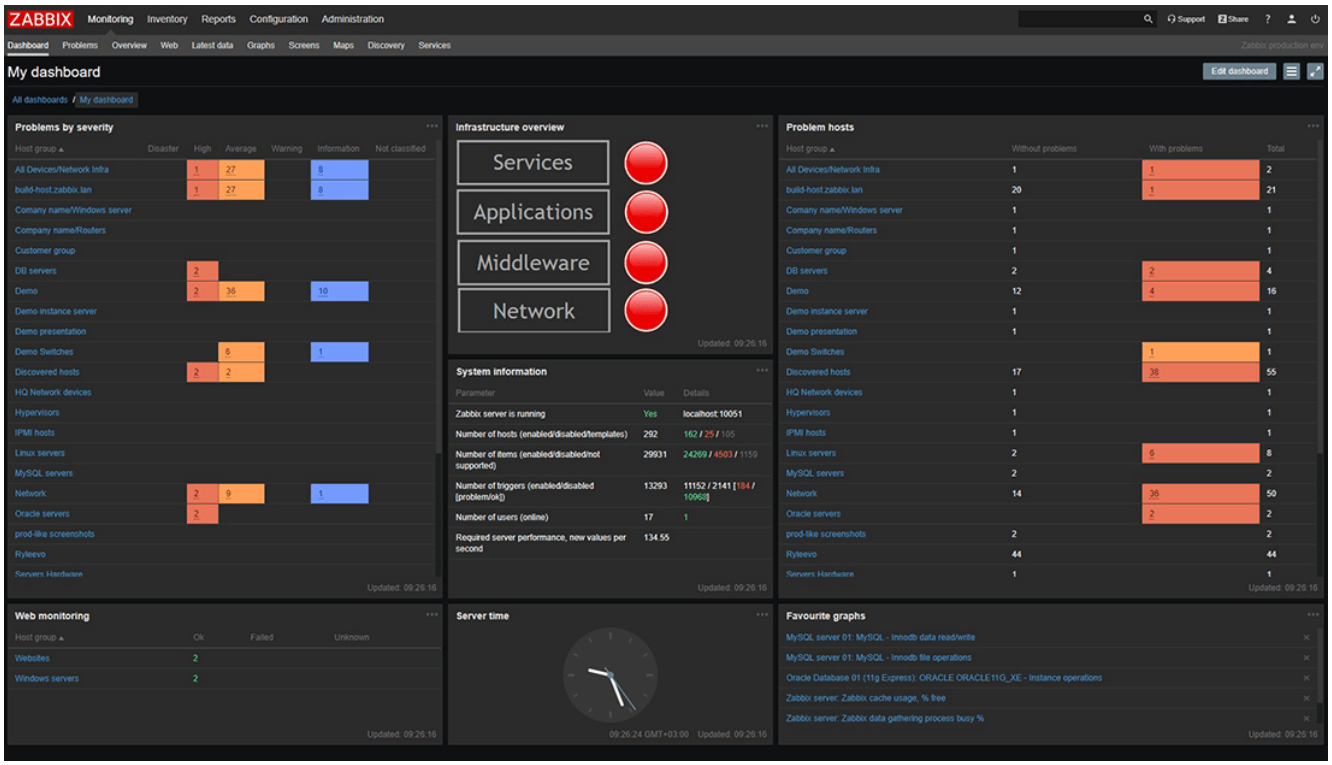


Рис.2.5. Інформаційна панель zabbix

Інструментарій програмного забезпечення пропонує дуже велику кількість функцій:

– Збір даних

У цій функції інструмент Zabbix перевіряє наявність вузьких місць у продуктивності програми та доступність програми. Інструмент також підтримує

спеціальну перевірку. Інструмент пропонує кілька служб моніторингу, таких як JMX, IPMI та SNMP.

– Система оповіщення

Користувач може бути повідомлений про проблему, яка виникла на мережевих серверах. Сповіщення також можна налаштувати. Користувач також може налаштувати дії так, щоб їх можна було автоматизувати, коли в системі виникла будь-яка проблема. Макрозмінні можна використовувати в сповіщеннях для інформування користувача за допомогою каналів зв’язку, таких як електронна пошта, SMS тощо.

– Побудова графіків у реальному часі

Інструмент Zabbix надає функцію моніторингу мережевих серверів і програми в режимі реального часу на предмет проблем з продуктивністю. Усі елементи можна негайно побудувати на графіку, оскільки інструмент має вбудовану функцію для створення графіків у режимі реального часу та відображення їх в інтерфейсі інструменту. Інструмент також надає функції для вимірювання часу відгуку веб-сайту та перевірки функціональності веб-сайту.

– Різні параметри візуалізації

Інструмент надає функцію для створення власних графіків, щоб легко поєднувати кілька елементів в одному перегляді. Звіти генеруються інструментом Zabbix, щоб можна було виконати аналіз проблем. Усі ресурси можна легко контролювати за допомогою інструменту моніторингу.

– Зберігання даних

Дані зберігаються в базі даних, яка підключена до інструменту. Інструмент також підтримує настроювану історію. Інструмент Zabbix підтримує різні типи баз даних, що допомагає легко керувати даними.

– Проста конфігурація та шаблони

Інструмент Zabbix широко використовується для цілей моніторингу окремими особами та організаціями, оскільки інструмент допомагає додати контрольований пристрій, відомий як хости. Після додавання хоста можна виконувати моніторинг активності хоста, а також можна застосовувати шаблони

для контрольованих пристроїв. Інструмент також пропонує функцію групової перевірки за допомогою шаблонів. Один шаблон може успадкувати властивість іншого шаблону, що забезпечує додаткову гнучкість для користувача. Zabbix proxy використовується для віддаленого моніторингу, і інструмент підходить для складних середовищ.

– Зручний веб-інтерфейс

Інструмент Zabbix пропонує веб-інтерфейс, розроблений мовою PHP. Веб-інтерфейс можна легко отримати з будь-якого місця. Журнали, створені веб-інтерфейсом, можна легко перевірити. Інструмент також має систему дозволів, у якій користувач може бути автентифікований, і лише дійсним користувачам дозволено використовувати інструмент. Доступність функцій може бути обмежена для окремих користувачів відповідно до їхнього пакету.

Варіанти безагентного моніторингу за допомогою Zabbix

Zabbix пропонує кілька варіантів моніторингу, крім агентів. Проста перевірка може підтвердити доступність і швидкість реагування стандартної служби, наприклад сповіщень або HTTP.

Розширення керування Java (JMX), веб-моніторинг та інші методи також є альтернативою використанню агентів. У Zabbix JMX можна використовувати для моніторингу додатків на основі Java. Веб-моніторинг використовується для перевірки доступності веб-сайтів і підтримує HTTP і HTTPS. Zabbix збирає дані про середню швидкість завантаження сценарію, помилки та повідомлення про помилки, час відповіді тощо.

Zabbix API

Інтерфейс програмування додатків Zabbix — це веб-інтерфейс API для створення нових програм, автоматизації завдань та інтеграції зі стороннім програмним забезпеченням, таким як go-zabbix, Zabbix::Tiny або Zabbix sender.

Формат JavaScript Object Notation (JSON) використовується для створення API як зовнішнього веб-інтерфейсу.

Zabbix API складається з багатьох методів, які згруповані в окремі API, кожен з яких виконує певну послугу. Наприклад, метод для створення нового хосту — host.create; метод входу як адміністратор — user.login.

Використовуючи API, користувачі можуть створювати програми для роботи та відображення інформації Zabbix.

Шаблони для додаткових можливостей моніторингу

Шаблони — це спеціальні доповнення, які розширюють функціональні можливості Zabbix. Деякі шаблони створені Zabbix і постачаються разом із програмним забезпеченням, готовим до використання, тоді як інші створені користувачами Zabbix. Шаблони дозволяють користувачам Zabbix контролювати мережеві пристрої таких постачальників, як Cisco, Dell, HP і Juniper. Інші шаблони можна використовувати для моніторингу серверів IBM, HP і Super Micro. Шаблони для служб на основі додатків включають Microsoft Exchange і Exchange Server, Zenoss, PowerDNS, Authoritative Server Stats тощо. Також можна створювати шаблони для моніторингу ОС і гіпервізорів.

2.2 Вимоги до комутаційного обладнання

Вимоги до комутаційного обладнання можуть відрізнятися залежно від конкретних потреб та сценаріїв використання, але загалом у сучасних рішеннях можна виділити кілька загальних вимог:

– Висока пропускна здатність: комутаційне обладнання має забезпечувати достатню пропускну спроможність передачі великого обсягу даних.

– Надійність і стійкість до відмов: обладнання повинно бути надійним і мати механізми автоматичного відновлення після збоїв.

– Гнучкість та масштабованість: обладнання має бути гнучким та масштабованим, щоб задовольняти мінливим вимогам мережі.

– Безпека: обладнання має забезпечувати захист від зовнішніх загроз та бути здатним контролювати доступ до мережі.

– Простота управління: обладнання повинно мати простий та зрозумілий інтерфейс керування для адміністраторів мережі.

– Енергоефективність: обладнання має бути енергоефективним, щоб знизити витрати на енергоспоживання та екологічні ризики.

– Підтримка новітніх стандартів та протоколів: обладнання має підтримувати новітні стандарти та протоколи для забезпечення сумісності та ефективної роботи з іншими пристроями в мережі.

Для написання дипломної роботи було використано високоякісне мережеве обладнання, що має такі характеристики:

Інтерфейс:

– кількість портів доступу - не менше 24;

– інтерфейси доступу-RJ-45 10/100/1000 Base-T;

– uplink порти - не менше 4 фіксованих портів Gigabit Ethernet.

SFP Комутація:

– продуктивність комутації - не менше 10 Гбіт / с;

– розмір буфера кадрів - не менше 256 кБайт;

– розмір таблиці MAC-адрес - не менше 8000.

Управління трафіком:

– підтримка протоколів групи SNMP;

– підтримка та тегування VLAN: підтримка IEEE 802.1 Q та 4,094 одночасних ідентифікаторів VLAN;

– відстеження групової адресації по протоколу IP;

– відстеження мережевого трафіку IGMP;

– відстеження мережевого трафіку MLD;

– черга на основі пріоритетів (SP);

– кільцевий список з ваговими коефіцієнтами (WRR);

– зважене довільне раннє виявлення (WRED).

Безпека:

– підтримка Port security;

– обмеження кількості MAC-адрес на порт;

– використання апаратних високошвидкісних спусків

– управління доступом (ACL);

– підтримка GUI або MIB;

– підтримка SSL;

– підтримка DHCP;

– підтримка IP Source Guard;

– запобігання ARP Spoofing;

– представлення парольної інформації в CLI і файлі конфігурації в зашифрованому вигляді.

Управління:

– підтримка SNMP;

– не менше 2-х ipv6;

– IMC - Intelligent Management Center;

– інтерфейс командного рядка;

– веб-браузер;

– можливість збереження файлу конфігурації в текстовому вигляді, з подальшим відновленням повної конфігурації комутатора при її втраті шляхом вставки даного текстового файлу у вікно терміналу через

– буфер обміну;

– генерація syslog повідомлень і SNMP Traps при зміні стану;

– SNMP Manager;

– Підтримка декількох файлів конфігурації;

– дозволяє контролювати вхід і вихід порту;

– підтримка ping (IPv6) і traceroute (IPv6);

– підтримка TFTP / FTP для завантаження файлів ПО;

– визначає MAC-адресу іншого хоста IP в тій же підмережі;

– підтримка статичних ARP. ARP дозволяє виявляти дубльовані IP-адреси;

– підтримка DHCP;

– протокол дейтаграм користувача (UDP);

– можливість перегляду серійного номера комутатора та інформації О SFP модулі (через CLI і SNMP).

Підтримка списку контролю доступу (ACL):

– підтримка не менше 100 ACL різного типу;

– підтримка ACL на основі портів;

– підтримка ACL на основі MAC-адрес (заборонені MAC-

– адреси не повинні вивчатися);

– підтримка ACL на основі IP адрес;

– підтримка ACL на основі портів TCP / UDP;

– підтримка ACL на основі 802.1 q.

Якість обслуговування:

– управління Broadcast дозволяє обмежувати швидкість широкомовного трафіку, щоб скоротити небажаного мережевого трафіку широкомовної розсилки;

– розширений Класифікатор на основі QoS, класифікує трафік з використанням декількох критеріїв відповідності, засновані на рівнях 2, 3 і 4;

– рівня пріоритету і обмеження швидкості для обраного трафіку на порт, VLAN, або всього комутатора;

– підтримка дисциплін обслуговування черг SP, WRR,

SP+WRR Групові розсилки:

– підтримка IGMP Snooping;

– Інтернет-протокол управління групи (IGMP) використовує

Підтримка IPv6:

– підтримка IGMP Snooping;

– Інтернет-протокол управління груп (IGMP) використовує Any-Source Multicast (ASM) або Source-Specific Multicast (SSM) для управління багатоадресної мереж IPv6.

Характеристики мережевого екрану:

– має бути 4 фільтруючих інтерфейсу;

– можливі типи інтерфейсу-Ethernet 10Base-T/100BASE-

– TX/1000BASE TX/10000BASE TX;

– швидкість, 10000 Мбіт / сек;

– кількість керуючих інтерфейсів - 1;

– можливі типи інтерфейсу-Ethernet 10Base-T/100BASE-

– TX/1000BASE TX;

Функціональні характеристики мережевого екрану:

– можливість управління сесіями;

– можливість багаторівневої, багато протокольної прихованої пакетної фільтрації;

– режим роботи за допомогою NAT;

– можливість аутентифікації вхідних і вихідних запитів;

– здатність блокування мережевих flood-атак;

– вивантаження файлів реєстрації подій і пакетів з

– використанням протоколів FTP і SYSLOG;

– захист каналу управління;

– здатність контролю інтерфейсів за допомогою довірених адрес;

– дзеркалювання трафіку;

– гаряче резервування при відмові обладнання.

Виходячи з вимог до комутаційного обладнання, для

створення системи моніторингу мережевих компонентів, що розглядаються в дипломній роботі:

– комутатор Mikrotik CRS328-24P-4S+RM;

– комутатор Mikrotik CRS328-4C-20S-4S+RM

– комутатор Mikrotik;

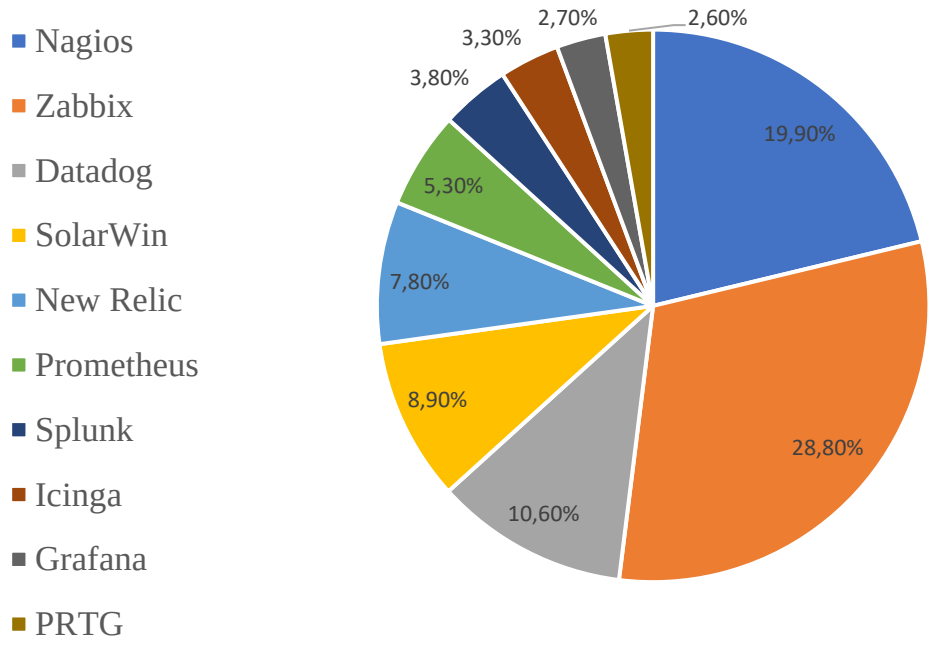
– шлюз Mikrotik CCR1072-1G-8S+;

– точка доступу UniFi UAP-AC-HD;

2.3 Статистика ринку програмного забезпечення для моніторингу

Згідно з звітом "Software market monitoring 2022" від компанії Datanyze, найпопулярнішими системами моніторингу на ринку є:

- Nagios – 19.9%
- Zabbix - 28.8%
- Datadog - 10.6%
- SolarWinds - 8.9%
- New Relic - 7.8%
- Prometheus - 5.3%
- Splunk – 3.8%
- Icinga – 3.3%
- Grafana – 2.7%
- PRTG Network Monitor - 2.6%



Діаграма 2.1. Статистика використання програмного забезпечення компаніями

За статистикою видно, що більшість компаній використовує програмне забезпечення від компанії Zabbix та Nagios.

Ці обидві системи моніторингу містять в собі:

– Безкоштовність: Обидві системи моніторингу є безкоштовними та відкритими, що робить їх доступними для широкого кола користувачів.

– Гнучкість і велика кількість налаштувань: Zabbix і Nagios мають широкий спектр функціональних можливостей, які можна налаштувати під конкретні потреби компанії. Це дозволяє адміністраторам моніторингу максимально адаптувати їх до власної інфраструктури.

– Широка підтримка протоколів та пристроїв: Обидві системи моніторингу підтримують велику кількість протоколів та пристроїв, що дозволяє використовувати їх для моніторингу різних типів обладнання та сервісів.

– Активна спільнота: Zabbix та Nagios мають велику спільноту користувачів та розробників, які постійно працюють над покращенням та доробкою систем. Це дозволяє швидко отримувати підтримку та вирішувати проблеми в процесі експлуатації.

– Надійність: Як правило, Zabbix та Nagios вважаються надійними та стабільними системами моніторингу, які здатні працювати в умовах високих навантажень та забезпечувати безперервний моніторинг інфраструктури.

В цілому, використання Zabbix і Nagios є популярним вибором для багатьох компаній але Zabbix бере гору тим,що підтримка протоколів протоколів та пристроїв більша, інтерфейс більш адаптований під користувача, є можливість створення власних шаблонів моніторингу та надійністю.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОВЕДЕННЯ МОНІТОРИНГУ ІНФРАСТРУКТУРИ ОГРАНІЗАЦІЇ НА БАЗІ РІШЕННЯ ZABBIX

Zabbix є потужною та гнучкою системою, яка може бути використана для моніторингу мереж будь-якого масштабу та складності. Він забезпечує високу надійність та продуктивність мережі, що робить його одним з найбільш популярних та поширених інструментів для управління мережею у світі.

Серед основних функцій Zabbix можна виділити:

– Моніторинг різних параметрів мережі, таких як використання ресурсів, трафік мережі, доступність пристроїв.

– Оповіщення про аномалії та збої в роботі мережі, що дозволяє оперативно реагувати на можливі проблеми.

– Автоматичне визначення нових пристроїв у мережі, що спрощує керування та моніторинг великих мереж.

– Звітність про продуктивність та доступність мережі, що дозволяє аналізувати та покращувати її роботу.

– Підтримка різних протоколів та технологій, таких як SNMP, IPMI, JMX.

– Інтеграція з іншими системами управління, такими як Nagios та BMC Remedy.

Адміністратору мереж який відповідає за безперебійну роботу всього мережевого обладнання, потрібно пильно обирати не тільки мережеве обладнання, а ще й програмне забезпечення для моніторингу стану інфраструктури. Ця робота полягає в тому, щоб забезпечити роботу обладнання та допомогти співробітникам організації виконувати свої обов'язки, особливо в умовах, коли деякі сервіси переходять в онлайн-режим. Щоб забезпечити безперебійну роботу, необхідно мати швидкий інтернет-зв'язок та ефективний інструмент моніторингу. Серед багатьох інструментів відиляється Zabbix, який з'явився в 1998 році і є потужною системою керування мережею з рядом функціональних можливостей для

моніторингу продуктивності, стану серверної інфраструктури та мережевих служб. Zabbix дозволяє моніторити стандартні та статистичні дані в режимі реального часу, що допоможе вирішувати будь-які проблеми, щойно вони виникають, і забезпечувати ефективну роботу всіх робочих процесів.

3.1. Рекомендації щодо встановлення та налаштування Zabbix

Першочергово протрібно вибрати операційну систему, де буде встановлено Zabbix. Zabbix підтримує велику кількість операційних систем, включаючи Windows, Linux, FreeBSD та інші.

Перед початком встановлення самого Zabbix потрібно створити віртуальну машину з такими мінімальними характеристиками:

– віртуальна машина з принаймні одним мережевим адаптером;
– RAM: 2048 МБ;
– Disk space 20 GB;
– CPU cores – 2.

Конфігурація віртуальної машини може змінюватись від того скільки хостів буде підключене до системи моніторингу.

Для створення віртуальної машини потрібно зайти на гіпервізор ProxMox, натиснути паравою клавішою по кластеру та обрати create vm

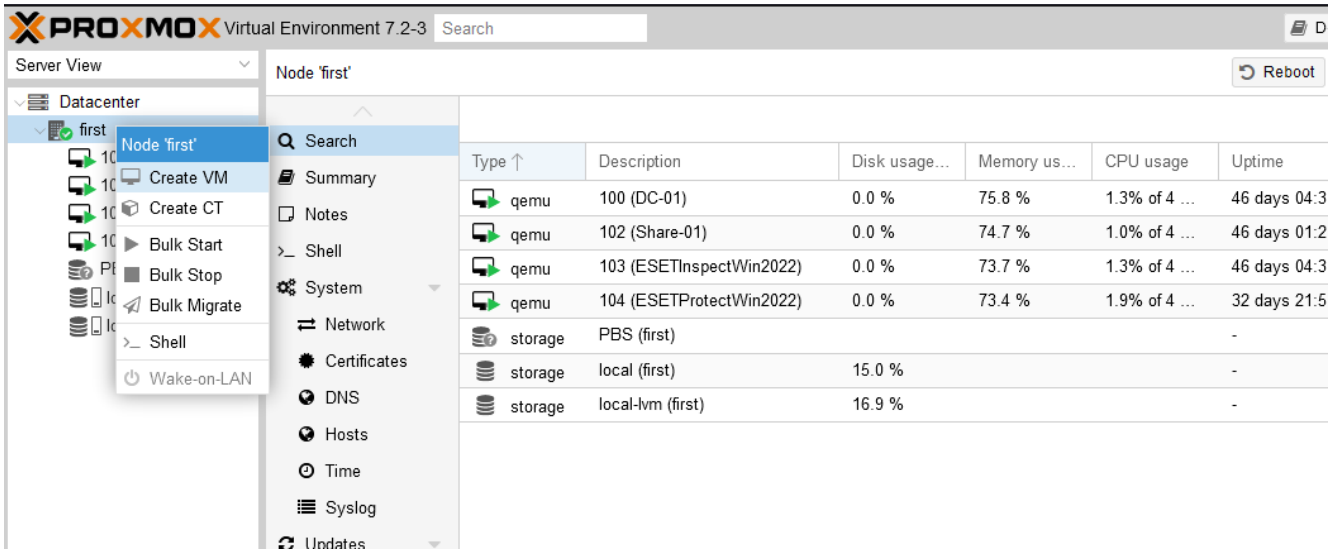


Рис.3.6. Створення віртуальної машини в кластері ProxMox

Далі у вікні конфігурації даємо назву віртуальної машини ZabbixMonitoring, обираємо start on boot, щоб після перезапуску серверу віртуальна машина запускалась в автоматичному режимі. У вкладці OS обираємо Ubuntu 20.04, яку заздалегіть завантажили на сервер.

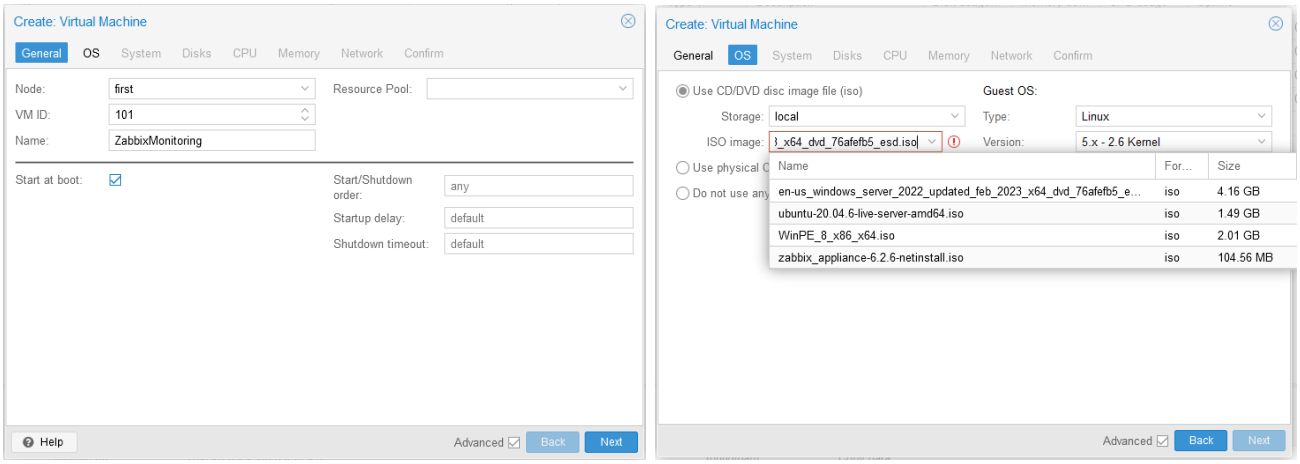


Рис.3.7. Перший етап створення віртуальної машини

У наступному вікні обираємо розмір диску та кількість ядер для віртуальної машини.

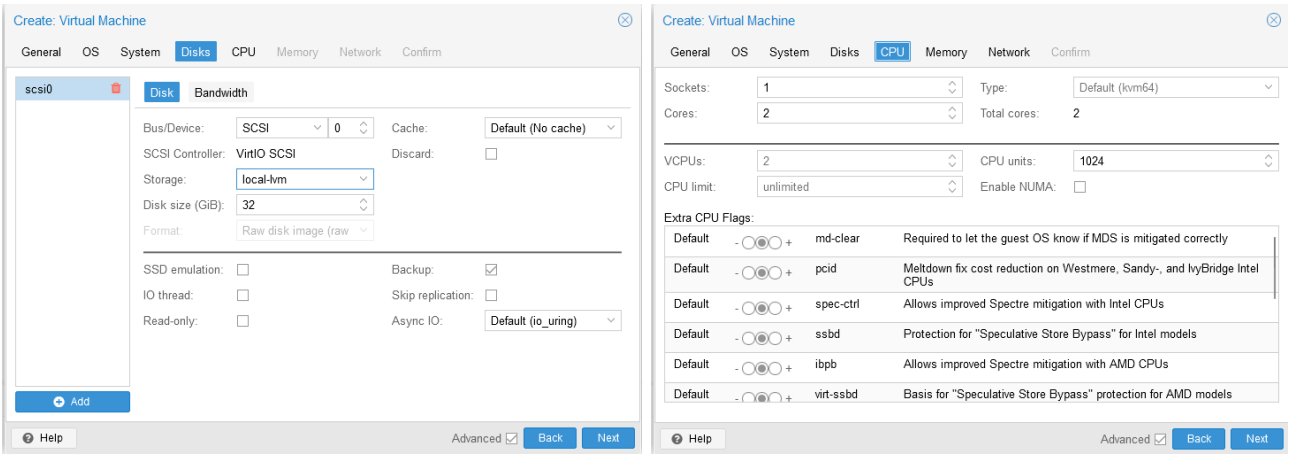


Рис.3.8. Налаштування диску та ядер віртуальної машини

У вкладці Memory ставимо необхідний обсяг оперативної пам’яті та настискаємо Next.

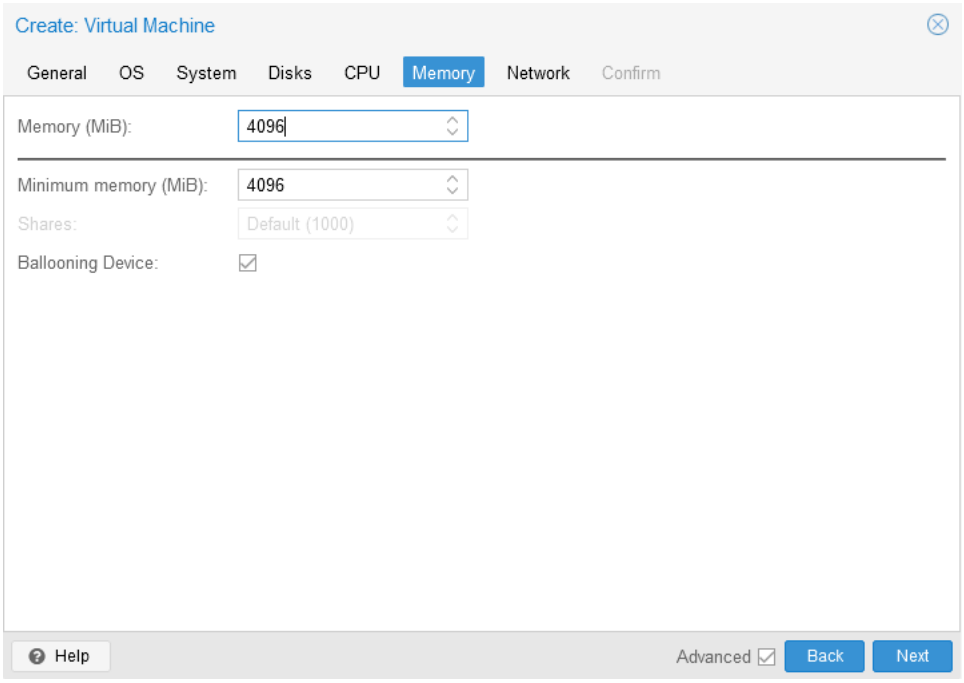


Рис.3.9. Налаштування обсягу оперативної пам’яті

Далі починається звичний процес встановлення Ubuntu. У процесі встановлення потрібно обрати мову системи – English, розмітити дисковий простір.

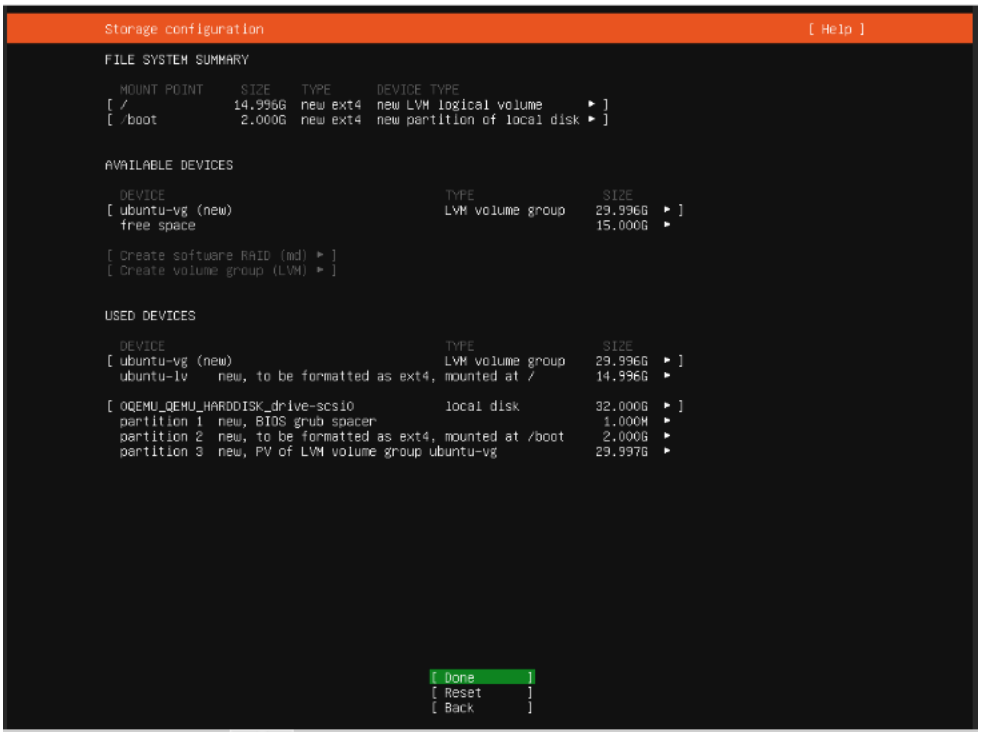


Рис.3.10. Розмітка дискового простору на віртуальній машині

Після цього створюємо користувача системи, встановити пароль адміністратора та даємо hostname машині – Zabbix.

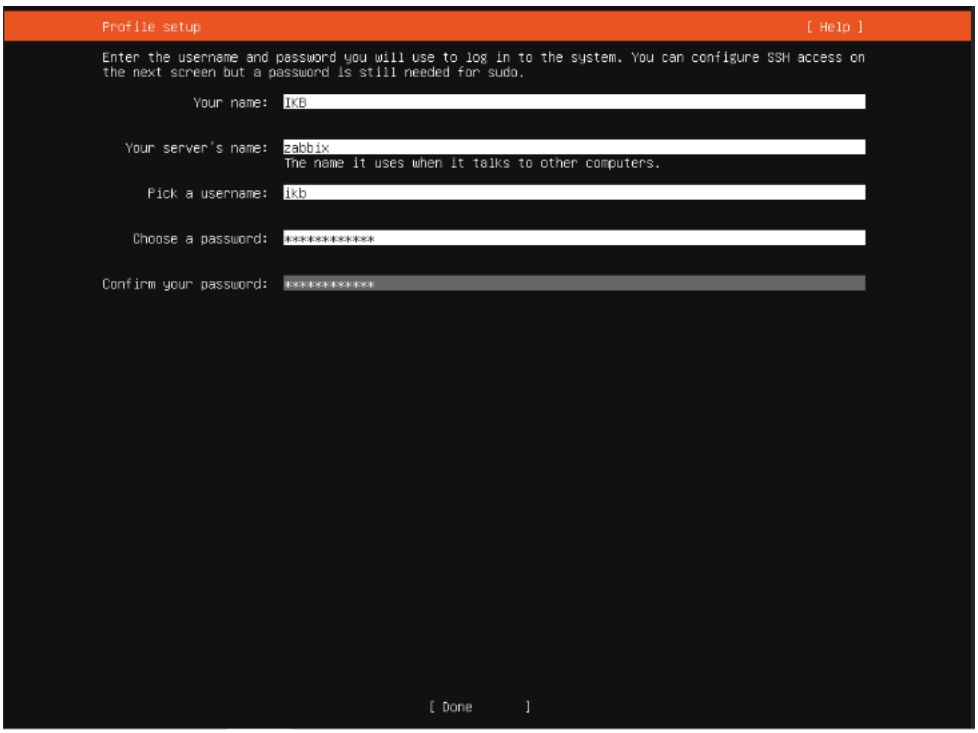


Рис.3.11. Створення облікового запису та задання hostname

Починається процес встановлення системи на віртуальну машину. Після того як система буде встановлена потрібно буде відмонтувати образ системи та перезапустити її, після цього можна заходити через ssh.

Поставивши всі оновленя системи починаємо встановлювати Zabbix за допомогою контейнера docker.

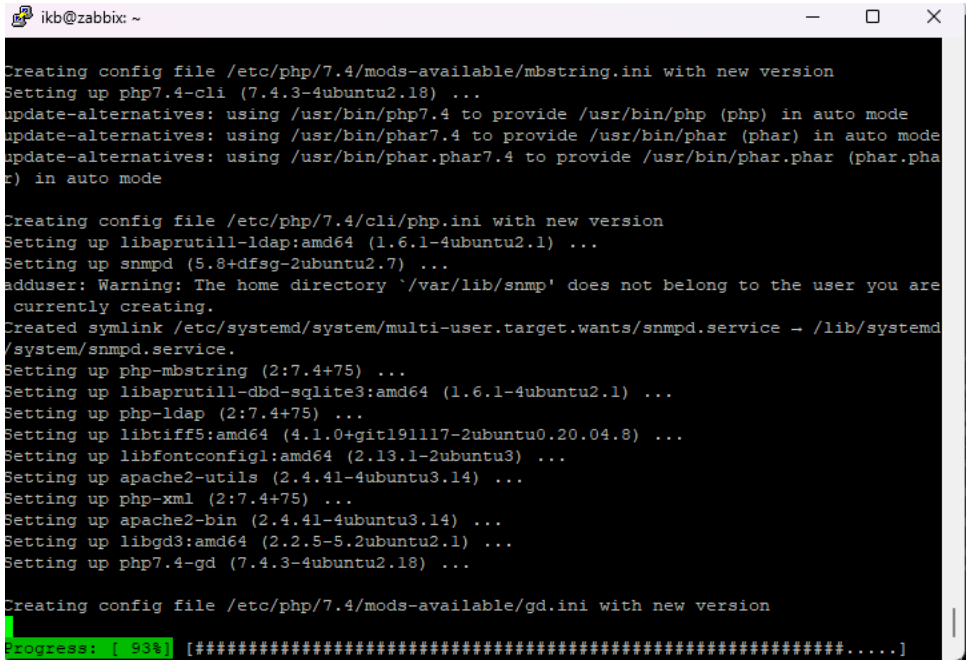


Рис.3.12. Процес встановлення ядра Zabbix та frontend

Потрібно встановити Zabbix agent на сам сервер для збору інформації про нього. Наступний крок – це встановлення mysql та налаштування бази даних та користувача цієї бази.

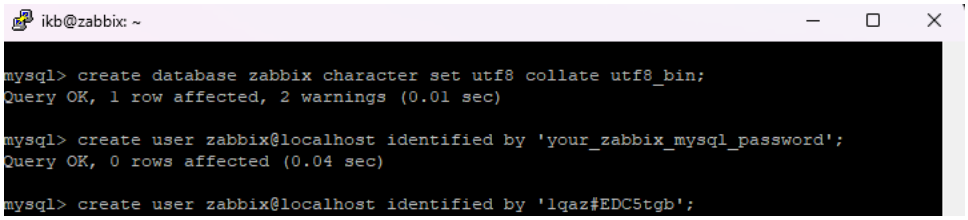


Рис.3.13. Налаштування бази та користувача цієї бази

Для автоматичного налаштування ngnix запустимо пакет налаштувань

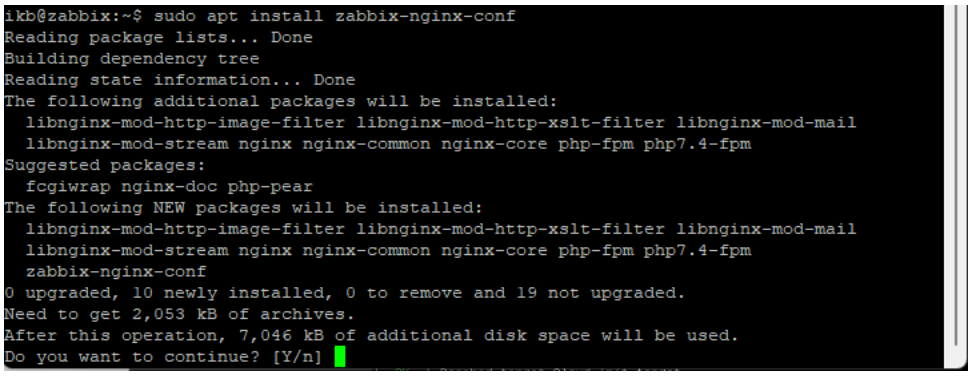


Рис.3.13. Автоматичне налаштування ngnix

Автоматично створиться файл в якому потрібно змінити порт веб сторінки Zabbix та доменне ім’я веб сторінки.

Рис.3.14. Зміна налаштувань у файлі конфігурації ngnix

Після зміни конфігурації потрібно перезавантажити файл та перевірити на помилки синтаксис.

Веб-інтерфейс Zabbix написаний мовою PHP, і для нього потрібна низка спеціальних налаштувань сервера PHP. Під час встановлення Zabbix було створено

файл конфігурації PHP-FPM, який містить ці налаштування. Він розташований у каталозі /etc/zabbix і автоматично завантажується PHP-FPM. Потрібно внести невелику зміну до цього файлу. Розкоментувати рядок часового поясу, та змінити його на свій часовий пояс. Потім зберегаємо файл та закриваємо.

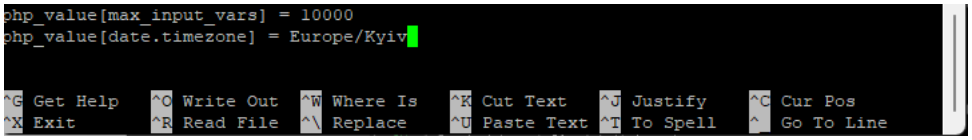


Рис.3.14. Зміна часового поясу

Далі перезапускаємо сервіс PHP-FPM, та переходимо до запуску самого серверу Zabbix. Після успішного запуску додаємо його в автозавантаження.

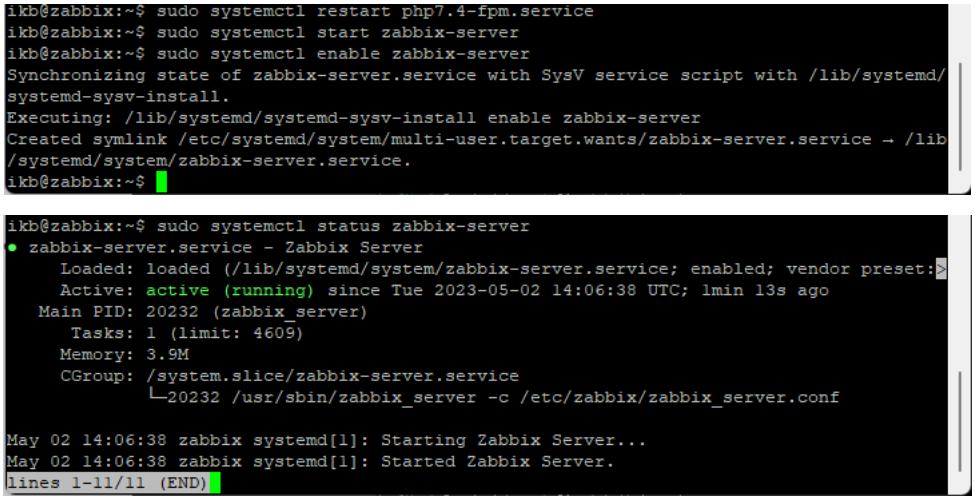


Рис.3.14. Запуск Zabbix серверу

Веб-інтерфейс дозволяє бачити звіти та додавати хости, які ви хочете відстежувати, але для цього потрібне певне початкове налаштування. Щоб перейти до веб версії потрібно в браузері перейдти за адресою http://zabbix.duikt.lan або https://zabbix.duikt.lan, якщо встановити Let's Encrypt. На першому екрані зустрічає вітальне повідомлення. Щоб продовжити, натисніть Next step (Далі).

На наступному екрані буде таблиц, де буде перераховано всі попередні вимоги для запуску Zabbix.

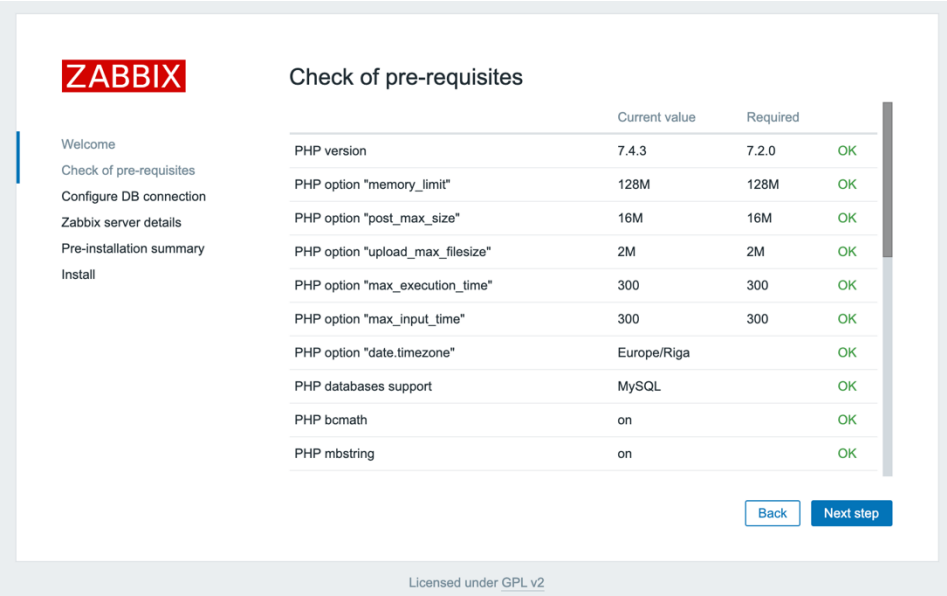


Рис.3.15. попередні вимоги для запуску Zabbix

Далі перед нами відкриється вікно входу. Увійдіть, використовуючи облікові дані за замовчуванням:

– Ім'я користувача: Admin
– Пароль: zabbix

Рис.3.16. Вікно входу в систему моніторингу

Після входу в веб-платформу Zabbix стандартно відображається англійський інтерфейс, проте ви можете переключити його на українську мову. Для цього слід обрати опцію «Administation» на панелі навігації, після чого вибрати рівень 2. У

розділі «User settings» в підрозділі «Profile» можна побачити інформацію про поточних користувачів Zabbix. За замовчуванням для входу в Zabbix web доступний лише один адміністратор з логіном "admin". Щоб змінити мову інтерфейсу, слід клацнути на користувача Admin, відкрити вікно налаштування властивостей і знайти в опції «Language» потрібну мову, яку бажаєте використовувати. Після вибору необхідної мови слід зберегти зміни, оновити сторінку браузера, щоб зроблені зміни вступили в силу.

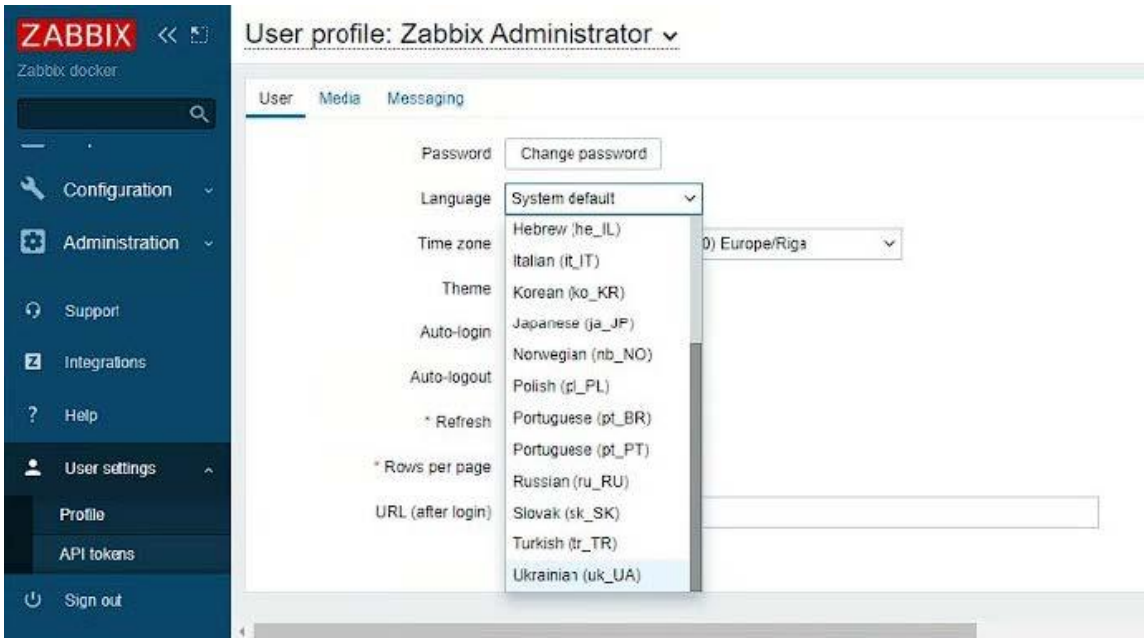


Рис.3.17. Зміна мови інтерфейсу

3.2. Рекомендації налаштування шаблонів та груп хостів

Управління та використання шаблонів

Центральною функцією Zabbix є його шаблон, оскільки він містить весь необхідний контент для моніторингу та графічного відображення. Після встановлення Zabbix користувач має доступ до безлічі шаблонів (наприклад, шаблон для мережевих пристроїв, операційних систем, загального програмного забезпечення тощо), які відповідають потребам 80% користувачів програми. Тому, як правило, немає необхідності вручну створювати нові шаблони.

У веб-інтерфейсі Zabbix користувач може знайти шаблони, вибравши опцію "Налаштування" і далі "Шаблони". За замовчуванням, шаблони містять декілька

вбудованих проектів, які містять набори вузлів мережі, елементів даних, тригерів, графіків, панелей, виявлення, веб-компонентів тощо. Ключові частини включають елементи моніторингу, тригери та графіки, які автоматично виявляються.

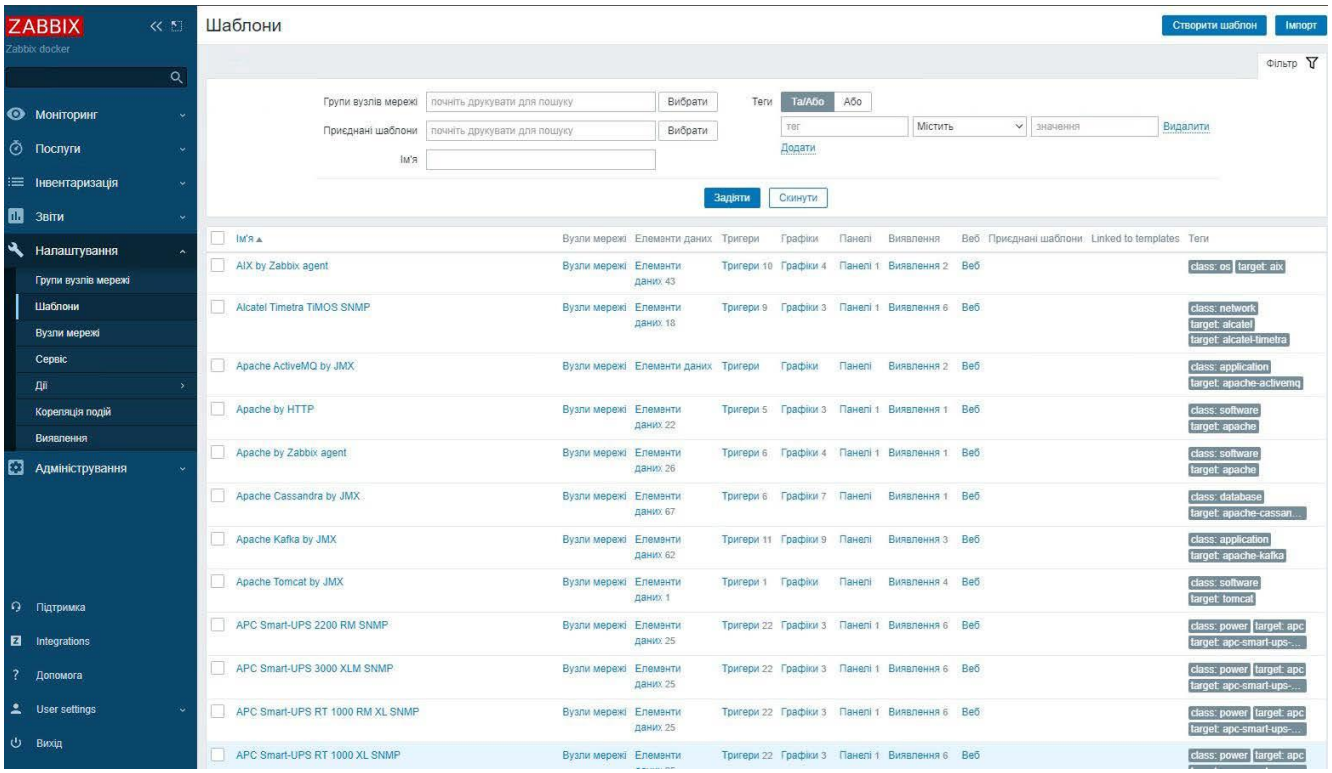


Рис.3.18. Меню шаблонів Zabbix

Створення груп хостів та хостів

Одним з головних завдань моніторингу в Zabbix є створення вузлів мережі. Якщо ви бажаєте моніторити параметри на сервері "x", необхідно спочатку створити вузол мережі з назвою, наприклад, "Сервер X". Тільки після цього ви зможете додавати елементи для моніторингу сервера. Вузли мережі можуть бути об'єднані у групи.

Щоб додати інтерфейс групи хостів, необхідно натиснути параметр налаштування на веб-інтерфейсі (рис. 3.19) і вибрати групу вузлів мережі. Вже існує декілька груп хостів за замовчуванням, і ви можете використовувати існуючі групи або створити нову групу, натиснувши "Створити групу вузлів мережі" у правому верхньому куті. Групу хостів потрібно створити перед додаванням хоста, оскільки опція групи не створюється в інтерфейсі створення хоста.

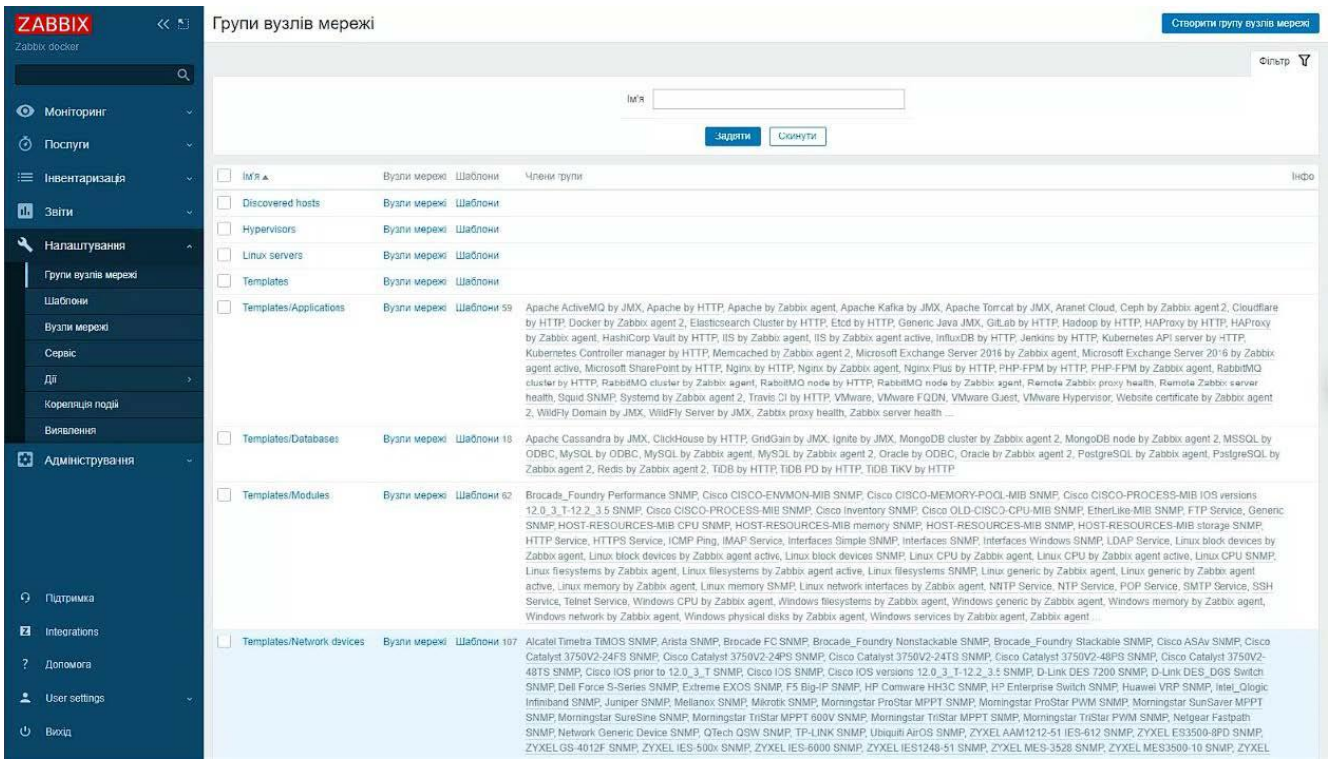


Рис.3.19. Меню вузлів Zabbix

Після створення групи хостів натисніть на параметр конфігурації в Інтернеті, потім виберіть "Вузли мережі" (рисунок 3.20), після цього ви можете додати інтерфейс хоста.

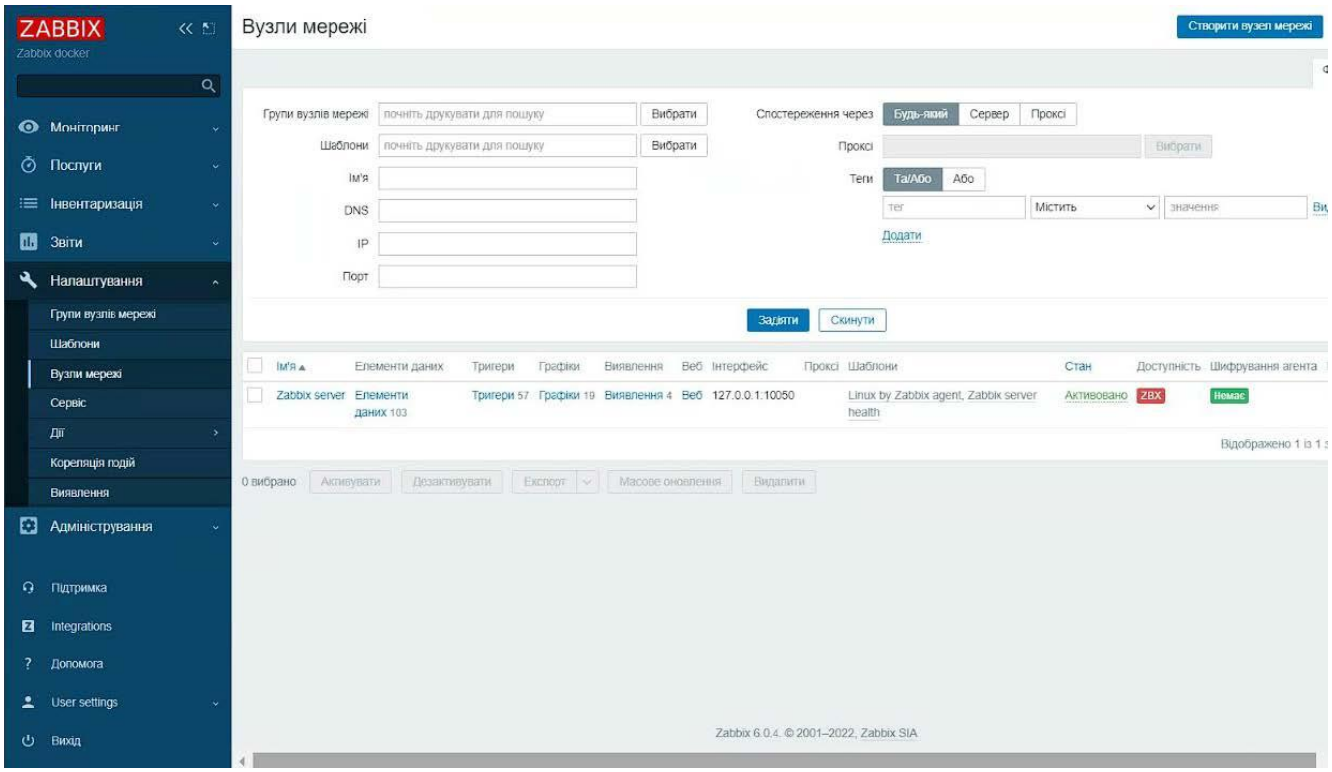


Рис.3.20. Додавання хостів

За замовчуванням у Zabbix існує тільки один хост, щоб додати інші, треба натиснути на кнопку "Створити вузол мережі", після відкриється вікно створення хоста.

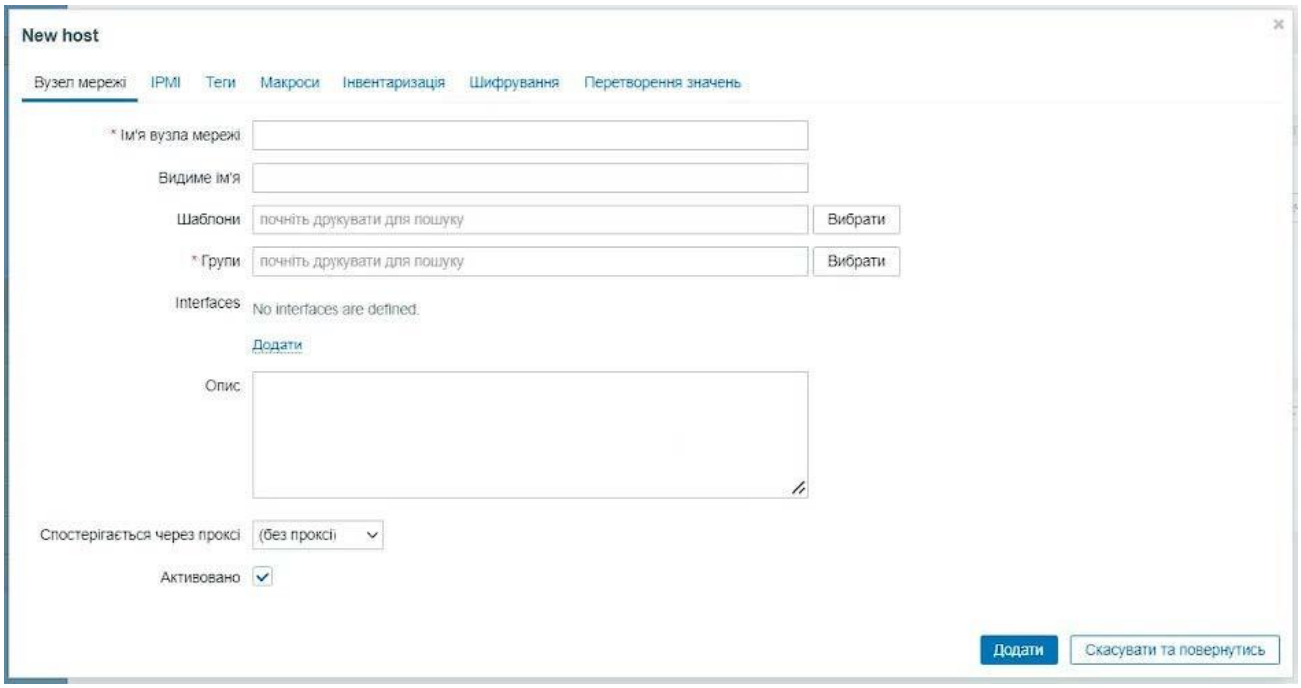


Рис.3.21. Створення хоста Zabbix

Ввівши всі потрібні данні, натискаємо кнопку «Додати», і якщо на вашому обладнанні налаштований SNMP у списку вузлів з’явиться пристрої які ви вказали.

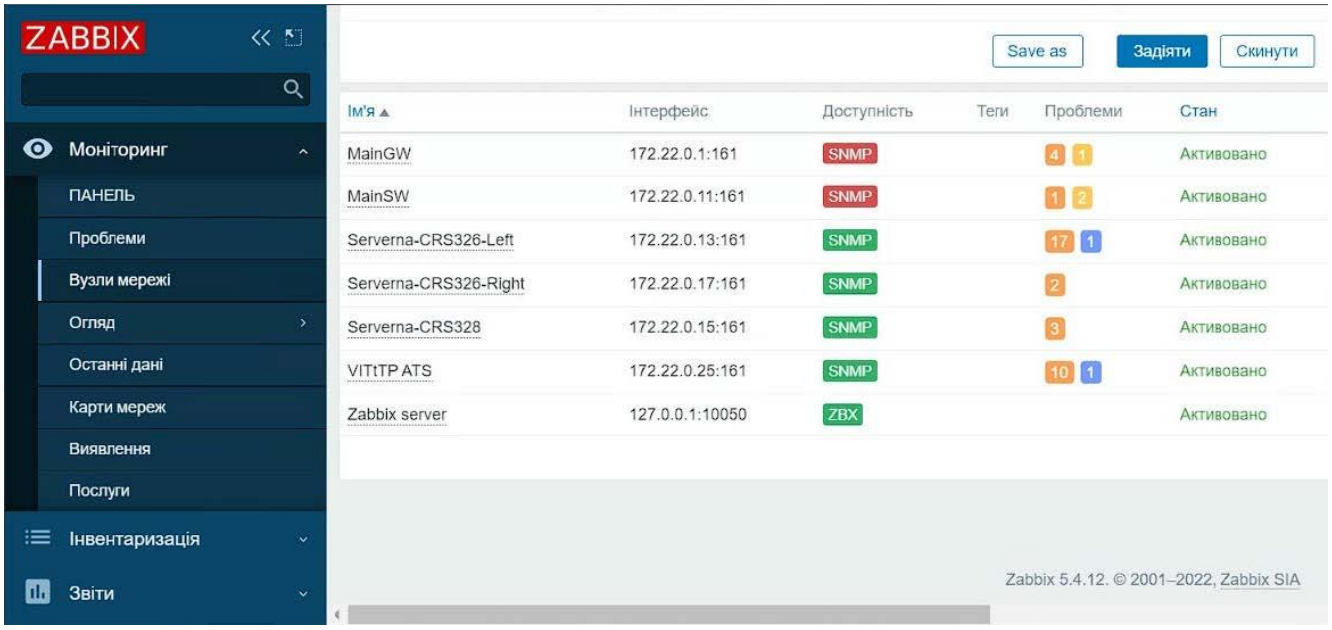


Рис.3.22. Перелік створених хостів

В результаті ми можемо спостерігати за станом доданих мережевих пристроїв на головній сторінці. Zabbix дозволяє спостерігати за такими параметрами як навантаження на процесор, чи температуру обладнання. На цьому базове налаштування системи моніторингу закінчено.

Рис.3.22. Головна панель моніторингу Zabbix сервера

3.3. Основні рекомендації щодо моніторингу мережі

Відправною точкою впровадження будь-якої системи моніторингу мережі є встановлення базової поведінки мережі. У документі має бути зазначено, що засвідчує нормальну поведінку мережі, прийнятний діапазон значень для всіх контрольованих параметрів і які пристрої підключено. У ньому також описано, як мережа взаємодіє з пристроями та службами за межами організації.

Ця інформація створює основні блоки, на яких будується все прийняття рішень щодо проектування системи моніторингу. Може виникнути спокуса пропустити цей крок, припускаючи, що ми знаємо все, що потрібно знати про мережу нашої організації. Але пам’ятайте, якщо фундамент хитний, кінцевий продукт не буде стійким або масштабованим.

Часто самі інструменти моніторингу мережі розміщуються в тій самій мережі, за якою вони здійснюють моніторинг. Це означає, що якщо мережа вимикається або значно сповільнюється, монітор також вийде з ладу, а це робить аналіз зібраних даних майже неможливим.

Таким чином, слід розгортати засоби моніторингу з урахуванням високої доступності та параметрів відновлення після відмови. Найпростіший і найдешевший спосіб — тиражувати та зберігати всі дані монітора в незалежному центрі обробки даних. Відмова може викликати автоматичне встановлення іншого мережевого монітора. Потім цю систему можна налаштувати для отримання інформації з цієї резервної копії в надзвичайних ситуаціях.

Сьогодні більшість підприємств мають команди NetOps, щоб зосередитися на мережевих операціях. Подібно до того, як команди DevOps займаються автоматизацією та перевіркою завдань розробки, команди NetOps прагнуть оптимізувати операції, пов’язані з мережею. Загалом, завдання моніторингу мережі в першу чергу лягає на них.

Більшість команд NetOps починають із базових, вузькоспеціалізованих інструментів з відкритим кодом і додають необхідні інструменти, коли виникає потреба. Після кількох років розширення групи мережевого моніторингу починають обробляти від трьох до десяти інструментів одночасно (відоме як розповсюдження інструментів).

Розпорошення інструментів є дуже неефективним, оскільки потрібен час і ресурси, щоб отримати з них релевантну інформацію, а потім встановити зв’язки. Щоб уникнути розповсюдження інструментів, компанії повинні почати з рішень моніторингу, які є масштабованими та можуть бути налаштовані для взаємодії з існуючими та новішими інструментами. Навіть якщо кількість інструментів, що використовуються, не можна звести до одного, взаємодія має бути однією з основних характеристик, на яку слід звернути увагу.

Топологія ланцюжка — це компонування, у якому ідентичні компоненти з’єднані в послідовність, як пелюстки квітки ромашки. На великих підприємствах найпоширенішим шлейфовим компонентом є комутатор.

Шторми тривоги виникають, коли сповіщення не розміщуються належним чином в проаналізованих і стратегічних місцях. Забагато сповіщень може спричинити втому та змусити команду NetOps ігнорувати законні сповіщення. Попереджувальні шторми також відволікають їх від виконання інших важливих операцій.

Для підтримки потоку даних через мережу задіяні різні пристрої. Параметри конфігурації маршрутизатора відрізняються від параметрів комутатора. Правильна конфігурація життєво необхідна для стабільної та безпечної мережі. Зазвичай зберігається конфігурація за замовчуванням, яка постачається з пристрою. Це недоцільно, оскільки вимоги організації можуть не збігатися зі значеннями за замовчуванням. Саме тут на допомогу приходить керування конфігурацією. Керування конфігурацією передбачає налаштування окремих значень без значного впливу на мережу.

Коли інструменти керування конфігурацією поєднуються з інструментами моніторингу, адміністратори можуть контролювати користувачів і пристрої з повною видимістю мережі. Це призводить до меншої кількості помилок і дозволяє тестувати незавершені зміни в меншому масштабі. Управління конфігурацією також автоматизує нові компоненти в мережі, одночасно зберігаючи оновлення базової лінії та карти мережі на моніторі.

Повну картину працездатності мережі утворює комбінація інформації, отриманої від різних підключених до неї пристроїв. Кожну точку даних, будь то розміри пакетів чи дані SNMP, необхідно проаналізувати разом з іншими, щоб побачити, які висновки можна з них отримати.

Цілі повинні бути встановлені на початку проекту моніторингу мережі, як і в будь-якій іншій великій діяльності. Потім ці цілі можна відфільтрувати до тих ідей, які необхідні для досягнення кожної з них. Ці дані можна потім відстежити, щоб побачити, звідки можна отримати інформацію. Також необхідно налаштувати моніторинг, щоб відфільтрувати непотрібні шуми. Такий аналіз вимагає практики. Якщо організації бракує часу або досвіду, має сенс найняти консультанта або поговорити з постачальником послуг.

Моніторинг мережі залежить від одного — інформаційної панелі, яка забезпечує повну видимість усіх аспектів мережі. Адміністратори повинні мати можливість помітити ненормальну поведінку, просто глянувши на інформаційну панель. Візуалізація важлива для будь-якої моніторингової діяльності. У той час як більшість інструментів моніторингу автоматично створюють мережеві карти, необхідно передбачити можливість додавати певні дані. Інформаційні панелі також потрібно налаштовувати відповідно до ролі особи, яка на них дивиться, і місця розташування.

Ідеальний спосіб спроектувати інформаційну панель — це зважити найважливіші компоненти, а решту показати як частину інцидентних потоків з першого погляду. Безладна інформаційна панель стане лише громіздкою, оскільки мережа розростається та сповільнює аналіз і виправлення.

Більшість реакцій на інциденти починаються з інформаційної панелі мережевого монітора. За винятком природних катаклізмів, усі інші загрози для мережі спочатку відображаються на моніторі. Ось чому мережеві монітори повинні бути оснащені матрицею ескалації. Матриця ескалації зазвичай є частиною планів реагування на інциденти. Це документ, який визначає, коли має відбутися ескалація, яких процесів слід дотримуватися та кого потрібно залучати на кожному рівні.

Будь-яка мережева проблема, помічена на інформаційній панелі, має пройти через правильні канали для вирішення. Це особливо актуально для великих підприємств із глобальними мережами, де працюють кілька адміністраторів і команд.

Типова мережа дотримується чотирирівневої моделі TCP/IP, а деякі все ще повертаються до семирівневої моделі взаємозв’язку відкритих систем (OSI). Кожен рівень прив’язаний до такої функції, як прикладний, транспортний, Інтернет і рівень доступу до мережі. Хороший інструмент моніторингу мережі забезпечує представлення інформації на кожному рівні цих рівнів. Це забезпечує повне покриття всіх аспектів мережі.

Окрім цього, звіти також повинні базуватися на потоках інцидентів і управлінні проблемами. Звіти мають вирішальне значення для моніторингу мережі, оскільки:

- Вони підтверджують існуючу мережу
- Вони висвітлюють історично значиму інформацію
- Вони розкривають тенденції, які можна використовувати для реорганізації або масштабування мережі
- Вони надають регуляторам докази відповідності

Як згадувалося раніше, мережевий моніторинг — це сукупність моніторингу додатків, моніторингу веб-служб і безлічі інших функцій моніторингу. Для кожного типу моніторингу необхідний відповідний тип експертизи, щоб отримати найбільш оптимальну необхідну інформацію. Кожен із них використовує власні протоколи зв’язку, а деякі навіть використовують API.

Позиція компанії безпосередньо пов’язана з її мережевою інфраструктурою. Мережа зростає разом із компанією, а це означає, що великим підприємствам потрібні віддані експерти для покращення продуктивності, стабільності та безпеки мережі. Компанії можуть створити систему моніторингу з нуля або підписатися на послуги залежно від того, які ресурси вони мають у своєму розпорядженні. Це життєво важливо, оскільки сфера моніторингу мережі простягається від щоденних операцій до захисту даних споживачів.

ВИСНОВКИ

В даній бакалаврській роботі було розглянуто питання моніторингу мереж в інформаційній системі. Моніторинг є важливим елементом забезпечення стабільності роботи мереж та підключених до них пристроїв, програм та систем. В процесі роботи було проаналізовано існуючі методи моніторингу та визначені їх переваги та недоліки. Було розглянуто важливі аспекти, такі як відстеження стану мережі, виявлення проблем, аналіз використання ресурсів та планування потреб у їх збільшенні.

В роботі коротко розглянуті протоколи SNMP, структура мережі Інтернет та основні протоколи маршрутизації. Також проведено порівняльний аналіз протоколів SNMP, ICMP і CDP, включаючи їх заголовки з детальним описом компонентів. Робота містить інформацію про формати додаткових заголовків, які можуть використовуватися протоколом SNMP. Крім того, проаналізовано основні характеристики протоколів моніторингу.

Отримані результати можуть бути корисними для тих, хто працює з мережами та хоче забезпечити їх стабільну та надійну роботу. Результати дослідження можуть бути використані для подальшого вдосконалення методів моніторингу та підвищення ефективності роботи мереж.

ПЕРЕЛІК ПОСИЛАНЬ

1. MikroTik Monitoring with LABS [Електронний ресурс]. – Режим доступу: https://www.udemy.com/course/mikrotik-monitoring-with-labs-the-dude/
2. What can Nagios help you do? [Електронний ресурс]. – Режим доступу: https://www.nagios.org/
3. Nagios Tutorial [Електронний ресурс]. – Режим доступу: https://www.javatpoint.com/nagios
4. Unleash your network's operational efficiency [Електронний ресурс]. – Режим доступу: https://www.cisco.com/
5. Nagios [Електронний ресурс]. – Режим доступу: https://coderlessons.com/tutorials/devops/vyuchi-nagios/nagios-kratkoe-rukovodstvo
6. What is jitter? How to test and reduce internet jitter [Електронний ресурс]. – Режим доступу: https://www.ringcentral.com/us/en/blog/what-is-jitter/
7. Network Jitter - Common Causes and Best Solutions [Електронний ресурс]. – Режим доступу: https://www.ir.com/guides/what-is-network-jitter
8. What is Remote Network Monitoring? (RMON) [Електронний ресурс]. – Режим доступу: https://www.atera.com/blog/what-is-remote-network-monitoring-rmon/
9. What is Remote Network Monitoring?) [Електронний ресурс]. – Режим доступу: https://www.dpstele.com/blog/what-is-rmon.php
10. What is NetFlow [Електронний ресурс]. – Режим доступу: https://blog.gigamon.com/2018/01/08/what-is-netflow/
11. What is NetFlow [Електронний ресурс]. – Режим доступу: https://www.solarwinds.com/netflow-traffic-analyzer/use-cases/what-is-netflow
12. What is NetFlow [Електронний ресурс]. – Режим доступу: https://www.ibm.com/topics/netflow
13. Офіційний сайт Zabbix [Електронний ресурс]. - Режим доступу: https://www.zabbix.com.

14. A summary of Network Traffic monitoring and analysis techniques [Електронний ресурс] – Режим доступу до ресурсу: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html#refs

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Бакалаврська робота
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОВЕДЕННЯ МОНІТОРИНГУ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ ZABBIX »

Виконав: АЯЙІ Френсіс Одіжі, БСД-41

Керівник: Гайдур Галина Іванівна

2

Об'єкт дослідження – підвищення ефективності сучасних методів моніторингу на базі програмного забезпечення Zabbix

Предмет дослідження – методи та засоби моніторингу мереж та програмного забезпечення

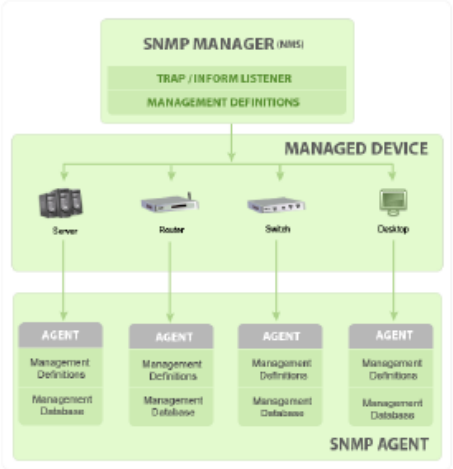
Мета роботи – є аналізі технологій, що пропонуються компанією Zabbix, яка дозволить ефективно відстежувати роботу мережевого обладнання та програмного забезпечення, виявляти та усувати неполадки та підвищувати продуктивність та безпеку корпоративних ресурсів.

Наукові завдання:

- визначити зміст проблеми побудови відмовостійких комп'ютерних мереж;
- дослідити існуючі підходи моніторингу мереж та сервісів організації;
- дослідити методи та засоби моніторингу на базі програмного забезпечення Zabbix;
- розробити алгоритм дій щодо моніторингу та швидкого реагування на інциденти в комп'ютерних мережах;
- розробити рекомендації щодо застосування методів та засобів моніторингу мереж та сервісів у мережі.

3

Аналіз змісту необхідності впровадження моніторингу корпоративних мереж



Моніторинг мережі повинен забезпечити:

- Повну візуалізацію IT та мережевої інфраструктури організації;
- Моніторинг, усунення несправностей і усунення проблем продуктивності мережі;
- Інструменти аналізу першопричини, коли виникають проблеми;
- Інформаційна панель із чіткими інструментами візуалізації та звітамиs;

Моніторинг мереж використовується для спостереження, аналізу та управління комп'ютерними мережами. Він відіграє важливу роль у забезпеченні надійності, безпеки та ефективності роботи.

- Виявлення та запобігання збоям
- Забезпечення безпеки мережі
- Оптимізація продуктивності
- Планування ємності
- Управління рівнем обслуговування (SLA)

4

Підходи до моніторингу інформаційних ресурсів організацій

Сервіси моніторингу дозволяють збирати різні данні за допомогою агентів:

- Мережеві пристрої
- Хмарні сервіси, контейнери, віртуальні машини
- Моніторинг операційних систем
- Лог-файли
- База даних
- Застосунки
- Сервіси
- IOT сенсори
- Моніторинг веб-сторінок
- Моніторинг кінцевих точок HTTP / HTTPS
- Підтримка всіх стандартних для галузі протоколів
- Збір даних з зовнішніх кінцевих точок API

Аналіз існуючих засобів моніторингу інформаційних ресурсів організацій

5

На сьогоднішній день існує безліч інструментів та програмних рішень для моніторингу інформаційних ресурсів організацій. Ось кілька популярних і широко використовуються серед них:

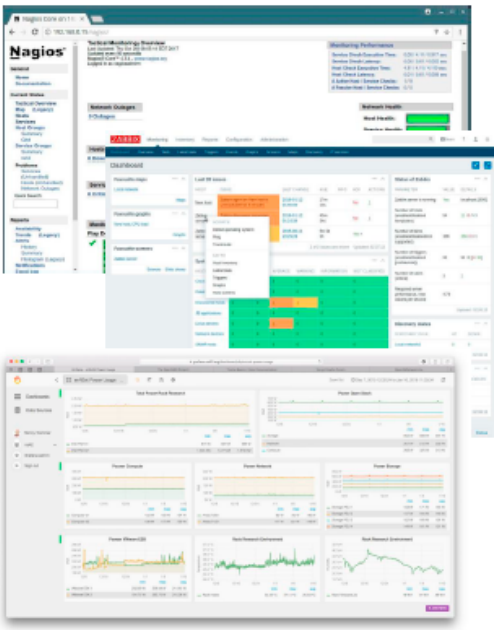
Nagios є одним з найбільш відомих та широко використовуваних інструментів моніторингу. Він надає можливості для моніторингу доступності, продуктивності та безпеки мережевих пристроїв, серверів, сервісів та програм.

ZZabbix є комплексною системою моніторингу, яка забезпечує спостереження за різними параметрами, включаючи продуктивність, доступність, події безпеки та використання ресурсів.

PRTG Network Monitor надає можливості для моніторингу мережевих пристроїв, серверів, програм, баз даних та інших ресурсів.

SolarWinds Network Performance Monitor надає моніторинг продуктивності мереж, пристроїв, програм та сервісів.

Splunk: Splunk є платформою для обробки та аналізу даних, яка може бути використана для моніторингу інформаційних ресурсів.



Чому саме Zabbix?

6

Zabbix налічує 24 роки роботи, є на сто відсотків відкритим з вихідним кодом і має понад 300 000 установок. Ця платформа добре відома в IT-спільноті.

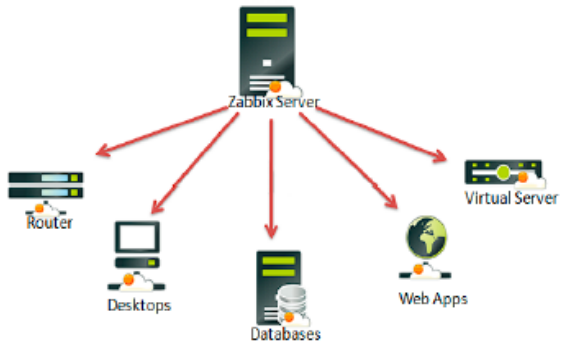
Форум Zabbix - гарне місце для того, щоб задавати питання, за вашою темою в безлічі місцевих спільнот на різних мовах, таких як українська або англійська.

- Масштабованість: Zabbix може бути масштабований залежно від розміру та складності мережі організації.
- Гнучкість налаштування: Zabbix пропонує широкі можливості налаштування та гнучкість у визначенні моніторингу різних типів ресурсів.
- Широкий спектр моніторингу: Zabbix підтримує моніторинг різних типів ресурсів, включаючи мережеве обладнання, сервери, програми, бази даних, віртуалізацію та інші.
- Оповіщення у реальному часі: Zabbix надає потужну систему оповіщень, яка дозволяє оперативно реагувати на проблеми та інциденти.
- Обширні аналітичні можливості: Zabbix надає засоби аналізу даних та створення звітів про продуктивність, доступність та використання ресурсів. Відкрите програмне забезпечення: Zabbix є програмним забезпеченням, що вільно розповсюджується, з відкритим вихідним кодом.

7

Призначення та можливості системи моніторингу Zabbix

Zabbix - це комплексна система моніторингу, яка призначена для нагляду і контролю за різноманітними ресурсами і об'єктами в інформаційних системах. Основні призначення Zabbix включають:



1.Моніторинг доступності: Zabbix дозволяє відстежувати доступність серверів, мережевих пристроїв, додатків та сервісів. Він періодично перевіряє ресурси і генерує оповіщення, якщо будь-який з них стає недоступним або працює некоректно.
2.Моніторинг продуктивності: За допомогою Zabbix можна вимірювати і аналізувати різні параметри продуктивності, такі як використання CPU, пам'яті, мережеву пропускну здатність, дискову активність тощо.
3.Моніторинг безпеки: Zabbix забезпечує виявлення потенційних загроз безпеці і контроль над безпековими подіями.
4.Моніторинг мережі: Zabbix може бути використаний для моніторингу мережевих пристроїв, таких як маршрутизатори, комутатори, firewall, а також мережеві сервіси.
5.Оповіщення і звіти: Zabbix має вбудовану систему оповіщень, яка дозволяє налаштовувати сповіщення про виявлені проблеми через різні канали, такі як електронна пошта, SMS, Slack тощо. Крім того, він надає можливість створення різноманітних звітів і графіків для аналізу даних моніторингу.

8

Zabbix Сервер

Zabbix Server - центральний компонент системи, який відповідає за збір, обробку і збереження даних моніторингу. Сервер Zabbix відстежує стан ресурсів, отримує дані від агентів, виконує правила моніторингу, генерує оповіщення та зберігає дані в базі даних.

Сервер Apache надає доступ до веб-інтерфейсу сервера Zabbix для отримання інформації.

База даних є ключовим елементом сервера Zabbix, можливо обрати MariaDB, MySQL і Postgresql.

9

Zabbix агент

Zabbix Agent - програмне забезпечення, яке встановлюється на кожному моніторингованому пристрої або сервері. Агент збирає дані про стан ресурсів, такі як CPU, пам'ять, диски, мережеві інтерфейси тощо, і передає їх на сервер Zabbix для подальшої обробки.

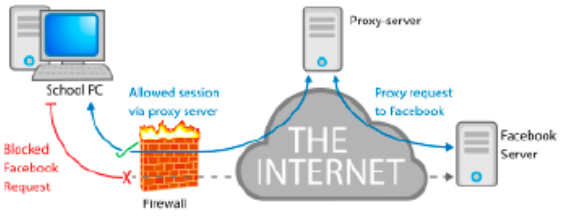
Існує 3 види агентів:

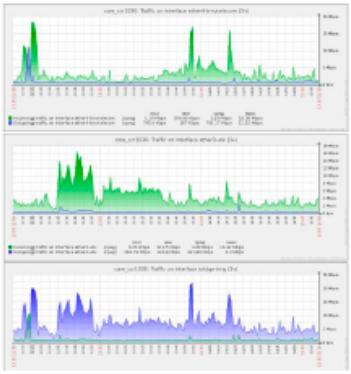
- Пасивний агент: прослуховує порт до тих пір, поки сервер не запитає дані і вже потім агент відправить їх
- Активний агент: він вирішує, коли і які дані відправляти
- Гібридний агент: відправляє активні дані в якості пасивного агента, використовуючи виняток, але піклуючись про те, щоб такого роду дані могли передаватися тільки по одному.

10

Додаткові можливості Zabbix

Proxy Servers - Proxy-сервери Zabbix є проміжними компонентами, які можуть використовуватися для розподіленого моніторингу. Вони дозволяють збирати дані моніторингу від різних місцезнаходжень і передавати їх на сервер Zabbix для централізованої обробки.





Шаблони (Templates) - Zabbix використовує шаблони для стандартизації правил моніторингу для певних типів ресурсів. Шаблони містять набори параметрів, які автоматично застосовуються до нових об'єктів моніторингу, що спрощує налаштування системи.

11

ВИСНОВКИ

В даній роботі було розглянуто питання моніторингу мереж в інформаційній системі. Моніторинг є важливим елементом забезпечення стабільності роботи мереж та підключених до них пристроїв, програм та систем. В процесі роботи було проаналізовано існуючі методи моніторингу та визначені їх переваги та недоліки. Було розглянуто важливі аспекти, такі як відстеження стану мережі, виявлення проблем, аналіз використання ресурсів та планування потреб у їх збільшенні.

В роботі коротко розглянуті протоколи SNMP, структура мережі Інтернет та основні протоколи маршрутизації. Також проведено порівняльний аналіз протоколів SNMP, ICMP і CDP, включаючи їх заголовки з детальним описом компонентів. Робота містить інформацію про формати додаткових заголовків, які можуть використовуватися протоколом SNMP. Крім того, проаналізовано основні характеристики протоколів моніторингу.

Отримані результати можуть бути корисними для тих, хто працює з мережами та хоче забезпечити їх стабільну та надійну роботу. Результати дослідження можуть бути використані для подальшого вдосконалення методів моніторингу та підвищення ефективності роботи мереж.

Дякую за увагу!
Доповідь закінчено