**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДВНЗ «КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА»**

**Навчально-науковий інститут «Інститут інформаційних технологій в економіці»**

**Кафедра комп’ютерної математики та інформаційної безпеки**

|  |
| --- |
| **ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМНИЙ АНАЛІЗ»**  **Галузь знань 12 «Інформаційні технології»** |
| **Спеціальність 124 «Системний аналіз»** |

Форма навчання: очна

*очна (денна), заочна, дистанційна*

**КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА**

на тему «

»

*(назва теми)*

здобувача Швиденко Дмитро Юрійович

*(прізвище, ім’я, по батькові) (підпис)*

Науковий керівник Колєчкіна Л. М., проф. кафедри сис. аналізу та кібербезпеки

*(науковий ступінь, учене звання, ПІБ)*

*(підпис)*

**Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)**

Завідувач кафедри: д.ф.-м.н., проф. Джалладова І.А.

*(підпис)*

**Київ 2023**

# **Зміст**

[**Зміст** 2](#_Toc137456486)

[**Вступ** 4](#_Toc137456487)

[Актуальність теми. 4](#_Toc137456488)

[Мета і завдання дослідження 4](#_Toc137456489)

[Об’єкт дослідження 4](#_Toc137456490)

[Предмет дослідження 4](#_Toc137456491)

[Методи дослідження 4](#_Toc137456492)

[**1. Інструменти які використані в роботі** 6](#_Toc137456493)

[**1.1 Zabbix, інструмент для системного аналізу** 6](#_Toc137456494)

[1.1.1 Історія та походження Zabbix 6](#_Toc137456495)

[1.1.2 Що таке Zabbix? 6](#_Toc137456496)

[1.1.3 Особливості Zabbix: 7](#_Toc137456497)

[1.1.4 Навіщо використовувати Zabbix? 7](#_Toc137456498)

[1.1.5 Переваги Zabbix 8](#_Toc137456499)

[1.1.6 Недоліки Zabbix 8](#_Toc137456500)

[1.1.7 Альтернативи систем аналізу Zabbix 8](#_Toc137456501)

[1.1.8 Підведення підсумків 8](#_Toc137456502)

[**1.2 Аналіз ефективності використання docker для системи Zabbix** 11](#_Toc137456503)

[1.2.1 Введення 11](#_Toc137456504)

[1.2.2 Докер 12](#_Toc137456505)

[1.2.3 Docker Inside 12](#_Toc137456506)

[1.2.4 Аналіз віртуальна машин проти Docker контейнерів 15](#_Toc137456507)

[1.2.5 Переваги Docker Container 18](#_Toc137456508)

[1.2.6 Недоліки Docker Container 19](#_Toc137456509)

[1.2.7 Продуктивність Docker 20](#_Toc137456510)

[1.2.8 Docker проти інших контейнерних технологій 22](#_Toc137456511)

[1.2.9 Вибір між ВМ та контейнерів 28](#_Toc137456512)

[1.2.10 Підведення підсумків 29](#_Toc137456513)

[**1.3 Віртуалізація серверів** 30](#_Toc137456514)

[1.3.1 Термінологія 30](#_Toc137456515)

[1.3.2 Огляд функцій 31](#_Toc137456516)

[1.3.3 Підведення підсумків 36](#_Toc137456517)

[**2. Підготовка для аналізу ефективності Zabbix** 37](#_Toc137456518)

[**2.1 Загальна архітектура для проведення аналізу** 37](#_Toc137456519)

[2.1.1 Сервер А 37](#_Toc137456520)

[2.1.2 Сервер Б 37](#_Toc137456521)

[2.1.3 Підведення підсумків 38](#_Toc137456522)

[**2.2 Конфігурація серверів** 38](#_Toc137456523)

[2.2.1 Конфігурація серверу А 38](#_Toc137456524)

[2.2.2 Конфігурація серверу Б 39](#_Toc137456525)

[2.2.3 Підведення підсумків 40](#_Toc137456526)

[**3. Аналіз ефективності Zabbix** 41](#_Toc137456527)

[**3.1 Початок роботи з zabbix** 41](#_Toc137456528)

[**3.2 Конфігурування zabbix** 42](#_Toc137456529)

[**3.3 Аналіз ефективності** 46](#_Toc137456530)

[3.3.1 Графіки 46](#_Toc137456531)

[3.3.2 Мапи 54](#_Toc137456532)

[3.3.3 Загальна інформація по кожному хосту 64](#_Toc137456533)

[3.3.4 Тригери 66](#_Toc137456534)

[**3.4 Підведення підсумків** 72](#_Toc137456535)

[**Джерела** 74](#_Toc137456536)

# **Вступ**

## Актуальність теми.

Дослідження інформаційних систем була не легка задача, але з часом з’являлось все більше і більше інструментів, які облегшують цей процес. Аналіз систем є для кожної компанії невід’ємною складовою, але у кожної компанії свої підходи та реалізація. Великий вибір інструментів аналізу систем на ринку може призвести до невизначеності, оскільки деякі з них можуть бути складні в розумінні та потребують багато часу на налаштування для першого аналізу.

## Мета і завдання дослідження

Дослідити ефективність використання інструменту для аналізу систем «Zabbix», з використанням докеру.

## Об’єкт дослідження

Два сервери, з яких буде збиратись дані моніторингу для аналізу систем за допомогою «Zabbix».

## Предмет дослідження

Аналітичний інструмент для дослідження та моніторингу систем «Zabbix», який повинен вхідні дані (напруги на сервер, напруги на мережу) аналізувати та вистроювати у вигляді графіків звіти.

## Методи дослідження

Після розгортання на серверах інструментів для аналізу систем, ми візуалізуймо звіти у вигляді веб-платформи. Всі звіти будуть відображатись на веб-сторінці. Вибір аналізу – це шаблони у Zabbix. На прикладі декількох шаблонів проаналізуємо ефективність інструменту.

# **1. Інструменти які використані в роботі**

## **1.1 Zabbix, інструмент для системного аналізу**

### 1.1.1 Історія та походження Zabbix

Zabbix був створений Олексієм Владишевим і зараз активно розвивається та підтримується Zabbix SIA. Zabbix — це рішення розподіленого моніторингу корпоративного рівня з відкритим кодом. Zabbix — це програмне забезпечення, яке контролює працездатність і цілісність багатьох параметрів мережі та серверів. Zabbix використовує гнучкий механізм сповіщень, який дозволяє користувачам налаштовувати сповіщення електронною поштою практично для будь-якої події. Це дозволяє швидко реагувати на проблеми сервера. Zabbix надає чудові функції звітності та візуалізації даних на основі архівних даних. Це робить Zabbix ідеальним для планування потужності.

### 1.1.2 Що таке Zabbix?

Zabbix визначається як інструмент моніторингу з відкритим кодом, який використовується для моніторингу серверів, мереж, ІТ-компонентів, хмарних служб і віртуальних машин. Інструмент моніторингу Zabbix використовується для забезпечення метрик моніторингу та відстеження використання мережі, споживання дискового простору та навантаження ЦП. Інструмент підтримує різні операційні системи, такі як Mac OS, Solaris, Linux та багато інших. Інструмент використовує окрему базу даних для зберігання даних і моніторингу програм. Інструмент моніторингу Zabbix розроблено мовою програмування C, а для веб-інтерфейсу використовується мова PHP.

### 1.1.3 Особливості Zabbix:

1. Візуалізація
2. Zabbix API
3. Повідомлення та виправлення
4. Легке розгортання
5. Безпека та аутентифікація
6. Метричний збірник
7. Виявлення проблеми
8. Розподілений моніторинг

### 1.1.4 Навіщо використовувати Zabbix?

1. Рішення з відкритим кодом
2. Дуже легке налаштування
3. Дуже проста конфігурація
4. Сервісне дерево високого рівня
5. Вбудована процедура прибирання
6. Високоефективні агенти для платформ на основі UNIX і WIN32
7. Низька крива навчання
8. Високий ROI. Простої дуже дорогі.
9. Низька вартість володіння
10. Централізована система моніторингу. Уся інформація (конфігурація, дані про продуктивність) зберігається в реляційній базі даних
11. Підтримка SNMP (v1,v2). І відлов, і опитування.
12. Можливості візуалізації

### 1.1.5 Переваги Zabbix

1. Гарний веб-інтерфейс.
2. Моніторинг як серверних, так і мережевих пристроїв.
3. Гнучкість у децентралізації користувачів.
4. Легко керувати та налаштовувати: уся конфігурація Zabbix здійснюється через веб-інтерфейс.
5. Підтримує Linux, Solaris, FreeBSD…
6. Довірена автентифікація користувача.
7. Повідомте про проблеми електронною поштою та SMS.

### 1.1.6 Недоліки Zabbix

1. Zabbix повинен містити Amazon RDS.
2. UI/UX має бути більш помітним і детальним.
3. Zabbix має надати більше шаблонів для повного моніторингу.

### 1.1.7 Альтернативи систем аналізу Zabbix

1. Datadog.
2. AppDynamics.
3. Dynatrace
4. LogicMonitor.
5. Монітор мережі PRTG.
6. checkmk.
7. Microsoft System Center.

### 1.1.8 Підведення підсумків

По-перше, Zabbix дозволяє системним аналітикам контролювати стан різних параметрів системи. Наприклад, Zabbix може моніторити навантаження на CPU, використання пам'яті, мережевий трафік, стан служб, апаратне забезпечення та інші важливі параметри. За допомогою цих даних аналітики можуть визначити, які процеси чи служби споживають надмірні ресурси та знайти причини перебоїв у роботі системи.

По-друге, Zabbix забезпечує зручний інтерфейс для відслідковування динаміки змін параметрів системи. Наприклад, аналітики можуть побачити, як змінюється завантаження CPU протягом дня чи тижня, що допоможе виявити регулярні навантаження та планувати їх заздалегідь. Крім того, Zabbix дозволяє налаштовувати сповіщення про відхилення від нормальних значень параметрів, що дозволяє оперативно реагувати на проблеми та запобігати серйозним наслідкам.

По-третє, Zabbix надає можливість аналізувати дані за допомогою різних інструментів. Наприклад, в Zabbix можна використовувати візуалізацію даних у вигляді графіків, діаграм чи таблиць, що допомагає аналітикам отримувати цілісну картину про стан системи. Крім того, Zabbix може збирати дані про системи з різних джерел та уніфікувати їх формат, що значно полегшує процес аналізу.

Загалом, Zabbix є потужним та ефективним інструментом для системного аналізу, оскільки він дозволяє системним аналітикам зосередитись на головних проблемах та виявити їх вчасно. Наприклад, якщо аналітик помічає, що середня відповідь на запити до бази даних значно збільшилась, він може відразу звернутись до логів та перевірити, що стало причиною такої затримки. Або якщо з'являються повідомлення про невдачі у роботі служби, аналітики можуть швидко визначити, яка саме служба відповідає за цю функціональність та виправити її недоліки.

Крім того, Zabbix є досить гнучким інструментом, що дозволяє налаштовувати моніторинг під конкретні потреби. Наприклад, аналітик може налаштувати моніторинг лише певних параметрів системи, які є найбільш важливими для його дослідження. Також Zabbix дозволяє налаштовувати сповіщення та повідомлення, які з'являться, коли відбудеться відхилення від нормальних значень параметрів. Це допомагає системним аналітикам оперативно реагувати на проблеми та вирішувати їх, не допускаючи серйозних наслідків.

Завдяки своїм можливостям та функціональності, Zabbix став одним з основних інструментів для моніторингу та аналізу комп'ютерних систем. Він дозволяє системним аналітикам ефективно та швидко виявляти проблеми, що допомагає збільшити продуктивність та стабільність системи.

Мета дипломної роботи, проаналізувати ефективність використання цього інструменту для системного аналізу.

## **1.2 Аналіз ефективності використання docker для системи Zabbix**

Docker надає деякі можливості, корисні для розробників і адміністраторів. Це відкрита платформа, яку можна використовувати для створення, розповсюдження та запуску додатків у портативному, легкому середовищі виконання та інструментів пакування, відомому як Docker Engine. Він також надає Docker Hub, який є хмарним сервісом для обміну програмами. Витрати можна зменшити, замінивши традиційну віртуальну машину докер-контейнером. Це чудово знижує витрати на перебудову платформи хмарної розробки.

### 1.2.1 Введення

Docker — це платформа з відкритим вихідним кодом, яка запускає програми та полегшує процес розробки та розповсюдження. Програми, вбудовані в докер, упаковані з усіма підтримуючими залежностями в стандартну форму,

яка називається контейнером. Ці контейнери продовжують працювати ізольовано поверх ядра операційної системи. Додатковий рівень абстракції може вплинути на продуктивність. Незважаючи на те, контейнерні технології існують уже понад 10 років, але докер, загалом нова надія, зараз є видатним серед найкращих інновацій, оскільки він супроводжує нові можливості, яких не мали попередні технології. Спочатку він дає можливість створювати та контролювати контейнери. Крім того, програми можуть бути легко упаковані розробником у легкі докер-контейнери. З цими віртуалізованими програмами можна легко працювати будь-де без будь-яких змін. Крім того, докер може передавати більше віртуальних ситуацій, ніж різні інновації, на одному обладнанні. Підсумовуючи, докер може легко координувати роботу зі сторонніми інструментами, які допомагають легко розгортати та керувати контейнерами докерів. Контейнери Docker можна легко розгорнути в хмарному середовищі. Ця дипломна робота є також оглядом технології докеру і аналізує її ефективність за допомогою систематичного огляду літератури.

### 1.2.2 Докер

Docker надає засоби для автоматизації програм, коли вони розгортаються в контейнерах. У середовищі, де програми віртуалізуються та виконуються, докер додає додатковий рівень механізму розгортання. Докер розроблений таким чином, щоб створити швидке та легке середовище, де можна ефективно запускати код, і, крім того, він надає додаткову можливість професійного робочого процесу для отримання коду з комп’ютера для тестування перед виробництвом. Докер дозволяє якомога швидше протестувати ваш код і розгорнути його у виробничому середовищі, а також докер надзвичайно простий. Звичайно, ви можете почати з докера з простою системою конфігурації, бінарного докера з ядром Linux.

### 1.2.3 Docker Inside

Існує чотири основні внутрішні компоненти Docker, включаючи Docker-клієнт і сервер, Docker-образи, Docker образи та Docker-контейнери. Ці компоненти будуть детально описані в наступних підрозділах.

Клієнт і сервер Docker

Docker можна пояснити як програму на основі клієнта та сервера, як показано на малюнку 3.2.1. Докер-сервер отримує запит від докер-клієнта, а потім обробляє його відповідним чином. Повний API RESTful (Representational

state transfer) і двійковий файл клієнта командного рядка постачається докером. Докер-демон/сервер і докер-клієнт можуть бути запущені на одній машині або локальний докерклієнт може бути підключений до віддаленого сервера або демона, який працює на іншій машині.

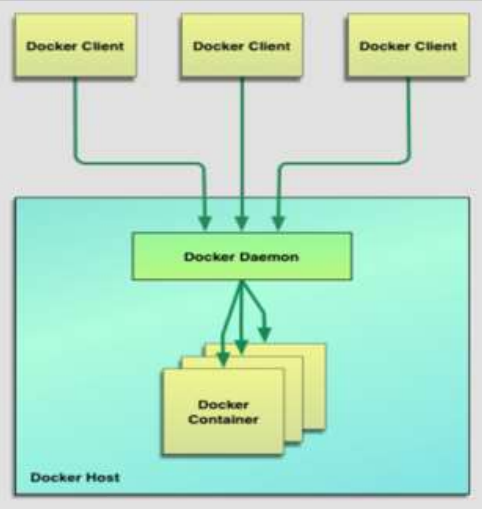


Рисунок 1.2.1 - Архітектура Docker

Docker образи

Існує два способи створення образу. Перший — створити зображення за допомогою шаблону, доступного лише для читання. Основою кожного образу є базове зображення. Образи операційної системи – це в основному базові

образи, наприклад Ubuntu 14.04 LTS або Fedora 20. Образи операційної системи створюють контейнер із можливістю повної запущеної ОС. Базове зображення також можна створити з нуля. Потрібні програми можна додати до базового образу, змінивши його, але необхідно створити новий образ. Процес створення нового створення образу називається «внесенням змін». Другий спосіб — створити докер-файл. Файл докерів містить список інструкцій, коли команда «Docker build» виконується з терміналу bash, вона

дотримується всіх інструкцій, наданих у файлі докерів, і створює образ. Це автоматизований спосіб побудови зображення.

Docker Registries

Образи докерів розміщуються в реєстрах докерів. Він працює відповідно до репозиторіїв вихідного коду, де зображення можна надсилати або витягувати з одного джерела. Існує два типи реєстрів: публічні та приватні. Docker Hub називається загальнодоступним реєстром, де кожен може завантажувати доступні зображення та надсилати власні, не створюючи зображення з нуля. Зображення можна поширювати в певну область (загальнодоступну чи приватну) за допомогою функції докер-хаба.

Контейнери Docker

Зображення докера створює контейнер докера. Контейнери містять весь набір, необхідний для програми, тому програму можна запускати ізольовано. Наприклад, припустимо, що є образ ОС Ubuntu із SQL SERVER, коли цей образ запускається за допомогою команди docker run, тоді буде створено контейнер з SQL сервером, який працюватиме в ОС Ubuntu.

### 1.2.4 Аналіз віртуальна машин проти Docker контейнерів

Віртуалізація — це стара концепція, яка використовувалася в хмарних обчисленнях після того, як IaaS було прийнято як вирішальний метод для створення системи, забезпечення ресурсами та багатокористування. Віртуалізовані ресурси відіграють основну роль у вирішенні проблем за допомогою основної техніки хмарних обчислень. На рисунку 1.2.2 показана архітектура віртуальної машини.

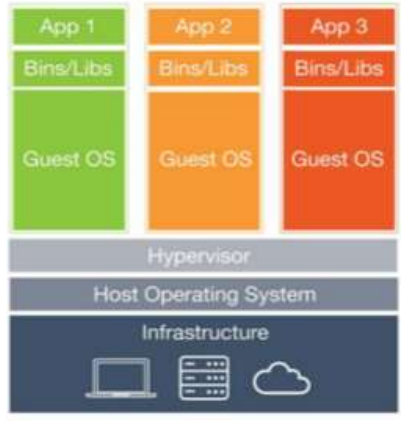


Рисунок 1.2.2 - Архітектура віртуальної машини

Гіпервізор лежить між хостовою та гостьовою операційними системами. Це віртуальна платформа, яка підтримує більше ніж одну операційну систему на сервері. Він працює між операційною системою та процесором. Віртуалізація ділить його на два сегменти: перший – паравіртуалізація, а другий – повна віртуалізація. На малюнку 1.2.3 зображено архітектуру Docker Container. Контейнерами Linux керує докер-інструмент, який використовується як метод віртуалізації на рівні операційної системи. На малюнку 1.2.3 показано, що в одному контрольному хості є багато контейнерів Linux, які є ізольованими. Такі ресурси, як мережа, пам’ять, процесор і блоковий ввід/вивід, виділяються ядром Linux, а також працює з контрольними групами без запуску машини віртуалізації.

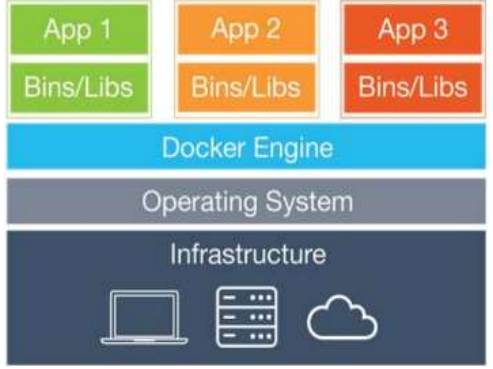


Рисунок 1.2.3 - Архітектура Docker Container

Відповідно до Waldspurger (2002), в контейнерах Linux архітектура має керувати центральним процесором і більш вміло розподіляти його ресурси. У будь-якому прикладі Hyper-V або VMWare через накладні витрати нелегко запустити більше десяти віртуальних машин. Значною мірою цю проблему вирішили контейнери. Контейнери використовують лише ті ресурси, які необхідні для служб або програм. Тому на слабко налаштованій машині можна виконати понад 50 запитів контейнерів. Наприклад, припустимо, що організація надає послуги безпеки електронної пошти. Основними функціями цих служб є перевірка електронної пошти на наявність вірусів, спаму та зловмисного програмного забезпечення. Крім того, вони можуть керувати пересиланням повідомлень до агента, журналів і звітів про збій доставки, якщо продукт встановлено в хмарі. Здебільшого в цих випадках не використовуються пов’язані залежності чи бібліотеки рівня ОС чи будь-які структури даних ядра. Тому варто контейнеризувати кожен компонент, помістивши їх у пісочницю за допомогою OpenVZ або Docker замість віртуальних машин. На багатьох підприємствах для тестування елементів використовуються віртуальні машини. У цьому процесі споживається багато ресурсів процесора та пам’яті. Тоді як контейнерна технологія дає гарантію своїм користувачам, що перевищення робочого навантаження не вплине на ефективність використання ресурсів. Контейнер займає менше часу для встановлення порівняно з віртуальними машинами, тому адаптивність контейнерів набагато вища, ніж віртуальних машин. Крім того, і Docker, і OpenVZ ретельно перевірялися з точки зору їхніх аспектів безпеки. Коли ізоляція знижується, це безпосередньо впливає на безпеку, яка також швидко знижується. Root користувачі Linux можуть легко отримати доступ до контейнерів, оскільки контейнери також використовують те саме ядро та операційну систему. Ізоляція докера не така сильна, як віртуальна машина, навіть якщо докер ізолює програму, яка працює в контейнері докерів, від основного хоста. Крім того, можливо, що деякі програми не зможуть працювати в контейнерній технології, і вони повинні працювати в іншій операційній системі.

### 1.2.5 Переваги Docker Container

За останні кілька років можна побачити попит і розвиток контейнерів Linux. Docker дуже швидко став популярним завдяки перевагам, які надає докер контейнер. Основними перевагами докера є швидкість, мобільність, масштабованість, швидка доставка та щільність.

Швидкість

Швидкість є однією з найбільш рекламованих переваг контейнерів. Коли висвітлюються переваги використання докерів, було б неймовірно не згадати про швидкість докерів у розмові (Chavis & Architect, 2015). Час, необхідний для створення контейнера, дуже швидкий, оскільки вони дійсно малі. Розробку, тестування та розгортання можна виконувати швидше, оскільки контейнери малі. Контейнери можуть бути відправлені на тестування після їх створення, а потім у виробниче середовище.

Портативність

Ті програми, які вбудовані в докер-контейнери, надзвичайно портативні. Ці портативні програми можна легко переміщати як єдиний елемент, а продуктивність залишається незмінною.

Масштабованість

Docker має можливість розгорнути його на кількох фізичних серверах, серверах даних і хмарних платформах. Його також можна запускати на будь-якій машині Linux. Контейнери можна легко перемістити з хмарного середовища на локальний хост, а звідти знову в хмару швидко. Регулювання можна легко зробити; шкала може бути просто налаштована користувачем відповідно до потреб.

Швидка доставка

Формат контейнерів Docker стандартизовано, тому програмістам не доводиться напружуватися над завданнями один одного. Відповідальністю адміністратора є розгортання та обслуговування сервера з контейнерами, тоді як відповідальністю програміста є догляд за програмами в контейнері докерів. Контейнери можуть працювати в будь якому середовищі, оскільки вони мають усі необхідні залежності, вбудовані в програми, і всі вони перевірені. Docker забезпечує надійне, послідовне та покращене середовище, тому результати можуть бути передбачуваними - досягається, коли коди переміщуються між системами розробки, тестування та виробництва (Chavis & Architect, 2015).

Щільність

Docker ефективніше використовує доступні ресурси, оскільки не використовує гіпервізор. Це є причиною того, що на одному хості можна запускати більше контейнерів порівняно з віртуальними машинами. Продуктивність Docker Containers вища через більшу щільність і відсутність накладних витрат ресурсів.

### 1.2.6 Недоліки Docker Container

* + Повна віртуалізація не забезпечується докером, оскільки вона залежить від ядра Linux, яке надається локальним хостом.
  + Наразі docker не працює на старих машинах. Він підтримує лише 64-розрядні локальні машини.
  + Повне віртуалізоване середовище має забезпечуватися контейнером докерів для машин Windows і Mac. Незважаючи на те, що boot2docker інструмент заповнює цю прогалину, але все ж слід перевірити, чи створює він перешкоди для прийняття користувачами цих систем, чи інтеграція та продуктивність з операційною системою хост-машини є адекватними.
  + Необхідно оцінити можливість проблем з безпекою. Створення довірчих двійкових файлів може бути простіше за допомогою цифрового підпису зображень докерів для майбутньої підтримки.
  + Важливо перевірити, чи викладацьке співтовариство чи науковий дослідник серйозно задумаються про прийняття докерів.

### 1.2.7 Продуктивність Docker

Microsoft використовували два сервери з однаковою конфігурацією в хмарному середовищі. Один сервер використовувався для докерів, а інший – для платформи Open Stack для KVM за допомогою інструменту віртуалізації. За словами Microsoft, ВМ працює самостійно. Цей фактор полегшує застосування та керування політикою мережі, безпеки, користувача та системи. Однак докер не містить гостьової операційної системи. Тому розповсюдження та збір зображень займає дуже мало часу. Час завантаження також дуже короткий. Це основні переваги використання Docker Cloud порівняно з VM Cloud. Scheepers (2014) порівнює технології віртуалізації LXC і Xen для порівняння деяких програм. Він пояснює, що Xen був би кращим вибором у сенсі рівномірного розподілу ресурсів, а продуктивність – ні. Однак LXC набагато кращий у сенсі отримання більшості апаратних ресурсів або для виконання менших ізольованих процесів. У приватних і точкових хмарах LXC є кращим варіантом. Microsoft оцінюють продуктивність трьох різних

середовищ: Native, Docker і KVM. Він уточнює, що контейнери та віртуальні машини є зрілими інноваціями, які отримали вигоду від останніх 10 років інкрементного обладнання та вдосконалення програм. Згідно з цим дослідженням, докер еквівалентний або перевершує виконання KVM для кожної ситуації, яку вони пробували. Їхні результати демонструють, що і KVM, і докер представляють несуттєві накладні витрати на процесор і пам’ять. Також було показано, що загальна продуктивність докера краща, ніж у локального хосту, оскільки програми виконувалися та відповідали швидше, ніж у локальному хості. Крім того, для виконання завдань у контейнері докерів використовувалося менше апаратних ресурсів. Docker — це дійсно вимоглива технологія майбутнього. Коли користувачі та розробники дізнаються більше про докер та його можливості, вони подумають про заміну традиційної віртуалізації на технологію докера. Docker надає багато простих і корисних функцій. Щоб отримати найкращу продуктивність і результати, настійно рекомендується змінити конфігурацію за замовчуванням. Контейнери забезпечують підвищену щільність, кращу продуктивність, масштабованість і зручність використання порівняно з традиційною віртуалізацією, оскільки контейнери розумно використовують свої ресурси, що зменшує ймовірність непотрібних накладних витрат. Контейнери кращі за продуктивністю, ніж віртуальні машини, оскільки контейнери потребують менше часу для запуску. Docker усунув найбільшу проблему «залежності». Тепер контейнери мають усі свої необхідні залежності, які допомагають належним чином створювати контейнери, і виконувати їх у будь-якому середовищі докерів. Додатковий шар ізоляції забезпечує контейнер, що підвищує безпеку контейнерів. Docker не такий небезпечний, як люди зазвичай думають, але він забезпечує повний захист.

### 1.2.8 Docker проти інших контейнерних технологій

У цьому розділі буде обговорено продуктивність віртуалізації програми та продуктивність контейнера докерів, а також буде порівняно та розглянуто оцінку інших технологій контейнеризації. В хмарі немає гостьової ОС докера, тому сховище та втрата ресурсів ЦП менші. Зображення не порушуються; час завантаження швидший, а час створення зображень короткий. Це переваги Docker Cloud порівняно з VM Cloud. Вони використовували два подібних сервера з однаковою конфігурацією в хмарному середовищі. Один сервер використовувався для докерів, а інший – для платформи Open Stack для KVM за допомогою засобу віртуалізації. В якості базової платформи використовувався Ubuntu Server. Щоб обчислити приблизний час завантаження, на кожному сервері було створено 20 зображень і перевірено час завантаження. На рисунку 1.2.4 показано, що час завантаження докера менший, ніж час завантаження KVM. Docker використовує хост-ОС, тоді як KVM використовує гостьову ОС. Таким чином, час завантаження докера коротший, ніж час завантаження KVM.

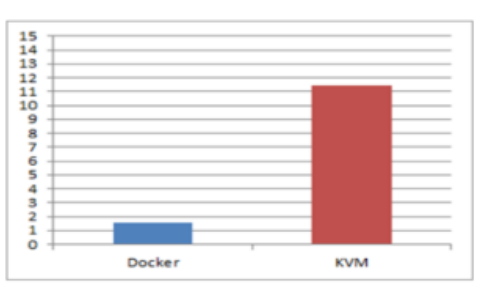


Рисунок 1.2.4 - Середній час завантаження Docker проти KVM

Для розрахунку оперативної швидкості використовувалася мова python. На малюнку 1.2.5 показано, що швидкість роботи 100 000 в середньому становить близько 4,5 с. Щоб виміряти швидкість роботи, вони отримують середній час процесу та стандартне відхилення, повторюючи той самий процес 100 разів на докері та віртуальній машині.

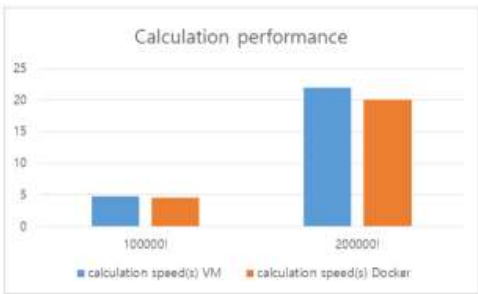


Рисунок 1.2.5 - Продуктивність обчислення ЦП

На рисунку 5 показано, що швидкість обчислення докера трохи вища, ніж швидкість обчислення ВМ. Висновок, що ВМ працює незалежно. Це одна з причин легкості застосування та керування політикою мережі, безпеки, користувача та системи. Однак докер не містить гостьової операційної системи. Таким чином, розповсюдження та збір зображень займає набагато менше часу. Його час завантаження також дуже короткий. Це основні переваги використання докер-хмари порівняно з VM Cloud. Технології віртуалізації LXC і Xen для порівняння деяких програм . Для цього використовує два сервери Core OS 324.3.0 і XenServer 6.2 з докером версії 0.11.1. Конфігурація цих систем — 4 ГБ оперативної пам’яті, чотириядерний процесор Intel Xeon і підтримка віртуалізації Intel VT-X. Базовою операційною системою є Ubuntu 12.04, і контейнери працюватимуть на обох машинах. 2 ГБ пам’яті виділено для першої віртуальної машини та Apache 2.2, WordPress 3.9 і PHP 5.3. Це було використано як сервер додатків. 1 ГБ пам’яті використовується другою віртуальною машиною з базою даних MYSQL 5.5. Ця база даних була заповнена зразком вмісту WordPress. Ця машина використовувалася як сервер бази даних. JMeter використовувався як інструмент тестування. На малюнку 1.2.6 показано, що під час виконання запиту SELECT у LXC спостерігалося менше накладних витрат порівняно з Xen. Основна увага під час виконання цього процесу порівняння полягає в тому, щоб побачити використання процесора та продуктивність швидкості мережі, оскільки це основні ресурси, що споживаються в цьому тесті.

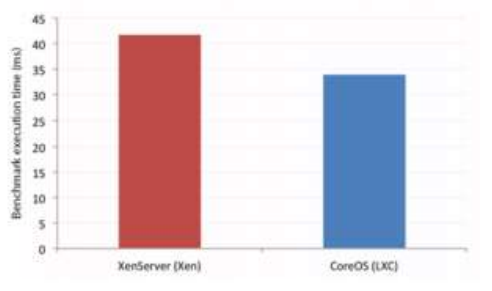


Рисунок 1.2.6 - Час у мілісекундах для виконання одного запиту на вибірку SQL

На малюнку 1.2.7 показано, що в налаштуваннях Xen виконання запиту INSERT у базі даних займало 16 секунд, тоді як у налаштуваннях LXC це займало більше часу — близько 335 секунд. Це показує нездатність контейнера LXC ефективно ізолювати ресурси.

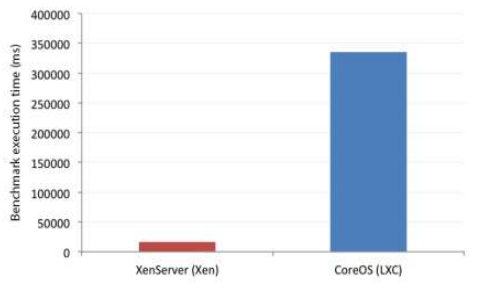


Рисунок 1.2.7 - Час у мілісекундах для виконання 10 000 запитів SQL INSERT

Висновок, що Xen був би кращим вибором у сенсі рівномірного розподілу ресурсів, продуктивність не залежить від інших завдань і виконується на одній машині. Однак LXC набагато кращий у сенсі використання більшості апаратних ресурсів або виконання менших ізольованих процесів. У приватних і точкових хмарах LXC є кращим варіантом. Оцінка продуктивність трьох різних середовищ: Native, Docker і KVM. Проблеми накладних витрат також висвітлюються в дослідженні. Були досліджені сценарії, коли більше одного апаратного ресурсу було використано повністю. Для проведення тестів використовувався сервер IBM x3650 M4, 16-ядерний процесор Xeon E5-2665, два Intel Sandy Bridge-EP 2,4 - 3,0 ГГц і 256 ГБ оперативної пам'яті. Щоб зробити нерівномірний доступ до пам'яті, два процесори були з'єднані між собою за допомогою зв'язку QPI. Хмарні провайдери також використовують подібний сервер. Базовою операційною системою були Ubuntu 13.10, докер версії 1.0, ядро Linux 3.11.0, libvirt версії 1.1.1 і QEMU 1.5.0. Цей малюнок 1.2.8 показує, що середній розмір 1 Мбайт використовувався для введення-виведення, трохи більше 60 секунд, вимірюючи продуктивність послідовного читання та запису. В цьому випадку, Докер і KVM можуть помітити невеликі витрати. В інших випадках KVM має майже чотириразову різницю в продуктивності.

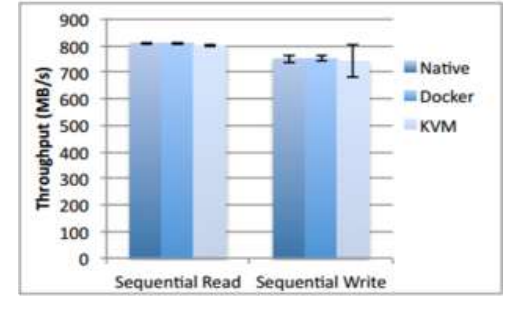


Рисунок 1.2.8 - Пропускна здатність послідовного вводу-виводу (МБ/с)

На малюнку 1.2.9 показано виконання нерегулярних робочих навантажень читання, запису та змішаних навантажень із використанням розміру квадрата 4 Кбайт і одночасності 128, що, як ми попередньо вирішили, забезпечує найкраще виконання для цього конкретного SSD. Як і слід було очікувати, докер не використовує накладних витрат, на відміну від Linux, однак KVM передає однакову кількість IOPS, оскільки кожна операція вводу-виводу повинна мати QEMU. Незважаючи на те, що максимальна продуктивність віртуальної машини залишається дуже високою, вона використовує більше циклів ЦП на операцію вводу-виводу, залишаючи менше ЦП доступним для роботи програми.

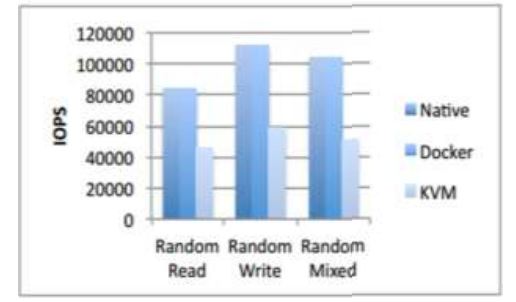


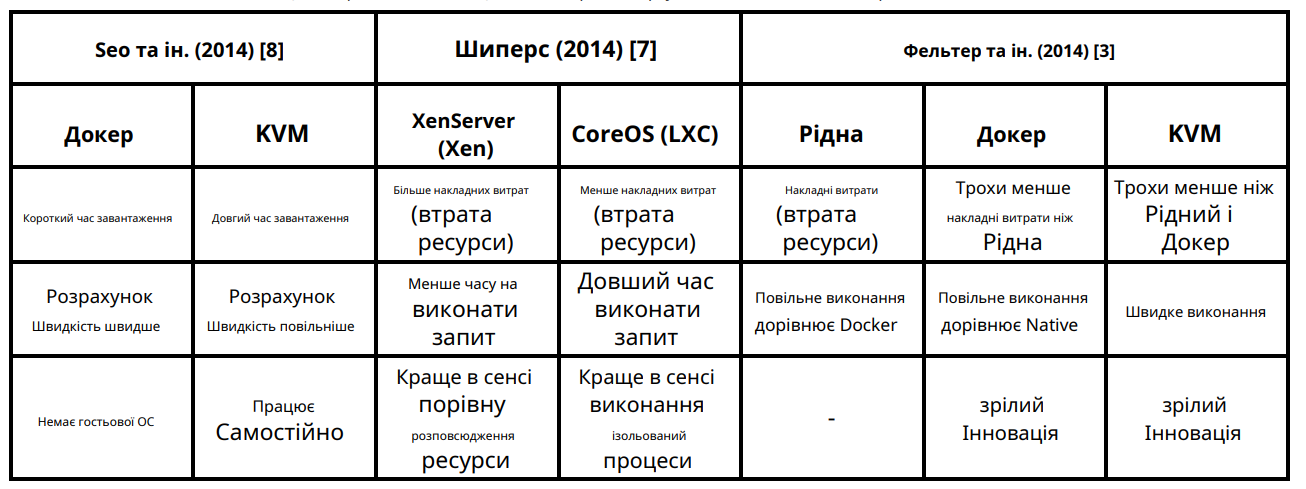
Рисунок 1.2.9 - Пропускна здатність послідовного вводу-виводу

Висновок, що контейнери та віртуальні машини є зрілими інноваціями, які отримали вигоду від інкрементального обладнання та вдосконалення програмування за останні 10 років. Коли все сказано та зроблено, докер еквівалентний або перевершує виконання KVM для кожної ситуації, яку ми пробували. Наші результати демонструють, що як KVM, так і докер представляють нерелевантні накладні витрати на виконання процесора та пам’яті. Підсумовуючи ці минулі роботи, незалежно від використання відмінних методів і наявності різноманітних центрів, одна загальна річ – вимірювання та порівняння продуктивності додатків і різних типів контейнерних і віртуалізованих технологій.

### 1.2.9 Вибір між ВМ та контейнерів

Таблиця 1.2.1 порівнює особливості різних контейнерних технологій і технологій віртуальних машин. Віртуальна машина використовує додатковий рівень між головною операційною системою та гостьовою операційною системою. Цей рівень відомий як гіпервізор. Тоді як Docker додає додатковий рівень між головними операційними системами та місцем віртуалізації та виконання додатків, який відомий як Docker Engine. Оскільки докер не використовує жодної гостьової операційної системи, це робить велику різницю в продуктивності між контейнером докерів і технологією віртуальної машини. У таблиці 1.2.1 також коротко порівнюється продуктивність програм, що працюють у різних контейнерах і віртуальних машинах. Як наведено в таблиці вище, згідно з цим продуктивність докера краща, ніж KVM, з точки зору часу завантаження та швидкості обчислень.

Таблиця 1.2.1 - Порівняльна таблиця на основі різних віртуальних машин і контейнерної технології



### 1.2.10 Підведення підсумків

Docker автоматизує програми, коли вони контейнеризовані. До основної операційної системи додається додатковий рівень механізму докерів. Докер працює швидше, ніж віртуальні машини, оскільки він не має гостьової операційної системи та менше накладних ресурсів. Тому для використання сервісу Zabbix ми використаємо контейнерну технологію.

## **1.3 Віртуалізація серверів**

Оскільки для дослідження ефективності використання аналізу систем Zabbix нам потрібні два сервери, скористуємось інструментами віртуалізації. Для цього був обраний інструмент – oracle virtual box. Розглянемо детально, що нам може запропонувати цей інструмент.

### 1.3.1 Термінологія

Коли ви маєте справу з віртуалізацією, а також для розуміння наступних розділів дослідження, це допоможе ознайомитися з деякою важливою термінологією, особливо з такими термінами:

* Головна операційна система (хост-ОС). Це ОС фізичного комп’ютера, на якому встановлено Oracle VM VirtualBox. Існують версії Oracle VM VirtualBox для хостів Windows, macOS, Linux і Oracle Solaris.
* Гостьова операційна система (гостьова ОС). Це ОС, яка працює всередині віртуальної машини. Теоретично Oracle VM VirtualBox може запускати будь-яку ОС x86, наприклад DOS, Windows, OS/2, FreeBSD і OpenBSD. Але щоб досягти майже рідної продуктивності гостьового коду на вашій машині, нам довелося пройти через багато оптимізацій, які характерні для певних ОС. Таким чином, хоча ваша улюблена ОС може працювати як гостьовий режим, ми офіційно підтримуємо та оптимізуємо для кількох вибраних, які включають найпоширеніші ОС.
* Віртуальна машина (ВМ). Це спеціальне середовище, яке Oracle VM VirtualBox створює для вашої гостьової ОС під час її роботи. Іншими словами, ви запускаєте гостьову ОС у віртуальній машині. Зазвичай віртуальна машина відображається у вигляді вікна на робочому столі комп’ютера. Залежно від того, який із різних інтерфейсів Oracle VM VirtualBox ви використовуєте, віртуальна машина може відображатися в повноекранному режимі або віддалено на іншому комп’ютері.

Всередині Oracle VM VirtualBox розглядає віртуальну машину як набір параметрів, які визначають її поведінку. Деякі параметри описують налаштування апаратного забезпечення, наприклад обсяг пам’яті та кількість призначених ЦП. Інші параметри описують інформацію про стан, наприклад, чи працює віртуальна машина чи збережена.

Ви можете переглянути ці параметри віртуальної машини в VirtualBox Manager у вікні налаштувань і за допомогою команди VBoxManage

* Гостьові доповнення. Це стосується спеціальних пакетів програмного забезпечення, які постачаються з Oracle VM VirtualBox, але призначені для встановлення всередині віртуальної машини для покращення продуктивності гостьової ОС і додавання додаткових функцій.

### 1.3.2 Огляд функцій

Нижче наведено короткий опис основних функцій Oracle VM VirtualBox:

1. Портативність. Oracle VM VirtualBox працює на великій кількості 64-розрядних операційних систем.

Oracle VM VirtualBox — це так званий розміщений гіпервізор, який іноді називають гіпервізором типу 2. У той час як залізо комп’ютеру або гіпервізор типу 1 працює безпосередньо на апаратному забезпеченні, Oracle VM VirtualBox вимагає встановлення наявної ОС. Таким чином, він може працювати разом із існуючими програмами на цьому хості.

Oracle VM VirtualBox значною мірою функціонально ідентичний на всіх хост-платформах, і використовуються однакові формати файлів і зображень. Це дає змогу запускати віртуальні машини, створені на одному хості, на іншому хості з іншою хост-ОС. Наприклад, ви можете створити віртуальну машину в Windows, а потім запустити її в Linux.

Крім того, віртуальні машини можна легко імпортувати та експортувати за допомогою відкритого формату віртуалізації (OVF), галузевого стандарту, створеного для цієї мети. Ви навіть можете імпортувати файли OVF, створені за допомогою іншого програмного забезпечення віртуалізації.

Для користувачів Oracle Cloud Infrastructure функціональні можливості поширюються на експорт та імпорт віртуальних машин до та з хмари. Це спрощує розробку додатків і розгортання у виробничому середовищі.

1. Гостьові доповнення: спільні папки, 3D-віртуалізація. Гостьові додатки Oracle VM VirtualBox — це пакети програмного забезпечення, які можна інсталювати всередині підтримуваних гостьових систем, щоб покращити їхню продуктивність і забезпечити додаткову інтеграцію та зв’язок із хост-системою. Після встановлення гостьових доповнень віртуальна машина підтримуватиме автоматичне налаштування роздільної здатності відео, безшовні вікна, прискорену 3D-графіку тощо.

Зокрема, гостьові додатки забезпечують спільні папки , які дають вам доступ до файлів у системі хоста з гостьової машини.

1. Комплексна апаратна підтримка. Серед інших функцій Oracle VM VirtualBox підтримує наступне:
   * Гостьова багатопроцесорна обробка (SMP). Oracle VM VirtualBox може представити до 32 віртуальних процесорів для кожної віртуальної машини, незалежно від того, скільки ядер ЦП фізично присутні на вашому хості.
   * Підтримка USB-пристроїв. Oracle VM VirtualBox реалізує віртуальний USB-контролер і дає змогу підключати довільні USB-пристрої до віртуальних машин без необхідності встановлення драйверів для окремих пристроїв на хості. Підтримка USB не обмежується певними категоріями пристроїв.
   * Апаратна сумісність. Oracle VM VirtualBox віртуалізує величезну кількість віртуальних пристроїв, серед яких багато пристроїв, які зазвичай надаються іншими платформами віртуалізації. Це включає в себе контролери жорстких дисків IDE, SCSI та SATA, кілька віртуальних мережевих карт і звукових карт, віртуальні послідовні та паралельні порти та вдосконалений програмований контролер переривань вводу/виводу (I/O APIC), який є в багатьох комп’ютерних системах. Це дозволяє легко клонувати образи дисків із реальних машин та імпортувати віртуальні машини сторонніх розробників у Oracle VM VirtualBox.
   * Повна підтримка ACPI. Інтерфейс розширеної конфігурації та живлення (ACPI) повністю підтримується Oracle VM VirtualBox. Це дозволяє легко клонувати образи дисків із реальних машин або віртуальних машин сторонніх розробників у Oracle VM VirtualBox. Завдяки унікальній підтримці статусу живлення ACPI Oracle VM VirtualBox може навіть повідомляти гостьовим ОС із підтримкою ACPI статус живлення хоста. Для мобільних систем, що працюють від акумулятора, гість може таким чином увімкнути енергозбереження та повідомити користувача про залишок заряду, наприклад, у повноекранних режимах.
   * Багатоекранна роздільна здатність. Віртуальні машини Oracle VM VirtualBox підтримують роздільну здатність екрана, яка у багато разів перевищує роздільну здатність фізичного екрана, що дозволяє розподіляти їх на великій кількості екранів, підключених до хост-системи.
   * Вбудована підтримка iSCSI. Ця унікальна функція дає змогу підключати віртуальну машину безпосередньо до сервера зберігання iSCSI без використання хост-системи. Віртуальна машина отримує прямий доступ до цілі iSCSI без додаткових витрат, необхідних для віртуалізації жорстких дисків у файлах-контейнерах.
   * Завантаження мережі PXE. Вбудовані віртуальні мережеві карти Oracle VM VirtualBox повністю підтримують віддалене завантаження за допомогою Preboot Execution Environment (PXE).
2. Багатогенераційні розгалужені знімки. Oracle VM VirtualBox може зберігати довільні знімки стану віртуальної машини. Ви можете повернутися в минуле та повернути віртуальну машину до будь-якого такого знімка та запустити звідти альтернативну конфігурацію віртуальної машини, фактично створивши ціле дерево знімків. Ви можете створювати та видаляти знімки під час роботи віртуальної машини.
3. Групи ВМ. Oracle VM VirtualBox надає групову функцію, яка дозволяє користувачеві організовувати та контролювати віртуальні машини як колективно, так і окремо. Окрім основних груп, будь-яка віртуальна машина також може входити до кількох груп, а також для груп, вкладених у ієрархію. Це означає, що ви можете мати групи груп. Загалом операції, які можна виконувати над групами, такі ж, як і ті, які можна застосовувати до окремих віртуальних машин: запуск, призупинення, скидання, закриття (збереження стану, надсилання вимкнення, вимкнення), скасування збереженого стану, відображення у файловій системі, Сортувати.
4. Чиста архітектура та безпрецедентна модульність. Oracle VM VirtualBox має надзвичайно модульну конструкцію з чітко визначеними внутрішніми інтерфейсами програмування та чітким розділенням коду клієнта та сервера. Це дозволяє легко керувати нею з кількох інтерфейсів одночасно. Наприклад, ви можете запустити віртуальну машину, просто натиснувши кнопку в графічному інтерфейсі користувача Oracle VM VirtualBox, а потім керувати цією машиною з командного рядка або навіть віддалено. Дивіться Розділ 1.18, «Альтернативні інтерфейси» .

Завдяки своїй модульній архітектурі Oracle VM VirtualBox також може розкрити свою повну функціональність і конфігурацію за допомогою комплексного набору для розробки програмного забезпечення (SDK), який забезпечує інтеграцію Oracle VM VirtualBox з іншими програмними системами.

1. Віддалений дисплей машини. Розширення віддаленого робочого столу VirtualBox (VRDE) забезпечує високопродуктивний віддалений доступ до будь-якої запущеної віртуальної машини. Це розширення підтримує протокол віддаленого робочого стола (RDP), спочатку вбудований у Microsoft Windows, зі спеціальними доповненнями для повної підтримки клієнтського USB.

VRDE не покладається на сервер RDP, вбудований у Microsoft Windows. Натомість VRDE підключається безпосередньо до рівня віртуалізації. Як результат, він працює з гостьовими ОС, відмінними від Windows, навіть у текстовому режимі, і також не потребує підтримки програм у віртуальній машині. VRDE детально описано в розділі 7.1 «Віддалений дисплей (підтримка VRDP)» .

Окрім цієї спеціальної можливості, Oracle VM VirtualBox пропонує вам більше унікальних функцій:

* + Розширювана автентифікація RDP. Oracle VM VirtualBox уже підтримує Winlogon у Windows і PAM у Linux для автентифікації RDP. Крім того, він містить простий у використанні SDK, який дозволяє створювати довільні інтерфейси для інших методів автентифікації.
  + USB через RDP. Використовуючи підтримку віртуального каналу RDP, Oracle VM VirtualBox також дозволяє локально підключати довільні USB-пристрої до віртуальної машини, яка працює віддалено на RDP-сервері Oracle VM VirtualBox.

### 1.3.3 Підведення підсумків

Проаналізовані можливості роботи інструменту віртуалізації VM VirtualBox. Це інструмент який повністю дозволить використовувати віртуальні машини як реальні сервера, які нам знадобляться для аналізу ефективності аналізу систем Zabbix. В них ми будемо створювати докер зображення, які зменшать затрати ресурсів “реального серверу”.

# **2. Підготовка для аналізу ефективності Zabbix**

## **2.1 Загальна архітектура для проведення аналізу**

Для проведення аналізу ефективності Zabbix знадобиться 2 сервер. Для розуміння на якому сервері будуть використані інструменти, дамо їм назву.

### 2.1.1 Сервер А

Це основний сервер, на якому буде встановлений докер контейнер з інструментом для системного аналізу – Zabbix server. Також щоб зберігати дані звітів, Zabbix потребує сконфігуроване зображення з PostgresSQL. Щоб візуалізувати дані знадобиться веб сервер – апачі або nginx, для цілей аналізу обрано Nginx web server, який буде також в докер контейнері. Щоб збирати метрики з системи знадобиться ще Zabbix агент.

### 2.1.2 Сервер Б

Це ще один сервер, в тій же локальній мережі, як і сервер А. На ньому в докер контейнері буде піднятий тільки Zabbix агент, який також буде збирати метрики з нього. ОС серверу – це ubuntu 22.04 server.

На рисунку 2.1.1 ілюстрована загальна архітектура, яка потрібна для тестування ефективності zabbix. ОС серверу – це ubuntu 22.04 server.

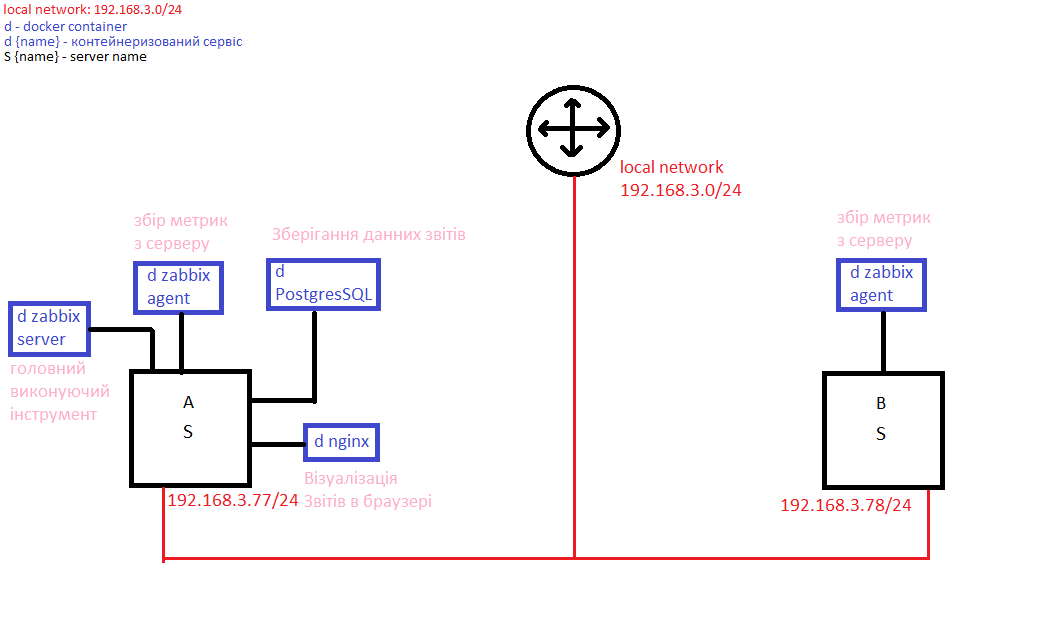


Рисунок 2.1.1 - загальна архітектура

### 2.1.3 Підведення підсумків

В цьому розділі ми проаналізували що нам знадобиться для дослідження

## **2.2 Конфігурація серверів**

### 2.2.1 Конфігурація серверу А

Після інсталяції ОС, необхідно для конфігурації створити скрипт, який необхідний для встановлення контейнерів забігс серверу, забігс агенту, PostgresSQL та Nginx.

Оскільки конфігурація не є частиною дослідження, тому все зроблено автоматизованим скриптом, який при виконані всі необхідні докер-контейнери піднімає і запускає.

Необхідно зайти на сервер, через FileZila або іншими можливостями зайти на сервер та перекинути 2 файли конфігурації: serverA-config.sh та docker-compose-serverA.yaml.

Зайдемо на сервер та виконаємо скрипт через bash, як на малюнку 2.2.1.

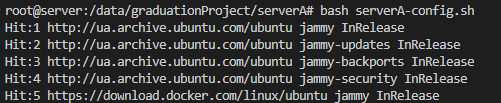


Рисунок 2.2.1 - процес виконання скрипту

Далі перевіримо, що наші контейнери сконфігуровані, командою: docker ps -a, як на малюнку 2.2.2

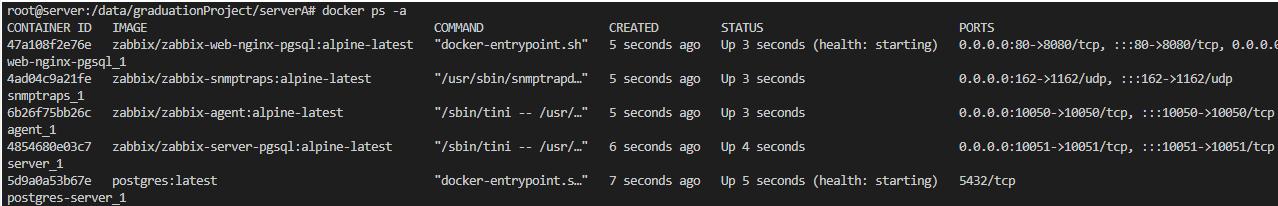


Рисунок 2.2.2 – список контейнерів на сервері А

Бачимо, що в строчці статусу «Up» - це свідчить про те, що контейнери піднялись та готови для роботи. На цьому конфігурація серверу А завершена.

### 2.2.2 Конфігурація серверу Б

На сервері Б для аналізу нам потрібен тільки контейнер з забігс агентом, який буде збирати метрики з серверу.

Необхідно зайти на сервер, через FileZila або іншими можливостями зайти на сервер та перекинути 2 файли конфігурації: serverB-config.sh та docker-compose-serverB.yaml.

Результати виконання скрипту подивимось на малюнку 2.2.3.



Рисунок 2.2.3 - процес виконання скрипту

Перевіримо, що контейнер з агентом піднятий, через команду docker ps, як на малюнку 2.2.4.



Рисунок 2.2.4 - список контейнерів на сервері Б

### 2.2.3 Підведення підсумків

Сервери налаштовані та всі інструменти інстальовані, далі ми можемо досліджувати ефективність використання Zabbix для системного аналізу.

# **3. Аналіз ефективності Zabbix**

## **3.1 Початок роботи з zabbix**

З попереднього розділу описана конфігурація серверу А, на якому лежить Веб сервер – nginx. Nginx слугує для візуалізації забігс серверу. Оскільки сервер А в локальній мережі має адресу 192.168.3.77, зайдемо на веб сторінку Zabbix серверу, на 80 порт - це стандартний http порт.

Коли ми зайдемо по адресі 192.168.3.77:80, ми попадаємо на сторінку логіну в забігс сервер, як на малюнку 3.1.1.

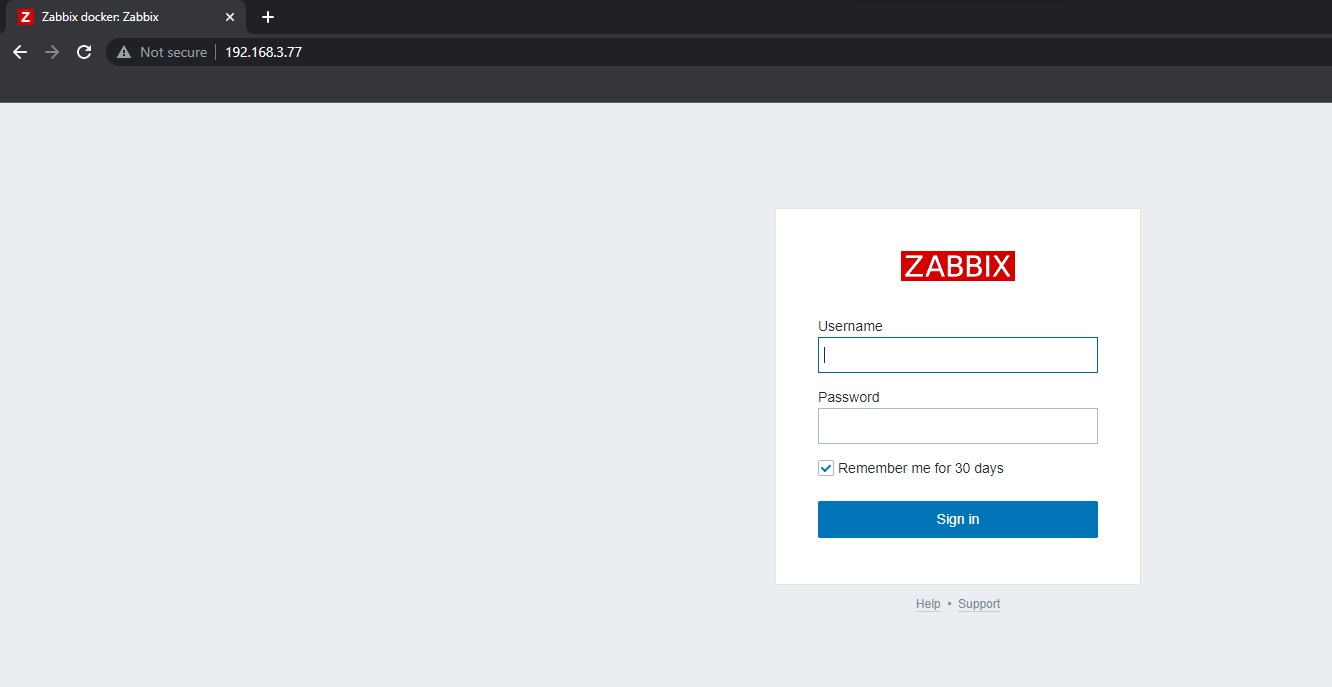


Рисунок 3.1.1 – сторінка логіну Zabbix серверу

Стандартний логін Admin, а пароль zabbix, далі перходимо на головну сторінку, яка стандартно сконфігурована через докер-забігс-сервер, ми можемо бачити головний екран, як на малюнку 3.1.2.

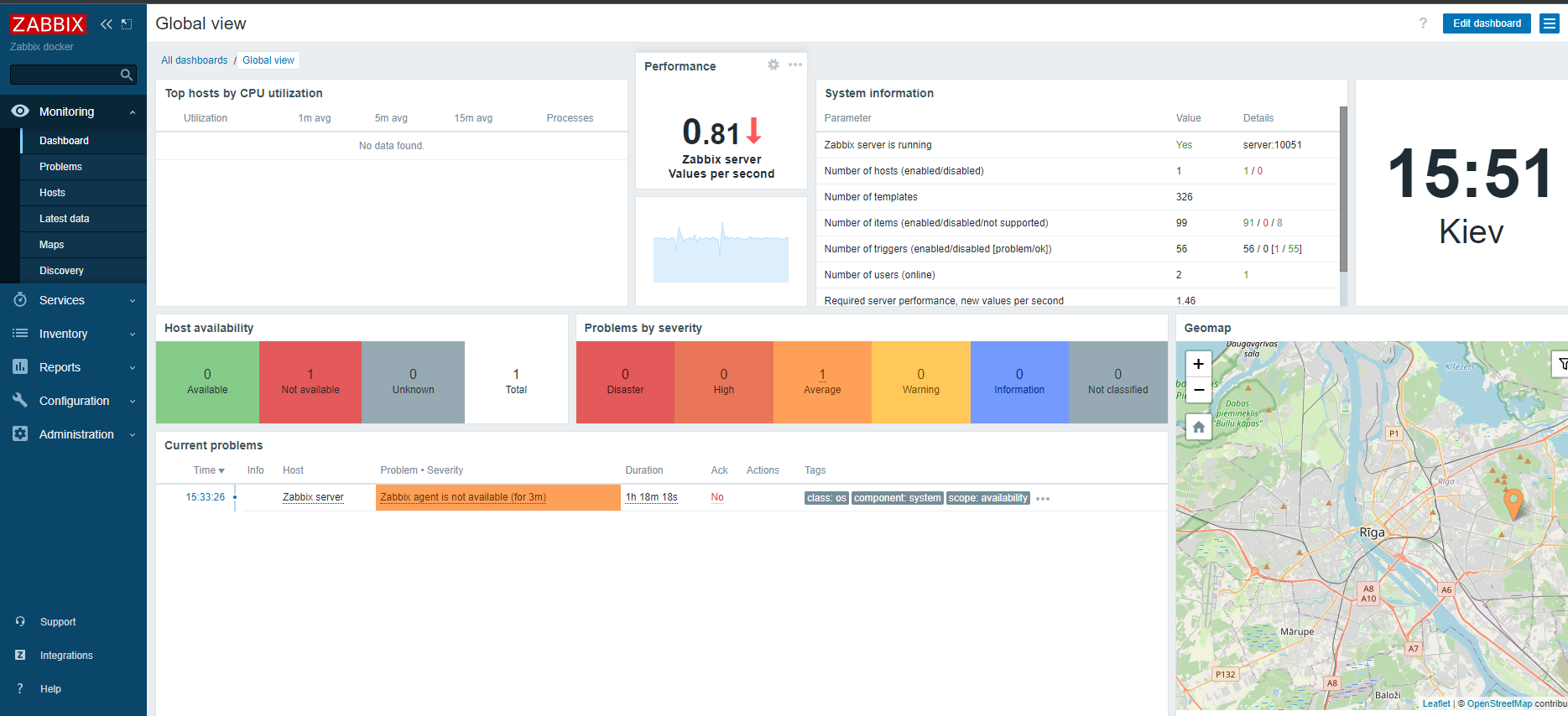


Рисунок 3.1.2 – головна сторніка Zabbix серверу

## **3.2 Конфігурування zabbix**

Щоб zabbix почав аналізувати хости, потрібно для початку перейти до вкладки «Configuration» і обрати підменю «Hosts», далі ми побачимо список хостів, які присутні в сервері. Малюнок 3.2.1 показує, як виглядає лист хостів в забігс сервері.

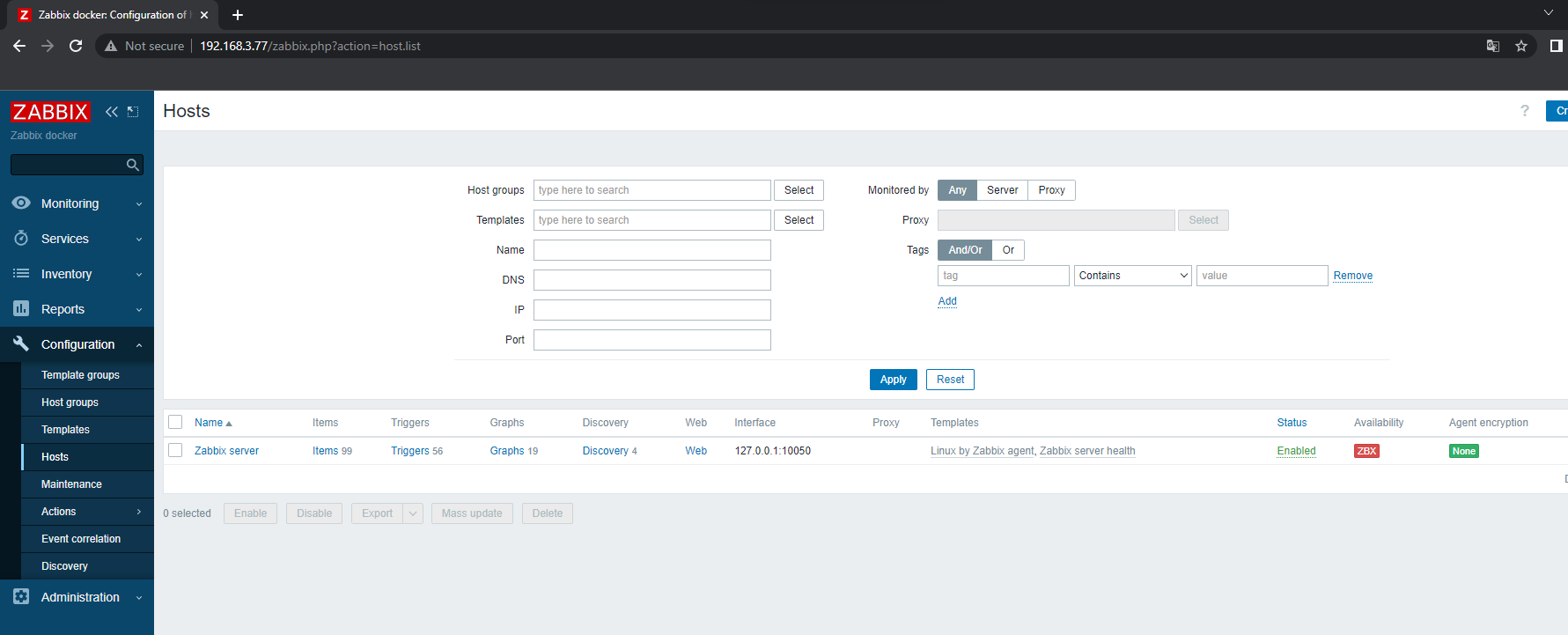


Рисунок 3.2.1 – сторінка хостів для аналізу Zabbix

Ми можемо побачити, що красним кольором виділена доступність серверу. Оскільки забігс сервер за замовчуванням шукає метрики з основного хоста-клієнту, а не контейнерезованного клієнту, потрібно його переконфігурувати.

Переходимо до конфігурації, необхідно обрати поки що єдиний сервер, як на малюнку 3.2.2.

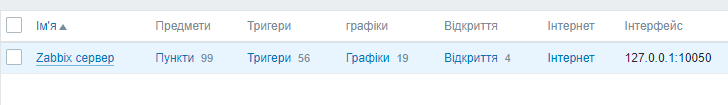


Рисунок 3.2.2 – вибраний основний забігс сервер

Далі ми попадаємо в сторінку конфігурацій хосту, де нам потрібно редагувати конфігурацію хосту. Стандартну конфігурацію можемо бачити на малюнку 3.2.3.

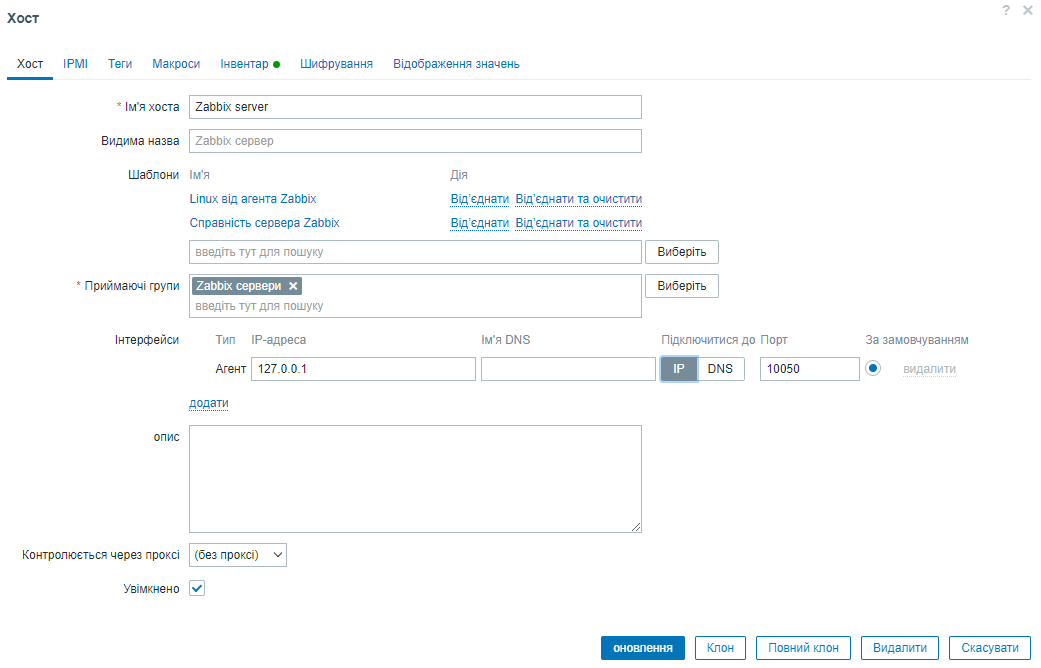


Рисунок 3.2.3 – стандартна конфігурація клієнту забігс серверу

Необхідно замінти на DNS ім’я, яке зазначене в docker-compose файлі, та зберегти конфігурацію. Зміни які вносились, можете побачити на малюнку 3.2.4.

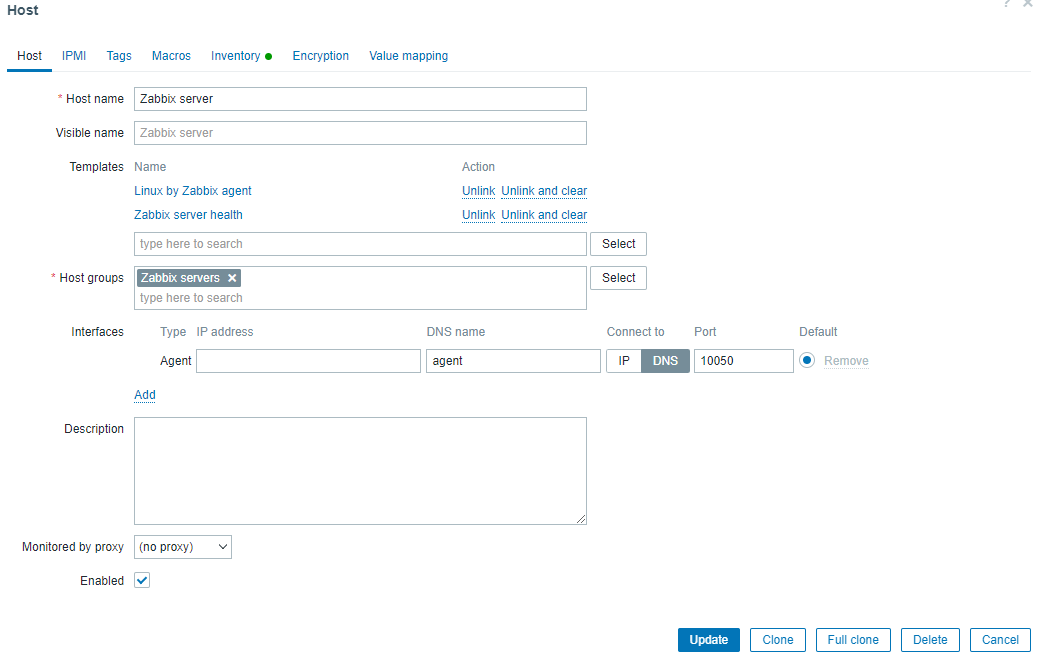


Рисунок 3.2.4 – змінена конфігурація клієнту забігс серверу

Після натискання «Update», зверху буде повідомлення про те, що конфігурація оновлена, як на малюнку 3.2.5.

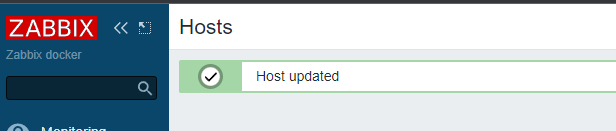


Рисунок 3.2.5 – повідомлення про оновлення інформації

Необхідно почекати на переініціалізацію конфігурації, хвилини 2, та оновити сторінку. Зараз можемо подивитися на те, що статус хосту змінився на зелений колір, як на малюнку 3.2.6.

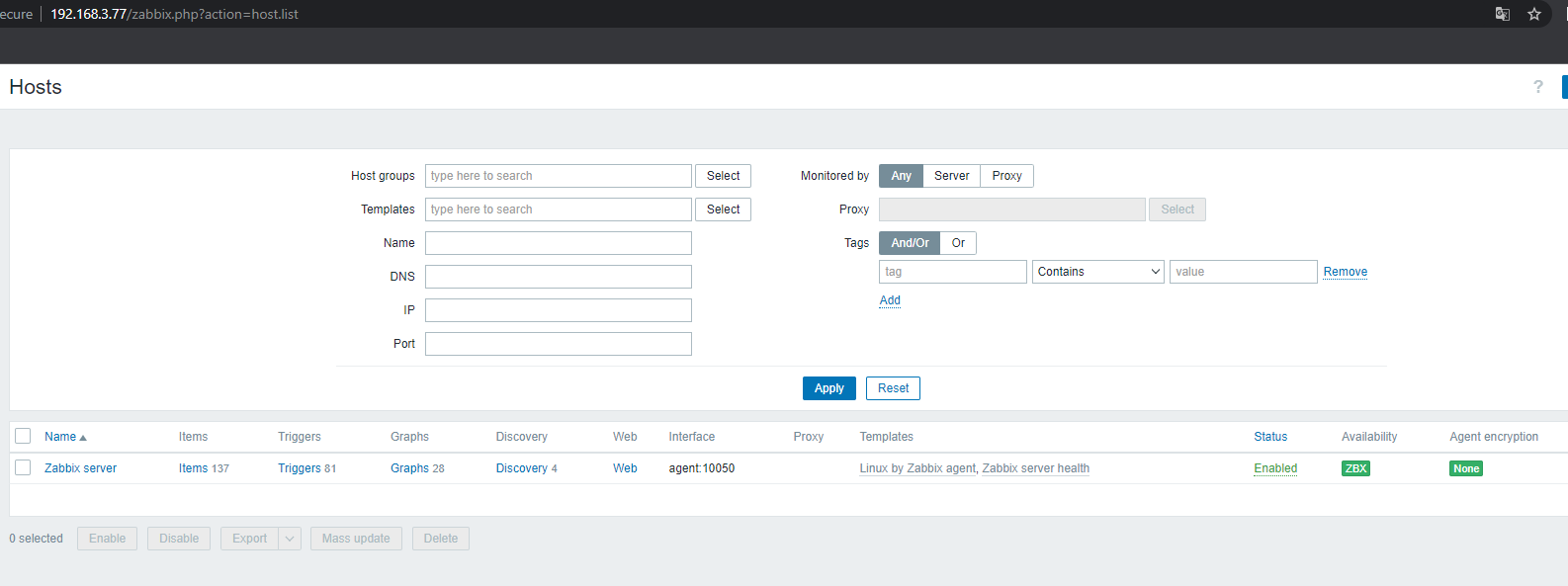


Рисунок 3.2.6 – зміна статусу хосту

Тепер головний хост – Сервер А готовий до візуалізації. Тепер аналіз системи становиться можливим, але перед початком дослідження ефективності використання, добавимо Сервер Б, згідно архітектурі яка допоможе нам в дослідженні, написана в пункті 2.1.

## **3.3 Аналіз ефективності**

### 3.3.1 Графіки

Коли ми сконфігурували забігс, почнемо аналіз ефективності цього інструменту, для аналізу систем.

Переходимо до першого пункту меню «Monitoring», та обираємо пункт «host», бачимо список доступних хостів, які ми сконфігурували. Сервер А та сервер Б, як показано на малюнку 3.3.1.

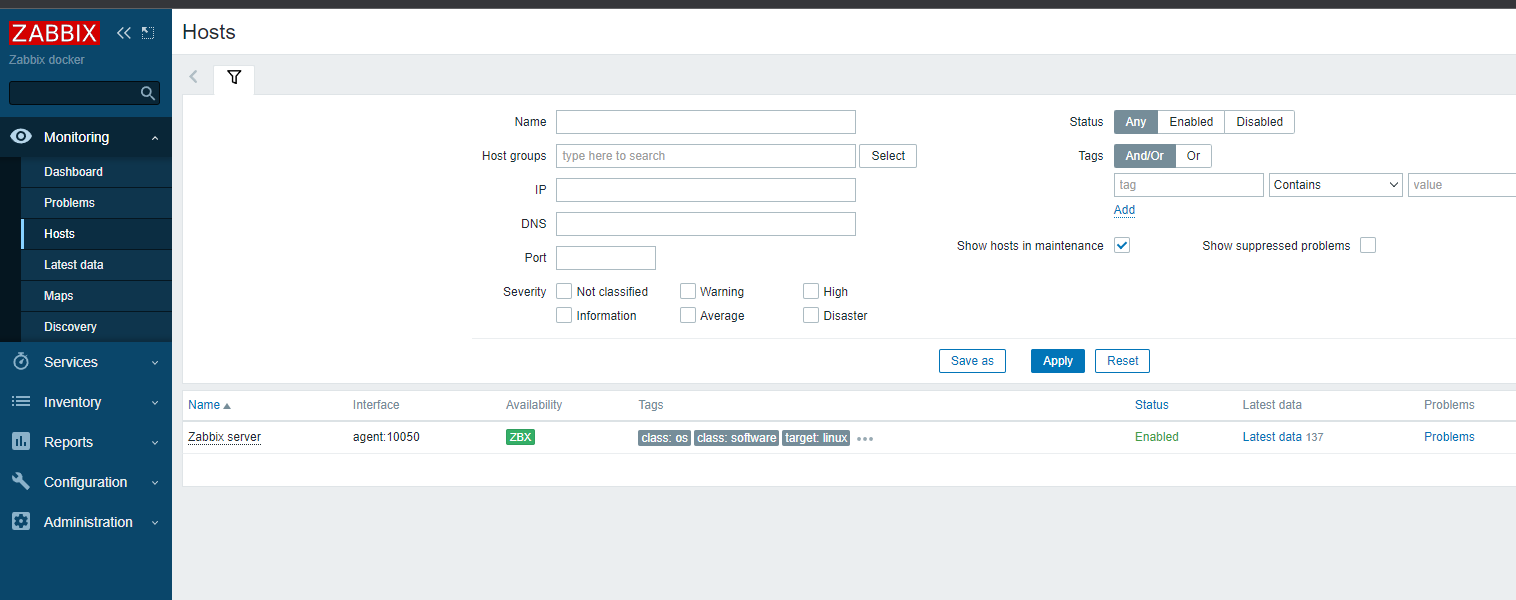


Рисунок 3.3.1 – Лист доступних хостів для аналізу систем

Для аналізу по стандартному шаблону ми повинні обрати один хост, це буде на прикладі серверу А, під назвою – Zabbix server, як зображено на малюнку 3.3.2.

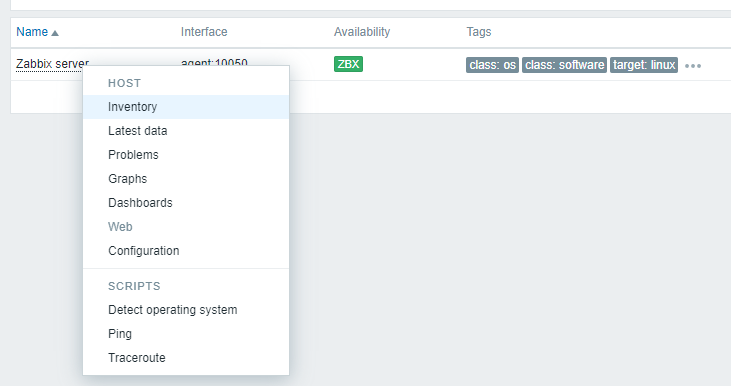


Рисунок 3.3.2 – вибір серверу А

Щоб створити звіт, ми повинні обрати пункт «Graphs», який дасть нам змогу візуалізувати аналіз системи з використанням графіків. Ми можемо бачити меню звіту, як на малюнку 3.3.3.

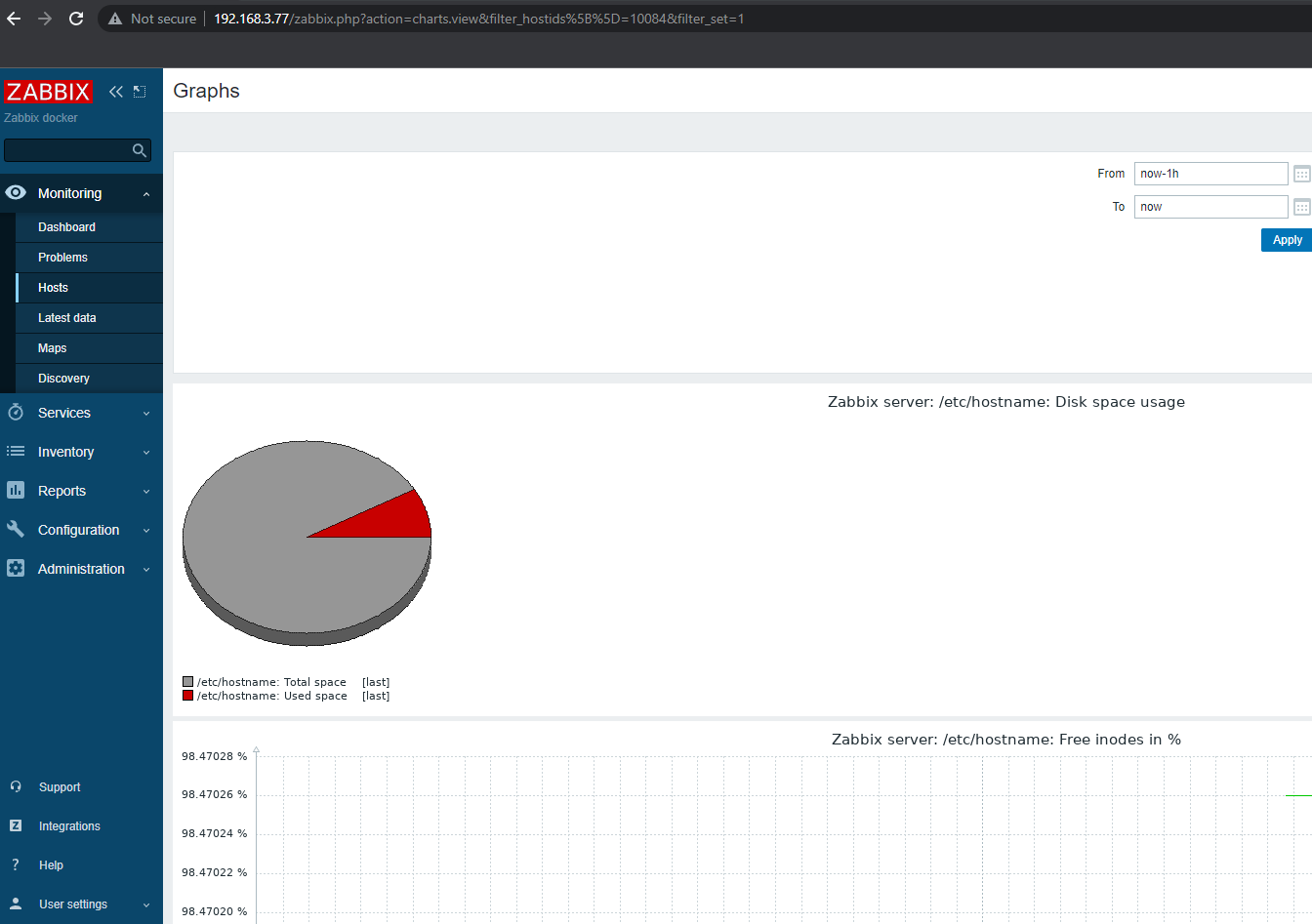
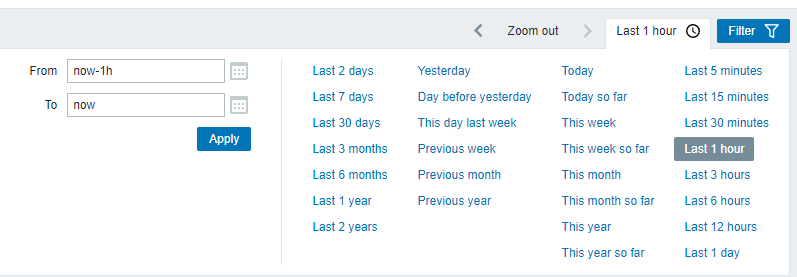


Рисунок 3.3.3 – меню створення звіту в графіках системи Серверу А

Перед початком аналізу графіків в звіті, ми можемо бачити зверху правого екрану меню вибору часового проміжку, за допомогою якого ми можемо обрати період з якого по який період дивитися графік. Вибір часового фільтру ми можемо бачити на малюнку 3.3.4.

Рисунок 3.3.4 – меню часового фільтру в звіті

Зараз ми подивимось один з самих найважливіших графіків серверів, це дисковий простір. Необхідно опустити сторінку до низу, щоб побачити графіки. Приклад показу графіку вільного простору показано на рисунку 3.3.5.

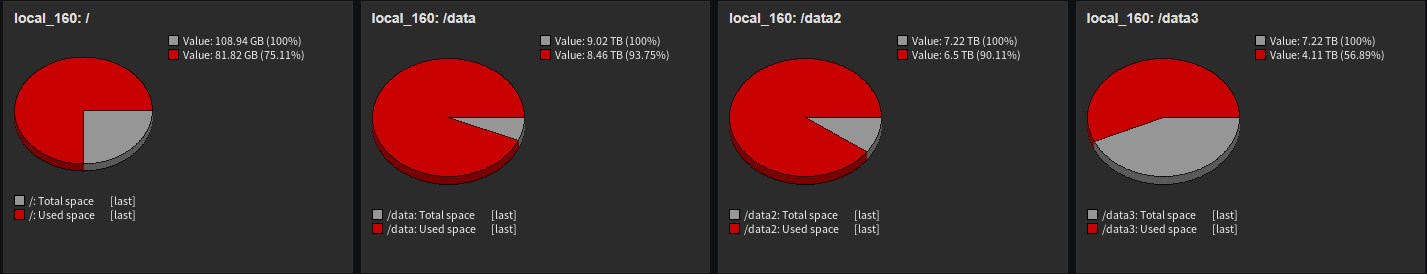


Рисунок 3.3.5 – Графіки вільного простору дисків

На цьому малюнку ми бачимо що в нас системі присутні декілька дисків, які змонтовані в різні місця. /- корінь системи як ми бачимо 108.94 гб всього на диску, а вже використано 81.82гб.

Інший графік /data – це диск, який змонтований в корінь системи, під назвою /data – на ньому 9тб всього простору. Із них зайнято 8.46тб.

Далі /data2 – третій диск, з вільним простором 7.22 ТБ, в ньому зайнято 6.5ТБ.  
І останній диск, /data3, 7.22 ТБ, на якому зайнято 4.11ТБ.

Зараз ми подивимось на не менш важливий графік, використання оперативної пам’яті на сервері. Скільки використано, та скільки залишилося вільної пам’яті, для цього промотаємо вниз, та побачимо графік як на прикладі рисунку 3.3.6.

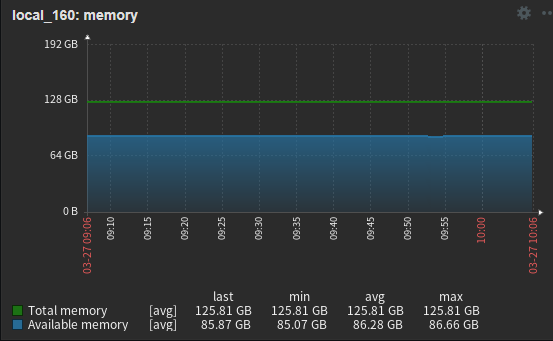


Рисунок 3.3.6 – Графіки використання RAM

Як ми бачимо, на сервері доступно 125,81 гб RAM, з них вільно 86,66 гб. Графік дає нам розуміння, що процеси які протікають на сервері, займають більше 60 гб RAM, і ми бачимо, що це стабільне використання за весь час. Якщо процеси на сервері завершити – ми на цьому графіку побачимо спад використання RAM.

Тепер подивимось на не менш цікавий графік, використання CPU ядер процесору. Ця інформація дуже важлива, тому що на відмінну від RAM, ядер на сервері менше, тому в перспективі моніторити використання процесору, від цього залежить доступність веб програм. Якщо велика кількість зв’язків клієнтів до серверу, це запускає безліч процесів, які займатимуть працею ядра процесору. Приклад, клієнт коли входить на сайт, від зразу отримує інформацію з баз даних. На стороні серверу це виглядає так: від 194.123.23.22 (або інша зовнішня адреса) приходить запит на вилучення інформації з бази даних. Необхідно запустити процес на кластері PostgresSQL, та відправити на цей запит відповідь.

Такі запити мають ієрархічну структуру виклику процесів, які по різному навантажують систему, самий важливий об’єкт моніторингу, від цього залежить кількість користувачів, які отримують інформацію у вигляді веб сторінки. Якщо ваша компанія захотять масштабувати підключення, це можливо зробити або через декілька серверів, які об’єднанні в кластер, або напряму ресурсами одного серверу. Тому моніторинг CPU є самим важливим. На малюнку 3.3.7 ми побачимо приклад графіку завантаженості.

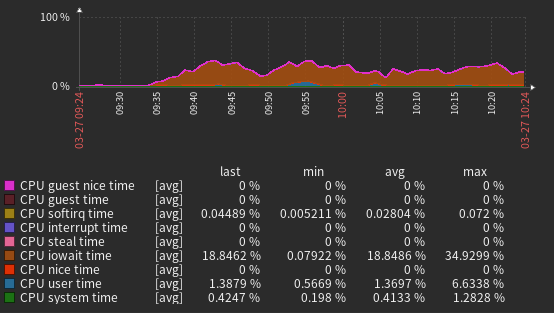


Рисунок 3.3.7 – Графік завантаженості CPU

Як ми бачимо по графіку, з 9:30 не було підключень, але в 9:35 клієнти почали заходити на веб сторінку додатку, це вантажить 34% від максимальної кількості ядер процесору. Це свідчить про те, що потрібно за цими показниками слідкувати, бо завантаження дуже велике.

Далі ми подивимось також важливу частину для веб серверів – це мережа. Оскілки linux складна операційна система, вона дозволяє максимально довільно конфігурувати все, що можливо. Тому в вашій системі можливо декілька мережевих адаптерів, які працюють по інструкції які в них описані. Нам важлива з’єднання з WAN мережею, внутрішні адаптери нас не цікавлять. Ця мережа – це прямий зв’язок клієнтів з сервером. На рисунку 3.3.8 показаний приклад цього графіку.

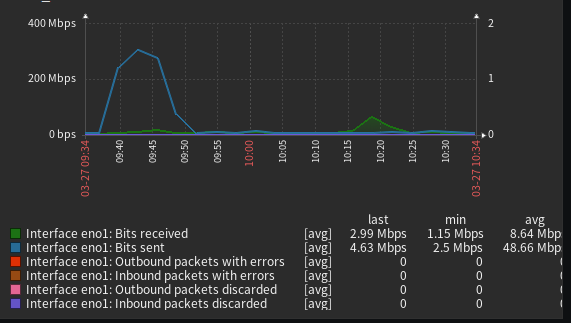


Рисунок 3.3.7 – Графік завантаженості WAN мережі

В даному випадку, це адаптер з найменуванням eno1, який відповідає за те, щоб був зв’язок з зовнішнім світом.

Тепер ми маємо інформацію, що в 9:40 через наш веб апі була велика вигрузка файлів. За двома останніми графіками ми бачимо причино-наслідкову частину загрузки CPU.

Але є ще цікава інформація. В нас як ми бачимо максимальна кількість навантаження на мережу серверу складає 400Mbps – це 50 MB/s. Але підключення до віртуального серверу проходить через основний хост, на якому проходить кабель стандарту cat 6. Цей стандарт представлений на загальному рисунку категорії кабелів - 3.3.8.

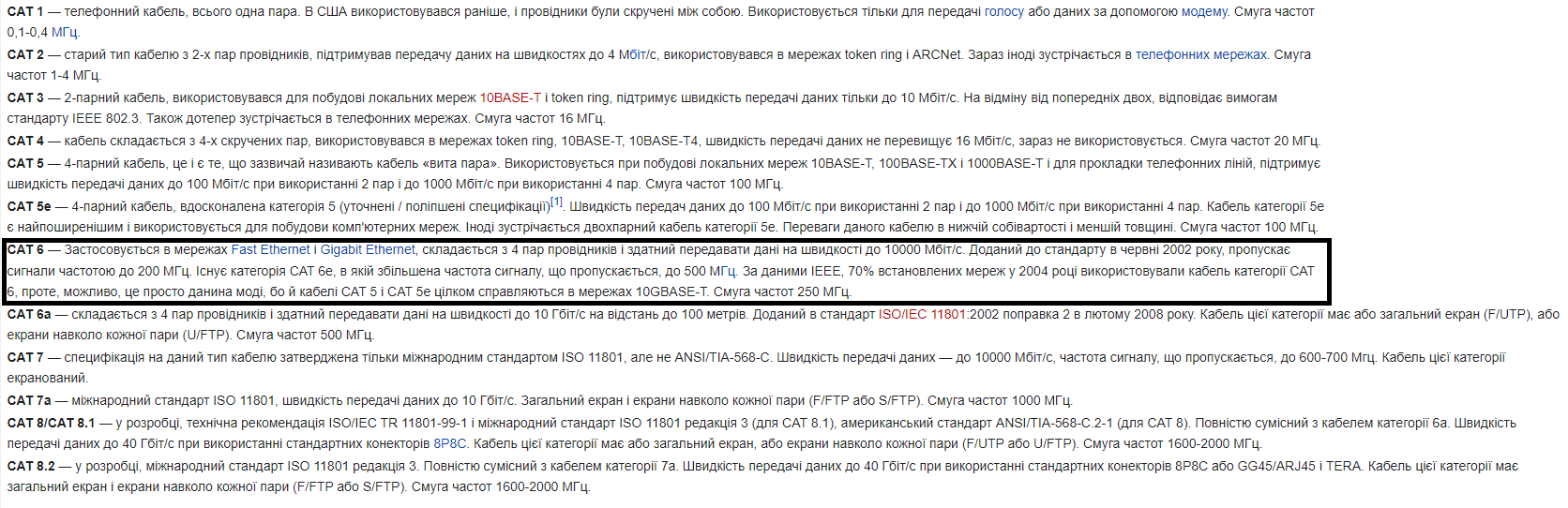


Рисунок 3.3.8 – пропускна можливість cat 6

Повинно бути 10ГБ/с, але якщо брати в розрахунок віртуалізацію, 5-6ГБ/с, але не 50 MB/s. Це дає нам уявлення, но на сервері через правила конфігурації встановлена максимальна кількість використання цього адаптеру до 400Mbps. Якщо необхідно більше, необхідно переконфігурувати мережу на сервері.

Підсумки:

Це не всі можливі графіки, які є в забігсі, але виділені самі важливі на думку DevOps інженерів графіки для веб застосунків. На цих графіках ми отримали інформацію, що в даний час відбувається з сервером. Ми отримали достатньо інформації щоб або продовжувати моніторинг, або зайти на сервер, і виправити проблеми, якщо вони присутні. Забігс надає повний опис процесів, які протікають на сервері, інформацію про CPU, RAM, дискового простору, дискової завантаженості та мережі.

### 3.3.2 Мапи

Забігс дозволяє створювати мапи, які для devops інженерів дуже важливі, на них можливо мати уявлення про мережу, яка знаходиться локально, та бачити “живі” хости, з наявними проблемами. Для створення мапи, необхідно перейти до Monitoring-Maps, і там натиснути «create map». Рисунок 3.3.9 для прикладу.

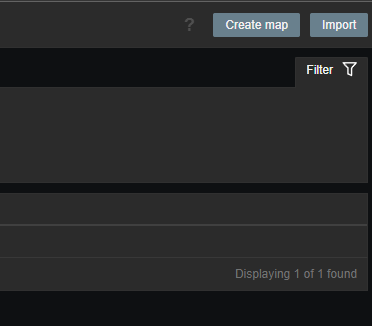


Рисунок 3.3.9 – створення мапи

А також на рисунку 3.3.10 ми побачимо вікно конфігурації цієї мапи.

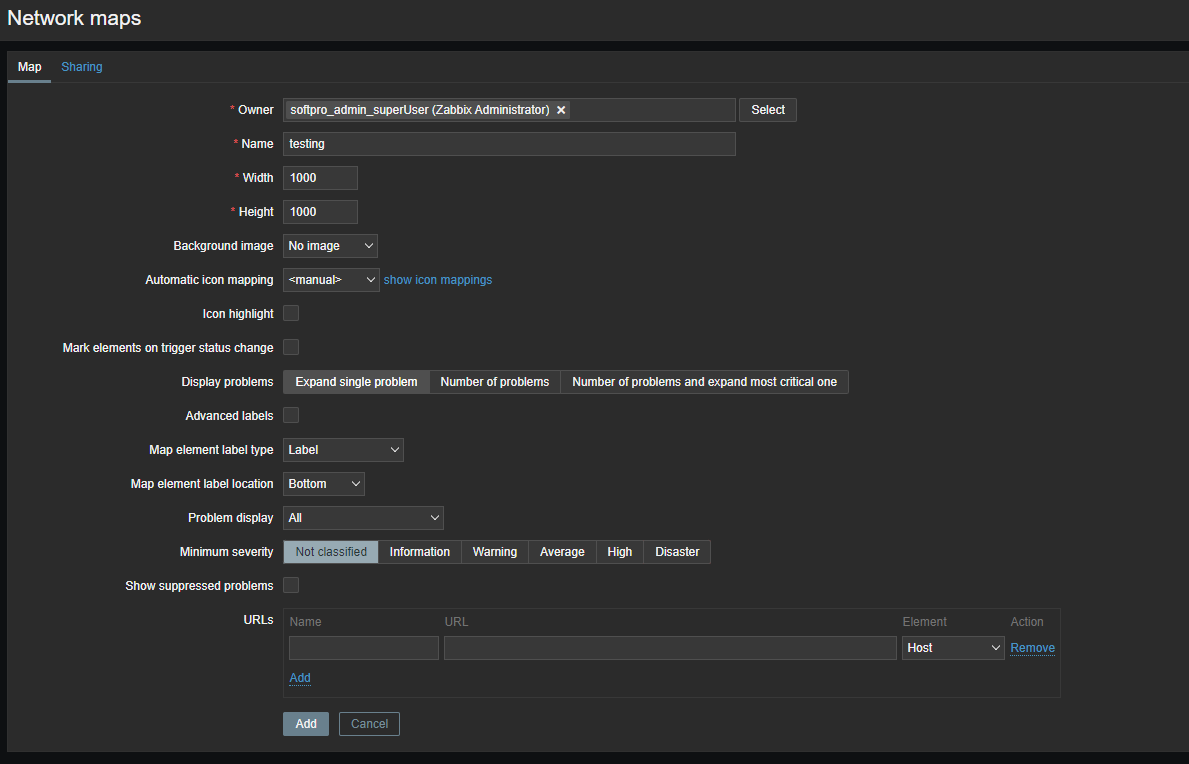


Рисунок 3.3.10 – конфігурація мапи

На цьому зображені ми бачимо красним кольором необхідні пункти. Творець – автоматично забігс обирає користувача, який зараз присутній на сервері. Ім’я мапи, довільне. Та важливі пункти – Висота та довжина робочого поля мапи. Обрано для тесту 1000х1000px.

Зараз ми бачимо робоче поле, як на рисунку 3.3.11.

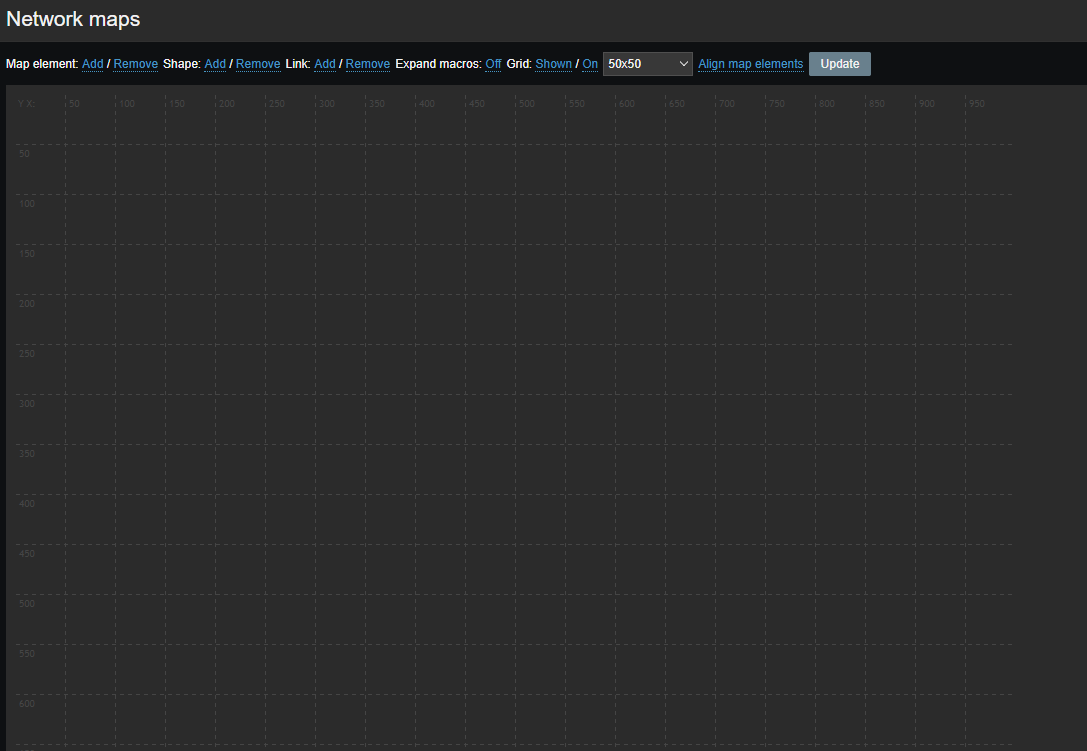


Рисунок 3.3.11 – меню створення мапи

Як ми бачимо, верхні інструменти дозволяють створити мапу. Щоб створити елемент, необхідно добавити його на мапу та сконфігурувати.

Для прикладу, ми добавимо один сервер, за яким будемо слідкувати. Приклад створення серверу представлений на рисунку 3.3.12.

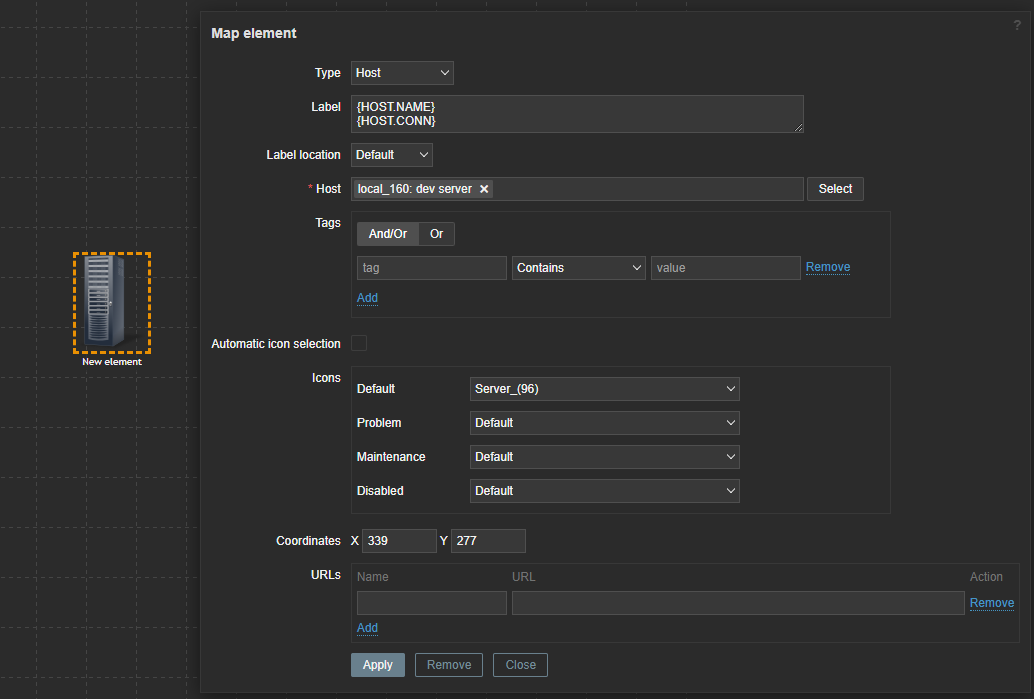


Рисунок 3.3.11 – меню створення хосту на мапі

Як ми бачимо, пункт Label – це мікро мова програмування. Тут описано виводити Ім’я серверу та статус серверу. Тип обраний – хост, та обраний хост local\_160: dev server для прикладу.

Далі ми повинні натиснути Apply, та подивится результат. Приклад рисунок 3.3.12.

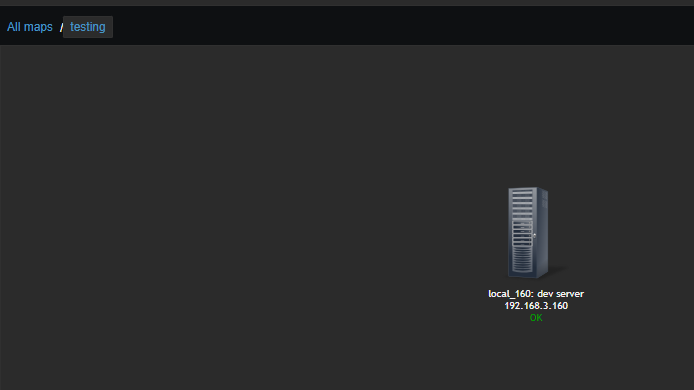


Рисунок 3.3.12 – результат створення елементу на мапі.

Але нам необхідно досліджувати ефективність забігс, тому ми перейдемо на вже сконфігуровану мапу, та подивимось можливості.

Сконфігурована мапа мережі представлена на рисунку 3.3.13.

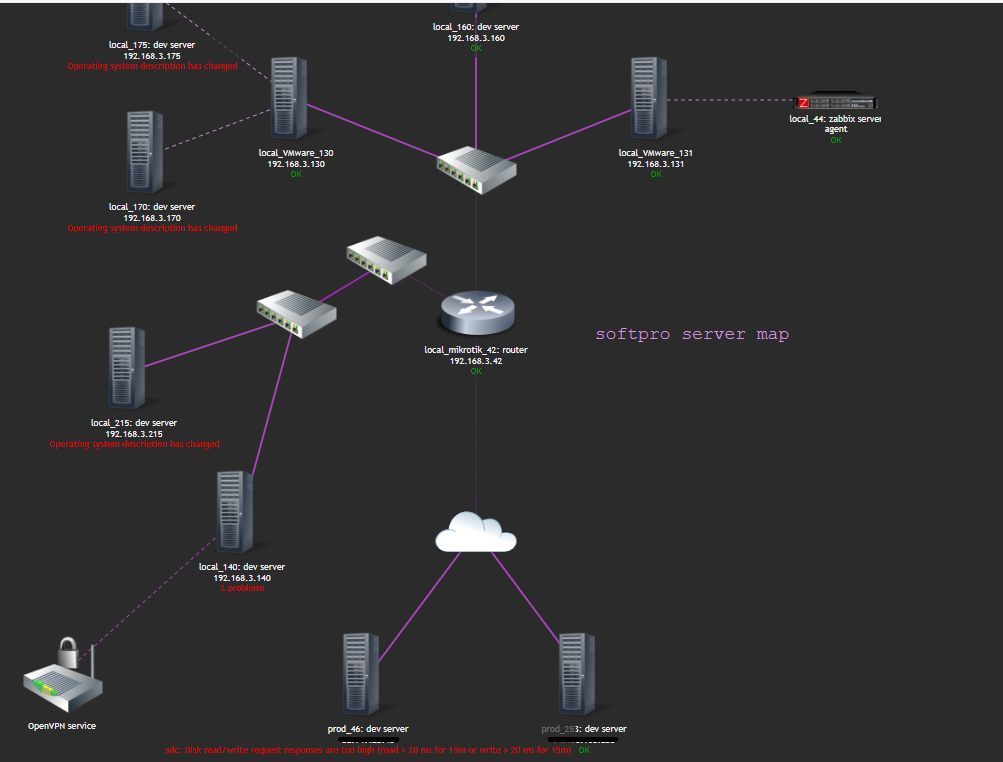


Рисунок 3.3.13 – Приклад сконфігурованної мапи мережі.

Ця мапа дає повне розуміння що у вас за локальна мережа, та які є взаємозв’язки. Приклад – OpenVPN сервіс, який є на 140 сервері, та вихід в глобальну мережу через роутер Mikrotik.

Окрім розуміння, що в нас присутнє в мережі, є відображення наявних проблем, а також надзвичайно корисні інструменти, які ми зараз оглянемо.

Перший інстурмент, самий примітивний, який можливо використати на мапі. Але це надає достатньо інформації, щоб переконатися, що сервер зараз справний по мережі, та має з’єднання з нашим роутером. Ця утіліта називається ping. Якщо не вдаватися до дрібниць, а виділити важливу інформацію, це ICMP протокол, який перевіряє якість з’єднання в мережі та надає інформацію, про доступність хосту.

Але для початку подивимось на глобальні можливості утіліт в забігсі. На рисунку 3.3.14 представлений повний список конфигурацій, на мапі з хостом.

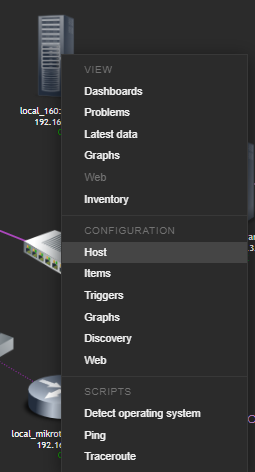


Рисунок 3.3.14 – Глобальні можливості мапи в zabbix

Нас цікавлять скріпти, які представлені в самому низі списку. Це не всі можливі скрипти, ми їх повинні власноруч писати, щоб використовувати в Zabbix. Але в стандартній конфігурації доступні тільки 3 скрипту, які ми зараз проаналізуємо. Зараз ми подивимось Ping, результат скрипту, на рисунку 3.3.15.

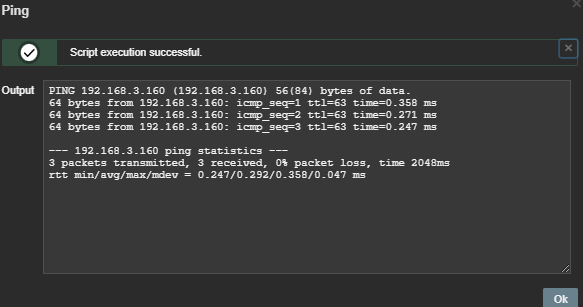


Рисунок 3.3.15 – Результат скрипту ping

Як ми бачимо на рисунку, всі пакети дійшли до серверу. Тут приведена інформація, яка буде зрозуміла DevOps та Network engineer. Ця інформація допоможе зрозуміти, доходять лі пакети даних до потрібного хосту, та виправити проблеми, які цьому процесу перешкоджають.

Далі ми проаналізуємо стандартний скрипт, traceroute. Але для початку, необхідно розуміти, що це за утиліта.

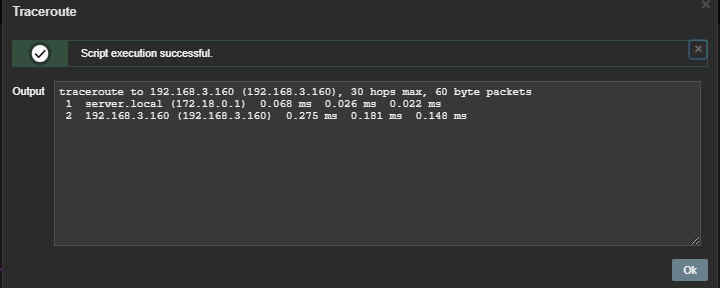
Traceroute (також відомий як трасування шляху пакета) - це утиліта мережевої діагностики, що використовується для визначення шляху, який пакет даних проходить від джерела до призначення в мережі Інтернет. Traceroute дозволяє відстежувати маршрут, який проходять дані на шляху до вказаної мережевої адреси, включаючи кількість кроків, час затримки на кожному кроці та інформацію про маршрутизатори, які обробляють кожен пакет даних.

Traceroute працює шляхом відправки пакетів даних до вказаної адреси зі збільшенням значення TTL (Time to Live - час життя) на кожному кроці. Кожен проміжний маршрутизатор, який обробляє пакет даних, зменшує значення TTL на одиницю та повертає пакет даних до відправника, який записує інформацію про маршрутизатор у вихідному повідомленні. Цей процес продовжується до того часу, поки пакет даних досягне вказаної мережевої адреси, або поки досягне максимальної кількості кроків, встановленої користувачем.

Кожен запис у вихідному повідомленні містить інформацію про номер кроку, адресу маршрутизатора, затримку на цьому кроці та інформацію про пакет даних, який використовується на цьому кроці. Інформація про затримку зазвичай вимірюється в мілісекундах і дозволяє користувачеві визначити місцезнаходження проблеми, якщо відстань між кроками збільшується.

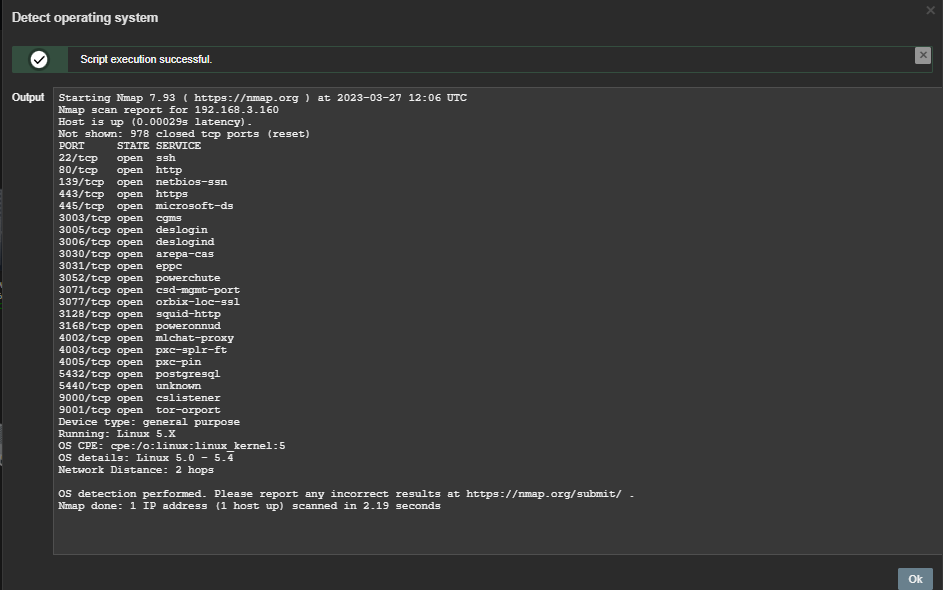
Traceroute є корисним інструментом для діагностики проблем з мережею, таких як відмови в обслуговуванні, повільна швидкість.

Після цієї інформації, ми приступаємо до аналізу цього скрипта на мапі мережі. Результат виконання представлений на рисунку 3.3.16.

Рисунок 3.3.16 – Результат скрипту traceroute

На цьому скрипту ми бачимо, що перший крок, це сервер забігс, який має ім’я server.local та має внутрішню мережу (172.18.0.1), яку за нас налаштував docker. І ще один крок, це вже нас сервер. Оскільки сервера в одній мережі, ми напряму отримаємо відповідь від серверу, без виходу в глобальну мережу. Траса пройдена успішно. Проблем немає, але якщо були, це інформація для інженерів, які конфігурують firewall в середині мережі. По цьому скрипту ми бачимо, що ми можемо моніторити проблеми, різного характеру.

І останній скрипт, останній скрипт який ми проаналізуємо, це «Detect operating system». Цей скрипт показує інформацію про систему, а точніше це замаскована утиліта nmpup, яка показує відкриті порти на сервері. На рисунку 3.3.17 показаний результат виконання скрипту.

Рисунок 3.3.17 – Результат скрипту Detect operating system

Як ми бачимо, цей скрипт детально показує які порти застосовані на цьому сервері. Із важливих – це 22, підключення до серверу. 80/443 – це відображення нашого веб додатку, на 5432 – це кластер бази даних PostgreSQL.

А також версію операційної системи.

Ми можемо зробити вивід що ці скрипти дають повну інформацію для інженерів. Якщо є наявні проблеми, цих скриптів достатньо, щоб перевірити працездатність серверів. Якщо необхідно більш детально аналізувати систему, забігс надає можливості створення власного скрипту, який буде застосовуватись на сервері.

### 3.3.3 Загальна інформація по кожному хосту

Якщо нам необхідно подивитися всі можливі метрики з серверу, забігс представляє цю можливість. Для цього необхідно перейти до Monitoring-Host, та подивитися на пункт Latest data, де представлені усі можливі метрики для групи хостів. На рисунку 3.3.18 зображено, де находиться панель.

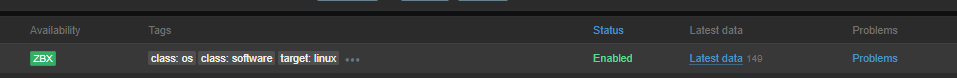
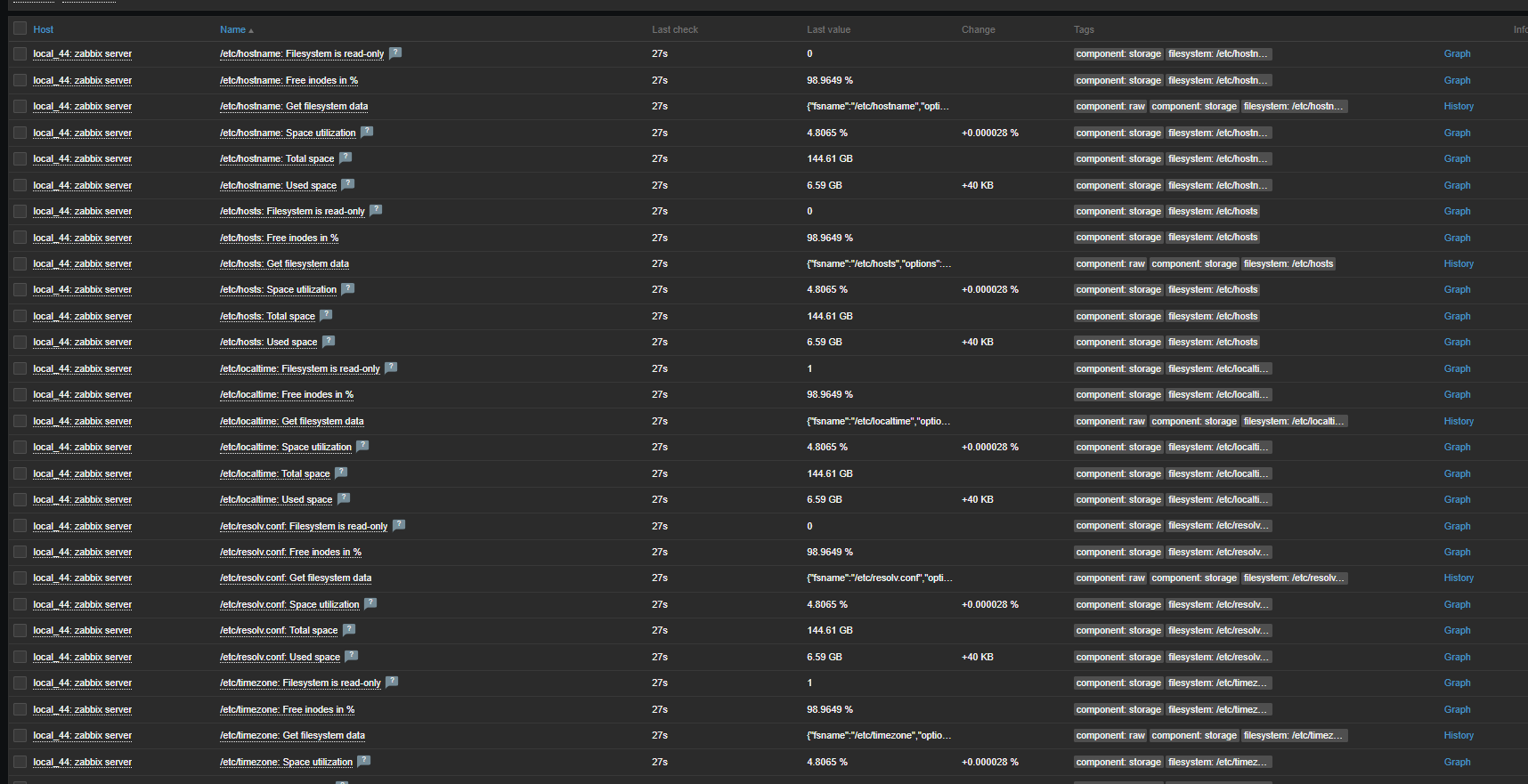


Рисунок 3.3.18 – Панель latest data

Переходимо по гіперпосиланню та бачимо метрики, які доступні для цього хосту. Рисунок 3.3.19 для прикладу.

Рисунок 3.3.19 – Метрики хосту

Це вся інформація які приходять від zabbix агенту на сервері на основний забігс сервер, на основі цих даних будуються графіки, які створені для аналізу системи. Цих метрик доволі багато, тому виділимо основне.

Ми бачимо Last cheack пункт, який свідчить про те, коли в останнє надходила інформація від агенту, ці конфігурації можливо міняти в конфігураціях агенту. Далі ми бачимо

Last value – що надходить від агенту значення. Якщо значення не мінялося, тоді в наступному пункті Change буде пустий пункт, якщо змінювалась, тоді буде нове значення.

Пункт Tags – це основний елемент. Цей елемент автоматично обирається, коли ми обираємо групу для хосту. Приклад: ми можемо створити групу лінукс сервери, де обираємо теги які необхідно відстежувати. Нам скоріше за всього непотрібні усі пункти, кешування, і т.п., тому ми можемо обрати тільки необхідні теги. Такі як filesystem, де будемо отримувати інформацію про файлову систему.

Цей інструмент управління групами дозволяє максимально ефективно використовувати надходження інформації від серверу. За допомогою тегів, ми обираємо потрібні нам конфіги для роботи з моніторингом. Нам для аналізу ефективності використання на стільки конфігурувати не потрібно.

### 3.3.4 Тригери

Останнє що нам потрібно для аналізу ефективності аналізу систем, це тригери. Тригери – це функція або перелік функцій, які викликають самі себе при певних умовах.

Тригери в забігсі – це функції реагування забігс, на перевищення значень метрик, які надходять з серверу. Простими словами розберемо на прикладі. Якщо більше 80% буде зайнято дискового простору на сервері, забігс це виведе в проблему, яка буде відображатись на мапі і в панелі хостів.

Забігс - це засіб автоматизації процесів взаємодії з клієнтами, що дозволяє налаштовувати тригери - автоматичні реакції на певні події. Щоб налаштувати тригери в Забігс, потрібно виконати наступні кроки:

1. Увійти в обліковий запис Забігс.
2. Вибрати меню "Тригери".
3. Натиснути кнопку "Створити новий тригер".
4. Вибрати подію, на яку потрібно налаштувати тригер. Наприклад, це може бути вхідний дзвінок або отримання повідомлення від клієнта.
5. Визначити умови, за яких має спрацювати тригер. Наприклад, це може бути часовий інтервал, під час якого тригер має бути активним, або кількість повідомлень від клієнта.
6. Визначити дії, які повинен виконати Забігс, коли спрацьовує тригер. Наприклад, це може бути автоматичне відповідь на повідомлення або передача дзвінка співробітнику компанії.
7. Зберегти налаштування тригера.

Тепер подивимось, як створювати тригери на прикладах. Рисунок 3.3.20 покаже, де знаходиться вкладка тригерів.



Рисунок 3.3.10 – Пункт меню тригерів

Як ми бачимо, в меню хостів в нас є елемент «Triggers», натискаємо на нього, та побачим наступне меню, яке зображено на рисунку 3.3.21.

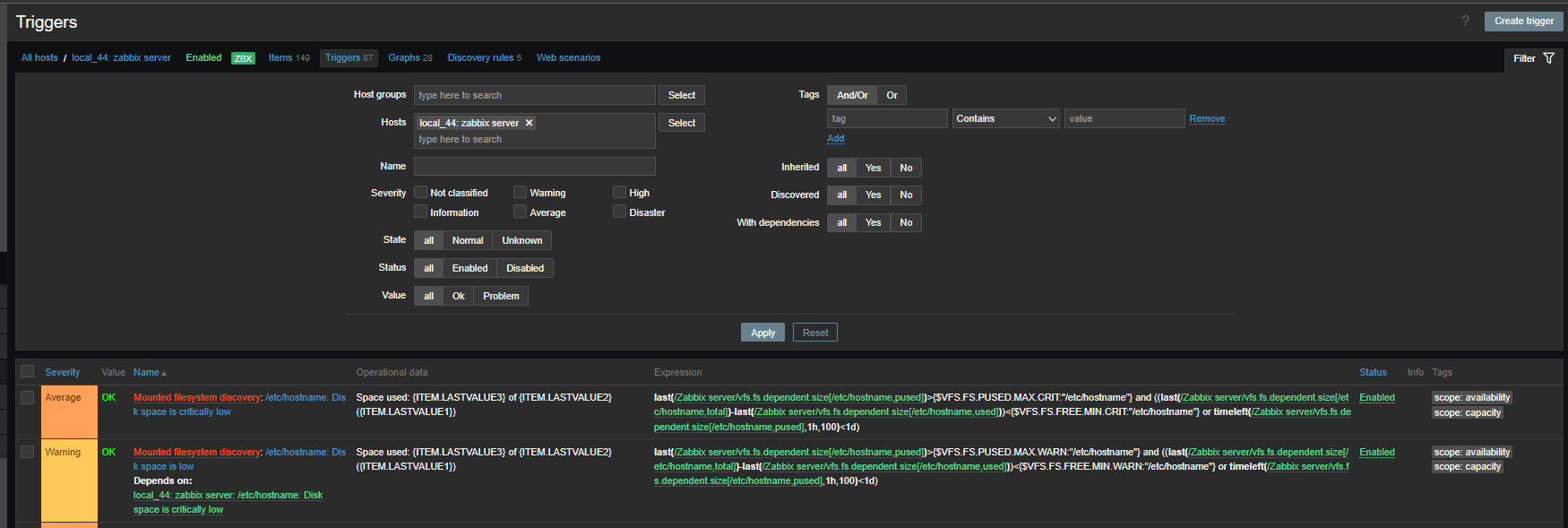


Рисунок 3.3.21– пунк меню тригерів

На цьому рисунку видно, що в нас вже скопилися повідомлення, на які потрібно реагувати. Їх можливо через це меню видалити, редагувати, копіювати. Але нас цікавить пункт створення тригеру, яке знаходиться в правій верхній частині на зображені. Натискаємо її та попадаємо до меню створення тригера, для цього серверу.

Перед створенням тригеру, нам потрібно зрозуміти, що ми повинні досліджувати і що вважати проблемою. Для аналізу, було обрано слідкувати за файлом підкачки. Умова тригеру, якщо файл підкачки використаний на 30%, то повинен створюватись повідомлення. Цей тригер був обраний для того, щоб продемонструвати роботу створення повідомлення, який допоможе нам дослідити ефективність використання. На рисунку 3.3.22 буде показане вікно конфігурації трігеру.

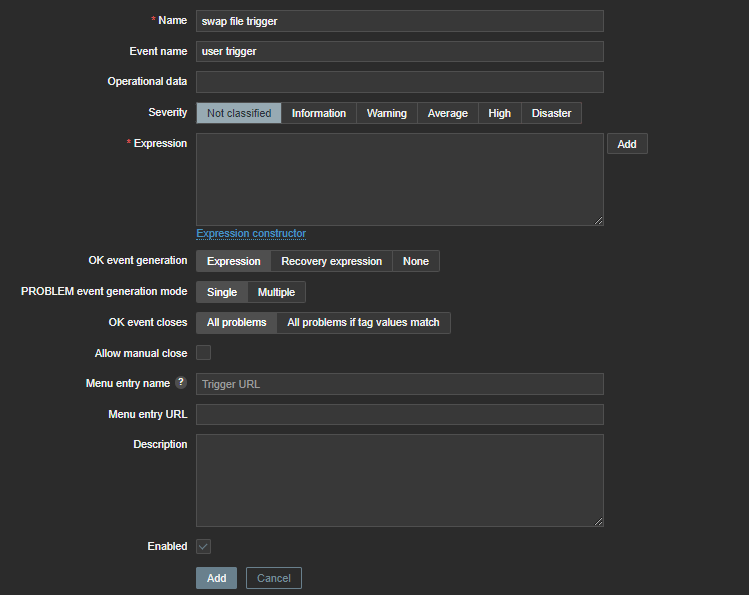


Рисунок 3.3.22– пунк меню тригерів

Зараз заповнено перші 2 пункту. Ім’я тригеру, та відображений ім’я. Для того щоб створити умову, необхідно обрати add в пункті Expression. Рисунок конфігурації умови представлений на рисунку 3.3.23.

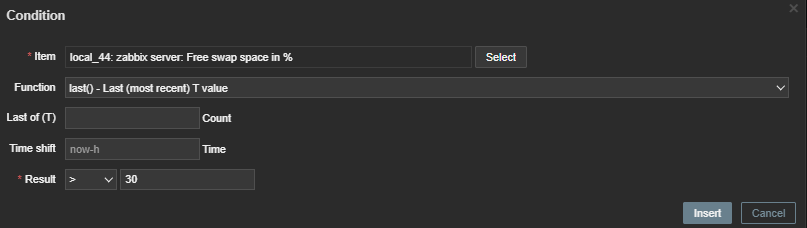


Рисунок 3.3.23– конфігурація умови тригеру

Ця конфігурація відповідає описаної умови, для того щоб її додати, необхідно обрати Insert. Тепер ми вертаємось в попереднє меню. Для того щоб закінчити редагування, натискаємо Add в самому кінці, як на рисунку 3.3.22, та дивимось результат. Ця умова повинна 100% спрацювати.

Щоб подивитися результат, ми повинні перейти в пункт меню з проблемами. Це можливо зробити, за допомогою меню Monitoring-Problems. Дивимось на результат. Рисунок 3.3.24.

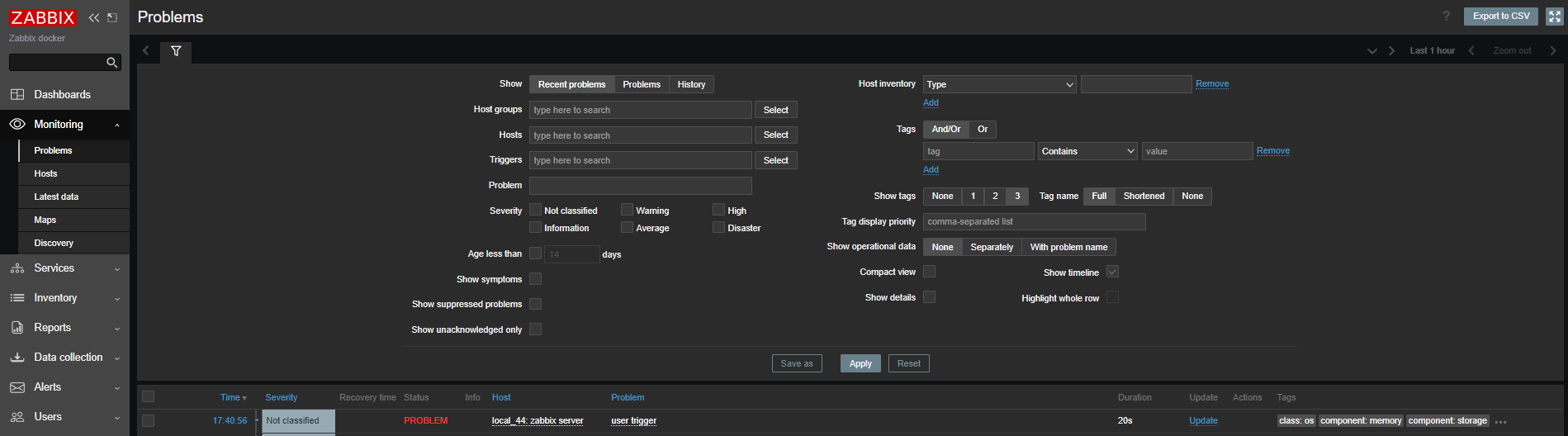


Рисунок 3.3.24 – результат створення тригеру

Як з цього прикладу видно, в нас з’явилася проблема на 44 сервері, який зараз видає помилку по проблемі user trigger. З цим інструментом ми можемо створювати власні умови, та класифікувати їх, для вчасного реагування.

## **3.4 Підведення підсумків**

Zabbix - це система моніторингу, яка дозволяє збирати і аналізувати різноманітну інформацію про працездатність комп'ютерних систем та мереж. Вона може бути використана для відслідковування метрик як фізичних серверів, так і віртуальних машин, контейнерів, мережевих пристроїв, баз даних, додатків та іншого.

Основні переваги використання Zabbix в системному аналізі включають:

1. Збір метрик в реальному часі: Zabbix забезпечує збір даних про працездатність систем в реальному часі, що дозволяє оперативно виявляти проблеми та відповідно реагувати на них.
2. Гнучкість: система може бути настроєна на збір різних типів метрик, включаючи метрики операційних систем, мережевих пристроїв, додатків, баз даних та інших. Крім того, можна налаштувати сповіщення про відхилення від норми значень метрик.
3. Масштабованість: Zabbix може бути використаний для моніторингу як невеликих, так і великих і складних середовищ. Система може бути налаштована на збір даних з декількох десятків і до кількох тисяч пристроїв.
4. Аналітика: система надає можливість аналізувати зібрані дані та будувати графіки для відображення динаміки значень метрик. З цими даними можна працювати, щоб покращити продуктивність та ефективність роботи систем.
5. Відкритий код: Zabbix є відкритою системою, що дозволяє розробникам вносити зміни та доповнення до неї. Це також дозволяє вирішувати проблеми та вдосконалювати систему швидко.

Отже, загальний висновок про Zabbix полягає в тому, що ця система моніторингу є потужним інструментом для системного аналізу та моніторингу комп'ютерних систем і мереж. Вона дозволяє збирати і аналізувати різноманітну інформацію про працездатність систем в реальному часі, а також може бути налаштована на збір даних з різних типів пристроїв. Зabbix також дозволяє аналізувати зібрані дані, щоб покращити продуктивність та ефективність роботи систем. Її масштабованість, гнучкість та відкритий код роблять її одним з кращих інструментів для системного аналізу та моніторингу.

# **Джерела**

[13.02.23] Інтернет ресурс з загальними відомостями Zabbix: <https://www.bookmyessay.com/zabbix-assignment/>

[15.02.23] Інтернет ресурс з загальними відомостями Virtual box: <https://www.virtualbox.org/manual/ch01.html#hostossupport>

[14.02.23] pdf, дослідження використання docker: <https://www.scribd.com/document/462316610/028-AnIntroductiontoDockerandAnalysisofitsPerformance-IJCSNS-20170327>

[15.02.23] Інтернет ресурс з контейнерами, інструментом Zabbix та параметрами для конфігурації: <https://hub.docker.com/u/zabbix>

[15.02.23] Інтернет ресурс з повною інструкцію використання docker engine: <https://docs.docker.com/engine/reference/builder/>

[15.02.23] Інтернет ресурс з повною інструкцію використання docker-compose: <https://docs.docker.com/compose/compose-file/>

[05.01.23] TCP/IP network administration, Крейг Хант, 1992р.

[05.01.23] Infrastructure and Application Performance Monitoring 1st Edition Brian Brazil, 2018р.

[05.01.23] VMware Cookbook: A Real-World Guide to Effective VMware Use, Ryan Troy, 2012.

[05.01.23] UNIX AND LINUX SYSTEM ADMINISTRATION, Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, 2012