МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка

до дипломного проєкту (роботи)
бакалавра
(ступінь вищої освіти (освітній ступінь))

на тему «РОЗРОБЛЕННЯ СИСТЕМИ ДИСТАНЦІЙНОГО МОНІТОРИНГУ ПРАЦЕЗДАТНОСТІ ОБЛАДНАННЯ НА ПІДПРИЄМСТВІ»

Виконав: студент 4 курсу, групи КНТ-520
спеціальності
123 Комп'ютерна інженерія

Освітня програма (спеціалізація)
Комп'ютерна інженерія
(код і назва спеціальності)

МОТОШИН О.А .
(прізвище та ініціали)
Керівник ІЛЬЯШЕНКО М.Б.
(прізвище та ініціали)
Рецензент КОЗІНА Г.Л.
(прізвище та ініціали)

2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Запорізька політехніка»

(повне найменування вищого навчального закладу)

Факультет Комп'ютерних наук і технологій

Кафедра «Комп'ютерні системи та мережі»

Ступінь вищої освіти (освітній ступінь) бакалаврський

Спеціальність 123 Комп'ютерна інженерія

(код і назва)

Освітня програма (спеціалізація) Комп'ютерна інженерія

(назва)

ЗАТВЕРДЖУЮ

Зав. кафедри Кудерметов Р.К.

"____" _____ 2024 року

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТУ

МОТОШИНА Олександра Андрійовича

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Розроблення системи дистанційного моніторингу працездатності обладнання на підприємстві

керівник проекту (роботи) ІЛЬЯШЕНКО М.Б., к.т.н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від "01" квітня 2024 року № 105

2. Строк подання студентом проекту (роботи) 01.06.2024 року

3. Вихідні дані до проекту (роботи) система моніторингу Cacti, мережеве обладнання, Ubuntu Server 20.04

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

1) Аналіз систем моніторингу;

2) Характеристика підприємства та вимоги до моніторингу;

3) Розробка системи дистанційного моніторингу у Cacti;

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

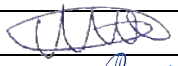
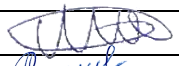
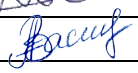
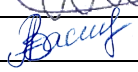
Пл1. Панель керування Cacti 1.2.9

Пл2. Процес налаштування Cacti

Пл3. Фрагмент сторінки додавання хоста

Пл4. Фрагмент графіка працездатності обладнання

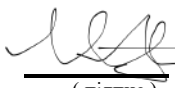
6. Консультанти розділів проекту (роботи)

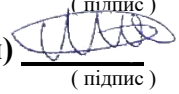
Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-3	ІЛЬЯШЕНКО М.Б., к.т.н., доцент		
Нормоконтроль	ПОЛЬСЬКА О.В., ст. викладач		

7. Дата видачі завдання 01.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Огляд літератури	20.04.2024 р.	
2	Аналіз технічного завдання	25.04.2024 р.	
3	Огляд існуючих ігрових програмних продуктів	30.04.2024р.	
4	Проєктування об’єктів розвиваючої гри	10.05.2024 р.	
5	Розробка програмного середовища та вимог програмного забезпечення	15.05.2024 р.	
6	Тестування ігрового програмного продукту	20.05.2024 р.	
7	Оформлення ПЗ	26.05.2024 р.	

Студент  **Олександр МОТОШИН**
(підпис) (ініціали та прізвище)

Керівник проєкту (роботи)  **Матвій ІЛЬЯШЕНКО**
(підпис) (ініціали та прізвище)

РЕФЕРАТ

ПЗ: 57 с., 22 рис., 2 табл., 16 джерел.

CACTI, SSH, UBUNTU SERVER, МОНІТОРИНГ, СИСТЕМА, ОБЛАДНАННЯ, ЛОМ, РОЗРОБКА, ВЕБ-ІНТЕРФЕЙС

Метою даного проєкту є створення дистанційного моніторингу працездатності обладнання на підприємстві.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- провести аналіз інструментів моніторингу локальної обчислювальної мережі;

- охарактеризувати діяльність підприємства у компетенції якої знаходяться локальні обчислювальні мережі та зібрати інформацію про програмне забезпечення;

- визначити інструменти моніторингу локальної обчислювальної мережі;

- реалізувати адаптацію системи моніторингу локальної обчислювальної мережі;

- встановити та налаштувати систему моніторингу;

- налаштувати мережеве обладнання для моніторингу;

- додати обладнання для моніторингу до веб-інтерфейсу системи моніторингу та перевірити її працездатність.

ЗМІСТ

ВСТУП

Інформаційні технології пов'язані із забезпеченням безперебійної роботи обчислювальних мереж. У зв'язку з чим виникає необхідність поліпшення існуючих способів моніторингу працездатності локальних обчислювальних мереж. Сучасний ринок інформаційних продуктів пропонує готове програмне забезпечення, що дозволяє провести моніторинг обладнання на працездатність, проте проведений аналіз виявив недоліки сучасних програмних засобів, це:

– стандартні рішення погано адаптуються до різних мереж;

– розширення мережі призводить до того, що контроль над мережею зменшується і виходить за межі закладених параметрів.

На даний момент моніторинг працездатності робочого обладнання локальних обчислювальних мереж (ЛВС) не здійснюється, тому поставлено завдання розробки та впровадження системи моніторингу.

Тема бакалаврської роботи: «Розроблення системи дистанційного моніторингу працездатності обладнання на підприємстві».

Об'єктом розробки цієї роботи є устаткування локальних обчислювальних мереж.

Предметом є система моніторингу працездатності обладнання локальних обчислювальних мереж.

Метою випускної кваліфікаційної є розробка системи моніторингу, що дозволяє стежити за працездатністю обладнання дистанційно.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- провести аналіз інструментів моніторингу локальної обчислювальної мережі;

- охарактеризувати діяльність підвідомчої організації у компетенціях якої знаходяться локальні обчислювальні мережі та зібрати інформацію про програмне забезпечення;

- визначити інструменти моніторингу локальної обчислювальної мережі;

- практично реалізувати адаптацію системи моніторингу локальної обчислювальної мережі до наявного обладнання, зокрема:

- встановити та налаштувати систему моніторингу;

- налаштувати мережеве обладнання для моніторингу;

- додати обладнання для моніторингу до веб-інтерфейсу системи моніторингу та перевірити її працездатність.

1 АНАЛІЗ СИСТЕМ МОНІТОРИНГУ

1.1 Функціонал систем моніторингу

Моніторинг необхідний компаніям, щоб бути впевненими, що певна система функціонує правильно. Однак процес моніторингу IT інфраструктури може бути досить складним і створювати труднощі, якщо він не налаштований відповідним чином. Незалежно від розміру компанії, не можна ігнорувати необхідність моніторингу серверів, баз даних, мережі, безпеки та інфраструктури. Важливо при цьому використовувати високоякісні інструменти для моніторингу. [1].

Постійний моніторинг допомагає уникнути простоїв у її роботі, підтримувати всі IT-сервіси у робочому стані та зберігати необхідний рівень їхньої якості, а також спланувати її модернізацію.

Раніше роль моніторингу здійснювали адміністратори, а інформація про стан систем у кращому разі збиралася ними ж у будь-яких неспеціалізованих програмах (через їхню відсутність), у гіршому взагалі ніяк не накопичувалася і не аггрегувалася. Усі відомості про систему були прив'язані до практичного досвіду роботи з інфраструктурою у конкретного спеціаліста і повністю губилися під час його відходу.

Зараз з'явилося безліч напів і повністю автоматизованих систем для моніторингу, які аналізують стан систем, збирають інформацію в колекції, які також можна вивчити при необхідності.

Існують досить специфічні види моніторингу, наприклад, від імені кінцевого користувача, коли задані проміжки часу циклічно емулюються його дії. Зазвичай це робот, планувальник завдань, що запускає спеціальний, заздалегідь визначений скрипт-сценарій, а потім рапортує про успіх виконання дій або про помилки, що виникли в процесі.

Для зберігання отриманої інформації зазвичай використовується база даних конфігурації під різними СКБД: інформація про об'єкти моніторингу

представлена, як набір конфігураційних одиниць. Кожен сервер, кожен мережевий пристрій — це одиниця, усе це зберігається у централізованої базі даних. Таке уявлення дозволяє потім інтегрувати систему моніторингу з візуальними уявленнями: діаграмами, графіками та ін.

Сама структура моніторингу значно видозмінюється з часом. Наприклад, одна з тонкощів виникла при появі та великому поширенні віртуалізації: якщо раніше була необхідність відслідковувати стан лише фізичних серверів, то тепер на кожному з них може бути ще кілька віртуальних.

Також системи моніторингу можна налаштувати виконання будь-яких стандартних сервісних дій. Наприклад, очищати кошик під час його заповнення або активувати архівування для будь-яких файлів, коли певний відсоток дискового простору стає зайнятим.

При виборі, розробці та впровадженні систем моніторингу, спочатку потрібно визначити об'єкти для спостереження, а також критичні події та показники, які впливатимуть на кількість оповіщень про несправності, частоту сканування та інші параметри. Для великих інфраструктур, таких як дата-центри, перед остаточним впровадженням часто створюється тестовий майданчик для оцінки правильності прийнятих рішень та встановлення порогових значень.

Впровадження таких рішень є особливо важливим при використанні сервісного підходу до роботи IT-підрозділів, коли всі процеси розглядаються з точки зору IT-сервісів, що надаються підрозділом. Кожен бізнес-сервіс корпоративної системи, за можливості, інтерпретується як IT-сервіс з визначеним рівнем якості надання. Після цього він описується у системі моніторингу як набір взаємозалежних компонентів IT-інфраструктури.

У результаті формується Угода про рівень якості сервісів (Service Level Agreement, SLA). Відповідно до SLA система здійснює збирання та зберігання інформації про якість надання IT-сервісів. На основі накопиченої інформації формуються звіти за певний період.

Аналіз звітної інформації дозволяє виконувати:

- оцінку рівня надання IT-сервісів;

- реорганізацію роботи IT-підрозділу;

- модернізацію IT-інфраструктури.

Системи моніторингу можуть бути орієнтовані на споживачів різного рівня. Для великих систем зазвичай використовується велика кількість різноманітних функцій, тоді як для невеликих достатньо загального аналізу вузлів та надсилання сповіщень. Серед основних функцій моніторингових систем можна виділити такі:

- спостереження - основна функція, що включає періодичний збір показників з вузлів обладнання, сервісів тощо;

- зберігання інформації - передбачає збір даних за основними показниками кожного об'єкта моніторингу, зазвичай зберігання здійснюється у базах даних;

- побудова звітів - здійснюється як з урахуванням поточних даних стеження, і за довгостроково збереженої інформації (наприклад, довгостроковий моніторинг навантаження на сервер може попередити, що споживані ресурси постійно збільшуються, отже необхідно збільшити доступні кошти або перенести частину завдань на інший сервер, вибір якого також можна здійснити на основі довгострокового звіту);

- візуалізація - звіти у візуальному форматі, такі як графіки, підказки та діаграми, сприяють легшому сприйняттю інформації. Можна вибирати для візуалізації кілька найважливіших індикаторів, тоді як у звітах будуть представлені всі показники;

- пошук вузьких місць - аналітичні дані моніторингу допомагають визначити, де в інфраструктурі найбільше знижуються загальні показники продуктивності;

- автоматизація сценаріїв - ця функція звільняє адміністраторів від рутинних завдань.

Завдяки засобам для реалізації всіх цих функцій адміністратору більше не потрібно вручну перевіряти стан кожної складової системи. Проблеми

вирішуються та несправності усуваються оперативніше, діагностика здійснюється багатовимірно та точно, а також можна планувати розширення інфраструктури.

Використання систем моніторингу та управління дозволяє:

- оптимізувати використання інформаційних ресурсів;

- підвищити якість IT-сервісів, швидкість усунення збоїв у роботі обладнання та програмного забезпечення, мінімізувати час простою сервісів;

- забезпечити надійність, безпеку та узгоджене функціонування всіх компонентів IT-інфраструктури;

- полегшити модернізацію IT-інфраструктури;

- значно підвищити ефективність роботи IT-підрозділу.

Для вибору системи моніторингу працездатності обладнання необхідно провести аналіз найпопулярнішого на даний момент програмного забезпечення. На ринку програмного забезпечення, що використовує моніторинг мереж та обладнання існує багато систем. Щоб обрати найкращу для нашого проєкту проведемо огляд декількох системи моніторингу: NetXMS, Nagios, Zabbix, Cacti.

1.2 Огляд NetXMS

NetXMS - це комплексна система моніторингу мережі з відкритим вихідним кодом, яка забезпечує повний контроль і управління IT-інфраструктурою. Вона призначена для забезпечення ефективного моніторингу всіх аспектів роботи мережі, серверів, додатків і послуг.

Основні функції та можливості NetXMS. Моніторинг мережі:

- підтримка різних протоколів моніторингу (SNMP, ICMP, HTTP, HTTPS, SSH тощо);

- виявлення і візуалізація топології мережі;

- моніторинг продуктивності мережевих пристроїв і ліній зв'язку;

- підтримка моніторингу різних операційних систем (Windows, Linux, UNIX);

- збір і аналіз даних про стан серверів, процесів, служб і додатків;

- моніторинг баз даних (MySQL, PostgreSQL, Oracle);

- гнучка система управління подіями з можливістю налаштування правил обробки;

- сповіщення через різні канали (email, SMS, Jabber, Slack тощо);

- інтеграція з системами управління інцидентами та допоміжними службами;

- інтерактивні дашборди та графіки;

- генерація звітів про стан інфраструктури і продуктивність;

- візуалізація історичних даних для аналізу тенденцій.

NetXMS – це система моніторингу мережі з відкритим вихідним кодом, що забезпечує моніторинг і керування різними аспектами IT-інфраструктури. Вона використовується для моніторингу мережевих пристроїв, серверів, додатків та інших компонентів IT-середовища [2].

Плюси NetXMS:

- відкритий вихідний код - є безкоштовним і відкритим програмним забезпеченням, що дозволяє користувачам модифікувати його відповідно до своїх потреб;

- широкий спектр функцій - підтримує моніторинг мережевих пристроїв, серверів, додатків, баз даних, віртуальних середовищ та іншого обладнання;

- платформна незалежність -працює на різних операційних системах, включаючи Windows, Linux і macOS;

- підтримка SNMP і агентів - - підтримує різні версії SNMP та власні агенти для збору детальних даних з пристроїв;

- масштабованість - підходить для моніторингу як невеликих мереж, так і великих корпоративних середовищ;

- гнучка система сповіщень - підтримує налаштування сповіщень через

різні канали, включаючи електронну пошту, SMS, і інтеграції з іншими системами сповіщень;

- візуалізація та звітність - має потужні засоби для візуалізації даних та створення звітів, що дозволяють користувачам легко аналізувати стан мережі та продуктивність систем;

- спільнота та документація - активна спільнота користувачів та розробників, а також детальна документація допомагають швидко вирішувати проблеми та знаходити відповіді на питання;

- NetXMS є програмою з відкритим кодом, що дозволяє знизити витрати на придбання ліцензій.

- система підтримує широкий спектр протоколів та технологій, що робить її універсальною для різних типів інфраструктур;

- NetXMS може бути використана як в малих мережах, так і в великих розподілених системах;

- велика і активна спільнота користувачів та розробників забезпечує швидке вирішення проблем і регулярні оновлення.

До мінусів NetXMS можна віднести наступне:

- складність налаштування - початкове налаштування та конфігурація можуть бути складними для новачків, потрібен час для вивчення та розуміння всіх функцій та можливостей системи;

- вимоги до ресурсів - може вимагати значних апаратних ресурсів для ефективної роботи у великих мережах;

- інтерфейс користувача - може виглядати застарілим у порівнянні з деякими сучасними комерційними рішеннями;

- відсутність деяких спеціалізованих функцій - може не мати деяких специфічних функцій або інтеграцій;

- підтримка та оновлення - офіційна підтримка може бути менш оперативною в порівнянні з платними рішеннями, що надаються комерційними постачальниками;

- для нових користувачів може бути складно швидко освоїти всі функції

та можливості системи;

- відсутність офіційної підтримки, хоча спільнота дуже активна, офіційна підтримка доступна лише через комерційні пропозиції;

- для деяких користувачів налаштування та інтеграція можуть бути складними і потребувати додаткового часу та знань.

NetXMS є потужним інструментом для моніторингу та управління IT-інфраструктурою. Він пропонує широкий спектр функцій і можливостей, які дозволяють забезпечити ефективний контроль за станом і продуктивністю мережі, серверів та додатків. Хоча система може вимагати певних знань і часу на освоєння, її гнучкість і масштабованість роблять її відмінним вибором для багатьох організацій. Приклад NetXMS продемонстровано на рисунку 1.1.

Рисунок 1.1 – Консоль NetXMS Windows

NetXMS – це потужний інструмент для моніторингу мережі, який підходить для різних середовищ. Він особливо привабливий для організацій, які бажають скоротити витрати на програмне забезпечення, але готові інвестувати час у налаштування та підтримку системи.

1.3 Огляд Nagios

Nagios – це одна з найпопулярніших систем моніторингу з відкритим вихідним кодом, що використовується для моніторингу IT-інфраструктури, включаючи сервери, мережеві пристрої, додатки та служби. Вона забезпечує своєчасне виявлення проблем, сповіщення про неполадки і відновлення після збоїв [3].

Nagios – це потужна система моніторингу з відкритим вихідним кодом, яка призначена для відстеження та управління станом мережевих ресурсів, серверів, додатків та служб. Nagios дозволяє адміністраторам вчасно виявляти та вирішувати проблеми, забезпечуючи високу надійність та продуктивність IT-інфраструктури.

Nagios був створений Етаном Галстедом (Ethan Galstad) у 1999 році і спочатку був відомий як NetSaint. У 2002 році проект був перейменований на Nagios. З тих пір система постійно вдосконалюється та розширюється, отримуючи нові функції та підтримку сучасних технологій. Nagios має активну спільноту користувачів та розробників, що сприяє швидкому вирішенню проблем та постійному оновленню системи.

Nagios є потужним та гнучким інструментом для моніторингу IT-інфраструктури, який забезпечує високий рівень надійності та продуктивності. Завдяки своїй розширюваності, активній спільноті та постійному розвитку, Nagios залишається одним з найпопулярніших рішень для моніторингу серед підприємств різного масштабу. Використання Nagios дозволяє адміністраторам вчасно виявляти та вирішувати проблеми, що сприяє забезпеченню стабільної та безперебійної роботи IT-систем.

Nagios є однією з провідних платформ для моніторингу IT-інфраструктури, яка надає можливість ефективного спостереження за мережею, серверами, додатками та іншими критичними компонентами. Спроектований для виявлення проблем, забезпечення безперервності бізнесу та мінімізації

простоїв, Nagios є надійним інструментом для адміністраторів і IT-фахівців.

Основна перевага Nagios полягає в його потужності та гнучкості. Система дозволяє моніторити широкий спектр метрик, таких як доступність серверів, використання ресурсів (процесора, пам'яті, дискового простору), продуктивність додатків, а також специфічні показники, важливі для бізнесу. Використовуючи плагіни, Nagios можна налаштувати для моніторингу практично будь-якого аспекту IT-інфраструктури, що робить його універсальним рішенням для різних організацій.

Інтерфейс Nagios надає можливість створювати користувацькі дашборди та графіки, які відображають стан систем у реальному часі. Це дозволяє адміністраторам швидко отримувати інформацію про поточний стан мережі та реагувати на виникаючі проблеми. Крім того, Nagios підтримує створення складних правил оповіщення та ескалації, що дозволяє автоматично інформувати відповідальних осіб про критичні події через електронну пошту, SMS або інші канали зв'язку.

Nagios також відомий своєю масштабованістю. Він може використовуватися як для моніторингу невеликих мереж, так і для великих розподілених інфраструктур. Це досягається за рахунок модульної архітектури та можливості розподілу навантаження між кількома інстанціями Nagios, що забезпечує високу продуктивність і надійність системи.

Ще однією важливою характеристикою Nagios є його відкритий вихідний код. Це не тільки робить платформу доступною для широкого кола користувачів без значних витрат, але й сприяє розвитку активної спільноти, яка постійно вдосконалює та розширює функціональність Nagios. Спільнота надає велику кількість додаткових плагінів та модулів, які можуть бути інтегровані в систему для підвищення її можливостей.

З точки зору управління IT-ресурсами, Nagios пропонує розширені можливості для автоматизації та інтеграції. Він може бути інтегрований з іншими системами управління IT, такими як CMDB (Configuration Management Database) та інструментами автоматизації, що дозволяє створювати комплексні

рішення для моніторингу та управління інфраструктурою.

Завдяки своїм потужним можливостям моніторингу, гнучкості у налаштуванні, масштабованості та відкритому вихідному коду, Nagios є відмінним вибором для організацій будь-якого розміру, які прагнуть забезпечити стабільну та ефективну роботу своєї IT-інфраструктури. Система допомагає вчасно виявляти та вирішувати проблеми, мінімізуючи простої та підвищуючи загальну продуктивність і надійність IT-сервісів.

Перевагами Nagios є наступні:

- відкритий вихідний код - є безкоштовним і відкритим програмним забезпеченням, що дозволяє користувачам налаштовувати його відповідно до своїх потреб;

- гнучкість та розширюваність - підтримує безліч плагінів і додатків, що дозволяє розширити його функціонал для моніторингу різних аспектів IT-інфраструктури;

- широка спільнота - велика кількість користувачів та розробників, які створюють і підтримують плагіни, надають документацію та допомогу через форуми і спільноти;

- підтримка різних платформ - працює на різних операційних системах, таких як Linux і Windows;

- сповіщення та ескалація - підтримує різні методи сповіщення (електронна пошта, SMS, повідомлення) і можливості ескалації проблем для забезпечення своєчасного реагування;

- інтеграція з іншими системами - може інтегруватися з різними системами управління та інструментами моніторингу для створення комплексного рішення.

До недоліків системи Nagios відносяться наступні:

- складність налаштування - початкове налаштування може бути складним і вимагати значного часу та знань для конфігурації та інтеграції всіх необхідних компонентів;

- інтерфейс користувача - базовий інтерфейс може виглядати застарілим

і незручним для деяких користувачів, хоча існують сторонні інтерфейси, які можуть покращити користувацький досвід;

- обмежена візуалізація - базові можливості візуалізації даних можуть бути обмеженими, що вимагає використання сторонніх рішень або плагінів для більш детальної візуалізації;

- вимоги до ресурсів - може вимагати значних апаратних ресурсів і налаштувань для забезпечення стабільної роботи;

- підтримка та оновлення - хоча є активна спільнота, офіційна підтримка та оновлення можуть не завжди бути на рівні комерційних продуктів.

Комерційна версія Nagios XI надає кращу підтримку, але за додаткову плату. Фрагмент журналів Nagios зображено на рисунку 1.2.

Рисунок 1.2 – Фрагмент журналів Nagios

Nagios залишається потужним і гнучким інструментом для моніторингу, особливо привабливим для організацій, які мають досвід в управлінні IT-інфраструктурою і готові інвестувати час у налаштування та підтримку системи.

1.4 Огляд Zabbix

Zabbix – це одна з провідних систем моніторингу з відкритим вихідним кодом, що забезпечує детальний моніторинг різних аспектів IT-інфраструктури, включаючи сервери, мережеві пристрої, додатки та служби. Він відомий своєю гнучкістю, потужними можливостями і великою спільнотою користувачів [4].

Zabbix є потужною та масштабованою платформою для моніторингу IT-інфраструктури, яка забезпечує безперервне спостереження за мережами, серверами, хмарними ресурсами та іншими IT-компонентами. Розроблений для виявлення проблем та аналізу продуктивності в реальному часі, Zabbix допомагає організаціям підвищити надійність та ефективність своїх IT-систем.

Однією з основних особливостей Zabbix є його здатність збирати дані з різних джерел, використовуючи різноманітні методи, такі як агентське та безагентське моніторинг, SNMP, IPMI, JMX та інші. Це дозволяє легко інтегрувати Zabbix у вже існуючу IT-інфраструктуру, надаючи гнучкість у налаштуванні та розширенні системи моніторингу.

Інтерфейс Zabbix є зручним і інтуїтивно зрозумілим, що спрощує управління та налаштування системи навіть для користувачів без глибоких технічних знань. Адміністратори можуть створювати користувацькі дашборди, які відображають ключові показники продуктивності (KPI) та інші важливі дані в режимі реального часу. Це допомагає швидко реагувати на потенційні проблеми та приймати обґрунтовані рішення на основі надійних даних.

Zabbix також підтримує можливість створення складних тригерів та сповіщень, які автоматично інформують відповідальних осіб про виявлені проблеми через електронну пошту, SMS, месенджери або інші канали зв'язку. Це значно знижує час реакції на інциденти та мінімізує можливі простої в роботі системи.

Крім того, Zabbix пропонує розширені можливості звітності та аналізу. Користувачі можуть створювати детальні звіти про стан інфраструктури,

продуктивність та використання ресурсів, що дозволяє планувати оптимізацію та модернізацію IT-систем. Інтеграція з іншими інструментами та платформами також сприяє розширенню функціональності Zabbix, дозволяючи створювати комплексні рішення для моніторингу.

Важливою перевагою Zabbix є його відкритий код, що робить платформу доступною для використання без ліцензійних витрат. Це дозволяє організаціям будь-якого розміру впроваджувати потужні інструменти моніторингу без значних інвестицій. Спільнота користувачів та розробників Zabbix є активною та підтримує розвиток платформи, пропонуючи нові модулі, плагіни та оновлення.

Підсумовуючи, Zabbix є комплексним рішенням для моніторингу IT-інфраструктури, яке поєднує в собі високу гнучкість, масштабованість та багатий функціонал. Відповідний для великих підприємств та малих компаній, Zabbix допомагає забезпечити стабільну та безперебійну роботу IT-систем, що є ключовим фактором успіху в сучасному бізнес-середовищі.

До переваг системи моніторингу Zabbix, належать наступні:

- відкритий вихідний код - є безкоштовним і відкритим програмним забезпеченням, що дозволяє користувачам змінювати та адаптувати його під свої потреби;

- комплексний моніторинг - підтримує моніторинг серверів, мережевих пристроїв, додатків, баз даних, віртуальних середовищ та хмарних служб, що забезпечує всеосяжний погляд на IT-інфраструктуру;

- масштабованість - підходить як для малих, так і для великих середовищ, здатний моніторити тисячі вузлів, що робить його придатним для використання в корпоративних умовах;

- гнучкість налаштувань - широкі можливості для налаштування, включаючи створення складних сценаріїв моніторингу та персоналізованих дашбордів;

- потужна система сповіщень - підтримує різні методи сповіщення (електронна пошта, SMS, повідомлення) і налаштовувані умови для сповіщень і

ескалацій;

- візуалізація та звітність - потужні засоби для візуалізації даних: графіки, карти мережі, дашборди та звіти, що допомагають аналізувати стан інфраструктури;

- підтримка агентів - може використовувати агенти для збору даних з систем або виконувати моніторинг без агентів через SNMP, IPMI, JMX та інші протоколи;

- інтеграція з іншими системами - підтримує інтеграцію з різними системами управління та інструментами моніторингу, що дозволяє створювати комплексні рішення.

Приклад інтерфейсу системи моніторингу Zabbix зображено на рисунку 1.3.

Рисунок 1.3– Інтерфейс системи моніторингу Zabbix

До недоліків відносяться наступні:

- складність налаштування - початкове налаштування може бути складним, вимагати значних знань і часу для правильної конфігурації всіх компонентів;

- вимоги до ресурсів - для моніторингу великих середовищ може потребувати значних апаратних ресурсів, а також оптимізації для забезпечення ефективної роботи;

- складність масштабування - налаштування великих розгортань може потребувати додаткових знань і досвіду;

- інтерфейс користувача - може бути не настільки інтуїтивно зрозумілим для нових користувачів, хоча він постійно вдосконалюється.

Zabbix є потужним інструментом для моніторингу IT-інфраструктури, який особливо приваблює організації, що шукають гнучке і масштабоване рішення з широким спектром можливостей. Незважаючи на певні труднощі в налаштуванні та навчанні, він забезпечує всеосяжний і детальний моніторинг різних компонентів IT-середовища.

1.5 Огляд Cacti

Cacti – це система моніторингу та графічного відображення даних з відкритим вихідним кодом, яка спеціалізується на зборі і візуалізації мережевих даних. Вона часто використовується для відстеження стану мережевих пристроїв, серверів та інших елементів IT-інфраструктури [5].

Перевагами системи моніторингу Cacti вважають:

- відкритий вихідний код - є безкоштовним і відкритим програмним забезпеченням, що дозволяє користувачам модифікувати його відповідно до своїх потреб;

- простота встановлення та налаштування - відносно легко встановити і налаштувати, особливо для базового моніторингу і графічного відображення даних;

- графічне відображення - забезпечує потужні можливості для створення графіків і візуалізації даних, що дозволяє користувачам легко аналізувати мережеву активність і продуктивність;

- підтримка SNMP - підтримує, що робить його зручним для моніторингу мережевих середовищ для збору даних з мережевих пристроїв;

- масштабованість - підходить для моніторингу як невеликих, так і великих мереж, завдяки можливості додавання великої кількості графіків і джерел даних;

- шаблони та плагіни - містить велику кількість готових шаблонів і плагінів, що дозволяють розширювати функціонал і адаптувати систему до конкретних потреб.

До недоліків даної системи належать:

- обмежений функціонал моніторингу - здебільшого зосереджений на графічному відображенні даних і має обмежені можливості для активного моніторингу та управління інцидентами;

- складність у налаштуванні складних сценаріїв - базове налаштування досить просте, але налаштування складних сценаріїв моніторингу може бути складним і вимагати значних зусиль;

- інтерфейс користувача - може здаватися застарілим і не таким інтуїтивним, як у деяких сучасних систем моніторингу;

- вимоги до ресурсів - при моніторингу великої кількості пристроїв і даних може вимагати значних апаратних ресурсів для забезпечення ефективної роботи;

- відсутність автоматизації - не має вбудованих засобів автоматизації управління інцидентами і сповіщень, що може вимагати інтеграції з іншими системами для цих цілей.

Cacti є потужним інструментом для графічного відображення даних і базового моніторингу мережі, який особливо підходить для невеликих і середніх мережевих середовищ.

Його головною перевагою є можливість легко створювати графіки і візуалізувати дані, що робить його корисним для аналізу мережевої активності та продуктивності (рис 1.4). Проте, для більш складних завдань моніторингу і управління інцидентами можуть знадобитися додаткові

інструменти або інтеграції з іншими системами.

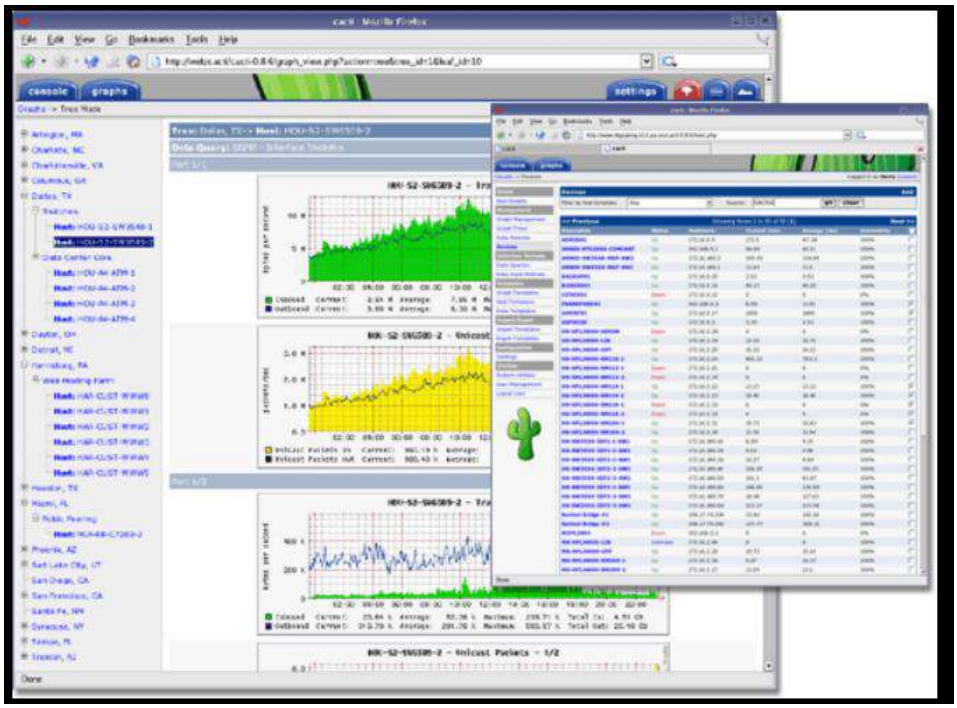


Рисунок 1.4 – Фрагмент моніторинг серверів та мережевих пристроїв у Cacti

Взявши до уваги всі вищеперелічені системи моніторингу було обрано систему Cacti з відкритим вихідним кодом, яка спеціалізується на зборі і візуалізації мережевих даних.

Важливі для замовника особливості Cacti:

- вільне ПЗ з відкритим кодом, написане на PHP та PQL;
- зберігання історії;
- працює в Windows та Linux;
- управління користувачами;
- потужна підтримка користувальницьких параметрів (порогів, оповіщень, реакцій).

Розглянувши обрани системи моніторингу мовно зробити порівняльний аналіз кожної із систем (табл. 1.1)

Таблиця 1.1 – Порівняння систем моніторингу обладнання ЛОМ

Показники	Системи моніторингу			
	Zabbix	NetXMS	Nagios	Cacti
Діаграми	Так	Так	Так	Так
SLA	Так	Так	Через плагін	Так
Логічне угруповання	Так	Так	Так	Так
Без агента	Підтримується	Так	Так	Ні
SNMP	Так	Так	Через плагін	Так
Syslog	Так	Через плагін	Через плагін	Через плагін (Syslog)
WMI	Так	Невідомо	Невідомо	Невідомо
NetFlow, s-Flow, j-Flow	Невідомо	Невідомо	Невідомо	Невідомо
Traffic Analisys	Невідомо	Невідомо	Невідомо	Невідомо
VoIP	Невідомо	Невідомо	Невідомо	Невідомо
Зовнішні скрипти	Так	Так	Так	Так
Плагіни	Так	Так	Так	Так
Складність створення плагінів	Легко	Складний	Легко	Середньо
Тригери / Тривоги	Так	Так	Так	Так
Доступ через Web	Повний доступ	Повний доступ	Перегляд, звіти, керування	Повний доступ
Розподілений моніторинг	Так	Так	Так	Невідомо
Метод зберігання даних	Oracle, MySQL, PostgreSQL	MySQL, PostgreSQL інші	Плоска база даних, SQL	RRDtool, MySQL, PostgreSQL
Ліцензія	GNU GPL	GNU GPL	GNU GPL	GNU GPL
Управління доступом	Так	Так	Так	Так

2 ХАРАКТЕРИСТИКА ПІДПРИЄМТСВА ТА ВИМОГИ ДО МОНІТОРНИГУ

2.1 Структура підприємства

Керівником центру інформатизації та нових технологій є директор. Під його керівництвом працює заступник директора, який відповідає за діяльність трьох відділів:

- адміністрація;

- відділ нових технологій;

- відділ інформатизації.

На даний момент підприємство надає технічну підтримку та сервісне обслуговування як підвідомчим установам, так і комерційним організаціям. Обслуговуються понад 300 робочих місць та більше 500 одиниць техніки.

Одночасно активно розвиваються такі напрями, як 3D моделювання, створення мультимедіа та друкованої продукції, онлайн-трансляції значущих подій в інтернеті. Організація також співпрацює з вищими навчальними закладами, бере участь у виставках, форумах та надає можливість студентам проходити виробничу практику, застосовуючи знання на практиці.

Види діяльності державної установи:

- діяльність у галузі електрозв'язку;

- розробка програмного забезпечення та консультування в цій галузі;

- створення і використання баз даних та інформаційних ресурсів, включаючи ресурси мережі Інтернет;

- консультування з апаратних засобів обчислювальної техніки;

- рекламна діяльність у сфері інформаційних технологій;

- надання інших послуг (робота з документами);

- технічне обслуговування та ремонт офісного обладнання та обчислювальної техніки;

- монтаж, ремонт та технічне обслуговування іншого електроустаткування, не включеного до інших категорій;

- виробництво фільмів, кліпів та відеовступів;

- монтаж інженерного обладнання;

- наукові дослідження та розробки у галузі природних та технічних наук;

- надання послуг у сфері міжсистемного зв'язку;

- оренда офісної техніки, включаючи обчислювальну техніку;

- створення та розвиток (модернізація) інформаційних систем та компонентів інформаційно-телекомунікаційної інфраструктури;

- технічний супровід та експлуатація, виведення з експлуатації

інформаційних систем та компонентів інформаційно-телекомунікаційної інфраструктури;

- надання програмного забезпечення, інженерної, обчислювальної та інформаційно-телекомунікаційної інфраструктури, включаючи рішення на основі «хмарних технологій».

2.2 Мережева характеристика підприємства

ЛОМ – це мережі, призначені для обробки, зберігання та передачі даних, які складаються з кабельної системи об'єкта (будівлі) або групи об'єктів (будівель).

Мережеве обладнання поділяється на пасивне та активне.

Активне обладнання включає електронні пристрої, які отримують живлення від електричної мережі або інших джерел і виконують функції посилення, перетворення сигналів тощо. Пасивне обладнання не потребує живлення від мережі і виконує функції розподілу або зниження рівня сигналу.

До активного обладнання належать [6]:

- мережевий адаптер
- концентратор;
- міст;
- комутатор (switch);
- маршрутизатор (роутер).

До пасивного обладнання належать:

- мережевий адаптер;
- репітер;
- мережевий концентратор;
- мережевий комутатор.

Мережева архітектура складається з наступних компонентів (рис. 2.1):

- апаратний гіпервізор vSphere ESXi Hypervisor, який встановлюється на фізичний сервер і ділить його на кілька віртуальних машин, на відміну від інших гіпервізорів, керування платформою vSphere здійснюється за допомогою засобів віддаленого керування;

- доменні служби Active Directory Server (ADS), які зберігають дані каталогу та керують обміном даними між користувачами та доменами, включаючи процеси входу користувачів, автентифікацію та пошук у каталозі;

- сервер у комп'ютерних мережах Proxy Server, який дозволяє клієнтам виконувати непрямі запити до інших мережних служб;

- багатофункціональний пристрій HP LaserJet Pro 400 MFPM425dn, що може використовуватися як продуктивний принтер, автоматичний сканер, копір або факс;

- багатофункціональна система Konica Minolta C224e, яка включає лазерний принтер та інші пристрої "все-в-одному";

- websmart комутатор D-link-DGS 1210-10p, що має розширені функції управління та безпеки, забезпечуючи кращу продуктивність і масштабованість;

- настільний принтер ECOSYS P2035d, компактний пристрій із функцією двостороннього чорно-білого друку в стандартній комплектації;

- багатофункціональний пристрій Kyocera 1035 формату A4;

- 4 IP-телефони, 2 відеокамери та 2 Wi-Fi точки доступу Ubiquiti.

Взаємодія між обладнанням кабінетів здійснюється за допомогою оптичного каналу зв'язку.

Для передачі даних з провайдером використовується мережевий протокол канального рівня PPP через Ethernet.

Мережева архітектура підприємства зображена на рисунку 2.1.

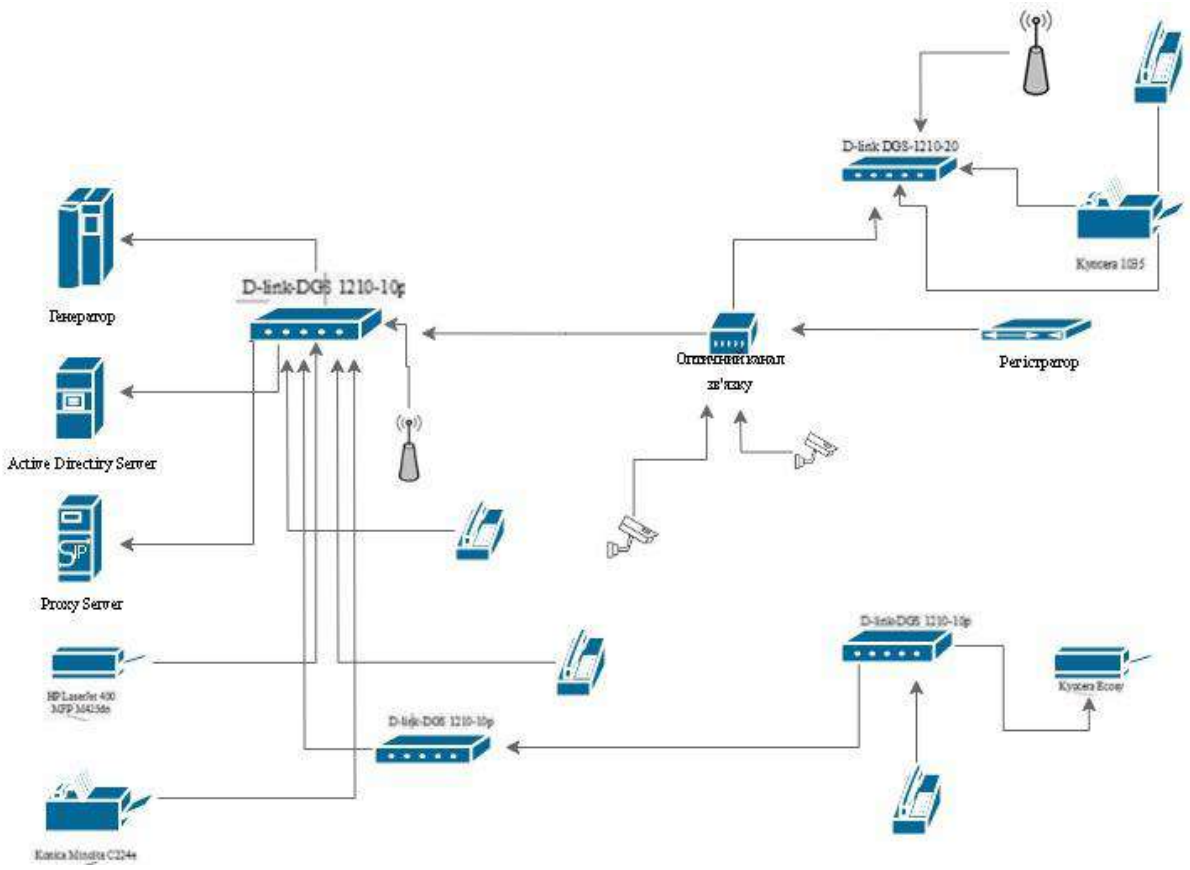


Рисунок 2.1 - Мережева архітектура підприємства

У таблиці 2.1 наведено програмні засоби з описом їх функцій. В установі використовується наступне обладнання компанії Cisco, для якого необхідно розробити систему моніторингу:

- комутатор SRW2008;
- комутатор AIR-AP1852I;
- роутер SPZ504G;
- комутатор R200-FOW34;
- роутер DS22-AIR500;
- маршрутизатор WS-2334F-22WE;
- маршрутизатор QER3-22FF;
- комутатор SPA124;
- комутатор SPA40GP;
- роутер CTS-GE44;
- маршрутизатор GE1R-2442.

Програмні продукти, які використовує підприємство у своїй роботі представлені у таблиці 2.1

Таблиця 2.1 – Програмні засоби

	Програмні засоби	Опис
1	Microsoft Windows: Pro, 7 Enterprise,8.1Pro, 8.1 Enterprise, 10 Linux (ubuntu)	Операційна система
2	Ubuntu Server 20.04	Серверна операційна система компанії
3	Skype	Безкоштовне програмне забезпечення з закритим кодом, що забезпечує текстовий, голосовий та відеозв'язок через Інтернет між комп'ютерами.
4	Proxy server firewallkerio	Програмний міжмережевий екран, розроблений компаніями Kerio Technologies та Tiny Software.
5	VMware vSphereHypervisor 5.0	Програмний продукт для віртуалізації рівня підприємства
6	Vip Net	Комплексний підхіддо забезпечення ІБ
7	Система Справа	Система електронного документообігу
8	Mozilla thunderbird	Безкоштовна програма для роботи з електронною поштою та групами новин, що вільно розповсюджується.
9	Mozila FireFox	Вільний браузер, розробкою та поширенням якого займається Mozil aCorporation
10	Advanced IP-scanner	Швидкий, надійний та зручний сканер IP-адрес для Windows.
11	7Zip	Вільний файловий архіватор з високим ступенем стиснення даних
12	TeamViewer 12	Інтелектуальне рішення, яке тісно інтегрується з бізнес-середовищем, забезпечуючи уніфікований та ефективний інтерфейс користувача.

У стандартному кабінеті розташовано п'ять робочих місць, що включають один комп'ютер та інше обладнання, необхідне роботи. Устаткування ЛОМ різне за призначенням, але тісно пов'язане між собою компонентами, що забезпечують високу продуктивність та безперебійність функціонування мереж. Це обладнання можна поділити на такі категорії, як активне, пасивне, комп'ютерне та периферійне обладнання. Моніторинг необхідний для того, щоб можна було стежити за обладнанням, оскільки воно може зламатися або дати збій будь-якої миті. Дистанційний моніторинг дозволяє стежити за обладнанням із будь-якого місця, головне – мати

відповідні права.

2.3 Вимоги до моніторингу

Моніторинг мережного устаткування – це система, орієнтована збір і аналіз інформації, що дозволяє виявляти внутрішні проблеми у роботі устаткування.

Моніторинг – віддалене стеження працездатністю деякого устаткування.

Вибір методів і об'єктів моніторингу залежить від багатьох чинників – конфігурації мережі [7], які у ній сервісів і служб, конфігурації серверів і встановленого ними ПЗ, можливостей ПЗ, що використовується для моніторингу:

- перевірка фізичної доступності устаткування;
- визначення ключових параметрів або показників, які будуть вимірюватися чи спостерігатися;
- перевірка стану занедбаних служб і сервісів;
- детальна перевірка не критичних, але важливих параметрів функціонування: продуктивності, завантаження тощо;
- перевірка параметрів, специфічних сервісів і служб даного конкретного оточення (наявність деяких значень у таблицях БД, вміст лог-файлів).

Вибір методів і об'єктів моніторингу залежить від конкретних цілей, вимог і характеристик вашої інфраструктури.

Засоби, які застосовуються для моніторингу та аналізу обчислювальних мереж, можна розділити на кілька класів [8]:

- системи управління мережею (Network Managemen tSystems) - програмні системи, що збирають дані про стан вузлів та комунікаційних пристроїв мережі, а також дані про трафік, що циркулює в мережі;
- засоби управління системою (System Management) - засоби, що часто

виконують функції, аналогічні функцій систем управління, але по відношенню до інших об'єктів;

- вбудовані системи діагностики та управління (Embeddedsystems) - системи, що виконуються у вигляді програмно-апаратних модулів, що встановлюються в комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційну систему;

- аналізатори протоколів (Protocolanalyzers) – програмні чи апаратно-програмні системи, обмежуються на відміну систем управління лише функціями моніторингу та аналізу трафіку в мережах.

SNMP (Simple Network Management Protocol) – це найпоширеніший протокол керування мережами. Підтримується сотнями виробниками. Його головні переваги – простота, доступність, незалежність від виробників.

Агент у протоколі SNMP – це обробний елемент, який забезпечує менеджерам, розміщеним на керуючий станціях мережі, доступом до значенням змінних MIB, і цим дає можливість реалізовувати функції з управління і спостереженню пристроями.

Враховуючи всі вищеописані вимоги до моніторингу, було вирішено використовувати Ubuntu Server 20.04.

2.4 Характеристика Ubuntu Server 20.04

Ubuntu Server 20.04, розроблена компанією Canonical, є однією з найпопулярніших операційних систем з відкритим вихідним кодом для серверних рішень. Вона отримала довгострокову підтримку (LTS), що робить її надійним вибором для підприємств будь-якого масштабу. Ця версія поєднує в собі новітні технології та поліпшення, спрямовані на підвищення продуктивності, безпеки та керованості.

Одна з найважливіших характеристик Ubuntu Server 20.04 – це

довгострокова підтримка (Long Term Support, LTS), яка гарантує оновлення та виправлення безпеки протягом п'яти років з моменту випуску. Це забезпечує стабільність та надійність, що є критично важливим для корпоративних середовищ, де відмовостійкість та безпека мають першорядне значення. Окрім стандартного п’ятирічного циклу підтримки, Canonical також пропонує можливість розширеної підтримки (Extended Security Maintenance, ESM) до десяти років, що робить Ubuntu Server 20.04 ще привабливішим для довгострокових проектів.

Ubuntu Server 20.04 активно інтегрує сучасні технології та підходи, що дозволяє забезпечити гнучкість та ефективність управління інфраструктурою. Серед них:

- контейнеризація з Docker дозволяє ізолювати додатки у контейнери, що сприяє кращій портативності, масштабованості та ефективному використанню ресурсів;

- оркестрація з Kubernetes Ubuntu Server 20.04 підтримує Kubernetes, що полегшує управління контейнеризованими додатками у масштабованих середовищах;

- автоматизація з Ansible Ansible дозволяє автоматизувати конфігурацію систем, розгортання додатків та управління IT-інфраструктурою, що суттєво знижує витрати часу та ресурсів.

Безпека є критично важливою складовою будь-якої серверної ОС. Ubuntu Server 20.04 пропонує низку інструментів і функцій для забезпечення високого рівня захисту:

- AppArmor Інструмент для забезпечення контролю доступу, що дозволяє обмежити можливості додатків, навіть якщо вони скомпрометовані;

- UFW (Uncomplicated Firewall), простий у використанні інструмент для налаштування брандмауера, що забезпечує базовий захист мережевих підключень;

- оновлення без перезавантаження (Livepatch), ця функція дозволяє встановлювати критичні оновлення ядра без необхідності перезавантаження

системи, що є надзвичайно важливим для високонавантажених серверів.

Ubuntu Server 20.04 має одну з найбільших спільнот користувачів та розробників, що сприяє швидкому вирішенню проблем і постійному вдосконаленню системи. Крім того, багатий репозиторій програмного забезпечення дозволяє легко встановлювати та оновлювати тисячі додатків, що забезпечує гнучкість та адаптивність системи під конкретні потреби користувачів.

Ubuntu Server 20.04 підтримує оптимізовані версії для різних архітектур, включаючи ARM і x86, що дозволяє ефективно використовувати ресурси серверів різних типів. Це особливо корисно для середовищ з високою щільністю серверів та обмеженими ресурсами, таких як дата-центри або хмарні середовища.

Ubuntu Server 20.04 забезпечує глибоку інтеграцію з основними хмарними платформами, такими як AWS, Azure, Google Cloud, а також з приватними хмарними рішеннями на базі OpenStack. Це дозволяє легко розгортати та керувати серверними ресурсами в хмарі, забезпечуючи при цьому високий рівень продуктивності та надійності.

Ubuntu Server 20.04 має інтуїтивно зрозумілий інсталятор, який дозволяє швидко встановити систему навіть користувачам з мінімальним досвідом. Зручні команди для керування пакетами через apt спрощують процес встановлення та оновлення програмного забезпечення, роблячи його швидким та ефективним.

Система пропонує потужні інструменти командного рядка, що дозволяють адміністратору ефективно керувати сервером. Віддалене керування через SSH дозволяє здійснювати адміністративні завдання з будь-якої точки світу, що забезпечує гнучкість та оперативність у вирішенні проблем.

Ubuntu Server 20.04 підтримує сучасні файлові системи, такі як ZFS та Btrfs, які забезпечують високу надійність та гнучкість у керуванні даними. Ці файлові системи пропонують такі можливості, як знімки (snapshots), що дозволяють легко створювати резервні копії та відновлювати дані у випадку

збоїв.

Ubuntu Server 20.04 забезпечує підтримку популярних технологій віртуалізації, включаючи KVM, LXD, та QEMU. Це дозволяє створювати та керувати віртуальними машинами та контейнерами з високою ефективністю, забезпечуючи гнучкість у розподілі ресурсів та підвищуючи продуктивність серверів.

Система добре інтегрується з інструментами для автоматизації та DevOps, такими як Terraform та Jenkins. Це сприяє автоматизації процесів розгортання та управління інфраструктурою, що дозволяє значно знизити витрати часу та ресурсів на адміністрування серверів.

Ubuntu Server 20.04 підтримує сучасні мережеві протоколи та технології, такі як IPv6, VLAN, та програмно-визначені мережі (SDN). Це забезпечує високий рівень гнучкості та масштабованості мережевої інфраструктури, дозволяючи ефективно управляти мережевими ресурсами та підвищувати продуктивність.

Система забезпечує зворотну сумісність, що дозволяє плавно переходити з попередніх версій Ubuntu Server без втрати даних та налаштувань. Це робить процес оновлення простішим і менш ризикованим для організацій, що використовують попередні версії ОС.

Ubuntu Server 20.04 підходить як для малих бізнесів, так і для великих підприємств, забезпечуючи високу продуктивність у різних умовах експлуатації. Завдяки підтримці масштабованих рішень та оптимізації використання ресурсів, ця версія може ефективно працювати у високонавантажених середовищах, забезпечуючи стабільну та надійну роботу серверів.

Ubuntu Server 20.04 є потужною, гнучкою та надійною операційною системою, яка пропонує широкий спектр функцій для ефективного управління IT-інфраструктурою. Її довгострокова підтримка, інтеграція сучасних технологій, висока безпека та продуктивність роблять її відмінним вибором для організацій будь-якого масштабу. Завдяки активній спільноті користувачів і

розробників, Ubuntu Server 20.04 постійно вдосконалюється, забезпечуючи актуальність та надійність у сучасному IT-середовищі.

Ubuntu Server 20.04 є одним із найпопулярніших виборів для встановлення системи моніторингу Cacti завдяки своїй стабільності, безпеці та активній підтримці [9].

Ось основні характеристики Ubuntu Server 20.04, які роблять його придатним для цього завдання:

а) стабільність і підтримка:

1) Ubuntu Server 20.04 є версією з довготривалою підтримкою (LTS), що гарантує оновлення безпеки та підтримку протягом п'яти років;

2) регулярні оновлення та патчі забезпечують високу стабільність системи;

б) безпека:

1) вбудовані функції безпеки, такі як AppArmor і підтримка брандмауера UFW (Uncomplicated Firewall), допомагають захистити сервер від загроз;

2) регулярні оновлення безпеки для захисту від нових вразливостей;

в) продуктивність:

1) оптимізована для серверних середовищ, що забезпечує високу продуктивність та ефективне використання ресурсів;

2) підтримка новітнього обладнання та технологій;

г) простота адміністрування:

1) добре задокументована система з великою кількістю доступних ресурсів і підтримки спільноти;

2) можливість автоматизації завдань за допомогою інструментів, таких як Ansible, Puppet або Chef;

д) пакетний Менеджер APT:

1) легкий доступ до великої кількості програмного забезпечення через офіційні репозиторії;

2) зручне управління залежностями і оновленнями;

е) віртуалізація і контейнери:

1) підтримка віртуалізації (KVM, QEMU) та контейнеризації (Docker, LXC), що дозволяє розгорнути ізольовані середовища для різних додатків.

Ubuntu Server 20.04 надає надійну та ефективну платформу для розгортання Cacti, що забезпечує моніторинг мережі та серверів, збір і аналіз даних, а також створення графіків продуктивності.

3 РОЗРОБКА СИСТЕМИ ДИСТАНЦІЙНОГО МОНІТОРИНГУ У CACTI

3.1 Налаштування мережного обладнання для моніторингу

Для моніторингу працездатності мережного обладнання необхідно підключити комутатор до комп'ютера та налаштувати віддалений доступ SSH.

Підключення до комутатора здійснюється за допомогою кабелю RJ-45 - RS 232, RS 232 – USB. Для знаходження кабелю RS 232 необхідно мати драйвер HL–340 USBtoCOM [10].

Для налаштування віддаленого доступу SSH змінимо ім'я (рис 3.1) нашого комутатора (за промовчанням ім'я Switch на *Switch01*).

```
Switch# configure terminal
Switch (config) # hostname Switch01
Switch01 (config) #.
```

Рисунок 3.1 - Зміна ім'я комутатора

Задаємо IP-адресу для інтерфейсу управління комутатором, для цього вказуємо інтерфейс для налаштування, а потім задаємо IP–адресу та маску (рис 3.2).

```
Switch01(config)# interface fa0/0
Switch01(config-if)# ip address 192.168.0.1 255.255.255.0
```

Рисунок 3.2 - Інтерфейс для налаштування

Далі включаємо інтерфейс, а потім виходимо з режиму конфігурації (рис 3.3) інтерфейсу Switch01 (config) #.

```
Switch01(config-if)# no shutdown
Switch01(config-if)# exit
Switch01 (config) #
```

Рисунок 3.3 - Режим конфігурації

Потім встановимо пароль для привілейованого режиму (рис 3.4):

```
Switch01(config)# enable secret pass1234
Switch01(config)# exit
Switch01 #
```

Рисунок 3.4 - Встановлення пароль

Налаштування SSH повинно починатись з процедури установки точного часу й дати (рис 3.5).

```
Switch01# clock set 12:00:00 1 June 2024
Switch01# conf t
```

Рисунок 3.5 - Встановлення точного час дату

Далі вказуємо домен, або пишемо, те що зображено на рисунку 3.6.

```
Switch01(config)# ip domain name geek-nose.com
```

Рисунок 3.6 - Вказується домен

Після цього виконуємо генерацію RSA-ключа для ssh (рис 3.7)

```
Switch01(config)# crypto key generate rsa
```

Рисунок 3.7 - Генерація RSA-ключа

Далі вказуємо версію SSH-протоколу (рис 3.8).

```
Switch01(config)# ip ssh version 2() Switch01(config)# ip ssh
```

Рисунок 3.8 - Версія SSH-протоколу

Потім додаємо кількість спроб підключення по SSH (рис 3.9).

```
autentification-retries 3
```

Рисунок 3.9 - Кількість спроб підключення

Після цього зберігаємо паролі у зашифрованому вигляді (рис 3.10).

```
Switch01(config)# service password-encryption
```

Рисунок 3.10- Паролі у зашифрованому вигляді

Далі переходимо до режиму конференції термінальних ліній (ліст3.11).

```
Switch01(config)# line vty 0 4
```

Рисунок 3.11 - режиму конференції

Потім дозволяємо підключення тільки за SSH (рис 3.12).

```
Switch01(config-line)# transport input ssh
```

Рисунок 3.12 - Підключення тільки за SSH

Далі активуємо автоматичне роз'єднання ssh-сесії через 25 хвилин (рис. 3.13).

```
Switch01(config-line)# exec timeout 25
```

Рисунок 3.13 - Автоматичне роз'єднання ssh-сесії

Після цього виходимо з режиму конфігурування (рис. 3.14).

```
Switch01 (config-line) # end
```

Рисунок 3.14 - Режиму конфігурування

Проводимо зберігаємо налаштування (рис 3.15).

```
Switch01# copy running-config startup-config
```

Рисунок 3.15 – Збереження налаштування

Таким самим чином виконуємо налаштування SSH (рис. 3.16). Для початку включаємо AAA протокол , потім створюємо користувача root, з максимальним рівнем привілеїв – 15, пароль pass1234 і правило доступу з назвою 01, що регламентують право заходити по SSH [11].

```
Switch01# conf t Switch01(config)# aaa new-model
Switch01(config)# username root privilege 15 secret pass1234
Switch01(config)# access-list 01 permit 192.168.0 0.0.0.255
```

Рисунок 3.16 - Налаштування SSH

Далі вказуємо перехід у режим конфігурації термінальних ліній (рис 3.17), із дозволом до входу відразу в привілейований режим та прив'язуємо створене правило доступу SSH до термінальної лінії [12]:

```
Switch01(config)# line vty 0 2
Switch01(config-line)# privilege level 15
Switch01(config-line)# access-class 23 in
Switch01(config-line)# logging synchronous
```

Рисунок 3.17 - Режим конфігурації термінальних ліній

Для відключення журнальних повідомлень наступною командою, коли комутатор чекає завершення команди, що вводиться, а також виведення звіту про її виконання, виконаємо наступні налаштування, починаючи з моменту виходу з режиму конфігурування (рис3.18).

```
Switch01 (config-line)# end
```

Рисунок 3.18 – Режим конфігурування

Далі зберігаємо налаштування (рис. 3.19)

```
Switch01# copy running-config startup-config
```

Рисунок 3.19 - режиму конференції

При необхідності термінового виправлення установок обладнання (рис. 3.20) знадобиться скидання пароля. Щоб його зробити, необхідно виконати такі дії, при натиснутій кнопці вибору режиму (mode) вставити шнур живлення (не відпускати кнопку, доки індикатор над портом 1, не горітиме, як мінімум 2 секунди) і ввести наступні команди:.

```
flash_init
load_helper
config.text
rename flash:config.text flash:config.old
enable
rename flash:config.old flash:config.text
copy startup run
conf t
copy run startup
```

Рисунок 3.20 - Виправлення установок обладнання

Наступний етап це вимкнення VTP. VLAN Trunking Protocol (VTP) — пропрієтарний протокол компанії Cisco Systems, призначений для створення,

видалення та перейменування VLAN на мережевих пристроях [13]. Режими роботи протоколу:

- Server (режим по замовчування) генерує оголошення VTP і передає оголошення з інших комутаторів;

- Client передає оголошення з інших комутаторів;

- Transparent не генерує оголошення VTP, передає оголошення з інших комутаторів.

Для перегляду інформації про налаштування VTP зробимо наступний запис (рис. 3.21).

```
sw# show vtp status
sw# show vtp added
counters sw# show vtp
password
```

Рисунок 3.21 - Інформація про налаштування VTP

3.2 Налаштування Ubuntu Server 20.04

На нашому підприємстві вже є встановлений Ubuntu Server версії 20.04. При необхідності можна також встановити систему за допомогою віртуального диску [14].

Для віддаленого керування буде потрібний SSH сервер, на рисунку 3.22 представлено фрагмент вибору програмного забезпечення.

Далі необхідно перевірити налаштування мережі. Відкриємо налаштування мережевих карток nano /etc/network/interfaces (рис. 3.23).

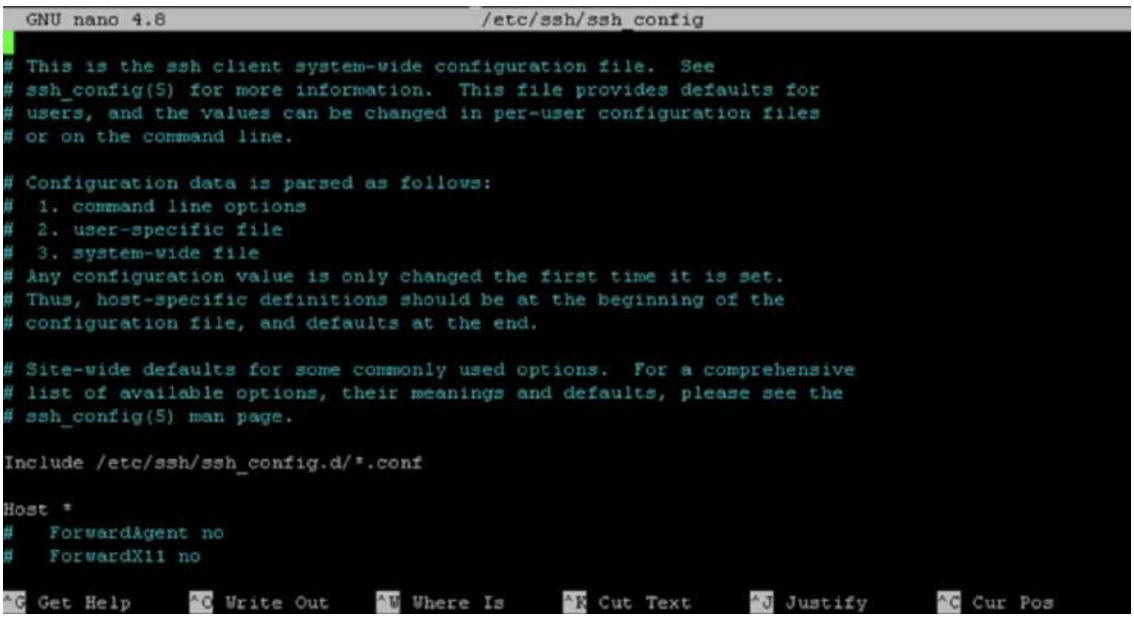


Рисунок 3.22 – Фрагмент вибору програмного забезпечення (SSH сервер)

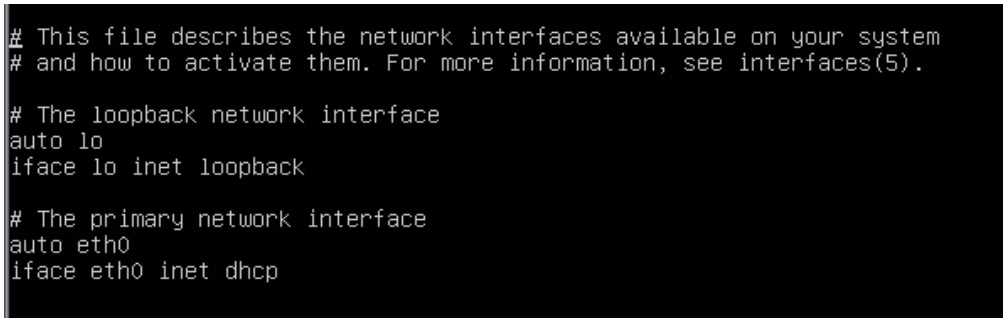


Рисунок 3.23 – Фрагмент перевірки налаштувань мережі

Як бачимо, у нашому випадку мережна адреса інтерфейс eth0 отримує DHCP.

Щоб дізнатися IP адресу, необхідно виконати команду ip addr.

Для перезапуску мережі вводимо в терміналі по черзі кожну з рядків (рис. 3.24).

```
Ifdown eth0
Ifup eth0
```

Рисунок 3.24 – Перезапуск мережі

Тепер перевіримо мережу, провевши пінгування будь-який вузол, наприклад google.com, командою ping google.com (рис. 3.25).

```
PING google.com (74.125.232.238) 56(84) bytes of data.
64 bytes from google.com (74.125.232.238): icmp_seq=1 ttl=58 time=60.3 ms
64 bytes from google.com (74.125.232.238): icmp_seq=2 ttl=58 time=67.6 ms
64 bytes from google.com (74.125.232.238): icmp_seq=3 ttl=58 time=65.0 ms
64 bytes from google.com (74.125.232.238): icmp_seq=4 ttl=58 time=67.6 ms
64 bytes from google.com (74.125.232.238): icmp_seq=5 ttl=58 time=65.1 ms
64 bytes from google.com (74.125.232.238): icmp_seq=6 ttl=58 time=62.6 ms
```

Рисунок 3.25 – Фрагмент перевірки зв'язку з google.com

На цьому перевірка Ubuntu Server завершено. На наступному етапі необхідно встановити Cacti версії 1.2.9.

3.3 Встановлення та налаштування Cacti 1.2.9 на Ubuntu Server 20.04

Почнемо з підключенням до віртуальної машини через SSH [15]. Для цього потрібно завантажити PuTTY(рис. 3.26).

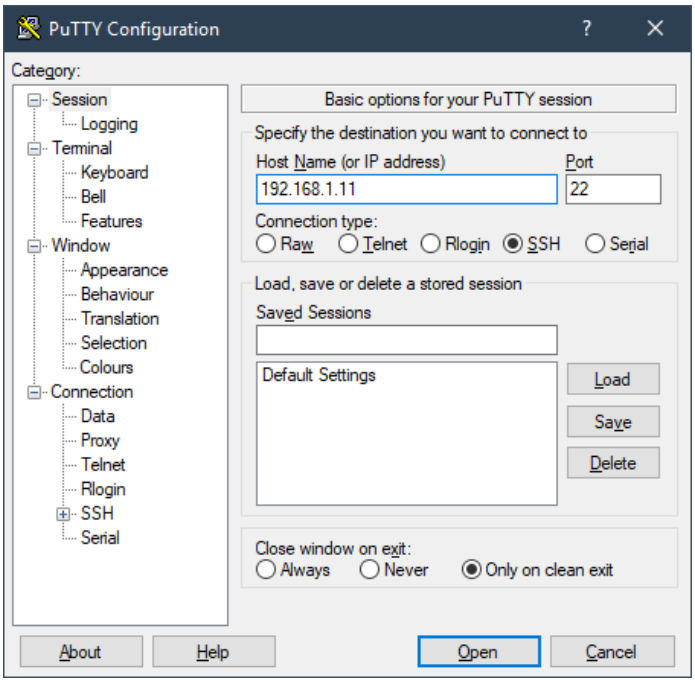


Рисунок 3.26 – Фрагмент підключення до віртуальної машини через SSH

Для встановлення Cacti на Ubuntu Server 20.04 необхідні наступні кроки,

починаючи з встановлення Apache, PHP і MySQL/MariaDB (рис. 3.27).

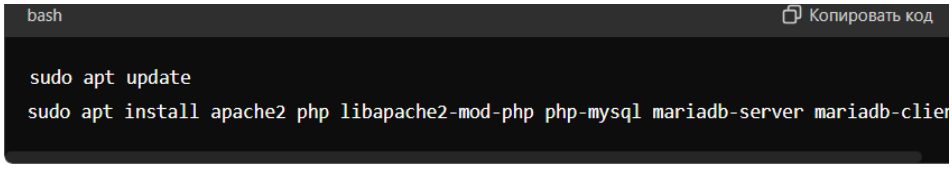


Рисунок 3.27 – становлення Apache.

Далі потрібно налаштування MySQL/MariaDB (рис. 3.28).

Рисунок 3.28 – Налаштування MySQL.

Після цього встановлення додаткових PHP-розширень (рис. 3.29).

Рисунок 3.29 – встановлення додаткових PHP-розширень.

Врешті решт, встановлення SNMP і RRDtool (рис. 3.29).

Рисунок 3.29 – Встановлення SNMP і RRDtool.

Наприкінці, відкриваємо веб-браузер і переходимо до `http://<ваш_сервер>/cacti`, при цьому дотримуємось вказівок на екрані для завершення налаштування та встановлення і налаштування Cacti (рис. 3.30).

Рисунок 3.30 – Встановлення і налаштування.

Для підвищення прав виконуємо команду `su`. Прі стандартному налаштуванні повноважень для файлів у Linux, звичайний користувач може:

- читати, писати та змінювати атрибути файлів у своєму каталозі;

- читати, писати, змінювати атрибути файлів у каталозі /tmp;

- виконувати програми там, де це не заборонено за допомогою прапора noexec;

- читати файли, для яких встановлений прапор читання для всіх користувачів.

Якщо необхідно зробити щось більше, нам знадобляться права `root` користувача linux. який має право робити все у файловій системі незалежно від того, які права встановлені на файл. Необхідно буде ввести пароль `root'a` (рис. 3.31).

Рисунок 3.31 – Фрагмент підвищення прав до суперкористувача

Тепер переходимо до встановлення та встановлюємо необхідні пакети [16]:

```
apt-get install apache2 php5 php5-mysql php5-snmp snmp php5-gd
rrdtool mysql-server php5-ldap zip unzip
```

Задаємо пароль для MySQL (рис. 3.32):

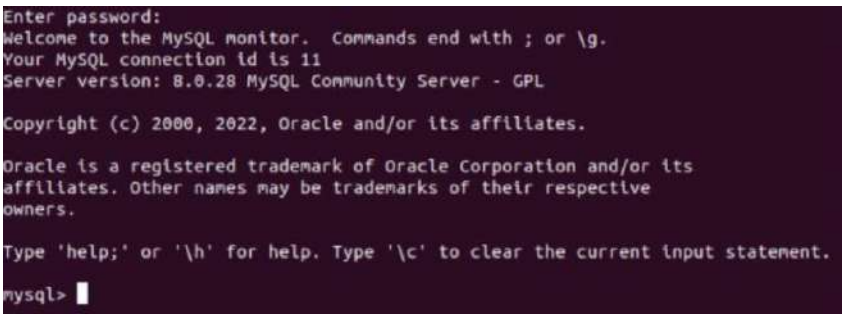


Рисунок 3.32 – Фрагмент встановлення пароля для MySQL

Далі перевіряємо чи всі необхідні для роботи Cacti PHP модулі. Їх має бути, як мінімум сім (рис. 3.33).

```
php –m | egrep '^(mysql|snmp|xml|session|sockets|ldap|gd)$'
gd
ldap
mysql
session
snmp
sockets
xml
```

Рисунок 3.33 – Фрагмент встановлення пароля для MySQL

За наявності потрібних модулів завантажуємо вихідний код Cacti та розпаковуємо його в локальну папку (рис. 3.34).

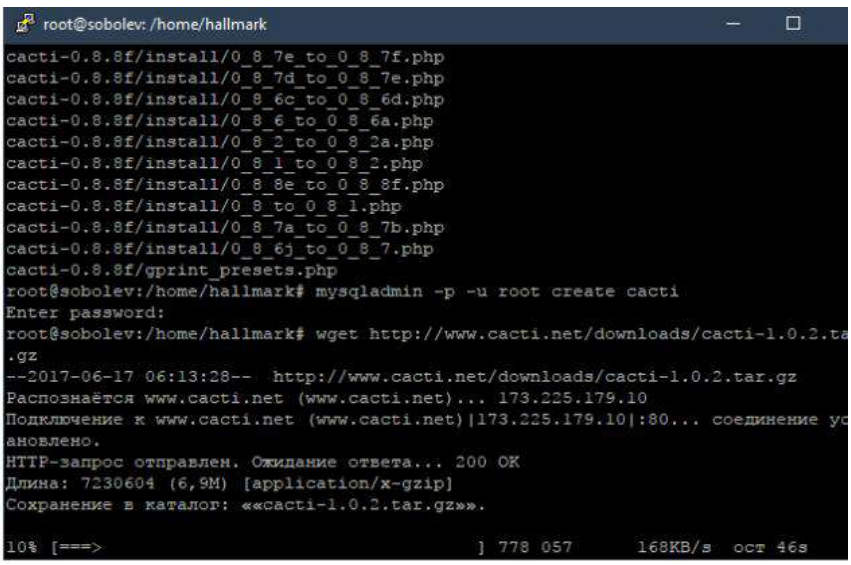


Рисунок 3.34 – Фрагмент скачування та розпакування вихідного коду

Переходимо до підготовці MySQL бази даних. Створимо БД і заповнимо структуру створеної бази Cacti (рис. 3.35).

```
root@sobolev:/home/hallmark# mysql -p -u root cacti < cacti-1.0.2/cacti.sql
Enter password:
root@sobolev:/home/hallmark#
```

Рисунок 3.35 – Фрагмент створення БД та заповнення структури Cacti бази

Робота з базою даних завершена, тепер прописуємо налаштування коннекту до БД у конфігурації Cacti (рис. 3.36).

```
vim cacti-1.2.9/include/config.php
$ database_type = " mysql "
$database_default = "cacti"
$database_hostname = "localhost"
$database_username = "cactivor"
$database_password = "your_password"
$database_port = "3306"
$ database_ssl = false
```

Рисунок 3.36 – Робота з базою даних

Залишилося додати Cron для роботи Poller-а та поставити йому права на виконання. Cron - це системний планувальник, який запускає PHP - скрипт кожні 5 хвилин, щоб Cacti зміг знімати дані з усього обладнання. Після цього необхідно перезавантажити веб-сервер (рис 3.37).

Наступна установка Cacti буде проходити через веб-інтерфейс по засланні http://192.168.1.11/cacti/.

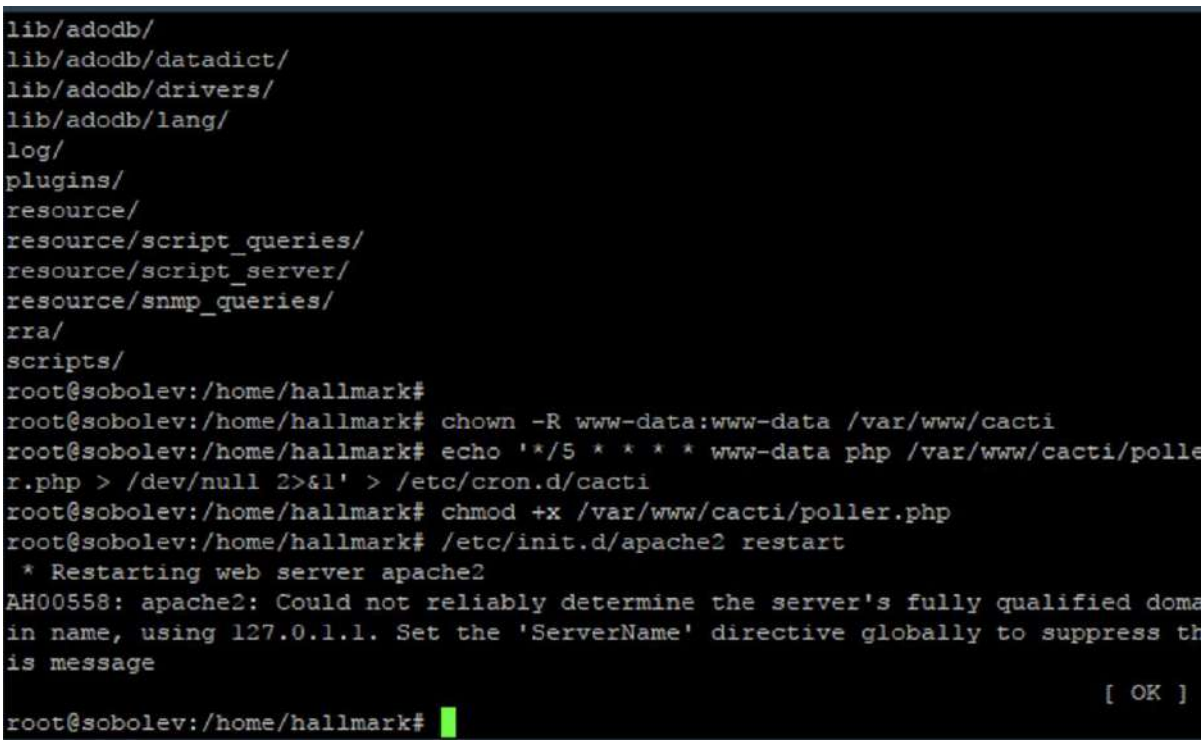


Рисунок 3.37 – Фрагмент додавання cron та перезавантаження веб-сервера

При переході побачимо таке вікно (рис. 3.38).

Натискаючи кнопку «Next» переходимо до наступного етапу. Тут просто тиснемо кнопку Finish (рис. 3.39).

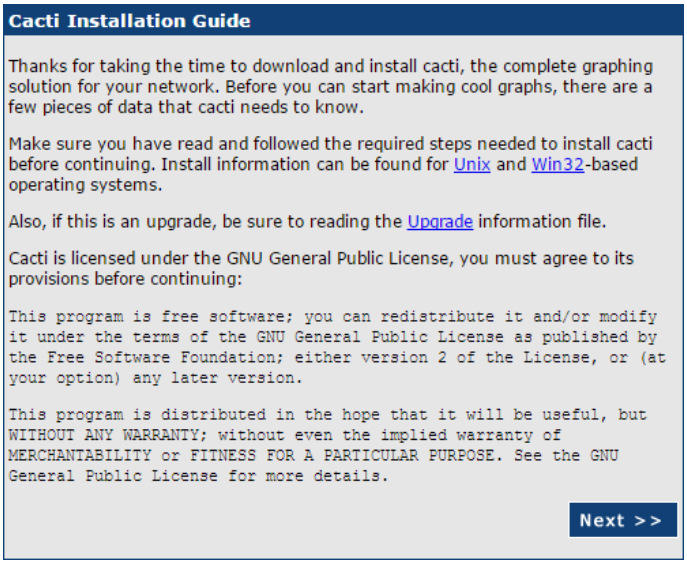


Рисунок 3.38 - Фрагмент початкового налаштування веб-інтерфейсу Cacti

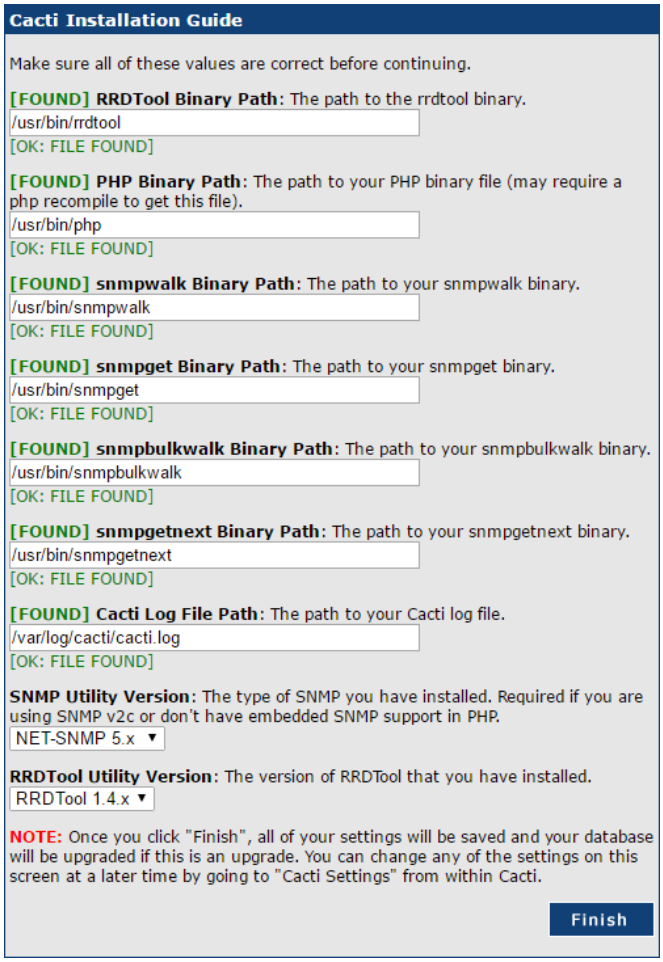


Рисунок 3.39 - Фрагмент закінчення початкового налаштування веб-інтерфейсу Cacti

Далі вводимо логін/пароль для входу до веб-інтерфейсу Cacti. Типово: admin/admin. Відразу знадобиться змінити пароль, що необхідно зробити (рис. 3.40).

Рисунок 3.40 – Фрагмент форми входу до веб-інтерфейсу Cacti

Після введення нового пароля потрапите до Cacti GUI (інтерфейс користувача). Тепер Cacti готовий до роботи (рис. 3.41).

Далі встановимо "spine poller" під Cacti 1.2.9. Poller - це програма, яка викликає "Spine", альтернативний метод запитів даних, написаний на C.

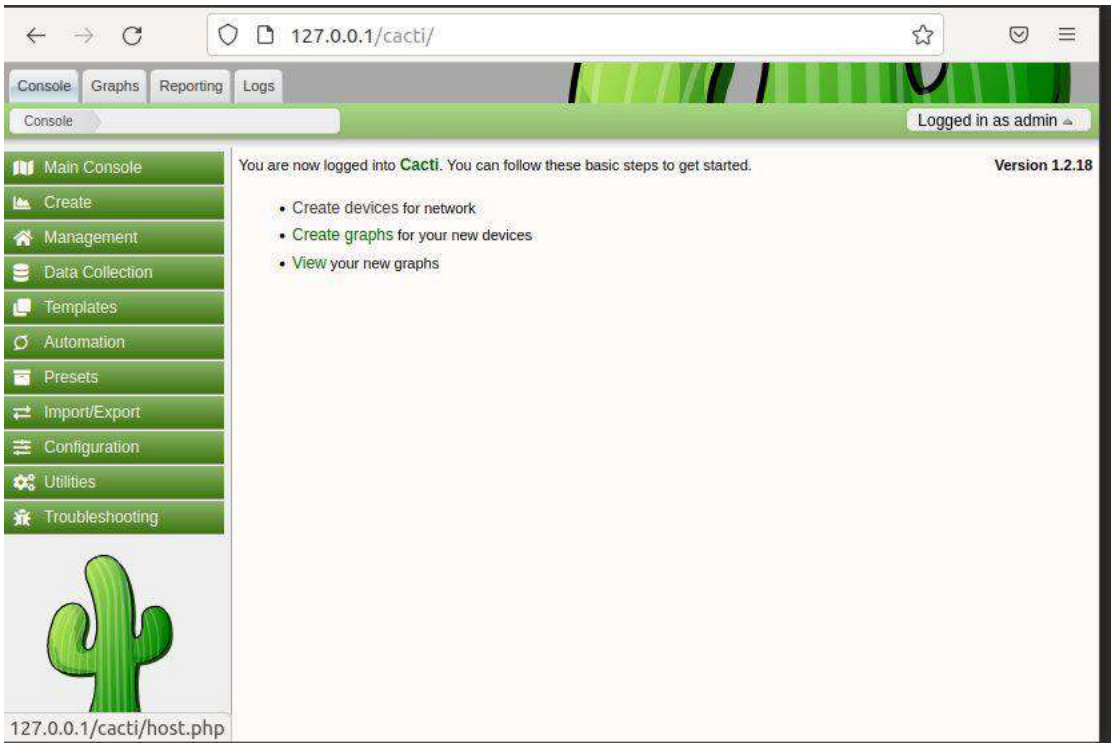


Рисунок 3.41 – Панель керування Cacti 1.2.9

Завантажуємо та розпаковуємо в локальну папку командою:

```
wgethttp://www.cacti.net/downloads/spine/cacti-spine-1.2.9.tar.gz
tar xzvf cacti-spine-1.2.9.tar.gz
```

Встановлюємо потрібні для компіляції пакети і виконуємокомпіляцію:

```
apt-get install libmysqlclient-dev libsnmp-dev automake libtool make
```

Активуємо новий тип Poller для цього зайдемо до демо у вкладку Poller та вибираємо spine (рис. 3.42).

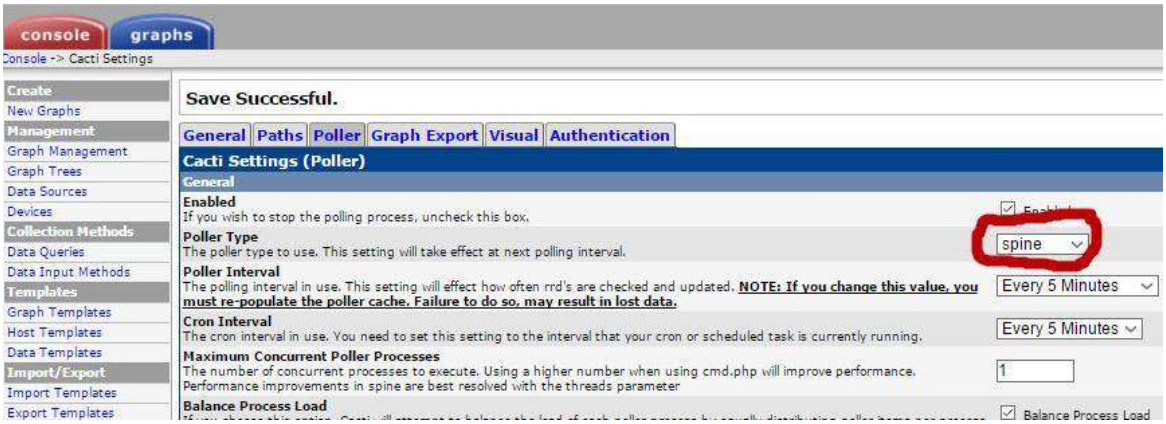


Рисунок 3.42 – Фрагмент вказівки типу Poller

Після цього все зберігаємо, чекаємо пару хвилин і переглядаємо лог-сторінку на наявність помилок Utilities - System Utilities - View Cacti Log File (рис. 3.43).

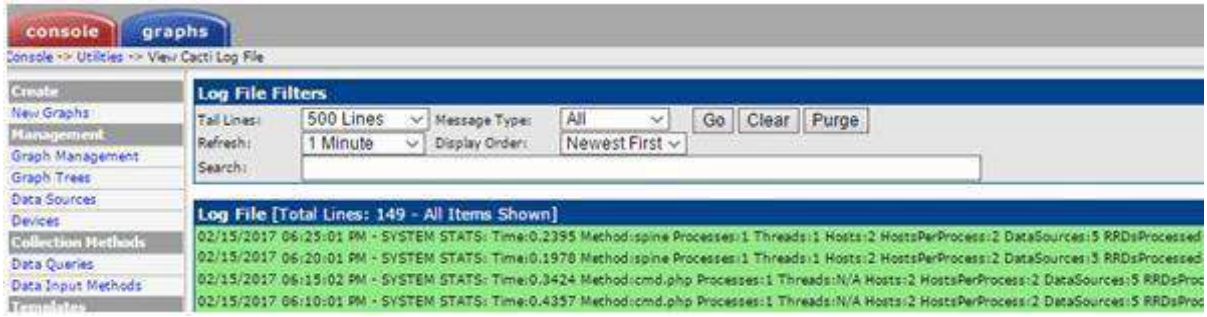


Рисунок 3.43 – Фрагмент перевірки помилок

Як видно, проблем немає – і всі дані нормально оновляться новим методом spine.

3.4 Додавання обладнання для моніторингу у веб-інтерфейсі Cacti

Додамо перше обладнання, яке потрібно моніторити. Для цього необхідно зайти у вкладку Devices і натиснути Add. Відкриється така сторінка (рис. 3.44):

Рисунок 3.44 – Фрагмент сторінки додавання хоста

У формі «Discription» вводимо назву обладнання, а у формі «Hostname» вводимо ip-адресу нашого обладнання. Далі вказуємо шаблон хоста «Host Template», вибираємо Generic SNMP-enable Host (якщо наше обладнання підтримує SNMP-протокол). У «SNMP Community» вказуємо раніше відомий public. Натискаємо кнопку «Create».

Тепер у вкладці «Graphs» з'явиться графік працездатності нашого обладнання, де ми бачимо вхідний (Inbound) та вихідний (Outbound) трафік. Працездатність обладнання характеризується тим, що приймає вхідний та вихідний трафік (рис.3.45).

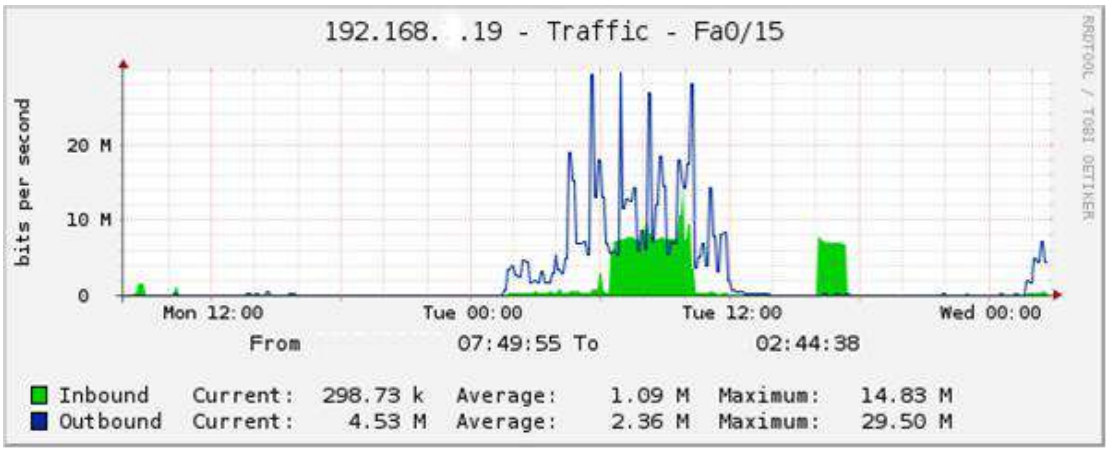


Рисунок 3.45 – Фрагмент графіка працездатності обладнання

Мета проєктного розділу полягає у тому, щоб виключити необхідність перевіряти кожне мережне обладнання вручну у разі відмови. Тепер це виключено, адже є дистанційний моніторинг цього обладнання, що включає миттєве відображення збоїв на екрані кожного монітора.

Розроблена система дозволяє дізнаватися про проблеми в інфраструктурі раніше чи одночасно з користувачами. Кожен співробітник підприємства тепер може подивитися працездатність мережного обладнання безпосередньо з веб-інтерфейсу через комп'ютер. Це, комплекс швидкої діагностики, який дає своєчасне оповіщення про труднощі у роботі сервісів та обладнання, надає точну інформацію, конкретні відомості про проблему та її характер.

ВИСНОВКИ

Метою роботи було створення дистанційного моніторингу працездатності обладнання на підприємстві.

В ході роботи над завданням було визначено необхідний функціонал систем моніторингу та проведено порівняльний аналіз систем моніторингу.

Була надана інформація щодо характеристики підприємства, означено вимоги для систем моніторингу та існуючої мережевої характеристики підприємства.

На основі проаналізованих систем була обрана система моніторингу Cacti 1.2.9 з розгортання на Ubuntu Server 20.04.

В процесі роботи над проєктом було проведено встановлення та налаштування системи моніторингу, мережевого обладнання та перевірено її працездатність.

Розроблена система дозволяє дізнаватися про проблеми в інфраструктурі раніше чи одночасно з користувачами. Кожен співробітник підприємства тепер може подивитися працездатність мережного обладнання безпосередньо з веб-інтерфейсу через комп'ютер.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ТОП 20 систем моніторингу IT інфраструктури [Електронний ресурс] – Режим доступу: https://itedu.center/ua/blog/ratings/monitoring_tools/ (дата звернення 30.03.2024).

2. Netxms [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/netxms (дата звернення 17.03.2024).

3. Використання системи моніторингу Nagios [Електронний ресурс] – Режим доступу: https://it.ridne.net/node/352 (дата звернення 24.03.2024).

4. Zabbix: What is Zabbix [Електронний ресурс] – Режим доступу: http://www.zabbix.com (дата звернення 01.05.2024).

5.. Cacti Linux моніторинг [Електронний ресурс] – Режим доступу: https://techexpert.tips/ru/ /cacti-linux/ (дата звернення 27.04.2024).

6. Архітектура мережі або мережева архітектура [Електронний ресурс] – Режим доступу: https://nettech.ua/news/arxitektura-seti-ili-setevaja-arxitektura (дата звернення 18.04.2024).

7. Огляд безкоштовних програм моніторингу серверів та комп'ютерної мережі [Електронний ресурс] – Режим доступу: https://uniteddc.net.ua/news/i/net-monitoring/ (дата звернення 30.04.2024).

8. Системи моніторингу та керування [Електронний ресурс] – Режим доступу:https://it-solutions.ua/servisi/sistemi-monitoringu-ta-keruvannya/ (дата звернення 29.03.2024).

9. Системи моніторингу стану [Електронний ресурс] – Режим доступу: https://www.skf.com/ua/products/condition-monitoring-systems (дата звернення 24.04.2024).

10. Забезпечення безпечного віддаленого доступу до Linux за допомогою SSH [Електронний ресурс] – Режим доступу: https://mediacom.com.ua/vikoristannya-ssh-dlya-bezpechnogo-viddalenogo-dostupu-do-linux-nalashtuvannya-ta-vikoristannya-navchannya-ta-praktika/ (дата звернення 27.04.2024).

11. Налаштування SSH сервера для безпечного доступу [Електронний ресурс] – Режим доступу: https://mediacom.com.ua/vikoristannya-ssh-dlya-bezpechnogo-viddalenogo-dostupu-do-linux-nalashtuvannya-ta-vikoristannya-navchannya-ta-praktika/ (дата звернення 18.05.2024).

12. Конфігурація та налаштування SSH для безпечного віддаленого доступу [Електронний ресурс] – Режим доступу: https://mediacom.com.ua/vikoristannya-ssh-dlya-bezpechnogo-viddalenogo-dostupu-do-linux-nalashtuvannya-ta-vikoristannya-navchannya-ta-praktika/ (дата звернення 22.05.2024).

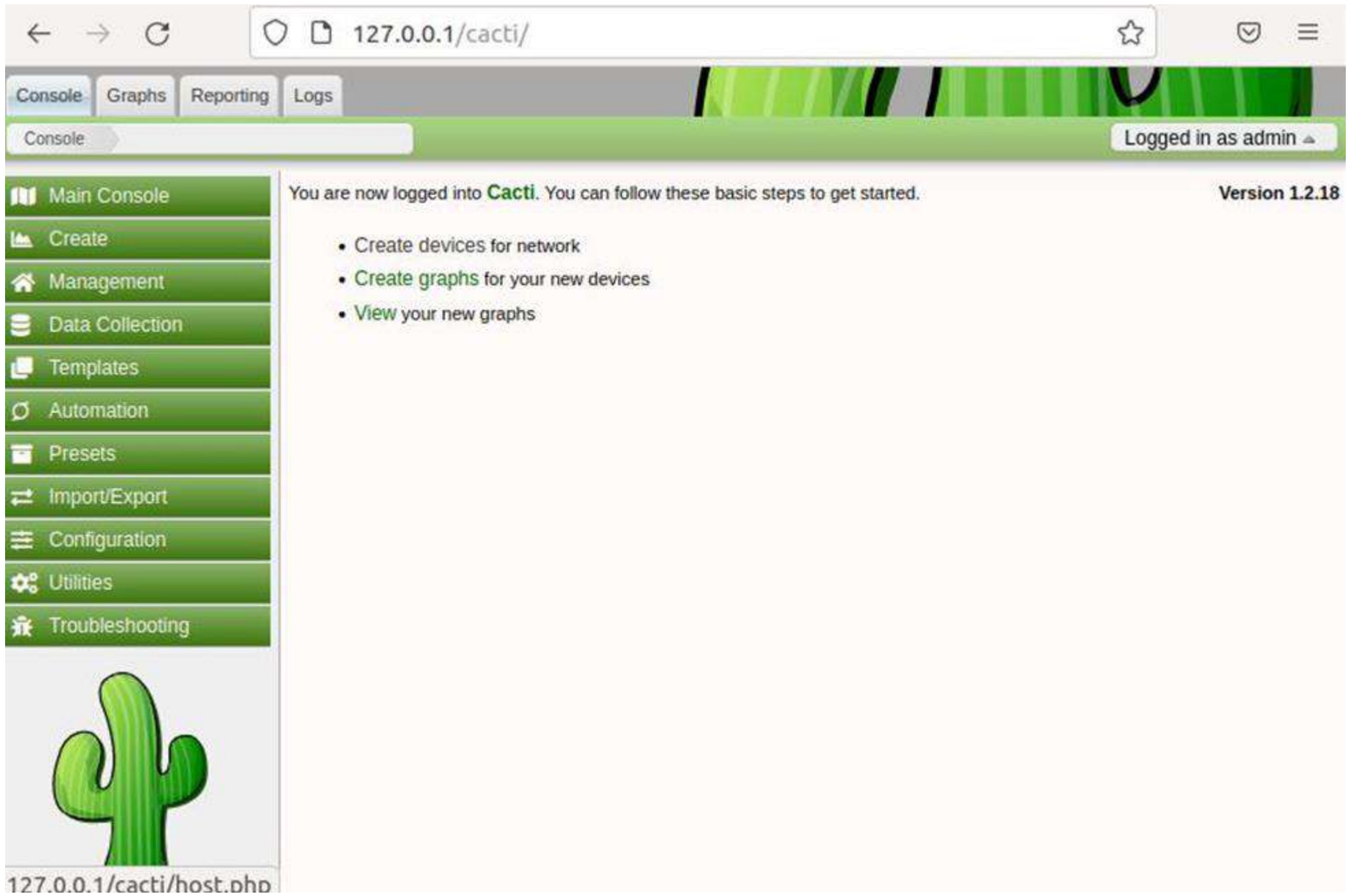
13. Режим роботи протоколу VTP [Електронний ресурс] – Режим доступу: https://imvk.net/cisco/urok-18-protokol-vtp (17.05.2024).

14. Налаштування Ubuntu Server 20.04, підключення по SSH, віддалене підключення до бази даних [Електронний ресурс] – Режим доступу: https://habr.com/sandbox/149730/ (дата звернення 03.05.2024).

15. Встановлення та налаштування Cacti до Ubuntu 20.04 ресурс] – Режим доступу: https://infoit.com.ua/linux/kak-ustanovit-i-nastroit-cacti-v-ubuntu-20-04/ (дата звернення 18.05.2024).

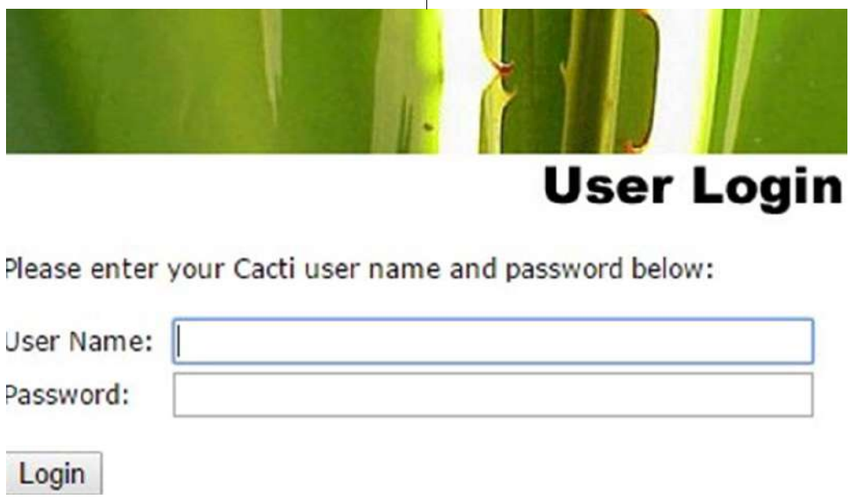
16. Встановлення серверу бази даних у Cacti [Електронний ресурс] – Режим доступу: https://infoit.com.ua/linux/kak-ustanovit-i-nastroit-cacti-v-ubuntu-20-04-mysql (дата звернення 23.04.2024).

Панель керування Cacti 1.2.9

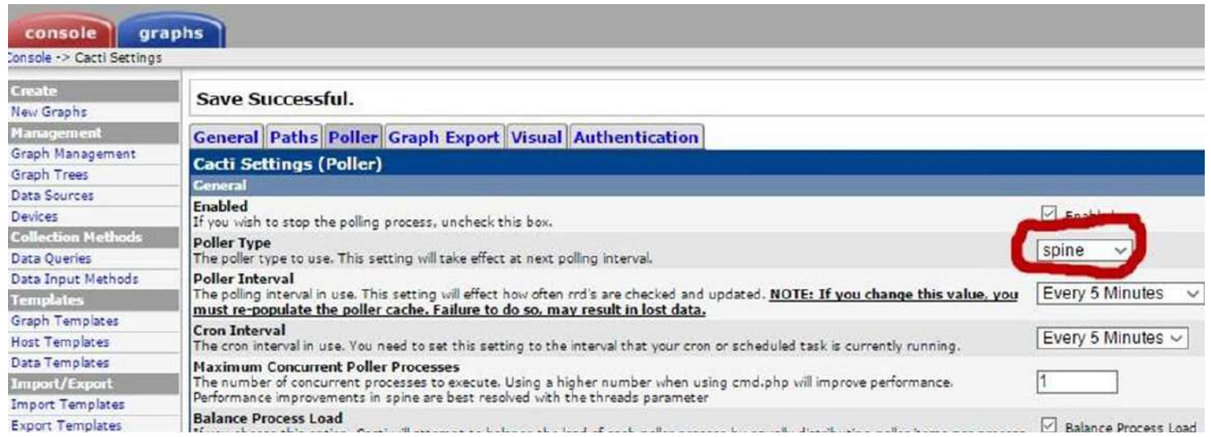


					13.02070849.00044 ПЛ1	
Зм.	Арк.	№ документу	Підпис	Дата	Розроблення системи дистанційного моніторингу працездатності обладнання на підприємстві	Літ. / Маса / Масштаб
Розробив		Мотошин О. А.				
Перевірив		Ільяшенко М.Б.				Аркуш 1 / Аркушів 1
Т.контр.						
Н.контр.		Польська О.В.			Панель керування Cacti 1.2.9	НУ «Запорізька політехніка», гр. КНТ-520
Затвердив		Кудерметов Р.К.				

Фрагмент форми входу до веб-інтерфейсу Cacti



Фрагмент вказівки типу Poller

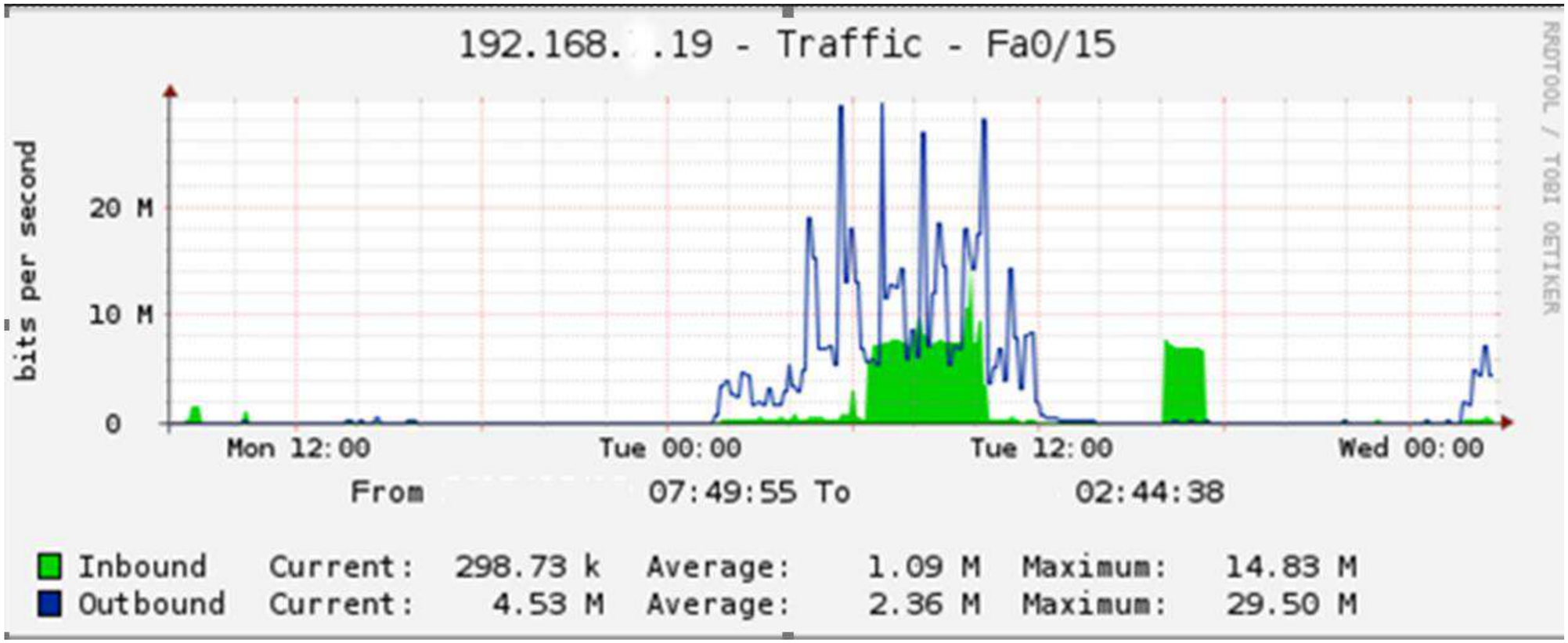


					13.02070849.00044 ПЛ2	
Зм.	Арк.	№ документу	Підпис	Дата	Розроблення системи дистанційного моніторингу працездатності обладнання на підприємстві	Літ. / Маса / Масштаб
Розробив		Мотошин О. А.				
Перевірив		Ільяшенко М.Б				Аркуш 1 / Аркушів 1
Т.контр.						
Н.контр.		Польська О.В.			Процес налаштування Cacti	НУ «Запорізька політехніка», гр. КНТ-520
Затвердив		Кудерметов Р.К.				

Фрагмент сторінки додавання хоста

					13.02070849.00044 ПЛЗ		
Зм.	Арк.	№ документу	Підпис	Дата	Розроблення системи дистанційного моніторингу працездатності обладнання на підприємстві	Літ.	Маса / Масштаб
Розробив		Мотошин О. А.					
Перевірив		Ільяшенко М.Б.				Аркуш 1	Аркушів 1
Т.контр.							
		—					
Н.контр.		Польська О.В.			Фрагмент сторінки додавання хоста	НУ «Запорізька політехніка», гр. КНТ-520	
Затвердив		Кудерметов Р.К.					

Фрагмент графіка працездатності обладнання



					13.02070849.00014 ПЛ4	
Зм.	Арк.	№ документу	Підпис	Дата		
Розробив		Мотошин А.О.			Розроблення системи дистанційного моніторингу працездатності обладнання на підприємстві	Літ. / Маса / Масштаб
Перевірив		Ільяшенко М.Б.				Аркуш 1 / Аркушів 1
Т.контр.						
Н.контр.		Польська О.В.			Фрагмент графіка працездатності обладнання	НУ «Запорізька політехніка», гр. КНТ-520
Затвердив		Кудерметов Р.К.				