

УДК 004.67

Лізунов С. І.<sup>1</sup>, Філобок Є.В.<sup>2</sup>

<sup>1</sup> канд. техн. наук, доц НУ «Запорізька політехніка»

<sup>2</sup> асп. НУ «Запорізька політехніка»

## **АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ІНТЕГРОВАНИХ СИСТЕМ МОНІТОРИНГУ ІНФРАСТРУКТУРИ**

Сучасний розвиток інформаційних технологій зумовлює необхідність надійного моніторингу інфраструктури для забезпечення стабільності та ефективності функціонування систем. Інтегровані системи моніторингу є одним з ключових інструментів управління інфраструктурою, які дозволяють оперативно виявляти, аналізувати та вирішувати проблеми, що виникають у роботі обладнання та програмного забезпечення. У цій статті буде розглянуто

можливості таких систем і їх більш детальну структуру, на прикладі системи Centeron.

### Аналіз існуючих інтегрованих систем моніторингу

Доречність використання певної системи моніторингу (далі СМ) на підприємстві або у компанії залежить від деяких факторів, таких як достатність ресурсів, кількість інфраструктури, яку потрібно моніторити та ризик менеджмент.

### Nagios

Nagios, як одна з перших і найбільш відомих СМ, має значні переваги, такі як широка спільнота користувачів, яка надає великий обсяг документації, підтримки та розширень. Багато користувачів відзначають його надійність і гнучкість у конфігурації, а також можливість інтеграції з іншими інструментами моніторингу (рис 1). В умовах швидко зростаючої інфраструктури, недовіки Nagios, такі як складність налаштування та нестабільність у високонавантажених середовищах, можуть стати суттєвими перешкодами [1].

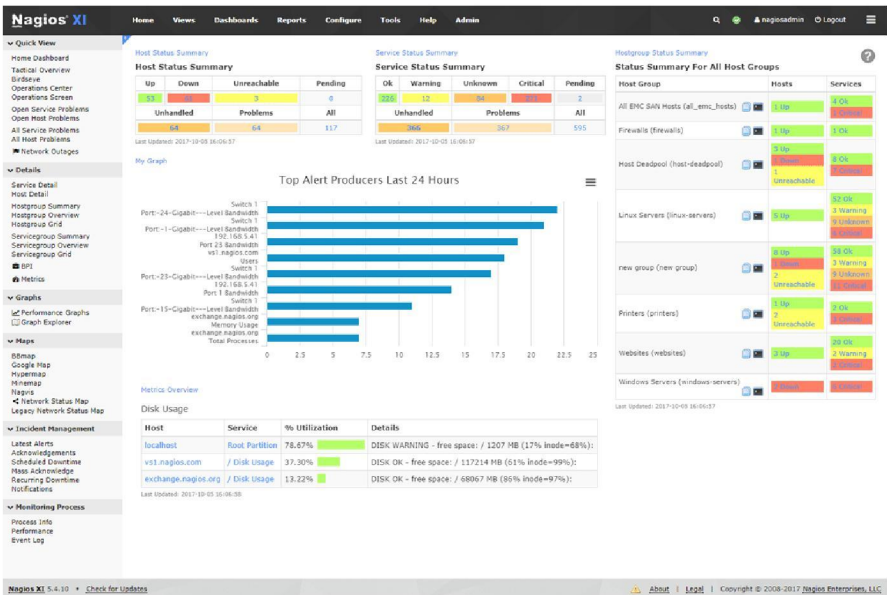


Рисунок 1 – Інтерфейс системи Nagios

### Zabbix

Zabbix відзначається простотою в налаштуванні, що робить його привабливим для використання навіть для початківців. Він має широкий

функціонал, включаючи моніторинг мережі, серверів та додатків. Потужна система аналітики дозволяє виявляти та передбачувати проблеми ще до того, як вони виникнуть. Використовується загалом для моніторингу мережевих систем та обладнання (рис 2). Відсутність підтримки деяких специфічних пристроїв і складність в налаштуванні опцій сповіщення можуть стати проблемою для деяких організацій [2].



Рисунок 2 – Інтерфейс системи Nagios

### Prometheus

Prometheus є системою моніторингу з відкритим кодом, яка зосереджена на моніторингу великих розподілених систем. Однією з його ключових переваг є здатність до масштабування і гнучкості налаштування, що дозволяє ефективно моніторити складні інфраструктурні середовища. Prometheus відзначається потужними засобами збору метрик та аналізу даних, що дозволяє виявляти проблеми та аналізувати їхні причини, використовується для створення графологічного представлення даних (рис 3).

Недоліком є те, що успішного впровадження Prometheus може знадобитися додатковий час і зусилля для налаштування та розгортання [3].

### Centreon

Centreon є однією з найбільш повних та функціональних інтегрованих систем на ринку. Вона надає широкі можливості моніторингу різноманітних компонентів інфраструктури, включаючи сервери, мережеве обладнання, бази даних та додатки.



## Структура СМ

Архітектура системи Centreon може бути гарним прикладом для розуміння того, як саме працює СМ. Основні складові цієї архітектури включають (рис 5):

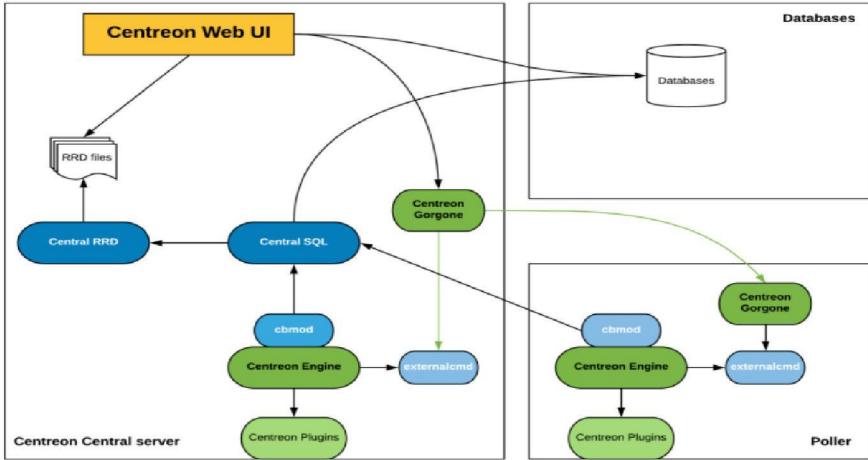


Рисунок 5 – Архітектура СМ Centreon

**Центральний сервер Centreon:** Це головний вузол системи, який відповідає за відображення та управління даними моніторингу. Він містить веб-інтерфейс для взаємодії з користувачем, моніторинговий двигун для збору даних, а також брокер для обміну інформацією між різними компонентами.

**Сервер баз даних:** Це місце, де зберігаються всі конфігураційні дані та зібрані метрики. Це допомагає забезпечити надійність та безпеку інформації.

**Поллери:** Це вузли, які відповідають за збір даних з об'єктами, що моніторяться, такими як сервери або мережеве обладнання. Вони виконують функцію збору даних і передачі їх до центрального сервера для подальшої обробки.

Коли мова йде про відображення стану сервісів у Centreon, процес починається зі збору даних. Поллери, що розташовані в мережі, активно моніторять різні компоненти та сервіси інфраструктури. За допомогою протоколу SNMP вони звертаються до мережевих пристроїв, щоб отримати необхідну інформацію про їх стан. Отримані дані надсилаються на центральний сервер Centreon, де вони аналізуються та обробляються. Центральний сервер визначає статус кожного сервісу на основі зібраних даних. Наприклад, якщо сервер недоступний або навантаження перевищує порогове значення, система встановлює статус "помилка" для цього сервісу.

Інформація про стан сервісів відображається на головній панелі веб-інтерфейсу Centreon (рис 6). Користувач може побачити список всіх сервісів, що моніторяться та їх стан, який представлений за допомогою кольорового кодування. Зелений колір означає, що сервіс працює нормально, червоний - що виникла помилка, а жовтий - що сервіс перебуває в стані попередження або відстежується. Крім того, Centreon може генерувати графіки та діаграми, які відображають зміни у стані сервісів з часом. Це допомагає адміністраторам відстежувати тенденції та вчасно реагувати на будь-які проблеми. Таким чином, завдяки інтегрованому підходу до збору та відображення даних, Centreon забезпечує зрозумілий та зручний інтерфейс для моніторингу стану інфраструктури.

All non-informative events order by last state change

Host Name	Service	Status	Duration	Status information
ib-blp-idf-1	realservice-status-Imap8	CRITICAL	2m 6s ago	Realservice 'Imap8' is down.
srv-DC-paris	memory	CRITICAL	3m 20s ago	Memory used : 6.70 Go - size : 7.00 Go - percent :
srv-DC-sydney	eventlog-System	CRITICAL	11m 6s ago	8 error found in System eventLog
Antivirus_server	Protection	CRITICAL	12m 10s ago	CRITICAL: Protection status is 'Warning' - 1 hosts
mail-mars-frontend	send-message-external	CRITICAL	16m 40s ago	Can't send SMTP message to 'test@externe.com'.
srv-mysql-01	load	WARNING	25m 51s ago	Load Average : 2.24, 1.87, 1.99
Antivirus_server_Sophos	Events	CRITICAL	28m 56s ago	CRITICAL: 268 critical event(s)
sw-newyork-02	memory	CRITICAL	29m 5s ago	Memory used : 8.16 Go - size : 9.00 Go - percent :
Antivirus_server_Sophos	Logical-Network	WARNING	34m 16s ago	WARNING: 1 host(s) are not controlled
rt-perth	memory	CRITICAL	34m 50s ago	Memory used : 5.66 Go - size : 6.00 Go - percent :
Antivirus_server	Events	WARNING	38m 4s ago	WARNING: 101 critical event(s)
mail-jupiter-frontend	load	WARNING	38m 6s ago	Load Average : 2.69, 2.50, 2.27
srv-DC-sydney	memory	CRITICAL	49m 35s ago	Memory used : 3.84 Go - size : 4.00 Go - percent :
messaging-blueimind	load	WARNING	57m 36s ago	Load Average : 3.18, 2.48, 2.44
eBS_Apps_Oracle_DB	oracle-shared-spool-ratio	WARNING	59m 38s ago	Shared pool hit ratio = 84.717% (memory used)
srv-oracle-users	disk-/	WARNING	1h 12m ago	Disk / - used : 38.36 Go - size : 43.00 Go - perce
SensorProbe-Datacenter-05	temperature	WARNING	1h 40m ago	Temperature sensor : 33C

Рисунок 6 – Веб інтерфейс інцидентів

Крім візуалізації стану сервісів, Centreon також надає можливості налаштування сповіщень про виявлені проблеми або події в інфраструктурі. Коли будь-який сервіс переходить у стан помилки або попередження, або коли досягається певний поріг важливих метрик, система автоматично відправляє сповіщення адміністраторам або відповідальним особам, за допомогою Email або іншого виду сповіщення, наприклад у Slack (рис 7).

Centreon може моніторити різні типи об'єктів інфраструктури, включаючи сервери, мережеве обладнання, бази даних, хмарні сервіси тощо.

Більшість популярних та затребуваних сервісів-перевірок вже вбудовані в базу Centreon, але відмінною перевагою є можливість створенні власних сервісів, написаних під певні потреби користувачів. Це дозволяє компаніям отримувати повну картину стану своєї інфраструктури та вчасно реагувати на будь-які проблеми чи загрози.

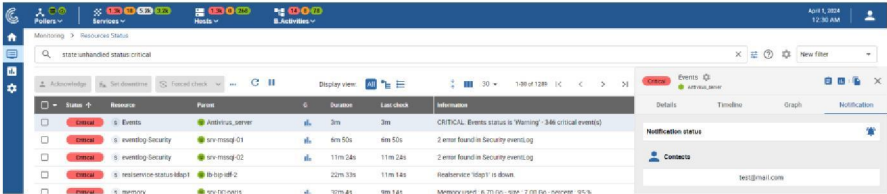


Рисунок 7 – Конфігурація сервісу зі сповіщенням через email

Також ця CM надає інструменти для аналізу зібраних даних та створення звітів про продуктивність та ефективність інфраструктури (рис 8). Ці звіти допомагають адміністраторам та керівництву розуміти тенденції в розвитку інфраструктури, виявляти проблемні аспекти та приймати обґрунтовані рішення з покращення ефективності.

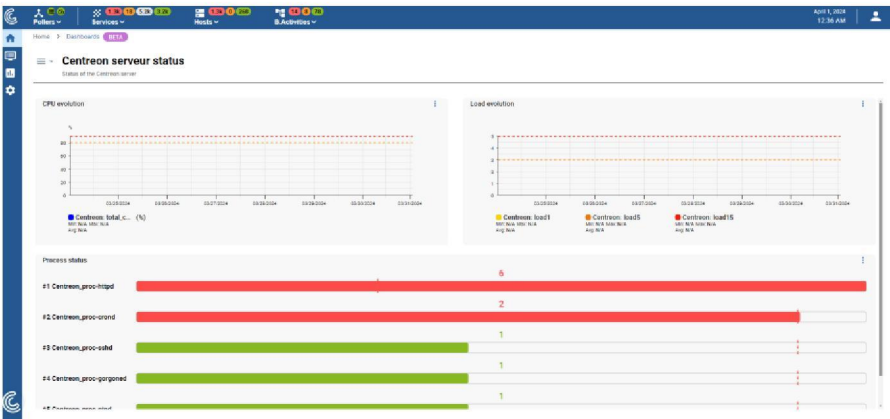


Рисунок 8 – Приклад дашборду у Centeron

У цілому, системи моніторингу є незамінним інструментом для сучасних компаній, які прагнуть забезпечити надійність, ефективність та безпеку своєї інфраструктури. Інтеграція таких систем у робочий процес дозволяє забезпечити ефективне управління та контроль за інфраструктурою, знизити ризики виникнення непередбачених ситуацій та збільшити загальну продуктивність бізнесу.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Nagios – система ІТ моніторингу [Електронний ресурс]. – Режим доступу: <https://idealsoft.com.ua/vendors/vendors-more/nagios/>
2. Що таке Zabbix | Основні функції та можливості. [Електронний ресурс]. – Режим доступу: <https://lvivservice.com.ua/sysadmin/chto-takoe-zabbix-osnovnye-funkczii-i-vozmozhnosti/>
3. Prometheus vs Zabbix: відмінне та подібне цих систем моніторингу [Електронний ресурс]. – Режим доступу: [https://itedu.center/ua/blog/comparisons/prometheus\\_vs\\_zabbix/](https://itedu.center/ua/blog/comparisons/prometheus_vs_zabbix/)
4. Centreon | IT Infrastructure Monitoring Software [Електронний ресурс]. – Режим доступу: <https://www.centreon.com/>