© Lizunov S., Filobok E., Vereshchaka M. Analysis of the possibilities of using integrated infrastructure monitoring systems // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 2, pp. 348-352. ©

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ/ INFORMATION SECURITY MANAGEMENT

DOI: 10.18372/2225-5036.30.19248

ВИКОРИСТАННЯ ІНТЕГРОВАНИХ СИСТЕМ МОНІТОРИНГУ ІТ-ІНФРАСТУКТУРИ

Сергій Лізунов, Євгеній Філобок, Максим Верещака

Національний університет «Запорізька політехніка»

ЛІЗУНОВ Сергій Іванович, к.т.н., доцент
Рік та місце народження: 1953 рік, м. Запоріжжя.
Освіта: Запорізький машинобудівний інститут (з 2020 року – Національний університет «Запорізька політехніка»), 1980 рік; очна аспірантура Московського енергетичного інституту, 1989 рік; Запорізький юридичний інститут МВС України, 2005 рік.
Посада: доцент кафедри інформаційної безпеки та наноелектроніки Національного університету «Запорізька політехніка».
Наукові інтереси: технічний захист інформації.
Публікації: більше 150 наукових публікацій.
E-mail: silizunov@ukr.net.
Orcid ID: 0000-0001-8977-8705.

ФІЛОБОК Євгеній Віталійович, аспірант
Рік та місце народження: 1999 рік, м. Запоріжжя, Україна.
Посада: аспірант, Національний університет «Запорізька політехніка».
Наукові інтереси: захист інформації в інформаційних мережах, технічний захист інформації.
Публікації: більше 10 наукових публікацій.
E-mail: filobock1999@gmail.com.
Orcid ID: 0000-0002-4105-3841.

ВЕРЕЩАКА Максим Павлович, аспірант
Рік та місце народження: 1995 рік, м. Дунаївці, Україна.
Посада: аспірант, Національний університет «Запорізька політехніка» .
Наукові інтереси: захист інформації в інформаційних мережах, технічний захист інформації.
Публікації: більше 10 наукових публікацій.
E-mail: max111095@gmail.com.
Orcid ID: 0009-0000-7685-1774.

Анотація. *У сучасну цифрову епоху стрімке розширення та ускладнення ІТ-інфраструктур зробило потребу в ефективних системах моніторингу таких інфраструктур більш критичною, ніж будь-коли. Ці системи відіграють ключову роль у забезпеченні безперебійної роботи як апаратного, так і програмного забезпечення, оперативно виявляючи та вирішуючи потенційні проблеми, включаючи захист інформації. Інтегровані рішення для моніторингу, такі як Zabbix, Nagios, Prometheus і Centreon, стали ключовими інструментами в управлінні інфраструктурою, кожне з яких пропонує унікальні функції для задоволення різних потреб моніторингу. Zabbix, відомий своєю масштабованістю та можливістю моніторингу широкого спектру пристроїв, пропонує широкі методи збору даних та гнучкі системи оповіщення. Він відмінно підходить для великомасштабних розгортань, дозволяючи організаціям контролювати тисячі пристроїв одночасно. Nagios, один з найстаріших і найвідоміших інструментів моніторингу, дуже добре налаштовується і підтримує велику кількість плагінів. Його сила полягає в гнучкості та великій спільноті, яка сприяє його постійному роз-*

витку, що робить його ідеальним рішенням для організацій, які потребують індивідуального підходу до моніторингу інфраструктури. Prometheus, з іншого боку, пропонує сучасний підхід до моніторингу, особливо ефективний у хмарних і контейнерних середовищах. Орієнтація на метрики в реальному часі та дані часових рядів у поєднанні з надійними можливостями оповіщення робить його популярним вибором для динамічних середовищ, де дані про продуктивність в реальному часі є важливими. Centreon, хоча і не такий широко відомий, як деякі з його аналогів, пропонує всебічний підхід до моніторингу інфраструктури. Він поєднує в собі гнучкість Nagios з інтуїтивно зрозумілим користувацьким інтерфейсом, що дозволяє адміністраторам легко контролювати різні компоненти. Система оповіщення Centreon в режимі реального часу дозволяє користувачам виявляти і вирішувати проблеми до їх ескалації, забезпечуючи стабільність системи. Структурований підхід до відображення сповіщень і типів моніторингу, від мережевих пристроїв до хмарних сервісів, робить її універсальним рішенням як для малих, так і для великих IT-середовищ. Хоча кожна система має свої сильні сторони, баланс між зручністю та універсальністю Centreon робить її особливо привабливою для організацій, які шукають рішення «все в одному».

Ключові слова: *моніторинг, захист інформації, система моніторингу, алерт, інфраструктура, критичний стан, система миттєвого сповіщення.*

Постановка проблеми

В сучасних умовах швидкого технологічного розвитку моніторинг IT-систем набуває особливого значення. Дослідження наявних систем моніторингу, аналіз їх архітектур, імплементація в існуючі проєкти та налаштування для специфічних платформ є актуальними завданнями. Для організацій, які шукають ефективні інструменти управління складними IT-інфраструктурами, такі платформи підвищують стабільність систем, покращують виявлення проблем у реальному часі та оптимізують операції. Це, в кінцевому рахунку, сприяє підвищенню рівня захищеності інформації, що обробляється. Тому виникає потреба в масштабованих, адаптивних рішеннях в умовах прискореного технологічного темпу. 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.

Аналіз останніх джерел та публікацій

Загальний процес роботи у таких системах один: система отримує великі масиви даних через спеціальні застосунки або порти, проводить аналіз чи відповідає отримана інформація усім критичним вимогам, та за потреби створює алерт оповіщення (рис. 1) [1].

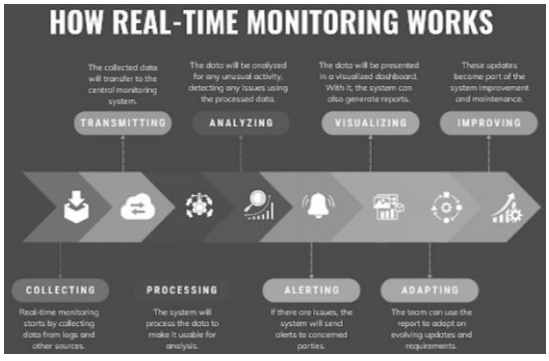

Рис. 1. Схема роботи СМ

Ці СМ дозволяють візуалізувати поточні проблеми у існуючій інфраструктурі.

Виклад основного матеріалу дослідження

Система моніторингу Nagios

Nagios, будучи однією з найперших і найбільш широко визнаних систем моніторингу, пропонує значні переваги. Вона може похвалитися великою спільнотою користувачів, яка надає велику документацію, підтримку та численні розширення. Багато користувачів цінують її надійність і гнучкість конфігурації, а також здатність легко інтегруватися з іншими інструментами моніторингу (рис. 2). Однак, в інфраструктурах, що швидко розвиваються, його недоліки, такі як складність налаштування та нестабільність при високих навантаженнях, можуть створювати значні проблеми [2].

Рис. 2. Інтерфейс системи Nagios

Однак, в інфраструктурах, що швидко розвиваються, його недоліки, такі як складність налаштування та нестабільність при високих навантаженнях, можуть створювати значні проблеми [2].

Система моніторингу Zabbix

Zabbix вирізняється зручним налаштуванням, що робить його доступним навіть для початківців. Його широкі функціональні можливості охоплюють моніторинг мережі, серверів і додатків, пропонуючи комплексний набір інструментів для різних IT-середовищ. Оснащений потужною аналітичною системою, Zabbix дозволяє проактивно виявляти та прогнозувати проблеми, підвищуючи операційну стабільність. Він зазвичай використовується для моніторингу мережевих систем та обладнання (рис. 3).

Проте деякі організації можуть зіткнутися з проблемами через обмежену підтримку певних спеціалізованих пристроїв і складність налаштування параметрів сповіщень [3].

Система моніторингу Prometheus

Prometheus - це система моніторингу з відкритим вихідним кодом, призначена для великих розподілених середовищ. Її відмінними рисами є масштабованість і гнучка конфігурація, що робить її добре придатною для моніторингу складної інфраструктури. Prometheus відомий своїми потужними можливостями збору метрик та аналізу даних, що дозволяє ефективно виявляти проблеми та аналізувати їх першопричини, які часто представлені візуально за допомогою графічних інструментів (рис. 4).

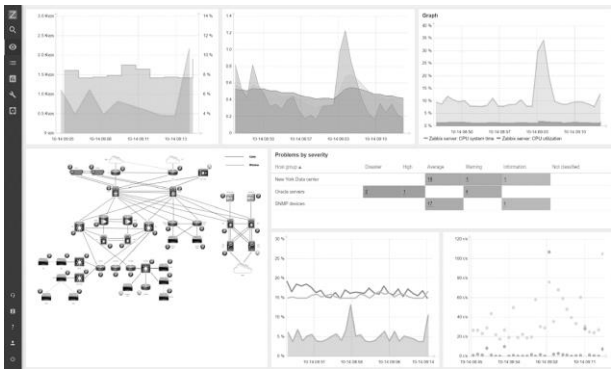

Рис. 3. Інтерфейс системи Zabbix

Рис. 4. Інтерфейс системи Zabbix

Успішне розгортання Prometheus може вимагати значного часу і зусиль, що може стати проблемою під час налаштування та інтеграції [4].

Система моніторингу Centreon

Centreon вважається однією з найбільш повних і функціональних інтегрованих систем моніторингу. Вона пропонує широкі можливості для моніторингу широкого спектру компонентів інфраструктури, таких як сервери, мережеві пристрої, бази даних і застосунки. Зручний інтерфейс підвищує її привабливість, що робить її популярним вибором для організацій, які шукають ефективні та доступні рішення для управління інфраструктурою [5].

Структура СМ Centreon

Архітектура Centreon є наочним прикладом того, як функціонує інтегрована система моніторингу. Її структура складається з декількох ключових компонентів (рис. 5).

1. Центральний сервер Centreon - це основний вузол системи, який відповідає за відображення та управління даними моніторингу. Він включає веб-інтерфейс для взаємодії з користувачами, механізм моніторингу для збору даних і брокер, який полегшує обмін інформацією між компонентами системи.
2. Сервер бази даних. На цьому сервері зберігаються всі конфігураційні дані та метрики, зібрані з пристроїв, що підлягають моніторингу, забезпечуючи надійність та безпеку даних.
3. Поллери. Ці вузли відповідають за збір даних з об'єктів моніторингу, таких як сервери та мережеві пристрої. Вони збирають ці дані та надсилають їх на центральний сервер для аналізу та обробки.

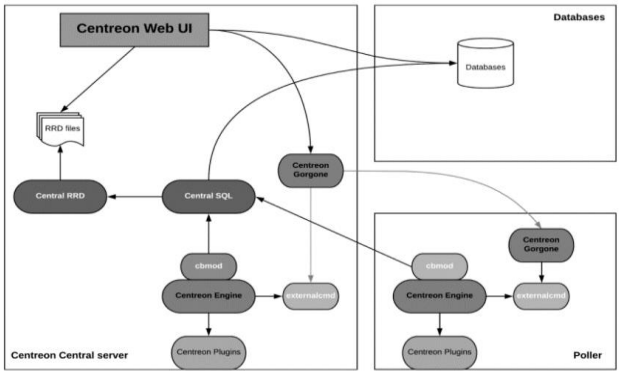

Рис. 5. Архітектура СМ Centreon

Процес відображення стану сервісу в Centreon починається зі збору даних. Поллери в мережі безперервно відстежують різні компоненти інфраструктури та сервіси, отримуючи доступ до мережевих пристроїв за допомогою протоколів, таких як SNMP, для збору інформації про їхній стан. Потім ці дані надсилаються на центральний сервер Centreon, де вони обробляються. На основі отриманої інформації центральний сервер визначає стан кожного сервісу. Наприклад, якщо сервер недоступний або його навантаження перевищує заданий поріг, система позначає послугу статусом «помилка» (рис. 6).

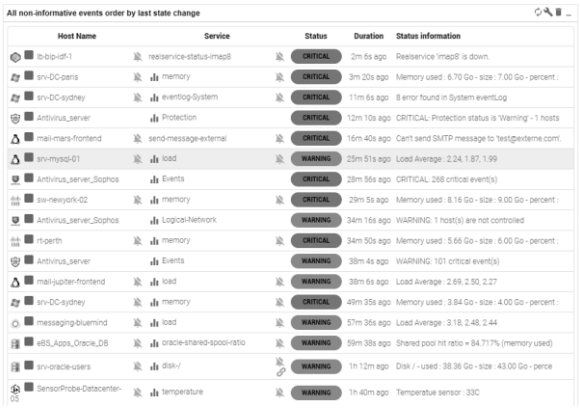

Рис. 6. Веб інтерфейс інцидентів

Цей статус послуги візуально відображається на головній панелі веб-інтерфейсу Centreon, де користувачі можуть переглянути повний список відстежуваних послуг, позначених кольором для позначення їхнього статусу. Зелений колір вказує на нормальну ро-

боту, червоний - на помилку, а жовтий - на попереджувальний стан або активний моніторинг. Крім того, Centreon генерує графіки та діаграми, що відображають зміни статусу послуг у часі, дозволяючи адміністраторам відстежувати закономірності та вирішувати проблеми на випередження. Завдяки такому інтегрованому підходу до збору та відображення даних, Centreon пропонує чіткий, зручний інтерфейс для ефективного моніторингу стану інфраструктури. На додаток до візуалізації статусів сервісів, Centreon пропонує надійні можливості сповіщення про події та проблеми в інфраструктурі. Коли служба переходить у стан помилки або попередження, або коли критичні показники перевищують встановлений поріг, система автоматично сповіщає адміністраторів або призначений персонал. Ці сповіщення можна налаштувати так, щоб вони надходили користувачам електронною поштою або через інші комунікаційні платформи, такі як Slack (рис. 7), забезпечуючи оперативне вирішення проблем.

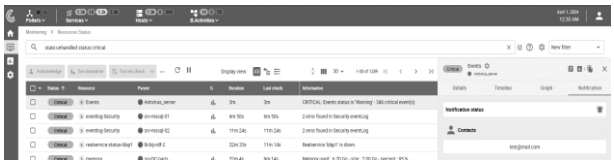

Рис. 7. Конфігурація сервісу зі сповіщенням через E-mail

Centreon може контролювати широкий спектр елементів інфраструктури, включаючи сервери, мережеві пристрої, бази даних і хмарні сервіси. Хоча багато популярних сервісів моніторингу попередньо налаштовані в базі даних Centreon, ключовою перевагою є його гнучкість, що дозволяє користувачам створювати власні сервіси, пристосовані до їхніх конкретних потреб. Така адаптивність дозволяє компаніям отримати комплексне уявлення про свою інфраструктуру і швидко реагувати на будь-які потенційні проблеми або загрози.

Крім того, Centreon надає потужні інструменти для аналізу зібраних даних і створення детальних звітів про продуктивність та ефективність інфраструктури. Ці звіти надають цінну інформацію, допомагаючи адміністраторам і керівництву визначати тенденції, виявляти потенційні проблемні області та приймати обґрунтовані рішення, спрямовані на підвищення операційної ефективності. Завдяки цим функціям Centreon підтримує як моніторинг в режимі реального часу, так і довгострокове стратегічне планування.

Висновки. В ході дослідження було проаналізовано значення систем моніторингу у інфраструктурі сучасних підприємств; розглянуті можливості інтеграції цих систем у робочі процеси організацій та їх вплив на управління інфраструктурою. Було більш детально вивчено комплексну систему моніторингу інфраструктури — Centreon, яка відзначається ефективним моніторингом різних компонентів, збором, візуалізацією та аналізом даних у режимі реального часу.

Її можливості з налаштування автоматичних сповіщень про критичні події та гнучкість у створенні власних служб моніторингу дозволяють організаціям швидко реагувати на будь-які проблеми, що виникають, сприяючи не лише безперебійній безпечній роботі, але й підвищенню продуктивності бізнесу в цілому.

Однак, розгортання таких систем вимагає продуманої конфігурації та адаптації до конкретних потреб кожної організації, з особливою увагою до масштабованості, кастомізації та інтеграції різних інструментів моніторингу, що може значно покращити ефективність управління складними інфраструктурами.

Список літератури

[1]. What Is Real-Time Monitoring: Definition, Process, Importance, Use Cases, And More? [Електронний ресурс]. – Режим доступу: https://edgedelta.com/company/blog/what-is-real-time-monitoring.

[2]. Nagios – система IT мониторинга [Електронний ресурс]. Режим доступу: https://idealsoft.com.ua/vendory/vendors-more/nagios/.

[3]. Що таке Zabbix | Основні функції та можливості. [Електронний ресурс]. Режим доступу: https://lvivservice.com.ua/sysadmin/chto-takoe-zabbix-osnovnye-funkczii-i-vozmozhnosti/.

[4]. Prometheus vs Zabbix: відмінне та подібне цих систем моніторингу [Електронний ресурс]. Режим доступу: https://itedu.center/ua/blog/comparisons/prometheus_vs_zabbix/.

[5]. Centreon | IT Infrastructure Monitoring Software [Електронний ресурс]. Режим доступу: https://www.centreon.com.

УДК 004.67

Lizunov S., Filobok E., Vereshchaka M. Analysis of the possibilities of using integrated infrastructure monitoring systems

Abstract. *In today's digital age, the rapid expansion and complexity of IT infrastructures has made the need for effective monitoring systems more critical than ever. These systems play a key role in ensuring the smooth operation of both hardware and software, identifying and resolving potential problems quickly. Integrated monitoring solutions such as Zabbix, Nagios, Prometheus, and Centreon have become key tools in infrastructure management, each offering unique features to meet different monitoring needs. Zabbix, known for its scalability and ability to monitor a wide range of devices, offers extensive data collection methods and flexible alerting systems. It is great for large-scale deployments, allowing organizations to monitor thousands of devices simultaneously. Nagios, one of the oldest and most well-known monitoring tools, is highly customizable and supports many plugins. Its strength lies in its flexibility and the large community that contributes to its continuous development, making it an ideal solution for organizations that need a customized approach to infrastructure monitoring. Prometheus, on the other hand, offers a modern approach to monitoring that is particularly effective in cloud and containerized environments. Its focus on real-time metrics and time-series data, combined with robust alerting capabilities, makes it a popular choice for dynamic environments where real-*

time performance data is essential. Centreon, while not as widely known as some of its peers, offers a comprehensive approach to infrastructure monitoring. It combines the flexibility of Nagios with an intuitive user interface that allows administrators to easily monitor different components. Centreon's real-time alerting system allows users to identify and resolve issues before they escalate, ensuring system stability. The structured approach to displaying alerts and monitoring types, from network devices to cloud services, makes it a versatile solution for both small and large IT environments. While each system has its own strengths, Centreon's balance between convenience and versatility makes it particularly attractive to organizations looking for an all-in-one solution.

Key words: *monitoring, information protection, monitoring systems, alert, infrastructure, critical condition, sudden notification system.*

Лізунов Сергій Іванович, к.т.н., доцент, доцент кафедри «Інформаційна безпека та наноелектроніка» Національного університету «Запорізька політехніка».

Serhii Lizunov, assistant professor of the Information Security and nanoelectronics Department, National University «Zaporizhzhia Polytechnic».

Філобок Євгеній Віталійович, аспірант Національного університету «Запорізька політехніка».

Yevhenii Filobok, post-graduate student, National University «Zaporizhzhia Polytechnic».

Верещака Максим Павлович, аспірант Національного університету «Запорізька політехніка».

Maksym Vereshchaka, post-graduate student, National University «Zaporizhzhia Polytechnic».

Отримано *14 червня 2024 року*, затверджено редколегією *26 червня 2024 року*