УДК 004.891

ДОСЛІДЖЕННЯ СУЧАСНИХ СИСТЕМ МОНІТОРИНГУ СТАНУ СЕРВЕРНОГО ОБЛАДНАННЯ

Гольцов В.В. *e-mail*: *vovladik141@gmail.com*
Науковий керівник к.т.н., доц. Холодняк Ю.В.
Таврійський державний агротехнологічний університет імені Дмитра Моторного

Постановка проблеми. Компаніям часто необхідно відстежувати які пристрої та користувачі автентифікуються та мають доступ до корпоративної мережі. Головна мета цього – контроль трафіку та виявлення різних кібератак на сервісне обладнання, що можуть завдати значних збитків і привести до крадіжки даних користувачів, і також завдати репутаційних збитків. Зараз багато різних компаній, що працюють в Україні, мають великий шанс, що їх сервісне обладнання зазнає один або декілька з видів кібератак. Щоб уникнути цього, першим шагом пропонується простежувати всю інформацію, яку отримують та надсилають сервера, а другим – блокувати дані або попереджувати працівників, що працюють з сервісним обладнанням. Програма моніторингу повинна містити простий, але масштабований інтерфейс, що дозволить швидко опанувати та налаштувати її під власні потреби.

Зараз у зв'язку з надзвичайною ситуацією в країні, розробляється багато програмного забезпечення, що потребує зв'язок з сервером. З іншого боку стали частіше проходити різні кібератаки, які направлені на перевантаження баз даних, або виводу мережевих пристроїв з ладу. На цей час майже не існує статей, що детально досліджують тему мережевих кібератак. Також розробляться багато вузькоспеціалізованих додатків, що призначенні для захисту від зовнішньої загрози, але опис цих програм майже не публікуються за для застереження їх від програмного злому.

Метою роботи є аналіз існуючих систем моніторингу стану серверного обладнання для розподілених та централізованих мереж з метою подальшої розробки власної. Для досягнення поставленої мети необхідно вирішити наступні завдання:

- проаналізувати найпоширеніші кібератаки на серверне обладнання в Україні;
- дослідити оптимальний шлях моніторингу трафіку, та оптимізації роботи з ним;
- визначити які дані треба відокремлювати від поточної інформації з подальшої ізоляцією.

Основні матеріали дослідження. Працюючи з комплексом програмно-технічних засобів, а саме з сервером та його архітектурою, програмуючи СУБД і, змінюючи інформацію у БД, то відповідно для цього повинен надаватись захист як фізичний, для охорони сервісного обладнання та його компонентів, так і інформаційний [1].

Стосовно проектування архітектури сучасних центрів обробки даних (ЦОД) необхідно здійснювати виходячи з розрахунку передбачення можливих відмов устаткування.

Інформаційні системи допускають розпаралелювання процесів збору, обробки, зберігання і надання даних користувачам, а також передбачають

механізми захисту від апаратних збоїв. Кластерні рішення і балансування навантаження ще більше підвищують надійність і доступність сервісів ЦОД. Механізми самокорекції, а також розвинені механізми моніторингу стану дозволяють зменшити вплив відмови окремих елементів на систему в цілому.

Сучасний центр обробки даних є комплексною інженерною спорудою, що забезпечує функціонування бізнес-процесів. Його основу складають три функціональні блоки:

— *телекомунікаційна система*, що реалізує взаємозв'язок елементів ЦОД, а також прийом/передачу даних між центром і користувачами його сервісів;

— *технічна архітектура* (сервери доступу, сервери додатків, сервери СУБД, сховища даних), що підтримує функціонування інформаційних систем, доступ користувачів до додатків і зберігання даних;

— *інженерна інфраструктура*, що забезпечує оптимальні умови для функціонування вищенаведених систем і діяльності обслуговуючого персоналу [2].

Кожен з цих блоків потребує захист, але саме технічна архітектура потребує більшого оснащення та перевірки всіх даних, що поступають. Зважаючи на це, існують програмні додатки, що допомагають відстежувати поточну інформацію. Можна навести декілька актуальних прикладів існуючих програм моніторингу стану серверів (табл. 1).

Таблиця 1. Порівняння програм моніторингу стану серверів

Програма / Критерій оцінки	Server and Application Monitor	Site24x7	Sematext Monitoring
Наявність документації користувача	Так	Ні	Так
Можливість розширення додатку за допомогою зовнішніх модулів	Так	Ні	Так
Робота зі хмарними технологіями	Так	Так	Ні
Кількість елементів керування (за досвідом користувачів)	Багато	Середнє	Середнє
Автоматичне відстежування протоколів та роботи серверу	Так	Так	Так
Створення звітів відстежуванної інформації	Так	Так	Ні

1) Server and Application Monitor. Це потужний додаток що відстежує продуктивність сервера та програми, сповіщаючи про будь-які проблеми та повідомляючи про них [3].

Розробник SolarWinds інтегрував можливість моніторингу віртуальних серверів як локальних, так і хмарних для понад 1200 різних програм. Він забезпечує розуміння продуктивності програми та показників використання сервера (рис. 1).

Рисунок 1. Візуальний інтерфейс «Server and Application Monitor»

Він має такі функції, як рішення для віддаленого моніторингу серверів, моніторинг інвентаризації серверів, моніторинг процесів сервера, автоматизований моніторинг мережі серверів і моніторинг справності серверів.

Мінусом програми можна зазначити великий масив функцій та модулів, що погано сприймаються нетехнічними користувачами.

2) Site24x7 – це хмарний інструмент моніторингу мережі, який цілодобово відстежує стан сервера та кінцевих веб-точок.

Додаток контролює мережеву інфраструктуру компанії. Це робиться шляхом контролю всього апаратного забезпечення та віртуальних ресурсів, як локальних, так і хмарних (рис. 2).

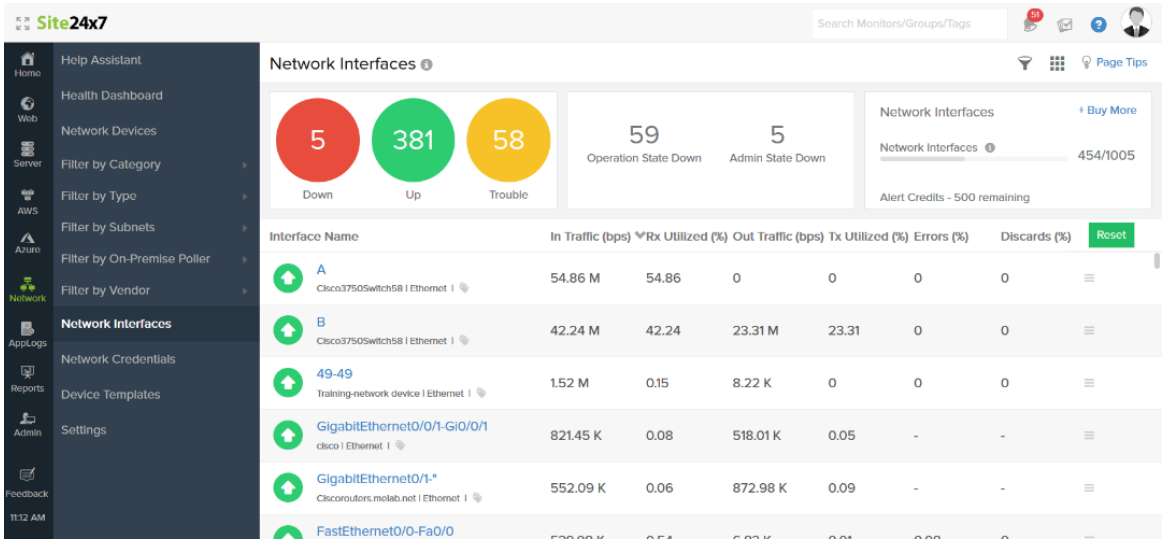

Рисунок 2. Візуальний інтерфейс «Site24x7»

Site24x7 спостерігає за справністю праці веб-сайту та сповіщає, коли виявляє конкретну аномалію. Рішення для моніторингу спостерігає за діяльністю таких служб, як протоколи передачі файлів (FTP - File Transfer Protocols), порогові значення подій, прості протоколи передачі пошти (SMTP - Simple Mail Transfer Protocols), керування продуктивністю додатків (APM - Application Performance Management) і моніторинг записів систем доменних імен (DNS - Domain Name Systems).

Мінуси: налаштування реєстратора транзакцій займає багато часу та розширений інтерфейс може бути складним для навігації у структурі сайту.

3) Sematext Monitoring [4]. Це єдиний інструмент моніторингу для серверів, програм і стеків у багатохмарних середовищах. Програма відстежує серверні процеси, а також усі системні пакети, їх версії, встановлення, видалення і тощо.

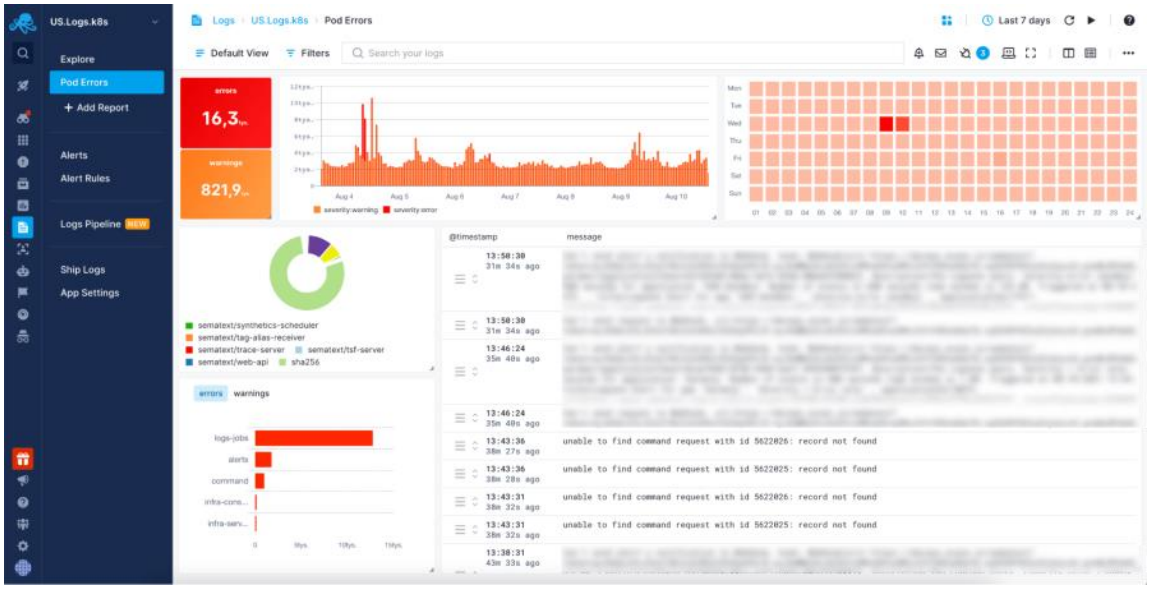

Рисунок 3 - Візуальний інтерфейс «Sematext Monitoring»

Також, рішення для моніторингу надає все необхідне в одному місці для кращого та швидшого усунення несправностей із виявленням аномалій, попередженням і кореляцією між усіма компонентами, кластерами та контейнерами. Усі показники, що стосуються вашого серверу, надаються для перегляду, включаючи ЦП, пам’ять, використання диска, введення-виведення, мережу, навантаження тощо.

З іншого боку програма не нова, хоча все ще оновлюється і відсутність документації для старих агентів робить вивчення інтерфейсу складнішим, і не ідеальність агентів для певної інтеграції, які повинні надсилати власні показники. Ще можна визначити обмежену підтримка відстеження транзакцій.

Усі вищезазначені приклади стосуються як централізованих систем, так і розподілених. Кожна програма передбачає подібне рішення, що можна налаштувати через інтерфейс додатка. Для нормального стану роботи сервера пропонується використовувати ряд основних показників, що потрібні для моніторингу ресурсів:

- **Моніторинг здоров’я** – це загальна інфраструктура, яка вимагає моніторингу стану апаратного забезпечення фізичного сервера, стану гіпервізора,

стан віртуальної машини, фізичної та віртуальної мережі, комутатори та маршрутизатори, а також системи зберігання.

- **Моніторинг продуктивності** – базова продуктивність, перевіряє стан ЦП, внутрішньої пам'яті і показники продуктивності мережі від гостьової віртуальної машини ОС, а також з гіпервізора. Ці показники зазвичай контролюються навіть у невіртуалізованих середовищ. Метрики віртуалізації можуть бути для конкретних сутностей, які вводяться через різні технології віртуалізації, наприклад, кластері концепції центрів обробки даних у **VMware**. Поведінки інших функцій віртуалізації також можна виміряти такими показниками, як частота міграцій віртуальної машини, або у задіяних функцій масштабованості. Є спеціалізовані програми, створені за допомогою віртуалізації як віртуалізація робочого столу (VDI). Моніторинг для такого рішення потребує збору додаткових параметрів з віртуальної машини, а також рівня гіпервізора, наприклад час обслуговування для віртуальної машини, наданої у відповідь на запит на підключення до робочого столу кінцевим користувачем.
- **Моніторинг потенціалу**. Сучасні організації справді динамічні, а використання ресурсів/вимоги до них постійно розвиваються. Отже, потрібно постійне планування різноманітних ресурсів, таких як сервери, робочі столи, мережа та сховище. Ця потреба вимагає періодичних перевірок як фізичних, так і віртуальних ресурсів. Моніторинг ємності вимагає наскрізного безперервного моніторингу ємності за такими ключовими показниками:

1) **Використання пам’яті**: використання пам’яті на кожному сервері, вузькі місця ємності та зв’язок із кількістю користувачів.

2) **Використання сервера**: пікове/середнє використання ресурсів сервера – пам’ять/ЦП/ресурс, вузькі місця сервера та кореляція з показниками робочого навантаження, такими як кількість користувачів.

3) **Використання мережі**: пікове/середнє використання мережі, пропускна здатність/вузькі місця та зв’язок із кількістю користувачів/віртуальної машини.

4) **Використання мережі**: пік/середнє використання мережі, пропускна здатність/вузькі місця та зв’язок із кількістю користувачів.

- **Безпека та моніторинг відповідності** - представляє новий набір ризиків для безпеки через розповсюдження віртуальних машин та автономних віртуальних машин. Жива міграція віртуальних машин потенційно може конфліктувати зі способом керування доступом і застосуванням ряду правил. ІТ-безпека та моніторинг відповідності стають критично важливими для захисту віртуалізованого середовища. Моніторинг безпеки та його відповідності потребують наскрізної перевірки активності через віртуалізацію, а саме:

1) **Розповсюдження віртуальної машини**: метрики для моніторингу активності віртуальної машини під час її клонування, копіювання чи міграції в межах мережі або навіть у інше місце зберігання.

2) **Показники конфігурації**: моніторинг конфігурації віртуального сервера, щоб переконатися, що вони відповідають стандартам і вказівкам щодо посилення, моніторинг конфігурації віртуальної машини для застосування політики ліцензування програмного забезпечення.

3) **Події віртуалізації**, які допомагають застосовувати/виявляти порушення ІТ-політики. Це включає моніторинг індивідуальної безпеки, політики безпеки організації.

4) **Контроль доступу**: моніторинг контролю доступу та звіти для примусового контролю доступу на основі ролей.

5) **Моніторинг відповідності**: Метрики для перевірки/аудиту IT-налаштувань і процесів для стандартів і такі нормативні акти, як HIPAA, SOX, GLBA.

Безпосередньо, архітектура програми повинна бути відкритою, щоб її було легко розширити, підключивши нові модулі на будь-якому рівні. На найнижчому рівні повинен знаходиться моніторинг збору даних, який взаємодіє з різними джерелами даних загального моніторингу. Він призначений для збору даних з усіх доступних джерел. Віртуальна інфраструктура являє собою апаратне забезпечення (сервер, мережа та сховище) та програмні компоненти (гіпервізори та програмне забезпечення для керування). Інші компоненти, з яких збирач даних моніторингу отримує дані, — це база даних конфігурації та наявні інструменти для моніторингу продуктивності програми. Верхній рівень моніторингу займається аналітикою Рівень аналітики обробляє зібрані дані та створює різноманітні аналітичні результатів. Основна перевага можливості збирати дані з різних джерел полягає в тому, щоб гарантувати, що отримані аналітичні результати є точними та дієвими. Тут наголошується на тому, що аналіз не повинен давати рекомендації щодо розміщення, які не відповідають певній безпеці чи мережевій політиці.

Платформа повинна надавати два зовнішні інтерфейси. Один — інтерфейс користувача, який відображає звіти на основі аналітичних модулів, інтегрованих із структурою. Інші можливості інтерфейсу користувача дозволяють адміністраторам налаштовувати параметри, що керують аналітичною обробкою. Наприклад, адміністратор може встановити порогові значення для використання в обчисленнях. Сповіщення та попередження можуть відображатися в інтерфейсі користувача або доставлятися до налаштованих кінцевих точок. Інший інтерфейс — це інтерфейс API, який дозволить іншим стороннім рішенням створювати можливості цієї структури. Інтерфейс API забезпечить доступ до необроблених даних, а також до результатів аналітичних обчислень.

Усі рівні інфраструктури повинні дотримуватися архітектури, що підключається з інтерфейсами, визначеними таким чином, що модулі можуть створюватися незалежно для розширення його можливостей, наприклад, незалежний модуль може бути написаний для додавання можливості збору даних для підтримки нового гіпервізора або надання додаткових аналітичних можливостей.

Висновки. Сьогодні існують різні програми для збору та аналізу даних, але кожна з них має певні складності, з якими може зіткнутися інженер або системний адміністратор, що може зменшити якість моніторингу даних, та піддати ризику роботу серверу. До розробки власної програми моніторингу у віртуалізованому середовищі треба мати широке рішення для підходу моніторингу та аналізу поточних даних. Для впровадження цього треба запропонувати відкриту систему моніторингу, яка призначена для подолання деяких із цих проблем. Є потреба у розробці консолідованої основи для моніторингу з додаванням модулів для розширення загальних можливостей. Цікавим є рішення повної віртуалізації процесів моніторингу з його подальшим використанням на практиці. Це потребує особливого рішення для моніторингу, що буде здатний автоматизувати виявлення та вирішення проблем з сервісним обладнанням. Проблема сьогодення полягає в тому, що рішення для моніторингу спеціалізуються лише на кількох аспектах загального моніторингу, і, отже, аналіз не можна підтвердити для аспектів, які не охоплюються системою, що вимагає ручного втручання для затвердження рекомендацій щодо конфігурації.

Список використаних джерел:

1. Некряч Д. О. Система захисту сервера автентифікації RADIUS від DoS атак: магістерська дис. техн. наук: 121 Програмна інженерія. Київ, 2020. 107 с.

2. Маноха Л. Ю., Гаркуша І. Д. Дослідження і обґрунтування доцільності створення центрів обробки даних в організаціях з розгалуженою інфраструктурою. *Наукові праці НУХТ*. К.: НУХТ, 2008. № 24. С. 5-6.

3. Nilesh Jayanandana. 10 Best Server Performance Monitoring Tools & Software in 2022: презентація. URL: https://sematext.com/blog/server-monitoring-tools/ (дата публікації: 06.06.2022).

4. Lawrence Williams. 10 BEST Server Monitoring Tools & Software (Nov 2022): презентація. URL: https://sematext.com/blog/server-monitoring-tools/ (дата публікації: 07.11.2022).

5. Chandran M., Walvekar J. Monitoring in a Virtualized Environment. *GSTF Journal on Computing*. 2014. Т. 1. №. 1.

6. Лупина І. Б. Пристрій багатокритеріального моніторингу стану металообробного обладнання: дис. техн. наук: 151 Автоматизація та комп’ютерно-інтегровані технології, 2021.147 с.

7. Суховерша В. О. Розробка веб-сервісу для моніторингу роботи серверного обладнання: дис. комп’ют. наук: 122 Комп’ютерні науки, 2021. 169 с.

8. Kadir E. A. et al. Wireless monitoring for big data center server room and equipments. *2015 International Conference on Science in Information Technology (ICSITech)*. IEEE, 2015. С. 187-191.