МОНІТОРИНГ РЕСУРСІВ ДОСТУПУ ДО ПОСЛУГ ІНТЕРНЕТ ДЛЯ СИСТЕМ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Куліков І.В., Сабурова С.О.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: svitlana.saburova@nure.ua,
ihor.kulikov@nure.ua

Abstract

Modern e-commerce systems require complex infrastructure, where downtime directly impacts revenue. This paper explores monitoring methods for ensuring high availability, performance, and compliance with system requirements for quality metrics and security of e-commerce platforms. A multi-layered monitoring architecture is proposed, integrating ICMP, SNMPv3, NetFlow/sFlow/IPFIX technologies, ELK stack log analysis, and quality of experience (QoE) assessment through synthetic and real-world user monitoring (RUM). A structured diagnostic methodology enables systematic incident investigation, from basic connectivity checks to application log analysis. The analysis shows that to effectively ensure the parameters of stability and productivity of e-commerce systems, it is necessary to implement a comprehensive monitoring system, using a variety of methods. The key factor is not only the prompt identification of the problem, but also the collection of business-oriented data: hundreds of successful transactions, something that directly contributes to the reduction of service capacity and trust clients.

Сучасна система електронної комерції – це складна багатокомпонентна інфокомунікаційна інфраструктура, доступність і продуктивність якої безпосередньо впливає на фінансову компоненту. Втрати, навіть від короткочасного простою веб-сайту або сервісу доставки, можуть бути значними, тому активний та ефективний моніторинг стає важливо критичним компонентом інфраструктури, що забезпечує параметри якості обслуговування та конкурентну перевагу.

Мета роботи: дослідження, систематизація та адаптація методів моніторингу ресурсів доступу до послуг Інтернет для забезпечення високої доступності, продуктивності та безпеки систем електронної комерції на основі надійної інфокомунікаційної інфраструктури.

Основним завданням є побудова архітектури багаторівневої системи моніторінгу, що використовує різні методики та технології для повної оцінки стану інфокомунікаційної інфраструктури та користувацьго досвіду.

Для оперативного виявлення проблем з доступом до ключових вузлів, таких як: фронтенд-сервери, API-шлюзи та сервіси доставки, найбільш ефективним на першому етапі є використання ICMP-моніторингу(ping,traceroute,mtr). Він дозволяє швидко виявити недоступність хосту, вимірювати затримку, визначати відсоток втрати пакетів та аналізовувати маршрут трафіку інфокомунікацій. Однак, слід мати на увазі, що ICMP-пакети часто фільтруються мережними екранами та ресурсами провайдерів, тому його результати потрібно корелювати з даними інших методів. Для отримання наочних даних, запускати ICMP-моніторинг потрібно регулярно з кількох географічно розподілених точок (synthetic monitoring).

Для отримання детальної інформації про стан мережного обладнання застосовується SNMP-моніторинг. Він дозволяє збирати метрики завантаження реурсів доступу, інтерфейсів,стану портів, наявність помилок, а також використання процесору та пам'яті задіяного обладнання. Для електронної комерції критично важливим є моніторинг пограничних маршрутизаторів та каналів, що зв'язують в цілому систему з технологією CDN (Content Delivery Network). Для забезпечення моніторингу та безпеки в робочих середовищах системи рекомендовано використовувати SNMPv3.

Аналіз трафіку за допомогою технологій NetFlow, sFlow/IPFIX дає змогу перейти від моніторингу окремих інтерфейсів до моніторингу об'єктів та потоку передачі даних. Це дозволяє ідентифікувати топ споживачів трафіку, виявляти DDoS-атаки, мережні аномалії та нехарактерні потоки передачі даних, що можуть свідчити про витік даних, тощо. Для електронної комерції це важливо для визначення найбільш навантажених API-ендпоінтів, аналізу навантаження в пікові години та планування місткості канальних ресурсів доступу до послуг Інтернет.

Ключову роль в глибокому аналізі відіграє моніторинг логів. Використання сучасних інструментів, таких як: стек ELK(Elasticsearch, Logstash, Kibana) або Greylog, дозволяє не просто збират дані, а й активно досліджувати причини інцидентів. Наприклад, аналіз access-логів вебсерверів, що дає змогу не тільки фіксувати помилки, а й моніторити динаміку часу відгуку по ендпоінтам, що дозволяє виявити «вузьке місце» у системі та мережі доступу ще до критичного прояву.

Також моніторинг потрібен для оцінки параметрів якості користувацького досвіду(QoE) за допомогою комбінації двох підходів: синтетичний моніторинг(synthetic monitoring) та моніторинг реальних користувачів(RUM). Синтетичні сценарії – імітують шлях користувача, запускаються з різних географічних точок та дозволяють виявити проблеми до того, як їх відчують реальні користувачі. Моніторинг реальних користувачів – збирає метрики безпосередньо з якості роботи браузерів клієнтів, надаючи дані з їхнього досвіду.

На основі проведеного дослідження запропоновано стандартний підхід до моніторингу та аналізу інцидентів, який включає наступні кроки:

1. Швидка перевірка ресурсів доступності: виконання команд ping та traceroute.
2. Аналіз стану мережних інтерфейсів: перевірка завантаження трафіку, наявність помилок та статусу портів споживача та служб Інтернет за допомогою SNMPv3.
3. Вивчення трафіку: аналіз за допомогою NetFlow на предмет аномалій, DDoS-атак або незвичайного трафіку.
4. Пошук причин в логах: аналіз логів веб-сервісів, додатків та БД на предмет порушення норм якості обслуговування через помилки.

Аналіз показує, що для ефективного забезпечення параметрів стабільності та продуктивності систем електронної комерції потрібно впровадити комплексну багаторівневу систему моніторингу, що поєднує різні методи. Ключовим фактором є не лише оперативне виявлення проблеми, але й збір бізнес-орієнтованих даних: відсоток успішних транзакцій, тощо, що безпосередньо впливає на покращення якості сервісу та довіру клієнтів.

*Л*ітература

1. Василевський О. М., Поджаренко В. О. Нормування показників надійності технічних засобів. Вінниця: ВНТУ, 2010. 130 с.

2. ДСТУ 2861-94 Державний стандарт України. Надійність техніки. Аналіз надійності. Основні положення. Київ: Держстандарт, 1994. 16 с.

3. Лемешко О. В., Єременко О. С., Невзорова О. С. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість. Харків: ХНУРЕ, 2020. 308 с.

4. Лемешко О. В., Єременко О. С., Євдокименко М. О., Шаповалова А. С., Слейман Б. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах // Монографія. Х.: ХНУРЕ, 2022. 198 с.

5. Ageyev D.V., Evlash D.V. Multiservice telecommunication systems design with network's incoming self-similarity flow // Proceedings of International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science. TCSET 2008. Lviv-Slavsko, 2008. P. 403 – 405.