УДК 004.75

АВТОНОМНЕ ВИЯВЛЕННЯ ТА УСУНЕННЯ «СІРИХ ЗБОЇВ» У ХМАРНИХ СЕРЕДОВИЩАХ ЗА ДОПОМОГОЮ АГЕНТА ACSA

Оліярник С.Я.
e-mail: sviatoslav.oliiarnyk@nure.ua
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна

This paper presents the Adaptive Control System Agent (ACSA) for the autonomous detection and targeted remediation of gray failures within cloud-native environments. Traditional infrastructure monitoring often fails to detect such differential observability states, leading to undetected application degradation. To address this gap, the proposed architecture integrates continuous synthetic canaries with targeted configuration management. By leveraging serverless computing components, such as AWS Lambda, the agent executes rapid, isolated recovery actions without disrupting the underlying host instances. The implemented hierarchical escalation algorithm effectively isolates faults and reduces Mean Time to Recovery (MTTR) by over 98% compared to standard virtual machine reboots. Experimental validation confirms that this approach minimizes service degradation, ensures continuous high availability, and optimizes overall system reliability.

Стрімкий розвиток контейнеризованих мікросервісних архітектур загострює проблему забезпечення стабільності та високої доступності сервісів (High Availability). Сучасні хмарні платформи критично вразливі до феномену «сірих збоїв» (Gray Failures) — складних системних станів, що характеризуються ефектом диференціальної спостережуваності (differential observability). У таких станах інфраструктурні детектори відмов фіксують нормальну роботу компонента (Status: Healthy), тоді як продуктивність застосунку з точки зору кінцевого користувача катастрофічно деградує [1]. Традиційні інструменти інфраструктурного моніторингу (Health Checks), орієнтовані на оцінку використання базових апаратних ресурсів (CPU, RAM), довели свою фундаментальну неспроможність своєчасно детектувати такі неявні аномалії. Це зумовлює необхідність переходу до телеметрії на основі клієнтського досвіду (Golden Signals, за методологією Google SRE) [2] та інтеграції концепцій агентоорієнтованої спостережуваності.

Метою доповіді є проєктування, практична реалізація та експериментальне дослідження ефективності спеціалізованого програмного агента ACSA (Adaptive Control System Agent), призначеного для автономного виявлення мережевих аномалій та проактивного, точкового відновлення працездатності розподілених вебсервісів в умовах часткової деградації.

Для надійного детектування ефекту диференціальної спостережуваності агент ACSA використовує концепцію синтетичного

моніторингу. На відміну від традиційних інструментів, скрипти-«канарки» (наприклад, на базі AWS CloudWatch Synthetics) проактивно імітують поведінку кінцевих користувачів, тестуючи ендпоінти ззовні за заданим розкладом. Це дозволяє фіксувати об'єктивні метрики успішності транзакцій та мережевих затримок. Щоб уникнути хибних спрацьовувань, система застосовує алгоритми виявлення викидів (Outlier Detection), що аналізують відхилення поточних даних від медіанних значень. Такий підхід перетворює неявні «сірі збої» на чітко детектовані аномалії, локалізовані до конкретного вузла [3].

Процес ліквідації інциденту функціонує як повністю автоматизований замкнений контур. Коли показники канарки перетинають критичний поріг, генерується системна тривога, яка через комунікаційну шину подій миттєво активує керуючу безсерверну функцію AWS Lambda. Ця функція визначає ідентифікатор скомпрометованого екземпляра та ініціює виконання ідемпотентних команд відновлення через захищений інтерфейс AWS Systems Manager (SSM Run Command). Використання ідемпотентних скриптів гарантує перевірку поточного стану служби перед втручанням, запобігаючи дублюванню дій. Це створює умови для швидкого відновлення працездатності без впливу на загальну інфраструктуру.

Удосконалено методологію автоматизованого управління IT-інцидентами шляхом розробки ієрархічного алгоритму ескалації відновлювальних дій. На відміну від класичних пласких скриптів реагування, запропонований підхід комплексно поєднує механізми безперервного синтетичного тестування клієнтських транзакцій (Synthetic Canaries), що імітують реальний трафік, із цільовим, низькорівневим управлінням конфігурацією через інтерфейси AWS Systems Manager (SSM). Такий підхід дозволяє точково перезапускати або налаштовувати лише окремі сервіси (наприклад, пули з'єднань вебсервера), а не всю віртуальну машину. Це допомагає уникнути перебоїв у роботі та значно економить час [3].

Стандартні механізми автоматичного відновлення хмарних провайдерів (наприклад, AWS EC2 Auto-Recovery) базуються на метриках інфраструктурного рівня та не здатні детектувати деградацію на рівні прикладного програмного забезпечення. Крім того, базовою реакцією таких систем є повне перезавантаження віртуальної машини, що призводить до обриву всіх мережевих з'єднань та простою тривалістю 60-90 секунд. Натомість розроблений агент ACSA, використовуючи синтетичний моніторинг, виявляє приховані збої та застосовує методику «точкового лікування» (цільовий перезапуск сервісу) [4]. Це дозволяє скоротити безпосередній час усунення несправності (Remediation Time) на понад 98% (до 1 секунди) без зупинки операційної системи та втрати суміжних обчислювальних процесів. Зменшення MTTR до мілісекундного діапазону та мінімізація часу деградації (MTTD) є прямим свідченням підвищення

загальної надійності системи згідно з критеріями ефективності Lean Software та DevOps-метрик [5].

Отже, розроблений інтелектуальний агент ACSA доводить високу ефективність у боротьбі з феноменом прихованих відмов у розподілених хмарних системах. Використання синтетичного моніторингу для виявлення диференціальної спостережуваності у поєднанні з ієрархічною ескалацією та гранулярним відновленням через AWS SSM дозволяє обійти обмеження традиційних інфраструктурних перевірок. Запропоноване рішення кардинально мінімізує час деградації сервісу, забезпечуючи високу доступність та стабільність клієнтського досвіду без застосування деструктивних методів повного перезавантаження.

Список використаних джерел:

1. Huang P., Guo C., Zhou L. [та ін.]. Gray failure: The Achilles' heel of cloud-scale systems. Proceedings of the 16th Workshop on Hot Topics in Operating Systems. 2017. P. 150–155. URL: https://doi.org/10.1145/3102980.3103005.

2. Beyer B., Jones C., Petoff J., Murphy N. R. Site reliability engineering: How Google runs production systems. O'Reilly Media, 2016. 524 p. URL: https://sre.google/books/.

3. Reliability Pillar – AWS Well-Architected Framework / Amazon Web Services. 2024. URL: https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/welcome.html (дата звернення: 09.03.2026).

4.Cloud security and surgical remediation actions / Sysdig. 2024. URL: https://www.sysdig.com/ (дата звернення: 09.03.2026).

5. Forsgren N., Humble J., Kim G. Accelerate: The science of lean software and DevOps: Building and scaling high performing technology organizations. IT Revolution, 2018. 288 p. URL: https://itrevolution.com/product/accelerate/.