УДК 004.85:004.75

АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДІВ АВАРІЙНОГО ВІДНОВЛЕННЯ СИСТЕМ В ХМАРНИХ СЕРЕДОВИЩАХ

Гунько Б. Г.
e-mail: borys.hunko@nure.ua
Науковий керівник – к.т.н., доц. Білова Т. Г.
Харківський національний університет радіоелектроніки, каф. КМІТ
м. Харків, Україна

This work is devoted to assessing the efficiency of disaster recovery methods within cloud environments. The fundamental strategies for ensuring business continuity were considered. A comparative analysis of these methods' efficiency is carried out based on Recovery Time Objective and Recovery Point Objective metrics. It has been found that the implementation of automation through the Infrastructure as Code approach and predictive Artificial Intelligence algorithms is effective solution for minimizing downtime and eliminating configuration inconsistency across environments in modern distributed systems.

Сучасна цифрова інфраструктура вимагає доступності, що вимірюється не годинами, а секундами. Провайдери хмарних послуг здатні забезпечити вищу стійкість системи [1]. Проте навіть міграція до хмари не усуває ризики, а лише частково їх мінімізує. Основною проблемою є невідповідність між швидкістю відновлення даних та готовністю інфраструктури. Справа в розсинхронізації конфігурацій між основним та резервним середовищем розгортання, коли через різницю в налаштуваннях та відсутність автоматичного аварійного відновлення під час інциденту адміністраторам доводиться вручну налаштовувати інфраструктуру, що збільшує Recovery Time Objective (RTO) та може призводити до нових помилок.

Розглянемо поширені стратегії disaster recovery (DR):

– backup and restore – регулярне резервне копіювання даних і систем для полегшення відновлення після аварії в резервному регіоні. Обчислювальні потужності інфраструктури не активні до моменту інциденту. Є найбільш економним з точки зору витрат та може забезпечувати низький показник Recovery Point Objective (RPO), але RTO є дуже високим;

– pilot light – запуск найбільш критичних служб, таких як бази даних та сховища файлів, в резервному регіоні разом з резервними копі даних. Запуск та масштабування додаткових служб відбувається за потреби у разі інциденту. Такий підхід вимагає додаткових коштів на підтримання постійно запущених сервісів, проте забезпечує менший, але все ще потенційно відчутний, час відновлення;

– warm standby – забезпечення зменшеної, але повністю функціональної копії виробничого середовища в резервному регіоні. В разі інциденту

ресурси масштабуються. Вимагає значних коштів для підтримання всієї інфраструктури особливо для великих систем, проте дозволяє значно скоротити RTO та забезпечити низький RPO;

– multi-site active/active – розгортання в повному масштабі в кількох географічних регіонах, які обслуговують трафік. При інциденті трафік перенаправляється на інший регіон. Має високу складність і вимагає значних фінансових витрат, проте допомагає забезпечити майже нульовий час простою при правильному виконанні [1].

Для поліпшення RTO пропонується автоматизувати процес DR та впровадження ШІ для передбачення аварійних ситуацій.

Інструменти Infrastructure as Code (IaC), такі як Terraform та Ansible, є невід'ємною частиною автоматизації процесу DR. Вони дозволяють визначати конфігурації інфраструктури за допомогою коду та створювати на його основі ресурси в хмарі. Це дозволяє в разі інциденту розгортати за допомогою однієї команди в терміналі всю інфраструктуру, що суттєво підвищує час відновлення. Окрім швидкості, ключовою перевагою IaC є детермінованість, оскільки середовища генеруються з одного репозиторію, вони гарантовано ідентичні, що повністю усуває проблему несумісності конфігурацій і дозволяє усунути людський фактор під час критичних збоїв. При використання IaC в CI/CD конвеєрах сценарії аварійного відновлення, такі як створення резервних копій і відновлення інфраструктури, виконуються в скрипті [2], що забезпечує розгортання всієї інфраструктури впродовж хвилин.

Перспективним є використання алгоритмів машинного навчання в діагностиці проблем в системі та ШІ-агентів для повного автономного підтримання інфраструктури системи в разі інцидентів. Основна концепція полягає у створенні циклів зворотного зв'язку, де системи постійно контролюють свій стан, аналізуючи логи, трейси та метрики, виявляють відхилення від бажаних умов, планують відповідні реакції та виконують коригувальні дії. Такий підхід робить систему більше стійкою до загроз, оскільки виявлення проблем і реакція на них відбувається на ранньому етапі.

Стратегія і підходи до аварійного відновлення систем мають формуватися в залежності від складності інфраструктури, її критичності, та фінансових спроможностей організації, проте для забезпечення найшвидшого повернення системи до нормального стану та мінімізації втрат даних важливо забезпечити автоматизацію процесу DR.

Список використаних джерел:

1. Сердюк Н. Основні складнощі при виборі архітектури хмарного додатка. Інформаційні системи та технології : Міжнар. науково-техн. конф., м. Харків, 17 листоп. 2020 р. Харків, 2020. С. 214–216.

2. Disaster recovery options in the cloud. https://docs.aws.amazon.com . URL: https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html (дата звернення: 09.03.2026).