АНАЛІЗ ПІДХОДІВ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ АРХІТЕКТУР EXTENDED CLOUD

Недоступ Д.М., Солом'яний М.В.

Кафедра «Інфокомунікаційної інженерії ім. В.В. Поповського»,
Харківський національний університет радіоелектроніки, Україна

E-mail: daniil_nedostup@nure.ua,
maksym.solomianyi@nure.ua

Abstract

An analysis of modern approaches to ensuring the resilience of Extended cloud architectures based on Fog and Edge Computing was conducted. Relevant and contemporary solutions for increasing cloud computing platforms' resilience are covered. Policy-based management is recommended as an effective approach to managing complex systems. These policies help set up fault-tolerance schemes and describe real-time strategies for adapting the system to external or internal adverse factors.

Розробка та впровадження інфокомунікаційних систем стають складнішими, масштабнішими та вразливішими. Тому сьогодні технологічний бізнес перш за все потребує надійної, стабільної, захищеної, оптимізованої, масштабованої та відмовостійкої інфраструктури для розробки технічних і технологічних продуктів.

Для виконання вищезазначених вимог все більше організацій при плануванні власної інфраструктури віддають перевагу саме Cloud Computing – хмарним обчисленням. Основні причини зростання популярності Cloud Computing полягають у підтримуваних бізнес-моделях, які в кінцевому підсумку призводять до зниження витрат і пропонують значну масштабованість та послуги з надання ресурсів на запит [1]. Ключові характеристики хмарних обчислень, а саме підтримка повсюдного підключення, еластичність, масштабованість і легкість розгортання, дозволяють використовувати подібні обчислювальні середовища для таких передових та актуальних мереж як Інтернет речей (Internet of Things, IoT) [2]. Сучасні тенденції використання технологій IoT створюють нові умови для обслуговування інфраструктури та підтримки відмовостійкості, які хмарні середовища не можуть задовільнити належним чином [3-5]. Ці вимоги включають, але не обмежуються географічною розподіленістю, низькою затримкою, визначенням місцезнаходження та підтримкою мобільності.

Нові моделі, такі як Edge та Fog Computing – граничні та хмарні обчислення, які прийнято називати Extended Cloud, розширюють можливості хмарних обчислень і допомагають виконати вищевказані умови щодо забезпечення відмовостійкості [2, 6]. Використовуючи дані моделі, можна підвищити якість надання послуг, оскільки зменшується затримка при передачі даних між кінцевими вузлами та хмарою. Незважаючи на всі переваги використання моделей Fog і Edge, перехід до Extended Cloud додає власних недоліків. Використовуючи хмарні обчислення, користувач обмежений у контролі над обладнанням, програмним забезпеченням і даними, що може призвести до проблем з безпекою. Збої, зумовлені даними проблемами, також порушують вимоги щодо відмовостійкості в системах, в той час, коли цей фактор повинен бути головною властивістю хмарних платформ.

Отже, було проведено аналіз сучасних підходів забезпечення відмовостійкості архітектур на базі Extended Cloud [1-3, 6]. Відмовостійкість визначається як «*здатність системи забезпечувати прийнятний рівень обслуговування за наявності проблем*» [2]. Зі свого боку прийнятний рівень обслуговування залежить від очікувань і вимог користувача. У поточних умовах користувачам потрібен швидкий доступ до інформації в будь-який час. Однак запропоновані хмарними обчисленнями властивості роблять реалізацію стандартних рішень забезпечення відмовостійкості більш проблематичною.

Тому для вирішення цієї проблеми в процесі використання Extended Cloud слід дотримуватися шестиступінчастої стратегії D^2R^2+DR (***D**efend, **D**etect, **R**emediate, **R**ecover, **D**iagnose and **R**efine*) [2]. В основі даної стратегії лежать циклічні процеси, які в реальному часі виявляють проблеми в роботі мережі та їх вплив на неї, а також аналізують показники (метрики), що можуть кількісно оцінити стан мережі [1].

Кожен окремий процес D^2R^2+DR має власну зону відповідальності та призначення, а саме:

1. *Defend* – першочерговий захист хмарних обчислень від внутрішніх і зовнішніх факторів, наприклад налаштування правил брандмауера.
2. *Detect* – виявлення, класифікація та аналіз проблем, які порушили оптимальний процес надання послуг.
3. *Remediate* – реабілітація процесів, вживання автономних дій для максимально швидкого поновлення надання послуг і зменшення збитків викликаних зовнішніми або внутрішніми несприятливими чинниками.
4. *Recover* – відновлення працездатності хмарних обчислень після повного усунення несприятливого чинника (відмови, збою) або ворожої кібер-атаки.
5. *Diagnose* – діагностика та аналіз усуненої проблеми.
6. *Refine* – прийняття рішень щодо запобігання проаналізованої проблеми в майбутньому, наприклад, реконфігурація певних компонентів або зміна логіки окремих процесів.

Головною перевагою стратегії D^2R^2+DR є використання політик для управління поведінкою системи [2]. Оскільки проблеми в роботі хмарної інфраструктури можуть виникати несподівано та непередбачувано, вони вимагають швидкого реагування на відновлення прийнятного рівня обслуговування. Щоб пом'якшити проблему, потрібні складні багатоетапні стратегії, які поєднують різні механізми моніторингу і виявлення, що впливають на поведінку механізмів відновлення [2]. Тому управління на основі політик виявляється достатньо ефективним для управління складними системами. Дані політики допомагають налаштовувати схеми відмовостійкості, а саме дозволяють описувати стратегії адаптації системи до зовнішних або внутрішних несприятливих чинніків у реальному часі, тим самим підвищуючи рівень відмовостійкості.

Таким чином, у нову еру все більшого розгортання програмно-конфігурованих інфокомунікаційних мереж (особливо з використанням Fog та Edge Computing) ключові властивості безпеки та відмовостійкості залишаються відкритими для подальшого вивчення. Деякі завдання, пов'язані з безпекою та відмовостійкістю, вже були вирішені в контексті Cloud Computing, однак вимоги, що висуваються новими областями надання послуг, наполегливо вказують на необхідність перегляду питань забезпечення безпеки та відмовостійкості.

Література:

1. *Moura J., Hutchison D.* Resilience Enhancement at Edge Cloud Systems. IEEE Access. 2022. Vol. 10, pp. 45190-45206. DOI: https://doi.org/10.1109/ACCESS.2022.3165744

2. *Shirazi S.N., Gouglidis A., Farshad A., Hutchison D.* The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective. IEEE Journal on Selected Areas in Communications. 2017. Vol. 35, No.11. P. 2586-2595. DOI: https://doi.org/10.1109/JSAC.2017.2760478

3. *Rak J., Hutchison D. (eds)* Guide to Disaster-Resilient Communication Networks. Computer Communications and Networks. Springer, Cham. 2020. 813 p. DOI: https://doi.org/10.1007/978-3-030-44685-7

4. *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. DOI: https://doi.org/10.30837/978-966-659-282-1

5. *Персіков М.А., Жерноклеєв В.С., Рибінський В.М.* Створення глобальної мережі розумних пристроїв на основі концепції Internet of Everything. Третя міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірник наукових праць. Харків: ХНУРЕ. 2019. С. 129. URL: http://openarchive.nure.ua/handle/document/8532

6. *Єременко О.С., Круглова А.О., Журавльова А.С., Персіков М.А.* Особливості забезпечення відмовостійкості в Cloud, Fog та Edge Computing системах. Матеріали шостої Міжнародної науково-технічної конференції «Проблеми електромагнітної сумісності перспективних бепроводових мереж зв'язку ЕМС-2020». Харків: ХНУРЕ, 2020. С. 95-96. URL: http://openarchive.nure.ua/handle/document/13939