КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2019.3.104111
УДК 004.7

Яскевич Владислав Олександрович
Кандидат технічних наук, доцент кафедри комп'ютерних наук і математики
Київський університет імені Бориса Грінченка, Київ, Україна
OrcID0000-0002-5796-2521
v.yaskevych@kubg.edu.ua

Клочко Олександр Юрійович
Аспірант
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0001-6552-2844
alexanderklochko@ukr.net

МЕТОДИ ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ ІНТЕРНЕТ СЕРВІСІВ

Анотація. В статті розглядається проблема забезпечення відмовостійкості інтернет сервісів. Вона набуває все більшої важливості внаслідок зростання кількісних параметрів функціонування інформаційних систем (користувачів, серверів, обсягів інформації в базах даних) і рівня складності. Внаслідок значного навантаження на сервери, на яких розгорнуто додатки, виникають відмови апаратного або програмного забезпечення. Актуальність пошуку додаткових шляхів забезпечення відмовостійкості, надійності й безперебійного функціонування комп'ютерних систем, що працюють у реальному масштабі часу, обумовлена зростанням вимог, що висуваються до безпеки виконуваних процесів або об'єктів, доступ до яких обмежений. Незважаючи на застосування наявних методів забезпечення відмовостійкості в хмарних інфраструктурах, існує проблема невідповідності фактичної готовності систем рівням «Стійка до відмов» (Fault Tolerance) і «З високою готовністю» (High Availability) для критичних і бізнес-критичних веб додатків. Також менше уваги приділяється методам підвищення відмовостійкості для високо-навантажених систем. Тому пошуки нових можливостей масштабування та балансування навантаження при побудові хмарних систем набувають особливого значення. Для проведення порівняльного аналізу алгоритмів балансування навантаження були запропоновані функціональні характеристики, згідно яких можливо робити обґрунтований вибір алгоритмів, що найбільше відповідають конкретним практичним обставинам і вимогам користувачів та провайдерів. До основних принципів реалізації стратегії відмовостійкості на цей час входять резервування, діагностування, реконфігурація, відновлення. В якості додаткових показників контролю відмовостійкості пропонується застосовувати повноту резервування елементів і вузлів системи, повноту і достовірність контролю, ймовірність відновлення резерву. Перші дві стратегії передбачають, що система, яка правильно виконує свій алгоритм функціонування, є безпечною. Стратегія безпечної поведінки при відмовах використовується спеціально для безпечних систем і полягає в переході системи в захисний необоротний стан у випадку виникнення відмови.

Ключові слова: веб сервіс; планування розподілу завдань; розподілені інформаційні системи; надійність

1. ВСТУП

У зростанні популярності і збільшенні користувачів мережі Інтернет останнім часом важливу роль відіграють інтернет сервіси і хмарні технології. Проблема забезпечення відмовостійкості інтернет сервісів набуває все більшої важливості внаслідок невпинної тенденції зростання кількісних параметрів функціонування інформаційних систем (користувачів, серверів, обсягів інформації в базах даних тощо),

ISSN 2663 - 4023

а, отже, і рівня складності. У різних інтернет-ресурсів і систем зростає кількість користувачів, що справляє значне навантаження на сервери, на яких розгорнуто додатки, внаслідок чого виникають відмови апаратного або програмного забезпечення. Подібні відмови в роботі систем є небезпечними, оскільки спричиняють втрату частини інформації, що призводить до багатьох негативних наслідків, зокрема, до значних фінансових втрат як у випадку сервісів електронної комерції. Наприклад, китайська інтернет-компанія Alibaba продала товарів на рекордні 160 млрд юанів ($25,3 млрд) у «День холостяка» 2018 року: в моменти пікового навантаження сервери Alibaba обробляли 256 тис. транзакцій за секунду..

Стан розробленості проблеми. Традиційно для підвищення відмовостійкості застосовуються технології апаратного та інформаційного резервування серверів і інформації, що обробляється. Апаратне резервування полягає в створенні дублікатів серверів або створенні віртуальних серверів, що дублюють оригінали. Віртуалізація передбачає створення набору обчислювальних ресурсів або їхнього логічного об'єднання, які абстрагуються від апаратної реалізації, що забезпечує відокремленість обчислювальних процесів, які виконуються на одному фізичному ресурсі [1]. Інформаційне резервування забезпечує збереження цілісності даних та підвищення надійності систем збереження даних. Воно реалізується за допомогою реплікації БД та створення резервних сховищ файлів [2].

Дослідженню шляхів вирішення проблеми підвищення відмовостійкості інтернет сервісів були розглянуті відомі методи, зокрема:

- використання кластера сервісів і балансування навантаження на кластер [3];
- багаторівневе кешування результатів SQL-запитів до БД [4];
-застосування для роботи з БД засобів об'єктно-реляційного відображення [5].

Окремим напрямом є розроблення рішень для високонавантажених сервісів в інфраструктурі великих веб сайтів, електронній комерції, провайдерах хостингу тощо [6].

Важливість такої властивості як відмовостійкість необхідно розглядати у взаємопов'язаності з іншими функціональними якостями інформаційних систем (ІС). Так, під надійністю системи розуміють її властивість зберігати працездатність в заданих умовах функціонування. Надійність є комплексною властивістю, що включає такі складові, як безвідмовність, ремонтопридатність, збережуваність і довговічність, а також безпечність, відмовостійкість та живучість. Відносно відмовостійкості в літературі поширені дещо відмінні дефініції, які, втім, збігаються в основному розумінні [1]. В контексті даної статті будемо спиратися на наступне визначення: відмовостійкість (Fault Tolerance) — це властивість системи зберігати повну або часткову працездатність у випадках відмов окремих елементів, що непов'язані із зовнішніми нерегламентованими діями [7].

Але з появою і глобальним розвитком хмарних технологій акцент в розробці інструментів підвищення відмовостійкості перемістився в сферу не апаратних, а програмних рішень. Зрозуміло, що апаратна складова систем не відійшла на задній план, залишаючись важливим фактором загальної відмовостійкості системи. Тим не менше, головні зусилля інтернет спільноти зосередилися на розробці і застосуванні нових рішень, що обумовлюються особливостями функціонування хмарних технологій. Таким чином, паралельно із пошуком засобів підвищення відмовостійкості апаратної частини систем активно розвиваються інструменти software.

Впровадження хмарних концепцій змінює пріоритети в сфері інформаційних технологій (ІТ). Першорядного значення набувають інформаційні ресурси, на розробку

ISSN 2663 - 4023

яких спрямовуються основні зусилля. Комп'ютерні пристрої як такі відступають на другий план. Незалежно від типу, марки, виробника й місце знаходження кожне з них лише повинне забезпечувати доступ до мережевих сервісів. При цьому хмарний підхід дозволяє створити доступне інформаційне середовище й забезпечити синхронізацію діяльності користувачів, що здійснюється з різних пристроїв (робоча станція, домашній комп'ютер, особистий планшет, смартфон і т.п.).

Мета статті. забезпечення надійності та відмовостійкості веб-сервісів.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Актуальність пошуку додаткових шляхів забезпечення відмовостійкості, надійності й безперебійного функціонування комп'ютерних систем, що працюють у реальному масштабі часу, обумовлена зростанням вимог, що висуваються до безпеки виконуваних процесів або об'єктів, доступ до яких обмежений. Розглядаючи шляхи або засоби забезпечення відмовостійкості, слід одразу наголосити на принциповій зміні підходів після появи і розвитку розподілених систем взагалі і хмарних технологій зокрема. Мається на увазі, що на початкових етапах становлення комп'ютерних мереж відмовостійкість їх функціонування забезпечувалася за аналогією з підходами до електричних мереж або мереж зв'язку. Тобто головним чином реалізовувався підхід апаратного резервування [2]. На той час це був виправданий підхід, зважаючи на те, що відмови апаратних пристроїв, їх компонент призводять в кращому випадку до тимчасових відмов функціонування системи, в гіршому — до втрати даних. Висока складність та мініатюрні розміри електронних пристроїв роблять їх дуже чутливими до якості електричного живлення. Комп'ютер, що є в складі ІС, може вийти з ладу не тільки внаслідок збою операційної системи, дій користувача чи зловмисника, а й в результаті збою апаратного пристрою. Навіть найкращі операційні системи є надійними настільки, наскільки надійною є їх апаратна платформа.

Хмарні диски захищено від апаратних відмов з використанням технологій відмовостійкості enterprise-класу RAID-DP, яка забезпечує збереження і доступність даних навіть при одночасному виході з ладу двох дисків. Фізичні ресурси, що їх використовує хмарна система збереження даних (СЗД), не мають точок відмови (SPo), які було б не зарезервовано.

Функціонування динамічно мінливої композиції веб-сервісів і утвореної ними слабозв'язаної системи в цілому не входить до компетенції жодного з учасників і повністю лягає на ініціатора утвореної композиції. На надійність функціонування сторонніх веб-сервісів ініціатор композиції вплинути не може, а в цілому вплинути на надійність композиції може, забезпечивши надмірність функціональних можливостей веб-сервісів композиції за рахунок резервування функціонально подібними веб-сервісами.

Створення сервісів пов'язане з конче важливим феноменом: сервіси між собою можуть конфліктувати. Для того, щоб знайти й усунути причини конфліктів і їхніх ініціаторів, ІТ-інфраструктура моделюється мережами Петрі. Відсутність конфлікту між наявними й доданими сервісами полягає в збереженні всіх властивостей базової моделі в новій моделі. Це означає, що конфліктів, які призводять до взаємного блокування чи блокування одним сервісом роботи іншого, в такій системі не відбуватиметься.

Планування розподілу задач у хмарних обчисленнях постає серйозним викликом для розробників. В загальній постановці робота з планування хмарних обчислень полягає у відправленні обчислювальних завдань багатьох користувачів до спільного

ISSN 2663 - 4023

пулу ресурсів згідно встановлених квот та поточної ситуації в хмарному середовищі. На даний час відсутній єдиний стандарт для планування роботи в середовищі хмарних обчислень. Управління ресурсами та планування розподілу завдань виступають ключовими технологіями хмарних обчислень, які відіграють вирішальну роль в ефективному використанні хмарних ресурсів і підвищенні відмовостійкості.

Незважаючи на застосування наявних методів забезпечення відмовостійкості в хмарних інфраструктурах, існує проблема невідповідності фактичної готовності систем рівням «Стійка до відмов» *(Fault Tolerance)* і «З високою готовністю» *(High Availability)* для критичних і бізнес-критичних веб додатків. Також менше уваги приділяється методам підвищення відмовостійкості для високо-навантажених систем. Тому пошуки нових можливостей масштабування та балансування навантаження при побудові хмарних систем набувають особливого значення.

Хмарні технології і Web сервіси належать до високонавантажених систем, тому можливості масштабування та балансування навантаження при побудові і забезпеченні функціонування хмарних систем набувають особливого значення. На даний момент інформація про такі аспекти "хмарних технологій" як масштабування та балансування навантаження розрізнена та вимагає систематизації та впорядкування. Для вирішення цієї задачі важливим являється вибір критеріїв. Також актуальним аспектом вирішення проблеми є вибір засобів балансування навантаження, які б найкращим чином відповідали задачам створення конкретного сервісу в певних умовах. Балансування навантаження напряму впливає на підвищення ефективності роботи хмарної системи, а також сприяє підвищенню її відмовостійкості. Для забезпечення узгодженої роботи вузлів обчислювальної мережі на стороні хмарного провайдера використовується спеціалізоване проміжне програмне забезпечення, що забезпечує моніторинг стану обладнання і програм, балансування навантаження, забезпечення ресурсів для вирішення завдання.

Хмарні системи автоматично контролюють і оптимізують використання ресурсів через вимір деяких абстрактних параметрів. Параметри варіюються в залежності від типу послуги. Наприклад, це можуть бути: розмір сховища даних, обчислювальна потужність, пропускна здатність і/або число активних записів користувача. Використання ресурсів контролюється і відстежується в автоматичному режимі з формуванням певних звітів. Таким чином і постачальник, і споживач отримують прозору інформацію щодо обсягу наданих (спожитих) послуг. Виміряти використані користувачем ресурси можна за показником часу, який був витрачений під час роботи додатків чи операційної системи або як загальну потужність процесора за певний період.

Важливою є здатність хмарних систем до швидкої адаптації. Обчислювальні можливості можуть швидко і гнучко резервуватися (головним чином в автоматичному режимі) для оперативного масштабування під завдання замовника, і також швидко звільнятися. З точки зору споживача доступні можливості часто виглядають нічим не обмеженими і можуть бути придбані в будь-якій кількості в будь-який час. Таким чином, масштабованість, відмовостійкість і безпека забезпечуються за рахунок автоматичного виділення і звільнення необхідних ресурсів залежно від потреб додатку.

Для проведення порівняльного аналізу алгоритмів балансування навантаження були запропоновані функціональні характеристики, згідно яких можливо робити обґрунтований вибір алгоритмів, що найбільше відповідають конкретним практичним обставинам і вимогам користувачів та провайдерів.

До основних принципів реалізації стратегії відмовостійкості на цей час входять

резервування, діагностування, реконфігурація, відновлення. В якості додаткових показників контролю відмовостійкості можна застосовувати повноту резервування елементів і вузлів системи, повноту і достовірність контролю, ймовірність відновлення резерву. Перші дві стратегії передбачають, що система, яка правильно виконує свій алгоритм функціонування, є безпечною. Стратегія безпечної поведінки при відмовах використовується спеціально для безпечних систем і полягає в переході системи в захисний необоротний стан у випадку виникнення відмови.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Функціонування динамічно мінливої композиції веб-сервісів і утвореної ними слабозв'язаної системи в цілому не входить до компетенції жодного з учасників і повністю лягає на ініціатора утвореної композиції. На надійність функціонування сторонніх веб-сервісів ініціатор композиції вплинути не може, а в цілому вплинути на надійність композиції може, забезпечивши надмірність функціональних можливостей веб-сервісів композиції за рахунок резервування функціонально подібними веб-сервісами.

Хмарні диски захищено від апаратних відмов з використанням технологій відмовостійкості enterprise-класу RAID-DP, яка забезпечує збереження і доступність даних навіть при одночасному виході з ладу двох дисків. Фізичні ресурси, що їх використовує хмарна СЗД, не мають точок відмови (SPo), які було б не зарезервовано.

IT-індустрія почала широко використовувати концепцію веб-сервісів, результатом чого стала поява сервіс-орієнтованої архітектури (Service-oriented architecture, SOA). Формальні специфікації цієї архітектури були опубліковані одразу двома групами - OASIS (Organization for the Advancement of Structured Information Standards) та The Open Group. SOA є парадигмою, призначеною для проектування, розробки та управління дискретними одиницями логіки (сервісів) в обчислювальному середовищі [4]. Насамперед, термін SOA з'явився для опису виконуваних компонентів (таких як веб-сервіси), які можуть викликатися іншими програмами, що виступають у ролі клієнтів або споживачів сервісів такого компонента.

Інфраструктура, що заснована на застосуванні веб-сервісів, користується високим рівнем абстракції й містить у собі пов'язану з даними семантичну інформацію, тобто веб-сервіси визначають не тільки дані, але й порядок обробки й перетворення цих даних у базові програмні додатки.

Наступне покоління мережі буде засноване на програмно-орієнтованих взаємодіях. Програмно-орієнтовані взаємодії будуть автоматично виконувати операції, які раніше обов'язково вимагали "ручного" втручання: - пошук і покупка товарів і послуг за найбільш вигідною ціною; - узгодження замовлень авіаквитків і місць у ресторані на певну дату (планування подорожей); - оптимізація комерційних операцій закупівлі товарів, виписки рахунків і доставки. Веб-сервіси є не тільки інтерфейсом об'єктів, програм, програмного забезпечення й баз даних для доступу до мережі. Об'єднання ряду веб-сервісів дозволяє здійснювати нові типи взаємодії. Використання веб-сервісів дуже вигідно з комерційної точки зору. За рахунок повсюдного поширення веб-сервісів Інтернет набуває все більшої ефективності, особливо при здійсненні комерційних операцій.

Сполучаючи прямій доступ до програмних додатків і комерційних документів, веб-сервіси наступного покоління мережі забезпечать повністю автоматичну

взаємодію, що дозволить звертатися безпосередньо до даних програм, ігноруючи знайомі веб-сторінки. Більш того, основні компоненти веб-сервісів, будуть надаватися й публікуватися безліччю різних компаній, що спеціалізуються на окремих функціональних елементах (перевірка повноважень, координація угод, ведення рахунків). Це забезпечить безпосередню взаємодію " додаток-додаток" - принцип, що лежить в основі веб-сервісів і визначає їхню суть і реалізацію.

Напрями подальших досліджень:

- Аналіз взаємозв'язків таких властивостей хмарних технологій як доступність, продуктивність, надійність, відмовостійкість;
- систематизація підходів до забезпечення відмовостійкості інтернет сервісів;
- порівняння характеристик методів і алгоритмів балансування навантаження за функціональними критеріями;
- обґрунтування та розробка інтернет сервісу із розподіленою архітектурою;
- автоматизація процесу розгортання інтернет сервісу в хмарному середовищі;
- дослідження ефективності запропонованих архітектурних та програмних рішень для підвищення відмовостійкості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Б. Г. Мудла, Г. С. Теслер, О. В. Федухін О.В. та ін. “Дослідження відмовостійких обчислювальних засобів у критичних інформаційних системах обробки інформації та керування об’єктами на основі мережної взаємодії”, ІПММС НАН України, №204U006760, 2004.

[2] А. Медведев, “Облачные технологии: тенденции развития, примеры исполнения”, Современные технологии автоматизации, № 2, с.6-9, 2013.

[3] M. P. Papazoglou, “Web Services: Principles and Technology”, Prentice Hall, vol. 21, pp. 139-14, 2012.

[4] P. Murray, B. Melander, B. Fusenig, M. Meulle, L. Vaquero, “Cloud Networking Architecture Description”, Scalable and Adaptable Internet Solutions, pp. 14-69, 2011.

[5] А. А. Билаш, А. Ю. Белобородов, К. А. Бохан под ред. В. С. Харченко, Технологии Web, Grid, Cloud для гарантоспособных ИТ-инфраструктур. Харків, Україна: Нац. аэрокосм. ун-т им. Н. Е. Жуковского "ХАИ", 2013.

[6] The cloud-ready data center network: Applying the lessons of cloud computing to vastly improve economics of networking and the user experience / Juniper Networks [Online]. Available: http://www.juniper.net/us/en/local/pdf/brochures/1600040-en.pdf. Accessed on: 12.07.2016.

[7] NIST Cloud Computing Standards Roadmap. – Special Publication 500-291, Version 2. – U. S. Department of Commerce; National Institute of Standards and Technology, 2013.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023

Vladyslav O. Yaskevych
PhD, assistant professor
Borys Grinchenko Kyiv University, Faculty of Information Technology and Management, Kyiv, Ukraine
OrcID 0000-0002-5796-2521
v.yaskevych@kubg.edu.ua

Klochko Y. Oleksandr
Graduate student
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0001-6552-2844
alexanderklochko@ukr.net

METHODS TO IMPROVE THE FAULT-TOLERANCE OF INTERNET SERVICES

Abstract. The article deals with the problem of ensuring the fault-tolerance of Internet services. It is becoming increasingly important due to the growth of the quantitative parameters of the functioning of information systems (users, servers, volumes of information in databases) and the level of complexity. Due to the heavy load on the servers on which the applications are deployed, there is a failure of hardware or software. The urgency of finding additional ways to ensure the fault tolerance, reliability and uninterrupted functioning of computer systems operating in real time, due to the increasing requirements for the security of running processes or objects, access to which is limited. Despite the use of existing methods for ensuring fault tolerance in cloud infrastructures, there is a problem of inconsistency between the actual availability of systems and the levels of "fault tolerance" (Fault Tolerance) and "High Availability" (High Availability) for critical and business critical web applications. Also, less attention is paid to methods of improving fault tolerance for highly loaded systems. Therefore, the search for new opportunities for scaling and load balancing when building cloud systems is of particular importance. To conduct a comparative analysis of load balancing algorithms, functional characteristics were proposed, according to which it is possible to make an informed choice of algorithms that most closely correspond to specific practical circumstances and the requirements of users and providers. The basic principles for implementing a resiliency strategy now include redundancy, diagnostics, reconfiguration, and recovery. As an additional indicator of failover control, it is proposed to apply the completeness of the booking of elements and components of the system, the completeness and reliability of the control, the probability of reserve recovery. The first two strategies assume that a system that correctly performs its functioning algorithm is safe. The safe behavior strategy for failures is used specifically for safe systems and consists in the transition of the system to a protective irreversible state in the event of a failure.

Keywords: web service; job scheduling; distributed information systems; reliability.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] B. G. Mudla, G. S. Tesler, O. V. Fedukhin O.V. etc. "Investigation of fault-tolerant computing means in critical information systems of information processing and object management on the basis of network interaction", IPMMS NAS of Ukraine, №204U006760, 2004. (in Ukrainian)

[2] A. Medvedev, “Cloud technologies: development trends, examples of performance”, Modern automation technologies, # 2, pp.6-9, 2013. (in Russian)

[3] M. P. Papazoglou, “Web Services: Principles and Technology”, Prentice Hall, vol. 21, pp. 139-14, 2012. (in English)

[4] P. Murray, B. Melander, B. Fusenig, M. Meulle, L. Vaquero, “Cloud Networking Architecture Description”, Scalable and Adaptable Internet Solutions, pp. 14-69, 2011. (in English)

[5] A. A. Bilash, A. Yu. Beloborodov, K. A. Bokhan, ed. V. S. Kharchenko, Web, Grid, Cloud Technologies for Guaranteed IT Infrastructures. Kharkiv, Ukraine: Nat. aerospace. un-t them. N.Ye. Zhukovsky "KhAI", 2013. (in Russian)

[6] The cloud-ready data center network: Applying the lessons of cloud computing to vastly improve economics of networking and the user experience / Juniper Networks [Online]. Available: http://www.juniper.net/us/en/local/pdf/brochures/1600040-en.pdf. Accessed on: 12.07.2016. (in English)

[7] NIST Cloud Computing Standards Roadmap. – Special Publication 500-291, Version 2., U. S. Department of Commerce; National Institute of Standards and Technology, 2013. (in English)