УДК 004. 056.53

Є. В. Ланських, *к.т.н., доцент,*
А. О. Литвиненко, *магістрант*
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
evlans@mail.ru, anna.litvinenko.z@gmail.com

ПІДВИЩЕННЯ НАДІЙНОСТІ ДАНИХ В СИСТЕМАХ ХМАРНИХ ОБЧИСЛЕНЬ

Стаття присвячена питанню надійності даних при роботі з системами хмарних обчислень. Розглядаються рівні та методи підвищення надійності дата-центрів. Проводиться порівняння рівнів надійності стандарту TIA EIA 942 та обирається найбільш оптимальний, який доцільно використовувати при оцінюванні дата-центру. Обґрунтовуються причини використання цього стандарту та вибір найоптимальнішого рівня надійності дата-центру. Розглядається технологія реплікації/резервування даних, що знаходяться в хмарі. Для забезпечення високої доступності хмарних обчислень запропоновано використовувати технологію high availability disaster recovery (HADR). Виділяються основні переваги використання цієї технології як при часткових, так і при повних аваріях.

Ключові слова: *системи хмарних обчислень, стандарт TIA EIA 942, рівні надійності дата-центрів, резервування даних у хмарі, забезпечення відмовостійкості, high availability disaster recovery (HADR).*

Як один із найбільш перспективних способів оптимізації IT-інфраструктури нині все частіше розглядаються хмарні обчислення.

Модель хмарних обчислень складається із зовнішньої (front end) і внутрішньої (back end) частин. Ці два елементи з'єднані по мережі, в більшості випадків через Інтернет. За допомогою зовнішньої частини користувач взаємодіє з системою; внутрішня частина – це власне сама хмара. Зовнішня частина складається з клієнтського комп'ютера або мережі комп'ютерів підприємства та програм, які використовуються для доступу до хмари. Внутрішня частина надає додатки, комп'ютери, сервери та сховища даних, що створюють хмару сервісів.

Останнім часом компанії в погоні за рейтингом та продуктивністю нехтують надійністю своїх дата-центрів [1].

Метою написання статті є визначення оптимального механізму забезпечення високого рівня доступності даних у системах хмарних обчислень.

Сучасні компанії намагаються знайти компроміс між вартістю обслуговування дата-центрів (додаткові системи охолодження, обладнання для резервування даних) та їх рівнем надійності.

Висока готовність хмарних обчислень передбачає наявність механізму резервування, який у разі відмови основної системи перенаправляє запити і завдання з обробки даних резервній системі. Оскільки технічні та системні вимоги завжди різняться, універсальної конфігурації не існує і повинні братися до уваги різні параметри системи, що впливають на її продуктивність, доступність, масштабованість і надійність.

При розробці стратегії побудови хмарних обчислень однією з найважливіших проблем є забезпечення надійності даних, що знаходяться в системі. На теперішній час найбільш використовуваним є стандарт TIA EIA 942 [2].

Пропонований інструмент для оцінки надійності дата-центру у вигляді певних параметрів і вимог до інженерних систем дозволяє оцінити і визначити рівень надійності центру обробки даних (ЦОД). Для кожного з виділених рівнів надійності в стандарті TIA EIA 942 наводиться детальний опис, вимоги та рекомендації до таких систем і елементів: архітектурних рішень, електропостачання, охолодження, безпеки, протипожежної системи, структурованої кабельної системи, системи кабелепроводів, телекомунікацій.

Центри обробки даних на теперішній момент класифікуються за чотирма рівнями надійності – tier 1, tier 2, tier 3, tier 4.

Перший рівень надійності ЦОД. Цей рівень застосовувався для дата-центрів в 60-і й 70-і роки минулого століття. Помилки і відмо-

ви в роботі систем і устаткування на цьому рівні призводять до збоїв у роботі всього ЦОД. Також робота центру обробки даних переривається для проведення профілактичних і ремонтних робіт. У ЦОД може не бути фальшпідлог, резервних джерел електропостачання та джерел безперебійного живлення (ДБЖ).

−Інженерна інфраструктура створена тільки для задоволення поточних потреб, тобто без резервування та надлишкових ресурсів (забезпечення потреб виражається у вигляді літери «N»).

−Час простою за рік – 28,8 годин.

−Коефіцієнт відмовостійкості – 99,671 %.

Другий рівень надійності ЦОД. Дата-центри на другому рівні мають невеликий рівень резервування працездатності систем і невеликі надлишкові ресурси в інженерних системах дата-центру, але все одно схильні до перебоїв через планові та непланові відмови роботи обладнання в дата-центрах. Для цього рівня необхідно мати фальшпідлогу, резервні джерела електропостачання ЦОД. Проведення технічних і ремонтних робіт потребує зупинки роботи центру обробки даних.

−Система не має повного резервування, проте встановлені додаткові елементи в системах охолодження і енергопостачання ЦОД (забезпечення потреб виражається у вигляді формули «N+1»).

−Час простою за рік – 22,0 години.

−Коефіцієнт відмовостійкості – 99,749 %.

Третій рівень надійності ЦОД. Дата-центр з цим рівнем надійності дозволяє провести ремонтно-профілактичні роботи без зупинки роботи ЦОД. Тобто можливі одночасно експлуатація і технічне обслуговування центру обробки даних аж до заміни компонентів системи, додавання і видалення обладнання, що вийшло з ладу. Щоб забезпечити третій рівень, необхідно спроектувати та побудувати два трубопроводи для охолодження системи, забезпечити резервними потужностями роботу всього обладнання з урахуванням виходу з ладу або профілактики системи електропостачання. Але помилки в роботі і відмови можуть викликати перебої в роботі дата-центру.

−Має кілька шляхів (каналів) для розподілу електроживлення та охолодження, але лише один із них активний; має резервовані компоненти (забезпечення потреб виражається у вигляді формули «N +1»).

−Час простою за рік – 1,6 години.

−Коефіцієнт відмовостійкості – 99,982 %.

Четвертий рівень надійності ЦОД. Відмовостійкий дата-центр з резервуванням усіх систем дозволяє виконати будь-які планові та позапланові роботи без переривання роботи ЦОД. На цьому рівні забезпечується надійний захист від збоїв. Щоб відповідати вимозі четвертого рівня надійності, необхідне дублювання всіх систем з урахуванням того, що в кожній системі та її «резервній копії» перебуватиме, як мінімум, ще один додатковий компонент, який забезпечує резервування за схемою «N+1». Тобто в дата-центрі має бути резервування системи на рівні «N+1», і сама система ще повинна бути, як мінімум, продубльована. Відмови можуть мати місце у випадках ручного аварійного відключення системи електропостачання та спрацювання системи пожежної безпеки. На четвертому рівні навіть структурована кабельна система повинна бути повністю зарезервована.

−Системи мають подвійне резервування з урахуванням, як мінімум, додаткового компонента. Має кілька активних шляхів розподілу навантаження й охолодження з резервними компонентами 2(N+1), тобто два ДБЖ з надмірністю N+1 кожен (забезпечення потреб виражається у вигляді формули «2(N+1)»).

−Час простою за рік – 0,4 години.

−Коефіцієнт відмовостійкості – 99,995 %.

На сьогоднішній день четвертий рівень надійності tier-4 засвідчує, що дата-центр є відмовостійким з резервуванням усіх систем. Щоб відповідати критеріям четвертого рівня надійності, дата-центру потрібно витрачати більше коштів на забезпечення надійності, що відбивається на вартості хмарних послуг. Тому нині найоптимальнішим є третій рівень надійності центру обробки даних. Дата-центр з цим рівнем надійності дає можливість провести ремонтно-профілактичні роботи без зупинки роботи центру обробки даних, але все ж таки помилки та рідкі перебої в роботі системи допустимі.

Одним із питань, що забезпечують відновлення системи третього та четвертого рівнів надійності, є здатність системи до самовідновлення після аварій. Час такого відновлення відіграє важливу роль у роботі системи та повинен бути мінімальним.

Для забезпечення відмовостійкості на рівні шлюзу встановлюють у фермі Web-серверів кілька шлюзів – по одному на кожному сервері. Точка входу Web-ферми (зазви-

чай це маршрутизатор або інвертований проксі-сервер) повинна підтримувати перенаправлення запитів наступному доступному Web-серверу у разі відмови основного сервера. Наступним кроком є активація системою технології High availability disaster recovery (HADR) [3] (рис. 1).

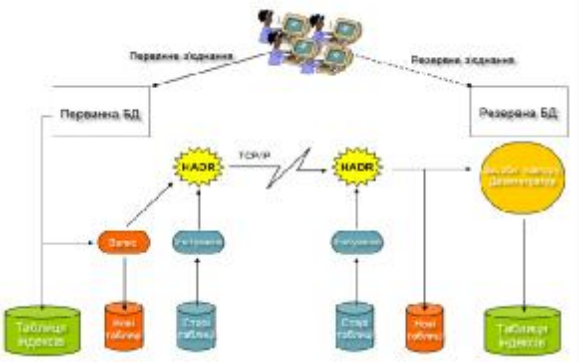

Рис. 1. Загальна архітектура HADR

HADR – це можливість реплікації бази даних, що забезпечує рішення високої доступності як при часткових, так і при повних аваріях систем. HADR захищає від втрати даних за рахунок реплікації змін даних з вихідної бази даних (вона називається первинною) в базу даних призначення (вона називається резервною).

Прикладні програми можуть звертатися тільки до поточної первинної бази даних. Зміни вносяться в резервну базу даних шляхом повтору транзакцій за даними таблиці індексів, які генеруються в первинній базі даних і передаються потім резервній базі даних.

Часткова відмова вузла може статися з причини відмови апаратури, мережі або програмного забезпечення (DB2 або операційної системи). Якщо HADR не використовується, після часткової аварії системи потрібне перезавантаження сервера або комп'ютера СУБД, де знаходиться база даних. Час перезапуску бази даних і комп'ютера, на якому вона розташована, непередбачуваний. Перш ніж база даних знову буде приведена в узгоджений стан і стане доступною, може пройти кілька хвилин. За допомогою HADR первинну базу даних можна підмінити резервною за кілька секунд. Клієнтів, що використовують вихідну первинну базу даних, можна перенаправити на резервну базу даних (яка тепер стала первинною базою даних) за допомогою автоматичного перенаправлення клієнтів або алгоритмів повтору операцій у прикладних програмах.

Повна відмова вузла може статися при аварійній ситуації (наприклад, при пожежі), яка призведе до знищення всього вузла. Оскільки HADR використовує TCP/IP для зв'язку між первинною і резервною базами даних, ці бази даних можна розташувати в різних місцях. Якщо аварія відбудеться на первинному вузлі, доступність даних збережеться, тому що дистанційна резервна база даних підмінить первинну базу даних з повними функціональними можливостями DB2. Після передачі функцій резервній системі можна взяти резервну копію первинної бази даних і повернути цю базу даних у стан первинної.

Коли вихідна первинна база даних буде повернута в пару HADR в ролі резервної бази даних, можна переключити ролі баз даних, щоб знову зробити вихідну первинну базу даних первинною базою даних.

При використанні HADR можна задати один із трьох режимів синхронізації, вибравши бажаний рівень захисту від потенційної втрати даних. Режим синхронізації визначає спосіб управління передачею записів журналу між первинною і резервною базами даних. Ці режими застосовуються, тільки коли первинна і резервна бази даних знаходяться в рівноправному стані:

SYNC (синхронний): цей режим забезпечує найбільший захист від втрати транзакцій, але при його використанні час відповіді транзакцій є максимальним серед трьох можливих режимів.

NEARSYNC (майже синхронний режим): мінімальна можливість втрати даних у разі одночасного виходу з ладу основної і резервної баз даних.

ASYNC (асинхронний): забезпечується найкраща продуктивність, однак існує ймовірність втрати даних у разі виходу з ладу основної або резервної бази даних, а також у разі збою мережевого підключення. У нього також найменший час відповіді транзакцій з усіх трьох режимів.

Оптимальним є майже синхронний режим, тому що він є компромісом між продуктивністю та надійністю. Асинхронний режим більш доцільно використовувати для критично важливих задач.

На сьогоднішній день питання надійності даних у системах хмарних обчислень залишається актуальним, адже зі зростанням обчислювальної спроможності ІТ-обладнання

зростають і проблеми з надійністю та коректністю його роботи.

Підводячи підсумок, можна сказати, що використання HADR дозволяє значно підвищувати рівень надійності даних та забезпечувати швидке відновлення працездатності системи хмарних обчислень за рахунок подвійної реплікації бази даних.

Список літератури

1. Niccolai, James (2013). Data centers play fast and loose with reliability credentials. IDG News Service.
2. Telecommunications Industry Association (TIA) [Internet]. Available from: http://www.tiaonline.org/cloud
3. Інформаційний центр IBM [Електронний ресурс]. – Режим доступу : http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp
4. Cnews [Internet]. Available from: http://cloud.cnews.ru/

References

1. Niccolai, James (2013). Data centers play fast and loose with reliability credentials. IDG News Service.
2. Telecommunications Industry Association (TIA) [Internet]. Available from: http://www.tiaonline.org/cloud
3. IBM information center [Internet]. Available from: http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp
4. Cnews [Internet]. Available from: http://cloud.cnews.ru/

Стаття надійшла до редакції 20.01.2014.

Y. V. Lanskykh, *Ph.D., associate professor,*
A. O. Lytvynenko, *undergraduate*
Cherkasy State Technological University
Schevchenko blvd, 460, Cherkasy, 18006, Ukraine
evlans@mail.ru, anna.litvinenko.z@gmail.com

THE GROWTH OF DATA RELIABILITY IN CLOUD COMPUTING SYSTEMS

The article is devoted to the problem of data reliability when working with cloud computing systems. The levels and methods of the growth of data centers reliability are considered. The comparison of reliability levels of TIA EIA 942 standard is made and the most optimal one, which it is expedient to use for data center evaluation, is chosen. The reasons for the use of this standard and the choice of the most optimal level of data center reliability are substantiated. The technology of replication/backup of data, located in a cloud, is considered. To provide high availability of cloud computing the technology of high availability disaster recovery (HADR) is offered to use. Its use allows to significantly raise the level of data reliability and ensure quick renewal of working capacity of cloud computing systems due to database double replication. The basic preferences of using this technology, both in partial and complete breakdowns, are highlighted.

The use of HADR allows to significantly improve data reliability level and to ensure quick renewal of working capacity of cloud computing system due to database double replication.

Key words: *cloud computing systems, TIA EIA 942 standard, data centers reliability levels, data backup in a cloud, fault-tolerance ensuring, high availability disaster recovery (HADR).*