

ОПТИМІЗАЦІЯ ПРОЦЕСІВ АВАРІЙНОГО ВІДНОВЛЕННЯ СЕРВІСІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

М. Кирик [ORCID: 0000-0001-9156-9347], С. Заблоцький [ORCID: 0009-0008-2265-4546],
В. Пограничний [ORCID: 0009-0003-3535-5880], А. Тарасенко [ORCID: 0009-0008-6938-4571]

Національний університет “Львівська політехніка”, вул. С. Бандери, 12, Львів, 79013, Україна

Відповідальний за рукопис: Василь Пограничний (e-mail: vasyly.pohranychnyi@lpnu.ua)

(Подано 1 лютого 2024 р.)

У статті описано оптимізацію процесу аварійного відновлення сервісів інформаційної інфраструктури за рахунок впровадження можливості відновлення роботи сервісу без застосування повного відновлення з місця зберігання резервних копій. Описано критерії та параметри мережі, які мають критичний вплив для відновлення у разі виникнення надзвичайних ситуацій, що дає змогу оцінити ефективність рішення при відновленні після аварій. Запропоновано модифікацію для параметра MTTR (середній час до відновлення) у випадках відновлення елемента системи з резервної копії або через відновлення конфігурації сервісу через інфраструктурний код, у такий спосіб прискорюючи процес відновлення сервісу інформаційної інфраструктури, що вийшов з ладу. Наведено схему організації відновлення інфраструктури шляхом створення резервної локації (Cold Site) для локальної інфраструктури за допомогою провайдерів виділеної хмари. Запропоноване рішення використовує можливості Proxmox Backup Server для створення регулярних резервних копій критично важливих компонентів дата-центру. Розроблено блок-схему методу відновлення сервісу з Cold Site та проведено дослідження, за результатами якого було зроблено висновок, що для деяких сервісів відновлення конфігурації з коду є більш ефективне і прискорює сам процес відновлення порівняно з повноцінним відновленням сервісу з місця зберігання резервних копій.

Ключові слова: надійність, відмовостійка система, надійне проектування, надзвичайні ситуації, Proxmox VE, віртуальна машина.

1. Вступ

Зростання обсягів даних та сервісів змусило компанії вдатися до використання хмарної інфраструктури. Деякі компанії, створюючи персональну приватну хмару, використовують Proxmox Virtual Environment, що дає змогу побудувати інфраструктуру, орендуючи лише обладнання у публічних дата-центрах. Однак дата-центри постійно стикаються з ризиком збоїв, як-от: відмови обладнання, природні катастрофи та кібератаки, що можуть призвести до втрати даних та тривалих періодів простою, відповідно і до серйозних фінансових та репутаційних втрат. Для мінімізації цих ризиків та забезпечення безперервності бізнесу критично важливо впровадити рішення для відновлення після аварій (Disaster Recovery – DR) [1].

Рішення для відновлення інфраструктури, що постраждала під час аварій у дата-центрі, – це комплексна стратегія та набір практик, спрямованих на забезпечення безперервності бізнесу та

доступності даних, що своєю чергою передбачає комбінацію технологій, процесів і політик для мінімізації впливу надзвичайних подій та швидкого відновлення критичних систем і даних. Створення комплексного плану відновлення після аварій у дата-центрі може допомогти мінімізувати потенційні ризики та загрози, підготуватися до можливих катастроф і зменшити їхній вплив на продуктивність та ефективність послуг, які надаються кінцевим клієнтам. Відновлення після аварій у дата-центрі можна вважати успішним, якщо організація здатна легко та швидко відновити роботу без серйозних перебоїв у бізнес-процесах. Одним із важливих кроків у ефективній стратегії відновлення після аварій у дата-центрі є планування способів відновлення кожного елемента системи для продовження роботи інфраструктури загалом [2].

Є декілька ключових аспектів, котрі потрібно враховувати під час відновлення сервісу. Різні сервіси потребують індивідуального підходу до відновлення для зменшення часу не надання послуги. Наприклад, для роботи деяких сервісів достатньо відновити лише файли конфігурації, а є сервіси, котрі потребують повного відновлення даних з місця зберігання резервних копій. Також обговорюються різні стратегії та конфігурації відновлення після аварій, як-от: локальні та віддалені резервні копії, а також знімки стану для створення точок відновлення без необхідності зупинки сервісів. Використання методів дедублікації оптимізує використання сховища резервних копій. Одним із можливих варіантів впровадження є Proxmox Backup Server (PBS), який призначений для безперебійної роботи з Proxmox Virtual Environment (PVE), PVE – це платформа управління віртуалізацією з відкритою кодовою базою, яка дає змогу компаніям будувати свої приватні дата-центри для створення та керування віртуальними машинами та контейнерами. Інтегруючись з PVE, PBS спрощує процес резервного копіювання та відновлення віртуальних машин та контейнерів у інфраструктурах на базі Proxmox.

Основні характеристики Proxmox Backup Server містять:

- інкрементальні резервні копії;
- резервне копіювання на основі знімків стану;
- дедублікацію та стиснення даних;
- кілька варіантів сховищ;
- шифрування та безпеку;
- віддалену синхронізацію;
- підтримку резервного копіювання на стрічкові носії.

Також PBS використовує інтегровану систему моніторингу для контролю стану процесів відновлення, актуальності та ефективності резервних копій, а також для попередження про потенційні пошкодження в процесі резервного копіювання. Моніторинг дає змогу оцінити продуктивність системи резервного копіювання, включно зі швидкістю резервного копіювання та швидкістю передавання даних. Ця інформація допомагає оптимізувати конфігурацію та розклад резервного копіювання [3].

2. Критерії та параметри інформаційної інфраструктури

Рішення для відновлення інфраструктури після аварій у дата-центрі є системою, що характеризується певним набором критеріїв і параметрів основних складових, як-от: резервне копіювання, розподілення обчислювальних та мережевих ресурсів.

Резервне копіювання серверів є важливим із декількох критичних причин:

Запобігання втраті даних: сервери зберігають цінні та здебільшого унікальні дані, зокрема інформацію про користувачів, ділові документи, медичні дані, конфігурації сервісів та баз даних. Регулярне резервне копіювання забезпечує можливість відновлення даних до попереднього стану у випадку їхнього випадкового видалення, пошкодження або втрати внаслідок природних або техногенних катаклізмів, військових дій чи кібератак, а також мінімізуючи час простою та ризики втрати даних.

Безперервність бізнесу (BCM-business continuity management) та відновлення після катастроф: у разі надзвичайних ситуацій, як-от: пожежа, повінь, військові дії або кібератака, наявність актуальних резервних копій дає змогу прискорити процес відновлення. Тож бізнес може швидше відновити роботу сервісів та знизити вплив на клієнтів та дохід.

Захист від шкідливих програм-вимагачів: атаки програм-вимагачів стають усе більш поширеними, вони шифрують дані компаній, утримуючи їх у заручниках до сплати викупу. Якщо в наявності є нещодавні резервні копії, то можна уникнути сплати викупу та відновити свої системи до стану, що передував атаці.

Тестувальні та розробницькі середовища: резервні копії є незамінними для створення тестувальних та розробницьких середовищ, які відтворюють актуальну систему. Тож є можливість тестувати зміни, оновлення або нові додатки, не ризикуючи цілісністю діючих даних або діючих виробничих систем.

Збої обладнання: навіть із найнадійнішим обладнанням та своєчасним і якісним обслуговуванням компоненти сервера можуть виходити з ладу. Резервні копії захищають дані від втрати через проблеми з обладнанням.

Людські помилки: іноді дані можуть бути випадково видалені або змінені помилково. Наявність резервних копій як запасного варіанту запобігає втраті даних та не дає перетворити ці помилкові дії на безвихідну ситуацію.

Версіонування даних: резервні копії дозволяють зберігати кілька версій даних, надаючи можливість повернутись до конкретного моменту в часі, коли було зроблено резервування.

Економія коштів: хоча реалізація резервних копій потребує інвестицій, вона може принести значну економію в довгостроковій перспективі за рахунок зменшення простою та витрат на відновлення даних [4].

Розподіл обчислювальних ресурсів серверів та вибір між кластеризацією з високою доступністю (HA) та заміною обладнання є важливими аспектами у процесі проєктування надійної та стійкої IT-інфраструктури. Обидва підходи спрямовано на забезпечення неперервної доступності та мінімізацію часу простою, але відрізняються за своїм впровадженням та вартістю. Розміщення серверів у різних локаціях, що часто називають географічним резервуванням, є потужною стратегією для запобігання надзвичайних ситуацій в дата-центрах та забезпечення неперервності бізнесу. Розподіляючи сервери по декількох локаціях, організації можуть зменшити вплив регіональних надзвичайних подій або локалізованих інцидентів, які можуть вплинути на один дата-центр.

Підхід з географічним резервуванням має кілька переваг:

Покращена доступність даних: реплікація даних між кількома локаціями забезпечує їхню доступність, оскільки до них можна отримати доступ з будь-якого резервного сайту.

Відновлення після надзвичайних ситуацій: географічне резервування може бути ключовим елементом комплексної стратегії відновлення після інцидентів. Дані та додатки можна відновити з альтернативного місця у випадку збою в роботі основного дата-центру.

Кластер високої доступності (High Availability – HA) складається з декількох серверів, які часто називають вузлами, що працюють разом, щоб забезпечити резервування та можливості аварійного перемикавання. Якщо один вузол у кластері виходить з ладу, то робоче навантаження автоматично перемикається на інший робочий вузол. Кластеризація HA забезпечує високий час безперервної роботи та мінімізує перебої у наданні послуг у випадку збоїв обладнання. Вона надає стійкість до збоїв та дає змогу безперебійно продовжувати операції. Кластери HA вимагають спеціалізованого програмного забезпечення та конфігурацій для управління аварійним перемиканням ресурсів, підтримки цілісності даних та обробки балансування навантаження між вузлами кластера. На рис. 1 показано організацію методу кластеризації високої доступності.

Заміна обладнання передбачає наявність запасних компонентів обладнання, які можуть бути швидко використані для заміни деталей що вийшли з ладу. Коли компонент сервера виходить із

ладу, то він замінюється запасним, щоб відновити функціональність системи. Такий підхід вимагає підтримання запасної інфраструктури для швидкого проведення заміни обладнання.

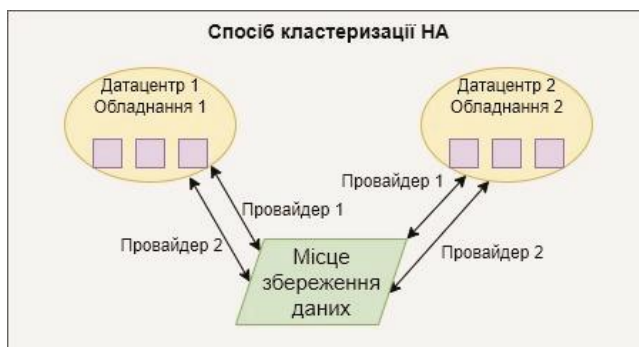


Рис. 1. Організація методу кластеризації високої доступності (НА)

Заміна обладнання, як правило, підходить для не критичних систем або середовищ, де вартість впровадження кластера високої доступності (НА) перевищує вигоди. На рис. 2 показано організацію методу заміни обладнання.



Рис. 2. Організація методу заміни обладнання

Розподіл мережі, відомий як надлишкове резервування або мережеве розмаїття, справді є важливим інструментом для запобігання надзвичайним ситуаціям, забезпечення надійності та стійкості критичних систем зв'язку. Розподіл мережевих ресурсів кількома шляхами, місцями або провайдерами дає змогу організаціям значно знизити ризик збоїв у мережі та покращити загальну доступність мережі під час надзвичайних ситуацій та інших непередбачуваних подій. Розподіл мережі створює додаткові шляхи для передавання даних. Якщо одне мережеве з'єднання або шлях виходить з ладу, то трафік може бути автоматично перенаправлений через альтернативні маршрути, забезпечуючи неперервне з'єднання. Це також дає змогу перенаправляти трафік із сайтів, постраждалих від надзвичайних ситуацій, до непошкоджених місць, зменшуючи вплив регіональних інцидентів або локалізованих збоїв у мережі. Використання різноманітних мережевих шляхів дає змогу компаніям уникати єдиних точок відмови, що призводить до покращення продуктивності та зниження затримок, а використання кількох інтернет-провайдерів (ISP) або мережевих операторів може знизити ризик масштабних проблем зі зв'язком через від'єднання одного провайдера.

Згідно з наведеною інформацією метод кластеризації має слабе місце – спільне зберігання даних і залежність від стабільного з'єднання з провайдером; цей метод потрібно використовувати в розподіленій мережі. Метод заміни не є оптимальним, оскільки деяка інформація може бути втрачена, а процес заміни займає деякий час.

Залежно від технічного завдання використовують методи кластеризації або метод заміни. Також можливе поєднання обох цих методів.

Основні параметри рішення для відновлення після катастрофи містять:

- середній час між збоями (MTBF): середній час між двома послідовними збоями кластера високої доступності;
- середній час на відновлення (MTTR): середній час, який необхідний для відновлення компоненту, що вийшов з ладу в кластері високої доступності, та відновлення його до повністю функціонального стану;
- середній час на повторне розгортання сервісу (MTSR): середній час, який необхідний для повторного розгортання пошкоджених сервісів з інфраструктурного коду;
- середній час на відновлення з резервної копії (MTRB): середній час, який необхідний для відновлення системи з резервного розташування (локального та/або віддаленого);
- доступність (A): відсоток часу, протягом якого кластер високої доступності (HA) є доступним і функціональним протягом конкретного періоду:

$$A = \frac{MTBF}{MTBF + MTTR} \cdot 100. \quad (1)$$

У деяких випадках, коли для відновлення роботи достатньо повторно запустити сервіс, який збережений у вигляді коду, параметр MTTR дорівнює часу, який буде витрачено на виконання операції конфігурації сервісу MTSR, без використання раніше створених резервних копій:

$$MTTR_1 = MTSR \quad (2)$$

У випадках, коли пошкоджено або скомпрометовано не тільки конфігурацію потрібного сервісу, але й інші дані, як-от: бази даних, особисті дані, дані доступу, код конфігурації або у випадку збою сервера, параметр MTTR дорівнює часу, необхідному для відновлення пошкодженого елемента інфраструктури з резервної копії $MTRB_{full}$:

$$MTTR_2 = MTRB_{full} \quad (3)$$

Коли відновлення з коду недостатнє і необхідно відновити дані з резервної копії для роботи сервісу - параметр MTTR буде складатися з суми параметрів MTSR та $MTRB_{data}$.

$$MTTR_3 = MTRB_{data} + MTSR \quad (4)$$

Показники продуктивності: параметри MTRB та MTSR, зазначені вище, можуть бути використані для оцінки різних показників продуктивності, як-от: середній час простою, очікувана кількість збоїв або ймовірність перевищення певного порогу часу простою.

3. Методи створення рішень для відновлення інформаційної інфраструктури після надзвичайних подій

План відновлення після аварій (DR) стосується стратегії організації щодо відновлення доступу та функціональності до її інформаційно-технологічної інфраструктури після таких подій, як природні або техногенні катаклізми, військові дії або кібератаки. План відновлення після аварій може містити різні методи для забезпечення неперервності сервісу. Відновлення базується на реплікації даних та доступності критичних сервісів, які залишаються неушкодженими під час надзвичайної ситуації. У випадку збою сервера через природну катастрофу, відмову обладнання або кібератаку, компанія може відновити втрачені дані з резервного розташування, де вони були заздалегідь збережені.

Основні методи, з якими координується план відновлення після надзвичайних ситуацій, передбачають:

- Резервне копіювання. Зберігання даних поза основним місцем або на зовнішніх носіях інформації. Однак цей метод надає лише мінімальну допомогу в забезпеченні неперервності сервісу, оскільки відсутнє резервне копіювання ІТ-інфраструктури, і у випадку інциденту її потрібно відновлювати вручну.

- Disaster Recovery as a Service (DRaaS), відновлення як послуга – ефективне й доступне рішення щодо забезпечення катастрофостійкості та відновленню інфраструктури в хмарі. Використовуючи DRaaS у випадку аварії на місці або хакерської атаки, сервіси переносять до хмарної інфраструктури провайдера хмарних послуг. Це дозволяє бізнесу продовжувати роботу в хмарі, навіть якщо їхні власні сервери не працюють. Однак цей метод може не працювати належним чином у випадках із локальними сервісами організацій.

- Резервне копіювання як послуга. Цей метод передбачає організацію резервного копіювання даних за участі сторонніх хмарних провайдерів, але недолік також полягає у відсутності реплікації IT-інфраструктури.

- Метод заміни обладнання – Hardware replacement. Це фізичне обладнання, яке знаходиться всередині дата-центру та призначене для заміни пошкодженого обладнання у разі відновлення після надзвичайних подій. Однак цей метод відновлення може бути не ефективним проти зовнішнього втручання в систему.

- Метод з використанням Cold Site. Cold Site – це резервний об'єкт з необхідною основною інфраструктурою, як-от: електропостачання, кондиціонування та комунікації, але там відсутнє попередньо встановлене обладнання та програмне забезпечення. Цей тип відновлення після надзвичайної ситуації передбачає попереднє забезпечення базової інфраструктури на резервному об'єкті або такому, що рідко використовується на сайті. Цей метод вимагає додаткових витрат для організації цієї платформи.

- Метод з використанням Hot Site. Hot Site – це резервний об'єкт, який містить необхідне апаратне і програмне забезпечення, а також активне мережеве під'єднання для можливості роботи в реальному часі. Якщо наданий сервіс має можливість децентралізації та організації кількох сайтів, які дублюють функціональність, то у випадку виходу з ладу одного елемента навантаження буде перенаправлено на другий елемент. Основним недоліком є організація витрат на дублювання сервісів. Дві найважливіші переваги наявності належно спроектованого плану відновлення після надзвичайних ситуацій:

- Економія коштів. Хоча організація плану відновлення після надзвичайних ситуацій може бути дорогою, ці кроки можуть захистити організації від втрати коштів і недоступності сервісу, що своєю чергою можуть призвести до великих фінансових збитків.

- Швидше відновлення. Використовуючи один або кілька методів відновлення та інструментів, організації можуть швидше відновити роботу своїх сервісів і здебільшого забезпечити безперервне обслуговування клієнтів.

На рис. 3 запропоновано схему організації плану відновлення після надзвичайних ситуацій. Ця схема містить кластер Proxmox VE HA, локальне резервне копіювання, резервний сайт, автоматизацію процесів та систему моніторингу.

Під час організації функціональної високої доступності (HA) у Proxmox необхідно організувати спільне зберігання даних між усіма вузлами кластера. Для віртуальних машин, які не будуть створені на спільному середовищі зберігання даних, функцію високої доступності не буде застосовано.

Кластер Proxmox VE може мати різні рівні резервності, як-от використання масивів RAID і програмних, і апаратних для зберігання даних, резервних джерел живлення, агрегації каналів мережевого зв'язку та резервного комунікаційного каналу. Proxmox VE HA не має функціональності для впровадження цих рівнів резервності; однак він доповнює їх, надаючи функціональність для міграції віртуальних машин між вузлами кластера так, щоб вони могли продовжувати працювати під час виходу їхнього вузла з ладу. HA-менеджер – це елемент Proxmox VE, який забезпечує повністю автоматизовану високу доступність для віртуальних середовищ Proxmox [8].

У випадках, коли вузол перестає бути доступним протягом певного часу (за замовчуванням це 60 секунд), його вважають неробочим та ізолюють. Ізоляція запобігає входу в мережу служб кластера протягом цього часу. Після цього віртуальні машини, для яких була увімкнена функція

НА, будуть переміщені до наступного доступного вузла в групі НА. У разі, коли ізольований вузол з віртуальними машинами все ще увімкнено, але мережеве з'єднання з ним нестабільне, Proxmox НА спробує перемістити віртуальні машини на інший вузол.

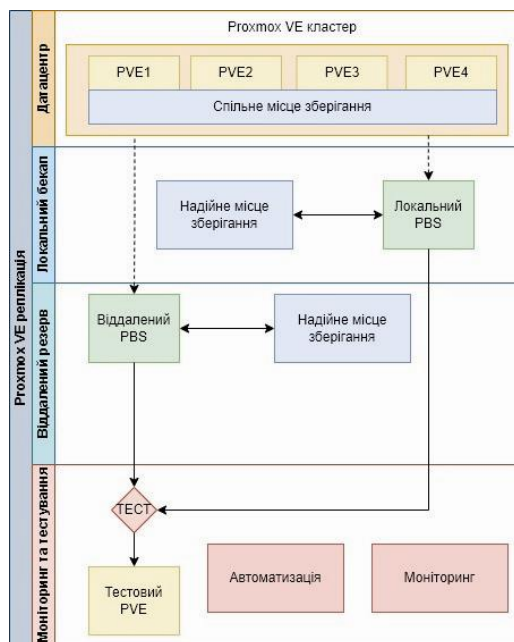


Рис. 3. Схема організації плану відновлення після катастроф

Основним недоліком організації функціональної високої доступності в Proxmox є те, що після повернення вузла з ізоляції та стабілізації мережі Proxmox НА не повертає віртуальні машини назад, це має бути зроблено вручну або автоматично за допомогою стороннього програмного забезпечення.

Локальне резервне копіювання реалізоване за допомогою PBS із використанням масиву RAID для забезпечення більш надійного зберігання даних. Інтегруючи Proxmox Backup Server у налаштування Proxmox VE High Availability компанії можуть мати комплексне рішення для відновлення після надзвичайних ситуацій, яке забезпечує захист даних, мінімальний час простою та спрощене управління резервним копіюванням. Зв'язка сервісів створює потужну комбінацію для захисту критично важливих віртуальних машин і контейнерів у високодоступному віртуалізованому середовищі.

Організовуючи резервний сайт, необхідно організувати захист для передавання та зберігання даних. Рис. 4 демонструє організацію віддаленого вузла для зберігання резервних копій, для плану відновлення після надзвичайної ситуації.

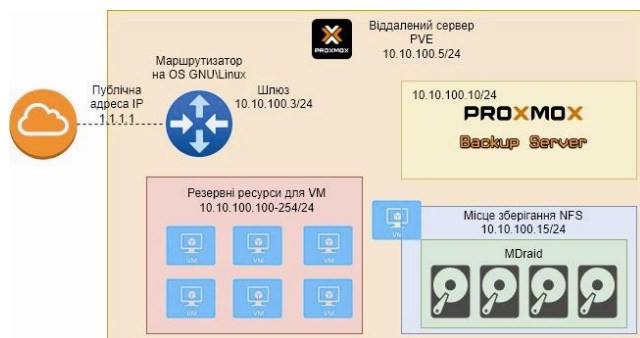


Рис. 4. Організація віддаленого вузла для зберігання резервних копій

Під час організації віддаленого резервного копіювання пропонуємо використовувати гіпервізор на Proxmox VE для сумісності з основним сайтом. Щоб захистити віддалений сайт від зовнішніх атак, необхідно використовувати програмний або апаратний маршрутизатор, якому буде присвоєно публічну IP-адресу для доступу до віддаленого сайту. Одним із прикладів є операційні системи маршрутизаторів, що базуються на ядрі Linux або BSD. У середині гіпервізора створюється локальна мережа, яка з'єднує внутрішні ресурси та маршрутизатор. Щоб забезпечити надійність збереження даних, рекомендуємо, по можливості, використовувати масив RAID. Масив RAID може бути апаратним або програмним. У випадку програмного масиву RAID необхідно перенаправити диски до віртуальної машини та зібрати mdraid всередині неї. Ця техніка допомагає уникнути проблем із завантаженням основної системи з дискового сховища.

- Резервування запасних ресурсів необхідне для критичного та швидкого відновлення послуг у випадку збою основного сайту.

Одним із ключових елементів запропонованого рішення є система моніторингу та автоматизації процесів резервного копіювання/відновлення. Використання механізмів автоматизації, як-от Jenkins та Ansible, дає змогу автоматизувати створення запланованих резервних копій та перевірку створених копій на тестовому сайті в автоматичному режимі. Jenkins допомагає уникнути людських помилок і надає результат та детальну інформацію про прогрес завдань. При створенні нових віддалених сайтів резервного копіювання, створені сценарії Ansible допомагають автоматизувати цей процес розгортання. Сценарії допомагають зменшити час відновлення роботи системи (MTTR) під час відновлення інфраструктури системи. Системи моніторингу, як-от Prometheus з Alertmanager (система сповіщення) та Grafana (система візуалізації), дають змогу бачити переважені або несправні елементи системи, що допомагає запобігти катастрофам та відстежувати виконання завдань для процесу резервного копіювання та відновлення системи після катастроф. Відстеження тенденцій використання ресурсів допоможе обрати оптимальні часові межі для налаштування завдань резервного копіювання, що своєю чергою зменшує вплив навантаження, створеного завданням резервного копіювання під час середнього часу між збоями (MTBF). Достовірність наданої інформації залежить від стабільності системи моніторингу [11].

Використовуючи запропоновані рішення, MTBF (середній час між збоями) та MTSR (середній час на відновлення сервісу) залежать від пропускну здатності з'єднувального каналу між основним та віддаленими сайтами.

4. Безпека при створенні резервного копіювання

У контексті зростаючої потреби в захисті даних шифрування в системах резервного копіювання Proxmox Backup Server набуває особливої актуальності. Цей аспект безпеки є критично важливим для забезпечення конфіденційності та цілісності даних у сучасних інформаційних системах. Шифрування, будучи фундаментальним елементом захисту даних, виконує критично важливу роль у забезпеченні конфіденційності та цілісності інформації в системах резервного копіювання, як-от Proxmox Backup Server.

Proxmox Backup Server впроваджує шифрування як засіб захисту даних, що забезпечує їхню конфіденційність шляхом перетворення інформації в нерозбірливий формат, доступний тільки під час під'єднання з відповідними ключами дешифрування. Ця технологія дає змогу захистити дані від несанкціонованого доступу і на етапі зберігання, і під час передавання між гіпервізором та бекап сервером.

У випадку Proxmox Backup Server шифрування на стороні кластера (AES-256 in GCM mod) є фундаментальною характеристикою, яка гарантує, що всі дані, які відправляються в позакластерну систему, вже зашифровані до того, як вони досягнуть місця зберігання. Це означає, що навіть у випадку фізичного доступу до сервера або мережеских атак на кластер чи канал передавання, зловмисники не зможуть використовувати ці дані.

Ключі шифрування, які використовують для цього процесу, вимагають ретельного управління та зберігання. З огляду на їхню важливість для доступу до зашифрованих даних, втрата або компрометація ключів може призвести до неможливості відновлення інформації. Тому забезпечення безпеки цих ключів є однією з основних задач системи управління шифруванням в Proxmox Backup Server. На рис. 5 зображено відбиток для Proxmox Backup Server.



Рис. 5. Відбиток Proxmox Backup Server

Захист даних під час їхнього передавання також є важливим аспектом шифрування в PBS. Використання протоколів, як-от TLS, дає змогу забезпечити зашифрованість та захищеність від моменту відправлення від клієнта до моменту їхнього прибуття на сервер резервного копіювання. Це важливо не тільки для захисту від зовнішніх атак, але й для запобігання потенційному перехопленню даних всередині мережі.

Вибір методу шифрування в PBS дає змогу користувачам адаптувати рівень безпеки до своїх потреб. Завдяки підтримці різних алгоритмів шифрування, користувачі можуть визначити, який із них найкраще підходить для їхніх вимог з точки зору балансу між безпекою та використанням системних ресурсів, щоб запобігти надмірному навантаженню ресурсів.

У Proxmox Backup Server шифрування є не лише додатковою опцією, а необхідністю для забезпечення високого рівня захисту даних у сучасному цифровому світі. Ретельне впровадження та управління шифруванням є ключем до забезпечення довіри користувачів та високого рівня захисту інформації [12].

5. Результати дослідження запропонованого методу

Апаратну складову дослідження реалізовано на основі фізичного сервера DELL PowerEdge R740xd та віддаленого виділеного сервера RISE-STOR-1 хмарного провайдера OVH. Фізичний сервер складається з двох CPU Intel(R) Xeon(R) Gold 5218R @ 2.10GHz, восьми модулів оперативної пам'яті по 16GB 2666 MHz загальним об'ємом 128GB. Два накопичувачі SSD об'ємом по 512GB, п'ять накопичувачів HDD по 1TB. Налаштовано два рейд-масиви типу RAID1 (SSD) та RAID6 (HDD), встановлено операційну систему ProxmoxVE v7.3.6. з базовою конфігурацією. Віддалений сервер складається з центрального процесора Intel Xeon-D 1521 - 4c/8t - 2.4 GHz/2.7 GHz, модуля оперативної пам'яті розміром 16 GB ECC 2133 MHz, накопичувача SSD NVMe розміром 500GB та чотирьох накопичувачів HDD по 6TB із програмним RAID5.

Згідно зі складовими параметрами MTTR розроблено алгоритм проведення відновлення інформаційних сервісів під час надзвичайних ситуацій (рис. 6).

Вхідні дані для перевірки алгоритму продемонстровано в табл. 1. Відповідні результати досліджень, відповідно до наведеного алгоритму, зображено в табл. 2.

Опираючись на результати досліджень, отримано діаграму залежностей часу відновлення від сервісу та методу відновлення.

Згідно з проведеним дослідженням за алгоритмом відновлення можна побачити, що здебільшого розгортання сервісів з коду або у разі розгортання з коду та відновленні даних є більш швидким ніж повноцінне відновлення віртуальної машини, що суттєво впливає на час плану

відновлення структури. Проте в деяких випадках відновлення з коду не має значних переваг у часі над відновленням з сховища зберігання резервних копій. Залежно від сервісу та ситуації потрібно обрати оптимальніший спосіб відновлення.

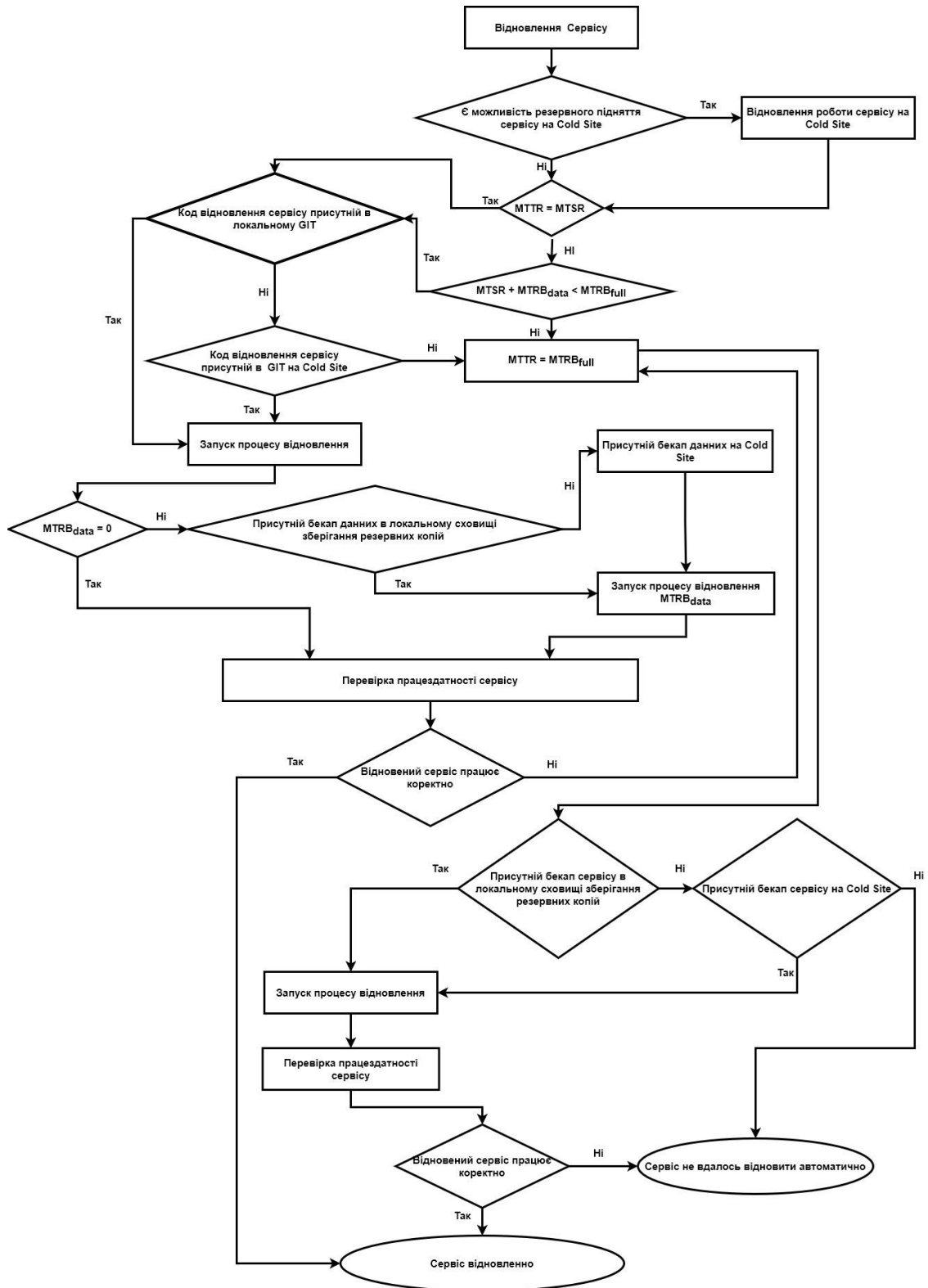


Рис. 6. Блок-схема методу відновлення

Таблиця 1

Вхідні дані для відновлювальних сервісів

Сервіс	Розмір ВМ. МВ	Розмір даних ВМ, МВ	Можливість відновлення на віддаленому ресурсі
AD CNTRL	61440	-	-
DHCP	20480	-	-
DNS	20480	-	+
WIKI	20480	40960	+
GIT	20480	40960	+
Jenkins	40960	-	+
MSSQL	61440	102400	+
PostgreSQL	61440	102400	+
MySQL	61440	102400	+
Docker registry	61440	102400	+
NAT	20480	-	-
SMB share	61440	102400	+
NFS share	61440	102400	+
Monitoring	61440	102400	+
Mail Server	61440	512000	+
VPN	20480	-	-
Print Server	61440	-	+
LDAP	61440	102400	+
RADIUS	20480	-	+
Licenses Srv	61440	-	+

Таблиця 2

Результати дослідження алгоритму відновлення

Сервіс	Локальний GIT, с	Локальний GIT та дані, с	Локальний бекап, с	Віддалений GIT, с	Віддалений GIT та дані, с	Віддалений бекап, с
AD CNTRL	-	-	1110	-	-	1967
DHCP	302	-	467	536	-	1096
DNS	299	-	500	536	-	1047
WIKI	-	1387	1179	-	2041	1728
GIT	-	1480	1229	-	2033	2152
Jenkins	728	-	1212	991	-	1432
MSSQL	-	-	3490	-	-	4426
PostgreSQL	-	-	3050	-	-	4524
MySQL	-	-	3138	-	-	4624
Docker registry	-	2593	3551	-	3631	4932
NAT	446	-	873	761	-	704
SMB share	-	2707	3629	-	3443	5007
NFS share	-	2542	3507	-	3690	4676
Monitoring	-	2469	3317	-	3503	4888
Mail Server	-	10808	11161	-	14917	15706
VPN	413	-	701	793	-	573
Print Server	-	-	1004	-	-	1840
LDAP	-	-	3497	-	-	4686
RADIUS	438	-	665	803	-	524
Licenses Srv	-	-	1543	-	-	2098

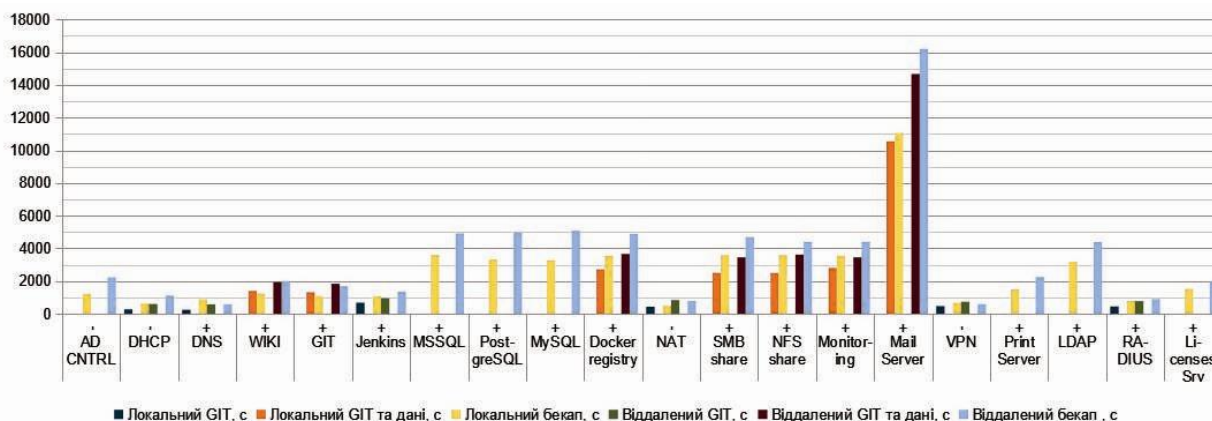


Рис. 7. Діаграма залежностей

Висновки

У роботі описано критерії та параметри мережі, які дозволяють оцінити ефективність рішення для відновлення після надзвичайної ситуації. Запропоноване додавання параметра MTTR дає змогу більш детально розрахувати та оцінити критичні значення, які мають бути покращені у рішенні для відновлення інфраструктури. MTTR показує час, необхідний для відновлення елемента системи з резервної копії. MTSR демонструє час, необхідний для відновлення сервісу з інфраструктурного коду.

Запропоноване рішення для організації мережі відновлення після надзвичайних ситуацій, що складається із захищеного шифрування, кластера Proxmox VE, локального резервного копіювання, віддаленого сайту резервного копіювання, системи моніторингу та автоматизації, допоможе зменшити час простою системи у випадку катастрофи. Це рішення забезпечує надійні параметри та якісне і захищене зберігання даних. Особливістю цього рішення є набір модулів безпечного віддаленого вузла резервного копіювання, модулів моніторингу та автоматизації. Програмний або апаратний маршрутизатор на стороні віддаленого вузла резервного копіювання використовують для протидії зовнішнім атакам, а також для встановлення безпечних комунікаційних каналів із основним сайтом. Для досягнення високої доступності параметри системи моніторяться з метою вибору оптимального часового вікна для резервного копіювання, а також контролю загального стану всіх елементів системи.

Розроблено алгоритм для обрання оптимального шляху відновлення сервісу на основі методу з використанням Cold Site. На основі декількох сервісів проведено дослідження алгоритму відновлення, у результаті чого з'ясовано, що більшість сервісів доцільніше розгортати з використанням кодової бази і тільки дані відновлювати з місця зберігання резервних копій, проте для деяких сервісів немає інших варіантів відновлення, окрім як із резервної копії.

Запропоноване рішення допомагає більш гнучко вибирати необхідні ресурси, використовувати їх оптимально, точніше розраховувати час резервного копіювання та відновлення. Результати цієї роботи вказують на перспективу подальших досліджень у цій галузі, оскільки час відновлення системи є важливим для здатності надавати вищий рівень сервісу користувачам інфраструктури на місці

Список використаних літературних джерел

- [1] J. Blough. "5 Basics for Disaster Recovery in the Data Center." *ServiceExpress.com*. <https://serviceexpress.com/resources/5-basics-disaster-recovery-preparation/> (accessed May 15, 2023).
- [2] NAKIVO Team. "Data Center Disaster Recovery: A Complete Guide." *nakivo.com*. <https://www.nakivo.com/blog/data-center-disaster-recovery-a-complete-guide/> (accessed Jun. 5, 2023).

- [3] B. Brazil, "Alerting," in *Prometheus: Up & Running: Infrastructure and Application Performance Monitoring*, 1th ed. Sebastopol, CA, USA: O'Reilly media, 2018, pp. 291-303.
- [4] M., Pokharel, S., Lee, J. S. Park, "Disaster recovery for sys-tem architecture using cloud computing," 2010 IEEE/IPSJ 10th International Symposium on Applications and the Internet (SAINT), 2010, pp. 303-308. doi: 10.1109/SAINT.2010.23.
- [5] S. Hochstetler, O. Magroski and P. Glasmacher, "High availability solutions," in *Deploying Mission Critical Applications with Linux on POWER*, 1th ed. Armonk, NY, USA: IBM Redbook, 2007, pp. 55-82. [Online]. Available: <https://www.redbooks.ibm.com/redbooks/pdfs/sg247286.pdf>
- [6] S. Peterson and J. Hilliard. "Network disaster recovery plan." *techtarget.com*. <https://www.techtarget.com/searchdisasterrecovery/definition/Network-disaster-recovery-plan> (accessed May 22, 2023).
- [7] K. Elgdamsi, M. Embarak, "Implementing a Disaster Recovery Solution for Datacenters Using VMware Site Recovery Manager," *TUJES*, vol. 04, no. 01, June 2023.
- [8] W. Ahmed, "Chapter 10. Proxmox High Availability," in *Mastering Proxmox - Third Edition: Build virtualized environments using the Proxmox VE hypervisor*, 3th ed. Birmingham, United Kingdom: Packt, 2017, pp. 491-520.
- [9] B. Meijer, L. Hochstein and R. Moser, "Chapter 22. CI/CD and Ansible," in *Ansible: Up and Running*, 3th ed. Sebastopol, CA, USA: O'Reilly media, 2022, pp. 567-589.
- [10] M. Heap, "Chapter 7: Orchestrating AWS," in *Ansible From Beginner to Pro*, 1th ed. New York, NY, USA: Apress Media, 2016, pp. 99-124.
- [11] J. Turnbull, "Scaling and Reliability," in *Monitoring with Prometheus*, 1th ed. Brooklyn, NY, USA: Turnbull Press, 2018, pp. 217-237.
- [12] *Proxmox VE Administration Guide RELEASE 8.1.3, 2023. Proxmox Server Solutions GmbH.*

OPTIMIZATION OF DISASTER RECOVERY PROCESSES OF INFORMATION INFRASTRUCTURE SERVICES

M. Kyryk, S. Zablotskyi, V. Pohranychnyi, A. Tarasenko

Lviv Polytechnic National University, S. Bandery Str., 12, 79013, Lviv, Ukraine

The article describes the optimization of the process of disaster recovery of information infrastructure services by implementing the ability to restore service functionality without requiring a full recovery from backup storage. It outlines the criteria and parameters of the network that have a critical impact on recovery in the event of emergencies, allowing for the assessment of the solution's effectiveness in post-disaster recovery. A modification to the MTTR (Mean Time To Recovery) parameter is proposed for cases involving system element recovery from a backup or through service configuration restoration via infrastructure as code, with data necessary for service operation retrieved from backup storage, thereby accelerating the recovery process of a failed information infrastructure service. The article presents a scheme for infrastructure recovery organization by creating a backup location (Cold Site) for local infrastructure using dedicated cloud providers. The proposed solution utilizes Proxmox Backup Server capabilities for regular backups of critically important data center components. Following the development of a flowchart for the service recovery method from the Cold Site, research findings indicated that, for some services, reinstating configurations from code is more advantageous and speeds up the recovery process more than complete service restoration from backup storage.

Keywords: *reliability, fault-tolerant system, reliable design, emergency situations, Proxmox VE, virtual machine.*