УДК 004

Г.Віднічук, магістр гр. КІ-23Мз
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ БЕЗПЕРЕРВНОЇ РОБОТИ ДОДАТКІВ ПРИ СЕРВЕРНІЙ ВІРТУАЛІЗАЦІЇ

У статті розроблено програмне забезпечення, яке призначено для системи безперервної роботи додатків при серверній віртуалізації. Метою розробки є дослідження та програмна реалізація системи безперервної роботи додатків при серверній віртуалізації. Об’єктом дослідження є процес безперервної роботи додатків при серверній віртуалізації. Предметом дослідження є методи безперервної роботи додатків при серверній віртуалізації. Методи дослідження базуються на методах теорії комп’ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи безперервної роботи додатків при серверній віртуалізації. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Широке поширення серверної віртуалізації й хмарних технологій вимагає нового підходу до реалізації рішень, що забезпечують безперервну роботу бізнес-додатків у випадку великих аварій і катастроф.

Виробники серверів і систем зберігання постійно вдосконалюють використовувані в цих продуктах засобу для запобігання апаратних і програмних збоїв, їхньої своєчасної ідентифікації й діагностики, а також оперативного усунення таких збоїв. У цьому зв'язку можна згадати спеціальні сервісні процесори, що контролюють стан устаткування, дублювання основних компонентів системи, функції гарячої заміни жорстких дисків, вентиляторів і блоків живлення. Нарешті, об'єднання двох і більше серверів в відказостійкий кластер дозволяє забезпечити продовження роботи додатків навіть у випадку повного виходу з ладу одного з них.

Однак всі ці міри виявляються неефективними, якщо з якихось причин буде зупинений весь центр обробки даних – наприклад, через повінь, пожежі або багатогодинного відключення електрики. Оскільки великі природні й техногенні катастрофи звичайно охоплюють цілі міста або регіони, захистити від них критичні для бізнесу додатка можна одним способом: побудувати віддалений на десятки або сотні кілометрів резервний ЦОД, щоб оперативно запустити там додатка у випадку подібних ситуацій. В ідеалі й той і інший повинні бути оснащені однаковими серверами й системами зберігання даних.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи безперервної роботи додатків при серверній віртуалізації.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи безперервної роботи додатків при серверній віртуалізації.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем безперервної роботи додатків при серверній віртуалізації.
– Дослідження системи безперервної роботи додатків при серверній віртуалізації.
– Програмна реалізація системи безперервної роботи додатків при серверній віртуалізації.

Об'єктом дослідження є процес безперервної роботи додатків при серверній віртуалізації.

Предметом дослідження є методи безперервної роботи додатків при серверній віртуалізації.

Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Представте, що ваш дата-центр (або сервер) сьогодні впав. Просто взяв і впав. Як показує практика, готові до цього далеко не всі:

– 93% компаній, які втрачали свій ЦОД на 10 і більше днів через катастрофу, стали банкрутами протягом року.

– Щотижня в США виходить із ладу 140 000 жорстких дисків.

– В 75% компаній немає рішень для аварійного відновлення.

– 34% компаній не тестують резервні копії.

– 77% тих, хто тестують, виявляли накопичувачі, які не читаються, у своїх бібліотеках.

Зараз поговоримо про технічні рішення, які в цьому допоможуть. Їхня вартість відрізняється від декількох тисяч до сотень тисяч доларів.

Висока доступність і аварійне відновлення

Дуже часто рішення для високої доступності (HA – High Availability) і аварійного відновлення (DR – Disaster Recovery) плутають. Насамперед, коли ми говоримо про безперервність бізнесу, ми маємо на увазі резервну площадку. Стосовно до IT – резервного ЦОД. Безперервність бізнесу – це не про резервне копіювання на бібліотеку в сусідній стійці (що теж дуже важливо). Це про те, що основний будинок компанії згорить, і ми через кілька годин або днів зможемо відновити роботу, розгорнувшись на новому місці:

Висока доступність:

– Рішення в межах одного ЦОД.

– Час відновлення < 30 хвилин.

– Нульова або близька до нуля втрата даних.

– Вимагає щоквартального тестування.

Аварійне відновлення:

– Містить у собі декілька віддалених ЦОД.

– Відновлення може займати години й навіть дні.

– Втрата даних може досягати багатьох годин.

– Вимагає щорічного тестування.

Виходить, потрібний резервний ЦОД. Які є варіанти? Звичайно виділяють три: гарячий, теплий і холодний резерви.

Холодний резерв

Холодний резерв має на увазі, що є якесь серверне приміщення, у яке можна завезти встаткування й розгорнути його там. При відновленні може плануватися закупівля «заліза», або його зберігання на складі. Потрібно враховувати, що більшість систем поставляється під замовлення, і швидко знайти десятки одиниць серверів, СЗД, комутаторів і інше буде нетривіальним завданням. Як альтернативу складуванню встаткування в себе, можна передбачити зберігання найбільш важливого або найбільш рідкого встаткування на складі ваших постачальників. При цьому, телекомунікаційні канали в приміщенні повинні бути присутнім, але висновок контракту із провайдером звичайно відбувається після ухвалення рішення про запуск «холодного» ЦОДа. Відновлення роботи в такому ЦОДі при катастрофічному збої основної площадки цілком може займати кілька тижнів. Переконаєтеся, що ваша компанія зможе проіснувати ці кілька тижнів без IT і не втратитися бізнесу (через відкликання ліцензії, або непоправного касового розриву, наприклад) – про це я писав раніше. Чесно говорячи, я б нікому не рекомендував цей варіант резервування. Можливо, я перебільшую роль IT у бізнесі деяких компаній.

Теплий резерв

Це значить, що в нас функціонує альтернативна площадка, у якій є активні інтернет і WAN-канали, базова телекомунікаційна й обчислювальна інфраструктура. Вона завжди «слабкіше» основний по обчислювальних потужностях, деяке встаткування там може бути відсутнім. Найважливіше – щоб на площадці завжди була актуальна резервна копія даних. Діючи «по старинці» можна організувати регулярне переміщення туди резервних копій на стрічках. Сучасний метод – реплікація бекапів по мережі з основного ЦОДа. Використання бекапа з дедуплікацією дозволить оперативно передавати резервні копії навіть по «тонкому» каналі між ЦОДами.

Гарячий резерв

От він, вибір спеціалістів, що підтримують IT-системи, простій яких навіть на кілька годин приносить компанії величезні збитки. Тут є все необхідне встаткування для повноцінної роботи IT-систем. Звичайно фундаментом такої площадки служить система зберігання даних, на яку синхронно або асинхронно дзеркалюються дані з основного ЦОДа. Для того, щоб гарячий резерв у годину Ікс зміг відробити вкладені в нього гроші, повинні проводитися регулярні тестові переклади систем, налаштування й версія ОС серверів на основній і резервній площадці повинні постійно синхронізуватися – вручну або автоматично.

Мінус гарячого й теплого резерву – дороге встаткування простоює чекаючи катастрофи. Виходом із цієї ситуації є стратегія розподіленого ЦОДа. При такому варіанті дві (або більше) площадки рівноправні – більшість додатків можуть працювати як на одній, так і на іншій. Це дозволяє задіяти потужності всього встаткування й забезпечити балансування навантаження. З іншого боку, серйозно підвищуються вимоги до автоматизації перекладу IT-сервісів між ЦОДами. Якщо обоє ЦОДа «бойові», бізнес вправі очікувати, що при очікуваному піку навантаження на один з додатків, його можна швидко перевести в більше вільний ЦОД. Найчастіше, у подібних ЦОДах є присутнім синхронна реплікація між СЗД, але можлива й невелика асинхроність (у межах декількох хвилин).

Три чарівних слова

Перед тим, як перейти безпосередньо до технологій катастрофостійкості IT-сервісів, нагадаю три «чарівних» слова, які визначають вартість будь-якого DR-рішення: RTO, RPO, RCO:

- RTO (Recovery time objective) – час, за яке можливо відновити IT-систему
- RPO (Recovery point objective) – скільки даних буде загублено при аварійному відновленні
- RCO (Recovery capacity objective) – яку частину навантаження повинна забезпечувати резервна система. Цей показник може вимірятися у відсотках, транзакціях IT-систем і інших величин.

RPO

Перший розподіл, що ми можемо провести між всім різноманіттям IT-рішень для забезпечення катастрофостійкості – чи забезпечують вони нульове RPO чи ні. Відсутність втрати даних при збої забезпечується синхронною реплікацією. Найчастіше, це робиться на рівні СЗД, але можливо реалізувати й на рівні СУБД або сервера (за допомогою просунутого LVM). У першому випадку сервер не одержує від СЗД, з якої він працює, підтвердження про успішність запису, поки СЗД не передала цю транзакцію другій системі й не одержала від її підтвердження, що запис пройшов успішно.

Синхронну реплікацію вміють робити 100% СЗД, що відносяться до середнього цінового сегмента й деякі системи початкового рівня від відомих вендорів. Вартість ліцензій для синхронної реплікації на «простих» СЗД починається від декількох тисяч доларів. Приблизно стільки ж коштує софт для реплікації на рівні серверів на 2-3 сервери. Якщо у вас немає діючого резервного ЦОДа, не забудьте додати вартість закупівлі резервного встаткування.

RPO у кілька хвилин може забезпечити асинхронна реплікація на рівні СЗД, ПЗ керування томами сервера (LVM – Logical volume manager), або СУБД. Дотепер standby-

копія бази даних залишається одним з найбільш популярних рішень для DR. Найчастіше функціонал “log shipping”, як це називається в адміністраторів СУБД, не ліцензується виробником окремо. Якщо у вас ліцензована БД – реплікуйте на здоров'я. Вартість асинхронної реплікації для серверів і СЗД не відрізняється від синхронної, див. попередній пункт.

Якщо ми говоримо про RPO у кілька годин, частіше це реплікація резервних копій з однієї площадки на іншу. Більшість дискових бібліотек уміють робити це, частина ПЗ для резервного копіювання – теж. Як я вже говорив, при такому варіанті здорово допоможе дедуплікація. Ви не тільки будете менше завантажувати канал передачею резервних копій, але й зробите це набагато швидше – кожний переданий бекап буде займати в десятки або сотні разів менше часу, чим у реальності. З іншого боку, треба пам'ятати, що перший бекап при дедуплікації однаково повинен передати в систему масу унікальних даних. «Справжню» дедуплікацію ви побачите після тижневого циклу резервного копіювання. При синхронізації дискових бібліотек – те ж саме. Якщо розрахунковий час передачі при вашій ширині каналу між ЦОД становить кілька днів і навіть тижнів (що може й коштувати чимало), їсти зміст спочатку поставити другу бібліотеку поруч, виконати синхронізацію й відвезти її в резервний ЦОД.

RTO

Коли стоїть завдання мінімізації часу відновлення (RTO), процес повинен бути максимально документований і автоматизований. Одне із кращих і найбільш універсальних рішень – HA-кластери з територіально рознесеними вузлами. Найчастіше, такі рішення будуються на базі реплікації СЗД, але можливі й інші варіанти. Лідируючі продукти в цій області, наприклад, Symantec Veritas Cluster, мають у своєму складі модулі по роботі зі СЗД, що перемикають напрямок реплікації, коли необхідно запустити знову сервіс на резервному вузлі. Для менш просунутих кластерів (наприклад Microsoft Cluster Services, убудований в Windows) основні виробники СЗД (IBM, EMC, HP) пропонують надбудови, роблячи зі звичайного HA-кластера катастрофостійкий.

Рідко хто замислюється про цікаву особливість переважною більшістю рішень по реплікації даних – їх «однозарядність». Ви можете одержати на резервній площадці тільки один стан даних. Якщо система із цими даними з якоїсь причини не стартувала – переходимо до плану «Б». Найчастіше це відновлення з резервної копії з великою втратою даних. З перерахованих мною технологій виключення складе тільки реплікація тих же бекапів. Відповіддю тут є використання класу рішень Continuous Data Protection. Їхня суть у тім, що всі записи, що приходять від сервера, позначаються й зберігаються в певному журнальному томі на резервній площадці. При відновленні системи можна вибрати будь-яку точку із цього журналу й одержати стан не тільки на момент аварії, у якій дані були зіпсовані, але й за кілька секунд. Такі рішення захищають від внутрішньої погрози – видалення даних користувачами. У випадку реплікації СЗД – їй однаково, що передавати – порожній тім або вашу найбільш критичну БД. При використанні CDP можна вибрати момент прямо перед видаленням інформації й відновитися на нього. Вартість систем CDP звичайно – десятки тисяч доларів. Один з найбільш удалих прикладів, на мій погляд – EMC RecoverPoint.

Останнім часом набирають популярність системи віртуалізації СЗД. Крім своєї основної функції – об'єднання масивів різних вендорів у єдиний пул ресурсів – вони можуть сильно допомогти й в організації розподіленого ЦОДа. Суть віртуалізації СЗД у тім, що між серверами й системами зберігання з'являється проміжний шар контролерів, що пропускають крізь себе весь трафик. Тому зі СЗД презентуються не прямо серверам, а цим віртуалізаторам. Вони, у свою чергу, роздають їх хостам. У шарі віртуалізації можна робити реплікацію даних між різними СЗД, а найчастіше є й більше просунуті можливості – снепшоти, багаторівневе зберігання й т.д. При цьому сама базова функція віртуалізаторів є самою потрібною для цілей DR. Якщо в нас є дві СЗД у різних ЦОДах, з'єднаних оптичною магістраллю, ми беремо томи з кожної з них і збираємо «дзеркало» на рівні віртуалізатора. У підсумку ми одержуємо один віртуальний тім на два ЦОДа, що і бачать сервери. Якщо ці

сервери віртуальні – починає працювати Live Migration віртуальних машин і можете «на ходу» переводити завдання між ЦОДами – користувачі нічого не помітять.

Повна втрата ЦОДа буде відпрацьована звичайним НА-кластером в автоматичному режимі за кілька хвилин. Мабуть, віртуалізація рознесених СЗД дозволяє забезпечити мінімальний час відновлення для більшості додатків. Для СУБД є неперевершений Oracle RAC і його аналоги, але вартість змушує задуматися. Віртуалізація SAN поки теж не дешева, для невеликих обсягів СЗД вартість рішення може бути менше $100К, але в більшості випадків ціна вище. На мій погляд, найбільш перевіреним рішенням є IBM SAN Volume Controller (SVC), найбільше технічно зробленим – EMC VPLEX.

До речі, якщо не всі ваші додатки ще живуть на віртуальному середовищі, варто спроектувати резервний ЦОД для них на віртуальних машинах. По-перше, вийде набагато дешевше, у других, зробивши це для резерву, недалеко й до міграції основних систем під керування якого-небудь гіпервізора.

Конкуренція на ринку аутсорсингу ЦОД робить більше вигідної оренду стійкомісць у ЦОДі провайдеру, у порівнянні з будівництвом і експлуатацією свого резервного центра. Якщо ви розміщаєте в нього віртуальну інфраструктуру, вийде серйозна економія на орендних платежах. Але й аутсорсингові ЦОДи вже не на вершині прогресу. Краще будувати резервну інфраструктуру відразу в «хмарі». Синхронізацію даних з основними системами при цьому можна забезпечити реплікацією на рівні сервера (є відмінне сімейство рішень DoubleTake від Vision Solutions).

Останній, але дуже важливий момент, про яке не можна забувати при проектуванні катастрофостійкої IT-інфраструктури – робочі місця користувачів. Те, що піднялася база даних, не означає поновлення бізнесу-процесу. Користувач повинен мати можливість виконувати свою роботу. Навіть повноцінний резервний офіс, у якому коштують виключені комп'ютери для ключових співробітників – не ідеальне рішення. У людини на втраченому робочому місці можуть бути довідкові матеріали, макроси, й інш., повноцінна робота без яких неможлива. Для найбільш важливих для компанії користувачів розумним виглядає перехід на віртуальні робочі місця (VDI). Тоді на робочому місці (будь те звичайний ПК або модний «тонкий» клієнт) не зберігаються ніякі дані, він використовується тільки як термінал, щоб достукатися до Windows XP або Windows 7, що працює на віртуальній машині в ЦОДі. Доступ до такого робочого місця легко організувати з будинку або з будь-якого комп'ютера у філіальній мережі. Наприклад, якщо у вас кілька будинків і одне з них недоступно, ключові користувачі можуть приїхати в сусідній офіс і сісти на робочі місця «менш ключових». Потім вони спокійно логіняться в систему, попадають у свою віртуальну машину й фірма оживає!

У завершення, от основні питання, які варто задати при оцінці DR-рішення:

- Від яких збоїв захищає?
- Які RPO/RTO/RCO забезпечує?
- Скільки коштує?
- Наскільки складна експлуатація?

Катастрофостійких рішень незліченна безліч – як коробкових, так і тих, які можна зробити практично своїми руками. Будь ласка, поділитеся в коментарях що є у вас і історіями, як ці рішення вас виручали. Якщо у вас працює щось із описаних вище систем або їхніх аналогів – залишайте відкликання, наскільки спокійно ви спите, коли IT-системи під їхнім захистом.

Розробка структурної схеми

Для перезапуску додатків на сервері резервного ЦОДа потрібно об'єднати його із сервером основного ЦОДа, створивши географічно розподілений кластер (ще недавно ця функціональність підтримувалася тільки Unix/ RISC-серверами старшого класу й мейнфреймами). Крім того, для оперативного перемикання додатка з основного центра обробки даних на резервний в останньому повинні перебувати актуальні копії даних потрібних додатків, для чого необхідні спеціальні засоби віддаленої синхронної й

асинхронної реплікації, які використовуються в дискових масивах старшого класу (наприклад, EMC Symmetrix SRDF), а також орендовані або власні високошвидкісні канали зв'язку, що з'єднують обидві площадки. Зрозуміло, через більші витрати на створення й експлуатацію резервного центра обробки даних тільки самі великі організації можуть дозволити собі побудувати допоміжну площадку для захисту своїх бізнес-критичних додатків від катастроф.

У результаті застосування віртуалізації для консолідації серверних додатків і впровадження приватних хмар з'явилася потреба в новому підході до захисту від катастроф. При класичному способі захист забезпечувався тільки для декількох додатків, основні характеристики яких (вимоги до продуктивності сервера й системи зберігання) мало мінялися згодом. Очевидно, що старі методи Disaster Recovery, орієнтовані на фізичні сервери, не можна застосовувати до хмар, де можуть працювати десятки віртуалізированних додатків з різними вимогами до обчислювальної потужності і ємності. Крім того, для розгорнутих у приватній хмарі додатків потрібно забезпечити гнучке виділення ресурсів, а також можливість швидкого запуску нових додатків, у тому числі висококритичних і тому нужденних у захисті від катастроф. Нарешті, у більшості хмар як апаратна платформа використовуються сервери стандартної архітектури, які не підтримують класичні рішення географічно розподілених кластерів, розроблені для Unix-систем і мейнфреймів.

Призначене для віртуальних машин vSphere розроблене програмне забезпечення «Програмне забезпечення менеджера безперервної роботи додатків при серверній віртуалізації» на базі розробленої технології реплікації віртуальних машин «Програмне забезпечення реплікації баз даних» і розробленого пакета керування віртуальними машинами «Програмне забезпечення керування віртуальними машинами» реалізує автоматичне виконання планів післяаварійного відновлення з використанням заданих правил.

«Програмне забезпечення менеджера безперервної роботи додатків при серверній віртуалізації» координує роботу «Програмного забезпечення керування віртуальними машинами», які обслуговують віртуалізированні сервери двох центрів обробки даних, тому, якщо з якоїсь причини в одному ЦОДі віртуальні машини зупиняються, відразу ж запускаються їхні копії в іншому. У плані післяаварійного відновлення визначається порядок вимикання й перезапуску віртуальних машин, вказуються виділювані їм ресурси в резервному центрі обробки даних і доступних мережних підключень. Крім того, плани післяаварійного відновлення можна створювати для окремих додатків і різних сценаріїв аварійних ситуацій.

«Програмне забезпечення реплікації баз даних» забезпечує незалежну від СЗД асинхронну реплікацію на рівні гіпервізора з можливістю налаштування цільових точок відновлення (RPO) і декількох точок відкату (point-in-time instance). Такий підхід дозволяє легко конфігурувати віртуальні машини vSphere без прив'язки до конкретної конфігурації фізичного сервера, набудовувати реплікацію на рівні дисків Virtual Machine Disk (VMDK) окремих віртуальних машин і проводити їхнє гранулярне відновлення.

Крім «рідної інтеграції» з «Програмним забезпеченням реплікації баз даних» (потрібно при використанні програмно обумовлених систем зберігання VSAN), «Програмне забезпечення менеджера безперервної роботи додатків при серверній віртуалізації» інтегрується з рішеннями по реплікації провідних виробників дискових масивів за допомогою спеціальних адаптерів. Його можна застосовувати й для тестування планів післяаварійного відновлення ключових додатків без переривання їхньої роботи. Тестування проводиться на тимчасових копіях реплікованих даних і в ізольованих мережах, тому функціонування робочих додатків обох центрів обробки даних не порушується. Крім того, це рішення дозволяє здійснювати безпечну міграцію додатків між ЦОДами за допомогою пакета «Програмне забезпечення безпечної міграції додатків між ЦОДами» і перерозподіляти навантаження між ними.

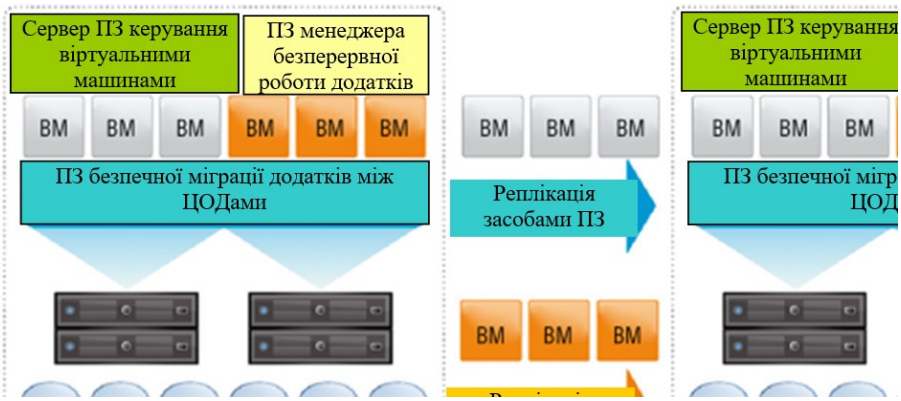

Рисунок 1 – Структурна схема системи

Післяаварійне відновлення як сервіс

При використанні розробленого програмного забезпечення «Програмне забезпечення менеджера безперервної роботи додатків при серверній віртуалізації», як і традиційних рішень захисту від катастроф, потрібний другий резервний центр обробки даних, територіально віддалений від основного. Більшість середніх по розмірі компаній, IT-бюджет яких невеликий, не мають фінансової можливості організувати другу площадку, але можуть впровадити катастрофостійке рішення за допомогою сервісів Disaster Recovery as Service (DRaaS), пропонованих провайдерами хмарних послуг. У моделі DRaaS роль резервного центра обробки даних виконує хмара провайдеру, і у випадку аварії на площадці замовника розташовані в ньому віртуальні машини і їхні додатки швидко перезапускаються.

Сервіс vCloud Air Disaster Recovery, якому можна розглядати як аналог «Програмне забезпечення менеджера безперервної роботи додатків при серверній віртуалізації» для DRaaS, призначений для аварійного відновлення віртуальних машин vSphere за допомогою гібридної хмари Air. Як і «Програмне забезпечення менеджера безперервної роботи додатків при серверній віртуалізації», він припускає використання реплікації розробленого програмного забезпечення «Програмне забезпечення менеджера безперервної роботи додатків при серверній віртуалізації» і інструментів керування віртуальним середовищем «Програмне забезпечення керування віртуальними машинами» і дозволяє задавати цільову точку відновлення від 15 хв і до 24 год, причому можна створювати до 24 точок відкоту. У ньому передбачені можливості тестування плану післяаварійного відновлення для різних сценаріїв аварій. Передплата на vCloud Air Disaster Recovery забезпечує захист до 500 віртуальних машин.

У випадку Amazon Web Services (AWS) послуги DRaaS передбачають три варіанти рішення: «гаряче» (warm), коли цільовий час відновлення RTO не перевищує однієї години; «холодне» (cold) з RTO від одного робочого дня; Pilot-Light – проміжний варіант, при якому час відновлення становить не більше 4 ч. При холодному методі використовується традиційне резервне копіювання на стрічкові картриджі, що зберігаються в захищеному сховищі, при гарячому – резервується вся серверна інфраструктура замовника, а у варіанті Pilot-Light у хмарі AWS створюється пул ресурсів у мінімальній конфігурації, що при необхідності можна швидко розгорнути в повній конфігурації для обслуговування додатків замовника.

Microsoft пропонує у своїй хмарі Azure відновлення віртуальних машин vSphere і Hyper-V, а також додатків, що працюють на фізичних серверах. У сервісі Azure Site Recovery (ASR) використовуються функції реплікації SQL AlwaysON і Active Directory, забезпечується скорочення цільової точки відновлення до 30 сек. Клієнти ASR можуть виконувати перезапуск своїх віртуальних машин у хмарі Azure в автоматичному режимі й вручну по команді оператора. Після усунення аварії автоматичне поновлення роботи віртуальних машин у ЦОДі й зворотна реплікація виробляються автоматично.

Послуги захисту від катастроф за допомогою публічної хмари доступні й у декількох російських операторів ЦОДів. Улітку компанія DataLine розгорнула сервіс DRaaS на базі своєї хмари CloudLine. За допомогою рішення для віддаленої реплікації Veeam програмне забезпечення, що розробляються, Replication користувачі цього сервісу можуть організувати реплікацію віртуальних машин у хмару CloudLine і настроїти перемикання на використання тиражованих копій при аварії у своєму центрі обробки даних. Поки реплікація в хмару реалізована для vSphere, але DataLine планує незабаром забезпечити захист і віртуальні машини Hyper-V.

У пропонованому системним інтегратором «Крок» сервісі DRaaS, створеному на базі побудованого в 2015 році хмари Cisco Powered, передбачені три варіанти забезпечення катастрофостійкості:

- перенос віртуальних машин у хмару;
- розгортання в хмарі нових серверів;
- використання хмари як резервного ЦОДа.

Компанія IT-Grad у своїй публічній хмарі реалізувала сервіс «Резервна площадка» для тих замовників, які або вже розгорнули власну віртуальну інфраструктуру, або планують використовувати технології віртуалізації на базі vSphere. Відказостійкість у цьому рішенні досягається за допомогою засобів vShpere і vCenter «Програмне забезпечення менеджера безперервної роботи додатків при серверній віртуалізації», а також технологій дзеркалювання SnapMirror і систем зберігання NetApp FAS. Для «Програмне забезпечення реплікації баз даних» цільова точка відновлення RPO становить від 15 хв до 24 год, а у випадку застосування NetApp SnapMirror цей показник RPO зменшується майже до нуля.

Звертання до сервісів DRaaS дозволяє малому й середньому бізнесу реалізувати за допомогою хмарних технологій захист від катастроф для своїх основних додатків без організації резервного центра обробки даних і застосування систем зберігання корпоративного класу.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів безперервної роботи додатків при серверній віртуалізації.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем безперервної роботи додатків при серверній віртуалізації.

– Досліджена система безперервної роботи додатків при серверній віртуалізації.

– На основі отриманих результатів досліджень створена програмна реалізація системи безперервної роботи додатків при серверній віртуалізації.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання безперервної роботи додатків при серверній віртуалізації. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
2. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
3. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
4. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
5. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the

Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
6. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
7. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
8. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
9. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
10. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
11. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
12. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
13. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
14. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
15. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
16. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
17. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
18. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
19. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
20. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
21. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
22. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
23. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
24. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
25. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
26. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.