

УДК 004.04

Копійка О. В., канд. техн. наук (Тел.: +380 (44) 249 29 23). E-mail: okopiyka@gmail.com
(Державний університет телекомунікацій, м. Київ)

ПРОЕКТУВАННЯ СЛУЖБ АРХІВУВАННЯ ТА ВІДНОВЛЕННЯ

Копійка О. В. Проектування служб архівування та відновлення. Розглядаються питання побудови дата-центрів з сучасною архітектурою і наявністю повного обсягу сервісів. Одним із сервісів є сервіс управління даними, до якого належать служби: пристроїв зберігання даних, управління даними, архівування та відновлення. Сформульовані основні вимоги та принципи програмно-апаратної реалізації служби архівування та відновлення. Проведено обґрунтування основних проектних рішень щодо організації цих служб.

Ключові слова: дата-центр, архівування, відновлення, управління даними, проектні рішення

Копейка О. В. Проектирование служб архивирования и восстановления. Рассматриваются вопросы построения дата-центров с современной архитектурой и наличием полного объема сервисов. Одним из сервисов является сервис управления данными, к которому относятся службы: устройств хранения данных, управления данными, архивирования и восстановления. Сформулированы основные требования и принципы программно-аппаратной реализации службы архивирования и восстановления. Проведено обоснование основных проектных решений по организации этих служб.

Ключевые слова: дата-центр, архивирование, восстановление, управление данными, проектные решения

Kopiyka O. V. Archival and recovery services projection. The article describes the questions of data centers construction with modern architecture and full range of services. One of the services is a data management service, which includes services: data storage device, data management, archival and recovery. There are represent main requirements and principles of software and hardware realization of archival and recovery service. The article presents the basic design decision of the organization of archival and recovery services.

Keywords: data center, archival and recovery services, data management service, design decision

I. Вступ та постановка задачі. При реалізації концепції побудови сучасної інфраструктури та надання "хмарових послуг" виникає завдання переходу до дата-центрів з сучасною архітектурою і наявністю повного обсягу сервісів [1...19].

В сучасних дата-центрах виділяють наступні сервіси: мережеві; управління даними; управління IT-інфраструктурою; інфраструктури додатків; безпеки [2,6,9,10,11].

В даній статті розглядаються служби архівування та відновлення сервісу управління даними для інфраструктури, яка складається з центрального центру обробки даних (ЦОД), резервного ЦОД та регіональних ЦОД.

Цілями служби архівування та відновлення як інфраструктури забезпечення безперервності бізнесу Корпорації є: *виконання найважливіших бізнес операцій, виживання підприємства і перезапуск бізнес операцій навіть у разі загальнодержавних катастроф; захист від пошкодження даних; тестування нових додатків на реальних бізнес даних; зменшення часу резервного копіювання і відновлення; виконання обслуговування апаратного та програмного забезпечення без переривання бізнес операцій; ефективно переміщення і міграція даних; захист регіональних ЦОД.*

Завданнями служби архівування та відновлення є: *відповідність вимогам бізнес-підрозділів щодо забезпечення необхідних параметрів відновлення даних і додатків (цільова точка відновлення і цільовий час відновлення) для різних категорій даних; захист даних від втрати в результаті настання надзвичайних обставин на рівнях додатку, сервера, офісу та регіону; управління та моніторинг системи в режимі, максимально наближеному до реального; забезпечення економічної оптимальності системи; масштабування системи для забезпечення майбутніх потреб; забезпечення захисту максимального спектра гетерогенних комп'ютерних систем, використовуваних в Корпорації.*

II. Рішення цілей та завдань служб архівування та відновлення

2.1. Ідентифікація та класифікація даних. Ідентифікація та класифікація даних служать основою їх економічного захисту відповідно до вимог бізнес-підрозділів Корпорації.

Поряд з використанням адміністративних методів ідентифікації та класифікації даних (опитування та узгодження з працівниками бізнес-підрозділів, IT персоналом і економістами)

використовуються програмні засоби управління ресурсами систем зберігання даних VisualSRM. Процес ідентифікації та класифікації даних є циклічним.

2.2. Багаторівневий захист і відновлення даних. Цифрові дані Корпорації захищаються відповідно до їх цінністю для бізнесу, вимогам за термінами відновлення, рівнів сервісу та з урахуванням фінансових можливостей.

Для виконання локальної та географічно віддаленої реплікації використовується програмне забезпечення SnapView / MirrorView (CLARiiON), CentraStar (Centera) і RepliStor (Windows, NetWin).

Для забезпечення автоматичної доступності критично важливих додатків використовується програмне забезпечення локальної та географічно розподіленої кластеризації: для *Windows систем* – Microsoft Cluster, Co-Standby Server AAdvanced; для *UNIX, Linux систем* – Automated Availability Manager (AAM).

2.3. Засоби управління реплікацією. Для автоматизації та спрощення робіт по реплікації даних використовується програмне забезпечення сімейства Replication Manager і вбудовані засоби управління реплікацією з командного рядка CLI.

2.4. Інтеграція реплікації з додатками. Для забезпечення узгодженої захисту взаємопов'язаних даних (MS SQL Server, Oracle, Exchange, SAP), в тому числі і взаємопов'язаних окремих додатків, використовуються спеціальне програмне забезпечення сімейства Replication Manager, Oracle RapidClone, а також спеціалізовані модулі для NetWorker.

2.5. Резервне копіювання на диски. Для досягнення істотного зменшення часу на виконання операцій резервного копіювання і відновлення даних в ролі пристрою розміщення резервних копій використовуються диски CLARiiON ATA і програмне забезпечення NetWorker.

Існує три класи резервного копіювання: надоперативне, оперативне, архівне.

Резервні копії *надоперативного* резервного копіювання для конкретного класу і для даних створюються або за допомогою засобів реплікації MirrorView і SnapView (CLARiiON) або Microsoft VSS (NetWin) з різною періодичністю і зберігаються на дисках CLARiiON ATA як в локальному офісі / ВЦ так і в віддалених офісі / ВЦ (залежно від класу даних). Ці резервні копії доступні для відновлення з диска протягом доби.

Резервні копії *оперативного* копіювання створюються за допомогою програмного забезпечення NetWorker і зберігаються на дисках CLARiiON ATA. Ці резервні копії доступні для відновлення з диска в термін від одного до двох тижнів, в залежності від класу даних.

Резервні копії *архівного* копіювання створюються безпосередньо з вихідних даних або перенесенням оперативних резервних копій, в залежності від класу даних, за допомогою програмного забезпечення NetWorker і зберігаються на носіях інформації тривалого зберігання. Ці резервні копії доступні для відновлення в строк до декількох років, в залежності від вимог керівництва і регулюючих органів для певних класу і типу даних.

Спільна робота програмного забезпечення NetWorker разом із засобами ієрархічного зберігання даних DiskXtender 2000 дозволяє істотно скоротити час створення резервних копій і вимоги до обсягу простору систем зберігання даних.

III. Опис функціонування системи резервного копіювання. Для забезпечення збереження цінних цифрових даних Корпорації для захисту від надзвичайних обставин рівня офісу та регіону оптимальна кількість резервних копій об'єкта даних, що захищаються розміщуються в резервному офісі конкретного ЦОД і в центральному ЦОД. Конфігурація ресурсів, які захищаються, документується в цифровому вигляді та на паперових носіях. Оригінали та дублікати документації на систему, ресурси що захищаються, і покрокова інструкція процесів відновлення зберігаються в кожному з двох офісів ЦОД (в ЦОД та відповідальному за дублювання інформації конкретного ЦОД), а також в центральному ЦОД.

Ключові компоненти системи (апаратні і програмні засоби, персонал) обов'язково дублюються і їх дублікати мають бути наявними, як в різних офісах конкретного ЦОД, так і в віддаленому ЦОД, відповідальному за дублювання інформації конкретного ЦОД. Дублікати

засобів централізованого управління та моніторингу системи разом з навченим персоналом знаходяться в резервному ЦОД.

Усі системні адміністратори офісів Корпорації повинні бути навчені способам створення резервної копії за запитом та відновлення даних підзвітних їм серверів за допомогою клієнтського програмного забезпечення NetWorker. У кожному з офісів кожного ЦОД мається дискова система CLARiiON з дисками FC і ATA, а також дискова бібліотека ADIC Scalar 100 з мінімум 2-мя пристроями копіювання на магнітну стрічку.

Опис функціонування системи наводиться на прикладі абстрактного об'єкта системи зберігання даних (логічний том, файлова система, каталог, файл). При зміні об'єкта ці зміни синхронно реплікується до резервного офісу ЦОД і асинхронно в центральний ЦОД.

З кожною з віддалених реплік і з базового об'єкта створюються локальні репліки, які використовуються для цілей створення оперативних (в локальному офісі) і архівних резервних копій (в резервному офісі та центральному ЦОД).

Локальна репліка використовується як надоперативна резервна копія.

З локальної репліки базового об'єкта створюється оперативна резервна копія, яка зберігається на дисках CLARiiON ATA. Застарілі оперативні резервні копії переміщуються відповідно до staging політики на магнітні стрічки (локально). З локальних реплік, створених з віддалених реплік, проводиться створення архівних резервних копій.

У разі переміщення об'єкта відповідно до політиками зберігання даних на магнітні стрічки він виключається зі списку операцій створення локальних архівних резервних копій на магнітну стрічку (так як він вже знаходиться на магнітній стрічці).

В результаті для захищеного об'єкта маємо: локальну *надоперативну* резервну копію (локальна репліка); локальну *оперативну* резервну копію; локальну *архівну* резервну копію; *віддалену репліку* (синхронна і асинхронна); *архівні* резервні копії у віддалених офісах.

IV. Архівування, резервування та відновлення даних Oracle, MS SQL Server, SAP.

Для зменшення часу проектів впровадження, оновлення та міграції, а також часу простоїв для додатків Oracle, MS SQL Server і SAP використовуються спеціалізовані рішення:

– для управління неструктурованими цифровими даними та архівуванням даних додатків SAP застосовується EMC Documentum Content Management and Archiving for SAP;

– для надання докладної інформації про використання, конфігурування і проактивному контролі ресурсів зберігання даних MS SQL Server і Oracle застосовується VisualSRM Database Edition. Для фізичного переміщення даних Oracle в сховища різного рівня відповідно до заданими політиками і з збереженням логічного представлення даних застосовується ПО DatabaseXtender;

– спеціалізований модуль NetWorker PowerSnap Module for SAP, який надає можливості управління множинними "моментальними копіями", швидкого відновлення з дотриманням узгодженості та виконання резервного копіювання без переривання роботи додатків для даних SAP;

– для створення узгоджених локальних реплік даних Oracle використовується програмне забезпечення Oracle RapidClone;

– для резервного копіювання даних Oracle і MS SQL Server використовуються відповідні модулі NetWorker.

V. Оптимізація систем зберігання даних Exchange. Електронна пошта є критичним для бізнесу Оператора додатком і забезпечення доступності та надійності зберігання даних серверів електронної пошти Exchange є одним з основних завдань забезпечення операційної ефективності всієї ІТ інфраструктури, для чого використовуються наступні рішення:

5.1. Консолідація архітектури. У процесах консолідації інфраструктури поряд з централізацією зберігання даних в середовищі SAN і NAS застосовуються спеціалізоване рішення VisualSRM з автоматизованого управління ресурсами зберігання даних Exchange.

5.2. Резервування та відновлення даних. Забезпечення вимог з резервного копіювання і швидкому відновленню даних Exchange аж до рівня відновлення окремого повідомлення забезпечують наступні технології:

- використання дисків CLARiiON ATA для зберігання резервних копій Exchange.
- автоматизоване управління інфраструктурою локальних реплік Replication Manager/SE.
- спеціалізовані модулі Legato NetWorker.

5.3. Інтелектуальне архівування даних. Для істотного скорочення розмірів бази даних Exchange, виключення дублювання повідомлень і вкладень, а також впровадження управління процесами архівування і видалення старих повідомлень на базі політик застосовуються такі технології і продукти:

- он-лайн архівне сховище Centera;
- диски CLARiiON ATA для зберігання резервних копій;
- засоби забезпечення автоматичного управління ресурсами Exchange - EmailXtender і VisualSRM.

VI. Автоматизація і централізація управління та моніторингу. Для централізованого та автоматизованого керування та моніторингу інфраструктури системи використовується програмне забезпечення VisualSRM, NetWorker Management Console і модулі NetWorker PowerSnap. Для централізованого управління життєвим циклом магнітних стрічок і поділу пристроїв стрічкових бібліотек використовується програмне забезпечення AlphaStor.

Засоби централізованого управління та моніторингу VisualSRM, NetWorker Management Console і AlphaStor розташовуються в центральних ВЦ і знаходяться в активному стані в Київському ЦОД.

VII. Служба архівування та відновлення. Oracle пропонує цілий набір спочатку доступних з базою даних добре інтегрованих рішень, націлених на захист даних і екстреного відновлення після катастроф.

Oracle пропонує наступні рішення щодо захисту даних:

– Oracle Data Guard – ефективний і надійний спосіб захисту даних і екстреного відновлення. Пропонується як складова частина Enterprise редакції бази даних Oracle;

– Oracle Streams – інтегрована особливість бази даних редакції Enterprise, може бути використано для підтримки однієї або кількох реплік основної бази даних. Ці репліки не обов'язково повинні бути ідентичні, – вони можуть бути лише піднабором основної бази даних або продуктом заданої трансформації. Streams підтримують двунправлену реплікацію з визначенням конфліктів і їх дозволом. Його унікальна гнучкість дозволяє підтримувати реплікацію даних між великою кількістю баз даних в будь-якій мережевий топології. Не дивлячись на те, що в деяких ситуаціях може знадобитися гнучкість Streams, перш за все ця технологія розроблена для інтеграції великих розподілених конфігурацій баз даних, а не виключно для забезпечення катастрофо стійкості;

– Oracle Advanced Replication – дозволяє копіювання і підтримку об'єктів у кількох базах даних складових розподілену систему баз даних. Oracle Advanced Replication дозволяє змінювати будь-які репліки баз даних і поширювати ці зміни автоматично в інші бази даних, підтримуючи глобальну узгодженість транзакцій і цілісність даних. У разі виходу з ладу однієї з баз даних, інші бази даних продовжують працювати;

– Oracle Recovery Manager – RMAN є утилітою Oracle для управління резервними копіями баз даних та їх відновленням. Для створення резервної копії за допомогою RMAN база даних може знаходитися у відкритому стані. Під час копіювання і відновлення RMAN аналізує дані на наявність їх фізичних руйнувань. RMAN здатний виробляти резервне копіювання і швидке відновлення окремих перекручених блоків;

– OSCP Validated Remote Mirroring – програма сертифікації сумісності дозволяє для партнерів підтвердити можливість використання їх продуктів на підставі технології віддаленого дзеркалювання спільно з базами даних Oracle.

Для замовників Oracle рекомендує наступне:

- використовувати Oracle Data Guard для захисту від катастроф, людських помилок і спотворень даних;
- використовувати продукти віддаленого дзеркалювання інших виробників для захисту і реплікації файлів і томів, які не належать базі даних;
- для створення резервних копій баз даних використовувати утиліту RMAN.

VIII. Технологія віддаленого дзеркалювання. В даний час багато вендорів систем зберігання пропонують або host-based (програмні) або storage system box-based (апаратні) продукти віддаленого дзеркалювання (Рис. 1). Подібні продукти забезпечують дзеркалювання іміджів дисків або томів на відстані. Ця можливість може використовуватися для аварійного відновлення, коли дані на основний (первинної) системі стають недоступними після катастрофи, і користувачам для забезпечення роботи необхідні дубльовані дані доступні на резервній системі.

При програмному віддаленому створення дзеркал, запис, ініційована хостом, надсилається як на локальний пристрій зберігання даних, так і на віддалений хост. Віддалений хост, в свою чергу, ініціює запис на віддалене пристрій зберігання.

При апаратній віддаленому створення дзеркал локальне та віддалене пристрій зберігання пов'язані через виділене з'єднання. Хост проводить запис на локальний пристрій зберігання. Локальний пристрій зберігання направляє запит записи на віддалене пристрій зберігання.

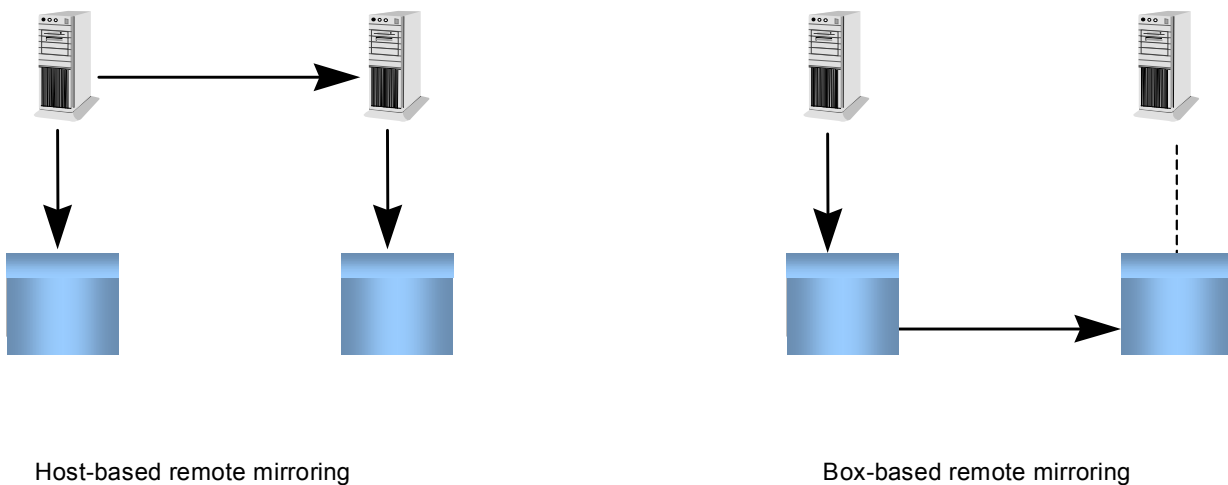


Рис. 1. Способи віддзеркалення даних

Програмне віддалене дзеркалювання, як правило, є більш гнучким, але має на увазі більш інтенсивне використання системних ресурсів.

Апаратне віддалене дзеркалювання вимагає виділеної мережі для пристроїв зберігання, як правило, більш дороге, але споживає меншу кількість системних ресурсів.

Існують два основні методи віддаленого дзеркалювання. Ініційована запис з первинної системи, запис може бути передана на резервну систему синхронно або асинхронно:

Синхронний режим: для програми на локальній системі запис не підтверджується доти, поки не буде зроблена запис, як на локальну, так і на віддалену систему зберігання. Тобто локальна система не дає підтвердження додатком про те, що запис проведена успішно до тих пір, поки не буде завершена локальна запис і не буде отримано підтвердження з віддаленої системи, що запис на віддалене пристрій зберігання проведена успішно.

Асинхронний режим: запис з локальної системи може бути підтверджено до отримання підтвердження запису на віддалену систему. Тобто локальна система може підтвердити додатку, що запис здійснено успішно, до того як він реально здійснений на віддалену систему.

Синхронний режим віддаленого дзеркалювання гарантує повну безпеку даних, але може значно вплинути на продуктивність первинної системи, у зв'язку з необхідністю очікування запису від віддаленої системи.

Асинхронний режим віддаленого дзеркалювання забезпечує найбільшу продуктивність, але його використання має на увазі певний ризик втрати даних у разі апаратного або програмного збою.

Програма для виробників програмного і апаратного забезпечення OSCP (Oracle Storage Compatibility Program) підтверджує сумісність рішень віддаленого дзеркалювання з базами даних Oracle. Oracle Data Guard пропонує технологію, яка надає великі можливості з аварійного відновлення даних для баз даних Oracle. Oracle використовує технологію баз даних Standby. Резервна (Standby) База Даних Oracle є копією первинної (Primary) Бази.

Oracle Data Guard – програмне забезпечення, що дозволяє створювати, підтримувати і контролювати одну або кілька резервних (standby) баз даних для захисту від збоїв, катастроф, помилок і спотворень даних (Рис. 2).

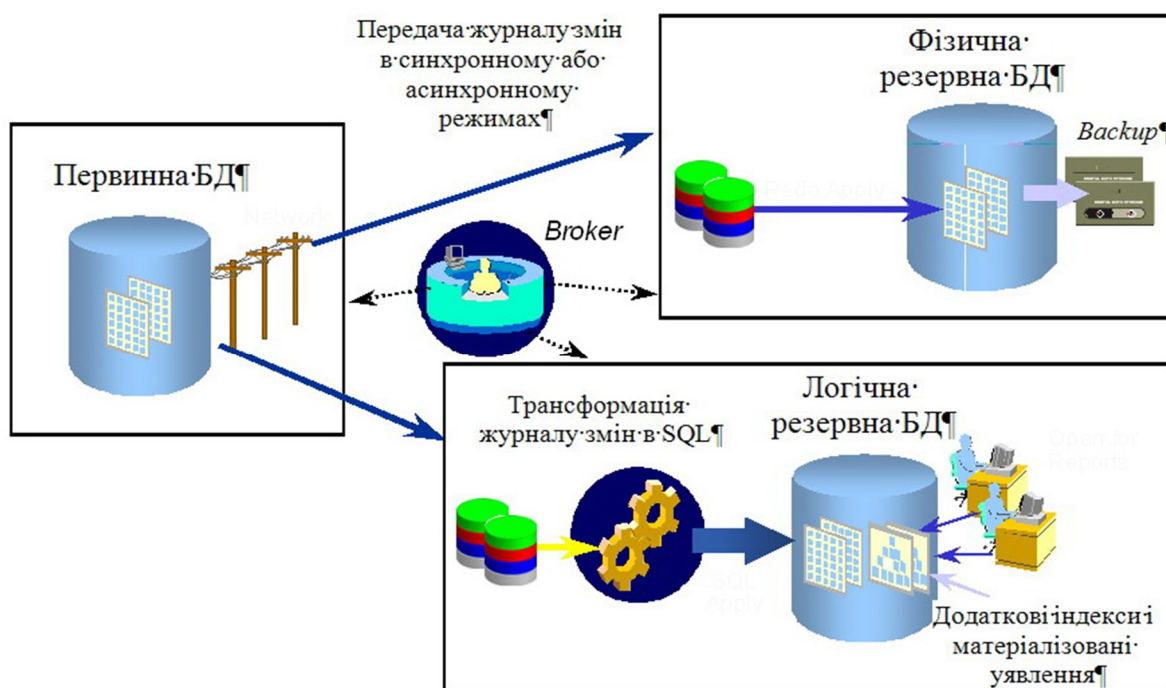


Рис. 2. Створення резервних баз даних

Oracle Data Guard підтримує резервні бази даних як транзакційно узгоджені копії первинної бази даних. Резервні бази даних можуть розташовуватися у віддалених резервних центрах на необмежено далекій відстані від первинної системи. Якщо первинна система стає недоступною в результаті планового або позапланового зупину, Data Guard може призначити роль первинної системи будь резервної базі даних, мінімізуючи час перебою в наданні сервісу і запобігаючи втрату даних.

Конфігурація Oracle Data Guard складається з однієї первинної бази даних і однієї або декількох (максимум до 9) резервних баз даних, при необхідності розподілених географічно.

Спочатку резервна база даних створюється з резервної копії основної або іншої резервної бази даних. Після створення Oracle Data Guard автоматично підтримує резервну базу даних як транзакційно узгоджену копію первинної. Це досягається шляхом перенесення та застосування журналу змін (redo logs) первинної бази даних на резервній системі. Журнал змін являє собою послідовність модифікації блоків бази даних на бінарному рівні.

Data Guard забезпечує два методи застосування журналу змін на резервній системі:

- Redo Apply, використовується для фізичної резервної бази даних;
- SQL Apply, використовується для логічної резервної бази даних.

Обидва методи відповідають своїм типам резервних баз даних підтримуваних Oracle.

Фізична резервна база даних забезпечує бінарно-ідентичну копію первинної бази даних. Вона має еквівалентну з первинною БД фізичну дискову структуру. Технологія Redo Apply застосовує журнал змін, використовуючи стандартну технологію відновлення сервера Oracle. Під час процесу синхронізації резервна база даних знаходиться в режимі mount і недоступна для інших операцій.

Логічна резервна база даних містить логічно еквівалентну первинній базі даних інформацію, хоча фізична організація і структура можуть розрізнятися. Технологія SQL Apply увазі перенесення інформації журналу змін на резервну базу даних, трансформації її в послідовність стандартних SQL команд і їх виконання в логічній резервній базі даних. Під час процесу синхронізації резервна база даних знаходиться в режимі open і її дані доступні для виконання SQL запитів і створення звітів. Таким чином, логічна резервна база даних одночасно може використовуватися і для захисту даних і для звітності, дозволяючи перенести небажану навантаження з первинною системою.

За допомогою Data Guard роль бази даних може бути "перемкнута" з первинною на резервну і навпаки. Існують два типи обміну ролями - switchover і failover.

При switchover первинна база даних змінюється роллю з однією з резервних баз даних. Первинна база даних стає резервною, а резервна первинною, відповідно. Це буває необхідно при виконанні запланованих сервісних робіт на первинній системі. При необхідності, наприклад, після закінчення робіт, баз даних можуть бути повернуті початкові ролі.

При failover відбувається необоротна передача ролі первинної бази даних однією з резервних. Це, як правило, може статися у разі катастрофічних явищ, що призвели до виходу з ладу первинної системи.

Швидкість перемикавання ролей не залежить від розміру бази даних, а залежить від інтенсивності змін до первинної системі. Для перемикавання необхідно досилання журналу змін з первинною бази даних на резервну систему (тільки для асинхронного режиму і в разі доступності первинної системи) і застосування всіх останніх змін на резервній базі даних. Для прискорення процесу перемикавання в Oracle можливе включення режиму безперервного застосування журналу змін на резервній системі.

У деяких ситуаціях бізнес не може дозволити собі втрату даних за будь-яку ціну. В інших ситуаціях, додатки вимагають максимальної продуктивності і можуть забезпечити відновлення потенційну втрату останніх змін. Data Guard забезпечує три основні режими захисту, здатних задовольнити різні вимоги:

– Maximum Protection – режим максимального захисту даних. Дані синхронно передаються на резервну базу даних з первинної системи. Транзакція на первинній базі даних не може бути завершена до тих пір, поки не буде підтвердження, що всі зміни ув'язнені в цій транзакції перенесені хоча б на одну резервну базу даних. У цьому режимі хоча б одна резервна база даних повинна бути робочому стані, в іншому випадку процесінг на первинній базі даних буде зупинений. Цей режим гарантує збереження даних;

– Maximum Availability – режим схожий на попередній, за винятком того, що в разі недоступності всіх резервних баз даних (наприклад, проблеми з мережею передачі даних), робота на первинній базі даних буде продовжена без зупину. Коли проблема буде усунена, резервні бази даних будуть автоматично синхронізовані з первинною;

– Maximum Performance – режим, що забезпечує дещо меншу ступінь захисту первинної бази даних (у разі катастрофи, можлива втрата незначної частини останніх змін), але забезпечує більш високу продуктивність, ніж інші два режими. У цьому режимі журнал змін асинхронно передається на резервні бази даних. Транзакції на первинній базі даних не залежать від успішності передачі журналу змін. У разі недоступності всіх резервних баз

даних робота на первинній продовжується в звичайному режимі. Після усунення проблем з недоступністю резервної базою даних її ресинхронізація проводиться автоматично.

Oracle Data Guard Broker – розподілена керуюча структура автоматизує створення, підтримку і контроль конфігурацій Data Guard через графічний інтерфейс.

Для додавання нових резервних баз даних в конфігурацію Data Guard немає необхідності переривати роботу сервісу забезпеченого первинною базою даних. При оновленні програмного забезпечення (накат "патчів") в більшості випадків так само немає необхідності навіть в короточасній зупинці системи. У разі необхідності вимикання системи для цих цілей, наявність в конфігурації логічної резервної бази даних дозволяє скоротити цей час до мінімуму - часу перемикання первинної ролі на цю резервну систему. Ці особливості практично забезпечують можливість роботи в режимі 24x7.

Наявність у системі управління Oracle Enterprise Manager інтерфейсу управління Data Guard Broker дозволяє просте і повне управління конфігурацією (наприклад, перемикання ролей баз даних здійснюється однією кнопкою), відстеження важливих показників продуктивності, оповіщення адміністраторів у разі настання певної події.

Фізична резервна база даних забезпечує надійне та ефективне відновлення після катастрофи та високодоступних рішень. Фізична база даних дозволяє виробляти швидке застосування журналів змін, внаслідок чого стабільну синхронізацію і швидке перемикання ролей. Крім цього, вона може бути використана як джерело для створення резервної копії первинної бази даних.

У той же час використання логічної резервної бази даних на додаток дає такі переваги:

- можливість виконання запитів і звітів дозволяє скоротити завантаження первинної системи – це дозволяє використовувати логічну резервну базу даних не тільки для забезпечення надійності;

- можливість додавання індексів, а так само перевизначення і трансформації таблиць, дозволяє оптимізувати виконання запитів і звітів;

- трансляція журнальної інформації в SQL команди забезпечує додаткову перевірку на спотворення даних;

- мінімізація часу простою в разі необхідності виконання оновлень програмного забезпечення пов'язаного із зміною словника бази даних.

Обидва типи резервних баз даних можуть застосовуватися разом, доповнюючи можливості один одного і забезпечуючи більш високу доступність системи.

Рішення, які використовують технології віддаленого дзеркалювання пропонують концептуально простий і повний захист даних. Проте, для даних розміщених всередині БД Oracle, рішення із застосуванням Oracle Data Guard насправді набагато ефективніше, менш витратні і більш оптимізовані для захисту даних і аварійного відновлення, ніж віддалене дзеркалювання. Не дивлячись на те, що віддалене дзеркалювання дає деякі додаткові можливості по захисті не-Oracle даних (наприклад, дані файлових систем або дані не-Oracle БД), використання Oracle Data Guard не вимагає додаткової інтеграції та придбання рішень, які використовують технології віддаленого дзеркалювання.

IX. Використання баз даних Oracle з технологіями віддаленого дзеркалювання.

Щодо використання баз даних Oracle з технологіями віддаленого дзеркалювання, застосування Oracle Data Guard дає наступні основні переваги:

9.1. Ефективне використання мережі. З використанням Oracle Data Guard на віддалену систему передаються тільки журнальні ("redo") дані. Однак, якщо для захисту даних використовується рішення з віддаленим дзеркалюванням, в реальному часі повинна здійснюватися синхронізація всіх змін вироблених в файлах даних, журнальних файлах, архівних журнальних файлах і керуючих файлах.

Записи у файли даних відбуваються незрівнянно частіше, ніж записи в журнальні файли, в зв'язку з тим, що кожен запис в журнальний файл зазвичай містить безліч змін. Це

позначає, що пропускна здатність мережі необхідна для передачі журнальної інформації значно менше, ніж для рішень з використанням віддаленого дзеркалювання.

Експерименти показали, що в загальному випадку обсяг мережевого трафіку при використанні Data Guard був в 5-10 разів менше, ніж при використанні віддаленого дзеркалювання. Кількість же операцій введення / виводу менше в десятки разів.

9.2. Можливість використання в глобальних мережах. Рішення з використанням віддаленого дзеркалювання часто мають дистанційні обмеження, що накладаються наступними комунікаційними технологіями (Fiber Channel, ESCON). Для досягнення більшого потрібне застосування додаткового обладнання інших виробників.

У результаті ми маємо три основні проблеми:

– *вартість*: рішення із застосуванням технології віддаленого дзеркалювання дороги, навіть не беручи до уваги вартість конвертерів і повторювачів, необхідних для збільшення можливої відстані між центрами. (Вартість IBM Peer-to-Peer Remote Copy знаходиться в діапазоні \$ 60К-\$ 80К, а розширювачів в районі \$ 600К);

– *затримки*: кожен пристрій вносить значну затримку, впливаючи на продуктивність промислової бази даних і роблячи таку конфігурацію невідповідною для синхронного режиму (що гарантує передачу даних без втрат);

– *спотворення даних*: рішенням може бути використання асинхронного режиму, який в свою чергу не в змозі забезпечити порядок запису на всі дзеркальовані томи, що зберігають файли бази даних.

У зв'язку з тим, що Oracle Data Guard на віддалену систему виробляє передачу тільки журнальної інформації, забезпечує транзакційну цілісність даних у всіх режимах передачі (синхронний або асинхронний) і не вимагає дорогих проміжних пристроїв, це рішення є найкращим для аварійного відновлення та захисту даних в глобальних мережах .

9.3. Велика стійкість і захист даних. Oracle Data Guard забезпечує набагато кращий ступінь захисту даних, ніж рішення, які використовують віддалене дзеркалювання. Технологія дзеркалювання виробляє поблочну синхронізацію будь-яких змін на віддалений сервер, в тому числі і спотворень даних, які відбулися в результаті збою системного програмного забезпечення або апаратури на первинній системі. Наприклад, якщо на диск проведено помилковий запис, або відбувається спотворення даних у файловій системі, або контролер диска спотворює блок при записі на диск, то віддалене дзеркалювання точно перенесе дану помилку на віддалену систему. Подібне копіювання спотвореної інформації виключено при використанні Oracle Data Guard, яка провадить передачу тільки журнальної інформації, яка перед застосуванням на віддаленій системі логічно перевіряється на правильність.

"SQL Apply" забезпечує ще більший захист даних, транслюючи журнал змін в серію SQL команд. Це забезпечує надійну перевірку будь-яких змін. Крім цього ця можливість дозволяє ігнорувати не бажані зміни даних (це налаштовується). Нічого подібного неможливе з використанням віддаленого дзеркалювання.

9.4. Більша гнучкість. Data Guard реалізований на горі стику апаратного та системного програмного забезпечення. Все, що необхідно цьому продукту для роботи - тільки стандартна TCP / IP мережа між первинною і резервною системою. Немає необхідності у використанні дорогих пристроїв. Крім усього іншого, це дозволяє несиметричні конфігурації пристроїв зберігання на первинних і резервних системах.

На противагу віддалене дзеркалювання часто вимагає ідентичну конфігурацію пристроїв того ж самого виробника.

9.5. Краща функціональність. Data Guard є цілим комплексом можливостей для забезпечення високої доступності, наприклад, Redo Apply (фізична резервна база даних), SQL Apply (логічна резервна база даних), безліч режимів захисту (від максимально захищеного до максимально швидкого), зміна ролей між первинною і резервною системою однією кнопкою, автоматичне визначення і ліквідація відставання змін, єдиний графічний інтерфейс для управління та моніторингу, каскадне розповсюдження журнальної інформації і т.д. Це

набагато більш всебічне і ефективне рішення, оптимізоване для захисту даних і аварійного відновлення, ніж рішення використовують технологію віддаленого дзеркалювання.

9.6. Швидка окупність. Використовуючи Oracle Data Guard, логічна резервна база даних може бути відкрита в режимах читання або читання / запис для створення звітів і виконання запитів під час здійснення синхронізації змін вироблених в первинній базі даних. Для прискорення виконання запитів, в логічній резервній базі даних, можуть бути створені додаткові індекси і матеріалізовані уявлення. Крім цього фізична резервна база даних може бути відкрита або в режимі синхронізації, або в режимі читання даних. Подібні режими зазвичай неприпустимі при використанні технології віддаленого дзеркалювання. В результаті резервні системи знаходяться в простій, що істотно скорочує їх коефіцієнт окупності.

Oracle Data Guard інтегрований з Oracle Recovery Manger – це дозволяє проводити резервне копіювання (backup) даних використовуючи для цих цілей резервну базу даних, тим самим, знімаючи небажану навантаження з первинною системи.

Oracle Data Guard підтримує перемикання ролей первинної та резервної системи в цілях твору оновлення (upgrade) системного програмного забезпечення або заміни / додавання обладнання. Тим самим, значно скорочується час простою викликаного цими операціями - зазвичай це неможливо при використанні технології віддаленого дзеркалювання.

При реалізації рішень видаленого дзеркалювання на апаратному рівні потрібна наявність окремого високошвидкісного каналу зв'язку для забезпечення зв'язку між синхронізуються пристроями зберігання. Крім цього, Oracle Data Guard є складовою частиною ядра бази даних Oracle. Немає необхідності виробляти додаткові закупівлі і роботи з інтеграції. Він повністю інтегрований з іншими високодоступними рішеннями від Oracle (наприклад, Real Application Cluster, Recovery Manager). Тим часом, рішення віддаленого дзеркалювання вимагають додаткової покупки програмного та / або апаратного забезпечення та інтеграції з базою даних.

9.7. Інші аспекти. Крім перерахованих вище існує безліч інших аспектів, які слід розглядати при виборі між рішеннями віддаленого дзеркалювання і Data Guard в цілях екстреного відновлення. Наприклад, для дуже великих баз даних важливим фактором може бути спосіб створення і перевідтворення резервної системи. Копіювання такої бази даних через мережу може бути дуже проблематичним. З використанням Data Guard віддалена резервна система може бути створена за допомогою резервної копії (backup) первинної бази даних (наприклад, з стрічки).

Ще один аспект - дозвіл мережевих проблем. Data Guard дозволяє режим Maximum Availability, що гарантує нульову втрату змін даних, за допомогою синхронної передачі на резервну систему. У разі тимчасової недоступності резервної системи робота на первинній базі даних буде продовжена без змін, коли віддалена система стане доступною знову, Data Guard самостійно зробить її синхронізацію без впливу на продуктивність первинної системи.

X. Висновки. У статті розглядається задача проектування служб, які відносяться до сервісів управління даними в дата центрах і визначаються відповідно до архітектури інфраструктури додатків. Проектними рішеннями, на яких побудована служба, є:

- ідентифікація та класифікація цифрових даних відповідно до їх цінності для ділових операцій Корпорації;
- захист даних відповідно до їх класу / категорії;
- використання стандартних компонентів багаторівневих сховищ даних EMC для розміщення резервних копій даних різного класу на сховищах інформації відповідної продуктивності, доступності, надійності та вартості;
- автоматизація і централізація управління та моніторингу;
- територіальний розподіл місць зберігання резервних копій;
- виключення єдиної точки відмови ключових компонентів системи.

Компонентами служби архівування та відновлення пропонуються:

- апаратні засоби (виділені сервера системи, дискові масиви CLARiiON з FC і ATA дисками, стрічкові бібліотеки ADIC, середа передачі даних системи);

- програмні засоби сімейства EMC Legato NetWorker;
- персонал – адміністратори системи.

Литература

1. Еталонні архітектури MSA. – К.: Майкрософт Україна; К.: Видавнича група ВНН, 2005. – 352 с.
2. Копійка О. В. Проектування сервісів управління IT-інфраструктурою в сучасних дата-центрах / О.В.Копійка// Зв'язок. – 2013. – № 5(105). – С.23-31.
3. Копейка О. В. Архитектура инфраструктуры приложений в дата-центрах / О. В.Копейка // Зв'язок. – 2013. – № 6(106). – С.19-26.
4. Копейка О. В. Архитектура мережі в сучасних дата-центрах / О.В.Копейка// Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – № 2(30). – С.34-41.
5. Копейка О. В. Архитектура системы управления IT-инфраструктурой в современных Дата-центрах / О.В.Копейка // Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – № 1(29). – С.29-37.
6. Копейка О. В. Проектирование сервисов безопасности в дата-центрах / О. В. Копейка // Сучасний захист інформації. – 2014. – №2. – С.10-15.
7. Копейка О. В. Архитектура системы безопасности IT-инфраструктуры в дата-центрах/ О. В. Копейка // Сучасний захист інформації. – 2014. – №1. – С.48-57.
8. Копейка О. В. Архитектура системы хранения данных современных Дата-центров / О. В. Копейка // Системи управління, навігації та зв'язку. – 2014. – №1(29). – С.85-88.
9. Копейка О. В. Сетевые службы и службы сетевых устройств в дата-центрах / О. В. Копейка//Системи управління, навігації та зв'язку. – 2013. – №4(28). – С.98-104.
10. Копейка О. В. Проектирование сервисов инфраструктуры приложений в дата-центрах / О. В. Копейка // Телекомунікаційні та інформаційні технології. – 2014. – №1. – С.19-27.
11. Копейка О. В. Проектування сервісів зберігання даних /О.В.Копейка// Телекомунікаційні та інформаційні технології. – 2014. – №2. – С.90-96.
12. Довгий С. О. Засади регіональної інформатизації / С. О. Довгий, О. В. Копійка, Ю. Т. Черепін. – К.: ВПЦ «ТИРАЖ», 2004. – 304 с.
13. Довгий С. А. Новые технологии в телекоммуникации: выбор технологической архитектуры. Современные тенденции развития / С. А.Довгий, О. В. Копейка, С. П. Поленок. – К.: Укртелеком, 2001. – 281 с.
14. Kopeika O. Softline applies TMF standards as a guide when building Resource Inventory solution for nation-wide carrier Ukraine Telecom / O. Kopeika, I. Tarasenko, A. Kisselevskiy, A. Karichenskiy, T. Valiulin // TM Forum Case Study Handbook, Volume 3, May 2007. – P. 27.
15. Разработка стандартов // – Режим доступа : <http://www.tiaonline.org/standards/>
16. Jew Jonathan. BICSI Data Center Standard: A Resource for Today's Data Center Operators and Designers // BICSI News Magazine, May/June 2010. – 28 p.
17. Niles, Susan. Standardization and Modularity in Data Center Physical Infrastructure // 2011, Schneider Electric. – P. 4.
18. Telecommunications Infrastructure Standard for Data Centers // TIA standard TIA-942. Telecommunications Industry Association. – April 2005. –135 p.
19. ANSI/BICSI 002-2011. Data Center Design and Implementation Best Practices // Committee Approval. – January 2011. – First Published: March 2011. – 367 p.

Дата надходження в редакцію: 02.09.2014 р.

Рецензент: д.т.н., проф. Беркман Л. Н.