denovo
Inspired by the Future

vmware CLOUD VERIFIED

DR та Backup рішення - як комплексний захист бізнесу

Зміст

DR та Backup рішення – як комплексний захист бізнесу

> Дані перетворились у ключовий актив для більшості сучасних організацій. Короткочасна недоступність необхідної інформації, не кажучи вже про її повну втрату, може стати серйозним ударом для будь-якого бізнесу. Тому як даним, так і цілим IT-інфраструктурам потрібні механізми відновлення працездатності після збоїв. Найбільш популярними підходами в даному випадку є такі методи як резервне копіювання та аварійне відновлення.

Коли говорять про цінності даних для організацій всіх рівнів, часто не беруть до уваги той факт, що важливим є не тільки їх наявність сама по собі, але і те, чи забезпечується до них **своєчасний доступ**. Доступ до інформації в ідеальному випадку повинен бути безперебійним. Але IT-інфраструктури, як відомо, схильні до збоїв і аварій, які можуть призвести до того, що дані можуть виявитися тимчасово або повністю втраченими.

При цьому, як показує практика, для більшості компаній неможливість доступу до важливих даних протягом хоча б кількох годин майже завжди чинить **серйозний негативний вплив на бізнес** і веде до значних матеріальних і репутаційних втрат. Для окремих компаній критичний період недоступності обчислюється навіть хвилинами, після чого можна починати підраховувати збитки.

Щоб уникнути подібних неприємностей, дані необхідно захищати, і найпопулярнішими варіантами вирішення цього завдання є такі методи як **резервне копіювання (backup)** і **аварійне відновлення (disaster recovery, DR)**. Незважаючи на те, що обидва вони служать одній меті, різниця між цими підходами досить істотна та про неї варто поговорити більш детально.

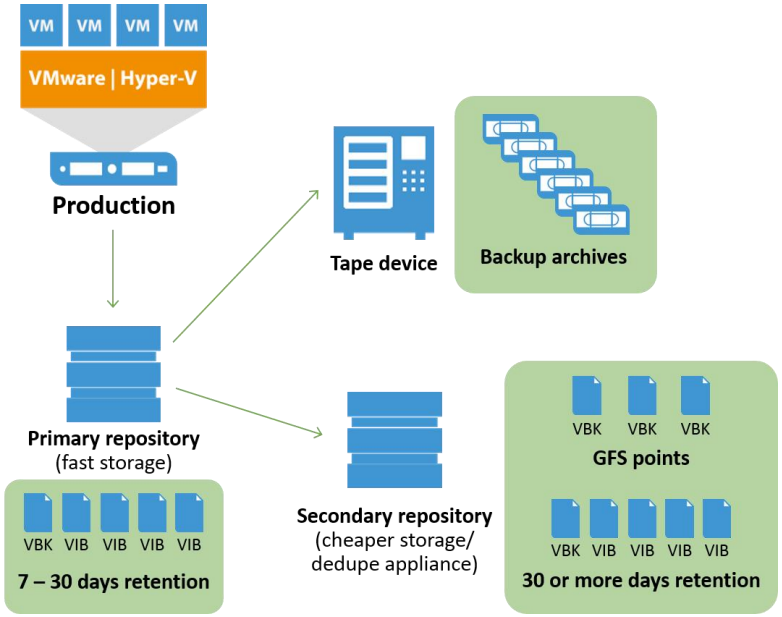
Концептуальні відмінності

Якщо спробувати позначити різницю між термінами "резервне копіювання" і "аварійне відновлення" максимально коротко, то звести її можна до того, що backup — всього лише **процес створення резервних копій** даних на зовнішніх носіях (будь-який самостійний накопичувач, СЗД, хмара), в свою чергу disaster recovery — це **комплекс взаємопов'язаних процедур**, що дозволяють відновити працездатність цілої IT-інфраструктури після збою. Таким чином, вже на цьому етапі очевидно, що обидва

терміни взаємопов'язані, але не тотожні. Якщо DR передбачає обов'язкову наявність backup, то в зворотному порядку цей взаємозв'язок не працює — володіння резервними копіями саме по собі зовсім не забезпечує відновлення працездатності системи після аварії. Щоб краще зрозуміти нюанси обох підходів, трохи заглибимося в деталі їх роботи.

> **Резервне копіювання передбачає** створення цифрових дублікатів різних елементів IT-інфраструктури — даних, віртуальних машин, образів операційних систем та подальше їх розміщення в захищеному сховищі. Це можуть бути спеціальні накопичувачі (жорсткі диски, магнітна стрічка), виділена СЗД, хмара або поєднання всього перерахованого.

Зрозуміло, копій може бути кілька. Їх оновлення (актуалізація) здійснюється регулярно, як правило, раз на день (тиждень, місяць, квартал) — в залежності від важливості та актуальності тих чи інших даних. Процес цей носить покроковий характер і здійснюється відносно повільно. Наявність резервних копій часто є обов'язковою нормативною вимогою для певних компаній та організацій.



На сучасному етапі розвитку технологій все більш популярним варіантом стає інструмент створення резервних копій в хмарі (Backup as a Service, BaaS). Оскільки даний варіант, з урахуванням всіх факторів, як правило, забезпечує оптимальну вартість зберігання в розрахунку на одиницю інформації при максимальній захищеності даних.

Резервне копіювання приваблює своєю надійністю і простотою, але є у цього методу і суттєві недоліки, а саме — в деяких випадках необхідність виконання операцій вручну і невисока швидкість відновлення.

Тобто якщо основна система пережила аварію, яка призвела до втрати даних, процес відновлення працездатності за допомогою резервних копій може зайняти кілька годин або навіть днів. І головне,

оскільки резервне копіювання виконується зазвичай не частіше, ніж раз на день, воно не забезпечує наявності найактуальнішої копії даних.

> У свою чергу **Disaster Recovery** — це набір взаємопов'язаних технологій та регламентів, що забезпечує мінімальний час простоїв в разі аварії — зазвичай в межах хвилин або навіть секунд. Тут теж в якийсь момент створюється повна, опорна репліка даних, але потім відбувається постійний запис змін (реплікація).

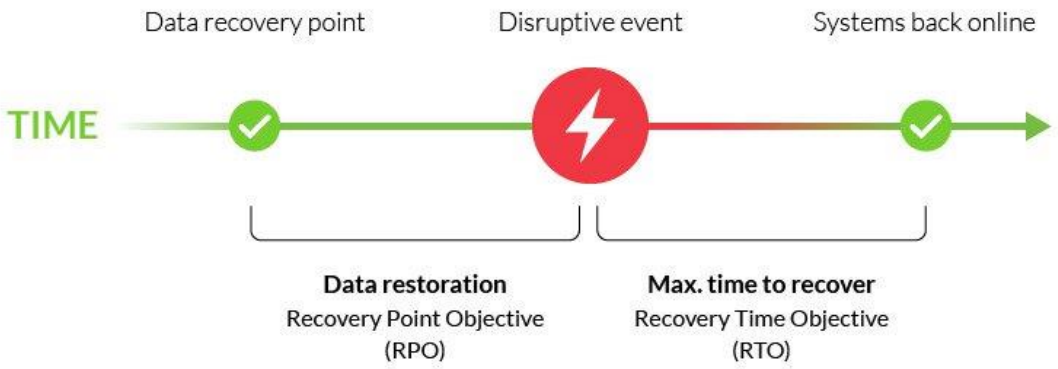
Головна особливість тут у тому, що більшість систем DR використовують метод періодичної або безперервної реплікації: в першому випадку копіювання даних здійснюється з перервою, що обчислюється годинами або хвилинами, у другому — в режимі, близькому до реального часу. Всі дії відбуваються автоматично, а час відновлення скорочується до мінімуму.

Для забезпечення максимальної надійності план аварійного відновлення може передбачати наявність декількох актуальних реплік в різних географічних точках — у власному дата-центрі, хмарі комерційного оператора тощо. Розподілений підхід до організації DR забезпечує ефективне і швидке відновлення не тільки в разі окремих збоїв IT-систем, але навіть при набагато більш серйозних катаклізмах (пожежа, стихійне лихо), що можуть призвести до повного фізичного знищення інфраструктури компанії.

Таке рішення вже називається катострофостійким, і за допомогою звичайного резервного копіювання його не збудувати. Сьогодні катастрофостійкість, як і багато інших сервісів, доступна з хмари, в якості послуги — в цьому випадку мова йде про Disaster Recovery as a Service (DRaaS).

У будь-якому випадку, про який би підхід — backup або DR — не йшлося, є два ключових параметри, які необхідно враховувати при плануванні заходів, пов'язаних з відновленням працездатності IT-інфраструктури після аварій та збоїв. Це **Recovery Point Objective** і **Recovery Time Objective**.

Перший, RPO, позначає час, протягом якого дані можуть бути втрачені без критичних наслідків для роботи організації. Даний параметр, фактично, визначає допустиме «відставання» репліки (або резервної копії) від актуальних даних. Що стосується RTO, то з його допомогою встановлюють час, протягом якого працездатність IT-системи повинна бути відновлена.



RTO і RPO на прикладі

Для кращого розуміння питання проілюструємо все вищесказане прикладом розгляду двох сценаріїв відновлення IT-системи. Отже, припустимо, резервна копія даних в компанії створюється кожен день о 19.00. Уявімо, що о 6.00 наступного дня стався серйозний збій в електроживленні власного дата-центру (одна з найбільш поширених причин аварії).

При цьому в компанії використовується підхід Disaster Recovery і безперервна реплікація. Через хвилину після отримання сигналу про аварію черговий оператор запускає процес відновлення — це можна зробити буквально натисканням однієї кнопки. І ще через чотири хвилини вся інфраструктура відновлена в хмарі оператора.

В даному прикладі RTO — сумарний час відновлення працездатності інфраструктури — склав 4 хвилини, а RPO — допустимий час простою — 5 хвилин (це цілком реальний сценарій для українських організацій, оскільки, наприклад, хмара De Novo забезпечує мінімальний RPO на рівні 5 хвилин). У підсумку о 6.05 все вже працює як раніше, а всі дані актуальні станом на момент аварії — о 6 ранку.

Тепер уявімо, що відновлюватися треба безпосередньо з тієї самої резервної копії, зробленої о 19.00 минулої доби. Почнемо з того, що в даному випадку у компанії є лише дані, а працездатність IT-інфраструктури ще треба буде відновити. Припустимо, це вдалося зробити протягом робочого дня, до 18.00 (сприятливий сценарій). В цьому випадку RTO складе 12 годин з моменту аварії, а дані будуть відновлені з копії, якій вже майже доба — RPO складе 23 години. У кожному індивідуальному випадку часові показники різні, але цей приклад добре ілюструє загальне співвідношення параметрів.

Це зовсім не означає, що якесь із цих рішень, backup або DR, краще, швидше. Кожне з них має свою сферу застосування, і це треба розуміти при виборі підходу для своєї компанії.

Резервне копіювання оптимальне для таких випадків:

- Наявність нормативних або експлуатаційних вимог щодо зберігання даних
- Дані не особливо вимогливі до часу відновлення, який може складати години і дні
- Важливі дані не оновлюються занадто часто

Аварійне відновлення буде найкращим рішенням якщо:

- Для IT-системи час відновлення є критичним фактором
- Зміни важливих даних відбуваються дуже швидко (щохвилини, щосекунди)
- Будь-який простій в роботі компанії призводить до відчутних збитків

Якщо говорити простою мовою, backup потрібен для захисту від логічного руйнування даних в результаті помилок програмного забезпечення або людини (фізичну цілісність забезпечує інфраструктура зберігання). Тому відновлення з backup — це завжди подорож назад у часі, до того моменту, коли дані ще не зруйнувалися. DR призначений, перш за все, для захисту від фізичної втрати даних і швидкого відновлення їх доступності в разі катастрофи (коли інфраструктурні засоби локальної відмовостійкості виявилися безсилі). Тому для DR RPO може (і бажано) бути нульовим (синхронна реплікація).

Backup може використовуватися для вирішення завдання DR, як і DR для завдання backup, але «суміжні» завдання вони вирішують менш ефективно. Тому часто використовується зв'язка **DR + backup** — в цьому випадку досягається **максимальна ефективність**. У той же час не цілком вірно сприймати ці підходи в якості альтернативних технологій — найчастіше вони використовуються спільно, в рамках загальної системи захисту IT-інфраструктури на підприємстві.

Розстановка пріоритетів

Звісно, всі дані важливі, але їх цінність для компанії може істотно відрізнятися. Є інформація, втрату якої, взагалі-то, ніхто і не помітить, але у будь-якої компанії є і особливо критичні дані, втрата яких загрожує серйозними наслідками — аж до краху бізнесу. Мільйонні збитки за секунду простою, про які часто говорять міжнародні аналітичні агентства — це ознака дуже великих світових компаній. Але навіть в нашій країні відсутність доступу до IT-інфраструктури протягом години-двох вже може дорого обійтися.

Типовий приклад — збій сервера з бухгалтерськими програмами під час формування квартального / річного звіту. Прострочення подачі документів може вилитися у великі штрафи. Насправді, правильно оцінити втрати від простою серверів і недоступності даних — непросте завдання, але, найчастіше, будь-який досвідчений IT-директор інтуїтивно розуміє, яка інформація є найбільш цінною і актуальною.

Звичайно, з технічної точки зору, ідеальним було б забезпечити Disaster Recovery відразу для всієї IT-інфраструктури організації, але це не завжди виправдано з економічної точки зору. Зрозуміло, що більш складний і комплексний підхід DR буде дорожче звичайного створення і зберігання резервних копій. У підсумку **варто розділити всі дані за рівнями пріоритету і важливості** — це дасть змогу істотно заощадити на забезпеченні відмовостійкості інфраструктури.

Для даних, що не надто критичні до часу відновлення — наприклад, для архівних, може застосовуватися відносно недорогий та повільний backup, а там, де потрібна мінімізація простою, скажімо, в продуктивних системах — використовується істотно більш швидкий DR.

На практиці рівнів може бути істотно більше двох…

Завантажити повну версію