

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Метод резервного копіювання даних для малих і середніх
підприємств на основі рішення Veeam»

на здобуття освітнього ступеня магістра

зі спеціальності 126 Інформаційні системи та технології

освітньо-професійної програми

*Кваліфікаційна робота містить результати власних досліджень.
Використання ідей, результатів і текстів інших авторів мають посилання
на відповідне джерело*

(підпис)

(Ім'я, Прізвище здобувача)

Виконав:
здобувач вищої освіти
група ІСДМ-61

Сінгаєвський Максим

Керівник:
науковий ступінь,
вчене звання

Олег Сеньков
к.т.н., доцент

Рецензент:
науковий ступінь,
вчене звання

Ім'я, ПРІЗВИЩЕ

Київ-2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій

Кафедра Інформаційних систем та технологій

Ступінь вищої освіти – «Магістр»

Спеціальність - 126 - Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ

Завідувач кафедри ІСТ

_____ Сторчак К.П.

“ ____ ” _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Сінгаєвському Максиму Миколайовичу

(прізвище, ім'я, по батькові)

1. Тема роботи: «Метод резервного копіювання даних для малих і середніх підприємств на основі рішення Veeam»

Керівник роботи: Сеньков Олег Вікторович к.т.н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від «15» жовтня 2024 року
№320.

2. Строк подання студентом роботи: 27 грудня 2024 року.

3. Вихідні данні до кваліфікаційної роботи:

Основні методи резервного копіювання.

Огляд продукту Veeam Backup & Replication.

науково-технічна література з питань, пов'язаних з резервним копіювання

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз існуючих підходів до резервного копіювання даних на малих і середніх підприємствах.
2. Оцінка особливості використання Veeam для створення резервних копій і відновлення даних.
3. Розглянути можливості оптимізації стратегії для забезпечення мінімальних витрат при максимальній надійності.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання: 15 жовтня 2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	15.10 – 19.10.24	ВИКОНАНО
2	Дослідження методів резервного копіювання	20.10 – 13.11.24	ВИКОНАНО
3	Аналіз програм для резервного копіювання	28.10 – 02.11.24	ВИКОНАНО
4	Дослідження Veeam Backup & Replication	02.11 – 09.11.24	ВИКОНАНО
5	Дослідження особливостей роботи Veeam на малих та середніх підприємствах	10.11 – 11.11.24	ВИКОНАНО
7	Оформлення роботи: вступ, висновки, реферат	07.11 – 20.12.24	ВИКОНАНО
8	Розробка демонстраційних матеріалів	19.12 – 25.12.24	ВИКОНАНО

Здобувач вищої освіти

(підпис)

Максим Сінгаєвський
(Ім'я, ПРІЗВИЩЕ)

Керівник роботи
кваліфікаційної роботи

(підпис)

Олег Сеньков
(Ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 95 стор., 29 рис., 30 джерел.

Мета роботи – розробити стратегію резервного копіювання для малих і середніх підприємств з використанням рішення Veeam, що дозволить забезпечити високу надійність збереження даних, швидке відновлення та мінімізацію ризиків втрати інформації.

Об'єкт дослідження – процеси резервного копіювання на основі рішення Veeam.

Предмет дослідження – процеси резервного копіювання та відновлення даних на малих і середніх підприємствах за допомогою програмного рішення Veeam. Це включає вивчення механізмів резервного копіювання, різноманітних типів резервних копій (повні, інкрементальні, диференціальні), а також методи та інструменти для забезпечення надійності, швидкості відновлення та збереження безпеки даних в умовах обмежених ресурсів МСП.

Короткий зміст роботи: Досліджено основні принципи та підходи до резервного копіювання даних для малих і середніх підприємств, описується важливість правильного вибору стратегії резервного копіювання, а також відбувається знайомство з основними типами резервних копій і технологіями, які використовуються для їх створення. Детально аналізується програмне забезпечення Veeam, його можливості та функціональність, особливості інтеграції з іншими ІТ-системами. Розглядаються переваги та недоліки Veeam як рішення для резервного копіювання, а також основні інструменти для автоматизації процесу резервного копіювання та відновлення даних.

КЛЮЧОВІ СЛОВА: РЕЗЕРВНА КОПІЯ, VEEAM BACKUP & REPLICATION, BACKUP, РЕПЛІКАЦІЯ, ВІРТУАЛЬНА МАШИНА, VM, ОБРАЗ

ABSTRACT

Text part of the master`s qualification work: 95 pages, 29 figures, 30 sources.

The purpose of the work is to develop a backup strategy for small and medium-sized enterprises using the Veeam solution, which will ensure high reliability of data storage, fast recovery and minimisation of information loss risks.

Object of research - backup processes based on the Veeam solution.

The subject of the study is the processes of data backup and recovery at small and medium-sized enterprises using the Veeam software solution. This includes the study of backup mechanisms, various types of backups (full, incremental, differential), as well as methods and tools to ensure reliability, speed of recovery and preservation of data security in the context of limited SME resources.

Summary of the work: The basic principles and approaches to data backup for small and medium-sized enterprises are explored, the importance of choosing the right backup strategy is described, and the main types of backups and technologies used to create them are introduced. The Veeam software, its capabilities and functionality, and features of integration with other IT systems are analysed in detail. The advantages and disadvantages of Veeam as a backup solution, as well as the main tools for automating the process of data backup and recovery are considered.

KEYWORDS: BACKUP, VEEAM BACKUP & REPLICATION, BACKUP, REPLICATION, VIRTUAL MACHINE, VM, IMAGE

ЗМІСТ

ВСТУП.....	9
РОЗДІЛ 1. ВВЕДЕННЯ В РЕЗЕРВНЕ КОПЮВАННЯ.....	10
1.1. Захист від апаратних збоїв	10
1.2. Захист від випадкового видалення	11
1.3. Документування.....	15
1.4. Основні утиліти для резервного копіювання	17
РОЗДІЛ 2. VEEAM: ОПИС ПРОДУКТУ	46
2.1. Відновлення за допомогою Veeam	49
2.2. Реплікація у Veeam	63
2.3. Впровадження Veeam в малі та середні підприємства	79
2.4. Переваги використання Veeam у МСП.....	82
РОЗДІЛ 3. ЗАСТОСУВАННЯ VEEAM НА ПІДПРИЄМСТВІ	84
3.1. Підготовка середовища	84
3.2. Конфігурація нового завдання	85
3.3. Успішне створення резервної копії.....	90
ВИСНОВКИ	91
ПЕРЕЛІК ПОСИЛАНЬ	93
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)	

ВСТУП

Актуальність теми: У сучасному цифровому світі малим і середнім підприємствам (МСП) необхідно швидко адаптувати свої інформаційні системи для забезпечення безпеки та доступності даних. Враховуючи обмежені ресурси, МСП часто стикаються з проблемою ефективного управління даними та збереження їх у разі аварій чи технічних збоїв. Однією з основних складових ІТ-стратегії є надійне резервне копіювання даних, яке дозволяє зберігати цілісність та доступність важливої інформації. У цьому контексті рішення Veeam, яке забезпечує ефективне та гнучке резервне копіювання, стає важливим інструментом для МСП. Актуальність теми полягає в тому, що у зв'язку з розвитком цифрових технологій та збільшенням обсягів даних, підприємства потребують сучасних і доступних методів резервного копіювання, які дозволяють знизити ризики втрати даних, забезпечити швидке відновлення в разі збоїв та мінімізувати витрати на підтримку ІТ-інфраструктури. Рішення Veeam є одним із найпопулярніших на ринку та надає прості у впровадженні, але потужні інструменти для резервного копіювання даних.

Метою роботи є розробка стратегії резервного копіювання для малих і середніх підприємств на основі рішення Veeam, яка дозволить забезпечити ефективне збереження даних, мінімізацію ризиків втрати інформації та оптимізацію витрат на зберігання і відновлення даних у разі їх втрати.

Об'єкт дослідження - процеси резервного копіювання та відновлення даних у малих і середніх підприємствах, зокрема використання рішення Veeam для резервного копіювання та відновлення даних.

Предметом дослідження є інструменти та методи резервного копіювання даних з використанням рішення Veeam для малих і середніх підприємств. Це включає оцінку та вибір типів резервних копій (повні, інкрементальні, диференціальні), налаштування та конфігурацію програмного забезпечення, а також розробку стратегії, що дозволяє оптимізувати використання ресурсів і забезпечити безперервність бізнесу.

Наукова новизна роботи полягає у в глибокому дослідженні та адаптації рішення Veeam для малих і середніх підприємств (МСП), що дозволяє розробити нову стратегію резервного копіювання даних, оптимізовану під умови обмежених ресурсів підприємств. У роботі здійснено детальний аналіз можливостей Veeam щодо автоматизації резервного копіювання, відновлення даних та інтеграції з існуючими ІТ-інфраструктурами МСП.

Апробація результатів магістерської роботи:

1. Сінгаєвський М.М. «Переваги використання блокчейну для резервного копіювання». Тези доповіді на VII Всеукраїнській студентській науковій конференції «Діджиталізація науки як виклик сьогодення» (25.10.2024, м. Полтава, Україна).

2. Сінгаєвський М.М. «Резервне копіювання та аварійне відновлення даних для малого та середнього бізнесу». Тези доповіді на V Міжнародній науковій конференції «Інновації та науковий потенціал світу» (25.10.2024; м. Умань, Україна).

1. ВВЕДЕННЯ В РЕЗЕРВНЕ КОПЮВАННЯ

В епоху цифрових технологій ми зберігаємо на своїх пристроях величезну кількість важливої інформації - фотографії, відео, робочі документи, особисті записи. Однак багато людей все ще недооцінюють ризики втрати своїх даних. Незалежно від того, чи це сталося через збій обладнання, випадкове видалення, кібератаки або стихійні лиха, втрата цінних файлів може мати руйнівні наслідки. Саме тут на допомогу приходять резервні копії.

Регулярне створення резервних копій даних - одна з найпростіших, але дуже важливих практик, яка гарантує, що ваша інформація залишиться в безпеці та буде доступною, коли це знадобиться. Це мережа безпеки, яка захищає вас від несподіванок, дарує душевний спокій і забезпечує безперервність бізнесу, особисту безпеку та цифрову стійкість.

Але чому саме так важливо створювати резервні копії даних? В цьому потрібно розібратись докладніше.

Причини втрати даних

1.1. Захист від апаратних збоїв

Однією з найпоширеніших причин втрати даних є вихід з ладу обладнання. Незалежно від того, наскільки просунуті або дорогі ваші пристрої, вони не застраховані від таких проблем:

- Збій жорсткого диска: Механічні накопичувачі можуть вийти з ладу через зношування, перегрів або навіть стрибок напруги.
- Збої в роботі твердотільних накопичувачів: Хоча твердотільні накопичувачі (SSD) надійніші за традиційні жорсткі диски, вони не є невразливими і можуть вийти з ладу без попередження.

- Пошкодження даних: Файли можуть бути пошкоджені через помилки на диску, пошкоджені сектори або невдалі оновлення.

Поломка обладнання - це не просто незручність, це може означати безповоротну втрату важливих даних, особливо якщо у вас немає резервної копії.

Регулярно створюючи резервні копії файлів, ви гарантуєте, що навіть якщо ваш основний пристрій вийде з ладу, ви зможете швидко і легко відновити свої дані. Ризик втрати цінних робіт, фотографій чи документів значно зменшується, якщо ви знаєте, що у вас є свіжа резервна копія.

1.2. Захист від випадкового видалення

З більшістю людей таке траплялося - хтось випадково видаляв файл або папку, які здавалися, більше не потрібні, а через мить усвідомлювали, що вони насправді були життєво необхідні. Незалежно від того, чи це особистий файл, чи проект на роботі, чи важливе вкладення в електронному листі, емоційна паніка від усвідомлення того, що щось було видалено, може бути приголомшливою.

Але хороша новина полягає в тому, що резервні копії - це захист від збоїв. Вони дозволяють відновити дані, втрачені через людську помилку. Насправді, багато хмарних сервісів, таких як Google Drive або iCloud, навіть пропонують історію версій, тобто ви можете відновити попередні версії документа, якщо ви внесли зміни, які не планували.

Однак без резервної копії видалені дані можуть бути втрачені назавжди, особливо якщо їх неможливо відновити за допомогою вбудованих засобів відновлення пристрою. Наявність резервних копій гарантує, що ви зможете виправити помилки та уникнути панічних рішень, таких як перезапис важливих файлів або використання неперевірених методів відновлення.

2. Зменшити ризик кібератак

Останніми роками кібератаки стають дедалі більшою загрозою як для приватних осіб, так і для бізнесу. Деякі з найнебезпечніших типів атак включають: Програми-вимагачі: під час цих атак хакери блокують або шифрують дані і вимагають викуп в обмін на ключ для розшифрування. Якщо у вас немає резервної копії, ви можете бути змушені заплатити викуп або повністю втратити свої дані. Шкідливе програмне забезпечення: Віруси або шкідливі програми можуть пошкодити або викрасти файли, завдавши їм незворотної шкоди.

У випадку атаки зловмисників наявність актуальних резервних копій може врятувати життя. Навіть якщо файли зашифровані або викрадені, можна просто відновити їх з резервної копії, уникнувши необхідності платити зловмиснику. Регулярне резервне копіювання допомагає захиститися від широкого спектру кіберзагроз, гарантуючи, що навіть якщо зловмисник отримає доступ до вашої системи, ваші дані залишаться в безпеці.

Безперервність бізнесу та аварійне відновлення. Для бізнесу ризики втрати даних набагато вищі. Втрата критично важливих бізнес-даних - будь то інформація про клієнтів, фінансова звітність або інтелектуальна власність - може призвести до значних фінансових втрат, репутаційних збитків та юридичних наслідків.

Дослідження показують, що багато малих підприємств, які зазнають значної втрати даних без резервного копіювання, ніколи не відновлюються, а 60% компаній припиняють свою діяльність протягом шести місяців після великої втрати даних.

Системи резервного копіювання є ключовою частиною планів безперервності бізнесу та аварійного відновлення. Вони допомагають компаніям швидко відновити свою діяльність після системного збою, кібератаки або стихійного лиха. Надійна стратегія резервного копіювання також необхідна для дотримання

галузових норм, які вимагають від компаній зберігати та захищати конфіденційні дані.

Регулярно створюючи резервні копії даних у захищених місцях за межами офісу, компанії гарантують, що зможуть відновити роботу з мінімальним часом простою, зменшуючи ризик значних фінансових втрат.

Захист від стихійних лих. Хоча люди часто зосереджуємося на технічних проблемах, таких як збої в роботі обладнання або кіберзагрози, стихійні лиха, такі як пожежі, повені, землетруси або торнадо, також можуть призвести до втрати даних. Фізичні пошкодження пристроїв, офісних будівель або будинків можуть ускладнити, а то й унеможливити відновлення.

Резервне копіювання за межами офісу- чи то в хмарі, чи у фізичному місці за межами основного робочого простору - допомагає зменшити ці ризики. Навіть якщо локальне обладнання буде пошкоджено без можливості відновлення, дані залишаться недоторканими і доступними завдяки резервній копії.

Хмарні сервіси, наприклад, зберігають дані в захищених центрах обробки даних, розташованих у різних географічних регіонах. У разі локальної катастрофи файли все одно можна буде відновити з іншого місця, що гарантує, їх безпеку.

Ефективна система резервного копіювання та відновлення даних є критично важливою для функціонування компанії будь-якого масштабу. Однак, в умовах обмеженого бюджету, ІТ-відділи часто стикаються з труднощами у фінансуванні таких систем. Як правило, на впровадження та підтримку резервного копіювання не виділяються достатні кошти, що може негативно вплинути на безпеку даних організації. Жодна втрата даних не є прийнятною. Незалежно від того, чи це електронна таблиця, яку створила одна людина, чи клієнтська база даних, що представляє години або дні рахунків-фактур і зусиль сотень людей.

Щоб визначити, які файли слід включити до резервних копій, запросіть на обід найбільш скептично налаштованих технічних спеціалістів вашої компанії. Краще запросити кількох таких фахівців разом. Попросіть їх уявити можливі сценарії, від яких потрібно захистити систему. Ці сценарії допоможуть вам зрозуміти, що має бути включено до резервних копій, а також спланувати сам процес. Задайте їм питання: «Які найгірші ситуації можуть призвести до втрати даних?» Ось кілька можливих відповідей:

1. Вся система загоряється і повністю знищується, залишаючи лише непізнану масу розплавленого металу і згорілого пластику.
2. Оскільки ця машина була критично важливою, ви створили її резервну копію на іншому вузлі поруч. І, звісно, цей вузол також згоряє разом із основною системою.
3. У вас є централізований сервер, який керує усіма резервними копіями та веде облік розташування томів резервних копій. Сервер вибухає, і він знаходиться поруч з «резервним» сервером, через що сильний жар руйнує й цю систему.
4. Ланцюгова реакція продовжується, виводячи з ладу ваші сервери DHCP, Active Directory, основний сервер NIS, сервери домашніх каталогів NFS та CIFS, а також сервер бази даних, де зберігається інвентар резервних томів і їх розташування. На цьому комп'ютері також зберігається телефонна база даних із усіма договорами на обслуговування, номерами постачальників та ескалаційними процедурами.
5. Ви ще не вивчили номер вашого нового постачальника послуг, тому він приклеєний до стіни поруч із сервером резервного копіювання. І, звісно, ви розумієте, що полум'я знищило цей папірець до невпізнання.
6. Полум'я активує спринклерну систему, і вода заливає всі резервні томи.

Такий підхід дозволить чітко визначити, що слід врахувати при створенні стратегії резервного копіювання для захисту від найгірших сценаріїв.

Тут ви переходите до відновлення. Ви перевірили всі томи і знайшли той, який потрібен для відновлення резервної копії сервера (це значно складніше, ніж здається!). Завдяки вашій майстерності, кмітливості та значній допомозі технічної підтримки відновлення все ж вдалося здійснити. І ось, система знову працює. Але скільки дисків було в системах, що вибухнули? Якими моделями вони були? Як були розбиті на розділи? Чи не були деякі з них об'єднані в більші томи або налаштовані як дзеркальне відображення? Де зберігається вся ця інформація? Якими були розміри дисків чи файлових систем?

Потрібно переконатись, що у вас буде доступ до критично важливої інформації в разі катастрофи: Резервні копії для резервних копій. Багато організацій почали централізувати управління своїми резервними копіями.

Однак, коли вся інформація про резервні копії централізується, виникає єдина точка відмови для всього процесу резервного копіювання. Відновити сервер резервного копіювання неможливо, бо немає доступу до бази даних резервних копій, а базу даних не можна відновити без самого сервера. Відновлення цього сервера має бути першим кроком у випадку будь-якої мультисистемної аварії.

Що стосується інвентаризації носіїв, не можна недооцінювати важливість її друкованої версії, збереженої поза офісом. Такий документ може стати порятунком у критичній ситуації. Враховуючи наявність єдиної точки відмови, відновлення сервера резервного копіювання має бути найбільш простим і добре задокументованим процесом відновлення. Можливо, має сенс створити спеціальні резервні копії цих даних, наприклад, за допомогою tar, ntbackup або rsync, щоб ще більше спростити їх відновлення в разі катастрофи.

1.3. Документування

Документування! Існує безліч причин для належного документування таких процесів, і відновлення після катастрофи — одна з них. Хороша документація є важливою частиною плану резервного копіювання. Вона повинна регулярно оновлюватися і бути легкодоступною. Ніхто не повинен опинятися в ситуації, коли

каже: «Я давно не налаштовував NIS/AD/NFS з нуля. Як це зробити знову?». Найкращий підхід — автоматизувати процес створення нових серверів. Якщо операційна система дозволяє це, витратьте час на написання скриптів, які автоматично встановлюють необхідні служби та налаштовують їх для вашого середовища. Об'єднайте їх у набір інструментів, що запускатиметься щоразу при створенні нового сервера. А ще краще, перевірте, чи є у постачальника операційної системи інструменти для автоматизації встановлення серверів, такі як Jumpstart від Sun, Ignite-UX від HP, Linux Kickstart або функції клонування Mac OS. Найнадійніший спосіб захисту від більшості видів втрат — це коли людина, відповідальна за резервне копіювання та відновлення, добре знайома з системами, які вона захищає. Якщо певний сервер вийде з ладу, ви повинні негайно знати, що на ньому розміщена база даних Oracle або SQL Server, і що для цих томів необхідно виконати відновлення.

Перш ніж обговорювати, чи варто робити резервну копію частини або всієї системи, давайте розглянемо поширену практику використання списків включення та чому вона може бути небезпечною. Також розглянемо кілька способів уникнення застосування списків включення.

Можна налаштувати систему резервного копіювання таким чином, щоб вона створювала резервні копії всього, за винятком елементів, зазначених у списку винятків, наприклад:

-для серверів Unix, Linux та Mac OS

-Include: * Exclude: /tmp, /junk1, /jun

Для Windows використовується:

- Include: * Exclude: *.tmp, *Temporary Internet Files*, ~*.*, *

Можна вказати системі резервного копіювання створювати резервні копії, наприклад, того, що входить до списку включення:

Для операційних систем Unix, Linux і Mac OS:

-Include: /data1, /data2, /data3

Для Windows:

Include: D:\, E:\

Однак, якщо утиліта для резервного копіювання не підтримує автоматичне виявлення дисків або файлових систем, потрібно докласти трохи зусиль, щоб створити резервну копію. Як скласти список систем, дисків, файлових систем і баз даних для резервного копіювання? Потрібно переглянути такі файли, як /etc/vfstab або реєстр Windows, і виокремити список дисків або файлових систем для резервного копіювання. Потім можна використовувати списки винятків, щоб виключити диски або файлові системи, які не потрібно резервувати.

1.4. Основні утиліти резервного копіювання та відновлення

Базові програми резервного копіювання — це програми резервного копіювання, на яких базуються всі некомерційні системи резервного копіювання. Вони виконують важливе завдання копіювання даних з одного місця в інше і зазвичай копіюють їх в інший формат (наприклад, Tar). Жоден із цих інструментів не має вбудованих функцій планування, а також не може створити каталог для відстеження резервних копій, які вони створюють. Якщо потрібно виконати ці завдання, знадобиться якась програма для планування. Це може бути простий пакетний сценарій. Завдання в системі Windows, сценарій оболонки та запис cron у системі Unix або Mac OS або одна зі складних програм з відкритим кодом, які обговорюються далі в цій книзі. Базові програми резервного копіювання включають рідні версії dump, cpio, tar і dd для систем Unix, ntbackup і відновлення системи для систем Windows, те ж саме для систем Mac OS, а також доступні версії GNU tar, cpio і rsync для всіх цих платформ.

Сріо може бути дуже потужним інструментом резервного копіювання для Unix- подібних систем. Найважливішою його особливістю є можливість приймати список файлів для резервного копіювання зі стандартного введення. Це єдина рідна утиліта, яка може це зробити. Цю функцію можна поєднати з використанням Touch Files і команди Find для створення додаткових резервних копій.

Однак, на відміну від дампа, сріо не може:

1. Виконувати інкрементне резервне копіювання без використання сенсорних файлів і пошуку.
2. Краще залишити atime та ctime без змін після створення резервної копії.

Якщо архіватор сріо такий потужний, чому tar популярніший? Однією з причин цього є те, що базові операції tar набагато простіші (і більш стандартизовані), ніж ті самі операції в сріо. Наприклад, кожна версія tar підтримує tar cf device і tar xf device, тоді як сріо іноді підтримує параметри -I та -O, а іноді ні. Якщо скласти всі параметри сріо, доступні в усіх різних версіях, то її можна отримати більше 40. Є також деякі аргументи, які використовують ту саму букву, але мають абсолютно різні функції в різних версіях Unix. Іншою причиною більшої популярності tar є розвиток GNU. Він поєднує потужність сріо з простотою використання tar.

dd. Команда dd не є резервною командою, якою користується більшість людей. Це команда дуже низького рівня, призначена для копіювання бітів інформації з одного місця в інше. Вона не має жодних знань про структуру даних, які вона копіює, і це їй не потрібно. Тому, на відміну від dump, tar і сріо, вона не використовується для копіювання групи файлів до резервного тому. Вона може копіювати окремий файл, частину файлу, необроблений розділ або частину необробленого розділу, і навіть може копіювати дані зі стандартного введення в стандартний вихід, змінюючи їх на шляху. Знову ж таки, хоча вона може скопіювати файл, вона не знає назви файлу чи вмісту, коли це робить. Вона просто

копіює байти, які знаходяться в тому місці, з якого їй сказали копіювати. Потім поміщає ці байти туди, куди їй сказали.

Хоча `dd` досить проста, вона надзвичайно гнучка. Вона може копіювати файли або розділи незалежно від формату. Може перекладати дані між двома різними платформами, наприклад, з EBCDIC на ASCII або з великого порядку байтів на маленький порядок байтів. Прекрасним прикладом гнучкості `dd` є сценарій резервного копіювання Oracle. Дані Oracle можуть зберігатися у файлах у файловій системі або на необроблених розділах диска. Оскільки сценарій не міг передбачити, яку конфігурацію використовуватиме кожен DBA, він використовував `dd`, оскільки міг копіювати як файли, так і необроблені розділи. Це дозволяє адміністратору баз даних використовувати конфігурацію, яка є найбільш доцільною для його програми, а сценарій автоматично зберігає обидві конфігурації. Він навіть створює резервні копії змішаної конфігурації, де частина даних міститься у файлах, а частина – у необроблених розділах. Саме такий тип гнучкості пропонує вам `dd`.

Дамп і відновлення. Дамп і відновлення вважаються багатьма найпотужнішими інструментами в наборі інструментів резервного копіювання Unix. Особливості дампа та відновлення включають можливість резервного копіювання файлів без зміни часу доступу та можливість використання міні-оболонки для інтерактивного вибору файлів для відновлення перед початком. Дамп і відновлення є відносно складними командами з простим інтерфейсом, основні параметри яких однакові в більшості систем Unix. Дамп і відновлення дуже суперечливі, і існує багато суперечок щодо того, чи можна належним чином створити резервну копію активної файлової системи.

Tar. Найкращою особливістю Tar є його широке застосування, головним чином завдяки простоті використання. Майже кожен пристрій знає, як читати том tar. Якщо це файл tar на диску або навіть стиснутий файл tar, такі програми, як WinZip, можуть автоматично розпакувати його та прочитати вміст. (WinZip не може відкрити архів `crio`.) Крім того, він набагато легше переноситься між платформами

Unix, ніж `dump` або `cpio`. Якщо потрібно зробити швидку резервну копію каталогу або набору файлів, важко перевершити простоту використання `tar`. Крім усього іншого, якщо потрібно зробити додаткові резервні копії, щоб зекономити час краще звернути увагу на використовувати GNU `tar` або `cpio`.

Asr (Apple System Restore) — утиліта для обробки зображень, доступна лише в системах Mac OS. Він в основному використовується як інструмент для клонування великих обсягів даних, подібно до того, як користувачі Windows використовують утиліту Ghost. Це утиліта на основі зображень, яку можна використовувати для копіювання безпосередньо з одного жорсткого диска на інший або створення образу диска жорсткого диска, подібного до файлу ISO в інших операційних системах. Такий файл має розширення `.dmg`.

Резервне копіювання та відновлення Windows Backup.Windows Backup (відомий також як Backup and Restore) — це вбудований інструмент для створення резервних копій у операційних системах Windows. Він дозволяє створювати резервні копії файлів, папок, системних образів та налаштувань, щоб у разі збою системи або втрати даних можна було відновити важливу інформацію. Windows Backup дозволяє створювати резервні копії окремих файлів і папок. Користувач може вибирати, які файли або папки важливі для збереження, чи дозволити Windows автоматично вибирати файли, такі як документи, зображення, відео, музика тощо. Крім резервного копіювання файлів, Windows Backup дозволяє створити системний образ — це точна копія операційної системи разом з усіма налаштуваннями, програмами та даними. Системний образ необхідний для повного відновлення комп'ютера у випадку серйозних проблем, таких як злам операційної системи або жорсткий диск. Windows Backup дозволяє налаштувати автоматичне створення резервних копій через певні інтервали (наприклад, щодня, щотижня або щомісяця). Це дозволяє користувачам не турбуватися про регулярне створення копій важливих файлів — система робить це автоматично. Резервні копії можна зберігати на різних носіях. Таких як: зовнішні жорсткі диски, мережеві ресурси,

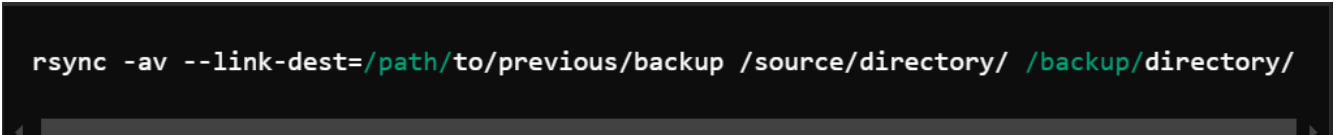
локальні диски. А для захисту даних можна використовувати функцію шифрування. Windows Backup надає можливість додатково захистити резервні копії паролем, що допомагає запобігти несанкціонованому доступу до них. Хоча Windows Backup є основним інструментом для резервного копіювання у Windows 7 та новіших версіях, він також має зворотну сумісність. Наприклад, можна відновлювати резервні копії, зроблені на старіших версіях Windows, в нових операційних системах.

Rsync інструмент для резервного копіювання в Unix-подібних системах. Rsync — це один з найпопулярніших і найпотужніших інструментів для резервного копіювання, синхронізації та переміщення файлів в операційних системах Linux і Unix. Завдяки своїй швидкості, гнучкості та широким можливостям налаштування, rsync став стандартом для адміністраторів систем і користувачів, які шукають ефективний спосіб організації зберігання даних і резервного копіювання.

rsync (скорочення від remote synchronization) — це інструмент для синхронізації файлів і директорій між двома місцями на локальному або віддаленому комп'ютері. Зазначу, що rsync працює на основі алгоритму, який дозволяє копіювати лише змінені файли або їх частини, що робить процес резервного копіювання та синхронізації набагато швидшим і економічнішим у плані використання ресурсів. rsync підтримує роботу як локально (на одному комп'ютері), так і по мережі, що дозволяє синхронізувати файли між кількома машинами через SSH, FTP, rsyncd (rsync-сервер) або інші протоколи.

Rsync використовує метод інкрементного копіювання, що дозволяє передавати тільки ті частини файлів, які змінилися, замість копіювання всього файлу. Початкове копіювання: Під час першого запуску rsync копіює всі файли з джерела в цільову директорію. Усі файли та директорії будуть передані цілком. Наступні копіювання (інкрементні): При наступних запусках rsync порівнює файли в джерелі та цілі. Він перевіряє: чи змінився вміст файлу (розмір, дата модифікації), чи додано нові файли або директорії. Якщо файл не змінювався, rsync не копіює його знову, а

якщо змінився — передає лише змінені частини файлу, використовуючи алгоритм диференціації змін (диференціація на рівні блоків). `rsync` працює так, що передає тільки різницю (зміни), а не весь файл. Це дозволяє значно заощаджувати ресурси, особливо для великих файлів. Якщо файл було видалено в джерелі, опція `--delete` дозволить видалити його з цільової директорії. Використання часу модифікації та розміру файлів: При порівнянні файлів `rsync` використовує час останньої модифікації та розмір файлу, щоб визначити, чи змінився файл. Це найбільш стандартний метод порівняння. Алгоритм диференціації: Якщо файли великі, `rsync` використовує складніший алгоритм для порівняння їх вмісту. Алгоритм порівнює блоки даних в файлі, і передає лише зміни в цих блоках. Це дозволяє передавати мінімальну кількість даних, навіть якщо файл значно змінився. Опція `--link-dest` для інкрементних резервних копій: Для створення справжніх інкрементних резервних копій, де зберігаються тільки зміни, використовується опція `--link-dest`. Вона дозволяє створювати нову копію даних, але зберігати старі файли як символічні посилання (якщо вони не змінилися).



```
rsync -av --link-dest=/path/to/previous/backup /source/directory/ /backup/directory/
```

Рисунок 1.1 створення копії даних з заміною даних

Виключення файлів: Використання опції `--exclude` дозволяє виключати певні файли або директорії з інкрементного копіювання, щоб не передавати непотрібні або тимчасові файли.

Якщо `rsync` використовується для синхронізації файлів між двома комп'ютерами, передача може здійснюватися через SSH, що забезпечує зашифроване з'єднання між комп'ютерами.



```
rsync -av /source/directory/ /destination/directory/
```

Рисунок 2.2 Застосування `rsync` для копіювання з однієї директорії в іншу

Резервне копіювання на Mac OS за допомогою Time Machine — це вбудований інструмент резервного копіювання в операційній системі macOS, який дозволяє автоматично створювати резервні копії всіх даних на комп'ютері, включаючи файли, налаштування, програми та навіть операційну систему. Це одне з найбільш зручних і інтуїтивно зрозумілих рішень для резервного копіювання, яке є частиною стандартного комплекту macOS і не вимагає додаткових налаштувань чи сторонніх програм. Основною особливістю Time Machine є його здатність здійснювати інкрементне копіювання. Це означає, що після створення початкової повної резервної копії, програма буде зберігати лише зміни, що відбулися в файлах після останнього копіювання. Наприклад, якщо ви створили новий документ чи внесли зміни до існуючого файлу, Time Machine збережуть лише ці зміни, а не копіюють усі файли знову. Такий підхід значно економить місце на зовнішньому диску, оскільки зберігаються тільки зміни, а не цілі файли щоразу. Кожного разу, коли Time Machine виконує резервне копіювання, він збирає дані з вашого комп'ютера та зберігає їх на зовнішньому жорсткому диску або на мережевому сховищі (NAS). Резервні копії створюються автоматично, без необхідності втручання користувача, що робить цей процес безперервним і не порушує робочий процес. Копії робляться щогодини, а також кожен день і кожен тиждень, залежно від обсягу даних і доступного місця на диску. Коли резервне сховище заповнюється, Time Machine автоматично видаляє старі копії, щоб звільнити місце для нових.

Одна з основних переваг Time Machine — це можливість відновлення даних у випадку втрати. Якщо ви випадково видалили файл або папку, або ж зазнали збою системи, Time Machine дозволяє легко відновити не тільки окремі файли, а й цілу систему, програми та налаштування. Вся інформація зберігається у вигляді інтерфейсу, який дозволяє швидко переглядати файли за певними датами і вибирати потрібні для відновлення. Таким чином, ви можете повернутися до

конкретної версії файлу або навіть відновити стару версію всієї операційної системи. Ще однією важливою функцією Time Machine є його здатність до відновлення після повної втрати даних, що робить його дуже корисним у разі апаратних збоїв чи необхідності перевстановлення macOS. Якщо ваш Mac вийшов з ладу, або ви хочете перенести всі дані на новий комп'ютер, Time Machine дозволяє швидко відновити всі файли, програми та налаштування на нову машину, що значно спрощує цей процес. Щоб почати використовувати Time Machine, достатньо підключити зовнішній диск або налаштувати мережеве сховище, і програма сама почне робити резервні копії. Вона може працювати в фоновому режимі, не заважаючи користувачеві, що робить цей процес абсолютно безперервним. Для цього Time Machine використовує стандартний графічний інтерфейс macOS, що дозволяє зручно налаштувати резервне копіювання і відновлення без необхідності складних маніпуляцій. Окрім цього, в програмі є можливість вибору конкретних файлів чи папок для резервного копіювання, а також виключення непотрібних даних за допомогою спеціальних налаштувань.

Time Machine — це не тільки зручний інструмент для збереження даних, але й ефективний засіб для повного відновлення системи. Якщо Mac не працює належним чином або його потрібно відновити після серйозного збої, можна скористатися функцією відновлення Time Machine через режим відновлення macOS. Це дозволяє повністю відновити систему, а також налаштування та всі додатки, не потребуючи повторного встановлення програм або переналаштування системи. Крім того, Time Machine працює дуже ефективно навіть для користувачів, які не мають технічного досвіду. Він має простий інтерфейс, який дозволяє буквально «клікнути і забути». Після налаштування користувачі можуть забути про процес резервного копіювання, оскільки він здійснюється автоматично, а програма лише нагадує про необхідність підключення резервного носія, якщо це потрібно. Однак Time Machine не є ідеальним для всіх сценаріїв. Одним із недоліків є обмеження по обсягу сховища, яке потрібно підключити до комп'ютера для створення резервних копій. Зазвичай це має бути зовнішній жорсткий диск або

мережевий носій, що здатний зберігати великий обсяг даних. Оскільки резервне копіювання зазвичай займає значний обсяг пам'яті, можливо, доведеться купити досить великий диск, щоб забезпечити ефективне резервне копіювання на довгий період. Загалом, Time Machine — це потужне, просте у використанні та надійне рішення для резервного копіювання даних на macOS. Всі його переваги, такі як автоматичне інкрементне копіювання, можливість відновлення файлів і системи, а також інтуїтивно зрозумілий інтерфейс, роблять Time Machine ідеальним вибором для більшості користувачів, що шукають простий і ефективний спосіб захисту своїх даних.

Резервне копіювання баз даних за допомогою MySQL Enterprise Backup (для комерційних користувачів). MySQL Enterprise Backup — це потужне рішення для резервного копіювання і відновлення баз даних, розроблене компанією Oracle для комерційних користувачів MySQL. Це інструмент, який надає підприємствам можливість здійснювати регулярне, ефективне та надійне резервне копіювання своїх баз даних, гарантуючи високу доступність та безпеку даних. MySQL Enterprise Backup є частиною пакету MySQL Enterprise Edition і пропонує численні функції, яких немає в стандартних інструментах для резервного копіювання, таких як `mysqldump`. Однією з ключових особливостей MySQL Enterprise Backup є його здатність виконувати гарячі резервні копії, що дозволяє проводити копіювання даних без вимкнення бази даних або її блокування. Це особливо важливо для великих або критичних бізнес-застосунків, де вимоги до доступності є високими. Гарячі резервні копії забезпечують мінімальний вплив на продуктивність сервера, дозволяючи базі даних продовжувати працювати під час виконання резервного копіювання.

MySQL Enterprise Backup підтримує повні, інкрементні та диференційні резервні копії. Повні копії дають змогу створювати цілісні резервні знімки бази даних, тоді як інкрементні копії зберігають лише зміни, що відбулися після останнього резервного копіювання, що дозволяє значно зменшити обсяг збережених даних і

скоротити час, необхідний для створення копії. Диференційні резервні копії зберігають зміни, які відбулися після останньої повної резервної копії, і є корисними для зменшення обсягу даних, які потрібно обробляти при відновленні. Одним із великих переваг MySQL Enterprise Backup є його здатність створювати фізичні резервні копії на рівні файлів. Це означає, що інструмент може створювати точні копії всіх файлів бази даних (включаючи дані, індекси та журнали транзакцій), що забезпечує можливість відновлення в разі апаратних збоїв чи інших надзвичайних ситуацій. Такі резервні копії швидше і ефективніше виконуються, ніж традиційні логічні копії, оскільки вони зберігають безпосередньо самі дані в їхньому фізичному вигляді, а не як SQL-дампи. Особливістю MySQL Enterprise Backup є його підтримка відновлення в режимі "точно до" (Point-in-Time Recovery, PITR), що дозволяє відновлювати базу даних до конкретного моменту часу. Ця функція надзвичайно важлива для випадків, коли потрібно відновити дані після помилки або пошкодження, яке сталося після певної дії, наприклад, помилкового запиту чи системного збою. За допомогою PITR, користувачі можуть відновити базу даних до точного часу, що дає змогу зберегти важливі дані, які були змінені після інциденту.

Важливою перевагою цього інструмента є його інтеграція з MySQL Cluster. MySQL Enterprise Backup може працювати в середовищі з багатьма серверами і забезпечує резервне копіювання та відновлення даних для розподілених баз даних, що працюють в кластерах. Це дає змогу зберігати цілісність і доступність даних навіть у великих і складних інфраструктурах, що потребують високої доступності та масштабованості. Ще однією важливою функцією є підтримка шифрування резервних копій. Це забезпечує додатковий рівень безпеки, оскільки резервні копії баз даних часто містять конфіденційну інформацію, таку як паролі, особисті дані користувачів та інші чутливі дані. За допомогою шифрування можна забезпечити, щоб резервні копії залишалися захищеними навіть у разі їх викрадення або несанкціонованого доступу. MySQL Enterprise Backup також забезпечує автоматизацію процесів резервного копіювання, що дозволяє знижувати

ймовірність помилок, пов'язаних з ручним виконанням цих операцій. Інструмент підтримує планування резервних копій, що дозволяє користувачам налаштовувати періодичність копіювання відповідно до своїх вимог, будь то щодня, щотижня чи в інші періоди.

Що стосується ефективності, MySQL Enterprise Backup підтримує відновлення лише необхідних даних, що дозволяє мінімізувати час на відновлення та витрати на ресурси. При відновленні можна вибрати лише ті таблиці або бази даних, які потребують відновлення, що значно пришвидшує процес відновлення після збою. Крім того, MySQL Enterprise Backup має зручний інтерфейс командного рядка, що дозволяє інтегрувати його в існуючі скрипти автоматизації та оркестрації. Це дає змогу легко інтегрувати резервне копіювання в процеси DevOps і забезпечує гнучкість при налаштуванні та управлінні резервними копіями. Одним із недоліків MySQL Enterprise Backup є те, що він є частиною комерційної версії MySQL, і для його використання потрібна ліцензія. Це може бути дорогим рішенням для невеликих компаній або стартапів, які шукають безкоштовні альтернативи. Однак для великих підприємств або критичних додатків, де важлива висока доступність і швидкість відновлення, інвестиції в MySQL Enterprise Backup можуть виправдати себе завдяки підвищеній надійності та безпеці.

Одночасне резервне копіювання багатьох клієнтів на один диск. Концепція одночасного резервного копіювання даних багатьох клієнтів на один диск стає все більш актуальною, оскільки компанії та організації продовжують використовувати мережеві та хмарні середовища. Ефективне керування резервним копіюванням для декількох пристроїв або клієнтів з одночасною консолідацією даних на одному диску вимагає врахування як технічних міркувань, так і логістичних викликів. Мета полягає в тому, щоб створити надійну стратегію резервного копіювання, яка збалансує простоту керування, оптимізацію ресурсів і цілісність даних. Такі схеми особливо поширені в компаніях, де централізоване зберігання даних є критично важливим, а кількість кінцевих точок (клієнтів), які потребують резервного

копіювання, є великою. Такі схеми можуть передбачати поєднання локальних і мережових сховищ, а в багатьох випадках для підвищення масштабованості та доступності використовуються хмарні сервіси. По суті, ідея резервного копіювання декількох клієнтів на один диск полягає у створенні централізованої системи резервного копіювання, в якій кожен клієнтський пристрій, наприклад, робочі станції, ноутбуки або сервери, надсилає свої дані в одне центральне сховище. Цим центральним сховищем зазвичай є диск великої ємності або сервер з достатнім обсягом пам'яті, але це може бути і хмарне сховище, залежно від інфраструктури. Процес зазвичай передбачає використання мережевого ресурсу, виділеного сервера резервного копіювання або навіть пряме підключення до центрального сховища, залежно від структури мережі. Поширеним підходом до реалізації одночасного резервного копіювання є використання програмного забезпечення для резервного копіювання або систем, які підтримують багатоклієнтські середовища. Ці системи часто працюють через центральну консоль, де адміністратор може керувати завданнями резервного копіювання для всіх клієнтів. У багатьох випадках клієнти налаштовані на виконання резервного копіювання за розкладом через певні проміжки часу. Програмне забезпечення для резервного копіювання повинно мати можливість працювати з кількома клієнтами, не перевантажуючи центральний диск, і гарантувати, що дані кожного клієнта ізольовані та належним чином управляються. Така ізоляція має вирішальне значення для запобігання пошкодженню даних одного клієнта іншим, особливо при використанні спільної файлової системи або при одночасному виконанні декількох резервних копій. Технічно існує кілька стратегій керування одночасним резервним копіюванням для багатьох клієнтів. Один підхід полягає в тому, щоб кожен клієнт створював резервні копії своїх даних в окремі папки або розділи на центральному диску, гарантуючи, що дані кожного клієнта логічно відокремлені. Цей метод особливо корисний, коли доступ до даних і їх відновлення повинні бути ефективними, оскільки він дозволяє адміністраторам швидко знаходити і відновлювати дані з конкретного клієнта, не просіюючи резервні копії інших. У більш просунутих

конфігураціях для резервного копіювання даних клієнтів можна використовувати інкрементне або диференціальне резервне копіювання, яке допомагає мінімізувати навантаження на систему резервного копіювання, зберігаючи лише зміни, внесені до даних з моменту останнього резервного копіювання.

Диск, на якому зберігаються резервні копії, також повинен мати відповідний розмір, щоб вмістити об'єднані дані від декількох клієнтів. Залежно від частоти резервного копіювання, загальний обсяг даних може бути значним, тому масштабованість стає важливим фактором. Деякі середовища використовують мережеві сховища (NAS) або мережі зберігання даних (SAN) як центральний диск для резервного копіювання, оскільки ці пристрої призначені для роботи з великими обсягами даних від декількох клієнтів. Ці типи рішень для зберігання даних часто підтримують конфігурації RAID, які забезпечують надмірність і підвищену надійність, гарантуючи, що навіть якщо один диск вийде з ладу, дані резервної копії залишаться в безпеці. Пропускна здатність і швидкість мережі - ще один важливий фактор при резервному копіюванні даних багатьох клієнтів на один диск. У середовищах з великою кількістю кінцевих точок швидкість передачі даних може бути вузьким місцем. Дуже важливо переконатися, що процес резервного копіювання не заважає нормальній роботі мережі. Багато систем резервного копіювання включають такі функції, як регулювання пропускної здатності, коли процеси резервного копіювання налаштовуються на запуск у неробочий час або при низькому мережевому трафіку, щоб мінімізувати перебої в роботі. Для віддалених працівників або клієнтів у географічно розподілених мережах можна використовувати хмарне резервне копіювання. Хмарні сервіси зазвичай дозволяють програмному забезпеченню для резервного копіювання надсилати дані на віддалений сервер, гарантуючи, що клієнти завжди матимуть актуальну інформацію без прямого доступу до локального сховища.

Безпека та шифрування також відіграють важливу роль у процесі резервного копіювання, особливо якщо ви працюєте з кількома клієнтами. Централізоване

резервне копіювання може створити єдину точку відмови, якщо заходи безпеки не є надійними. Шифрування як на рівні даних у дорозі, так і на рівні даних у стані спокою гарантує, що резервні копії будуть захищені від несанкціонованого доступу. Це стає особливо важливим у середовищах, де створюються резервні копії конфіденційних або персональних даних, а дотримання таких нормативних актів, як GDPR або HIPAA, може вимагати додаткових гарантій. Рішення для резервного копіювання часто містять вбудовані засоби шифрування, але для задоволення конкретних потреб організації можна використовувати додаткове програмне забезпечення для шифрування сторонніх розробників. Безпека та шифрування також відіграють важливу роль у процесі резервного копіювання, особливо якщо ви маєте справу з кількома клієнтами. Централізоване резервне копіювання може створити єдину точку відмови, якщо заходи безпеки недостатньо ефективні. Шифрування як на рівні даних у дорозі, так і на рівні даних у стані спокою гарантує, що резервні копії будуть захищені від несанкціонованого доступу. Це стає особливо важливим у середовищах, де створюються резервні копії конфіденційних або персональних даних, а дотримання таких нормативних актів, як GDPR або HIPAA, може вимагати додаткових гарантій. Рішення для резервного копіювання часто містять вбудовані засоби шифрування, але для задоволення конкретних потреб організації можна використовувати додаткове програмне забезпечення для шифрування сторонніх розробників. Хоча резервне копіювання багатьох клієнтів на один диск забезпечує значну зручність, воно також створює потенційні проблеми, пов'язані з відновленням даних. У разі збою або втрати даних процес відновлення даних з одного центрального резервного диска може стати складним, особливо якщо дані з різних клієнтів не були належним чином організовані або ізольовані. Цю проблему можна вирішити, використовуючи ефективну систему каталогізації та індексації, яка відстежує, які дані належать якому клієнту, що робить відновлення швидшим та ефективнішим. Крім того, заходи надмірності, такі як конфігурації RAID або використання декількох дисків для зберігання резервних

копій, можуть забезпечити можливості відмовостійкості, знижуючи ризик втрати даних через вихід з ладу диска.

Ще одним важливим аспектом керування одночасним резервним копіюванням є планування та автоматизація завдань резервного копіювання. При великій кількості клієнтів ручне керування кожним процесом резервного копіювання може бути громіздким і схильним до людських помилок. Більшість сучасних систем резервного копіювання дозволяють автоматизувати планування, коли резервне копіювання виконується через регулярні проміжки часу, не вимагаючи постійного контролю. Автоматизовані системи резервного копіювання також пропонують можливість генерувати журнали та сповіщення, які повідомляють адміністраторів про збій резервного копіювання або виникнення проблем. Такий рівень автоматизації допомагає забезпечити постійне резервне копіювання для всіх клієнтів без необхідності постійного нагляду.

У середовищах, де клієнти мають різні потреби в резервному копіюванні, наприклад, різні обсяги даних або частоту резервного копіювання, виникає необхідність налаштувати процес резервного копіювання для кожного клієнта. Деякі системи дозволяють здійснювати детальний контроль, коли адміністратори можуть налаштувати конкретні параметри резервного копіювання для кожного клієнта, наприклад, встановити різні політики збереження, типи резервного копіювання (повне, інкрементне або диференційоване) або розклад резервного копіювання. Така гнучкість гарантує, що система резервного копіювання пристосована до потреб кожного клієнта, зберігаючи при цьому ефективність централізованої інфраструктури резервного копіювання. Крім того, фізичне або віртуальне розташування диска резервного копіювання відіграє важливу роль у його ефективності. Якщо диск фізично знаходиться в тому ж офісі або центрі обробки даних, що і клієнти, дуже важливо впровадити план аварійного відновлення, який враховує потенційні локальні катастрофи, такі як пожежі, повені або перебої в подачі електроенергії. У багатьох організаціях резервне копіювання

за межами офісу або в хмарі використовується разом з локальними резервними копіями для створення додаткового рівня захисту. Провайдери хмарних сховищ пропонують послуги, які автоматично синхронізують дані з локальних систем до віддалених центрів обробки даних, забезпечуючи додатковий рівень безпеки та надмірності.

Насамкінець, резервне копіювання даних багатьох клієнтів на один диск створює як можливості, так і проблеми. Переваги централізованого резервного копіювання включають легше керування, економію витрат на обладнання для зберігання даних і спрощення відновлення даних. Однак таке налаштування вимагає ретельного планування для забезпечення масштабованості, безпеки та надійності. Вибір програмного забезпечення для резервного копіювання, обладнання для зберігання даних та мережевої архітектури є ключовими рішеннями, які можуть вплинути на успіх такої стратегії. Враховуючи ці фактори та впроваджуючи найкращі практики управління резервним копіюванням, організації можуть гарантувати, що їхні системи резервного копіювання є ефективними, безпечними та здатними швидко відновлювати дані в разі виникнення проблем.

Хмарне резервне копіювання. Традиційні форми зберігання даних, такі як жорсткі диски та фізичні сервери, часто не відповідають вимогам сучасного цифрового ландшафту, який постійно розвивається і розширюється. Хмарні сховища вирішують цю проблему, пропонуючи спосіб зберігати дані віддалено, на серверах, які обслуговуються сторонніми провайдерами, і доступ до яких здійснюється через Інтернет. Це означає, що користувачі можуть зберігати свої файли без потреби у фізичних пристроях або інфраструктурі на місці, що пропонує значні переваги з точки зору зручності, безпеки та економічної ефективності.

Однією з найважливіших переваг хмарних сховищ є доступність. Хмарні сервіси дозволяють користувачам отримувати доступ до своїх файлів практично з будь-якого пристрою - комп'ютера, планшета чи смартфона - і з будь-якої точки світу, за умови наявності підключення до Інтернету. Такий рівень доступності

трансформував те, як ми працюємо, співпрацюємо та обмінюємося інформацією. Люди можуть отримати доступ до своїх фотографій, документів і відео в дорозі, не турбуючись про передачу файлів між різними пристроями. Компанії також використовують хмарні сховища для покращення співпраці. Команди можуть працювати разом у режимі реального часу, обмінюючись документами, вносячи правки та відстежуючи прогрес у різних місцях. Це дозволило компаніям подолати географічні бар'єри, об'єднавши таланти з різних куточків світу для роботи над спільними проектами. Простота обміну файлами та співпраця в режимі реального часу призвели до підвищення продуктивності та ефективності в багатьох галузях, особливо в таких сферах, як маркетинг, дизайн, розробка програмного забезпечення та управління проектами.

Хмарні сховища також пропонують надзвичайну гнучкість і масштабованість, дозволяючи користувачам налаштовувати обсяг сховища відповідно до своїх потреб. На відміну від традиційних систем зберігання даних, які вимагають фіксованих обсягів фізичного простору, хмарне сховище може розширюватися або зменшуватися за необхідності. Для бізнесу це означає, що вони можуть легко масштабувати свої потреби в сховищах у відповідь на зростання, сезонні потреби або зміну вимог до даних. Їм не потрібно турбуватися про те, що не вистачить місця, або інвестувати в додаткове обладнання, що може бути дорогим і трудомістким. Натомість хмарні провайдери зазвичай пропонують модель оплати за фактом використання, що дозволяє компаніям платити лише за те сховище, яке вони фактично використовують. Це не лише зменшує авансові витрати, але й забезпечує передбачуваність поточних витрат. Масштабованість хмарних сховищ є однією з ключових причин їхньої популярності серед стартапів та малих підприємств, які можуть скористатися гнучким, недорогим рішенням без необхідності великих інвестицій у фізичну інфраструктуру.

Безпека - ще одна сфера, де хмарні сховища досягли значних успіхів. Хоча віддалене зберігання даних на перший погляд може здатися ризикованим, хмарні

провайдери інвестують значні кошти в надійні заходи безпеки, щоб захистити інформацію своїх клієнтів. Багато хмарних сервісів використовують шифрування для захисту даних під час передачі та в стані спокою, що унеможлиблює доступ сторонніх осіб до конфіденційної інформації. Двофакторна автентифікація та багаторівневі протоколи безпеки також широко використовуються для захисту облікових записів користувачів, додаючи ще один рівень захисту від кіберзагроз. Крім того, провайдери хмарних сховищ зазвичай зберігають свої дані на декількох серверах, часто в різних географічних точках, а це означає, що навіть якщо один сервер виходить з ладу, дані все одно доступні з іншого сервера, що забезпечує підвищену надійність і безвідмовність роботи. Для бізнесу такий рівень безпеки є вкрай важливим, особливо коли йдеться про конфіденційні дані, такі як інформація про клієнтів, фінансова звітність або інтелектуальна власність. Можливість покластися на хмару для вирішення цих проблем безпеки дозволяє компаніям зосередитися на своїх основних операціях, не турбуючись про підтримку інфраструктури безпеки на місці.

Простота доступу, масштабованість і безпека хмарних сховищ також призвели до значних змін у тому, як люди керують своїми персональними даними. Такі сервіси, як Google Drive, Dropbox та iCloud, спростили користувачам зберігання та організацію своїх файлів в Інтернеті, з додатковою перевагою - автоматичним резервним копіюванням. Користувачам більше не потрібно турбуватися про втрату важливих документів або фотографій через збій комп'ютера або збій обладнання, оскільки ці файли надійно зберігаються в хмарі. Хмарне сховище також дозволяє легко синхронізувати дані на різних пристроях, гарантуючи, що остання версія файлу завжди доступна, незалежно від того, який пристрій використовується. Наприклад, якщо користувач редагує документ на своєму смартфоні, зміни автоматично відображаються на його ноутбукі або планшеті, забезпечуючи безперебійну роботу на різних пристроях. Крім того, багато хмарних сервісів зараз пропонують широкі можливості безкоштовного зберігання даних, що робить їх

доступними для широкого кола користувачів, від випадкових споживачів до професійних користувачів з більш вимогливими потребами до зберігання.

Незважаючи на численні переваги, хмарні сховища не позбавлені проблем. Однією з головних проблем для багатьох користувачів є залежність від підключення до Інтернету. Оскільки хмарне сховище базується на Інтернеті, користувачі повинні мати доступ до стабільного та швидкого з'єднання, щоб завантажувати, вивантажувати та отримувати доступ до своїх даних. У регіонах, де інтернет-зв'язок поганий або ненадійний, це може стати суттєвою перешкодою для впровадження хмарних сховищ. Крім того, хоча провайдери хмарних сховищ впроваджують надійні заходи безпеки, жодна система не є повністю захищеною від загроз. Витоки даних, спроби злому та кібератаки є постійними проблемами в цифрову епоху, і хмарні сервіси зберігання даних не позбавлені цих ризиків. Хоча хмарні провайдери інвестують значні кошти в безпеку, централізація даних у кількох великих центрах обробки даних збільшує ймовірність масштабних зломів, тому користувачам важливо бути пильними і застосовувати надійні методи безпеки, наприклад, використовувати надійні паролі та двофакторну автентифікацію.

Ще однією проблемою є питання конфіденційності даних. Оскільки хмарні сховища передбачають зберігання та управління даними сторонніми провайдерами, виникають питання про те, хто має доступ до цих даних і як вони використовуються. Хоча більшість авторитетних хмарних провайдерів мають політику конфіденційності, яка захищає інформацію користувачів, занепокоєння щодо державного нагляду, видобутку даних та корпоративного доступу до приватної інформації залишаються. Оскільки хмарні сховища стають все більш інтегрованими в повсякденне життя, це піднімає важливі питання про право власності на дані та контроль над ними. Наприклад, якщо хмарний провайдер зазнає витоку даних, хто несе відповідальність за наслідки? Які права мають користувачі щодо доступу, передачі чи видалення своїх даних з серверів

провайдера? Ці питання стають все більш важливими, оскільки хмарні сховища стають центральним аспектом як особистого, так і професійного життя.

Вплив хмарних сховищ на навколишнє середовище також викликає все більше занепокоєння. Хмарні провайдери експлуатують великі центри обробки даних, які споживають значну кількість енергії для живлення та охолодження серверів. Оскільки попит на хмарні сховища продовжує зростати, зростає і енергоспоживання цих центрів обробки даних, що посилює занепокоєння щодо вуглецевого сліду хмарних обчислень. Однак багато великих хмарних провайдерів працюють над вирішенням цієї проблеми, інвестуючи у відновлювані джерела енергії та підвищуючи енергоефективність своїх дата-центрів. Деякі компанії, такі як Google і Microsoft, взяли на себе зобов'язання досягти вуглецевої нейтральності, тоді як інші вивчають способи компенсувати використання енергії за рахунок кредитів на відновлювану енергію або шляхом прямого придбання екологічно чистої енергії. Оскільки попит на хмарні сховища продовжує зростати, для галузі буде важливо знайти стійкі рішення, які мінімізують вплив цієї технології на навколишнє середовище.

Підсумовуючи, можна сказати, що хмарні сховища докорінно змінили спосіб зберігання та управління даними. Вона зробила дані доступними з будь-якої точки світу, надала компаніям масштабовані та безпечні рішення для зберігання даних, а приватним особам запропонувала спосіб зберігати свої особисті файли, не турбуючись про фізичне обладнання. Однак, як і будь-яка інша технологія, хмарне зберігання даних пов'язане з певними проблемами, особливо коли йдеться про безпеку, конфіденційність та вплив на навколишнє середовище. Незважаючи на ці проблеми, хмарні сховища продовжують розвиватися і залишаються важливим інструментом як для особистого, так і для професійного використання. З розвитком технологій хмарні сховища, ймовірно, стануть ще більш інтегрованими в наше повсякденне життя, пропонуючи ще більше переваг і можливостей, водночас вирішуючи проблеми, які з ними пов'язані.

Network-Attached Storage, NAS. Мережеві сховища (Network-Attached Storage, NAS) - це спеціалізована технологія, яка стала важливим рішенням як для бізнесу, так і для домашніх користувачів, які потребують надійного, централізованого та масштабованого сховища. На відміну від традиційних зовнішніх жорстких дисків, які підключаються до одного комп'ютера, системи NAS призначені для підключення до мережі, що дозволяє декільком пристроям отримувати доступ до одного і того ж простору зберігання через Інтернет або локальну мережу (LAN). Це робить їх ідеальним рішенням для середовищ, в яких дані потрібно спільно використовувати, отримувати до них доступ і створювати резервні копії на декількох пристроях. Концепція NAS полягає в наданні користувачам централізованого сховища, доступного через мережу, що забезпечує зручність та ефективність. Пристрій NAS зазвичай складається з одного або декількох жорстких дисків, розміщених в одному корпусі, оснащених спеціальною операційною системою, яка керує файлами, користувачами та протоколами доступу. Ці системи часто налаштовуються, мають розширюваний обсяг пам'яті, що робить їх придатними для широкого спектру застосувань - від домашніх медіа-серверів до рішень для резервного копіювання на рівні підприємства.

Однією з ключових переваг NAS є простота налаштування та використання. NAS розроблені за принципом «підключи і працюй», що вимагає мінімальних технічних знань для встановлення. Пристрій потрібно просто підключити до маршрутизатора або комутатора, а потім налаштувати за допомогою веб-інтерфейсу або спеціального програмного забезпечення. Після налаштування користувачі можуть отримати доступ до сховища віддалено - зі стаціонарного комп'ютера, ноутбука, смартфона або планшета, якщо вони підключені до однієї мережі, або, в деяких випадках, через Інтернет, якщо увімкнено віддалений доступ. Така безперешкодна інтеграція в домашню або офісну мережу дозволяє легко обмінюватися файлами, співпрацювати та керувати сховищем, що робить NAS універсальним рішенням для різноманітних потреб. У бізнесі NAS виявилися безцінними для створення централізованого

файлового сервера, де співробітники можуть отримувати доступ і зберігати документи, електронні таблиці та інші файли з будь-якого пристрою в офісі або віддалено. Така централізація спрощує управління даними та їх безпеку, оскільки дані зберігаються в єдиному безпечному місці, а не розкидані по декількох комп'ютерах або пристроях. Для особистого використання NAS слугує потужним інструментом для зберігання медіафайлів, таких як музика, фільми та фотографії, які потім можна транслювати на різні пристрої, включаючи смарт-телевізори, комп'ютери та мобільні пристрої.

Ще однією важливою особливістю NAS є його здатність підтримувати стратегії резервування даних і резервного копіювання. Багато пристроїв NAS оснащено функцією RAID (надлишковий масив незалежних дисків), яка дозволяє користувачам налаштовувати кілька жорстких дисків у різних конфігураціях для підвищення надійності даних. RAID може забезпечити захист від апаратних збоїв, дублюючи дані на декількох дисках або розподіляючи дані по дисках таким чином, щоб їх можна було відновити, якщо один диск вийде з ладу. Це робить NAS надійним рішенням для забезпечення цілісності даних, особливо в середовищах, де постійно створюються або змінюються великі обсяги даних. При правильній конфігурації RAID-масиву NAS може забезпечити безпеку даних без необхідності використання складних рішень для резервного копіювання. Крім того, багато систем NAS постачаються з вбудованим програмним забезпеченням для резервного копіювання, що дозволяє користувачам автоматично створювати резервні копії важливих файлів зі своїх комп'ютерів, гарантуючи їх безпечне зберігання на пристрої NAS. Для підприємств ця функція може стати важливою частиною плану відновлення після збоїв, пропонуючи ефективний і надійний спосіб відновлення файлів у разі втрати даних.

NAS також пропонує підвищену продуктивність порівняно з традиційними пристроями зберігання даних. Підключаючись безпосередньо до мережі, NAS-пристрої можуть забезпечити більш високу швидкість передачі даних,

особливо при використанні з гігабітною або більш високошвидкісною мережею. Це особливо корисно в середовищах, де потрібен спільний доступ до великих обсягів даних або потокова передача мультимедійних даних. Наприклад, у бізнес-середовищі, де доступ до великих файлів мають одночасно кілька співробітників, NAS може забезпечити швидший і ефективніший пошук даних, ніж окремі жорсткі диски, підключені до окремих комп'ютерів. Аналогічно, для домашніх користувачів, які хочуть зберігати і транслювати відео високої чіткості або великі медіатеки, NAS - це рішення, яке може впоратися з вимогами до пропускної здатності, що пред'являються кількома пристроями, які одночасно отримують доступ до одного і того ж контенту. Просунуті моделі NAS можуть навіть підтримувати потокову передачу мультимедійних даних у форматі 4K, забезпечуючи плавний і безперебійний доступ користувачів до мультимедійного контенту, що зберігається на пристрої.

Незважаючи на те, що переваги NAS очевидні, існують також міркування, які користувачі повинні враховувати при виборі та налаштуванні системи. Перше - це початкові витрати. Хоча рішення NAS можуть бути доступними для домашніх користувачів, вартість може значно зростати в міру збільшення обсягу пам'яті та додавання додаткових функцій. Висококласні моделі, призначені для використання в бізнесі, з декількома відсіками, великою ємністю і розширеними функціями, такими як розширені протоколи безпеки і підтримка віртуалізації, можуть коштувати дорого. Крім того, користувачі повинні враховувати вартість самих жорстких дисків, оскільки вони, як правило, не входять до комплекту NAS і їх потрібно купувати окремо. Однак, незважаючи на початкові інвестиції, багато користувачів вважають, що NAS забезпечує відмінну цінність в довгостроковій перспективі, пропонуючи економічно ефективне рішення для централізованого зберігання даних, яке усуває потребу в дорогій серверній інфраструктурі або підписці на хмарне сховище.

Ще одним фактором, який слід враховувати при використанні NAS, є швидкість мережі. Хоча NAS може забезпечити вищу швидкість передачі даних, ніж традиційні зовнішні жорсткі диски, фактична продуктивність буде залежати від потужності та швидкості мережі, до якої підключено пристрій. Для оптимальної роботи потрібна швидка і стабільна локальна мережа, особливо для передачі великих файлів або одночасного доступу з декількох пристроїв. Для забезпечення найкращої роботи системи NAS може знадобитися модернізація мережевої інфраструктури, наприклад, перехід на гігабітний Ethernet або впровадження швидших бездротових протоколів, таких як Wi-Fi 6. Крім того, віддалений доступ до NAS-пристрою через Інтернет вимагає налаштування мережевого маршрутизатора на переадресацію портів або використання VPN (віртуальної приватної мережі) для безпечного підключення до пристрою, що може вимагати додаткових налаштувань і технічних знань.

Попри ці труднощі, гнучкість і функціональність NAS роблять його привабливим варіантом для багатьох користувачів. Для домашніх користувачів це централізоване місце для зберігання особистих файлів, резервних копій і медіатек, з додатковою зручністю віддаленого доступу. Він може слугувати персональною хмарою, надаючи користувачам можливість доступу до своїх даних з будь-якої точки світу, зберігаючи при цьому повний контроль над їх зберіганням. Для бізнесу NAS є потужним інструментом для управління та захисту даних, пропонуючи високу доступність, надмірність і масштабованість без необхідності дорогого і складного налаштування сервера. Можливість налаштування системи NAS з різними конфігураціями RAID- масивів і ємністю зберігання робить її легко адаптованою до різних сценаріїв використання, як для малого бізнесу з кількома співробітниками, так і для великого підприємства з великими потребами в зберіганні даних. Оскільки підприємства продовжують генерувати величезні обсяги даних, а приватні особи накопичують все більше мультимедійних файлів і документів,

очікується, що попит на надійні та ефективні рішення для зберігання даних, такі як NAS, буде зростати. Крім того, з появою нових технологій, таких як 5G і високошвидкісні мережі, потенціал систем NAS, що пропонують ще більш високу продуктивність і надійні функції, буде тільки збільшуватися.

FTP/SFTP.Резервне копіювання за допомогою протоколів FTP (File Transfer Protocol) і SFTP (Secure File Transfer Protocol) давно перетворилося на важливий метод зберігання і відновлення даних в професійному середовищі. Ці протоколи дозволяють користувачам віддалено передавати і зберігати файли, пропонуючи надійний спосіб резервного копіювання критично важливих даних. Хоча FTP і SFTP часто використовуються для передачі файлів через Інтернет, їх застосування для резервного копіювання даних надає значні переваги, включаючи віддалений доступ, безпеку і масштабованість. FTP, будучи одним з найстаріших і найбільш широко використовуваних протоколів для передачі файлів, дозволяє користувачам завантажувати файли на віддалений сервер, що дає можливість створювати резервні копії файлів за межами підприємства, де вони менш схильні до локальних катастроф, таких як повені, пожежі або крадіжки. SFTP, з іншого боку, є розширенням FTP, яке додає додатковий рівень безпеки за допомогою шифрування, гарантуючи, що файли передаються і зберігаються безпечно, що має вирішальне значення при роботі з конфіденційними даними.

Основна відмінність між FTP і SFTP полягає в тому, що SFTP шифрує як дані, так і безпосередньо вхідні команди, що робить його набагато безпечнішим, ніж FTP, який передає інформацію у вигляді відкритого тексту. Ця додаткова безпека особливо важлива для підприємств, які працюють з конфіденційними або приватними даними і повинні забезпечити захист своїх резервних копій від несанкціонованого доступу або кіберзагроз. Резервне копіювання через FTP/SFTP - відмінне рішення як для малих, так і для великих організацій, яким потрібен надійний і економічно ефективний спосіб забезпечити безпеку своїх даних. Воно дозволяє користувачам налаштовувати

резервне копіювання за розкладом, забезпечуючи регулярне оновлення та захист даних без необхідності ручного втручання. Користувачі також можуть налаштувати процеси резервного копіювання по FTP/SFTP на автоматичний запуск у заздалегідь визначений час, наприклад, вночі, коли менше активності, щоб уникнути переривання звичайних бізнес-операцій. Така автоматизація гарантує постійне резервне копіювання критично важливих файлів, не покладаючись на людський фактор і не забуваючи ініціювати процес. Однією з ключових переваг використання FTP/SFTP для резервного копіювання є можливість зберігати файли віддалено, що забезпечує додатковий рівень захисту від втрати даних. Зберігання резервних копій за межами офісу означає, що навіть у разі катастрофічних подій на локальному рівні, таких як збій обладнання, пошкодження даних або стихійне лихо, резервні копії файлів залишаться в безпеці і будуть доступні. Віддалене зберігання також може звільнити цінний локальний простір для зберігання, дозволяючи компаніям і приватним особам зберігати великі обсяги даних, не перевантажуючи свої основні системи зберігання. Для компаній можливість віддаленого резервного копіювання також полегшує дотримання норм і стандартів захисту даних, які вимагають створення резервних копій за межами офісу або географічно розподіленого зберігання. Крім того, резервні копії FTP/SFTP можна налаштувати на зберігання декількох версій файлів, що може бути особливо корисно для відновлення попередніх версій документів або додатків у разі випадкових змін або пошкодження даних. Такий контроль версій дозволяє компаніям відкочуватися до більш ранніх моментів часу, гарантуючи, що вони зможуть відновити файли до певної версії без необхідності відновлювати весь набір даних. Резервне копіювання через FTP/SFTP також підтримує функцію масштабування, оскільки компанії можуть збільшувати обсяг дискового простору на віддалених серверах, не турбуючись про фізичні обмеження локальних пристроїв зберігання даних. Зі збільшенням обсягу даних користувачі можуть легко налаштувати обсяг резервного копіювання,

придбавши додатковий простір у свого постачальника послуг або перейшовши на вищий рівень обслуговування. Така масштабованість гарантує, що резервне копіювання по FTP/SFTP залишається гнучким і перспективним рішенням, здатним адаптуватися до зростаючих потреб у зберіганні даних.

Для домашніх користувачів резервне копіювання через FTP/SFTP може бути не менш корисним. Воно дозволяє надійно зберігати важливі файли, такі як фотографії, документи та відео, на віддаленому сервері, гарантуючи захист даних у разі збою обладнання або інших непередбачуваних подій. Багато людей також вважають за краще використовувати FTP/SFTP для резервного копіювання, щоб не покладатися на хмарні сервіси, що надаються великими корпораціями, які можуть мати занепокоєння щодо конфіденційності або права власності на дані. Керуючи власними резервними копіями через FTP/SFTP, користувачі зберігають повний контроль над своїми даними, вибираючи, де і як вони зберігаються. Однак, незважаючи на численні переваги, резервне копіювання через FTP/SFTP також пов'язане з певними проблемами. Однією з найсуттєвіших перешкод є потреба в технічних знаннях для налаштування та керування процесом резервного копіювання. Хоча процес є простим для тих, хто знайомий з FTP/SFTP і конфігураціями серверів, він може бути складним для менш технічних користувачів. Щоб налаштувати резервне копіювання за допомогою FTP/SFTP, користувачам потрібен доступ до сервера з достатнім обсягом пам'яті, FTP/SFTP-клієнт, а також певне розуміння мережевих налаштувань, дозволів на файли і протоколів безпеки. Це може зробити процес налаштування складнішим, ніж просте використання хмарних сервісів резервного копіювання, які часто надають зручні інтерфейси та автоматичну конфігурацію.

Ще одним викликом є забезпечення повної автоматизації та надійності процесу резервного копіювання. Без належного налаштування резервне копіювання може не виконуватися за розкладом або, в деяких випадках, завантажувати не всі заплановані файли. Крім того, користувачі повинні

стежити за цілісністю резервних копій, щоб переконатися, що дані були правильно перенесені і доступні в разі відновлення. Для цього може знадобитися періодичне тестування, щоб переконатися, що файли можна відновити без проблем. Швидкість мережі також може впливати на ефективність резервного копіювання по FTP/SFTP. Передача великих файлів мережею може зайняти певний час, а якщо мережеве з'єднання повільне або нестабільне, процес резервного копіювання може затягнутися або перерватися. Для компаній, які мають справу з великими масивами даних, це може призвести до довгих вікон резервного копіювання, особливо якщо резервне копіювання відбувається в робочий час, коли пропускна здатність мережі необхідна для інших завдань. Щоб зменшити цю проблему, користувачі можуть планувати резервне копіювання на непікові години, щоб мережа не перевантажувалася під час процесу резервного копіювання. Крім того, для великих обсягів резервного копіювання користувачам може знадобитися оптимізація конфігурації FTP/SFTP для підвищення швидкості, наприклад, увімкнувши стиснення під час передачі файлів. Крім того, слід ретельно контролювати безпеку самого процесу резервного копіювання. У той час як SFTP пропонує шифрування і захист, FTP цього не робить, що робить файли вразливими до перехоплення під час передачі. При використанні FTP для резервного копіювання дуже важливо переконатися, що з'єднання захищене шифруванням SSL/TLS, яке може допомогти захистити дані під час передачі. Для тих, хто використовує SFTP, важливо впровадити надійну політику паролів і використовувати автентифікацію на основі ключів для додаткової безпеки. Віддалене зберігання резервних копій також вимагає від користувачів дотримання законів і правил про конфіденційність даних. Залежно від регіону, можуть існувати обмеження щодо місця зберігання даних, особливо якщо вони містять конфіденційну інформацію, таку як особиста ідентифікація, фінансові записи або дані про стан здоров'я. Користувачі повинні переконатися, що FTP/SFTP-сервер, який вони

використовують, відповідає відповідним законам про захист даних, щоб уникнути потенційних юридичних проблем. Крім того, рішення для резервного копіювання за допомогою FTP/SFTP не мають таких функцій, як синхронізація файлів або резервне копіювання в режимі реального часу, які характерні для інших методів резервного копіювання, наприклад, хмарних сервісів.

Це означає, що користувачам може знадобитися налаштувати власну систему на інкрементне резервне копіювання, щоб забезпечити завантаження лише нових або змінених файлів, замість того, щоб щоразу завантажувати весь набір даних. Це може допомогти заощадити час і пропускну здатність, але вимагає додаткової конфігурації та налаштування. Незважаючи на ці проблеми, резервне копіювання через FTP/SFTP залишається надійним і безпечним методом резервного копіювання критично важливих даних. При правильній конфігурації, заходах безпеки та моніторингу воно може стати надійним рішенням для компаній і приватних осіб, яким необхідно забезпечити безпеку, доступність і можливість відновлення своїх файлів. Якщо користувачі усвідомлюють потенційні обмеження і готові інвестувати час і ресурси, необхідні для налаштування і підтримки системи, резервне копіювання по FTP/SFTP пропонує гнучкий, економічно ефективний і безпечний спосіб захисту цінних даних від втрати або пошкодження. Завдяки віддаленому зберіганню, масштабованості та надійним заходам безпеки воно є важливим інструментом для тих, хто прагне впровадити комплексну стратегію захисту даних.

2. VEEAM: ОПИС ПРОДУКТУ

Veeam Backup & Replication - це комплексне рішення для захисту даних і аварійного відновлення. За допомогою Veeam Backup & Replication можна створювати резервні копії на рівні образів віртуальних, фізичних і хмарних машин і відновлюватися з них. Технології, що використовуються в продукті, оптимізують передачу даних і споживання ресурсів, що допомагає мінімізувати витрати на зберігання і час відновлення в разі аварії.

Veeam Backup & Replication надає централізовану консоль для адміністрування операцій резервного копіювання, відновлення та реплікації на всіх підтримуваних платформах (віртуальних, фізичних, хмарних). Також консоль дозволяє автоматизувати і планувати рутинні операції захисту даних та інтегруватися з рішеннями для оповіщення і генерації звітів про відповідність нормативним вимогам.

Основні функціональні можливості Veeam Backup & Replication включають: резервне копіювання: створення резервних копій на рівні образів віртуальних, фізичних, хмарних машин, а також резервних копій файлових ресурсів і сховищ об'єктів. Veeam Backup & Replication створює резервні копії віртуальних машин на рівні образів. Він розглядає VM як об'єкти, а не як набір файлів. Під час резервного копіювання VM Veeam Backup & Replication копіює образ VM як єдине ціле на рівні блоків. Резервні копії на рівні образу можна використовувати для різних типів відновлення, включаючи миттєве відновлення, відновлення всієї VM, відновлення файлів VM, відновлення на рівні файлів тощо. Технологія резервного копіювання зазвичай використовується для віртуальних машин з меншим часом напрацювання на відмову. Коли основна VM виходить з ладу, знадобиться деякий час для відновлення даних VM зі стисненого і дедуплікованого файлу резервної копії.

Veeam Backup & Replication створено для віртуальних середовищ. Він працює на рівні віртуалізації та використовує підхід на основі образів для резервного копіювання VM. Veeam Backup & Replication не встановлює агентське програмне забезпечення всередині гостьової ОС VM для отримання даних VM. Для резервного копіювання віртуальних машин використовуються можливості моментальних знімків VMware vSphere. Під час резервного копіювання віртуальної машини Veeam Backup & Replication звертається до VMware vSphere із запитом на створення знімка віртуальної машини. Знімок віртуальної машини можна розглядати як копію віртуальної машини в певний момент часу, яка містить віртуальні диски, стан системи, конфігурацію тощо. Veeam Backup & Replication використовує цю миттєву копію як джерело даних для резервного копіювання.

Veeam Backup & Replication копіює дані VM з вихідного сховища даних на рівні блоків. Він отримує дані VM, стискає і дедуплікує їх і зберігає у файлах резервних копій у сховищі резервних копій у власному форматі Veeam.

У Veeam Backup & Replication резервне копіювання - це процес, керований завданнями. Щоб виконати резервне копіювання, потрібно налаштувати завдання резервного копіювання. Завдання резервного копіювання - це одиниця конфігурації операції резервного копіювання. Завдання резервного копіювання визначає, коли, що, як і куди копіювати. Одне завдання резервного копіювання можна використовувати для обробки однієї або декількох віртуальних машин. Ви можете наказати Veeam Backup & Replication запускати завдання автоматично за розкладом або запускати їх вручну. Перший сеанс резервного копіювання завжди створює повну резервну копію образу VM. Наступні сеанси резервного копіювання є інкрементними - Veeam Backup & Replication копіює тільки ті блоки даних, які змінилися з моменту останнього сеансу резервного копіювання. Для відстеження змінених блоків даних Veeam Backup & Replication використовує різні підходи. Veeam Backup & Replication виконує резервне копіювання VM наступним чином: коли запускається новий сеанс завдання резервного копіювання, Veeam запускає процес Veeam Backup Manager на сервері резервного копіювання. Veeam Backup Manager зчитує параметри завдання з бази даних конфігурації і створює список завдань VM для обробки. Для кожного диска VM, доданого до завдання, Veeam створює нове завдання.

Veeam Backup Manager підключається до Veeam Backup Service. До складу Veeam Backup Service входить компонент планування ресурсів, який керує всіма завданнями і ресурсами в інфраструктурі резервного копіювання. Планувальник ресурсів перевіряє, які ресурси інфраструктури резервного копіювання доступні, і призначає проксі-сервери резервного копіювання та сховища резервних копій для обробки завдань. Veeam Backup Manager встановлює з'єднання з Veeam Data Movers на цільовому сховищі резервного копіювання та проксі-сервері резервного копіювання і задає ряд правил для передачі даних, наприклад, правила обмеження мережевого трафіку тощо.

Veeam Data Movers на проксі-сервері резервного копіювання та сховищі резервних копій встановлюють з'єднання один з одним для передачі даних. Veeam Backup Manager запитує інформацію про віртуальні машини та хости віртуалізації у Veeam Broker Service. Якщо для завдання ввімкнено обробку зображень з урахуванням додатків, Veeam Backup & Replication підключається до гостьових ОС ВМ, розгортає непостійні компоненти середовища виконання або, за необхідності, постійні компоненти агентів у гостьових ОС ВМ і виконує завдання обробки в гостьових ОС. Veeam Backup & Replication запитує vCenter Server або хост ESXi для створення знімка ВМ. Диски ВМ переводяться в стан «тільки для читання», і кожен віртуальний диск отримує дельта-файл. Усі зміни, які користувач вносить у віртуальну машину під час резервного копіювання, записуються в дельта-файли. Вихідний Veeam Data Mover зчитує дані віртуальної машини з диска віртуальної машини, доступного тільки для читання, і переносить їх до сховища резервних копій в одному з транспортних режимів. Під час інкрементних сеансів роботи вихідний Veeam Data Mover використовує СБТ, щоб отримати тільки ті блоки даних, які змінилися з моменту попереднього сеансу роботи. Якщо СБТ недоступний, вихідний Veeam Data Mover взаємодіє з цільовим Veeam Data Mover у сховищі резервних копій, щоб отримати метадані резервної копії, і використовує ці метадані для виявлення блоків, які змінилися з моменту попереднього сеансу роботи. Під час транспортування даних віртуальних машин джерело Veeam Data

Mover виконує додаткову обробку. Він відфільтровує нульові блоки даних, блоки файлів підкачки та блоки виключених файлів гостьової ОС віртуальної машини. Потім Veeam Data Mover стискає дані ВМ і транспортує їх до кінцевого пристрою Veeam Data Mover. Після того, як проксі-сервер завершує зчитування даних ВМ, Veeam Backup & Replication запитує сервер vCenter Server або хост ESXi, щоб зафіксувати знімок ВМ.

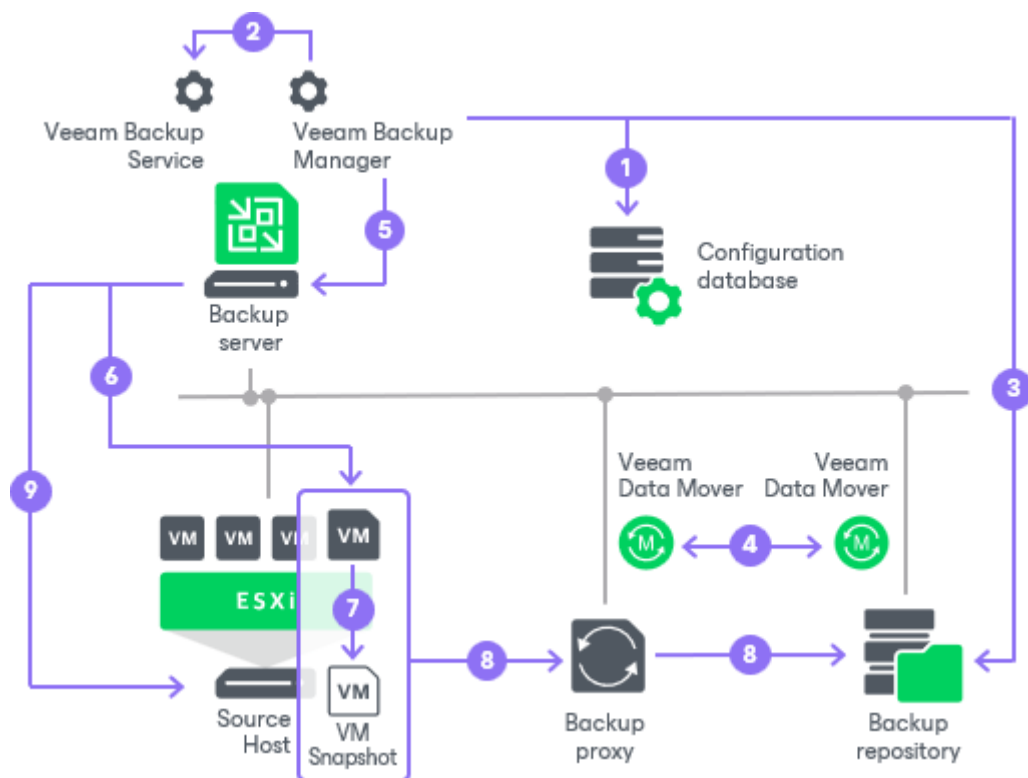


Рисунок 2.1 Виконання резервного копіювання Veeam

2.1. Відновлення за допомогою Veeam

Відновлення за допомогою Veeam: виконання відновлення з файлів резервних копій в оригінальне або нове місце. Veeam Backup & Replication пропонує ряд варіантів відновлення для різних сценаріїв аварійного відновлення, включаючи миттєве відновлення, відновлення на рівні образів, відновлення на рівні файлів, відновлення елементів додатків тощо.

Відновлення віртуальних машин - відновлення цілих віртуальних машин до різних середовищ захисту даних: VMware vSphere, Hyper-V, Amazon EC2 тощо.

Миттєве відновлення до VMware vSphere - миттєве відновлення робочих навантажень (віртуальних машин, екземплярів EC2, фізичних серверів тощо) безпосередньо зі стиснених і дедуплікованих файлів резервних копій у вигляді віртуальних машин VMware vSphere. Під час виконання миттєвого відновлення Veeam Backup & Replication монтує відновлені образи віртуальних машин на хост безпосередньо з резервних копій, що зберігаються в сховищах резервних копій. Миттєве відновлення допомагає поліпшити показники часу відновлення (RTO), мінімізувати збої та простої виробничих робочих навантажень. Однак Instant Recovery створює «тимчасові резервні копії» віртуальних машин з обмеженою продуктивністю вводу/виводу. Щоб забезпечити повну продуктивність вводу/виводу відновлених віртуальних машин, необхідно завершити миттєве відновлення - перенести відновлені віртуальні машини у виробниче середовище. Якщо ви не хочете мігрувати відновлену VM, ви можете припинити її публікацію. Це призведе до видалення відновленої віртуальної машини.

Використовуйте миттєве відновлення для віртуальних машин рівня 1 з низькою толерантністю до переривання роботи і простоїв. Окрім аварійного відновлення, Instant Recovery також можна використовувати для тестування.

За допомогою Instant Recovery to VMware vSphere можна миттєво відновити різні робочі навантаження (віртуальні машини, екземпляри EC2, фізичні сервери тощо) як віртуальні машини VMware vSphere. Миттєве відновлення в VMware vSphere може бути корисним, наприклад, якщо потрібно перенести інфраструктуру з одного середовища в інше або відновити інфраструктуру за лічені хвилини, але з обмеженою продуктивністю.

Під час відновлення Veeam Backup & Replication запускає робочі навантаження безпосередньо зі стиснених і дедуплікованих файлів резервних копій. Це допомагає поліпшити показники часу відновлення (RTO), мінімізувати збої і час простою виробничих робочих навантажень. Робочі навантаження відновлюються за лічені хвилини.

У ході виконання миттєвого відновлення Veeam Backup & Replication монтує образи робочих навантажень на хост безпосередньо з резервних копій, що зберігаються в сховищах резервних копій. Це означає, що Veeam Backup & Replication створює повнофункціональні «тимчасові резервні копії» з обмеженою продуктивністю вводу-виводу. Окрім аварійного відновлення, Instant Recovery також можна використовувати для тестування. Замість того, щоб витягувати образи робочих навантажень у виробниче сховище для регулярного тестування аварійного відновлення (DR), можна запустити робоче навантаження безпосередньо з файлу резервної копії, завантажити його і переконатися, що гостьова ОС і програми функціонують належним чином.

Миттєве відновлення в Microsoft Hyper-V - для миттєвого відновлення робочих навантажень безпосередньо зі стислих і дедуплікованих файлів резервних копій у вигляді віртуальних машин Microsoft Hyper-V. Багато в чому цей метод схожий на Instant Recovery to VMware vSphere. За допомогою Instant Recovery to Microsoft Hyper-V можна миттєво відновити різні робочі навантаження (віртуальні машини, екземпляри EC2, фізичні сервери тощо) як віртуальні машини Microsoft Hyper-V. Миттєве відновлення в Microsoft Hyper-V може бути корисним, наприклад, якщо потрібно перенести інфраструктуру з одного середовища в інше або відновити інфраструктуру за лічені хвилини, але з обмеженою продуктивністю.

В процесі відновлення Veeam Backup & Replication запускає робочі навантаження безпосередньо зі стиснених і дедуплікованих файлів резервних копій. Це допомагає поліпшити показники часу відновлення (RTO), мінімізувати збої і простої виробничих робочих навантажень. Робочі навантаження відновлюються за лічені хвилини.

В процесі виконання миттєвого відновлення Veeam Backup & Replication створює фіктивні віртуальні машини і монтує на них диски робочих навантажень безпосередньо з резервних копій, що зберігаються в сховищах резервних копій. Ці фіктивні віртуальні машини мають обмежену продуктивність вводу-виводу. Щоб

забезпечити повну продуктивність вводу/виводу, необхідно перенести віртуальні машини на робочий сервер.

Окрім аварійного відновлення, миттєве відновлення також можна використовувати для тестування. Замість того, щоб витягувати робочі навантаження у робоче сховище для регулярного тестування аварійного відновлення (DR), можна запустити робоче навантаження безпосередньо з файлу резервної копії, завантажити його і переконатися, що гостьова ОС і додатки працюють належним чином. Миттєве відновлення підтримує масову обробку, тому можна миттєво відновити кілька робочих навантажень одночасно. Якщо виконується миттєве відновлення для кількох робочих навантажень, Veeam Backup & Replication використовує механізм планування ресурсів, щоб розподілити та використати оптимальні ресурси, необхідні для миттєвого відновлення. Докладні відомості див. в розділі Планування ресурсів.

Як працює миттєве відновлення в Microsoft Hyper-V.Veeam Backup & Replication зчитує конфігурацію робочого навантаження з файлу резервної копії в сховищі резервних копій і створює фіктивну віртуальну машину з порожніми дисками на цільовому хості. Перед створенням фіктивної VM Veeam Backup & Replication аналізує конфігурацію робочого навантаження і приймає рішення про генерацію для цієї VM: Якщо Veeam Backup & Replication виявляє системний розділ EFI, створюється віртуальна машина покоління 2.

Якщо Veeam Backup & Replication виявляє завантажувальний розділ BIOS, створюється віртуальна машина 1-го покоління.Якщо Veeam Backup & Replication виявляє хоча б один розділ GPT, створюється віртуальна машина 2 покоління.В інших випадках Veeam Backup & Replication створює віртуальну машину 1-го покоління.В інших аспектах створена VM має ті самі налаштування, що й робоче навантаження у файлі резервної копії. Якщо вибрано попередній розподіл дискового простору для відновлених VM, Veeam Backup & Replication попередньо розподіляє дисковий простір на початку процесу миттєвого відновлення.

Veeam ініціює створення захисного знімка для фіктивної віртуальної машини, після чого віртуальна машина запускається. Якщо процес миттєвого відновлення з якихось причин завершиться невдачею, захисний знімок гарантує, що дані не будуть втрачені. У сховищі резервних копій і на цільовому хості Veeam Backup & Replication запускає дві пари Veeam Data Movers, які використовуються для монтування дисків віртуальної машини з файлу резервної копії на фіктивну віртуальну машину.

На цільовому хості Veeam запускає власний драйвер Veeam. Драйвер перенаправляє запити до файлової системи відновленої ВМ (наприклад, коли користувач звертається до якоїсь програми) і зчитує необхідні дані з файлу резервної копії в сховищі резервних копій за допомогою пари Veeam Data Movers, які підтримують монтування дисків. Міграція відновлених віртуальних машин на робочий сервер. Коли починається процес міграції, Veeam Backup & Replication запускає ще одну пару Veeam Data Movers - один Veeam Data Mover у сховищі резервних копій і один на цільовому хості. Ця пара Veeam Data Movers у фоновому режимі копіює дані відновленої віртуальної машини зі сховища резервних копій на цільовий хост і заповнює диски віртуальної машини, запущеної на цільовому хості.

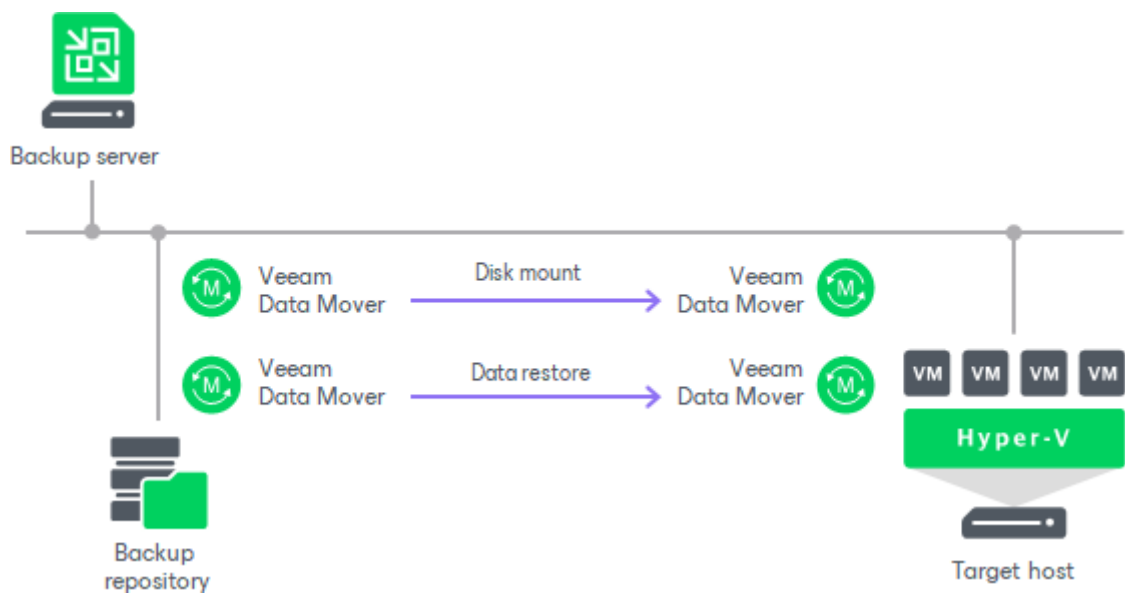


Рисунок 2.2 Як працює миттєве відновлення в Microsoft Hyper-V

Драйвер на цільовому хості знає, які дані вже були відновлені назавжди, і не перенаправляє запити до таких даних, зчитуючи їх безпосередньо з дисків відновленої віртуальної машини. Таким чином, продуктивність миттєво відновленої VM буде зростати по мірі копіювання більшої кількості даних. Коли віртуальна машина буде повністю відновлена, всі служби Veeam Data Movers зупиняються.

Instant Recovery to Nutanix AHV - миттєве відновлення робочих навантажень безпосередньо зі стислих і дедуплікованих файлів резервних копій у вигляді віртуальних машин Nutanix AHV. Зверніть увагу, що для відновлення в Nutanix AHV на сервері резервного копіювання необхідно встановити плагін Nutanix AHV Plug-in. Докладнішу інформацію див. в розділі «Встановлення» в посібнику користувача Veeam Backup for Nutanix AHV. Під час виконання миттєвого відновлення Veeam Backup for Nutanix AHV монтує образ робочого навантаження на сервер монтування безпосередньо зі стисненого та дедуплікованого файлу резервної копії. Оскільки немає необхідності витягувати робоче навантаження з файлу резервної копії та копіювати його у робоче сховище, можна виконати відновлення з будь-якої точки відновлення за лічені хвилини.

Образ робочого навантаження залишається в стані «тільки для читання», щоб уникнути несподіваних модифікацій. За замовчуванням, всі зміни на віртуальних дисках, які відбуваються під час роботи відновленого робочого навантаження, реєструються у допоміжних файлах журналу повторних дій, що знаходяться в кластері Nutanix AHV. Ці зміни або об'єднуються, якщо робоче навантаження буде перенесено у виробниче середовище, або відкидаються, якщо операція відновлення буде скасована.

Відновлення всієї віртуальної машини - відновлення всієї віртуальної машини. Під час відновлення віртуальних машин ви витягуєте образи віртуальних машин з резервних копій у робоче сховище. Повне відновлення віртуальної машини вимагає

більше ресурсів і часу, ніж миттєве відновлення, але відновлює віртуальні машини з повною продуктивністю вводу/виводу. За допомогою Veeam можна відновити цілу віртуальну машину з файлу резервної копії до попереднього стану або до попереднього моменту часу, якщо оригінальна віртуальна машина вийшла з ладу. Під час відновлення всієї віртуальної машини Veeam витягує образ віртуальної машини з резервної копії у робоче сховище, потім Veeam витягує дані віртуальної машини зі сховища резервних копій у вибране сховище, реєструє віртуальну машину на обраному хості ESXi і, якщо необхідно, вмикає її.

Повне відновлення VM забезпечує повну продуктивність дискового вводу/виводу, в той час як миттєве відновлення забезпечує «тимчасовий резерв» для віртуальної машини, оскільки пропускна здатність vPower NFS обмежена.

Як працює повне відновлення віртуальної машини. Віртуальну машину можна відновити у вихідне або нове місце розташування. Якщо відновити VM у вихідне місце розташування, Veeam вимкне вихідну VM і відновить лише ті диски, які містяться у файлі резервної копії. Всі інші диски залишаються без змін.

При відновленні віртуальної машини в нове місце можна вказати нові параметри віртуальної машини, такі як нове ім'я VM, хост і сховище даних, де буде розміщена віртуальна машина, формат диска (тонкий або товстий резерв) і мережеві властивості. Veeam змінить конфігураційний файл віртуальної машини та збереже дані VM у вибраному місці.

Щоб виконати повне відновлення VM, Veeam використовує один з наступних транспортних режимів: якщо проксі-сервер резервного копіювання підключений безпосередньо до мережі SAN або має доступ до сховищ даних NFS, Veeam використовує транспортний режим прямого доступу до сховища. Veeam Data Movers, розгорнуті на сховищі резервних копій і проксі-сервері резервного копіювання, отримують дані VM з файлу резервної копії і поміщають їх безпосередньо в потрібне сховище даних. Коли Veeam відновлює VM, вона

виконує циклічну перевірку надмірності (CRC) для TCP-трафіку, що проходить між Veeam Data Movers, встановленими на сховищі резервних копій і проксі-сервері резервного копіювання. Це відбувається за умови, що в налаштуваннях мережевого трафіку ввімкнено багатопотокову передачу даних. Veeam обчислює і порівнює контрольні суми для блоків даних, що надходять з вихідного Veeam Data Mover, і блоків даних, отриманих на цільовий Veeam Data Mover. Якщо перевірка CRC не спрацьовує, Veeam Backup & Replication автоматично повторно надсилає блоки даних без жодного впливу на завдання відновлення.

Якщо проксі-сервер резервного копіювання віртуалізований і знаходиться на хості ESXi, на який потрібно відновити віртуальну машину, Veeam використовує режим транспортування Virtual appliance. Режим Virtual appliance використовує можливості VMware ESXi щодо швидкого додавання дисків до віртуальної машини і, таким чином, усуває необхідність передавати дані резервного копіювання через мережу. Veeam Data Movers, розгорнуті в сховищі резервних копій і проксі-сервері резервного копіювання, отримують дані віртуальної машини з файлу резервної копії і поміщають їх безпосередньо в потрібне сховище даних через стек вводу/виводу ESXi.

Якщо неможливо використовувати режими прямого доступу до сховища і транспортування через віртуальний пристрій, Veeam Backup & Replication використовує режим мережевого транспортування.

Поетапне відновлення - запуск виконуваних сценаріїв для VM перед відновленням у виробниче середовище. Поетапне відновлення є частиною повного відновлення VM. Поетапне відновлення дозволяє запустити виконуваний сценарій для віртуальних машин перед тим, як відновити їх у робоче середовище. Поетапне відновлення є частиною всієї операції відновлення віртуальних машин. Щоб виконати поетапне відновлення, необхідно вибрати режим поетапного відновлення у майстрі повного відновлення VM і вказати параметри поетапного відновлення.

Поетапне відновлення може допомогти переконатися, що відновлені віртуальні машини не містять ніяких особистих або конфіденційних даних. Наприклад, можна доручити Veeam запустити сценарій Windows PowerShell, який видалить користувачів Active Directory:

```
$UserName = "John.Smith"
$ADUser = Get-ADUser -Filter 'Name -like $UserName'
if (!$ADUser)
{
    [Environment]::Exit(1)
}
Remove-ADUser -Identity $UserName -Confirm:$false
```

Рисунок:2.3 Сценарій видалення всіх користувачів з Active Directory

Під час відновлення VM Veeam Backup & Replication використовує метод Veeam Quick Migration. Методи vMotion і Storage vMotion використовувати не можна. Докладні відомості про метод швидкої міграції див. в статті Швидка міграція.

Як працює поетапне відновлення. Для поетапного відновлення Veeam використовує попередньо налаштовану віртуальну лабораторію, виконуваний сценарій, розташований на сервері резервного копіювання, і облікові дані для підключення до віртуальних машин і запуску сценарію. Veeam виконує поетапне відновлення наступним чином:

У віртуальній лабораторії Veeam запускає віртуальні машини безпосередньо зі стиснених і дедуплікованих файлів резервних копій, які знаходяться в сховищі резервних копій. Для цього Veeam Backup & Replication використовує службу Veeam vPower NFS.

Якщо для запуску сценарію вибрано групу додатків, Veeam спочатку запускає віртуальні машини з групи додатків у потрібному порядку. Veeam копіює сценарій із сервера резервного копіювання на VM, які планується відновити.

Для підключення до віртуальних машин Veeam використовує облікові дані, вказані в налаштуваннях поетапного відновлення.

Veeam запускає скопійований сценарій на кожній VM.

Для запуску сценарію Veeam використовує ту саму технологію, що й для сценаріїв попереднього блокування та відновлення.

Усі зміни VM, які відбуваються під час виконання сценарію, записуються в дельта-файли VM.

За замовчуванням Veeam зберігає дельта-файли на сервері vPower NFS. Можна змінити місце призначення для дельта-файлів VM у налаштуваннях віртуальної лабораторії.

Після завершення виконання сценарію Veeam виконує безпечне завершення роботи віртуальних машин у віртуальній лабораторії.

Veeam відновлює віртуальні машини у зміненому стані у робочому середовищі.

Для цього Veeam Backup & Replication копіює дані VM зі сховища резервних копій і дельта-файлів на цільовий хост за допомогою Veeam Quick Migration.

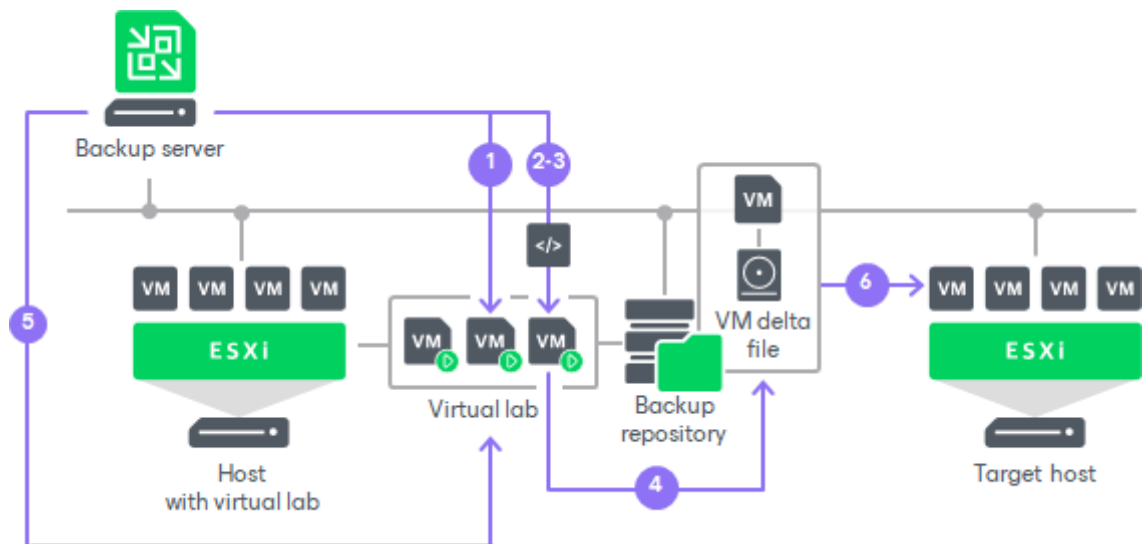


Рисунок 2.4 Поетапне відновлення в Veeam

Відновлення в Amazon EC2 - відновити робочі навантаження різних середовищ захисту даних як екземпляри EC2. Veeam дозволяє відновлювати різні робочі навантаження (віртуальні машини, екземпляри Google VM, фізичні сервери тощо) в Amazon Elastic Compute Cloud (Amazon EC2) як екземпляри EC2. Екземпляр EC2 - це віртуальна машина в Amazon EC2 з попередньо налаштованою комбінацією обчислювальних ресурсів. За допомогою Veeam можна виконувати такі операції: відновлення робочих навантажень в Amazon EC2 з резервних копій. Перенесення робочих навантажень з локальної інфраструктури в хмару. Створювати тестове середовище в хмарі для усунення несправностей, тестування патчів і оновлень тощо.

Відновлення в Microsoft Azure - відновити робочі навантаження з різних середовищ захисту даних у вигляді віртуальних машин Microsoft Azure. Veeam можна використовувати для виконання таких завдань: відновлення робочих навантажень з резервних копій Veeam у Microsoft Azure. Перенесення робочих навантажень з локальної інфраструктури в хмару. Створення тестового середовища в хмарі для усунення несправностей, тестування виправлень і оновлень тощо.

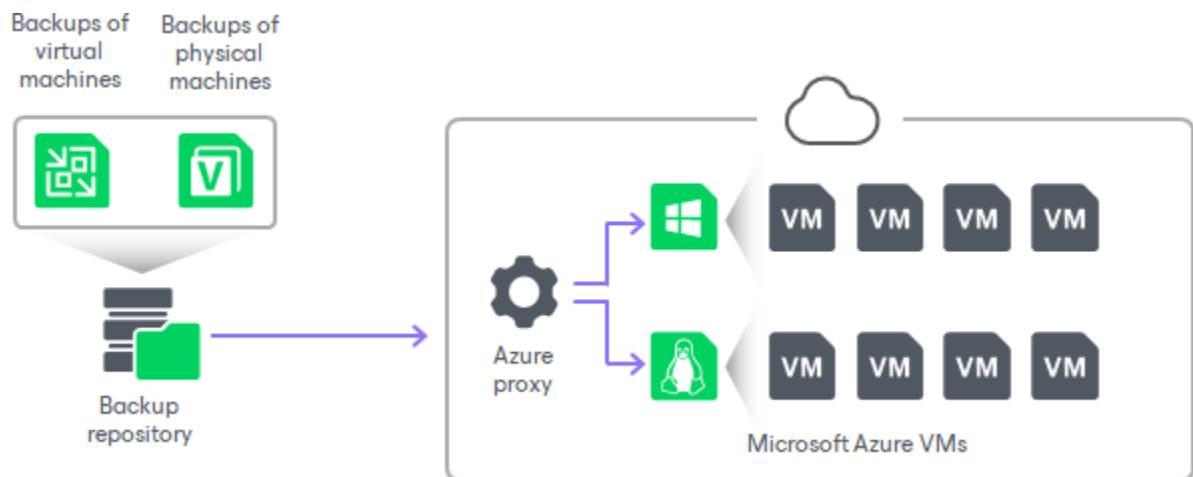


Рисунок 2.5 Відновлення резервних копій в Microsoft Azure

Відновити в Google Compute Engine (GCE) - відновити робочі навантаження різних середовищ захисту даних як екземпляри Google VM. За допомогою Veeam

можна виконати такі операції: відновлення комп'ютерів у Google Compute Engine з резервних копій. Перенести машини з локальної інфраструктури в хмару. Створити в хмарі тестове середовище для усунення несправностей, тестування виправлень і оновлень тощо.

Відновлення в Nutanix AHV - відновити робочі навантаження різних середовищ захисту даних як VM Nutanix AHV. У разі аварії можна відновити всю віртуальну машину Nutanix AHV з резервної копії або знімка. Veeam Backup для Nutanix AHV дозволяє відновлювати одну або кілька віртуальних машин за раз, у вихідне або нове місце розташування.

Підтримувані робочі навантаження. Для відновлення машин у кластері Nutanix AHV можна використовувати такі резервні копії та знімки: знімки PD Nutanix AHV, створені за допомогою Veeam Backup для Nutanix AHV. Знімки віртуальних машин Nutanix AHV, створені за допомогою Veeam Backup для Nutanix AHV. Резервні копії VM Nutanix AHV, створені Veeam Backup для Nutanix AHV (включаючи VM з підключеними групами томів і VM без підключених дисків). Резервні копії віртуальних машин Microsoft Hyper-V і VMware vSphere, створені за допомогою Veeam. Резервні копії віртуальних і фізичних машин, створені за допомогою Veeam Agent для Microsoft Windows і Veeam Agent для Linux. Резервні копії віртуальних машин, створених за допомогою vCloud Director. Резервні копії екземплярів Amazon EC2, створені за допомогою Veeam Backup for AWS. Резервні копії віртуальних машин Microsoft Azure, створені за допомогою Veeam Backup for Microsoft Azure. Резервні копії екземплярів віртуальних машин Google Cloud, створені за допомогою Veeam Backup for Google Cloud. Резервні копії oVirt KVM VM, створені Veeam Backup для Oracle Linux Virtualization Manager і Red Hat Virtualization. Резервні копії віртуальних машин Proxmox VE, створені Veeam Backup для Proxmox VE. Відновлення віртуальних машин підтримується лише для знімків, що зберігаються в кластері Nutanix AHV, а також для резервних копій, що зберігаються в сховищах резервних копій, об'єктних сховищах і на рівні

продуктивності, ємності та архіву масштабованого сховища резервних копій (за винятком резервних копій, що зберігаються на рівні архіву, який складається зі сховища Amazon S3 Glacier Instant Retrieval; для цих резервних копій можна виконати миттєве відновлення).

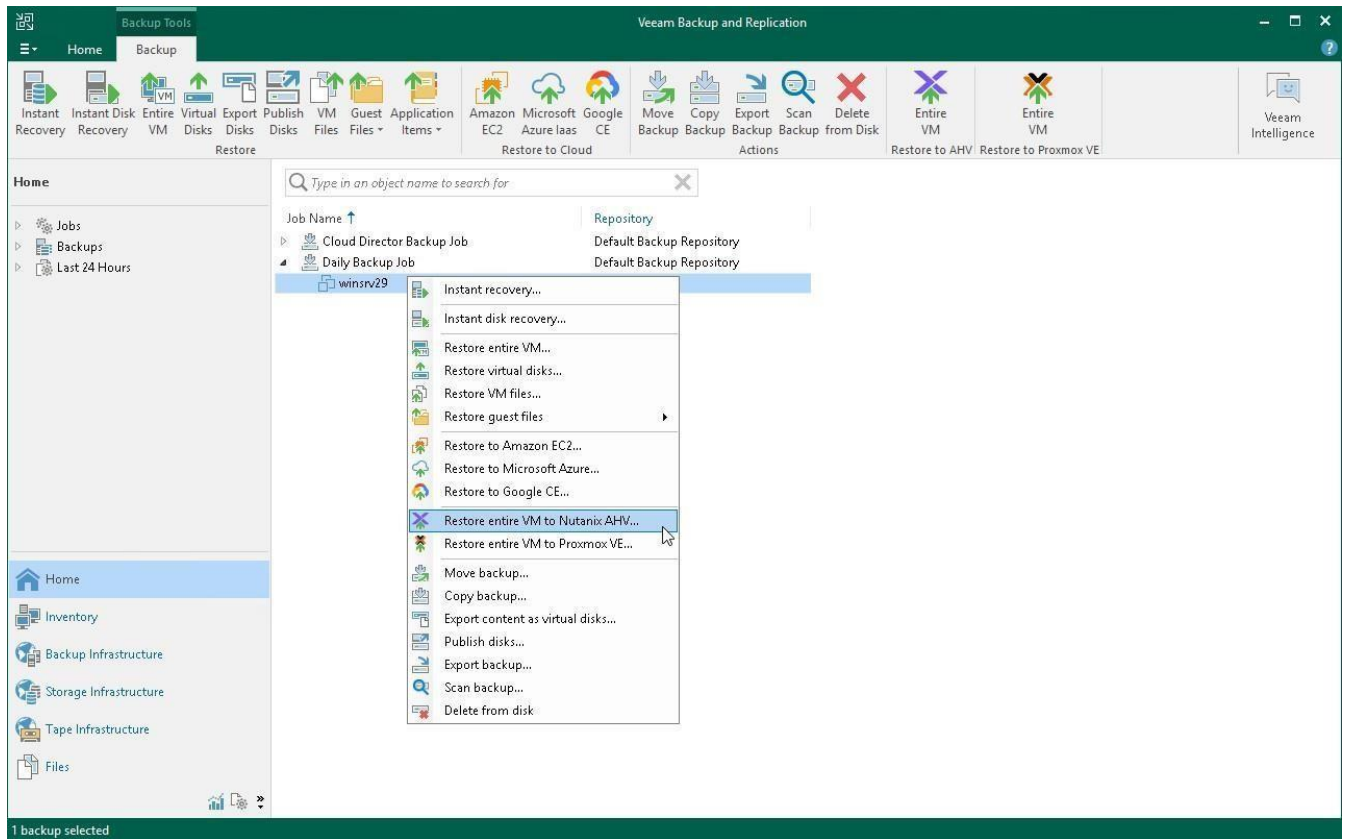


Рисунок 2.5 Відновлення Nutanix AHV в vVeeam

Відновлення в Proxmox VE - відновити робочі навантаження різних середовищ захисту даних як віртуальні машини Proxmox VE. У разі аварії можна відновити всю віртуальну машину Proxmox VE з резервної копії. Veeam Backup для Proxmox VE дозволяє відновити одну або кілька віртуальних машин за раз, у вихідне або нове місце розташування. Щоб відновити машини в Proxmox VE, можна використовувати наступні резервні копії: Резервні копії віртуальних машин Proxmox VE, створені за допомогою Veeam Backup для Proxmox VE. Резервні копії віртуальних машин Nutanix AHV, створені за допомогою Veeam Backup для Nutanix AHV. Резервні копії oVirt KVM VM, створені Veeam Backup для Oracle Linux Virtualization Manager і Red Hat Virtualization. Резервні копії віртуальних

машин Microsoft Hyper-V і VMware vSphere, створені Veeam.Резервні копії віртуальних машин, створених за допомогою vCloud Director.Резервні копії екземплярів Amazon EC2, створені за допомогою Veeam Backup for AWS.Резервні копії віртуальних машин Microsoft Azure, створені за допомогою Veeam Backup for Microsoft Azure.Резервні копії екземплярів віртуальних машин Google Cloud, створені за допомогою Veeam Backup for Google Cloud.Резервні копії віртуальних і фізичних машин, створені за допомогою Veeam Agent для Microsoft Windows і Veeam Agent для Linux

Відновлення віртуальних машин підтримується лише для резервних копій, що зберігаються в сховищах резервних копій, об'єктних сховищах і на рівні продуктивності, ємності та архіву масштабованого сховища резервних копій (за винятком резервних копій, що зберігаються на рівні архіву, який складається зі сховища Amazon S3 Glacier Instant Retrieval).

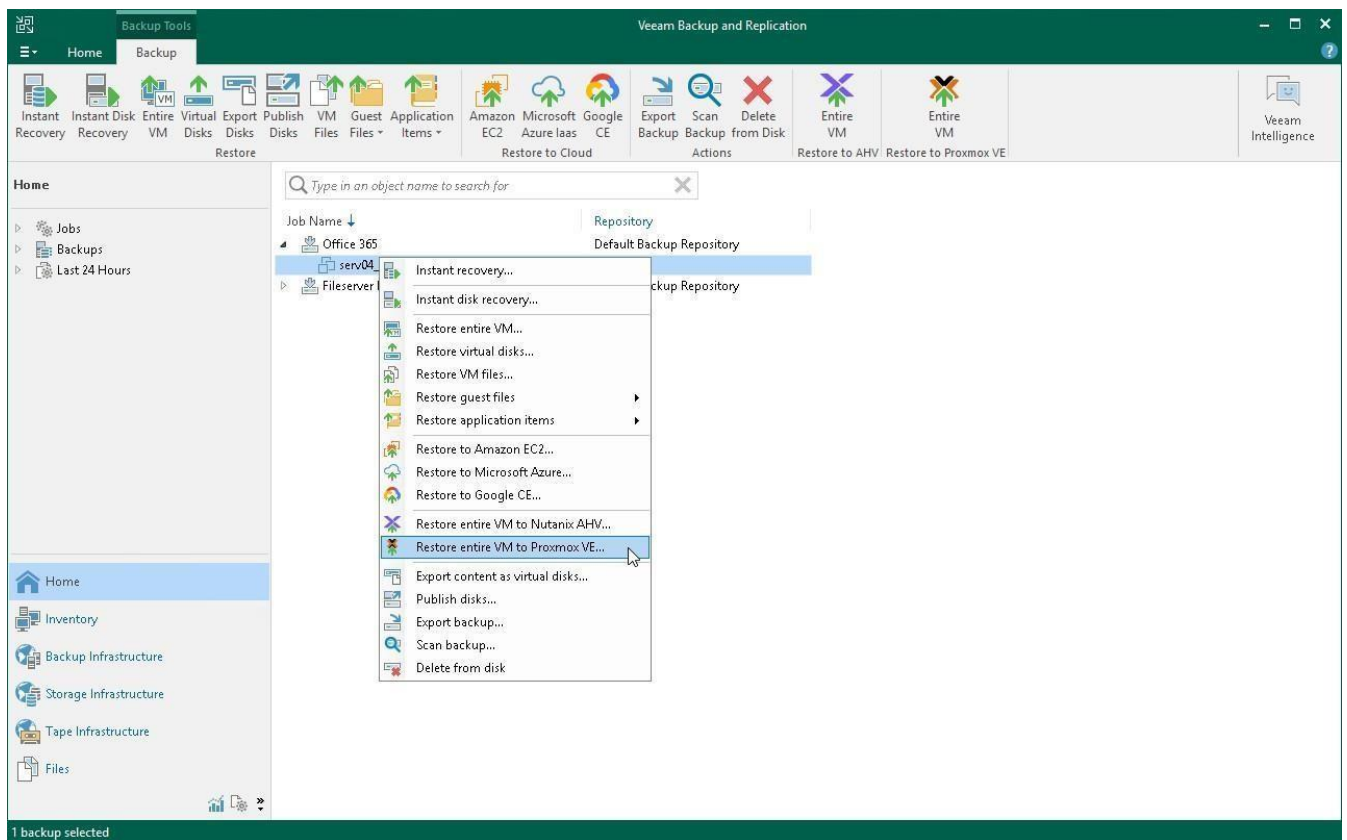


Рисунок 2.6 Відновлення Proxmox VE в Veeam

Відновлення OLVM і RHV - можна відновити робочі навантаження різних середовищ захисту даних як VM OLVM і RHV.

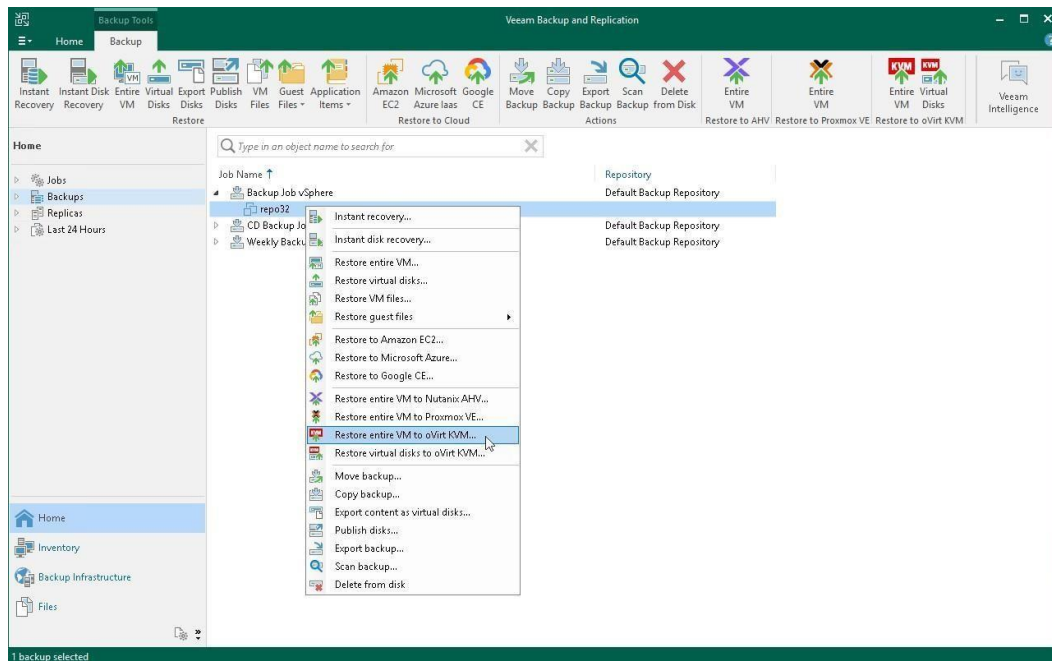


Рисунок 2.6 Відновлення OLVM в Veeam

2.2. Реплікація у Veeam

Реплікація у Veeam: створення точної копії віртуальної машини та підтримка синхронізації копії з оригінальною віртуальною машиною. Безперервний захист даних (CDP): технологія реплікації, яка допомагає захистити критично важливі VM і досягти точки відновлення (RPO) за лічені секунди. Реплікація - це технологія, яка допомагає захистити критично важливі віртуальні машини VMware. Під час реплікації віртуальної машини Veeam створює точну копію віртуальної машини у власному форматі VMware vSphere на цільовому хості. Veeam Backup & Replication підтримує цю копію синхронізованою з вихідною віртуальною машиною. Реплікація забезпечує мінімальний час відновлення (RTO) у разі аварії, оскільки репліки VM перебувають у стані готовності до запуску. Рекомендується реплікувати віртуальні машини, для яких потрібен час відновлення, що обчислюється годинами. Якщо вам потрібна RPO в секундах, варто розглянути можливість безперервного захисту даних (CDP).

Для реплікації віртуальних машин Veeam Backup & Replication використовує можливості моментальних знімків VMware vSphere. Під час реплікації Veeam звертається до VMware vSphere із запитом на створення знімка віртуальної машини. Знімок віртуальної машини можна розглядати як копію віртуальної машини в певний момент часу, яка включає віртуальні диски, стан системи, конфігурацію тощо. Veeam використовує знімок як джерело даних для реплікації.

Під час першого циклу реплікації Veeam копіює дані вихідної віртуальної машини, що працює на вихідному хості, і створює її повну репліку на цільовому хості. На відміну від файлів резервних копій, віртуальні диски реплік зберігаються в розпакованому вигляді у вихідному форматі. Всі наступні цикли реплікації є інкрементними. Veeam копіює тільки ті блоки даних, які змінилися з моменту останнього сеансу реплікації. Для відстеження змінених блоків даних Veeam використовує різні підходи.

Щоб виконати інкрементне резервне копіювання, V має знати, які блоки даних змінилися з моменту попереднього сеансу роботи.

Для віртуальних машин VMware з апаратним забезпеченням версії 7 і вище Veeam використовує вбудовану функцію VMware vSphere - VMware vSphere Changed Block Tracking (CBT). Замість сканування VMware VMFS (файлової системи віртуальної машини) Veeam запитує CBT через VMware VADP (VMware vStorage API for Data Protection) і отримує список блоків, які були змінені з моменту останнього сеансу роботи. Використання CBT підвищує швидкість і ефективність інкрементного резервного копіювання на рівні блоків.



Рисунок 2.7 Як працює інкрементальне резервне копіювання в Veeam

використовує СВТ для таких операцій:

- Резервне копіювання
- Реплікація
- Відновлення всієї ВМ
- Відновлення диска ВМ

Veeam вмикає СВТ за замовчуванням. За потреби її можна вимкнути в налаштуваннях завдання.

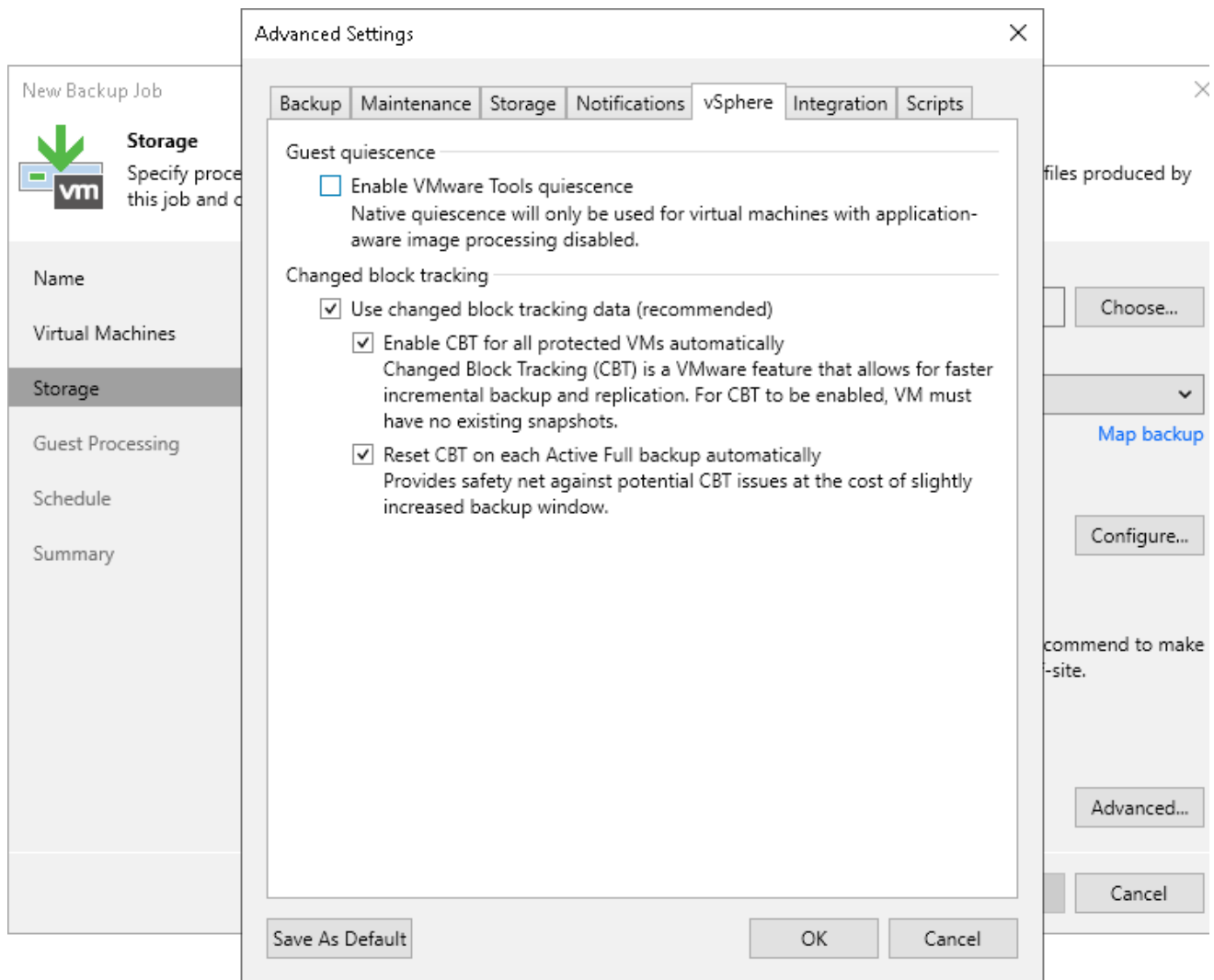


Рисунок 2.8 Налаштування в розділі vSphere

У деяких ситуаціях Veeam не може використовувати VMware vSphere CBT, наприклад, якщо на віртуальних машинах використовується більш рання

версія віртуального обладнання. Якщо Veeam не може використовувати VMware vSphere CBT, він переходить на власний механізм фільтрації Veeam. Замість того, щоб відстежувати змінені блоки даних, Veeam відфільтровує незмінні блоки даних.

Під час обробки віртуальних машин Veeam консолідує вміст віртуальних дисків, сканує образ віртуальної машини та обчислює контрольну суму для кожного блоку даних. Контрольні суми зберігаються як метадані у файлах резервних копій поруч із даними віртуальних машин. Під час запуску інкрементного резервного копіювання Veeam відкриває всі файли резервних копій у ланцюжку попередніх повних та інкрементних резервних копій, зчитує метадані з цих файлів і порівнює їх з контрольними сумами, розрахованими для віртуальної машини в її поточному стані. Якщо знайдено збіг (що означає, що блок вже існує в резервній копії), цей блок відфільтровується.

Veeam дозволяє виконувати локальну реплікацію для сценаріїв високої доступності та віддалену реплікацію для сценаріїв аварійного відновлення. Щоб полегшити реплікацію через глобальну мережу або повільні з'єднання, Veeam оптимізує передачу трафіку. Воно відфільтровує непотрібні блоки даних, такі як дублікати, нульові блоки, блоки файлів підкачки та блоки виключених файлів гостьових ОС віртуальних машин, а також стискає трафік реплікації. Veeam також дозволяє використовувати WAN-прискорювачі та застосовувати правила мережевого дроселювання, щоб завдання реплікації не використовували всю пропускну здатність мережі.

WAN-прискорювачі - це спеціальні компоненти, які Veeam використовує для прискорення роботи в глобальній мережі. WAN-прискорювачі відповідають за глобальне кешування даних і дедуплікацію даних. Технічно WAN-прискорювачі додають новий рівень в інфраструктуру резервного копіювання - між Veeam Data Movers на стороні джерела та Veeam Data Mover на стороні призначення.

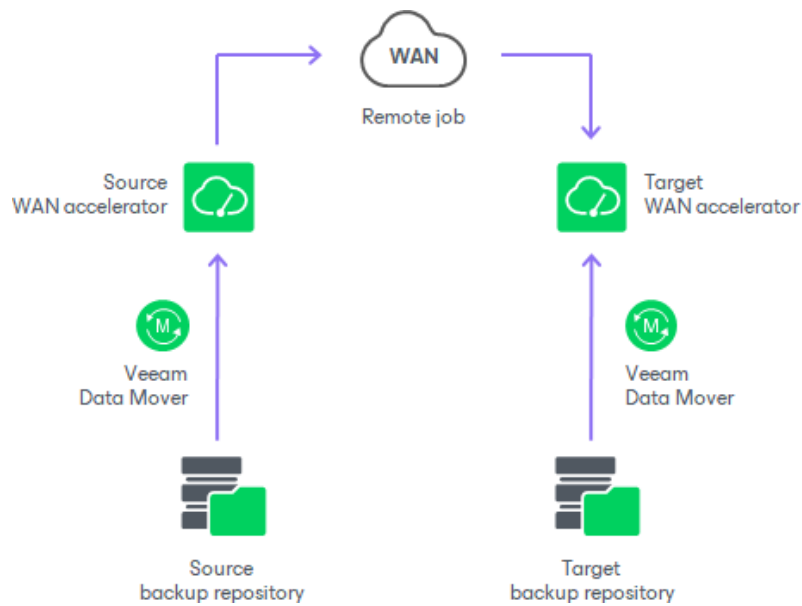


Рисунок 2.9 Робота WAN-прискорювачів в Veeam

Розгортання WAN-прискорювачів. Щоб увімкнути технології WAN-прискорення та дедуплікації даних, в інфраструктурі резервного копіювання потрібно розгорнути пару WAN-прискорювачів. Один WAN-прискорювач розгортається на сайті-джерелі, ближче до вихідного сховища резервних копій або вихідного хоста. Інший WAN-прискорювач розгортається на цільовому сайті, ближче до цільового сховища резервних копій або цільового хоста. На кожному WAN-прискорювачі Veeam Backup & Replication створює папку VeeamWAN, яка містить такі дані:

Папка VeeamWAN на вихідному WAN-прискорювачі зберігає файли з дайджестами, необхідними для дедуплікації. Для отримання додаткової інформації див. статтю Як працює WAN-прискорення. Папка VeeamWAN на цільовому WAN-прискорювачі зберігає дані глобального кешу.

Як працює WAN-прискорення. Коли створюється завдання на віддалену локацію, у його властивостях можна вибрати використання WAN-прискорення. Процедура копіювання даних з увімкненим WAN-прискоренням виконується наступним чином: [Для завдання резервного копіювання] Veeam Backup & Replication розпаковує файл резервної копії, щоб проаналізувати його вміст. Служба Veeam WAN Accelerator на вихідному WAN-прискорювачі аналізує

блоки даних файлу, що передається, і створює файл з дайджестами для цих блоків даних.

Створений файл з дайджестами зберігається в папці VeeamWAN на вихідному WAN-прискорювачі.

Veeam Backup & Replication стискає дані файлу резервної копії (для резервної копії) або дані віртуальної машини (для реплікації) і копіює їх на цільову сторону. Під час наступного циклу роботи служба Veeam WAN Accelerator Service на вихідному WAN-прискорювачі аналізує блоки даних у файлі, які повинні бути передані цього разу, і створює дайджести для цих блоків даних. Служба Veeam WAN Accelerator порівнює створені дайджести з дайджестами, які були раніше збережені в папці VeeamWAN на вихідному WAN-прискорювачі.

Якщо виявлено дублікати блоків даних, то фактичний блок даних у файлі резервної копії не копіюється через мережу WAN. Замість цього він береться з глобального кешу і записується в точку відновлення в папці резервної копії або на цільовому томі даних.

Крім того, Veeam Backup & Replication аналізує точки відновлення, які були раніше скопійовані на цільову сторону. Якщо виявляються дублікати, Veeam Backup & Replication не копіює такі блоки через WAN, а бере їх з раніше скопійованих точок відновлення. В результаті Veeam копіює на цільову сторону тільки нові блоки даних і використовує блоки даних, які вже зберігаються в глобальному кеші або в точках відновлення в цільовому сховищі резервних копій.

Якщо цільовий WAN-прискорювач використовується кількома робочими місцями, цільове сховище резервних копій може вже містити блоки даних потрібного типу (наприклад, в резервному сховищі), то Veeam не копіює такі блоки через глобальну мережу, а тягне їх на цільовий сервер. У цій ситуації Veeam Backup & Replication скопіює необхідні блоки даних до глобального кешу перед початком

процесу копіювання і використовуватиме їх у подальшому. Докладні відомості див. в статті Прискорення WAN з багатьох до одного.

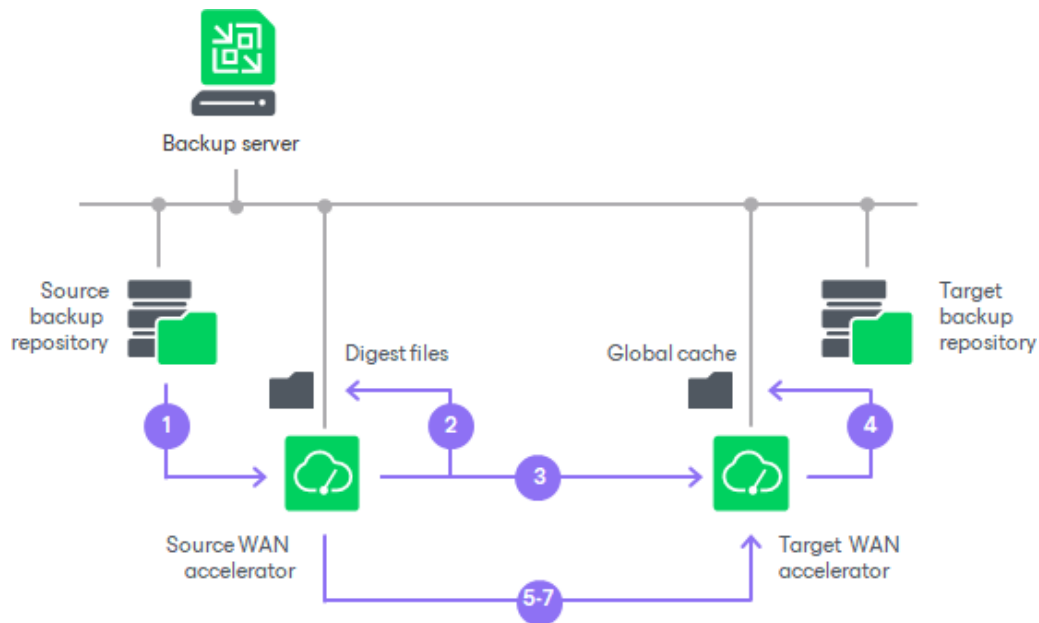


Рисунок 2.10 Схема роботи Wan-accelerator

Якщо WAN-прискорення виконується в режимі Високої пропускної здатності, то процедура передачі даних з WAN-прискоренням має наступні особливості: глобальний кеш не використовується. Таким чином, цільовий WAN-прискорювач не потребує додаткового дискового простору для зберігання папки глобального кешу.

Дедуплікація виконується тільки з використанням попередніх точок відновлення для оброблюваної ВМ на цільовому сховищі. Таким чином, Veeam Backup & Replication

виконує менше операцій дедуплікації та економить ресурси і час на обробку даних.

Розмір блоку даних, що використовується механізмом відстеження змінених блоків під час дедуплікації, менший, ніж у режимі низької пропускної здатності. Це зменшує обсяг надлишкових даних для передачі завдань у віддалених місцях, які планується запускати одночасно. Вихідний WAN-прискорювач вимагає багато ресурсів процесора та оперативної пам'яті і не може обробляти кілька завдань паралельно. В якості альтернативи можна створити одне завдання на віддалене розташування для всіх віртуальних машин, які планується обробляти на одному вихідному WAN-прискорювачі.

Однак цільовий WAN-прискорювач можна призначити кільком завданням у віддаленому розташуванні.

Резервне копіювання резервних копій: копіювання файлів резервних копій у вторинне сховище. Основна мета резервного копіювання - захистити дані від катастроф, збоїв у роботі віртуальних або фізичних машин. Однак наявність лише однієї резервної копії не забезпечує необхідного рівня безпеки. Первинна резервна копія може бути знищена разом з робочими даними, і у користувача не залишиться резервних копій, з яких можна буде відновити дані.

Для побудови успішного плану захисту даних і аварійного відновлення рекомендується дотримуватися правила 3-2-1:

3: Необхідно мати принаймні три копії даних: оригінал виробничих даних і дві резервні копії.

2: Для зберігання копій даних необхідно використовувати щонайменше два різних типи носіїв, наприклад, локальний диск і хмарне сховище.

1: Принаймні одну резервну копію необхідно зберігати за межами офісу, наприклад, у хмарі або на віддаленому сервері.

Таким чином, у наявності має бути щонайменше дві резервні копії, і вони повинні знаходитися в різних місцях. Якщо катастрофа знищить робочі дані та локальну резервну копію, їх все одно можна буде відновити з резервної копії, що зберігається на віддаленому сервері.

Щоб допомогти застосувати правило 3-2-1, Veeam Backup & Replication пропонує можливості резервного копіювання. Резервне копіювання дозволяє створювати кілька екземплярів одних і тих самих даних у різних місцях, як на локальному, так і на віддаленому сервері. Резервні копії мають той самий формат, що й ті, що створюються завданнями резервного копіювання, і з них можна відновити дані, коли це буде потрібно.

Резервне копіювання - це процес, керований завданням. Veeam повністю автоматизує процес резервного копіювання і дозволяє задавати параметри збереження, щоб підтримувати потрібну кількість точок відновлення, а також створювати повні резервні копії для архівування.

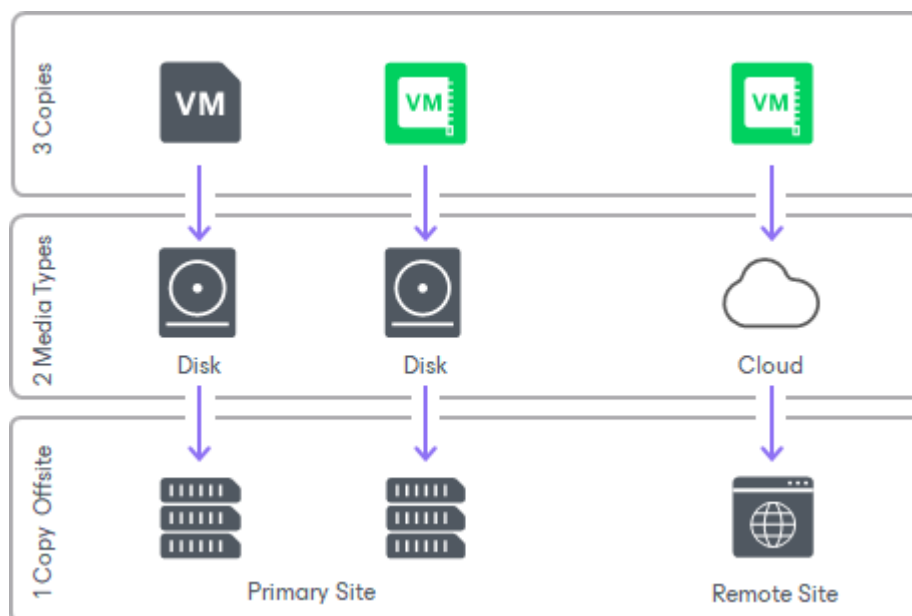


Рисунок 2.11 Схема методу резервного копіювання 3-2-1

Підтримка систем зберігання: резервне копіювання та відновлення віртуальних машин з використанням можливостей нативних знімків, створених на системах зберігання. Докладнішу інформацію можна знайти в Посібнику з інтеграції знімків систем зберігання даних. Підтримка стрічкових пристроїв: зберігання копій резервних копій на стрічкових пристроях.

Перевірка відновлення: тестування резервних копій і реплік віртуальних машин перед відновленням. SureBackup - це технологія Veeam, яка дозволяє тестувати резервні копії машин і перевіряти, чи можна з них відновити дані. Можна перевірити будь-яку точку відновлення резервної копії комп'ютера.

Veeam публікує машини з групи додатків і машину, що перевіряється, в ізольованому середовищі - віртуальній лабораторії. Машини запускаються безпосередньо зі стислих і дедуплікаційних файлів резервних копій, які

знаходяться в сховищі резервних копій. Для цього Veeam використовує службу Veeam vPower NFS. Для SureBackup Veeam Backup & Replication використовує звичайне резервне копіювання на основі образу. Завдання SureBackup може працювати в двох різних режимах перевірки відновлення:

Повне тестування відновлюваності. Veeam запускає машини в ізолюваному середовищі безпосередньо з резервної копії і виконує тести в реальних додатках. Цей режим гарантує відновлюваність виробничих робочих навантажень у разі аварійного відновлення.

Тільки перевірка резервної копії та сканування вмісту. Veeam виконує перевірку цілісності резервної копії та аналіз її вмісту, щоб виявити сліди шкідливого програмного забезпечення або будь-які інші небажані або конфіденційні дані. Ці тести не вимагають створення віртуальної лабораторії або групи додатків.

Тестування повної відновлюваності. Під час перевірки можливості відновлення Veeam Backup & Replication виконує такі дії: якщо завдання SureBackup налаштоване на перевірку та наявність шкідливого програмного забезпечення, Veeam сканує дані машин з групи додатків за допомогою антивірусного програмного забезпечення та вказаного правила YARA. Veeam виконує ряд тестів на машинах у групі додатків і на машині, що перевіряється: тест серцебиття, пінг-тест і тест додатків.

Якщо завдання SureBackup налаштовано на перевірку файлів резервних копій, Veeam виконує циклічну перевірку надмірності для файлу резервної копії, з якого запускається машина, що перевіряється, і, за бажанням, для файлів резервних копій, з яких запускаються машини в групі додатків. Перевірка файлів резервних копій виконується після завершення всіх перевірочних тестів.

Після завершення процесу перевірки відновлення Veeam виводить машини з резервної копії та створює звіт про їхній стан. Звіт надсилається адміністратору резервного копіювання електронною поштою.

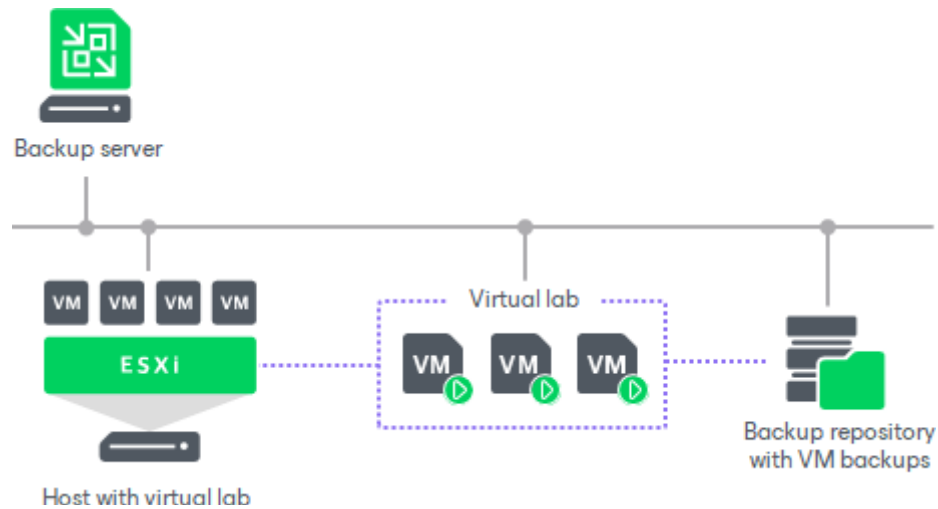


Рисунок 2.12 Повне тестування відновлюваності в Veeam

Під час перевірки резервний образ машини залишається в стані, доступному тільки для читання. Всі зміни, які відбуваються під час роботи машини, записуються у файли журналів повторного виконання, які зберігаються у сховищі даних, вибраному в налаштуваннях віртуальної лабораторії. Після завершення процесу відновлення журнали повторного виконання видаляються.

Щоб виконати перевірку відновлення, потрібно створити наступні об'єкти: група додатків. Під час верифікації відновлення може знадобитися запуск перевіреної машини з групою машин, від яких вона залежить. Група додатків забезпечує повну функціональність додатків, що працюють на машині, і дозволяє запускати ці додатки так само, як у виробничому середовищі. У більшості випадків машина працює не сама по собі, а у взаємодії з іншими сервісами та компонентами. Щоб перевірити таку машину, спочатку потрібно запустити всі служби та компоненти, від яких вона залежить. Для цього Veeam використовує групу додатків.

Група додатків створює «оточення» для машини, що перевіряється. Група додатків містить один або кілька комп'ютерів, від яких залежить машина, що перевіряється. На цих машинах запущені програми і служби, які повинні бути

активовані, щоб забезпечити повнофункціональну роботу машини, що перевіряється. Зазвичай група додатків містить принаймні контролер домену, DNS-сервер і DHCP-сервер.

Коли відбувається налаштування групи додатків, потрібно вказати роль кожного комп'ютера і його пріоритет завантаження. Крім того, можна вказати, які тести потрібно виконати для перевірки комп'ютерів у групі програм.

Коли запускається завдання SureBackup, Veeam спочатку запускається на віртуальних лабораторних машинах з групи додатків у потрібному порядку і виконує на них необхідні тести. Таким чином, Veeam створює необхідне середовище для перевіреної машини. Тільки після того, як всі машини з групи додатків запущені і протестовані, Veeam запускає перевірену машину у віртуальній лабораторії.

Наприклад, якщо ви потрібно перевірити сервер Microsoft Exchange Server, потрібно протестувати його функціональність у взаємодії з контролером домену та DNS-сервером. Згодом потрібно додати до групи додатків віртуальний контролер домену та DNS-сервер. Коли Veeam запускає завдання SureBackup, він спочатку запускає і перевіряє контролер домену і DNS-сервер у віртуальній лабораторії, щоб уможливити перевірку сервера Microsoft Exchange Server.

Віртуальна лабораторія. Віртуальна лабораторія - це ізольоване віртуальне середовище, в якому запускається і тестується перевірена машина і машини з групи додатків. У віртуальній лабораторії Veeam запускає віртуальні машини з групи додатків і перевірену віртуальну машину. Віртуальна лабораторія використовується не тільки для процедури перевірки SureBackup, але також для U-AIR, пісочниці On-Demand Sandbox і поетапного відновлення.

Сама по собі віртуальна лабораторія не вимагає виділення додаткових ресурсів. Однак віртуальні машини, що працюють у віртуальній лабораторії, споживають ресурси процесора і пам'яті хоста ESXi, на якому розгорнуто віртуальну

лабораторію. Усі зміни у віртуальних машинах, які відбуваються під час перевірки відновлення, записуються до файлів журналів повторного виконання. За замовчуванням Veeam зберігає журнали повторного копіювання у сховищі даних, вибраному в налаштуваннях віртуальної лабораторії, і видаляє їх після завершення процесу відновлення.

Віртуальна лабораторія повністю ізольована від виробничого середовища. Мережева конфігурація віртуальної лабораторії є дзеркальним відображенням мережевої конфігурації виробничого середовища. Наприклад, якщо перевірені віртуальні машини і віртуальні машини з групи додатків розташовані в двох логічних мережах у виробничому середовищі, віртуальна лабораторія також матиме дві мережі. Мережі у віртуальній лабораторії будуть зіставлені з необхідними виробничими мережами.

Віртуальні машини в ізольованих мережах мають ті самі IP-адреси, що й у виробничій мережі. Це дозволяє віртуальним машинам у віртуальній лабораторії функціонувати так, як якщо б вони працювали у виробничому середовищі.

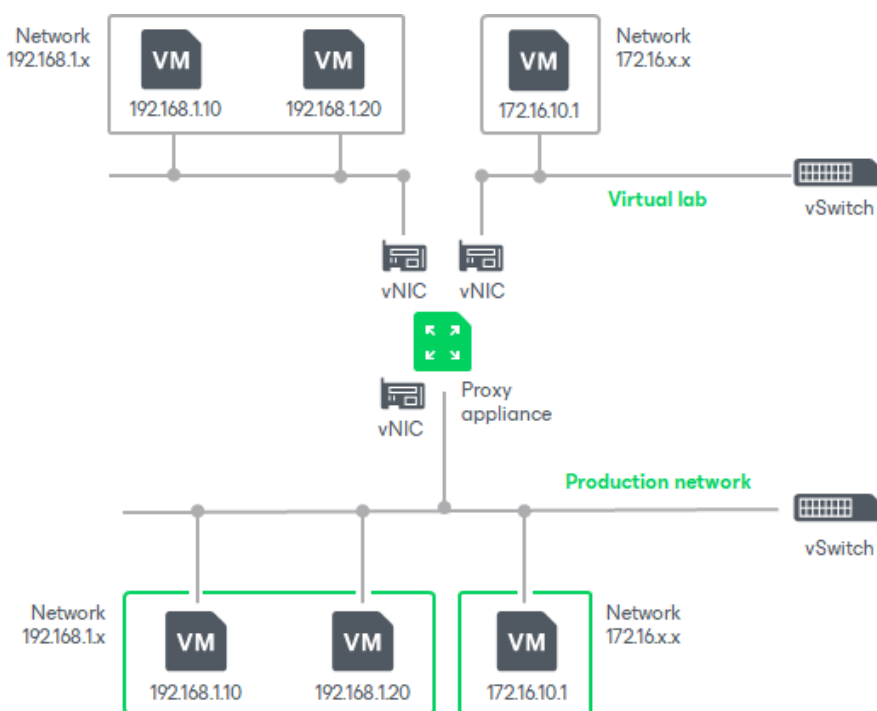


Рисунок 2.13 схема роботи віртуальної лабораторії в Veeam

Завдання SureBackup. Завдання SureBackup - це завдання для виконання перевірки відновлення. Їх можна запустити вручну або запланувати його автоматичний запуск за розкладом. Завдання SureBackup може виконуватися в двох різних режимах: Повне тестування відновлюваності та Перевірка резервних копій і лише сканування вмісту.

У режимі повного тестування відновлюваності завдання SureBackup об'єднує всі параметри та політики перевірки відновлення, такі як група програм і віртуальна лабораторія, що використовуються, резервні копії машин, які потрібно перевірити у віртуальній лабораторії, тощо. Він запускає машини в ізольованому середовищі безпосередньо з резервної копії і виконує тести з робочими програмами. Цей режим гарантує відновлення робочих навантажень у разі аварійного збою.

У режимі «Тільки перевірка резервної копії та сканування вмісту» завдання SureBackup виконує тільки перевірку цілісності резервної копії та аналіз її вмісту для виявлення слідів шкідливого програмного забезпечення або будь-яких інших небажаних або конфіденційних даних. Ці перевірки не вимагають створення віртуальної лабораторії або групи програм.

Завдання SureBackup можна запустити вручну або запланувати його автоматичне виконання. Коли завдання SureBackup виконується в режимі тестування повного відновлення, Veeam спочатку створює середовище для перевірки відновлення:

Veeam запускає віртуальну лабораторію. У віртуальній лабораторії Veeam Backup & Replication запускає машини з групи додатків у потрібному порядку.

Машини з групи додатків продовжують працювати, поки перевірені машини (машини з пов'язаного завдання) не завантажаться з резервних копій і не будуть протестовані. Якщо Veeam не знаходить дійсну точку відновлення для жодної з машин з групи програм, завдання SureBackup не виконується.

Коли віртуальна лабораторія готова, Veeam Backup & Replication запускає перевірені машини на потрібну точку відновлення і, залежно від налаштувань завдання, перевіряє їх по черзі або створює кілька потоків і перевіряє кілька машин одночасно.

Якщо Veeam Backup & Replication не знаходить дійсної точки відновлення для жодного з перевірених комп'ютерів, перевірка цього комп'ютера завершується невдачею, але завдання продовжує виконуватися.

За замовчуванням можна запустити і перевірити до трьох машин одночасно. Кількість машин, які можна запускати і тестувати одночасно, можна збільшити. Слід пам'ятати, що якщо ці машини є вимогливими до ресурсів, продуктивність завдання SureBackup, а також продуктивність хоста ESXi, на якому розміщена віртуальна лабораторія, може знизитися.

Після завершення процесу перевірки машини з групи додатків вимикаються. За бажанням можна залишити комп'ютери з групи програм увімкненими, щоб виконати перевірку вручну або ввімкнути відновлення на рівні елемента програми під керуванням користувача.

У деяких випадках розклад завдання SureBackup може перекривати розклад пов'язаного з ним завдання резервного копіювання. Файл резервної копії може бути заблокований завданням резервного копіювання, і завдання SureBackup не зможе перевірити таку резервну копію. У цій ситуації Veeam не запустить завдання SureBackup, доки завдання резервного копіювання не завершиться.

Scale-Out Backup Repositories: система сховищ, яка дозволяє розподіляти дані між рівнями продуктивності, ємності та архівування. Масштабоване сховище резервних копій складається з одного або декількох сховищ резервних копій або сховищ об'єктів, які називаються рівнем продуктивності, і можуть бути розширені сховищами об'єктів для довгострокового та архівного зберігання: рівнем ємності та рівнем архіву. Усі пристрої та

системи зберігання всередині масштабованого сховища резервних копій об'єднуються в систему, а їхні ємності підсумовуються. Ця функція надає наступні переваги: забезпечує зручний спосіб керування сховищем резервних копій. Масштабоване сховище резервних копій можна розширити в будь-який момент: якщо в областях масштабованого сховища резервних копій не вистачає місця, можна додати нову область до наявного масштабованого сховища резервних копій. Наприклад, якщо дані резервних копій зростають і сховище резервних копій досягає граничного обсягу, можливо додати нову систему зберігання до масштабованого сховища резервних копій. У результаті не доведеться переміщати резервні копії до сховища резервних копій більшого розміру.

Підтримується будь-який об'єкт резервного копіювання, що адмініструється Veeam: Сервери Windows або Linux з локальним або DAS сховищем, мережеві ресурси, дедуплікаційні пристрої зберігання, об'єктні сховища. При цьому зберігаються всі функції будь-якого пристрою або системи зберігання даних. Дозволяє налаштовувати гранульовану політику продуктивності.

Забезпечує практично необмежену ємність хмарного сховища: можливо доручити Veeam вивантажувати дані з екстенсивів у хмару для довгострокового зберігання.

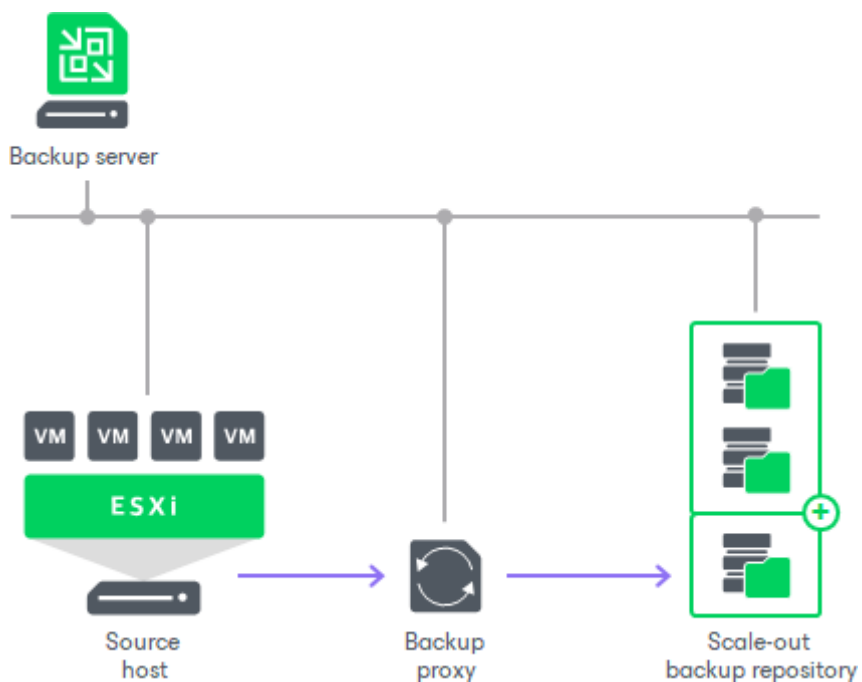


Рисунок 2.14 схема роботи системи сховищ в Veeam

2.3. Впровадження Veeam в малі та середні підприємства

Впровадження системи резервного копіювання та реплікації є важливим кроком для малих та середніх підприємств (МСП), які прагнуть забезпечити безпеку своїх даних, не залежно від того, чи працюють вони в локальній інфраструктурі, чи використовують хмарні технології. Одним із ефективних рішень, що відповідають вимогам таких компаній, є рішення для резервного копіювання та реплікації, яке дозволяє надійно зберігати дані і швидко їх відновлювати. Впровадження таких рішень, як Veeam Backup & Replication, для МСП включає кілька ключових етапів, що допомагають забезпечити стабільність бізнесу навіть у разі непередбачених ситуацій.

Першим етапом впровадження є аналіз потреб підприємства, що є надзвичайно важливим для успішної реалізації проекту. Підприємства повинні оцінити, які саме дані та системи є критичними для їхньої діяльності. Наприклад, це можуть бути фінансові записи, клієнтські дані, документи, бази даних або інші важливі файли. Відповідно до цих потреб обирається оптимальна стратегія резервного копіювання.

Крім того, важливо оцінити існуючу інфраструктуру компанії: використовуються чи локальні сервери, віртуалізовані середовища, або хмарні технології. Це дозволяє визначити, яку інфраструктуру необхідно побудувати або оновити для ефективного впровадження рішення для резервного копіювання. Аналіз потреб також враховує вимоги до швидкості відновлення даних (так звані цілі відновлення, RTO) та допустимого рівня втрат даних (RPO), що дозволяє правильно налаштувати систему для досягнення необхідних рівнів безпеки та доступності.

Після того, як потреби підприємства чітко визначено, наступним етапом є планування впровадження. На цьому етапі обираються найбільш підходящі стратегії резервного копіювання та відновлення, враховуючи, які обсяги даних необхідно зберігати та з якою частотою потрібно проводити копіювання. Малі та середні підприємства часто стикаються з обмеженнями в бюджеті, тому важливо визначити, які функціональні можливості є критичними, а від яких можна відмовитись для оптимізації витрат. Також на етапі планування визначається, де будуть зберігатися резервні копії — на локальних серверах, в хмарі або в гібридній інфраструктурі. Для цього важливо вибрати зручні та безпечні місця для зберігання даних, враховуючи вимоги до доступності та безпеки. Крім того, потрібно визначити політики відновлення даних, які відповідатимуть вимогам бізнесу щодо максимально допустимих затримок при відновленні роботи підприємства після інциденту. Планування також включає визначення необхідних ресурсів для забезпечення належного рівня захисту даних.

Реалізація є наступним етапом, де відбувається безпосереднє впровадження рішення в інфраструктуру компанії. Під час реалізації налаштовується саме програмне забезпечення для резервного копіювання та реплікації, відбувається інсталяція на сервери та віртуальні машини, а також налаштування політик резервного копіювання, що були визначені на попередньому етапі. Після налаштування всієї інфраструктури проводиться тестування системи. Тестування є важливим етапом, оскільки дозволяє перевірити, чи правильно зберігаються

резервні копії даних і чи можуть вони бути успішно відновлені у разі необхідності. У рамках реалізації також потрібно провести навчання персоналу, що дозволить фахівцям підприємства ефективно користуватися новою системою та здійснювати підтримку в разі виникнення будь-яких проблем. Моніторинг і підтримка також є невід'ємною частиною процесу реалізації, оскільки вони дозволяють оперативно реагувати на будь-які неполадки в роботі системи.

Прикладом успішного впровадження може бути досвід однієї з невеликих медіа-компаній, яка вирішила перейти на автоматизовану систему резервного копіювання для своїх великих відеоархівів. До впровадження системи компанія використовувала застарілі методи копіювання даних вручну, що призводило до значних ризиків втрати важливої інформації та зайвих витрат часу на відновлення. Після ретельного аналізу потреб компанія обрала Veeam Backup & Replication як рішення, яке дозволило автоматизувати процес резервного копіювання та реплікації даних. Завдяки чітко спланованій стратегії компанія змогла налаштувати резервне копіювання з мінімальним часом відновлення, що значно підвищило надійність і стабільність роботи. В результаті, компанія зменшила час на відновлення даних на 60% та забезпечила більш високий рівень безпеки своїх важливих архівів.

Іншим прикладом є маленька ІТ-фірма, яка надавала послуги з розробки програмного забезпечення. Компанія мала справу з великими обсягами даних, що зберігалися на локальних серверах і віртуальних машинах. Через відсутність належної системи резервного копіювання фірма втратила частину важливих даних після збоїв в серверному обладнанні, що спричинило значні затримки в проектах. Після впровадження системи Veeam Backup & Replication фірма змогла автоматизувати резервне копіювання, налаштувати реплікацію даних на віддалену локацію та створити систему відновлення, яка відповідала вимогам до швидкості і надійності. Це дозволило фірмі уникнути подібних проблем у майбутньому і значно покращити ефективність роботи з клієнтами.

Таким чином, впровадження системи резервного копіювання та реплікації, як Veeam Backup & Replication, може стати важливим кроком для малих і середніх підприємств, що дозволяє підвищити безпеку даних та забезпечити ефективне відновлення після технічних інцидентів. Ретельний аналіз потреб, правильне планування та якісна реалізація дозволяють досягти високого рівня захисту та зменшити ризики для бізнесу. Реальні приклади з життя показують, як навіть невеликі компанії можуть успішно впровадити такі рішення, забезпечивши стабільність своєї діяльності і збільшивши ефективність бізнес-процесів.

2.4. Переваги використання Veeam у МСП

Одна з основних переваг використання Veeam у малих та середніх підприємствах полягає в значному зниженні ризику втрати даних. Для МСП дані є основним активом, і їх втрата може призвести до серйозних фінансових і репутаційних втрат. Відомо, що для таких компаній витрати на відновлення після втрати даних можуть бути значними, а час, витрачений на пошук і відновлення втрачених файлів, — критичним. Рішення Veeam допомагає створити ефективні стратегії резервного копіювання, що включають регулярне оновлення резервних копій і можливість відновлення даних у найкоротші терміни. Це дозволяє мінімізувати ймовірність втрати важливої інформації та дає компаніям можливість швидко відновити свою діяльність у разі непередбачених ситуацій, таких як збої в системах чи кіберінциденти.

Ще однією важливою перевагою використання Veeam є оптимізація витрат. Малий та середній бізнес зазвичай має обмежений бюджет на ІТ-інфраструктуру, і тому важливо забезпечити ефективне використання коштів при виборі рішень для резервного копіювання. В порівнянні з іншими рішеннями на ринку, Veeam пропонує більш доступну та масштабовану модель. МСП не потрібно інвестувати в дорогі апаратні засоби або складні рішення, що потребують значних затрат на утримання. Вартість впровадження та підтримки Veeam є конкурентоспроможною і дозволяє компаніям отримувати високоякісне рішення без значних

капіталовкладень. Крім того, Veeam пропонує гнучкість, оскільки компанії можуть обирати найбільш підходящі стратегії резервного копіювання та реплікації, що дозволяє адаптувати витрати під їхні конкретні потреби і можливості.

Використання Veeam також суттєво підвищує ефективність бізнес-процесів. Однією з найбільших проблем для малих і середніх підприємств є час, необхідний для відновлення даних після інцидентів. Збої в роботі серверів або програмного забезпечення можуть призвести до значних простоїв, що негативно впливає на продуктивність і доходи компанії. Завдяки швидкому і автоматизованому відновленню даних, яке забезпечує Veeam, компанії можуть звести до мінімуму час, втрачаючи на відновлення після збоїв. Відновлення відбувається майже миттєво, що дозволяє підприємствам швидко повернутися до роботи і продовжити бізнес-процеси без значних втрат. Це особливо важливо для МСП, де навіть короткочасні простої можуть мати серйозні наслідки для їх фінансових результатів.

Загалом, використання Veeam у малих та середніх підприємствах дозволяє створити надійне та доступне рішення для захисту даних, яке мінімізує ризики втрати інформації, оптимізує витрати на ІТ-інфраструктуру і значно підвищує ефективність бізнес-процесів. Це дозволяє підприємствам не лише забезпечити стабільну роботу в умовах сучасних технологічних викликів, але й зміцнити свою конкурентоспроможність на ринку.

3. ВИКОРИСТАННЯ VEEAM НА ПІДПРИЄМСТВІВ

3.1 Підготовка середовища

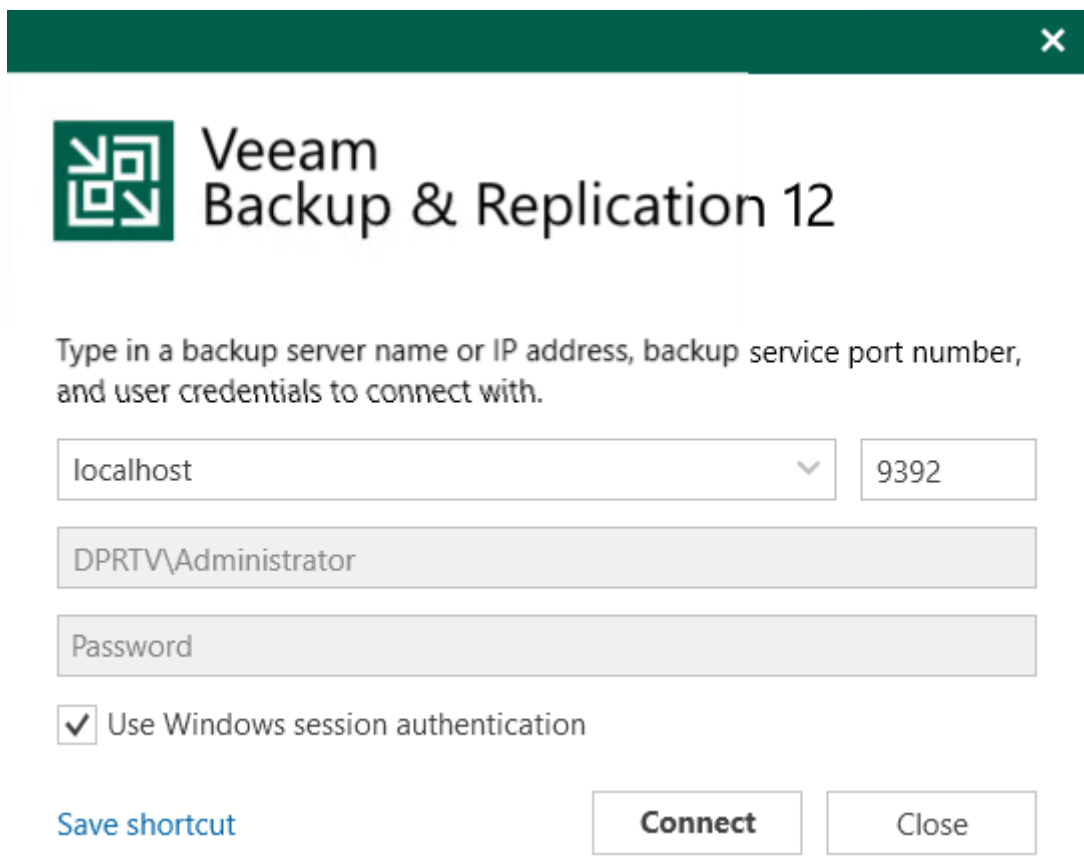


Рис. 3.1 Підключення до Veeam

Підключаємось до Veeam який розгорнутий на сервері компанії.

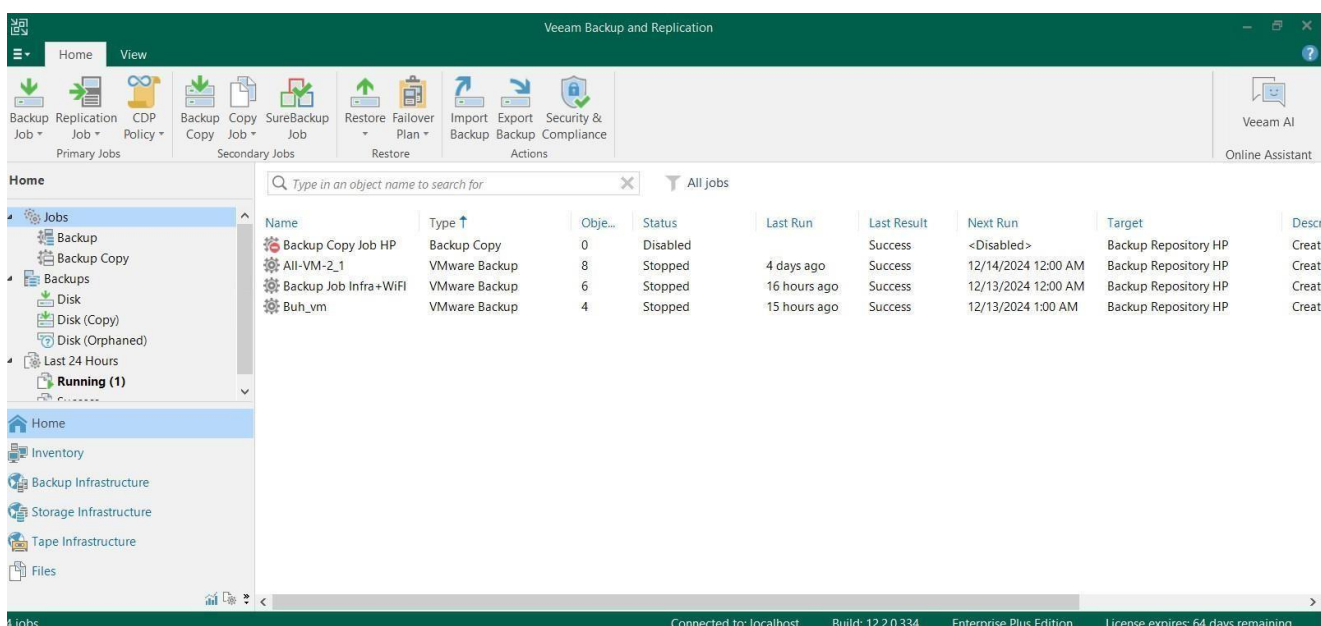


Рис. 3.2 Інтерфейс Veeam

Можна переглянути інтерфейс та вже доступні завдання які робляться автоматично за розкладом.

3.2. Конфігурація нового завдання

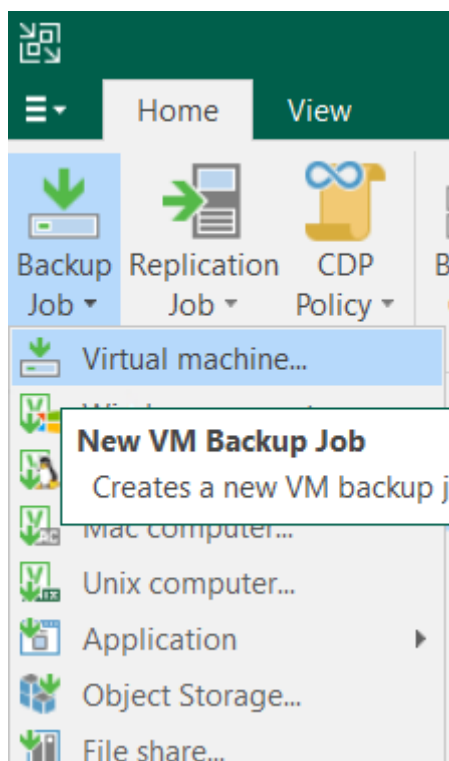


Рис. 3.3 Створення нового завдання для резервного копіювання

Для того аби створити нове завдання на резервне копіювання я обираю що саме буде копіювати Veeam.

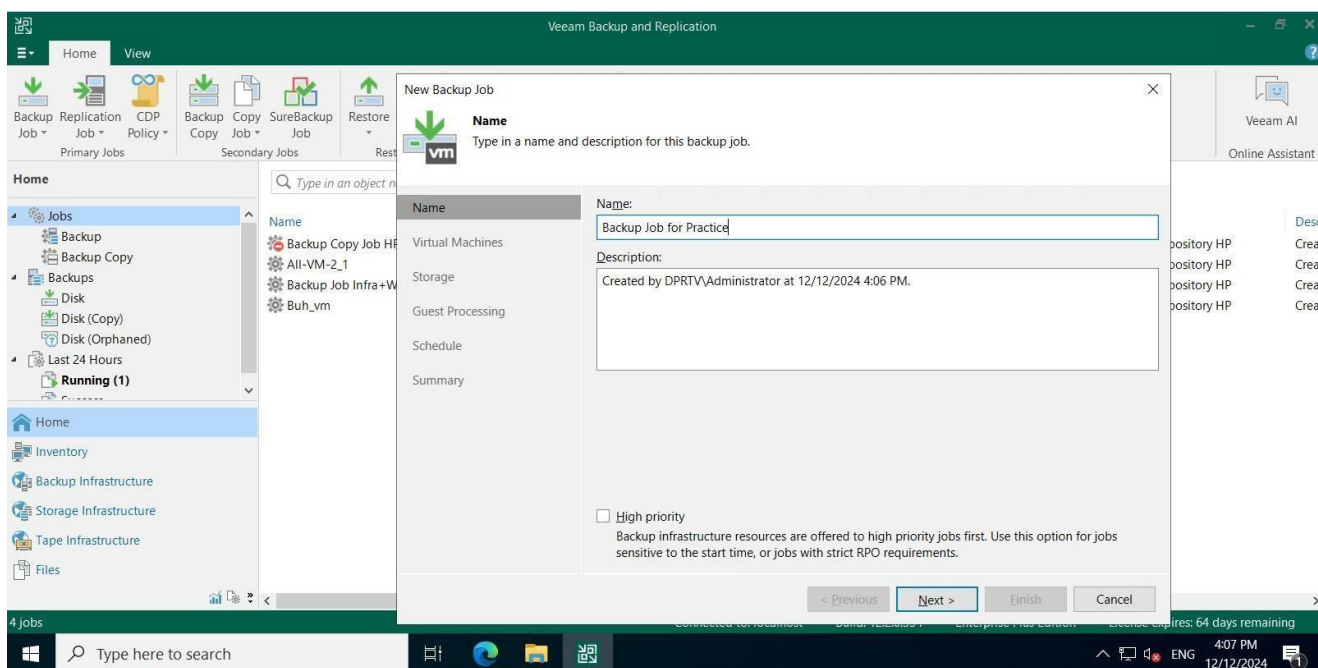


Рис. 3.4 задаємо назву для завдання

Створюючи нове завдання необхідно задати йому назву як на рисунку 3.2

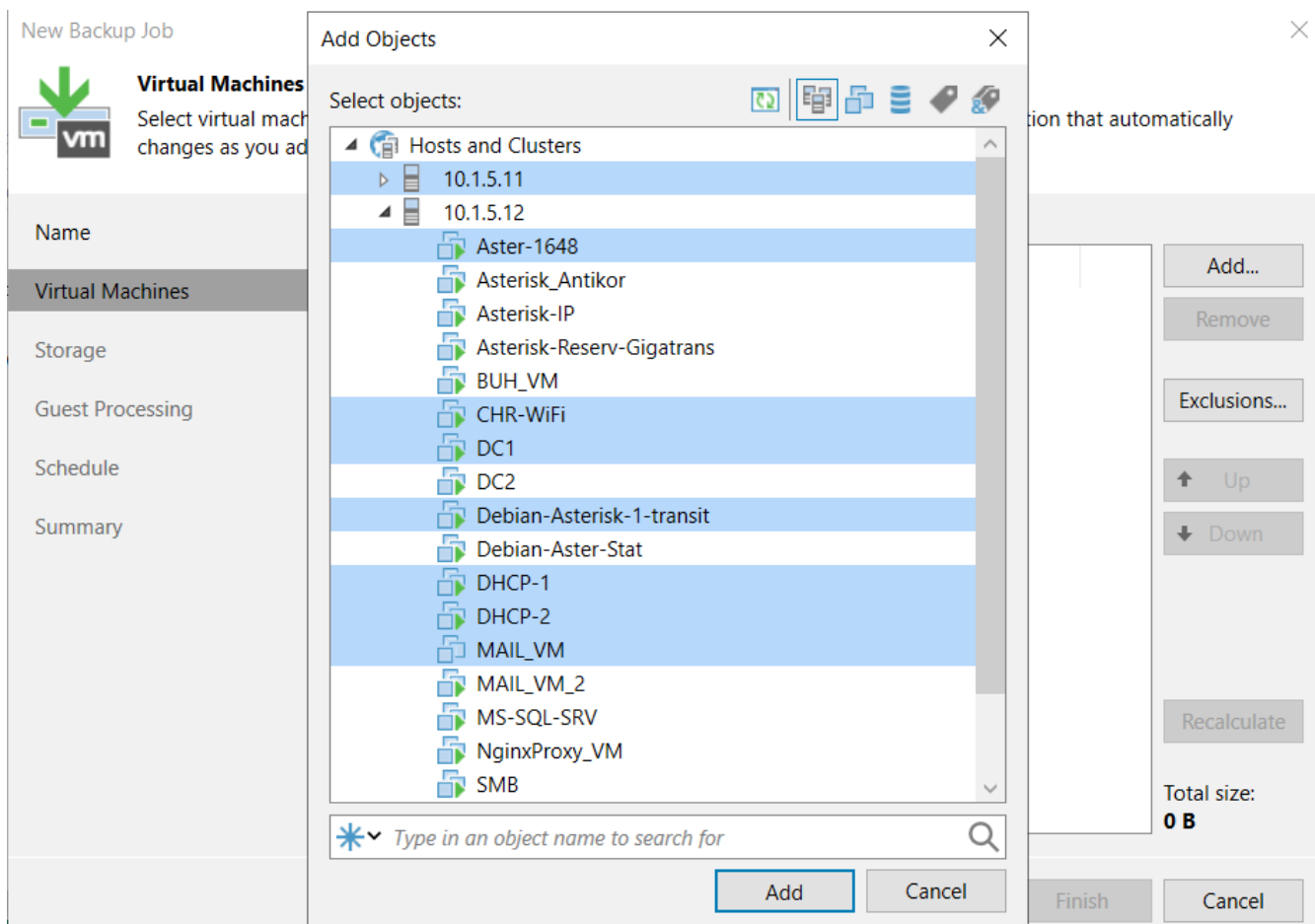


Рис. 3.5 Вибір серверів та віртуальних машин розміщених на них

Для створення резервної копії обираємо необхідний сервер та віртуальні машини розміщені на ньому в моєму випадку це в моєму випадку це домен контролери та DHCP-сервер, а також сервер на якому розгорнута поштовий клієнт.

New Backup Job ✕

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Name	Backup proxy: Automatic selection Choose...
Virtual Machines	Backup repository: Backup Repository HP (Created by DPRTV\Administrator at 7/15/2024 5:17 PM.) ▼
Storage	3.60 TB free of 7.99 TB Map backup Retention policy: 7 days ! ☐ Keep certain full backups longer for archival purposes GFS retention policy is not configured Configure... ☐ Configure secondary destinations for this job Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site. Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings. Advanced...
Guest Processing	
Schedule	
Summary	

< Previous
Next >
Finish
Cancel

Рис. 3.6 Вибір репозиторію де будуть зберігатись резервні копії

Можна вибрати репозиторій де будуть зберігатись резервні копії в моєму випадку це репозиторій який налаштовано по iSCSI.

New Backup Job ✕

Guest Processing

Choose guest OS processing options available for running VMs.

Name	☐ Enable application-aware processing Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot. Customize application handling options for individual machines and applications Applications...
Virtual Machines	☐ Enable guest file system indexing and malware detection Indexing enables global file search functionality, automatic detection of suspicious file system activity and known malware files. Customize advanced guest file system indexing options for individual machines Indexing...
Storage	Guest interaction proxy: Automatic selection Choose...
Guest Processing	Guest OS credentials: Select existing credentials or add new ▼ Add... Manage accounts
Schedule	Customize guest OS credentials for individual machines and operating systems Credentials...
Summary	Verify network connectivity and credentials for each machine included in the job Test Now

< Previous
Next >
Finish
Cancel

Рис 3.8. Додаткові налаштування для віртуальних машин

Тут ми можемо задати додаткові налаштування як наприклад засікати заражені файли чи відсікати підозрілу активність на віртуальній машині.

New Backup Job ×



Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

Name	☒ Run the job automatically
Virtual Machines	☒ Daily at this time: 01:00 AM Everyday Days...
Storage	☐ Monthly at this time: 10:00 PM Fourth Saturday Months...
Guest Processing	☐ Periodically every: 1 Hours Schedule...
Schedule	☐ After this job: All-VM-2_1 (Created by DPRTV\Administrator at 3/27/2024 11:08 AM
Summary	Automatic retry ☒ Retry failed items processing: 3 times Wait before each retry attempt for: 10 minutes Backup window ☐ Terminate the job outside of the allowed backup window Window... Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

< Previous
Apply
Finish
Cancel

Рис. 3.9. Вибір розкладу за яким буде робитись резервне копіювання

Я можу задати розклад для резервного копіювання це може бути будь який час чи день для зручності а також кількість спроб якщо не вдасться з першого разу.

Type in an object name to search for		All jobs					
Name	Type	Obj...	Status	Last Run	Last Result	Next Run	Target
Backup Copy Job HP	Backup Copy	0	Disabled		Success	<Disabled>	Backup Repository HP
All-VM-2_1	VMware Backup	8	Stopped	4 days ago	Success	12/14/2024 12:00 AM	Backup Repository HP
Backup Job for Practice	VMware Backup	5	Stopped			12/13/2024 1:00 AM	Backup Repository HP
Backup Job Infra+WiFi	VMware Backup	6	Stopped	16 hours ago	Success	12/13/2024 12:00 AM	Backup Repository HP
Buh_vm	VMware Backup	4	Stopped	15 hours ago	Success	12/13/2024 1:00 AM	Backup Repository HP

Рис. 3.10. Завдання готове

На рисунку 3.10 можна побачити що саме завдання готове на 1 годину ночі, цей час вибраний тому що саме опівночі відбувається найменше навантаження на сервер.

3.3. Успішне створення резервної копії

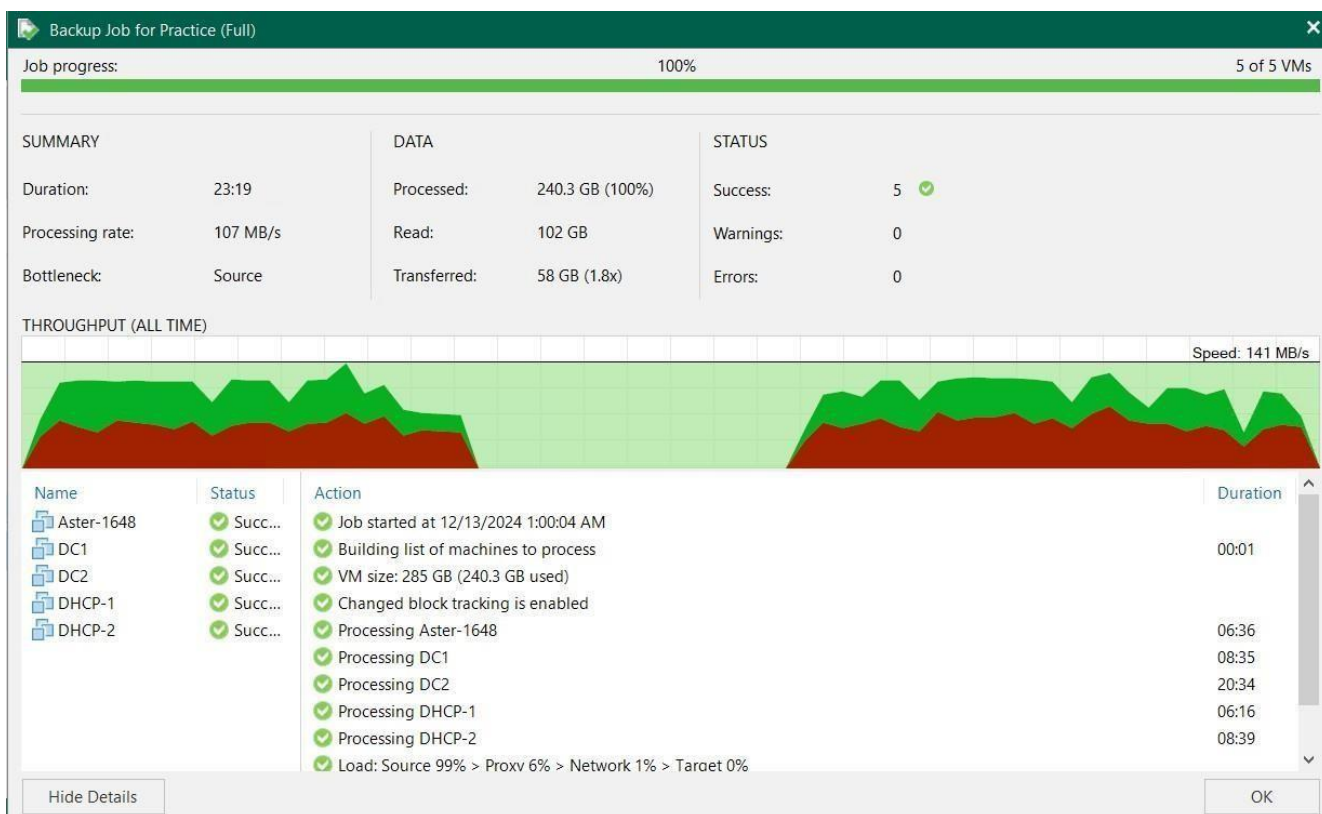


Рис. 3.11. Завдання резервного копіювання виконано успішно

Як можна побачити завдання було виконано успішно і veeam зробив резервні копії віртуальних машин.

Name	Date modified	Type	Size
Aster-1648.28D2024-12-13T010004_6C05...	12/13/2024 1:06 AM	Veeam Backup & ...	6,273,308 ...
Aster-1648_24291.vbm	12/13/2024 1:06 AM	Veeam Backup & ...	11 KB
DC1.42D2024-12-13T010004_9E64.vbk	12/13/2024 1:08 AM	Veeam Backup & ...	18,416,784 ...
DC1_54FEE.vbm	12/13/2024 1:08 AM	Veeam Backup & ...	11 KB
DC2.40D2024-12-13T010004_07DC.vbk	12/13/2024 1:20 AM	Veeam Backup & ...	16,025,660 ...
DC2_3996A.vbm	12/13/2024 1:20 AM	Veeam Backup & ...	11 KB
DHCP-1.43D2024-12-13T010004_9C46.vbk	12/13/2024 1:19 AM	Veeam Backup & ...	8,992,732 ...
DHCP-1_BF8A4.vbm	12/13/2024 1:20 AM	Veeam Backup & ...	11 KB
DHCP-2.46D2024-12-13T010004_C65C.vbk	12/13/2024 1:23 AM	Veeam Backup & ...	8,709,372 ...
DHCP-2_B2FAB.vbm	12/13/2024 1:23 AM	Veeam Backup & ...	11 KB

Рис. 3.11. Резервні копії у вигляді файлів

На рисунку 3.11 можна побачити резервні копії у вигляді файлів якщо нам потрібно буде витягнути їх на зовнішній носій.

ВИСНОВКИ

Для малих і середніх підприємств, які часто мають обмежені ресурси, надійне резервне копіювання є критично важливим для забезпечення безперервності бізнесу та захисту від втрати даних. Рішення, такі як Veeam, дозволяють ефективно організувати цей процес і мінімізувати ризики, пов'язані з недоступністю даних через технічні збої чи кіберзагрози. Використання Veeam дозволяє малим і середнім підприємствам застосовувати стратегію резервного копіювання з гнучким налаштуванням і високою масштабованістю. Це дає можливість обирати оптимальні методи резервування, зокрема через гібридні або хмарні рішення, що ідеально підходить для компаній з обмеженими фінансовими та технічними можливостями. Veeam пропонує безпечне та швидке відновлення даних, знижує час простою системи і забезпечує високий рівень автоматизації. Вбудовані функції резервного копіювання на рівні віртуальних машин та фізичних серверів дозволяють підприємствам адаптувати стратегію під конкретні вимоги та зміни в ІТ-інфраструктурі. Завдяки доступності рішень Veeam, підприємства можуть реалізувати стратегію резервного копіювання, що поєднує високу ефективність і помірні витрати. Ліцензування за принципом "оплати за використання" дозволяє зменшити початкові витрати та адаптувати масштаби резервного копіювання до реальних потреб бізнесу. У процесі впровадження та розвитку стратегії резервного копіювання на основі Veeam, підприємства отримують можливість інтеграції з іншими сучасними ІТ-рішеннями, такими як автоматизація процесів управління даними та забезпечення кібербезпеки, що може забезпечити конкурентні переваги в довгостроковій перспективі. Важливим аспектом стратегії резервного копіювання є забезпечення безпеки даних та відповідності вимогам законодавства (наприклад, GDPR). Veeam пропонує рішення, які допомагають підприємствам зберігати відповідність стандартам безпеки даних і виконувати вимоги щодо архівування та збереження інформації.

Впроваджуючи стратегію резервного копіювання, малим і середнім підприємствам слід зосередитися на ретельному плануванні та тестуванні процесів відновлення даних, визначити критичні для бізнесу дані, та регулярно оновлювати стратегію з урахуванням змін у технологіях та бізнес-цілях.

ПЕРЕЛІК ПОСИЛАНЬ

1. "Резервне копіювання та відновлення: Недорогі рішення для резервного копіювання для відкритих систем « - В. Кертис Престон (2020) с. 142-182
2. "Освоєння VMware vSphere 7 » - Скотт Лоу (2020) с. 138-254
3. "Захист даних: Забезпечення доступності даних « - Ерік А. Герцог (2020) с. 87-214
4. "Практичне резервне копіювання та відновлення за допомогою ZFS » - Адам Рабін (2020) с. 205-243
5. "Резервне копіювання та аварійне відновлення за допомогою Veeam » - Грег Хакетт (2020) с. 208-257
6. "Хмарне резервне копіювання для бізнесу: Посібник для початківців « - Роберт Бредлі (2020) с. 125-268
7. "Мистецтво резервного копіювання даних: Практичний посібник « - Грегорі Браун (2020) с. 79-154
8. "Захист даних своїми руками: Резервне копіювання та відновлення для ІТ-спеціалістів « - Рамеш Ядав (2020) с. 115-189
9. "Посібник з резервного копіювання: Посібник із захисту ваших даних « - Вільям Сміт (2020) с. 248-294
10. "Безпека даних та резервне копіювання: Кращі практики для малого та середнього бізнесу « - Джошуа Девіс (2020) с. 176-236
11. "Розуміння хмарних сховищ та рішень для резервного копіювання » - Адам Мур (2020) с. 198-325
12. "Системи резервного копіювання та відновлення: Методи та технології « - Джон Джонс (2020) с. 136-228

13. "Автоматизовані рішення для резервного копіювання: Посібник зі спрощення відновлення даних « - Том Каллахан (2020) с. 122-214
14. "Рішення для мережевого резервного копіювання для підприємств » - Лінда Макдональд (2020) с. 166-247
15. "Резервне копіювання даних та аварійне відновлення для підприємств » - Марія Вільямс (2020) с. 69-301
16. "Побудова надійної стратегії резервного копіювання даних » - Мартін Андерсон (2020) с. 91-177
17. "Сучасні рішення для резервного копіювання з інтеграцією в хмару » - Майкл Девіс (2020) с. 84-157
18. "Переосмислення стратегій резервного копіювання: Рішення для зростаючих потреб у даних « - Семюель Уайт (2020) с. 103-205
19. "Біблія хмарного резервного копіювання » - Брайан Ніл (2020) с. 95-173
20. "Резервне копіювання як послуга: Використання хмарних технологій для захисту даних « - Анна Вільямс (2020) с. 86-211
21. "Просунуті методи резервного копіювання: Комплексний посібник « - Девід Кларк (2020) с. 148-195
22. "Гібридні хмарні та резервні рішення для ІТ-команд » - Роб Вільямс (2020) с. 111-132
23. "Кращі практики резервного копіювання для сучасних підприємств » - Едвард Томпсон (2020) с. 92-173
24. "Резервне копіювання та відновлення даних для систем Windows » - Тім Фішер (2020) с. 287-366
25. "Аварійне відновлення та резервне копіювання з Hyper-V » - Стів Томчак (2020) с. 98-139
26. "Революція резервного копіювання: Хмара та автоматизація для захисту даних « - Сара Джексон (2020) с. 52-147
27. "Ефективні стратегії резервного копіювання та зберігання для центрів обробки даних » - Білл Стюарт (2020) с. 24-96

28. "Аварійне відновлення: Посібник для власників бізнесу та ІТ-фахівців « - Джонатан Дженкінс (2020) с. 174-225
29. "Хмарні рішення для резервного копіювання: Кращі практики для сучасного бізнесу « - Баррі Сондерс (2020) с. 80-99
30. "Резервне копіювання та відновлення: Захист даних в епоху хмарних технологій» - Річард Лі (2021) с.40-300

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

1

Магістерська робота на тему:
“Метод резервного копіювання даних для малих і середніх підприємств на основі рішення Veeam”

Виконав: студент групи ІСДМ-61

Сінгаєвський Максим

Керівник: К.Т.Н., доцент

Олег Сеньков

КИЇВ-2024

Актуальність теми:

У сучасному цифровому світі малим і середнім підприємствам (МСП) необхідно швидко адаптувати свої інформаційні системи для забезпечення безпеки та доступності даних. Актуальність теми полягає в тому, що у зв'язку з розвитком цифрових технологій та збільшенням обсягів даних, підприємства потребують сучасних і доступних методів резервного копіювання, які дозволяють знизити ризики втрати даних, забезпечити швидке відновлення в разі збоїв та мінімізувати витрати на підтримку ІТ-інфраструктури. Рішення Veeam є одним із найпопулярніших на ринку та надає прості у впровадженні, але потужні інструменти для резервного копіювання даних.

Мета роботи:

Метою роботи є розробка стратегії резервного копіювання для малих і середніх підприємств на основі рішення Veeam, яка дозволить забезпечити ефективне збереження даних, мінімізацію ризиків втрати інформації та оптимізацію витрат на зберігання і відновлення даних у разі їх втрати.

2

Предмет дослідження

Предметом дослідження є інструменти та методи резервного копіювання даних з використанням рішення Veeam для малих і середніх підприємств. Це включає оцінку та вибір типів резервних копій (повні, інкрементальні, диференціальні), налаштування та конфігурацію програмного забезпечення, а також розробку стратегії, що дозволяє оптимізувати використання ресурсів і забезпечити безперервність бізнесу.

Наукова новизна

Наукова новизна роботи полягає в глибокому дослідженні та адаптації рішення Veeam для малих і середніх підприємств (МСП), що дозволяє розробити нову стратегію резервного копіювання даних, оптимізовану під умови обмежених ресурсів підприємств. У роботі здійснено детальний аналіз можливостей Veeam щодо автоматизації резервного копіювання, відновлення даних та інтеграції з існуючими ІТ-інфраструктурами МСП.



Основною метою Veeam Backup & Replication є забезпечення надійного захисту даних через резервне копіювання, реплікацію та відновлення для віртуальних та фізичних інфраструктур. Це рішення допомагає гарантувати безперервність бізнес-процесів, дозволяючи швидко відновлювати дані або цілі віртуальні машини після збоїв або аварій. Важливою складовою є також реплікація віртуальних машин на віддалені сервіси для забезпечення резервування на випадок серйозних проблем із основною інфраструктурою. Крім того, Veeam підтримує інтеграцію з хмарними платформами, що дає змогу зберігати резервні копії в хмарі та автоматизувати процеси збереження і відновлення даних.

Основні можливості Veeam

Backup



Резервне копіювання (Backup):

- Безперервне захоплення даних: Регулярне створення резервних копій віртуальних машин (VM), фізичних серверів, додатків та інших даних для забезпечення їх захисту від втрати або пошкодження.
- Забезпечення швидкого відновлення: Можливість швидко відновити дані або цілі віртуальні машини на випадок аварій або непередбачуваних ситуацій.

Реплікація (Replication):

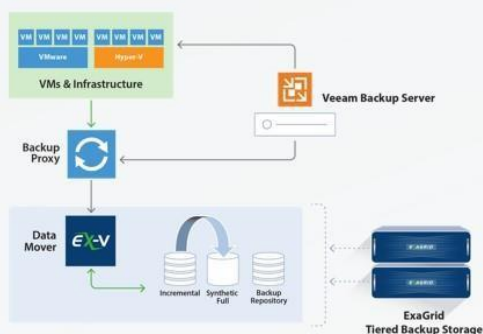
- Створення резервних копій в реальному часі: Реплікація віртуальних машин на віддалений сервер для забезпечення безперервної роботи в разі збою на основному сервері.
- Можливість швидкого відновлення після збоїв: Використання реплік для швидкого відновлення операційної діяльності без тривалих простоїв.

Реплікація



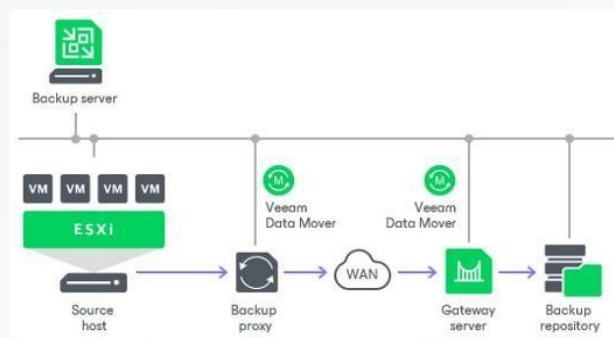
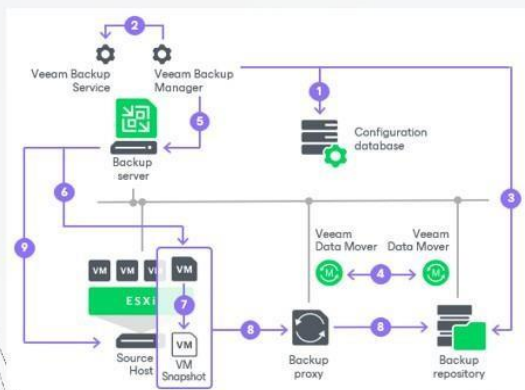
До технологічних можливостей Veeam входить:

- Глибоке відновлення даних
- Інтеграція з хмарними середовищами
- Технології дедуплікації та стиснення
- Безперервне резервне копіювання (Continuous Data Protection, CDP)



Стратегія резервного копіювання для малих та середніх підприємств на основі рішення Veeam Backup & Replication повинна забезпечувати надійний захист даних, мінімізацію ризиків втрати інформації та гарантувати швидке відновлення в разі аварії. План стратегії полягає в:

1. Оцінка інфраструктури та потреб: Спочатку необхідно оцінити поточну інфраструктуру підприємства, визначити критичні дані та додатки, а також обсяг даних, який потребує резервного копіювання. Враховуються як фізичні, так і віртуальні сервери, бази даних, файлові системи та хмарні сервіси.
2. Резервне копіювання віртуальних машин: Використовувати можливості Veeam для створення резервних копій віртуальних машин (VM), що дозволяє швидко відновлювати ці машини в разі неполадок. Важливо вибрати частоту резервного копіювання, що відповідає потребам бізнесу, наприклад, щодня або декілька разів на день для критичних VM.



Загальні впровадження. Частота та типи копій:

- Щоденне резервне копіювання: Для критичних даних створювати резервні копії щодня. Наприклад, для баз даних та важливих документів.
- Щогодинне резервне копіювання: Для змінних даних, таких як файли, що часто змінюються, можна використовувати резервне копіювання через кожну годину.
- Резервне копіювання один раз на тиждень (повне): Раз на тиждень створювати повне резервне копіювання, що дозволить мінімізувати час відновлення в разі серйозного збою.

В. Місця для зберігання резервних копій:

1. Локальне зберігання (On-premises storage):

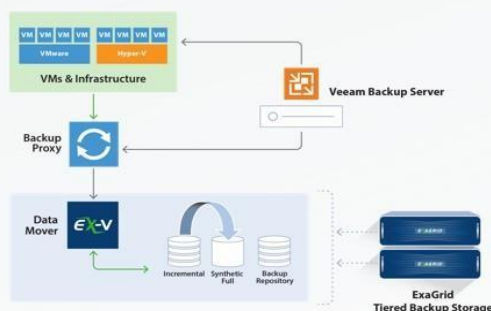
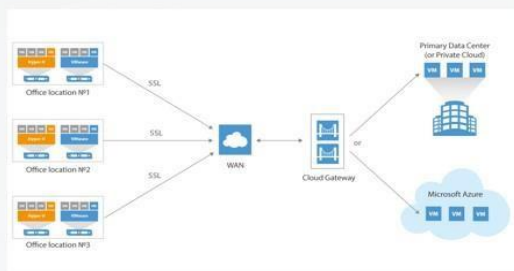
1. Використання власних серверів або NAS/SAN для зберігання резервних копій.
2. Застосування Veeam для створення резервних копій на локальних дисках або зовнішніх пристроях, зокрема за допомогою Veeam Backup & Replication.
3. Вибір формату резервних копій (наприклад, файли VBK для збереження цілісності).

2. Хмарне зберігання:

1. Зберігання резервних копій в хмарі (Amazon S3, Azure, Google Cloud) для додаткового захисту і в разі катастрофічних подій.
2. Використання Veeam Cloud Connect для безпечного зберігання резервних копій у хмарі.

3. Мультирегіональне резервне копіювання:

1. Використання декількох локацій для резервних копій (локальне зберігання + хмара) для забезпечення більшої безпеки.



План відновлення (Disaster Recovery Plan):

• Розробити чіткий план відновлення на випадок збою (Disaster Recovery Plan, DRP), який включає:

- Визначення критичних систем та даних.
- Оцінка часу відновлення (RTO - Recovery Time Objective) та втрат даних (RPO - Recovery Point Objective).
- Процедури відновлення для різних типів інцидентів (відновлення з резервної копії, відновлення VM, відновлення даних).
- Тестування відновлення даних для перевірки ефективності стратегії.

4. Тестування та моніторинг

• Тестування відновлення: Регулярно тестувати відновлення даних, щоб гарантувати, що резервні копії працюють належним чином.

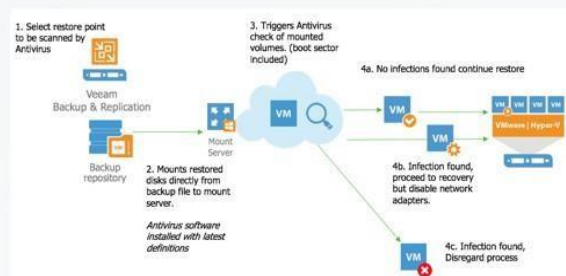
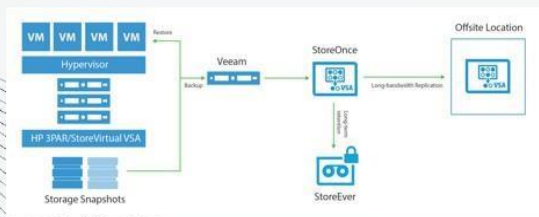
• Моніторинг стану копій: Використовувати Veeam ONE для моніторингу стану резервного копіювання, перевірки на помилки, помітки неуспішних резервних копій та іншої важливої інформації.

• Інтеграція з системами сповіщень: Для автоматичного сповіщення адміністратора в разі невдачі резервного копіювання або відновлення.

5. Безпека та шифрування:

• Шифрування резервних копій: Використовувати шифрування для захисту резервних копій на всіх етапах (як на локальних, так і на хмарних серверах).

• Ідентифікація та доступ: Обмежити доступ до резервних копій тільки авторизованим особам через системи контролю доступу та багатофакторну аутентифікацію.



Висновки

Для малих і середніх підприємств, які часто мають обмежені ресурси, надійне резервне копіювання є критично важливим для забезпечення безперервності бізнесу та захисту від втрати даних. Рішення, такі як Veeam, дозволяють ефективно організувати цей процес і мінімізувати ризики, пов'язані з недоступністю даних через технічні збої чи кіберзагрози. Використання Veeam дозволяє малим і середнім підприємствам застосовувати стратегію резервного копіювання з гнучким налаштуванням і високою масштабованістю.

1. Сінгаєвський М.М. «Переваги використання блокчейну для резервного копіювання». Тези доповіді на VII Всеукраїнській студентській науковій конференції «Діджиталізація науки як виклик сьогодення» (25.10.2024, м. Полтава, Україна).

2. Сінгаєвський М.М. «Резервне копіювання та аварійне відновлення даних для малого та середнього бізнесу». Тези доповіді на V Міжнародній науковій конференції «Інновації та науковий потенціал світу» (25.10.2024; м. Умань, Україна).

**ДЯКУЮ ЗА
УВАГУ**

