

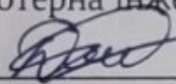
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

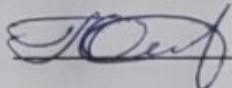
до випускної кваліфікаційної роботи бакалавра
на тему: «Проект інфраструктури резервного копіюван-
ня для корпоративної мережі організації»

Виконав студент 4-го курсу групи КІ-20-1

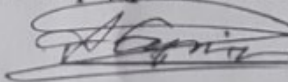
спеціальності 123 «Комп'ютерна інженерія»

 Михайло ДЕХТЯР

Керівник доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена ГОЛОВНЯ

Рецензент завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій ЄФІМЕНКО

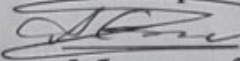
Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Дехтяр Михайло Сергійович

Тема роботи: «Проект інфраструктури резервного копіювання для корпоративної мережі організації»

затверджена Наказом університету від 5 березня 2024 р. №97

Термін здачі студентом закінченої роботи 9 червня 2024 р.

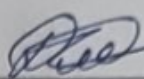
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
Об'єктом дослідження є процеси управління даними в корпоративних мережах, що охоплюють процеси зберігання, обробки, передачі та захисту інформації.
Предметом дослідження є інфраструктура резервного копіювання даних у корпоративній мережі організації, зокрема технології та методи резервного копіювання, планування та впровадження стратегії резервного копіювання, управління процесом резервного копіювання та відновлення даних, а також забезпечення безпеки та надійності збереженої інформації.

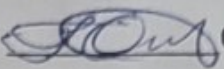
Обладнання та програмне забезпечення:

1. Veeam Backup and Replication.
2. Гіпервізори VMware Workstation Pro, ESXi, Hyper-V.
3. Віртуальне середовище Proxmox.
4. Операційні системи Windows 2016.

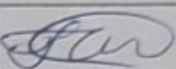
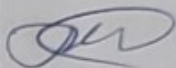
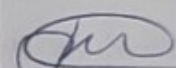
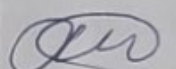
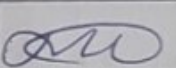
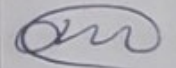
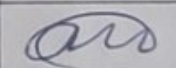
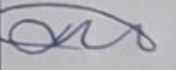
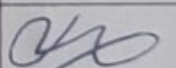
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

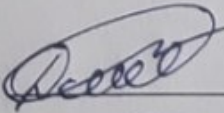
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

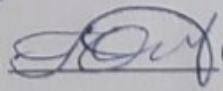
Студент  Михайло Дехтяр

Керівник  Олена Головня

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	20.03.2024-01.04.2024	
2	Написання вступної частини кваліфікаційної роботи	01.04.2024-03.04.2024	
3	Аналіз основних теоритичніх відомостей технологій резервного копіювання	03.04.2024-11.04.2024	
4	Проектування корпоративної мережі резервного копіювання	18.04.2024-24.04.2024	
5	Вибір обладнання та технологій	24.04.2024-01.05.2024	
6	Налаштування корпоративної мережі резервного копіювання	01.05.2024-16.05.2024	
7	Написання висновків	16.05.2024-20.05.2024	
8	Оформлення кваліфікаційної роботи	20.05.2024-02.06.2024	
9	Підготовка презентації до захисту	02.06.2024-05.06.2024	

Студент  Михайло Дехтяр

Керівник  Олена Головня

АНОТАЦІЯ

Пояснювальна записка містить: 81 сторінка текстової частини, 37 рисунків, 4 таблиці та 18 джерел.

Метою кваліфікаційної роботи є розробка проєкту інфраструктури резервного копіювання для корпоративної мережі організації.

У цій роботі розглянуто основні методи резервного копіювання та відновлення даних, а також детально проаналізовано особливості використання Veeam Backup and Replication. Розглянуто різні підходи до резервного копіювання, такі як повне, інкрементне та диференціальне копіювання, їх переваги та недоліки.

У практичній частині роботи продемонстровано процес створення резервних копій віртуальних машин за допомогою Veeam Backup and Replication. Описано етапи налаштування резервного копіювання, створення резервних завдань та управління ними. Крім того, показано процес відновлення віртуальних машин з резервних копій, включаючи відновлення на різних рівнях – від окремих файлів до повної віртуальної машини.

Результатом проведеного дослідження є проєкт, заявлений у темі роботи, що демонструє інфраструктуру на базі Veeam Backup and Replication. Проєкт підтверджує, що даний інструмент є надійним та ефективним рішенням для захисту даних у віртуальних середовищах, забезпечуючи швидке та зручне відновлення у разі втрати даних.

Ключові слова: РЕЗЕРВНЕ КОПІЮВАННЯ, ВІДНОВЛЕННЯ, VEEAM BACKUP AND REPLICATION, ВІРТУАЛЬНІ МАШИНИ, ВІРТУАЛІЗАЦІЯ, ГІПЕРВІЗОР.

ККІК.КР.Б – 123 – 06 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата
Розроб.		Дехтяр М.С.		14.06.24
Керівник		Головня О.С.		14.06.24
Реценз.		Єфіменко А.А.		14.06.24
Н. контр.		Голоско О.С.		14.06.24
Затверд.		Єфіменко А.А.		14.06.24

Проект інфраструктури резервного копіювання для корпоративної мережі організації

Літ.	Арх.	Архивіс
	4	86

ФІКТ, Гр. КІ-20-1

ANNOTATION

The explanatory note contains: 81 pages of text, 37 figures, 4 tables, and 18 references.

The purpose of the work is to build a backup infrastructure project for the organisation's corporate network.

This paper descusses the creating backup copies of virtual machines using Veeam Backup and Replication. The stages of configuring backups, creating backup jobs, and managing them are described. In addition, the process of restoring virtual machines from backups is shown, including restoring at different levels - from individual files to a complete virtual machine.

The result of the research is the project stated in the thesis topic, which demonstrates an infrastructure based on Veeam Backup and Replication. The project confirms that this tool is a reliable and effective solution for protecting data in virtual environments, providing fast and convenient recovery in case of data loss.

Keywords: BACKUP, RECOVERY, VEEAM BACKUP AND REPLICATION, VIRTUAL MACHINES, VIRTUALIZATION, HYPERVISOR.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО РЕЗЕРВНЕ КОПІЮВАННЯ.....	10
1.1 Призначення технології резервного копіювання.....	10
1.2 Основні методи резервного копіювання.....	12
1.3 Види резервного копіювання.....	15
1.4. Основні етапи резервного копіювання	17
1.5. Методи відновлення даних	20
РОЗДІЛ 2 ПРОЄКТУВАННЯ ІНФРАСТРУКТУРИ РЕЗЕРВНОГО КОПІЮВАННЯ ДЛЯ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ.....	23
2.1 Аналіз вимог до системи резервного копіювання.....	23
2.2 Вибір віртуального середовища та програмного забезпечення.....	25
2.3 Архітектура мережі резервного копіювання.....	40
Висновок до другого розділу.....	54
РОЗДІЛ 3: Налаштування та тестування інфраструктури на базі Veeam Backup and Replication.....	56
3.1 Налаштування інфраструктури резервного копіювання.....	56
3.2 Створення та керування завданнями резервного копіювання.....	63
3.3 Тестування ефективності та надійності резервного копіювання.....	71
Висновок до третього розділу.....	80
ВИСНОВКИ.....	81
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	82
ДОДАТКИ.....	84

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Бекап (backup)- резервна копія

AD - Active Directory

ОС- операційна система

ОМV- Openmediavault

NAS- Network Attached Storage

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Інфраструктура резервного копіювання для корпоративної мережі організації є надзвичайно важливою складовою сучасного бізнесу. В умовах зростаючої кількості кіберзагроз, ризиків втрати даних через технічні збої або людські помилки, забезпечення надійного резервного копіювання стає ключовим аспектом для стабільного функціонування будь-якої компанії. Резервне копіювання дозволяє вирішити ряд критичних проблем, таких як забезпечення безперервності бізнес-процесів, захист від кіберзагроз, відповідність нормативним вимогам, збереження історичних даних та оптимізація витрат. Втрата важливих даних може призвести до значних фінансових збитків і зупинки діяльності організації. Наявність ефективної системи резервного копіювання дозволяє швидко відновити роботу у випадку втрати даних. Зростаюча кількість атак програм-ви-магачів та інших шкідливих програм становить серйозну загрозу для безпеки да-них, тому резервне копіювання забезпечує можливість відновлення даних без ви-плати викупу кіберзлочинцям. Багато галузей економіки мають суворі нормативні вимоги щодо зберігання та захисту даних, дотримання яких допомагає уникнути юридичних проблем і штрафів. Інвестування у надійне резервне копіювання доз-воляє уникнути значних витрат, пов'язаних з відновленням втраченої інформації та простоем бізнесу.

Метою кваліфікаційної роботи є розробка проєкту інфраструктури резерв-ного копіювання для корпоративної мережі організації.

Визначена мета обумовлює наступні завдання:

- Провести аналіз наявних технологій та методів резервного копіювання, оціни-ти їх переваги та недоліки.
- Визначити вимоги до апаратного та програмного забезпечення для реалізації інфраструктури резервного копіювання.
- Розробити проєкт інфраструктури резервного копіювання для корпоративної мережі організації.
- Розробити план впровадження системи резервного копіювання, включаючи етапи тестування та налаштування.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Об’єктом дослідження є процеси управління даними в корпоративних мережах, що охоплюють процеси зберігання, обробки, передачі та захисту інформації.

Предметом дослідження є інфраструктура резервного копіювання даних у корпоративній мережі організації, зокрема технології та методи резервного копіювання, планування та впровадження стратегії резервного копіювання, управління процесом резервного копіювання та відновлення даних, а також забезпечення безпеки та надійності збереженої інформації.

У процесі виконання кваліфікаційної роботи було розроблено проект інфраструктури резервного копіювання для корпоративної мережі організації, який включає вибір оптимальних технологій та методів резервного копіювання, розробку плану впровадження системи, а також рекомендації щодо забезпечення безпеки та надійності збереженої інформації.

Апробація результатів:

1. Дехтяр М.С., Головня О.С. Вакур інфраструктура для малих та середній підприємств на базі платформи Veeam Backup & Replication. Тези XIV Міжнародної науково-технічної конференції "Інформаційно-комп'ютерні технології - 2024", 28-29 березня 2024 року. Житомир : «Житомирська політехніка», 2024. С. 77-78.
2. Головня О.С., Магурін О.О., Дехтяр М.С. Добір віртуалізаційного програмного забезпечення для прототипу хмарної мережної інфраструктури. Тези VI Всеукраїнської науково-технічної конференції "Комп'ютерні технології: інновації, проблеми, рішення", 29-30 листопада 2023 року. Житомир : «Житомирська політехніка», 2023. С. 118-119.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО РЕЗЕРВНЕ КОПІЮВАННЯ

1.1 Призначення технології резервного копіювання

Технологія резервного копіювання є невід'ємною частиною сучасної інформаційної інфраструктури, забезпечуючи надійний захист даних від втрат та забезпечуючи їхню доступність у разі непередбачених ситуацій. Основна мета резервного копіювання полягає у створенні копій критично важливих даних, які можуть бути використані для їх відновлення у випадку збою, помилок користувачів, зловмисних дій або інших причин. Нижче наведено основні завдання, для яких призначені технології резервного копіювання. [4]

Захист від втрати даних

Одна з головних цілей резервного копіювання полягає у захисті даних від втрат, які можуть бути спричинені різними факторами, зокрема переліченими нижче.

- **Збої обладнання.** Жорсткі диски, сервери, системи зберігання даних та інші апаратні компоненти можуть виходити з ладу, що може призвести до втрати важливої інформації.
- **Програмні помилки.** Помилки в програмному забезпеченні, збої операційних систем або додатків можуть викликати пошкодження даних.
- **Людський фактор.** Випадкове видалення файлів, помилкове форматування дисків або інші дії користувачів можуть призвести до втрати важливої інформації.
- **Зловмисні дії.** Атаки зловмисників, такі як віруси, трояни, програми-зидирники та інші кіберзагрози, можуть пошкодити або видалити дані.

Резервні копії даних дозволяють мінімізувати ризик втрати інформації та забезпечують можливість її відновлення у випадку інцидентів.

Забезпечення безперервності бізнесу

Безперервність бізнесу є критично важливою для будь-якої організації. Втрата даних або тривалий простій можуть призвести до значних фінансових втрат, завда-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

ння шкоди репутації та інших негативних наслідків. Технології резервного копіювання відіграють ключову роль у забезпеченні безперервності бізнесу, дозволяючи швидко відновити роботу після інцидентів, зокрема за наступними напрямками.

- **Швидке відновлення.** Сучасні технології резервного копіювання дозволяють швидко відновити дані та системи, що мінімізує час простою та знижує вплив інцидентів на бізнес.
- **Планування відновлення після аварій.** Резервне копіювання є важливою складовою планів відновлення після аварій, які включають процедури та стратегії відновлення даних і систем у разі великих катастрофічних подій.

Збереження історичних даних

Резервне копіювання також дозволяє зберігати історичні версії даних, що може бути корисним для різних цілей, у тому числі наступних.

- **Аудит та комплаєнс.** Збереження історичних даних є важливим для дотримання вимог регуляторних органів та проведення аудитів. Організації можуть зберігати резервні копії як доказу відповідності вимогам законодавства.
- **Аналіз даних.** Історичні резервні копії можуть використовуватися для аналізу даних, виявлення трендів та проведення досліджень.
- **Відновлення попередніх версій.** У разі помилкових змін або пошкодження даних, резервні копії дозволяють відновити попередні версії файлів або баз даних.

Підтримка гнучкості та масштабованості

Сучасні технології резервного копіювання забезпечують високу гнучкість та масштабованість, що дозволяє організаціям адаптувати рішення під наступні свої потреби.

- **Підтримка різних середовищ.** Резервне копіювання може здійснюватися для фізичних серверів, віртуальних машин, хмарних середовищ та інших інфраструктур.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Масштабованість.** Технології резервного копіювання дозволяють легко масштабувати рішення в міру зростання об'ємів даних та змін у вимогах бізнесу.
- **Гнучкість налаштувань.** Можливість налаштування різних параметрів резервного копіювання, таких як частота, тип резервних копій (повні, інкрементальні, диференціальні), шифрування даних та інші.

Забезпечення безпеки даних

Захист резервних копій від несанкціонованого доступу та зловмисних дій є важливим аспектом безпеки даних. Технології резервного копіювання включають різні методи для забезпечення безпеки, зокрема перелічені нижче.

- **Шифрування.** Резервні копії можуть шифруватися для захисту даних від несанкціонованого доступу.
- **Аутентифікація та контроль доступу.** Системи резервного копіювання забезпечують аутентифікацію користувачів та контроль доступу до резервних копій, що дозволяє обмежити доступ до лише авторизованих осіб.
- **Захист від змін.** Резервні копії можуть бути захищені від змін або видалення, що забезпечує їхню цілісність та надійність.

Таким чином, технологія резервного копіювання виконує важливі функції щодо захисту даних, забезпечення безперервності бізнесу, збереження історичних даних, підтримки гнучкості та масштабованості, а також забезпечення безпеки даних. Ці функції є критично важливими для успішної роботи сучасних організацій в умовах постійних загроз та швидких змін у інформаційному середовищі.

1.2 Основні методи резервного копіювання

Основні принципи бекапу визначаються потребами організації щодо забезпечення безпеки та доступності даних. Кожен принцип має свої переваги та обмеження, які варто враховувати при виборі стратегії бекапу. [5] [13]

Повний бекап є найбільш об'ємистим і затратним у ресурсах методом, оскільки він передбачає створення повної копії всіх даних. Проте він є найпростішим у відновленні, оскільки для відновлення даних потрібна лише остання

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

повна копія та жодних інших диференційних або інкрементальних копій.

Припустимо, що у вас є сервер, на якому зберігаються важливі дані компанії. Для здійснення повного бекапування ви створюєте копію всіх даних на цьому сервері. Перша повна копія може зайняти значну кількість часу та ресурсів, оскільки потрібно скопіювати всі файли та дані з сервера. Припустимо, що ви зробили перший повний бекап у п'ятницю о 18:00, а повністю операція бекапування закінчиться лише ввечері в суботу. Через значну тривалість та ресурсомісткість створення повних бекапів нерідко використовується наступний метод бекапування.

Інкрементальне бекапування ефективно використовує простір для зберігання, оскільки зберігає лише зміни з моменту попередньої копії. Проте для відновлення даних потрібно мати доступ до оригінальної повної копії та всіх інкрементальних копій з моменту останньої повної копії, що може ускладнити процес відновлення.

Припустимо, що у вас є сервер з важливими даними, і ви використовуєте інкрементальне бекапування для збереження цих даних. Перший повний бекап був створений в п'ятницю о 18:00. Далі, кожну годину ви створюєте інкрементальний бекап, який зберігає лише зміни, які відбулися після попереднього бекапу.

Наприклад, після першого повного бекапу ви створили інкрементальний бекап о 19:00, який зберігає всі зміни, які відбулися за годину після першого бекапу. Наступний інкрементальний бекап створюється о 20:00 і зберігає всі зміни, які відбулися за цю годину. Якщо відбувається втрата даних або потрібно відновити дані до конкретної точки у часі, вам спочатку потрібно відновити останній повний бекап, який містить всі дані станом на п'ятницю о 18:00. Після цього ви відновлюєте всі інкрементальні бекапи, які були створені після цього часу, починаючи з останнього інкрементального бекапу. Цей підхід дозволяє ефективно використовувати простір для зберігання, оскільки ви зберігаєте лише зміни, які відбулися після останнього повного бекапу, а не всі файли знову.

Диференційне бекапування забезпечує проміжний підхід між повним бекапом і інкрементальним бекапуванням. Воно зберігає всі зміни від початку створен-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

ня диференційних копій, що дозволяє відновлювати дані за допомогою останньої повної копії та останньої диференційної копії.

Диференційне бекапування передбачає створення копії всіх змінених або нових даних з моменту останнього повного бекапу. Наприклад, якщо перший повний бекап був зроблений в п'ятницю, то кожен наступний диференційний бекап буде містити всі зміни, які були внесені до даних після п'ятничного бекапу. Основна перевага диференційного бекапу полягає в тому, що для відновлення даних потрібно мати доступ лише до останнього повного бекапу та останнього диференційного бекапу. Це робить процес відновлення даних менш складним у порівнянні з інкрементальним бекапуванням, де потрібно мати доступ до всіх інкрементальних копій з моменту останнього повного бекапу.

Проте, недоліком диференційного бекапу є те, що з часом розмір копій може зростати, оскільки вони зберігають всі зміни з моменту останнього повного бекапу. Тому важливо регулярно виконувати повні бекапи, щоб уникнути надмірного збільшення розміру копій. [6]

Спектральне бекапування є найбільш ефективним у відновленні даних, оскільки воно створює точну копію даних у реальному часі. Проте воно вимагає великих обсягів простору для зберігання та високих витрат на обладнання.

Вибір оптимального принципу бекапу залежить від конкретних потреб та можливостей організації. Комбінація різних принципів може бути використана для забезпечення найбільш ефективного та надійного захисту даних.

Спектральне бекапування є одним з найефективніших методів забезпечення безпеки даних. У цьому методі кожен біт даних зберігається неодноразово на різних носіях, що дозволяє відновити дані в разі втрати одного з носіїв. Наприклад, уявімо собі організацію, яка використовує спектральне бекапування для збереження своїх даних. Кожен раз, коли користувач зберігає документ, програма автоматично робить кілька копій цього документа на різних серверах або зовнішніх носіях. Це забезпечує захист даних від втрати в разі виходу з ладу одного з серверів або носіїв. У разі відновлення даних, користувач може використати програму для відновлення останньої збереженої версії документа з іншого сервера або носія. Та-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

кий підхід гарантує, що дані завжди доступні і захищені від втрати. Спектральне бекапування є надійним методом забезпечення безпеки даних і використовується в багатьох сферах, де безпека даних є важливою, таких як фінансові установи, медичні установи та інші.

Метод бекапування снапшотами (точкове бекапування, snapshot backup) використовується для створення точних копій даних у певний момент часу. Снапшот - це віртуальна копія файлової системи або диска, яка фіксує стан даних на певний момент часу без копіювання кожного файлу окремо.

Приклад використання снапшотів може бути таким: у вас є сервер з базою даних, і ви регулярно створюєте снапшоти цієї бази даних. Кожен снапшот фіксує стан бази даних у певний момент часу, дозволяючи відновити дані до цього стану в майбутньому, якщо виникне потреба. Однією з переваг снапшотів є швидкість їх створення та відновлення. Оскільки снапшот фіксує лише зміни з моменту попереднього снапшоту, а не всі дані знову, це може значно зменшити час, потрібний для створення копії даних та відновлення їх до попереднього стану. Проте слід зазначити, що снапшоти зазвичай зберігаються на тому ж самому пристрої, що і дані, тому вони можуть бути вразливі до втрати в разі пошкодження пристрою. Тому важливо додатково зберігати снапшоти на інших носіях або в інших місцях для забезпечення надійності бекапування.

1.3 Види резервного копіювання

У даному підрозділі розглядаються різновиди резервного копіювання, такі як локальне, віддалене та хмарне. Кожен вид копіювання розглядається з точки зору сфери застосування та особливостей використання. [12]

Локальне резервне копіювання (Local Backup). Цей вид передбачає створення копій даних на пристроях, що знаходяться у тому ж місці, що й джерело даних. Локальне копіювання зазвичай використовується для невеликих обсягів даних та вимагає від користувача наявності фізичного доступу до пристрою для відновлення даних.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Локальне копіювання даних може бути реалізоване за допомогою зовнішнього жорсткого диска, який підключається до комп'ютера або сервера. Наприклад, організація може щоденно створювати повні копії важливих даних на зовнішній жорсткий диск через програмне забезпечення резервного копіювання.

Копії даних можна створювати за допомогою програмного забезпечення, що автоматично робить резервні копії зазначених файлів та папок на підключений зовнішній жорсткий диск. Такий метод забезпечує відносно швидке відновлення даних у випадку втрати або пошкодження оригіналу. Після закінчення копіювання зовнішній жорсткий диск може бути відключений від комп'ютера та зберігатися в безпечному місці, щоб запобігти втраті даних через фізичні пошкодження або крадіжку.

Віддалене резервне копіювання (Offsite Backup). Цей вид включає передачу копій даних на віддалені сервери або пристрої для зберігання даних. Віддалене копіювання забезпечує захист даних від фізичних ризиків, таких як пожежі, повені або крадіжки, але вимагає наявності надійного Інтернет-з'єднання для передачі даних.

Віддалене копіювання даних може бути реалізоване за допомогою використання віддалених серверів або хмарних сервісів для зберігання копій даних. Наприклад, організація може використовувати спеціальні сервіси резервного копіювання, які автоматично відправляють копії даних на віддалений сервер через Інтернет. Після налаштування сервісу резервного копіювання, дані автоматично копіюються на віддалений сервер у зашифрованому вигляді для забезпечення безпеки під час передачі. Цей процес може відбуватися з регулярністю, наприклад, щоденно або щогодини, залежно від налаштувань. У випадку втрати або пошкодження оригінальних даних, організація може відновити їх з віддаленого сервера. Для цього важливо мати доступ до Інтернету та правильні дозволи на відновлення даних з віддаленого сховища. Віддалене копіювання дозволяє забезпечити надійний захист даних від фізичних ризиків, таких як пожежі або повені, оскільки копії знаходяться в безпечному місці, віддаленому від місця джерела даних.

Хмарне резервне копіювання (Cloud Backup). Цей вид передбачає зберігання копій даних на серверах хмарних сервісів. Він дозволяє зберігати великі об-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

сяги даних без необхідності володіння власними фізичними пристроями для зберігання. Хмарне копіювання зазвичай використовується для автоматизації резервного копіювання та забезпечення доступності даних з будь-якої точки з'єднання з Інтернетом.

Хмарне копіювання даних використовує хмарні сервіси для зберігання копій інформації. Наприклад, компанія може використовувати платний хмарний сервіс, який автоматично копіює дані на серверах по всьому світу через Інтернет.

Користувачі можуть встановити програмне забезпечення, яке автоматично відправляє копії даних до хмари. Це може бути налаштовано для регулярного або надзвичайного резервного копіювання. Завдяки хмарному зберігання, дані можна відновити з будь-якого місця, де є доступ до Інтернету, що забезпечує високу доступність даних. Однією з переваг хмарного копіювання є його гнучкість і масштабованість. Користувач може зберігати стільки даних, скільки потрібно, без необхідності покупки додаткового обладнання. Хмарне зберігання також може забезпечити захист даних від фізичних пошкоджень або крадіжки, оскільки дані зберігаються на віддалених серверах.

Кожен з цих методів має свої особливості використання та вимоги до інфраструктури, тому вибір конкретного методу залежить від потреб користувача та характеристик його системи.

1.4. Основні етапи резервного копіювання

Процес резервного копіювання включає кілька етапів, що дозволяють забезпечити безпеку даних і відновлення інформації у випадку втрати або пошкодження оригіналу. Основні етапи процесу резервного копіювання є наступними.

Підготовка до копіювання. На цьому етапі визначаються дані, які потрібно скопіювати, і вибирається метод копіювання. Також важливо встановити регулярність копіювання та місце збереження резервних копій.

Підготовка до копіювання даних передбачає ретельне планування і визначення параметрів процесу копіювання. Наприклад, перед початком копіювання необхідно зробити аналіз даних, визначити їх важливість та критичність для подальшої

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

роботи організації. Також слід врахувати можливі ризики, що можуть виникнути під час процесу копіювання, і розробити план їх усунення.

Після визначення обсягу та видів даних для копіювання важливо вибрати оптимальний метод копіювання. Наприклад, для даних, які змінюються рідко, можна використовувати повне копіювання, а для постійно змінюваних даних - інкрементальне або диференційне копіювання. Додатково, варто встановити регулярність копіювання, яка може бути щоденною, щотижневою або за іншим графіком, залежно від потреб організації та частоти змін у даних. Також важливо визначити час копіювання, щоб мінімізувати вплив на продуктивність робочого процесу.

У цілому, підготовка до копіювання даних - це складний процес, який вимагає уважного аналізу та планування, але він дозволяє забезпечити надійний та безпечний захист даних організації.

Вибір методу копіювання. Залежно від потреб і можливостей організації вибирається метод копіювання. Це може бути повний, інкрементальний, диференційний, спектральний або інший метод копіювання, який найкраще підходить для конкретних потреб.

При резервному копіюванні даних можна використовувати різні методи, такі як повне копіювання або інкрементальне копіювання. Наприклад, якщо ви вирішили використовувати повне копіювання, то кожен раз у вас буде повний обсяг копійованих даних. Це може займати багато часу і ресурсів, але забезпечить повну безпеку даних. З іншого боку, якщо ви використовуєте інкрементальне копіювання, система буде копіювати лише ті файли, які були змінені після попереднього резервного копіювання. Це ефективний метод, який зменшує час і обсяг даних, які потрібно копіювати, але може зростати кількість копій, які необхідно зберігати для повного відновлення даних.

Виконання копіювання. Після підготовки та вибору методу копіювання виконується сам процес копіювання даних. Дані копіюються з джерела на обране місце збереження, де створюються резервні копії.

При виборі місця для збереження резервних копій даних важливо враховувати доступність, безпеку та надійність зберігання. Наприклад, для локального

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

копіювання можна використовувати зовнішній жорсткий диск, який підключається до комп'ютера або сервера за допомогою USB або іншого інтерфейсу. Цей метод забезпечує швидкий доступ до даних і може бути ефективним для невеликих обсягів даних.

Також можна використовувати мережеве сховище (Network Attached Storage, NAS) для збереження резервних копій. NAS підключається до мережі і може забезпечити централізоване зберігання даних для всіх пристроїв у мережі. Це зручно для резервного копіювання даних з кількох комп'ютерів або серверів.

Іншим варіантом може бути використання хмарного сховища для збереження резервних копій. Хмарне сховище дозволяє зберігати дані в інтернеті, що забезпечує високу доступність і захист даних від фізичних пошкоджень або крадіжок.

Вибір конкретного методу залежить від потреб організації, обсягу даних та рівня безпеки, який вимагається для збереження даних.

Збереження резервних копій. Після завершення копіювання резервні копії даних зберігаються у безпечному місці. Це може бути зовнішній жорсткий диск, мережеве сховище, віддалений сервер або хмарне сховище.

Процес резервного копіювання допомагає забезпечити безпеку даних та готовність до відновлення інформації у випадку непередбачених обставин. Важливо регулярно перевіряти та оновлювати процес копіювання для забезпечення ефективного захисту даних.

Один із ключових аспектів планування - це визначення часу початку копіювання. Часто його рекомендують проводити в нічний час, коли навантаження на мережу і сервер менше, щоб уникнути впливу на продуктивність роботи. Тривалість копіювання повинна бути оптимальною, щоб не перешкоджати іншим процесам організації. Важливо врахувати інтервали між копіюванням. Вони можуть бути різними залежно від частоти змін у даних. Наприклад, для важливих даних можна встановити щоденне або навіть кількаразове копіювання на день, а для менш критичних даних - щотижневе або менш часте. Крім цього, план копіювання має передбачати моніторинг процесу копіювання та можливість коригування в разі виявлення проблем. Наприклад, автоматичні повідомлення про стан резервного

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

копіювання дозволять оперативно реагувати на виникнення проблем та забезпечити безперервність процесу.

В цілому, план копіювання даних є важливим елементом будь-якої інформаційної стратегії організації і дозволяє забезпечити надійний захист важливої інформації.

1.5. Методи відновлення даних

Відновлення даних з резервних копій - це важлива складова стратегії захисту даних. Для відновлення даних зазвичай використовуються різні методи, залежно від типу та обсягу копіювання.

Повне відновлення з повного бекапу. Цей метод використовується для повного відновлення всіх даних з повного бекапу. Він є найпростішим способом відновлення, оскільки всі дані знаходяться в одному місці і не потребують додаткових операцій.

Припустимо, що компанія має регулярно створювані повні резервні копії даних. У випадку втрати або пошкодження оригінальних даних, вони можуть використовувати ці бекапи для відновлення інформації. Наприклад, якщо сервер зазнав несправності або був підданий кібератаці, інформацію можна відновити з останнього повного бекапу. Для цього адміністратор встановлює час, коли бекап був створений, та відновлює дані з цього бекапу на основний сервер або на інше місце збереження. Таким чином, компанія може відновити свою роботу із збереженням усіх необхідних даних.

Відновлення з інкрементального бекапу. Інкрементальний бекап зберігає лише змінені або нові файли з моменту останнього повного або інкрементального бекапу. Для відновлення даних потрібно спочатку відновити останній повний бекап, а потім накладати на нього інкрементальні копії за потреби.

Припустимо, що після нещасного випадку чи кібератаки компанія втратила частину своїх даних. Вони використовують систему інкрементального бекапу для збереження інформації про змінені файли з моменту останнього повного або інкрементального бекапу. Щоб відновити дані, спочатку відновлюється останній повний бекап, який містить основний обсяг інформації. Після цього на цей повний бекап

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

накладаються інкрементальні бекапи за кожен день, починаючи від дня попереднього бекапу до дня, коли сталася проблема. Таким чином, шляхом поетапного відновлення останнього повного бекапу та послідовного накладання на нього інкрементальних бекапів можна відновити дані до останнього збереженого стану.

Відновлення з диференційного бекапу. Диференційний бекап зберігає всі змінені файли з моменту останнього повного бекапу. Для відновлення даних потрібно відновити останній повний бекап, а потім додати до нього всі зміни з диференційних копій.

Таким чином, можна відновити дані до певного моменту часу, використовуючи лише останній повний бекап та всі зміни з диференційних копій, що дозволяє зменшити час відновлення порівняно з повним відновленням з інкрементальних копій.

Відновлення з точкового бекапу (Snapshot Backup). Точковий бекап зберігає стан системи на певний момент часу. Для відновлення даних потрібно відновити систему до стану на момент створення точкового бекапу.

Даний метод дозволяє відновити систему до певного моменту часу, зберігаючи всі дані та налаштування, які були актуальні на цей момент. Точкові бекапи є швидким та ефективним способом відновлення системи після втрати даних або неполадок, оскільки вони дозволяють відновити систему до попереднього стану без необхідності відновлення кожного файлу окремо.

Кожен з цих методів має свої переваги і недоліки, і вибір методу відновлення залежить від потреб і можливостей організації.

Висновки до першого розділу

У першому розділі розглянуто фундаментальні аспекти технології резервного копіювання, які мають ключове значення для забезпечення безпеки та цілісності даних у корпоративних середовищах. Технологія резервного копіювання є критично важливою для захисту даних від втрат, викликаних різноманітними факторами, такими як апаратні збої, помилки користувачів, віруси та зловмисні атаки. Ці загрози можуть мати серйозні наслідки для організацій, включаючи втрату важливої інформації та значні фінансові збитки. Резервне копіювання дозволяє швидко від-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

новлювати дані та мінімізувати час простою бізнес-процесів, що є надзвичайно важливим для забезпечення безперервності бізнесу.

Використання різних підходів до резервного копіювання, таких як інкрементальне, диференційоване та повне резервне копіювання, дозволяє оптимізувати використання ресурсів та забезпечити надійне збереження інформації. Таким чином, розуміння та впровадження фундаментальних аспектів технології резервного копіювання є критично важливими для кожної організації.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ ІНФРАСТРУКТУРИ РЕЗЕРВНОГО КОПІЮВАННЯ ДЛЯ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1 Аналіз вимог до системи резервного копіювання

Для ефективного проєктування корпоративної мережі резервного копіювання важливо провести детальний аналіз вимог до системи. Цей аналіз дозволяє визначити основні параметри, які будуть впливати на вибір апаратного та програмного забезпечення, архітектуру мережі, а також на процеси резервного копіювання та відновлення даних. Основні аспекти, які потрібно врахувати під час аналізу, включають обсяги даних, частоту резервного копіювання, вимоги до безпеки та час відновлення.

Перше, що потрібно визначити, це обсяги даних, які необхідно копіювати. Це включає як загальний обсяг даних, так і типи даних (документи, бази даних, електронна пошта тощо). Необхідно також врахувати темпи зростання обсягу даних, щоб система резервного копіювання могла масштабуватися відповідно до потреб компанії. Важливо проаналізувати, які дані є критичними для бізнесу і які з них потрібно резервувати частіше.

Частота резервного копіювання залежить від важливості даних і від того, наскільки часто вони змінюються. Наприклад, критичні дані, які змінюються щогодини, можуть потребувати частого копіювання (щогодинного або навіть безперервного), тоді як менш важливі дані можна копіювати раз на день або раз на тиждень. Визначення оптимальної частоти резервного копіювання допомагає забезпечити баланс між витратами на зберігання даних і вимогами до їх доступності.

Захист даних є ключовим аспектом будь-якої системи резервного копіювання. Важливо врахувати вимоги до безпеки, які включають шифрування даних під час зберігання і передачі, а також контроль доступу до резервних копій. Необхідно також врахувати відповідність системи резервного копіювання вимогам законодавства та галузевим стандартам щодо захисту даних. Крім того, важливо розробити політику безпеки, яка включає регулярне тестування відновлення даних для перевірки їхньої цілісності та доступності.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

Час відновлення є критичним параметром, який визначає, скільки часу знадобиться на відновлення даних у разі збою або втрати. Це включає як час, необхідний для відновлення окремих файлів, так і для повного відновлення системи. Важливо встановити цілі щодо часу відновлення (RTO – Recovery Time Objective) і максимально допустимого обсягу втрат даних (RPO – Recovery Point Objective). Ці параметри допомагають визначити, які технології і методи резервного копіювання слід використовувати для досягнення необхідного рівня доступності даних.

Крім основних аспектів, важливо також врахувати додаткові вимоги, такі як сумісність з наявною інфраструктурою, простота управління системою, можливості для автоматизації процесів резервного копіювання та відновлення, а також загальні витрати на впровадження та підтримку системи резервного копіювання. Проведення детального аналізу вимог до системи резервного копіювання дозволяє створити ефективну, надійну та масштабовану систему, яка відповідає потребам компанії та забезпечує безпеку і доступність критичних даних. [5]

Для практичного підрозділу системи резервного копіювання, проєктована інфраструктура включає наступні вимоги.

Обсяги даних:

- Сервери Active Directory для забезпечення корпоративної системи.
- Віртуальні машини AD на Hyper-V і VMware ESXi.
- Файлові сервери на базі OpenMediaVault для зберігання файлів резервних копій.

Частота резервного копіювання:

- Щоденне резервне копіювання всіх критичних даних.
- Інкрементальні копії кожні 6 годин.

Вимоги до безпеки:

- Використання шифрування даних під час зберігання і передачі.
- Контроль доступу до резервних копій за допомогою системи аутентифікації і авторизації.

Час відновлення:

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

- Встановлено RTO для AD сервера – не більше 4 годин.
- Встановлено RPO для файлових серверів – не більше 1 години.
- Відновлення окремих файлів та конфігурацій повинно здійснюватись в межах 30 хвилин.

Сумісність з інфраструктурою:

- Інтеграція з наявними серверами VMware, Hyper-V, та файловими серверами на базі OpenMediaVault.
- Простота управління за допомогою централізованого управління через Veeam Backup & Replication.

Автоматизація процесів:

- Автоматизовані сценарії резервного копіювання для мінімізації ручної роботи.
- Регулярне тестування відновлення даних для забезпечення цілісності резервних копій.

2.2 Вибір віртуального середовища та програмного забезпечення

У цьому підрозділі розглядається вибір засобів та програмного забезпечення для створення ефективної та надійної системи резервного копіювання корпоративної мережі. Основна увага приділяється серверному обладнанню, сховищам даних і вибору програмного забезпечення для резервного копіювання, зокрема Veeam Backup and Replication.

Вибір гіпервізора. У таблиці 1.1 наведено результати порівняння гіпервізорів VMware Workstation, Oracle VirtualBox, Parallels Desktop, MS Hyper-V, KVM та QEMU. Під час порівняння враховано підтримку різних гостьових ОС, інтеграцію з хмарою, легкість використання, підтримку технології Snapshots, ліцензійні витрати та надійність.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 1.1 – порівняння гіпервізорів.

Гіпервізор	Підтримка різних ОС	Інтеграція з хмарою	Легкість використання	Підтримка Snapshots	Ліцензійні витрати	Надійність
VMware Workstation	+	+	+	+	+	+
VirtualBox	+	-	+	+	-	-
Parallels Desktop	+	+	+	+	+	+
Hyper-V	+	+	-	+	+/- залежить від версії	+/-
KVM	+	+	-	+	-	+
QEMU	+	+	-	+	-	+/-

Для реалізації частини інфраструктури було обрано VMware Workstation Pro. Гіпервізор є потужним і багатофункціональним рішенням для десктопної віртуалізації, яке дозволяє запускати кілька операційних систем на одному фізичному комп'ютері. Цей продукт відомий своєю стабільністю, високою продуктивністю та широким набором можливостей для розробників, тестувальників та ІТ-фахівців.

Workstation Pro підтримує широкий спектр операційних систем, включаючи Windows, Linux та інші. Це дозволяє користувачам запускати різні операційні системи на одному фізичному комп'ютері, що є особливо корисним для розробки та тестування програмного забезпечення. Графічний інтерфейс є інтуїтивно зрозумілим і зручним у використанні. Він дозволяє легко створювати, налаштовувати та керувати віртуальними машинами. Користувачі можуть просто перетягувати файли між віртуальними машинами та основною системою, налаштовувати параметри мережі та зберігання, а також створювати та управляти моментальними знімками (snapshots). Продукт забезпечує високу продуктивність віртуальних машин завдяки оптимізації використання апаратних ресурсів. Він підтримує багатоядерні процесори, великий обсяг оперативної пам'яті та сучасні технології зберігання даних, що дозволяє запускати ресурсоємні додатки та операційні системи без значно-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

го впливу на продуктивність основної системи. Користувачі можуть створювати моментальні знімки віртуальних машин для збереження стану системи на конкретний момент часу. Це особливо корисно для тестування та відкату змін. Крім того, Workstation Pro підтримує клонування віртуальних машин, що дозволяє швидко створювати копії існуючих середовищ для тестування або розробки. Це рішення інтегрується з іншими продуктами VMware, такими як VMware vSphere. Це дозволяє легко переносити віртуальні машини між десктопним середовищем та хмарною інфраструктурою, забезпечуючи безперервність роботи та гнучкість управління віртуальними середовищами. Workstation Pro пропонує розширені можливості налаштування мережі, включаючи підтримку віртуальних локальних мереж (VLAN), налаштування мережевих адаптерів та створення ізольованих мереж для тестування. Це дозволяє користувачам створювати складні мережеві топології для симуляції різних сценаріїв. Ця програма підтримує шифрування віртуальних машин, що забезпечує захист даних від несанкціонованого доступу. Це особливо важливо для корпоративних користувачів, які працюють з конфіденційною інформацією.

Workstation Pro є ідеальним рішенням для різних категорій користувачів. Розробники програмного забезпечення можуть використовувати його для створення різних тестових середовищ, що дозволяє легко тестувати програми на різних операційних системах та конфігураціях. Системні адміністратори використовують Workstation Pro для налаштування та тестування серверних систем, симуляції мережевих середовищ та відпрацювання сценаріїв відновлення після аварій. Тестувальники можуть створювати та використовувати різні конфігурації систем для тестування програмного забезпечення, забезпечуючи високу якість продукту перед його випуском. Навчальні заклади використовують Workstation Pro для навчання студентів роботі з різними операційними системами, мережевими технологіями та програмним забезпеченням.

Цей продукт є потужним інструментом для віртуалізації, який забезпечує високу продуктивність, гнучкість та зручність у використанні. Його широкі можливості дозволяють користувачам ефективно створювати та керувати віртуальними машинами, тестувати різні конфігурації систем та забезпечувати безперервність

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

бізнесу. Завдяки інтеграції з іншими продуктами VMware та підтримці різних операційних систем, Workstation Pro є незамінним інструментом для розробників, тестувальників та системних адміністраторів.

Вибір віртуального середовища (Virtual environment). У табл. 1.2 продемонстровано результати порівняння віртуальних середовищ Proxmox VE, VMware vSphere, MS Hyper-V, oVirt, XenServer та OpenStack, враховуючи наявність у них підтримки віртуальних машин на базі KVM, віртуальних контейнерів на базі LXC, інтеграцію з хмарою, наявність веб-інтерфейсу, підтримку кластерів та ліцензійні витрати.

Таблиця 1.2 – порівняння засобів віртуалізації.

Віртуальне середовище	Підтримка KVM	Підтримка LXC	Інтеграція з хмарою	Управління через веб-інтерфейс	Підтримка кластерів	Ліцензійні витрати
Proxmox VE	+	+	+	+	+	-
VMware vSphere	-	-	+	+	+	+
Microsoft Hyper-V	-	-	+	+	+	+/-
oVirt	+	-	+	+	+	-
XenServer (Citrix Hypervisor)	-	-	+	+	+	+
OpenStack	+	+	+	+	+	-

Proxmox Virtual Environment (VE) є потужною платформою для віртуалізації з відкритим вихідним кодом, що поєднує віртуалізацію на основі KVM і контейнеризацію LXC.

VMware vSphere є комерційною платформою віртуалізації, яка пропонує широкий набір функцій для підприємств, але має високі ліцензійні витрати. Microsoft Hyper-V інтегрований у Windows Server і забезпечує надійну віртуалізацію, особливо в середовищах, що використовують інші продукти Microsoft, однак обмежений функціональністю у безкоштовній версії. oVirt є рішенням з відкритим вихідним

кодом, схожим на Proxmox, але вимагає складнішої конфігурації та підтримки. XenServer (Citrix Hypervisor) також є безкоштовним з опціями для платних функцій, але менш зручний для новачків. OpenStack забезпечує масштабовану віртуалізацію для великих хмарних середовищ, проте потребує значних ресурсів для впровадження та обслуговування.

Proxmox VE поєднує в собі простоту використання, потужний функціонал та відкритий вихідний код, що робить його привабливим для малого та середнього бізнесу, а також для індивідуальних користувачів. Він підтримує обидві технології віртуалізації (KVM і LXC), що забезпечує гнучкість і масштабованість. Інтуїтивний веб-інтерфейс полегшує управління і налаштування, а наявність великої спільноти користувачів та документації сприяє швидкому вирішенню проблем і оптимізації налаштувань. Вибір Proxmox VE виправданий для тих, хто шукає безкоштовне або економічно вигідне рішення з широкими можливостями віртуалізації та контейнеризації без необхідності значних ресурсів на впровадження та підтримку.

Ця платформа забезпечує високу продуктивність завдяки використанню сучасних технологій віртуалізації та оптимізації ресурсів. Proxmox підтримує багатоядерні процесори, великі об'єми оперативної пам'яті та сучасні технології зберігання даних, що дозволяє запускати ресурсоємні додатки та операційні системи з високою ефективністю. Важливою особливістю є можливість створення кластерів з високою доступністю (HA), що забезпечує безперервну роботу критично важливих додатків і сервісів. Це досягається за допомогою автоматичного перемикання на резервні вузли у випадку відмови основного вузла, що мінімізує час простою і втрату даних.

Proxmox підтримує резервне копіювання і відновлення даних на рівні віртуальних машин і контейнерів. Це дозволяє забезпечити захист даних і швидке відновлення у разі збоїв або втрати даних. Інтегровані інструменти резервного копіювання дозволяють автоматизувати процес створення копій і відновлення, що значно спрощує управління інфраструктурою. Програмне забезпечення також підтримує різні методи зберігання даних, включаючи локальні диски, мережеві файлові

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

системи (NFS), iSCSI та інші. Це дозволяє використовувати наявні ресурси зберігання і легко інтегрувати Proxmox в наявну IT-інфраструктуру.

Proxmox має вбудовані інструменти для моніторингу та звітності, що дозволяють відстежувати стан системи, продуктивність віртуальних машин і контейнерів, а також виявляти і усувати потенційні проблеми. Інтеграція з іншими системами моніторингу, такими як Zabbix і Nagios, забезпечує додаткові можливості для адміністраторів. Proxmox активно підтримується і розвивається спільнотою розробників та ентузіастів. Це забезпечує регулярні оновлення, нові функції та виправлення помилок, що робить платформу стабільною і надійною для використання в промислових умовах.

Proxmox є ідеальним рішенням для організацій різного масштабу, які шукають потужну, гнучку і надійну платформу для віртуалізації. Його відкритий вихідний код, висока продуктивність, підтримка кластерів з високою доступністю і широкий спектр функцій роблять Proxmox відмінним вибором для розгортання і управління віртуальними середовищами.

Вибір операційної системи для інфраструктури резервного копіювання

Сервери для резервного копіювання виконують роль центрального вузла, який керує процесами резервного копіювання і відновлення даних. Вибір серверів залежить від обсягу даних, частоти резервного копіювання та вимог до часу відновлення. Сервери повинні мати достатню обчислювальну потужність, оперативну пам'ять і ємність для зберігання тимчасових файлів резервних копій. Рекомендовано обирати сервери з багатоядерними процесорами, великим обсягом оперативної пам'яті та високошвидкісними дисковими системами.

Ubuntu Server є популярним вибором для серверних рішень, завдяки своїй стабільності, простоті налаштування та великій кількості доступних пакетів. Він є відмінним вибором для тих, хто шукає відкрите програмне забезпечення без ліцензійних витрат. Однак, налаштування Veeam Backup and Replication на Ubuntu може вимагати додаткових зусиль для забезпечення повної сумісності, особливо у середовищах, де активно використовуються продукти Microsoft.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

CentOS, заснований на Red Hat Enterprise Linux, є надійною платформою з тривалим циклом підтримки. Це стабільне і передбачуване рішення, яке підходить для середовищ, що потребують високої стабільності. Втім, налаштування Veeam Backup and Replication на CentOS також може вимагати додаткових знань і зусиль для повного налаштування та забезпечення сумісності з усіма необхідними компонентами.

Red Hat Enterprise Linux є комерційним дистрибутивом, що пропонує високий рівень підтримки та стабільності. Він часто використовується у великих підприємствах, де потрібна сертифікована та підтримувана операційна система. Хоча RHEL є надійним і підтримується, його використання передбачає значні ліцензійні витрати. Крім того, налаштування Veeam Backup and Replication на RHEL може бути складнішим і вимагати більш глибоких технічних знань.

Windows Server є ідеальною платформою для розгортання Veeam Backup and Replication завдяки своїм широким можливостям, надійності та високій продуктивності. Операційна система надає стабільне середовище для роботи з резервними копіями та відновленням даних, забезпечуючи високий рівень безпеки і сумісність з різними програмними продуктами.

Однією з основних переваг використання Windows Server як бази для Veeam Backup and Replication є її надійність і продуктивність. Ця операційна система підтримує сучасні апаратні рішення, включаючи багатоядерні процесори, великі об'єми оперативної пам'яті та швидкі дискові підсистеми. Це дозволяє ефективно обробляти великі об'єми даних і забезпечувати високу швидкість резервного копіювання і відновлення.

Windows Server включає покращені функції безпеки, такі як Credential Guard і Device Guard, що є важливими для захисту резервних даних від несанкціонованого доступу та атак. Credential Guard захищає облікові дані, використовуючи апаратні засоби безпеки, а Device Guard дозволяє створювати політики для запуску тільки довірених додатків. Це забезпечує додатковий рівень захисту для серверів резервного копіювання.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Інтеграція з Active Directory у Windows Server надає можливість централізованого управління обліковими записами та доступом до ресурсів. Це спрощує управління правами доступу до резервних копій та налаштування політик безпеки. З Active Directory можна легко інтегрувати Veeam Backup and Replication, забезпечуючи безпечний доступ до даних і серверів.

Windows Server підтримує Storage Spaces Direct (S2D), що дозволяє створювати високодоступні і масштабовані сховища для резервних копій. S2D об'єднує локальні диски серверів в єдиний пул зберігання, забезпечуючи високу продуктивність і надійність. Це особливо корисно для організацій, які мають великі об'єми даних і потребують надійного зберігання резервних копій.

Операційна система забезпечує розширені можливості віртуалізації за допомогою Hyper-V, що дозволяє створювати і керувати віртуальними машинами для резервного копіювання та відновлення. Hyper-V підтримує високу продуктивність і масштабованість, що дозволяє ефективно використовувати апаратні ресурси і забезпечувати швидке відновлення віртуальних машин у разі збоїв.

Windows Server також включає в себе розширені мережеві можливості, такі як програмно-обумовлена мережа (SDN), що дозволяє централізовано керувати мережевими ресурсами і забезпечувати високу гнучкість і безпеку. Це спрощує налаштування мережевих з'єднань для серверів резервного копіювання і забезпечує надійний обмін даними між серверами та сховищами.

Розширені інструменти управління та автоматизації, такі як PowerShell і Windows Admin Center, забезпечують ефективне управління сервером резервного копіювання. PowerShell дозволяє автоматизувати рутинні завдання та створювати сценарії для налаштування і управління Veeam Backup and Replication, а Windows Admin Center надає зручний веб-інтерфейс для централізованого управління сервером.

Використання Windows Server як бази для Veeam Backup and Replication забезпечує високу продуктивність, надійність та безпеку. Завдяки інтеграції з сучасними технологіями зберігання, віртуалізації та мережевими рішеннями, ця операційна система надає оптимальне середовище для розгортання і управління інфра-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

структурою резервного копіювання, забезпечуючи безперервність бізнесу та захист даних.

Вибір сховища даних

Сховища даних повинні забезпечувати надійне зберігання резервних копій та швидкий доступ до них у разі необхідності відновлення. Вибір сховищ залежить від обсягу даних, які необхідно резервувати, та вимог до доступності і швидкості відновлення. Можна використовувати різні типи сховищ, включаючи локальні дискові масиви (NAS, SAN), віддалені сховища або хмарні сервіси. Важливо враховувати можливість масштабування сховищ, щоб забезпечити зберігання зростаючих обсягів даних.

Під час вибору NAS було розглянуто декілька варіантів. FreeNAS (TrueNAS Core) базується на FreeBSD і підтримує файлову систему ZFS, що забезпечує високу надійність і захист даних. Unraid використовує Linux та файлову систему XFS або Btrfs і пропонує гнучкість у виборі дисків і конфігурацій зберігання. Rockstor також базується на Linux та використовує файлову систему Btrfs, зосереджуючись на простоті використання та управлінні даними.

OpenMediaVault відрізняється простотою встановлення і налаштування, що робить його зручним для користувачів без глибоких технічних знань. OMV, на базі Debian, підтримує широкий спектр плагінів, що розширюють його функціонал, та має інтуїтивно зрозумілий веб-інтерфейс. На відміну від FreeNAS, який орієнтований на потужніші серверні рішення з використанням ZFS, OMV пропонує більш гнучкий підхід до апаратних вимог, що підходить для домашнього використання та малих офісів. У порівнянні з Unraid і Rockstor, OMV забезпечує кращу інтеграцію з наявними Linux-інструментами і спільнотою, що робить його надійним вибором для створення NAS-сервера з мінімальними витратами на адміністрування та підтримку.

OpenMediaVault (OMV) – це популярна операційна система на базі Linux, яка призначена для створення та управління мережевими сховищами даних (NAS). Вона забезпечує зручний і потужний спосіб організації резервного копіювання за

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

допомогою протоколу SMB (Server Message Block), який є стандартом для обміну файлами в мережах з Windows.

OpenMediaVault підтримує різні протоколи для обміну даними, включаючи SMB/CIFS, FTP, NFS, Rsync, та інші, що дозволяє легко інтегруватися в існуючу інфраструктуру і забезпечити доступ до даних з різних платформ. Використання SMB дозволяє організувати зручне і ефективне середовище для резервного копіювання даних з Windows-систем та інших пристроїв, що підтримують цей протокол.

OpenMediaVault надає простий у використанні веб-інтерфейс, який дозволяє адміністратору легко налаштовувати сервер і управляти ним. За допомогою цього інтерфейсу можна створювати і налаштовувати SMB-ресурси (SMB shares), керувати правами доступу, налаштовувати квоти на використання дискового простору, а також здійснювати моніторинг стану системи.

Одна з головних переваг OpenMediaVault – це можливість використовувати різноманітні дискові конфігурації для зберігання даних. Система підтримує створення RAID-масивів (0, 1, 5, 6, 10), що забезпечує додатковий рівень захисту даних та підвищує надійність сховища. Це особливо важливо для резервного копіювання, оскільки дозволяє зменшити ризик втрати даних у разі відмови одного з дисків.

OpenMediaVault також підтримує розширення функціональності за допомогою плагінів. Наприклад, можна встановити плагін для автоматизації резервного копіювання за допомогою Rsync або використовувати плагіни для інтеграції з хмарними сервісами для резервного копіювання. Це дозволяє адаптувати систему під конкретні потреби і забезпечити більш гнучке управління резервним копіюванням.

Безпека є одним з ключових аспектів при використанні OpenMediaVault для резервного копіювання. Система підтримує управління доступом на основі користувачів і груп, що дозволяє точно налаштовувати права доступу до даних. Також можна налаштувати шифрування для захисту даних, що зберігаються, і використовувати функції журналювання для відстеження дій користувачів.

Для забезпечення безперебійної роботи та швидкого доступу до резервних копій, OpenMediaVault надає інструменти для моніторингу системи. Адміністратори можуть отримувати повідомлення про стан системи, використання дискового

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

простору, помилки та інші важливі події. Це дозволяє своєчасно реагувати на проблеми і підтримувати високу доступність сервера.

OpenMediaVault є відмінним вибором для організації резервного копіювання за допомогою протоколу SMB завдяки своїй гнучкості, надійності та зручному управлінню. Він забезпечує високу сумісність з різними платформами, підтримує різні конфігурації зберігання і надає потужні інструменти для захисту даних і моніторингу системи. Завдяки цим можливостям, OpenMediaVault може ефективно використовуватися як центральний вузол для резервного копіювання даних в корпоративних і домашніх мережах.

Вибір програмного забезпечення для резервного копіювання

У табл. 1.3 наведено результати порівняння таких засобів резервного копіювання, як Veeam Backup & Replication, Acronis Cyber Backup, Commvault Backup & Recovery, Veritas Backup Exec, IBM Spectrum Protect, Dell EMC Avamar залежно від підтримки фізичних серверів, підтримки віртуальних середовищ, підтримки хмарних середовищ, легкості використання, дедуплікації даних, захисту від програм-вимагачів, масштабованості та ліцензійних витрат.

Таблиця 1.3 – порівняння засобів резервного копіювання.

Рішення	Підтримка фізичних серверів	Підтримка віртуальних середовищ	Підтримка хмарних сховищ	Легкість використання	Дедуплікація даних	Захист від програм-вимагачів	Масштабованість	Ліцензійні витрати
Veeam Backup & Replication	+	+	+	+	+	+	+	-(до 10 хостів)
Acronis Cyber Backup	+	+	+	+	+	+	+	+

Commvault Backup & Recovery	+	+	+	-	+	+	+	-
Veritas Backup Exec	+	+	+	+	-	-	+	-
IBM Spectrum Protect	+	+	+	-	+	-	+	-
Dell EMC Avamar	+	+	+	+	+	-	+	-

Програмне забезпечення для резервного копіювання відіграє ключову роль у забезпеченні ефективного та надійного процесу резервного копіювання і відновлення даних. Одним з провідних рішень на ринку є Veeam Backup and Replication.

Veeam Backup and Replication – це провідне програмне забезпечення для резервного копіювання та відновлення даних, яке забезпечує високий рівень надійності та ефективності для корпоративних середовищ. Його основною метою є захист даних від втрат та забезпечення швидкого відновлення у разі збоїв. У цьому підрозділі розглядаються основні можливості та функції Veeam Backup and Replication, а також його переваги для корпоративного резервного копіювання.

Основні можливості та функції Veeam Backup and Replication

Veeam Backup and Replication надає широкий спектр функцій, що дозволяють забезпечити надійний захист даних і швидке відновлення:

- **Резервне копіювання на рівні образів (Image-Based Backup).** Veeam створює повні резервні копії віртуальних машин (VM), захоплюючи повний стан

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

системи на момент резервування, включаючи операційну систему, налаштування, додатки та дані.

- **Інкрементальні резервні копії (Incremental Backups).** Veeam підтримує інкрементальні резервні копії, що дозволяє зменшити час і обсяг резервування, зберігаючи лише змінені дані з моменту останнього резервного копіювання.
- **Резервне копіювання в хмару (Cloud Backup).** Підтримка резервного копіювання даних у хмарні сховища, такі як Amazon Web Services (AWS), Microsoft Azure та інші, забезпечуючи додатковий рівень захисту та доступність даних.
- **Інтеграція з сховищами даних (Storage Integration).** Veeam має вбудовану інтеграцію з багатьма провідними сховищами даних, включаючи NetApp, Dell EMC, HPE та інші, що дозволяє ефективно керувати даними та оптимізувати процес резервного копіювання.
- **Відновлення окремих файлів і об'єктів (Granular Recovery).** Можливість відновлення окремих файлів, папок, електронних листів, баз даних та інших об'єктів без необхідності відновлення всієї резервної копії.
- **Швидке відновлення віртуальних машин (Instant VM Recovery).** Функція, що дозволяє миттєво запускати віртуальні машини безпосередньо з резервної копії, мінімізуючи час простою та забезпечуючи швидкий доступ до критично важливих даних.
- **Моніторинг та звітність (Monitoring and Reporting).** Інструменти для моніторингу стану резервного копіювання, створення звітів про успішність та відстеження продуктивності, що дозволяють підтримувати високу ефективність системи.

Переваги Veeam Backup and Replication для корпоративного резервного копіювання

Veeam Backup and Replication має ряд переваг, що роблять його одним з найкращих рішень для корпоративного резервного копіювання:

- **Надійність та відмовостійкість.** Veeam забезпечує високий рівень надійності, мінімізуючи ризик втрати даних завдяки функціям резервного копію-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

вання на рівні образів, інкрементальних копій та інтеграції з провідними сховищами даних.

- **Швидкість та ефективність.** Інкрементальні резервні копії та швидке відновлення віртуальних машин дозволяють значно скоротити час на резервне копіювання та відновлення даних, що є критично важливим для підтримання безперервності бізнесу.
- **Гнучкість та масштабованість.** Підтримка різних середовищ, включаючи фізичні сервери, віртуальні машини та хмарні ресурси, дозволяє адаптувати систему до змінних потреб бізнесу та забезпечувати масштабованість інфраструктури.
- **Простота у використанні.** Інтуїтивний інтерфейс та автоматизовані процеси спрощують налаштування та управління резервним копіюванням, що дозволяє ІТ-персоналу ефективно виконувати свої завдання.
- **Захист від кібератак.** Вбудовані функції безпеки, такі як шифрування даних та захист резервних копій від змін, забезпечують додатковий рівень захисту від кібератак та несанкціонованого доступу.
- **Підтримка різних платформ.** Veeam підтримує широкий спектр платформ, включаючи Windows, Linux, VMware, Hyper-V та інші, що дозволяє використовувати його в різних ІТ-середовищах.

Veeam Backup and Replication є потужним інструментом для забезпечення надійного резервного копіювання та відновлення даних у корпоративних середовищах. Його основні можливості та функції, такі як резервне копіювання на рівні образів, інкрементальні копії, інтеграція з хмарними сховищами та швидке відновлення віртуальних машин, забезпечують високу ефективність і надійність. Переваги Veeam, такі як надійність, швидкість, гнучкість, простота у використанні та захист від кібератак, роблять його одним з найкращих виборів для корпоративного резервного копіювання.

Окрім Veeam Backup and Replication, важливо розглянути системи управління та програми для відновлення даних, які інтегруються з основним програмним забезпеченням. Це можуть бути додаткові інструменти для моніторингу, звітності

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

та автоматизації процесів резервного копіювання і відновлення. Вибір таких інструментів залежить від специфічних потреб компанії та вимог до управління інфраструктурою резервного копіювання.

Вибір апаратного та програмного забезпечення для системи резервного копіювання є критичним етапом у створенні надійної та ефективної інфраструктури. Правильний вибір серверів, сховищ даних та програмного забезпечення, такого як Veeam Backup and Replication, забезпечує високу доступність даних, безпеку та швидкість відновлення, що є ключовими факторами для успішного функціонування корпоративної мережі.

Veeam Agent

Veeam Agent – це програмний інструмент для резервного копіювання та відновлення даних, розроблений компанією Veeam Software. Він забезпечує захист даних на фізичних машинах, віртуальних середовищах і в хмарі, підтримуючи різні операційні системи, включаючи Windows, Linux та macOS.

Однією з ключових можливостей Veeam Agent є створення резервних копій на рівні образів. Це дозволяє створювати повні копії системи, включаючи операційну систему, додатки, налаштування та дані. Такий підхід забезпечує можливість повного відновлення системи в разі збою. Крім того, Veeam Agent підтримує інкрементальні резервні копії, що зменшує обсяг даних, які потрібно зберігати, і час, необхідний для резервного копіювання.

Veeam Agent підтримує різні типи сховищ для зберігання резервних копій. Це можуть бути локальні диски, мережеві сховища (NAS), зовнішні USB-накопичувачі або хмарні сервіси. Така гнучкість дозволяє вибирати оптимальні рішення для зберігання залежно від потреб та наявних ресурсів.

Для зручності користувачів Veeam Agent пропонує інтуїтивно зрозумілий інтерфейс, який спрощує процес налаштування та управління резервними копіями. Можна легко створювати і планувати завдання резервного копіювання, налаштовувати розклад для автоматичного виконання цих завдань та відстежувати їх виконання. Гнучкі параметри планування дозволяють налаштовувати резервні копії таким чином, щоб мінімізувати вплив на продуктивність системи.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

Ще однією важливою функцією Veeam Agent є можливість відновлення на рівні файлів і системи. Це означає, що користувачі можуть відновлювати як окремі файли або папки, так і весь образ системи, що дуже корисно у випадках випадкового видалення файлів або при необхідності повного відновлення після серйозного збою.

Безпека даних є ключовим аспектом Veeam Agent. Програмне забезпечення підтримує шифрування резервних копій для захисту даних під час зберігання та передачі. Це забезпечує додатковий рівень захисту конфіденційних даних від несанкціонованого доступу.

Veeam Agent може інтегруватися з Veeam Backup & Replication, що дозволяє централізовано управляти резервним копіюванням і відновленням даних у змішаних середовищах. Це забезпечує єдиний інтерфейс для управління резервними копіями фізичних і віртуальних машин, а також хмарних ресурсів, що робить процес управління більш ефективним і зручним.

Таким чином, Veeam Agent є потужним інструментом для резервного копіювання і відновлення даних, який забезпечує високу надійність, продуктивність і безпеку. Завдяки своїй гнучкості та універсальності, Veeam Agent дозволяє ефективно захищати дані в різних середовищах і мінімізувати ризики втрати даних, забезпечуючи безперервність бізнесу.

2.3 Архітектура мережі резервного копіювання

У цьому підрозділі розглядається архітектура мережі резервного копіювання, яка включає топологію, розміщення серверів і сховищ даних, а також зв'язки між ними. Описуються заходи безпеки, необхідні для захисту даних під час процесу резервного копіювання і зберігання.

Об'єкт резервного копіювання

Active Directory (AD) на базі Windows Server 2016 є критичним компонентом корпоративної IT-інфраструктури, що забезпечує централізоване управління користувачами, групами, політиками безпеки та іншими ресурсами мережі. Захист і відновлення AD є життєво важливими для забезпечення безперервної роботи ор-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

ганізації. Veeam Agent для Windows забезпечує надійне резервне копіювання та відновлення AD, що дозволяє мінімізувати час простою і втрату даних.(пошукати чи повторюється) [2]

Для резервного копіювання AD з використанням Veeam Agent на базі Windows Server 2016 важливо забезпечити повне резервне копіювання сервера. Veeam Agent створює резервні копії на рівні образів, що дозволяє захопити повний стан системи, включаючи операційну систему, базу даних AD, конфігурації та інші критичні дані. Це забезпечує можливість повного відновлення сервера у випадку серйозного збою. Після початкового повного резервного копіювання Veeam Agent підтримує інкрементальні резервні копії, зберігаючи лише змінені дані. Це зменшує час і обсяг збережених резервних копій, а також оптимізує використання дискового простору.

Veeam Agent використовує технологію Microsoft Volume Shadow Copy Service (VSS) для створення консистентних резервних копій Active Directory. Це забезпечує коректність і цілісність резервних копій, дозволяючи уникнути проблем під час відновлення. Для зручності користувачів Veeam Agent пропонує інтуїтивно зрозумілий інтерфейс, який спрощує процес налаштування та управління резервними копіями. Можна легко створювати і планувати завдання резервного копіювання, налаштовувати розклад для автоматичного виконання цих завдань та відстежувати їх виконання. Гнучкі параметри планування дозволяють налаштовувати резервні копії таким чином, щоб мінімізувати вплив на продуктивність системи.

Відновлення Active Directory може здійснюватися на різних рівнях, залежно від масштабу інциденту. Якщо потрібно відновити окремі об'єкти, такі як користувачі, групи або організаційні одиниці, Veeam Agent дозволяє здійснювати відновлення на рівні об'єктів. Це дозволяє швидко відновити конкретні дані без необхідності повного відновлення сервера. У випадку збою доменного контролера Veeam Agent дозволяє виконати повне відновлення сервера на новий або наявний сервер. Відновлення повного образу сервера включає операційну систему, конфігурації AD і всі необхідні дані, що дозволяє швидко відновити роботу AD. Відновлення

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

системного стану, що включає критичні компоненти AD, такі як база даних AD, журнал змін і SYSVOL, також можливо з Veeam Agent.

Використання Veeam Agent для резервного копіювання AD надає численні переваги. Використання VSS гарантує, що всі резервні копії є консистентними і готовими до відновлення у будь-який момент, що особливо важливо для критичних служб, таких як AD. Підтримка різних варіантів зберігання резервних копій, включаючи локальні диски, мережеві сховища і хмарні сервіси, дозволяє адаптувати рішення під конкретні потреби організації та забезпечити масштабованість у міру зростання обсягів даних. Інтуїтивний інтерфейс Veeam Agent спрощує процес налаштування і управління резервними копіями, а також забезпечує високу продуктивність завдяки підтримці інкрементальних резервних копій і оптимізації процесів резервного копіювання, мінімізуючи вплив на продуктивність системи.

Таким чином, Veeam Agent для Windows є потужним інструментом для резервного копіювання та відновлення Active Directory на базі Windows Server 2016. Завдяки своїй гнучкості та універсальності, Veeam Agent дозволяє ефективно захищати дані, мінімізувати ризики втрати даних і забезпечити безперервність бізнесу.

Для розгортання Active Directory (AD) було обрано віртуальні платформи Hyper-V та ESXi, які забезпечують тісну інтеграцію з Veeam Backup & Replication для надійного резервного копіювання та відновлення.

Hyper-V та Veeam Backup & Replication

Hyper-V, платформа віртуалізації від Microsoft, пропонує широкі можливості для розгортання AD. Завдяки тісній інтеграції з Veeam Backup & Replication, забезпечується ефективне резервне копіювання та відновлення AD:

- **Application-aware Processing.** Veeam забезпечує консистентність додатків під час створення резервних копій. Це означає, що всі транзакції та зміни в AD зберігаються, що гарантує цілісність даних.
- **VSS Integration.** Використання Volume Shadow Copy Service (VSS) дозволяє створювати консистентні копії AD, що усуває проблеми з цілісністю даних під час відновлення.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Granular Recovery.** Veeam дозволяє відновлювати окремі об'єкти AD, такі як користувачі, групи та політики, без необхідності відновлення всього сервера.
- **Efficient Backup Modes.** Підтримка інкрементальних, повних та диференціальних копій оптимізує використання ресурсів і часу.

ESXi та Veeam Backup & Replication

VMware ESXi є популярною платформою віртуалізації, яка також інтегрується з Veeam Backup & Replication, забезпечуючи надійне резервне копіювання та відновлення AD:

- **VMware Tools Integration.** Інтеграція з VMware Tools забезпечує консистентність додатків під час створення резервних копій AD.
- **Changed Block Tracking (CBT).** Використання CBT дозволяє швидко та ефективно резервувати дані, відслідковуючи лише зміни з моменту останнього бекапу.
- **Instant VM Recovery.** Функція дозволяє швидко відновлювати AD-сервер безпосередньо з резервної копії, мінімізуючи час простою.
- **Veeam Explorers.** Спеціалізовані інструменти для відновлення окремих об'єктів AD, такі як користувачі, групи та політики, що забезпечує швидке відновлення конкретних даних без необхідності повного відновлення віртуальної машини.

Переваги обраного рішення

- **Надійність.** Тісна інтеграція з Veeam Backup & Replication забезпечує високу надійність резервного копіювання та відновлення AD, що є критично важливим для безперебійної роботи бізнесу.
- **Гнучкість.** Платформи Hyper-V та ESXi дозволяють легко масштабувати інфраструктуру відповідно до потреб організації.
- **Простота відновлення.** Можливість відновлення окремих об'єктів AD без необхідності повного відновлення системи зменшує час відновлення і мінімізує вплив на бізнес-процеси.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Автоматизація.** Підтримка автоматизації завдань резервного копіювання та відновлення знижує адміністративні витрати та підвищує ефективність роботи IT-відділу.

Вибір платформ Hyper-V та ESXi для розгортання AD з інтеграцією Veeam Backup & Replication дозволяє забезпечити надійне резервне копіювання та швидке відновлення критично важливих даних, що є ключовим аспектом для підтримання безперервності бізнесу.

Розміщення серверів і сховищ даних

Розміщення серверів і сховищ даних є важливим аспектом архітектури мережі резервного копіювання. Це включає вибір місця для серверів резервного копіювання, сховищ даних та їх взаємодії з іншими компонентами мережі.

- **Сервери резервного копіювання:** Вони повинні бути розміщені у захищених і доступних місцях, які забезпечують безперебійне живлення, охолодження та фізичну безпеку. Сервери можуть бути централізованими або розподіленими залежно від вимог до продуктивності та масштабованості.
- **Сховища даних:** Можуть бути локальними або віддаленими. Локальні сховища забезпечують швидкий доступ до резервних копій і мінімальний час відновлення даних, але вразливі до локальних аварій. Віддалені сховища (offsite storage) забезпечують захист від локальних катастроф, але можуть збільшити час відновлення через мережеві затримки. Хмарні сховища є популярним варіантом, оскільки вони забезпечують високу доступність і масштабованість.

Зв'язки між компонентами

Зв'язки між серверами резервного копіювання, сховищами даних і іншими компонентами мережі повинні бути надійними і високошвидкісними. Це включає мережеві з'єднання, які забезпечують передачу даних між різними вузлами мережі.

- **Локальні мережі (LAN).** Використовуються для з'єднання серверів і сховищ даних у межах одного приміщення або будівлі. Вони забезпечують високу швидкість передачі даних і мінімальні затримки.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

- **Віддалені мережі (WAN).** Використовуються для з'єднання віддалених сховищ даних або хмарних сервісів з основною мережею. WAN-з'єднання повинні бути захищеними і надійними, щоб забезпечити безперебійну передачу даних.

Заходи безпеки

Захист даних є критичним аспектом архітектури мережі резервного копіювання. Основні заходи безпеки включають:

Контроль доступу. Встановлення політики доступу, яка обмежує доступ до резервних копій лише авторизованим користувачам і системам. Це включає використання багаторівневого контролю доступу і аутентифікації.

Фізична безпека. Захист серверів і сховищ даних від фізичних загроз, таких як крадіжка, пожежа або повінь. Це включає використання захищених приміщень, систем пожежогасіння та безперебійного живлення.

Регулярне тестування. Проведення регулярних тестів відновлення даних для перевірки цілісності і доступності резервних копій. Це допомагає виявити і усунути потенційні проблеми до того, як вони вплинуть на бізнес-процеси.

Шифрування у Veeam Backup & Replication. Шифрування в Veeam Backup & Replication забезпечує захист даних під час резервного копіювання і зберігання, гарантує конфіденційність і цілісність даних, а також відповідає нормативним вимогам та галузевим стандартам.

У Veeam Backup & Replication передбачено як шифрування під час передачі даних, так і шифрування під час зберігання даних, а також механізм керування ключами шифрування. Детальніше шифрування у описане у додатку Б.

Архітектура мережі резервного копіювання повинна забезпечувати надійність, масштабованість і безпеку процесів резервного копіювання і відновлення даних. Правильний вибір топології, розміщення серверів і сховищ даних, а також заходи безпеки допоможуть створити ефективну систему, яка забезпечує безперебійну роботу компанії і захист її критичних даних.

Реалізація процесу резервного копіювання

Налаштування програмного забезпечення

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Перше, що потрібно зробити при реалізації процесу резервного копіювання, це налаштувати програмне забезпечення. Для цього необхідно здійснити наступні кроки.

- **Встановлення програмного забезпечення.** Встановлення Veeam Backup and Replication на обрані сервери резервного копіювання. Під час встановлення важливо переконатися, що сервери відповідають мінімальним вимогам програмного забезпечення щодо апаратного забезпечення та операційної системи.
- **Налаштування сховищ даних.** Конфігурування сховищ даних у програмному забезпеченні для зберігання резервних копій. Це можуть бути локальні сховища, віддалені сховища або хмарні сховища. У налаштуваннях вказуються параметри доступу, шифрування та резервування.
- **Налаштування резервних завдань.** Створення і конфігурація завдань резервного копіювання в програмному забезпеченні. У цьому процесі визначаються джерела даних, що підлягають резервному копіюванню, вибирається метод резервного копіювання (повне, інкрементальне, диференційне), а також встановлюються графіки виконання завдань.

Конфігурація апаратних засобів

Апаратна інфраструктура має бути налаштована для забезпечення надійного резервного копіювання. Основні етапи є наступними.

- **Підключення серверів і сховищ.** Всі сервери резервного копіювання та сховища даних повинні бути належним чином підключені до мережі. Це включає підключення до мережевих комутаторів, налаштування IP-адрес та забезпечення високошвидкісного і надійного з'єднання.
- **Налаштування мережевих з'єднань.** Забезпечення високої пропускної здатності мережевих з'єднань між серверами резервного копіювання та сховищами даних. Це може включати використання виділених мережевих сегментів для резервного копіювання або налаштування VLAN для ізоляції трафіку резервного копіювання.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Встановлення і налаштування апаратних RAID-контролерів.** Для забезпечення надійності і швидкості доступу до даних важливо використовувати RAID-масиви для сховищ даних. Налаштування RAID-контролерів включає вибір типу RAID (наприклад, RAID 5 або RAID 10) і конфігурацію масивів дисків.

Планування завдань резервного копіювання

Планування завдань резервного копіювання є критично важливим для забезпечення регулярності і надійності процесу. Основні етапи перелічено нижче.

- **Визначення графіків резервного копіювання.** Встановлення часу і частоти виконання завдань резервного копіювання. Це може бути щоденне, щотижневе або щомісячне резервне копіювання, залежно від вимог компанії до відновлення даних і обсягу змін.
- **Планування черговості завдань.** При великій кількості даних може бути необхідно планувати черговість виконання завдань, щоб уникнути перевантаження мережі або серверів. Це може включати розподіл завдань резервного копіювання на різні часові інтервали або дні тижня.
- **Автоматизація процесу.** Використання функцій автоматизації програмного забезпечення для резервного копіювання для створення скриптів і політик, які автоматично запускають резервні копії відповідно до встановлених графіків.

Моніторинг процесу

Моніторинг процесу резервного копіювання є необхідним для своєчасного виявлення і усунення проблем. Основні аспекти моніторингу є наступними.

- **Використання моніторингових інструментів.** Налаштування інструментів моніторингу, що входять до складу Veeam Backup and Replication, для відстеження стану резервних завдань, використання ресурсів і виявлення помилок.
- **Перегляд логів і звітів.** Регулярне переглядання логів і звітів про виконання резервних копій для виявлення можливих проблем або аномалій. Це включає

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

перевірку успішності завдань, швидкості виконання і обсягу скопійованих даних.

- **Налаштування сповіщень.** Встановлення системи сповіщень, яка інформує відповідальних осіб про успішне завершення резервних копій або про виникнення помилок. Це може бути налаштовано через електронну пошту, SMS або інші канали зв'язку.

Реалізація процесу відновлення даних

Процедури відновлення даних

Процес відновлення даних з резервних копій включає кілька ключових етапів, які забезпечують успішне і швидке відновлення втрачених або пошкоджених даних:

- **Ідентифікація даних для відновлення.** Першим кроком є визначення, які саме дані потребують відновлення. Це може бути окремий файл, каталог або цілий сервер. Важливо знати точну дату і час резервного копіювання, з якого будуть відновлюватися дані, щоб забезпечити максимальну актуальність відновлених даних.
- **Вибір відповідної резервної копії.** Після ідентифікації даних необхідно вибрати відповідну резервну копію для відновлення. Це може бути повна копія, інкрементальна або диференційна копія залежно від конкретної ситуації. Програмне забезпечення Veeam Backup and Replication дозволяє легко знаходити і вибрати потрібну резервну копію.
- **Запуск процесу відновлення.** Відновлення даних запускається через інтерфейс програмного забезпечення. Veeam Backup and Replication надає зручний майстер відновлення, який проводить користувача через усі необхідні кроки, включаючи вибір джерела відновлення, цільового місця для відновлення і додаткових параметрів, таких як відновлення прав доступу та атрибутів файлів.

Тестування відновлення даних

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

Для забезпечення надійності і працездатності резервних копій необхідно регулярно проводити тестування відновлення даних. Це включає наступні дії.

- **Періодичне тестування.** Встановлення графіку регулярного тестування процесу відновлення, щоб переконатися, що всі резервні копії є працездатними і можуть бути використані для відновлення даних. Це може включати відновлення тестових файлів або каталогів на спеціально виділених серверах або середовищах.
- **Відновлення критично важливих даних.** Особливу увагу слід приділити відновленню найбільш критично важливих для компанії даних, таких як бази даних, файли конфігурації та інші бізнес-критичні документи. Періодичне тестування цих даних дозволить виявити можливі проблеми і усунути їх заздалегідь.
- **Документування результатів тестування.** Всі результати тестування відновлення повинні бути документовані. Це включає запис часу відновлення, виявлених проблем і заходів, вжитих для їх усунення. Документування допомагає створити чітку картину готовності до відновлення і є важливою частиною плану відновлення після аварій.

Заходи для мінімізації часу відновлення

Час відновлення даних є критичним показником для будь-якої компанії. Існує кілька заходів, які можуть допомогти мінімізувати час відновлення.

- **Використання швидких носіїв.** Збереження резервних копій на швидких носіях, таких як SSD або NVMe диски, може значно прискорити процес відновлення. Використання високошвидкісних мережевих з'єднань також допомагає зменшити час передачі даних під час відновлення.
- **Оптимізація резервних завдань.** Використання інкрементальних або диференційних копій для зменшення обсягу даних, які потрібно відновлювати. Це зменшує навантаження на систему і скорочує час відновлення.
- **Автоматизація процесу відновлення.** Використання автоматизованих скриптів і політик для відновлення даних. Це дозволяє зменшити час, необ-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

хідний для запуску процесу відновлення, і мінімізувати ризик людських помилок.

- **Розподіл навантаження.** Використання кількох серверів для паралельного відновлення даних може значно зменшити загальний час відновлення. Це особливо важливо для великих обсягів даних або для відновлення кількох серверів одночасно.
- **Готовність персоналу.** Навчання і регулярні тренування ІТ-персоналу щодо відновлення даних. Готовність персоналу швидко реагувати на надзвичайні ситуації і ефективно виконувати процес відновлення є ключовим фактором для мінімізації часу відновлення.

Розробка інфраструктури

На рис. 2.1 показано схему мережі для проєкту інфраструктури резервного копіювання.

192.168.11.0/24

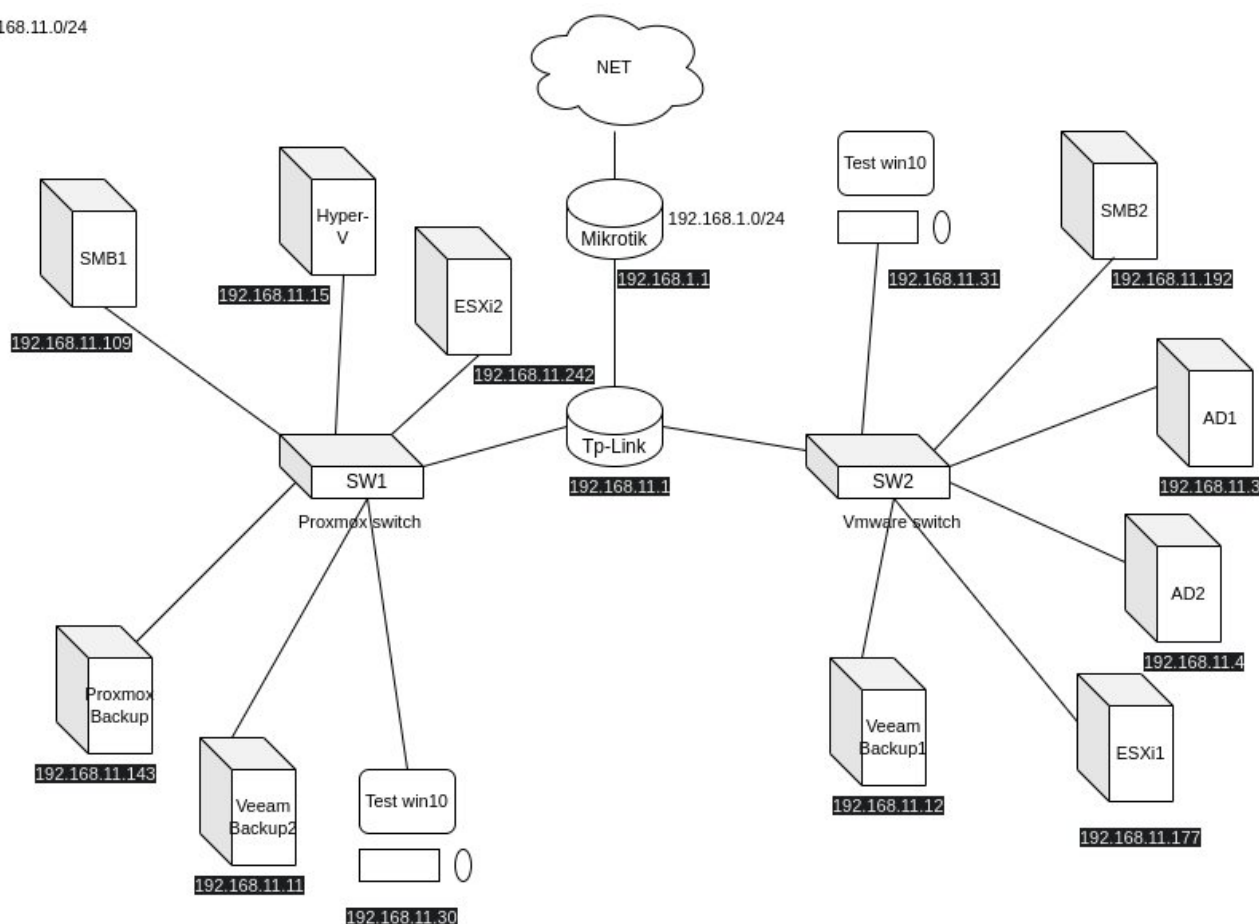


Рис 2.1. Схема мережі

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 1.4 – Схема адресації.

Пристрій	Ір-адреса/Маска
TP-LINK 1500ax	192.168.11.1/24
Active Directory 1	192.168.11.3/24
Active Directory 2	192.168.11.4/24
Veeam Backup Server 1	192.168.11.12/24
Veeam Backup Server 2	192.168.11.11/24
Hyper-V Server	192.168.11.15/24
ESXi 1	192.168.11.177/24
ESXi 2	192.168.11.242/24
OMV 1	192.168.11.109/24
OMV 2	192.168.11.192/24
Proxmox Backup Server	192.168.11.143/24
Windows 10 Test VM 1	192.168.11.30/24
Windows 10 Test VM 2	192.168.11.31/24

Ця схема зображає мережеву інфраструктуру для резервного копіювання з використанням різних віртуалізаційних та зберігаючих рішень.

Мережеве підключення:

- Мережа використовує підмережу з IP-адресами у діапазоні 192.168.11.0/24.
- Центральний маршрутизатор (Mikrotik) підключений до зовнішньої мережі (NET) і має внутрішню IP-адресу 192.168.1.1.
- Mikrotik підключений до основного комутатора (Tp-Link) з IP-адресою 192.168.11.1.

Комутатори:

- SW1 (Proxmox switch): обслуговує пристрої, які використовують Proxmox для віртуалізації.
- SW2 (VMware switch): обслуговує пристрої, які використовують VMware для віртуалізації.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Сервери та пристрої підключені до SW1:

- SMB1: сервер для зберігання файлів (SMB), IP-адреса 192.168.11.109.
- Hyper-V: сервер для віртуалізації, IP-адреса 192.168.11.15.
- ESXi2: сервер для віртуалізації з використанням VMware ESXi, IP-адреса 192.168.11.242.
- Proxmox Backup: сервер для резервного копіювання з використанням Proxmox, IP-адреса 192.168.11.143.
- Veeam Backup2: сервер для резервного копіювання з використанням Veeam, IP-адреса 192.168.11.11.
- Test win10: тестова машина з Windows 10, IP-адреса 192.168.11.30.

Сервери та пристрої підключені до SW2:

- SMB2: сервер для зберігання файлів (SMB), IP-адреса 192.168.11.192.
- AD1: сервер Active Directory, IP-адреса 192.168.11.5.
- AD2: другий сервер Active Directory, IP-адреса 192.168.11.4.
- ESXi1: сервер для віртуалізації з використанням VMware ESXi, IP-адреса 192.168.11.177.
- Veeam Backup1: сервер для резервного копіювання з використанням Veeam, IP-адреса 192.168.11.12.
- Test win10: тестова машина з Windows 10, IP-адреса 192.168.11.31.

Інтерпретація схеми:

- Центральний маршрутизатор (Mikrotik) забезпечує підключення до зовнішньої мережі і маршрутизацію між різними підмережами всередині організації.
- Tr-Link є основним комутатором, який з'єднує дві підмережі (Proxmox switch та VMware switch).
- SW1 і SW2 поділяють навантаження між двома різними типами віртуалізаційних середовищ (Proxmox та VMware), забезпечуючи розподілене та гнучке управління ресурсами.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

- Сервери для резервного копіювання (Veeam Backup1, Veeam Backup2, Proxmox Backup) підключені до відповідних комутаторів для забезпечення резервного копіювання та відновлення даних з різних серверів та середовищ.
- Сервери SMB забезпечують зберігання даних, а сервери Active Directory (AD1, AD2) управляють автентифікацією та авторизацією в мережі.

Робота резервного копіювання в даній мережі

Мережа, зображена на схемі, включає різноманітні сервери та пристрої, які забезпечують резервне копіювання та відновлення даних. Детально розглянемо, як відбувається процес резервного копіювання у цій інфраструктурі.

Початкове резервне копіювання:

- Коли запускається процес резервного копіювання, Veeam Backup & Replication на сервері Veeam Backup (наприклад, Veeam Backup1 на IP-адресі 192.168.11.12) підключається до серверів, які потрібно резервувати (наприклад, ESXi1 на IP-адресі 192.168.11.177 або AD1 на IP-адресі 192.168.11.5).
- Veeam збирає дані з цих серверів, створюючи повні резервні копії, які включають операційні системи, додатки, файли та налаштування.

Інкрементальне резервне копіювання:

- Після створення початкової повної резервної копії, Veeam переходить до інкрементальних резервних копій. Це означає, що кожне наступне резервне копіювання включає тільки зміни, які відбулися з моменту останнього резервного копіювання. Це значно зменшує обсяг даних, які потрібно копіювати, і час, необхідний для завершення процесу.

Зберігання резервних копій:

- Резервні копії зберігаються на спеціалізованих серверах для зберігання, таких як SMB1 (IP-адреса 192.168.11.109) та SMB2 (IP-адреса 192.168.11.192). Ці сервери забезпечують надійне зберігання резервних копій з можливістю швидкого доступу до них.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

- Також можуть використовуватися інші сховища, наприклад, сервери Proxmox Backup (IP-адреса 192.168.11.143) для додаткової безпеки та резервного копіювання.

Відновлення даних:

- У разі потреби відновлення даних, адміністратор використовує Veeam Backup & Replication для вибору потрібної резервної копії та серверу, який потрібно відновити.
- Veeam дозволяє відновлювати як цілі сервери або віртуальні машини, так і окремі файли або об'єкти (наприклад, окремі записи в Active Directory).
- Відновлення може бути виконане безпосередньо з резервної копії на місці або на новий сервер/віртуальну машину.

Захист від втрат даних:

- Сервери резервного копіювання (Veeam Backup1 та Veeam Backup2) використовують різні механізми для захисту даних від втрат, такі як дедуплікація, шифрування та захист від програм-вимагачів.
- Регулярні перевірки цілісності резервних копій та тестування процесів відновлення забезпечують додатковий рівень надійності.

Мережа побудована таким чином, щоб забезпечити максимальну надійність та ефективність процесів резервного копіювання та відновлення. Використання різних серверів для зберігання резервних копій, різних віртуалізаційних платформ та резервних серверів (як Veeam, так і Proxmox) гарантує захист даних у випадку збоїв та мінімальні втрати часу на відновлення.

Висновок до другого розділу

У другому розділі детально розглянуто проектування корпоративної мережі резервного копіювання, що є важливим етапом для забезпечення стабільної роботи інформаційних систем підприємства. Розробка такої мережі включала вибір відповідного програмного та апаратного забезпечення, що дозволяє забезпечити максимальну надійність і ефективність процесів резервного копіювання. Особливу

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

увагу було приділено інтеграції різних платформ віртуалізації, таких як ESXi, Hyper-V та VMware Workstation Pro, що дозволило створити гнучку та стійку до збоїв інфраструктуру. Аналіз і вибір цих платформ базувався на їх здатності забезпечувати високу продуктивність, легкість управління та масштабованість. Важливим аспектом було також налаштування серверів і мережевих з'єднань, які забезпечують безперебійну роботу системи та швидке відновлення даних у разі аварій. У результаті виконаних робіт, проектування мережі резервного копіювання забезпечило високий рівень захищеності даних від можливих загроз, таких як апаратні збої, помилки користувачів та кібератаки, а також дозволило мінімізувати час простою бізнес-процесів завдяки швидкому відновленню критично важливої інформації.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3: Налаштування та тестування інфраструктури на базі Veeam Backup and Replication

3.1 Налаштування інфраструктури резервного копіювання

Налаштування серверів

Основою нашої корпоративної інфраструктури є AD на базі Windows Server 2016. Задля забезпечення повноти картини резервного копіювання його буде розгорнуто на декількох платформах: ESXi, Hyper-V та VMware Workstation Pro (остання- задля імітації розгорнутості на фізичному сервері без віртуалізації). Всі ці платформи підтримуються Veeam Backup and Replication для створення бекапів. ESXi та Hyper-V додатково бекапуються за допомогою Proxmox Backup Server та розгорнуте на них AD бекапується за допомогою Veeam Backup and Replication.

Таким чином, розгортання AD (рис 3.1) на різних платформах забезпечує гнучкість та надійність нашої інфраструктури. Використання Veeam Backup and Replication спільно з Proxmox Backup Server дозволяє створювати надійні резервні копії та оперативно відновлювати дані у разі збою. Ця комбінація забезпечує високу доступність та цілісність даних у нашій корпоративній мережі. [2]

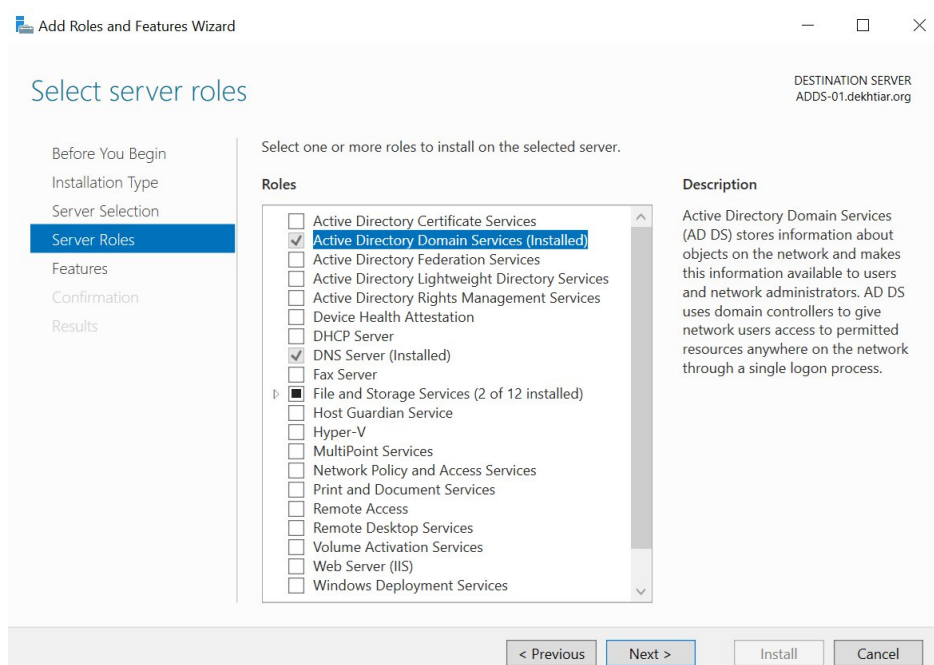


Рис. 3.1. Вибір ролей для серверу.

Розгортання Proxmox та PBS

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

Завантажуємо ISO-образ Proxmox VE з офіційного сайту та записуємо його на USB-накопичувач. Після завантаження сервера з цього носія проходимо через майстер встановлення, вибираємо диск для інсталяції, налаштовуємо мережеві параметри та задаємо облікові дані адміністратора. Після завершення встановлення сервер перезавантажується, і доступ до веб-інтерфейсу Proxmox VE здійснюється через браузер. [8]

Після встановлення Proxmox VE налаштовуємо мережеві інтерфейси для забезпечення доступу до інтернету та локальної мережі. Додаємо сховища для віртуальних машин, використовуючи локальні диски або мережеві сховища (NFS, iSCSI). Створюємо віртуальні машини, задаючи необхідні ресурси, такі як процесори, пам'ять та дисковий простір. Налаштовуємо резервне копіювання віртуальних машин за допомогою інтеграції з Proxmox Backup Server (рис. 3.2).

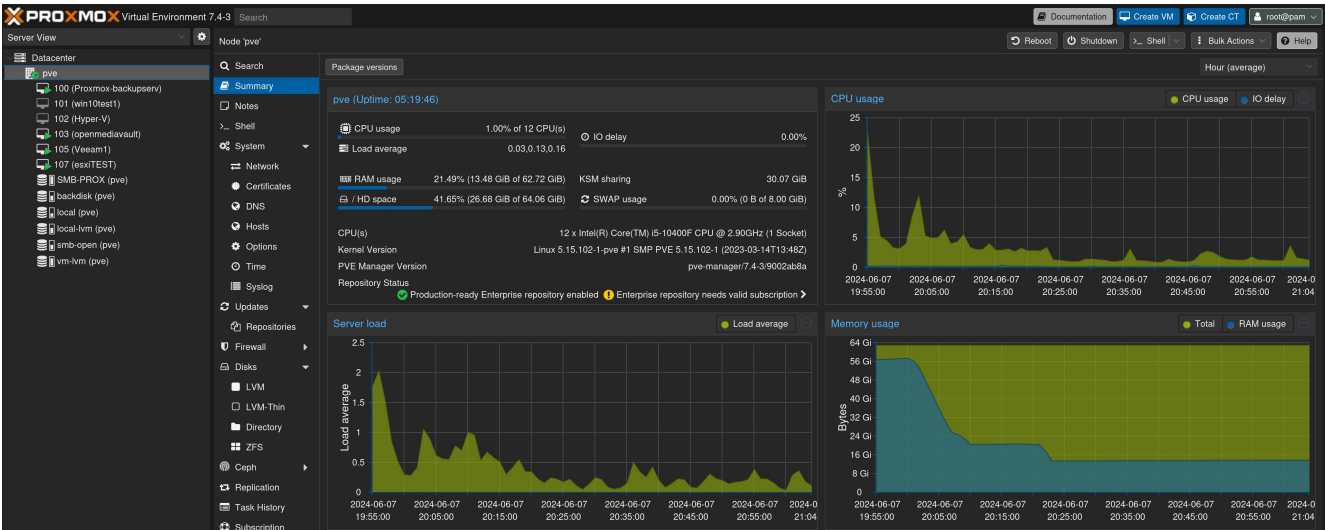


Рис. 3.2. Proxmox server.

Розгортання Hyper-V та ESXi

Hyper-V, роль віртуалізації від Microsoft, встановлюється на сервері з Windows Server 2016. Для цього активуємо Hyper-V через "Server Manager" або за допомогою PowerShell. Після встановлення сервера, налаштовуємо мережеві адаптери та створюємо віртуальні машини для розгортання служб, таких як AD (рис. 3.3).[10]

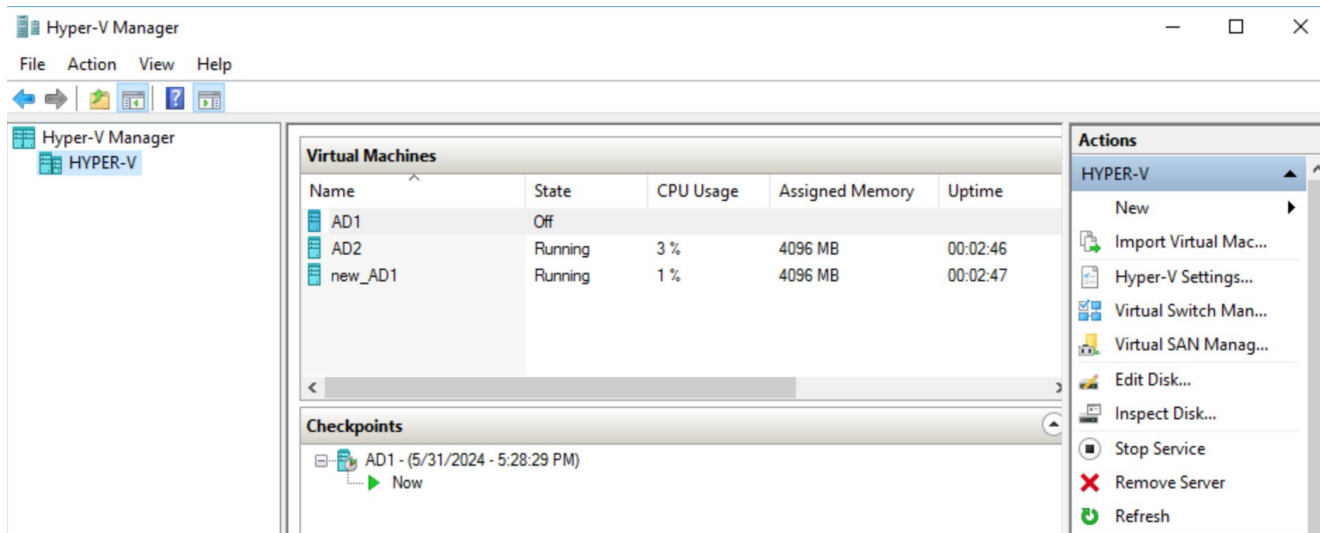


Рис. 3.3. Розгорнуті віртуальні машини.

ESXi, гіпервізор від VMware, встановлюється безпосередньо на фізичний сервер, але в нашому випадку на Proxmox та VMware Workstation. Завантажуємо сервер з ESXi інсталяційного носія, проходимо через майстер встановлення та налаштовуємо основні параметри, такі як мережеві налаштування та облікові дані адміністратора. Після встановлення та налаштування ESXi встановлюємо віртуальні машини, включаючи розгортання служб AD (рис. 3.4). [9]

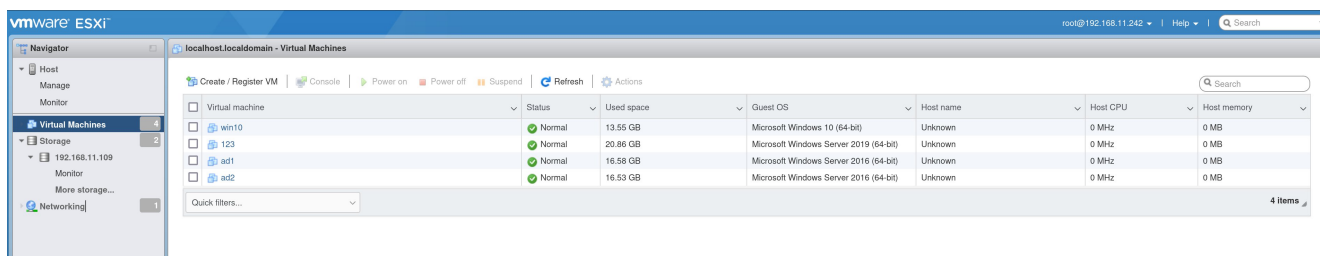


Рис. 3.4. Розгорнуті віртуальні машини.

Розгортання OpenMediaVault (OMV)

Створюємо нову віртуальну машину в інтерфейсі Proxmox, запускаємо віртуальну машину та завантажуємося з ISO-образу OMV. Проходимо майстер встановлення, вибираємо диск віртуальної машини та налаштовуємо основні параметри системи, такі як мережеві налаштування та облікові дані адміністратора. Після чого в Proxmox додаємо диски для майбутніх мережених ресурсів. Після завершення встановлення перезавантажуємо віртуальну машину. Доступ до веб-інтерфейсу OMV здійснюється через браузер за IP-адресою віртуальної машини. Створюємо мережеві ресурси, користувачів та роздаємо дозволи (рис. 3.5). [11]

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

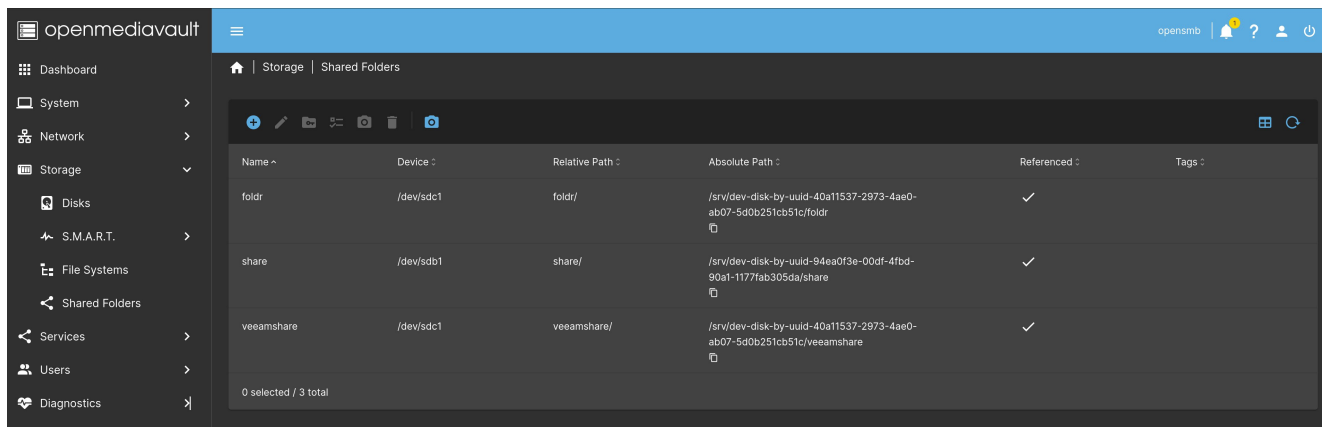


Рис. 3.5. Мережеві папки.

Veeam Backup Server

Veeam Backup and Replication має певні системні вимоги, які повинні бути виконані для успішної інсталяції. Програмне забезпечення сумісне з операційними системами Windows Server 2012 R2, 2016, 2019 та 2022. Мінімальні апаратні вимоги включають сучасний багатоядерний процесор (рекомендовано Intel Xeon або аналогічний), не менше 4 ГБ оперативної пам'яті (рекомендовано 8 ГБ або більше) та мінімум 50 ГБ вільного дискового простору для установки та зберігання резервних копій. Для забезпечення ефективної роботи також потрібна мережа з мінімальною пропускну здатністю 1 Гбіт/с. Додатково, необхідно мати встановлений Microsoft .NET Framework 4.7.2 або новішу версію та Microsoft SQL Server (2012 або новіший) для бази даних Veeam.

Перед початком інсталяції необхідно виконати декілька підготовчих етапів. Спочатку слід перевірити сумісність операційної системи та наявність усіх необхідних оновлень для апаратного забезпечення. Потім потрібно встановити всі передумови, зокрема Microsoft .NET Framework 4.7.2 або новішу версію та Microsoft SQL Server, якщо він ще не встановлений. Важливо зробити резервну копію критично важливих даних перед початком інсталяції, щоб уникнути втрат у випадку виникнення непередбачених проблем. Крім того, слід перевірити, що у вас є адміністративні права доступу на сервері, де буде встановлено Veeam Backup and Replication, та забезпечити доступ до інтернету для завантаження необхідних компонентів.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

Процес інсталяції Veeam Backup and Replication починається з завантаження інсталяційного пакету з офіційного сайту Veeam. Після завантаження, запускаємо інсталяційний файл та виконуємо інструкції майстра встановлення.

Після завершення інсталяції майстер повідомить вас про успішне завершення процесу та запропонує запустити Veeam Backup and Replication. На цьому етапі програма готова до налаштування та використання.

Налаштування Veeam Backup and Replication починається з додавання сховища даних. В нашому випадку це локальне та віддалене мережеве сховище (рис. 3.6).

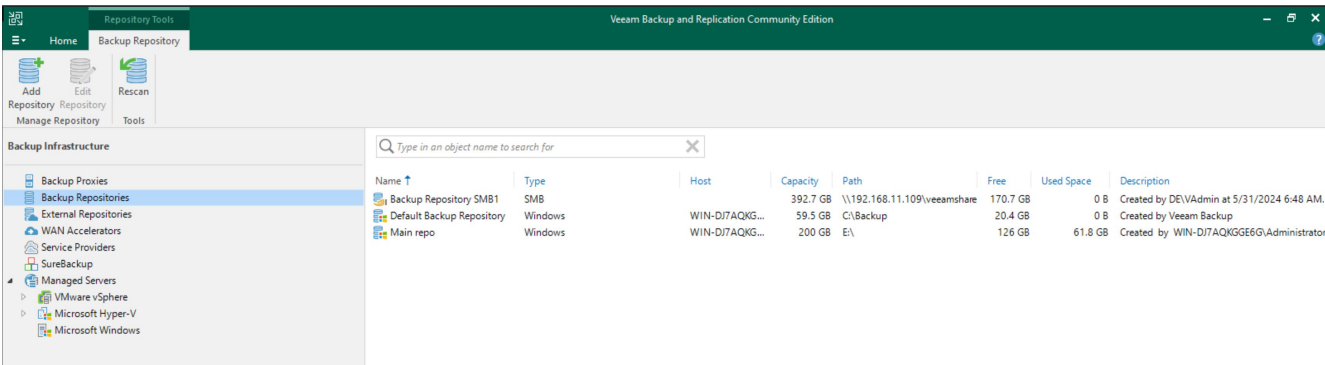


Рис. 3.6. Сховища даних у Veeam Backup and Replication.

Переглянемо збережені резервні копії та їх місцезбереження (рис. 3.7).

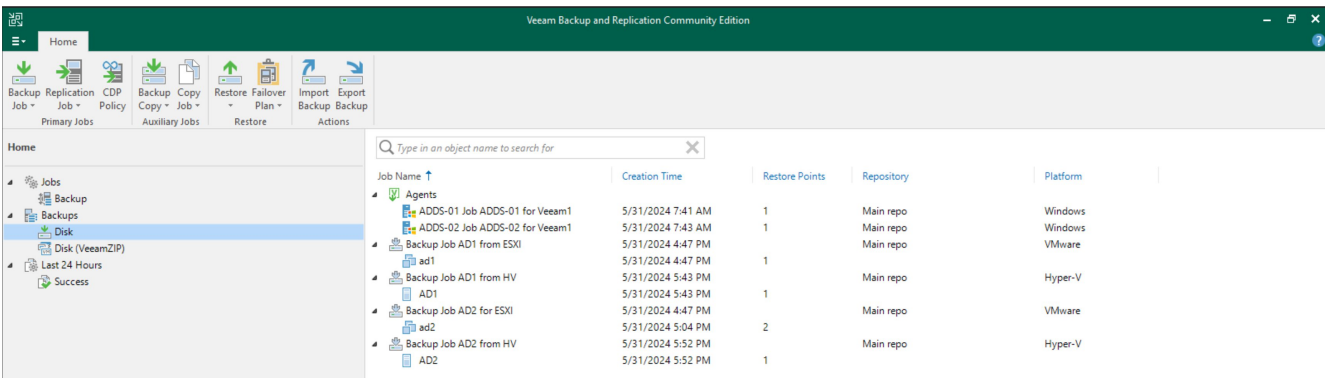


Рис. 3.7. Резервні копії.

Також потрібно додати сервери з яких будуть бекапуватись віртуальні машини (рис. 3.8), а також додати необхідні акаунти для доступу до них. Всі необхідні дії для резервного копіювання відбуваються через акаунт, зареєстрований в домені.

[3][1]

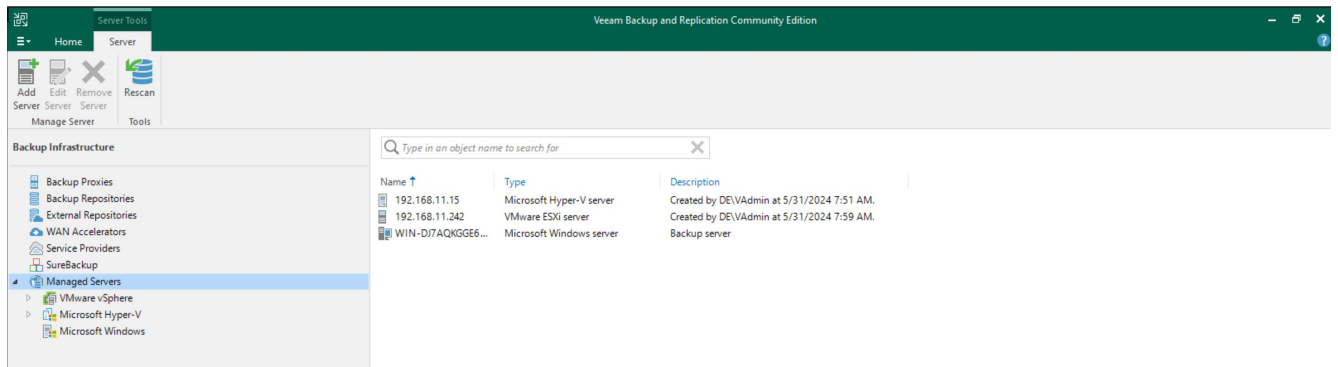


Рис. 3.8. Додані сервери.

Встановлення та налаштування Veeam Agent

Для роботи з фізичними серверами використовується додаток, який інтегрується з Veeam Backup and Replication сервером. Для роботи його необхідно встановити безпосередньо на сервер, який буде копіюватись в зручне місце - мережеву папку, хмарне сховище або на головний бекап сервер. Встановлення відбувається запуском додатку, заздалегідь завантаженого на сервер. Після встановлення створюємо завдання для резервного копіювання (рис. 3.9).

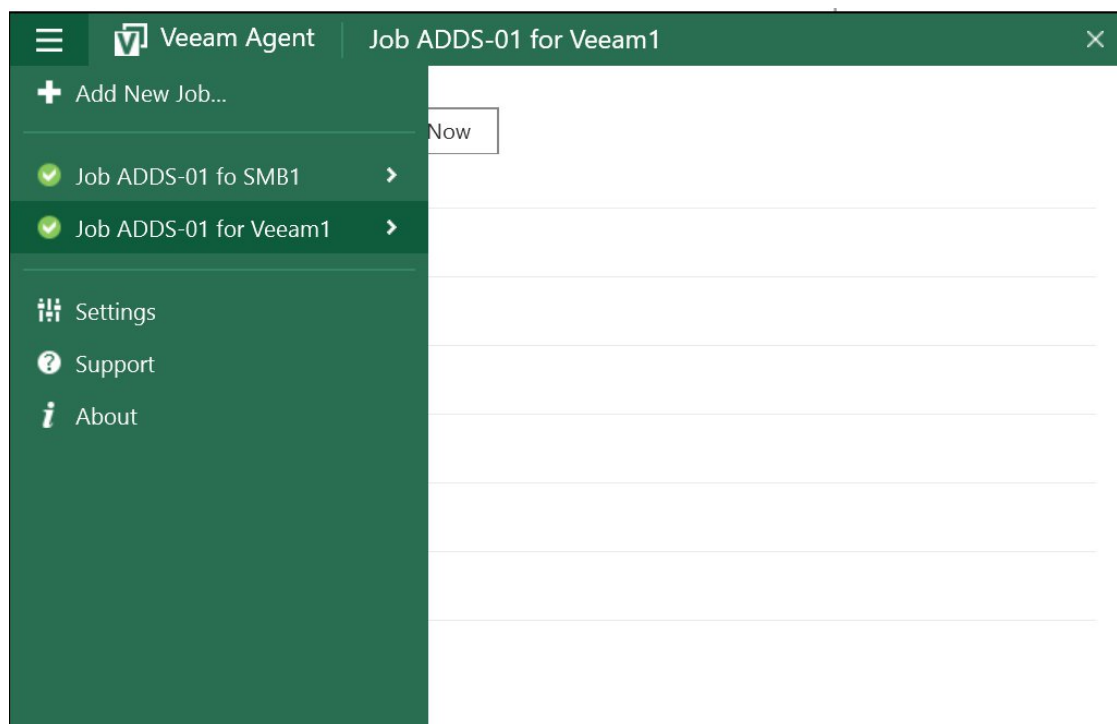


Рис. 3.9. Створені завдання.

Налаштування мережевих з'єднань

Для комутації в мережі використовується роутер TP-LINK 1500AX та комутатори Прохтох та VMware. В мережі використовується два фізичних пристрої для створення віртуальних середовищ- ноутбук та імпровізований сервер на базі зви-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

чайного комп'ютера. Обидва вони під'єднані до мережі по ethernet кабелю та створюють віртуальну мережу. На ноутбучі піднято сервіси VMware (рис. 3.11), а на комп'ютері повноцінно встановлений Proxmox (рис. 3.10). Всі інші сервери є віртуальними машинами.

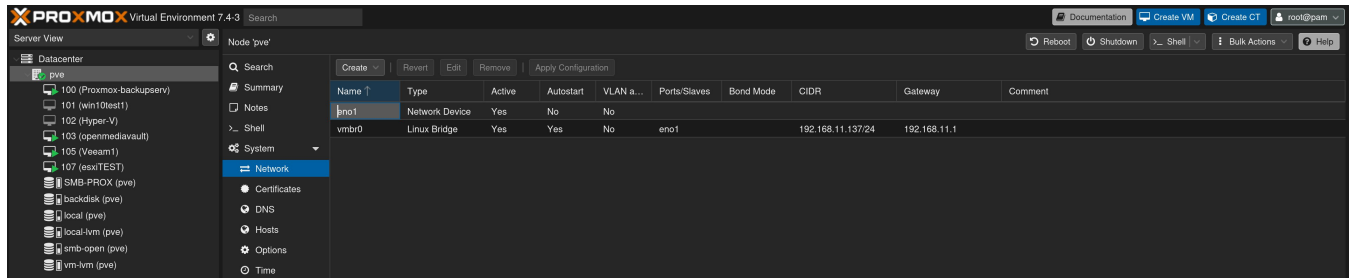


Рис. 3.10. Мережа Proxmox.

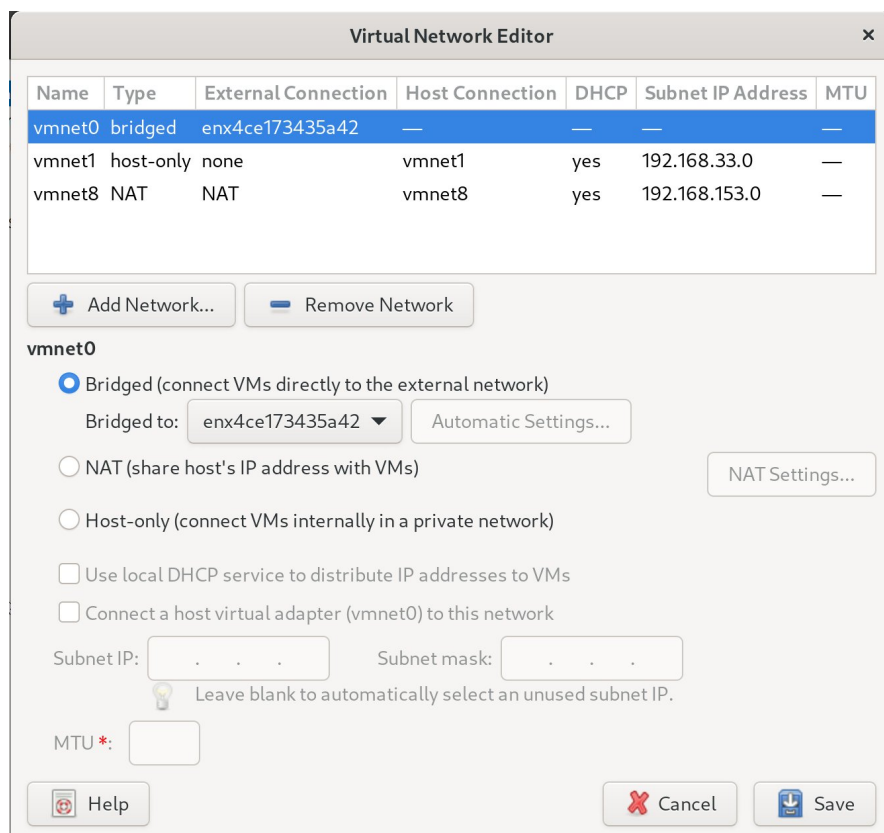


Рис. 3.11. Мережа VMware.

Налаштування політик резервного копіювання та часу бекапування

Налаштування безпеки паролів та акаунтів

Складність паролів:

Паролі повинні містити мінімум 12 символів, включаючи великі та малі літери, цифри та спеціальні символи.

Термін дії паролів:

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

Паролі повинні змінюватися кожні 90 днів.

Заборона повторного використання:

Не дозволяється використовувати попередні паролі.

Блокування акаунтів:

Після 5 невдалих спроб входу акаунт блокується.

Розмежування прав доступу:

Кожен користувач має тільки ті права, які необхідні для виконання його обов'язків.

Аудит та моніторинг:

Регулярний аудит та моніторинг активності користувачів на серверах резервного копіювання.

Час бекапування

Найкращий час для виконання резервних копій - це період найменшого навантаження на систему, зазвичай уночі або у вихідні дні. Це мінімізує вплив процесу резервного копіювання на продуктивність системи та забезпечує максимальну доступність ресурсів для користувачів у робочий час.

В нашому випадку кількість резервних копій є невеликою тому час для бекапування буде обрано о 10 вечора кожного дня. Але зі зростанням кількості даних часову політику буде змінено. [7]

3.2 Створення та керування завданнями резервного копіювання

Створення завдань резервного копіювання

Процес створення завдань повного резервного копіювання у Veeam Backup and Replication починається з запуску майстра створення завдань.

1. Запуск майстра створення завдань: Відкриваємо консоль Veeam Backup and Replication та переходимо до розділу "Backup & Replication". У вкладці "Home" натискаємо "Backup Job" і вибираємо тип резервного копіювання, який бажаємо створити (наприклад, для віртуальних машин, фізичних серверів або робочих станцій). [17]

2. Налаштування загальних параметрів: Вказуємо ім'я завдання та додаємо опис для зручності ідентифікації.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

3. Вибір об'єктів для резервного копіювання: Додаємо об'єкти, які потрібно включити до резервного копіювання. Це можуть бути віртуальні машини, фізичні сервери, робочі станції або окремі файли та папки.
4. Налаштування параметрів резервного копіювання: Вибираємо тип резервного копіювання (повне, інкрементальне або диференційне) та налаштовуємо інші параметри, такі як режим збереження, метод транспортування даних та налаштування дедуплікації.
5. Вибір сховища для резервних копій: Вказуємо сховище (Backup Repository), де будуть зберігатися резервні копії. Можемо вибрати один з попередньо налаштованих репозиторіїв або створити новий.
6. Налаштування параметрів запланованих завдань: Визначаємо розклад для виконання завдань резервного копіювання. Налаштовуємо завдання на щоденне, щотижневе або щомісячне виконання, а також задаємо конкретний час запуску.
7. Налаштування параметрів завдання: Вказуємо додаткові налаштування, такі як оповіщення про завершення завдання, обробку збоїв та налаштування відновлення.
8. Завершення та запуск завдання: Переглядаємо всі налаштування та натискаємо "Finish", щоб завершити створення завдання. Завдання буде додано до списку завдань і готове до запуску згідно з налаштованим розкладом (рис. 3.12).

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

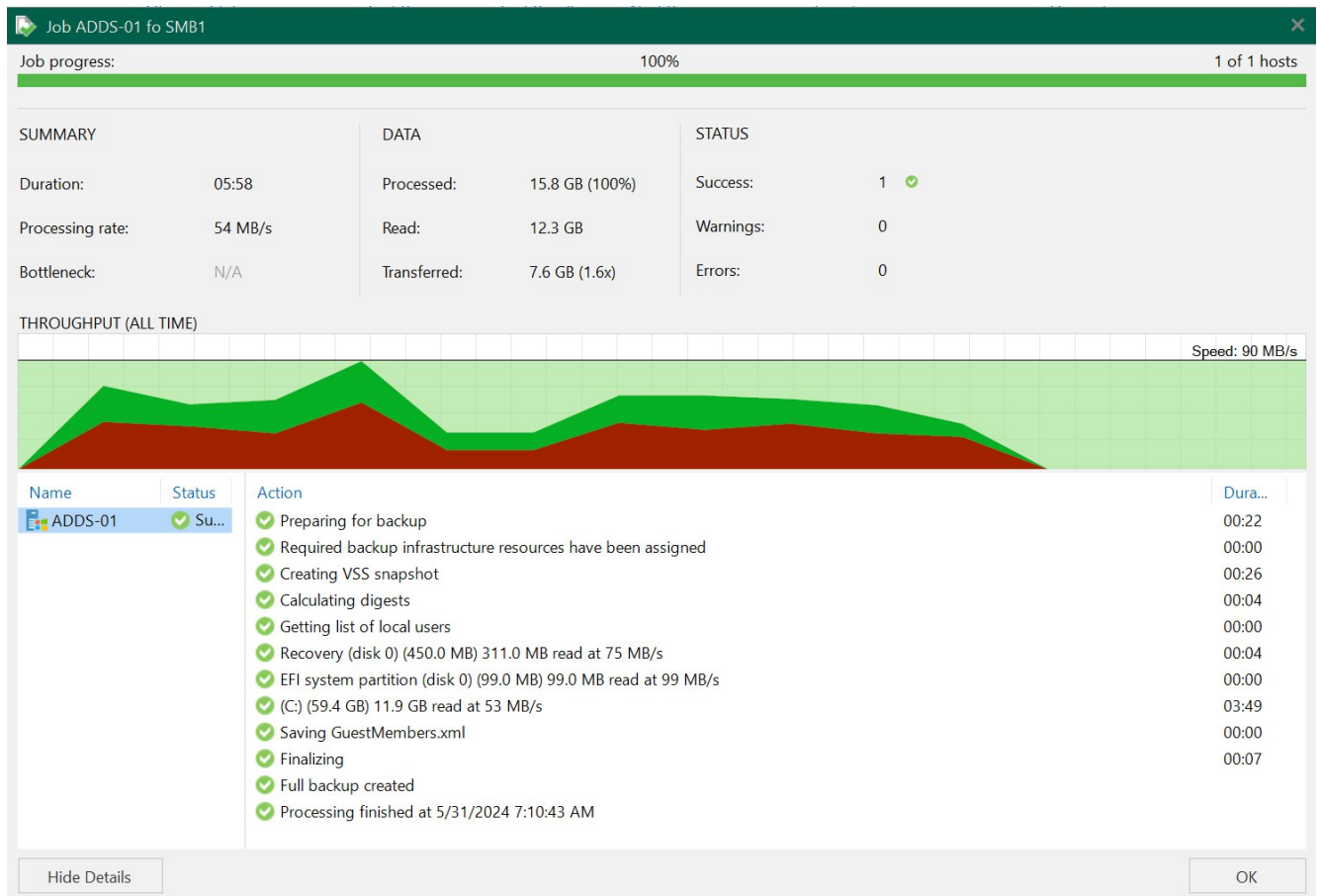


Рис 3.12. Виконане завдання резервного копіювання.

Створення завдання повного резервного копіювання у Veeam Agent

Процес створення завдання резервного копіювання у Veeam Agent починаємо з запуску Veeam Agent.

1. Запуск Veeam Agent: Відкриваємо Veeam Agent на комп'ютері або сервері, де плануємо створити завдання резервного копіювання.
2. Створення нового завдання резервного копіювання: Натискаємо "Add Job" або "Create Backup Job", щоб розпочати процес створення завдання резервного копіювання.
3. Налаштування загальних параметрів: Вказуємо ім'я завдання та додаємо опис для зручності ідентифікації.
4. Вибір об'єктів для резервного копіювання: Вибираємо, що саме бажаємо резервно копіювати. Це може бути весь комп'ютер, окремі диски, томи або конкретні файли та папки.

5. Вибір сховища для резервних копій: Вказуємо місце збереження резервних копій. Це може бути локальний диск, мережеве сховище (NAS), зовнішній диск або хмарне сховище.
6. Налаштування параметрів резервного копіювання: Вибираємо тип резервного копіювання (повне, інкрементальне або диференційне) та налаштовуємо додаткові параметри, такі як дедуплікація, шифрування та метод транспортування даних.
7. Налаштування розкладу резервного копіювання: Визначаємо розклад для виконання завдань резервного копіювання. Налаштовуємо завдання на щоденне, щотижнєве або щомісячне виконання, а також задаємо конкретний час запуску.
8. Налаштування додаткових параметрів: Вказуємо додаткові налаштування, такі як оповіщення про завершення завдання, обробку збоїв, налаштування відновлення та інші специфічні параметри.
9. Перевірка налаштувань та запуск завдання: Переглядаємо всі налаштування, щоб переконатися, що вони правильні, та натискаємо "Finish" або "Create", щоб завершити створення завдання. Завдання буде додано до списку завдань і готове до запуску згідно з налаштованим розкладом (рис. 3.13).

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

←

Restore point details

Job ADDS-01 for Veeam1

×

Backed up items: Recovery;EFI system partition (dis.

Backup duration: 0:03:53

Restore point size: 7.61 GB

Total backup size: 7.61 GB

Average backup duration: 0:03:53

Free disk space: calculating...

Action	Duration
✓ Creating VSS snapshot	0:00:22
✓ Calculating digests	0:00:06
✓ Getting list of local users	
✓ Recovery (disk 0) (450.0 MB) 311.0 MB read at 115 MB/s	0:00:02
✓ EFI system partition (disk 0) (99.0 MB) 99.0 MB read at 99 MB/s	
✓ (C:) (59.4 GB) 12.0 GB read at 116 MB/s	0:01:44
✓ Saving GuestMembers.xml	
✓ Finalizing	0:00:06
✓ Full backup created	
✓ Processing finished at 5/31/2024 7:44:27 AM	

Restore Files

Restore Volumes

Рис 3.13. Виконане завдання резервного копіювання.

Планування завдань. У Veeam Backup and Replication можна налаштувати гнучке планування завдань, що дозволяє автоматизувати процес резервного копіювання. Визначте час та частоту запуску завдань, враховуючи робочі години та періоди меншого навантаження на систему, щоб мінімізувати вплив на продуктивність (рис. 3.14).

Edit Backup Job [Backup Job AD1 from HV]

×

Schedule

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

Name

Virtual Machines

Storage

Guest Processing

Schedule

Summary

✓ Run the job automatically

● Daily at this time:

10:00 PM

Everyday

Days...

○ Monthly at this time:

10:00 PM

Fourth

Saturday

Months...

○ Periodically every:

1

Hours

Schedule...

○ After this job:

Backup Job AD1 from ESXI (Created by DE\VAdmin at 5/31/2024 4:45

Automatic retry

✓ Retry failed items processing:

3

times

Wait before each retry attempt for:

10

minutes

Backup window

□ Terminate job if it exceeds allowed backup window

If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

Window...

< Previous

Apply

Finish

Cancel

Рис 3.14. Налаштування розкладу резервного копіювання.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

Управління завданнями. У консолі Veeam Backup and Replication ви можете переглядати всі активні та заплановані завдання. Для кожного завдання доступна детальна інформація про статус, тривалість, обсяг даних та результат виконання. Ви можете запускати, зупиняти або повторно запускати завдання вручну, а також вносити зміни в налаштування завдань при необхідності (рис. 3.15).

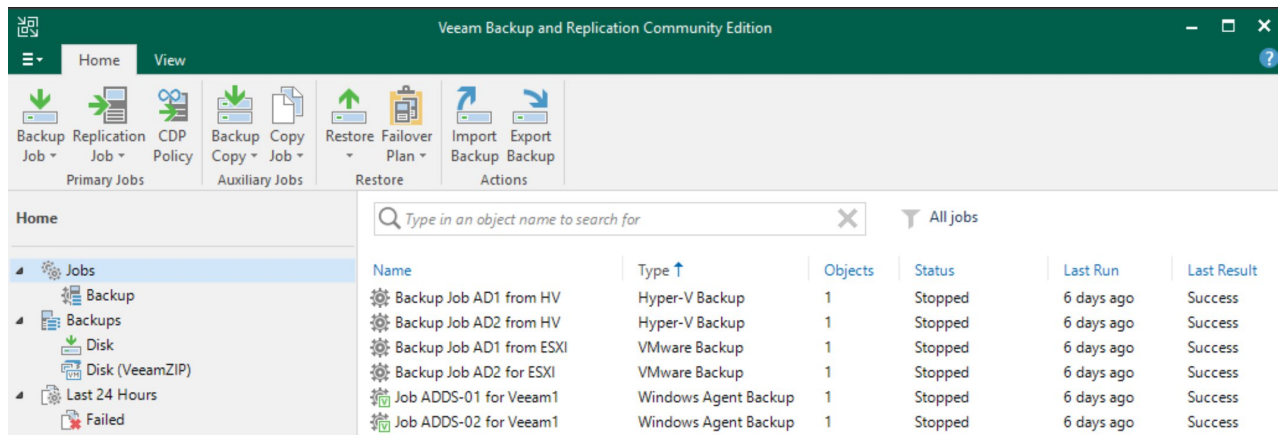


Рис 3.15. Детальна інформація про заплановані завдання.

Моніторинг завдань. Veeam Backup and Replication надає інструменти для моніторингу всіх аспектів резервного копіювання. У консолі доступний огляд статусу завдань, журнал подій та історія виконання завдань. Ви можете налаштувати оповіщення про успішне виконання завдань або про виникнення помилок, щоб оперативно реагувати на будь-які проблеми (рис. 3.16).

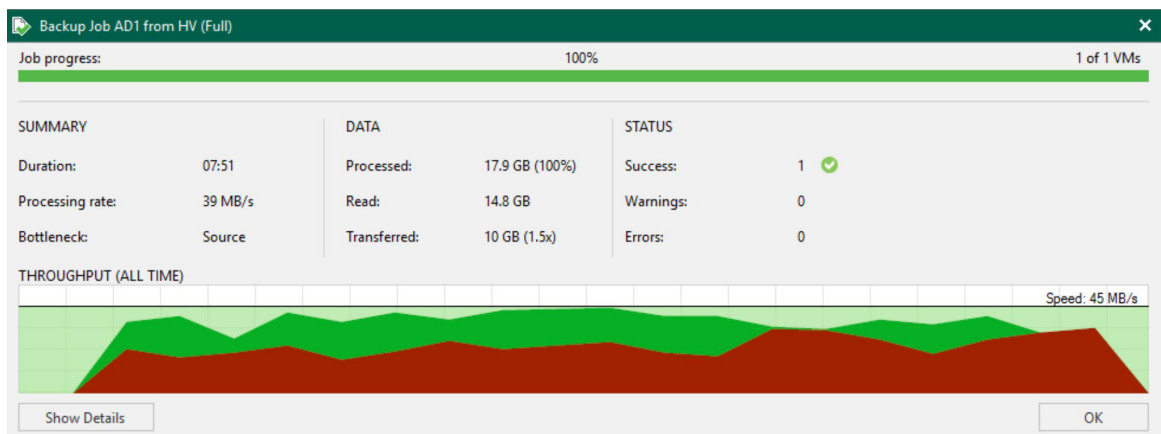


Рис 3.16. Детальна інформація про виконання завдання бекапування.

Звіти. Створення регулярних звітів дозволяє аналізувати ефективність системи резервного копіювання. Veeam Backup and Replication надає можливість створювати детальні звіти про стан завдань, обсяг збережених даних, продуктивність си-

стеми та інші ключові показники. Звіти можуть бути автоматично генеровані та відправлені на електронну пошту для зручного перегляду (рис. 3.17).

Backup job: Backup Job AD1 from HV (Full)

Created by DE\VAdmin at 5/31/2024 5:42 PM.

Success

1 of 1 VMs processed

Friday, May 31, 2024 5:43:13 PM

Success	1	Start time	5:43:13 PM	Total size	60 GB	Backup size	10 GB	
Warning	0	End time	5:51:04 PM	Data read	14.8 GB	Dedupe	4.1x	
Error	0	Duration	0:07:51	Transferred	10 GB	Compression	1.5x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
AD1	Success	5:43:28 PM	5:50:57 PM	60 GB	14.8 GB	10 GB	0:07:29	

Рис 3.17. Звіт про успішно виконане бекапування.

Резервне копіювання в Proxmox

Процес налаштування резервного копіювання в Proxmox VE з використанням Proxmox Backup Server (PBS) включає кілька основних кроків.

Спочатку підготовлюємо сховище на Proxmox Backup Server для зберігання резервних копій. Через веб-інтерфейс PBS у розділі "Storage" створюємо нове сховище, вказуючи його основні параметри, такі як тип сховища (диск або NFS), шлях до каталогу та налаштування дедуплікації. В нашому випадку це буде сховище створене на OMV з використанням протоколу SMB. [16] [18]

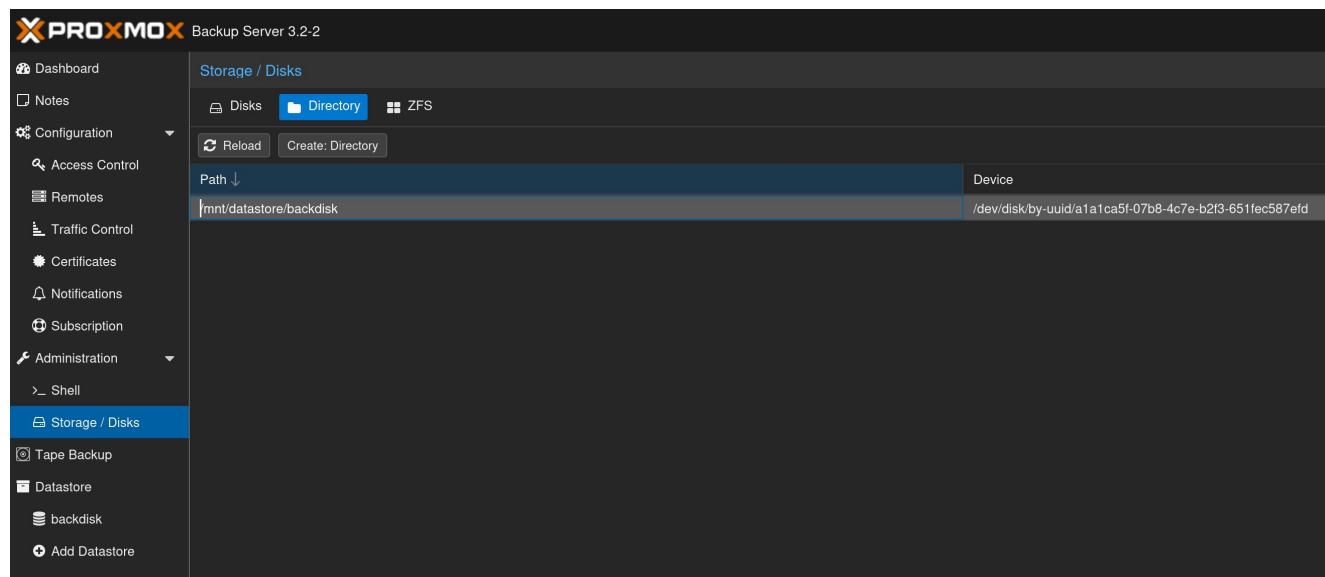


Рис 3.18. Додавання сховища.

Наступним кроком додаємо Proxmox Backup Server до Proxmox VE. У веб-інтерфейсі Proxmox VE, в розділі "Datacenter", переходимо до "Storage" і додаємо нове сховище, вибираючи тип "Proxmox Backup Server". Вводимо параметри підключення, включаючи IP-адресу PBS та токен доступу (рис. 3.19).

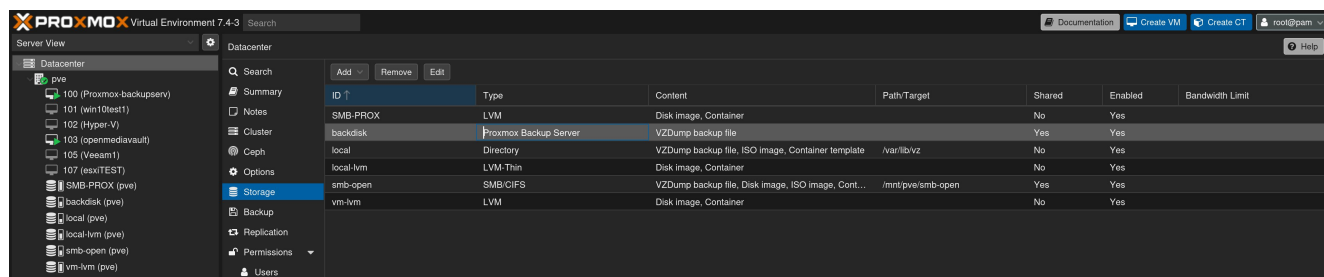


Рис 3.19. Додавання сховища резервного копіювання.

Далі налаштовуємо завдання резервного копіювання. У розділі "Datacenter" вибираємо "Backup" і створюємо нове завдання резервного копіювання. Обираємо віртуальні машини та контейнери для резервного копіювання, визначаємо частоту резервного копіювання (наприклад, щодня або щотижня), час запуску завдань та інші параметри, такі як дедуплікація і компресія даних. Завдання можуть запускатися автоматично за розкладом або вручну (рис. 3.20).

Create: Backup Job

General
Retention
Note Template

Node: -- All --
Storage: backdisk
Schedule: 10:00
Selection mode: Include selected VMs
Send email to:
Email: Notify always
Compression: ZSTD (fast and good)
Mode: Snapshot
Enable: ☒

Job Comment:

ID	Node	Status	Name	Type
☐ 100	pve	running	Proxmox-backupserv	Virtual Machine
☐ 101	pve	stopped	win10test1	Virtual Machine
☐ 102	pve	stopped	Hyper-V	Virtual Machine
☐ 103	pve	running	openmediavault	Virtual Machine
☐ 105	pve	stopped	Veeam1	Virtual Machine
☒ 107	pve	stopped	esxiTEST	Virtual Machine

Repeat missed: ☐

Help
Advanced ☒
Create

Рис 3.20. Створення завдання резервного копіювання.

Моніторинг виконаних завдань відбувається у полі "Васкуп" кожної віртуальної машини (рис. 3.21).

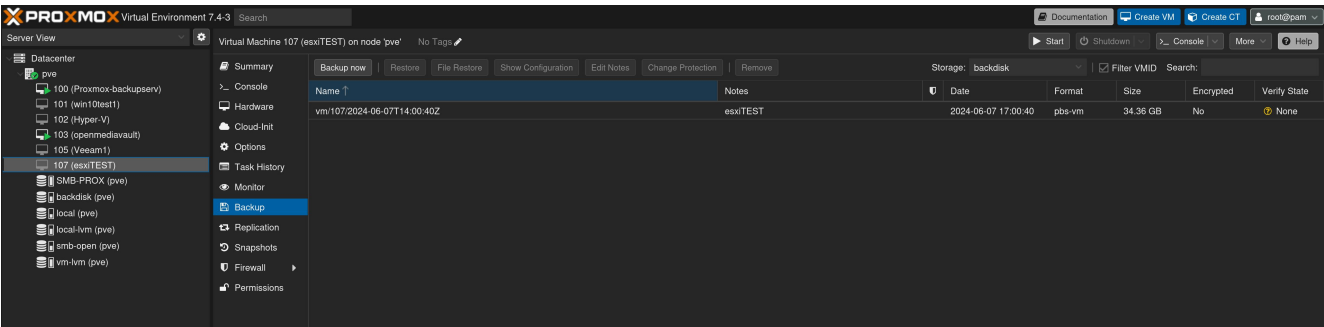


Рис 3.21. Успішний бекап.

3.3 Тестування ефективності та надійності резервного копіювання

Відновлення роботи віртуальних машин

Veeam Backup and Replication пропонує кілька варіантів відновлення для забезпечення максимальної гнучкості та швидкості при відновленні даних. Ці варіанти включають повне відновлення віртуальних машин, відновлення окремих файлів і об'єктів, відновлення додатків і баз даних, а також миттєве відновлення віртуальних машин.

Повне відновлення віртуальних машин дозволяє відновити всю віртуальну машину до попереднього стану. Цей процес включає розгортання резервної копії на наявній або новій інфраструктурі віртуалізації, що може бути критично важливим у випадку серйозних збоїв або втрати даних (рис. 3.22-3.25). [15]

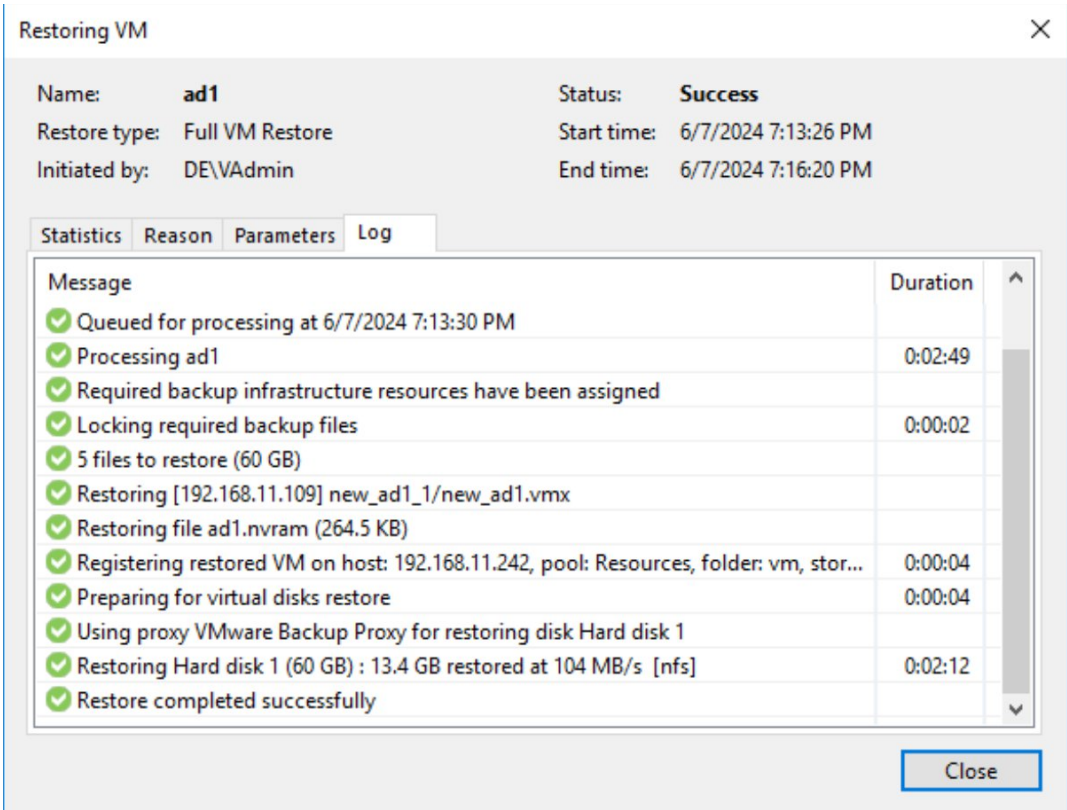


Рис. 3.22. Відновлення віртуальної машини на базі ESXi.

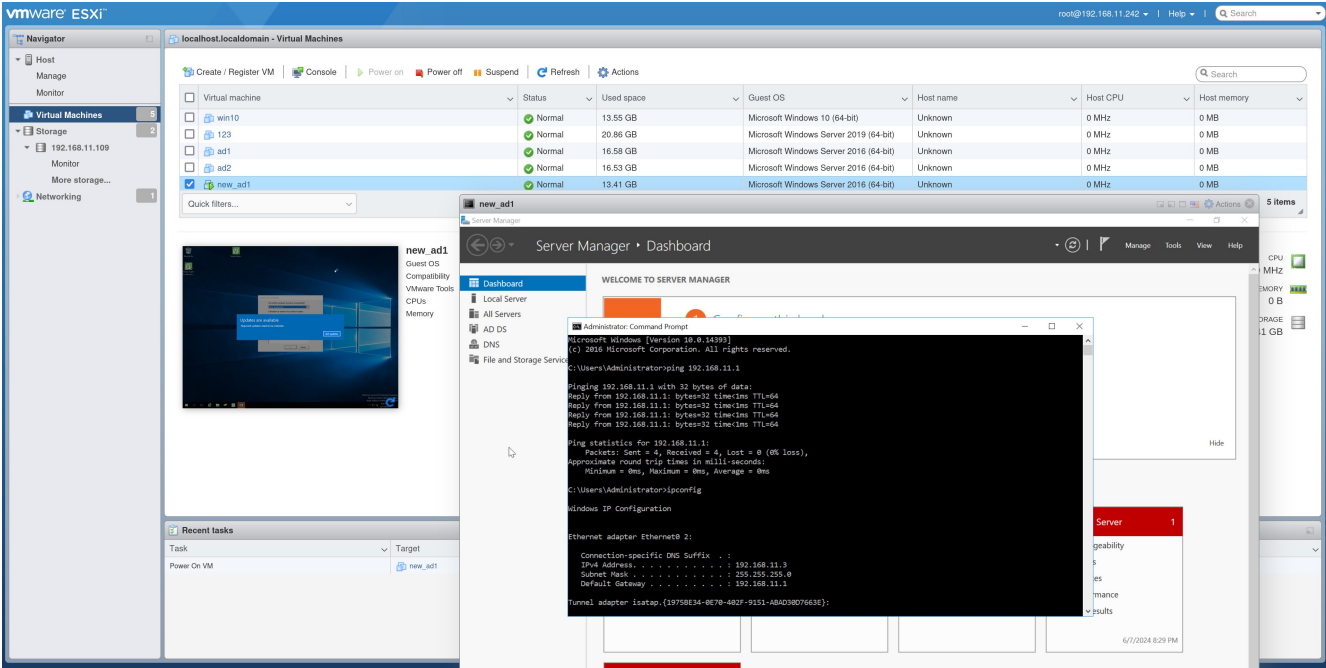


Рис. 3.23. Відновлення віртуальної машини на базі ESXi.

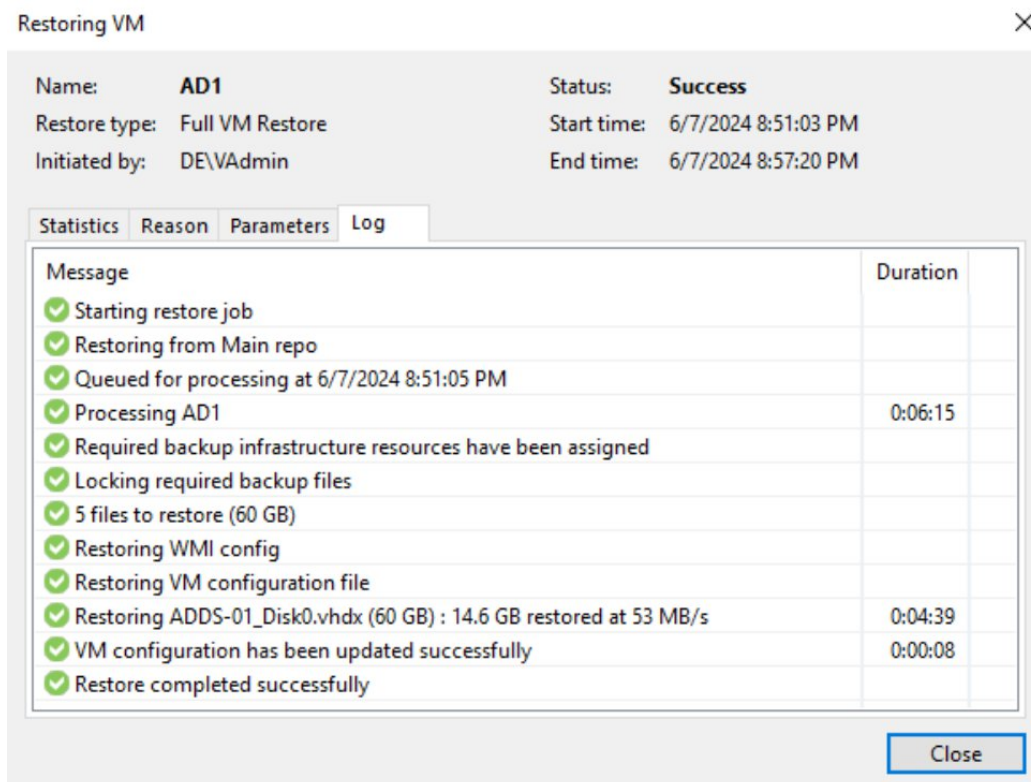


Рис. 3.24. Відновлення віртуальної машини на базі Hyper-V.

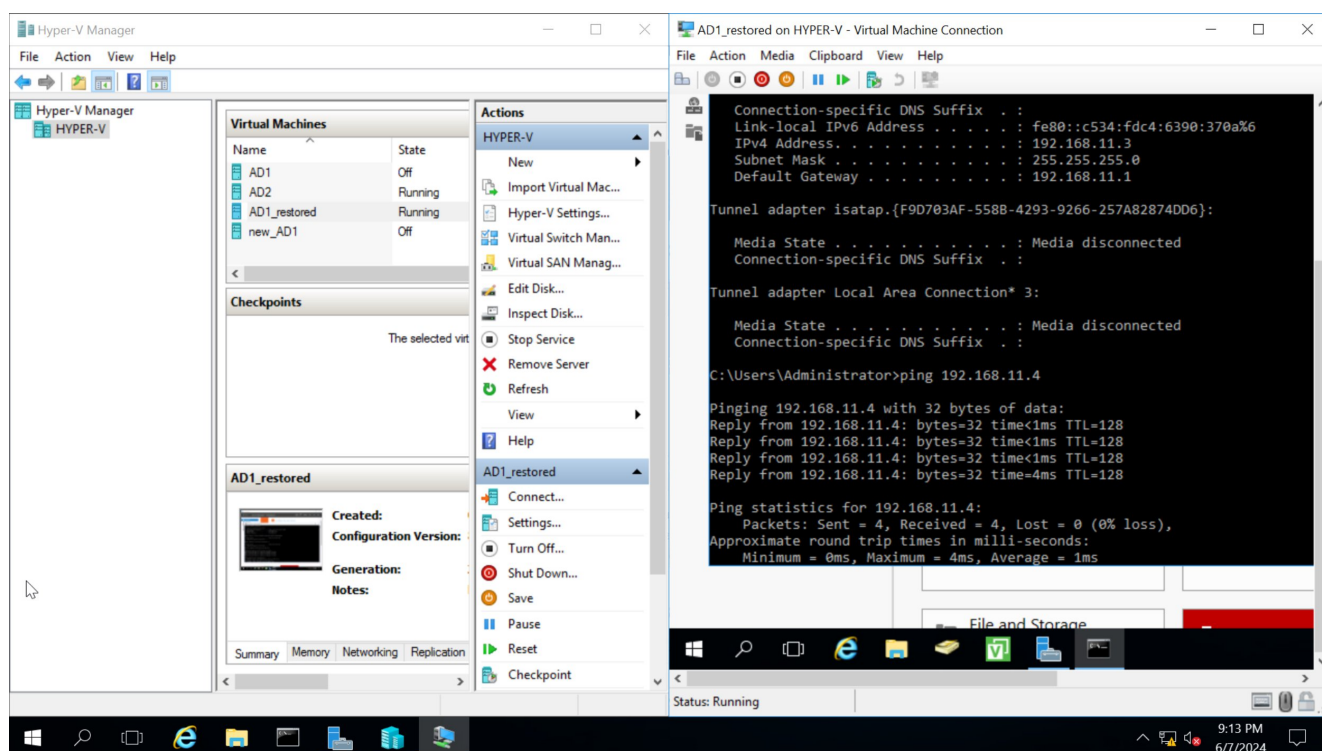


Рис. 3.25. Відновлення віртуальної машини на базі Hyper-V.

Миттєве відновлення віртуальних машин є унікальною функцією Veeam, яка дозволяє запустити віртуальну машину безпосередньо з резервної копії. Це значно зменшує час простою та забезпечує майже миттєвий доступ до критичних систем і даних, поки триває процес повного відновлення (рис. 3.26-3.29).

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

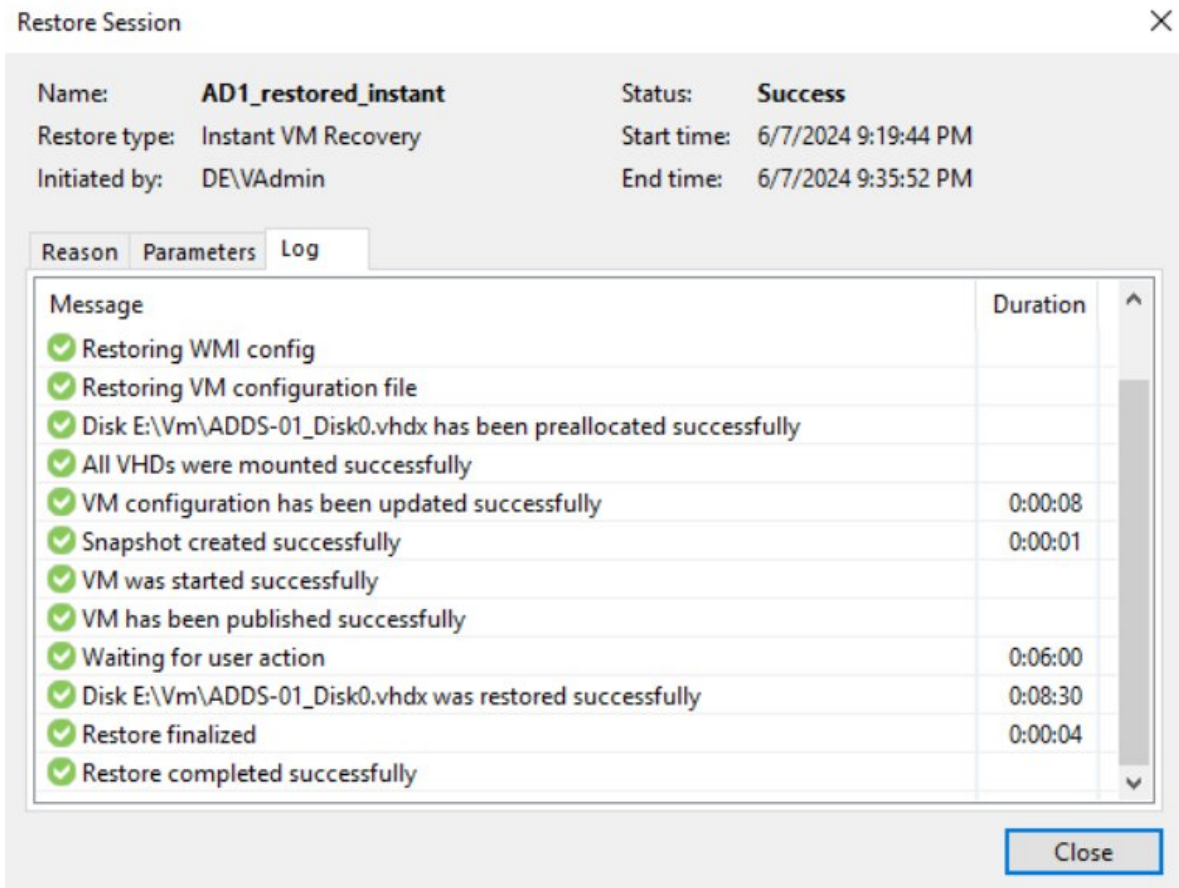


Рис. 3.28. Відновлення роботи миттєво на Нурег-V.

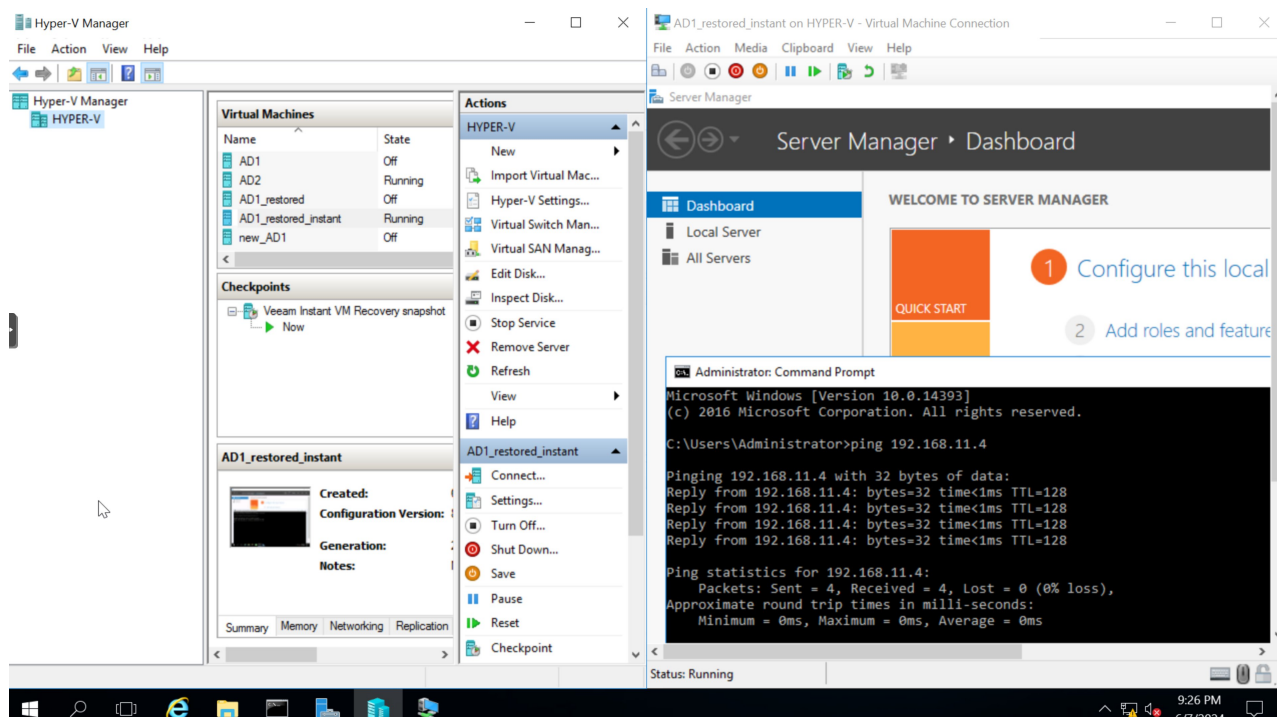


Рис. 3.29. Відновлення роботи миттєво на Нурег-V.

Відновлення окремих файлів і об'єктів дає можливість швидко відновлювати конкретні файли або об'єкти без необхідності відновлювати всю віртуальну маши-

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

ну. Це корисно в ситуаціях, коли потрібно відновити лише частину даних, наприклад, окремий документ або електронний лист (рис. 3.30-3.31). [14]

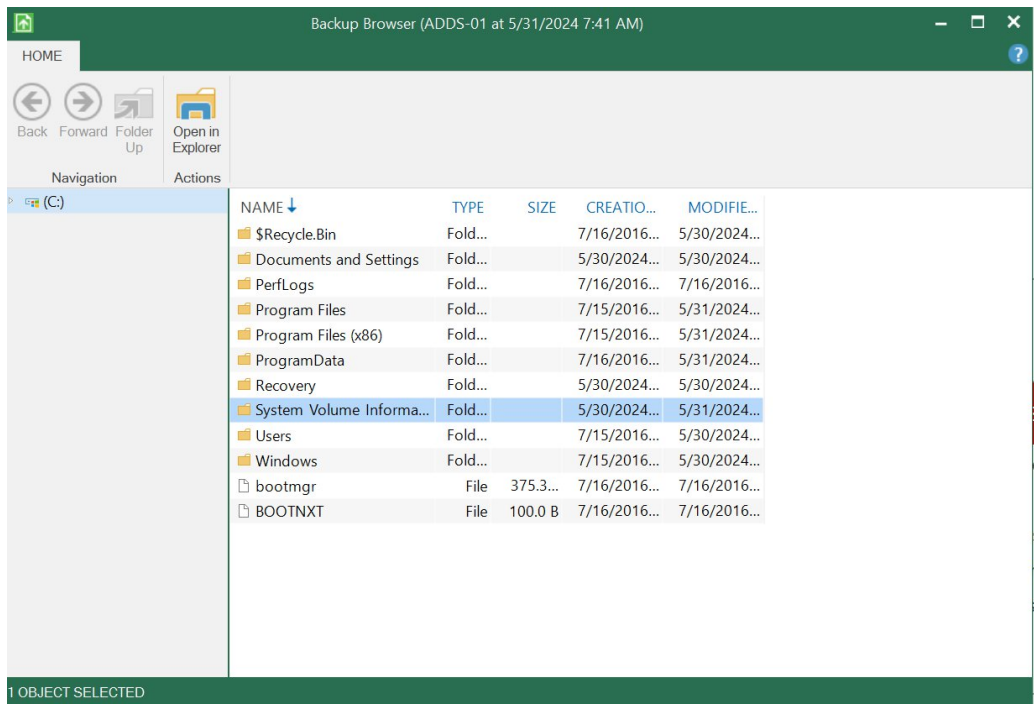


Рис. 3.30. Відновлення на рівні файлів.

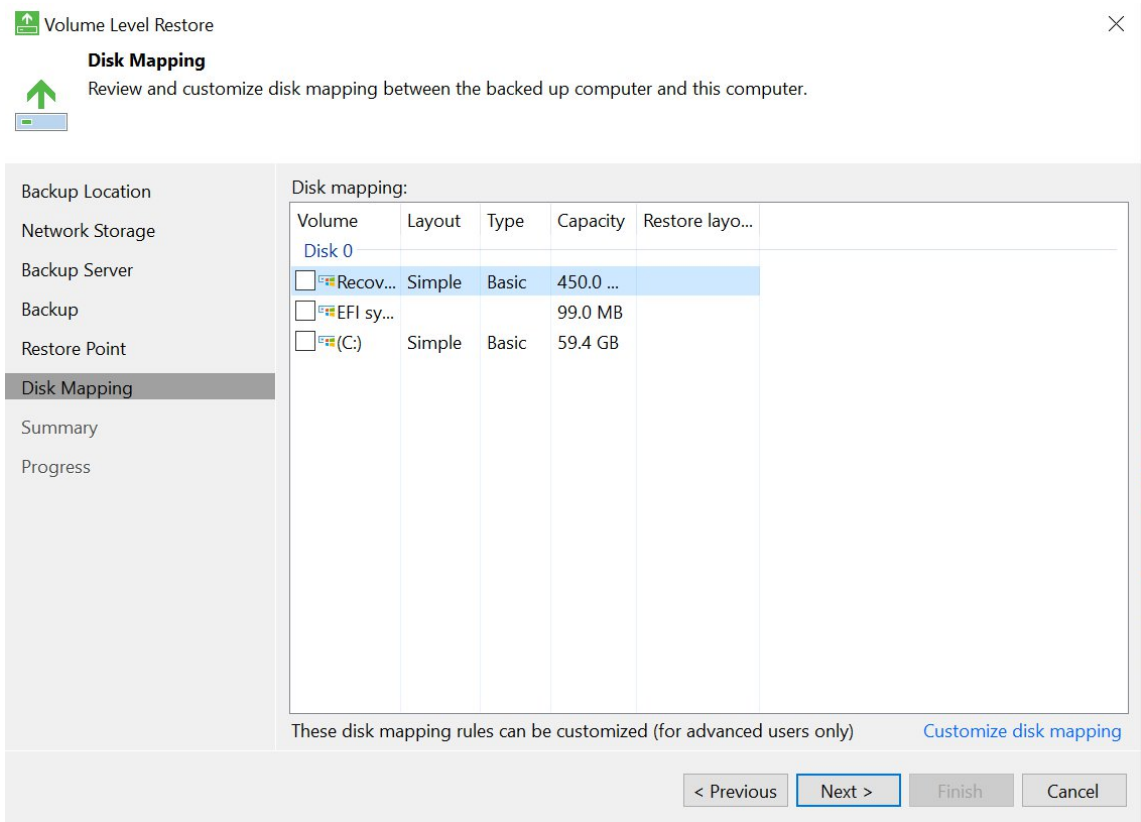


Рис. 3.31. Відновлення дисків.

Відновлення фізичного сервера

Запускаємо Veeam Agent для Windows на робочій станції або сервері. Переходимо до розділу "Recovery Media" і створюємо завантажувальний носій (USB або ISO-образ). Цей носій містить всі необхідні інструменти для відновлення системи (рис. 3.32).

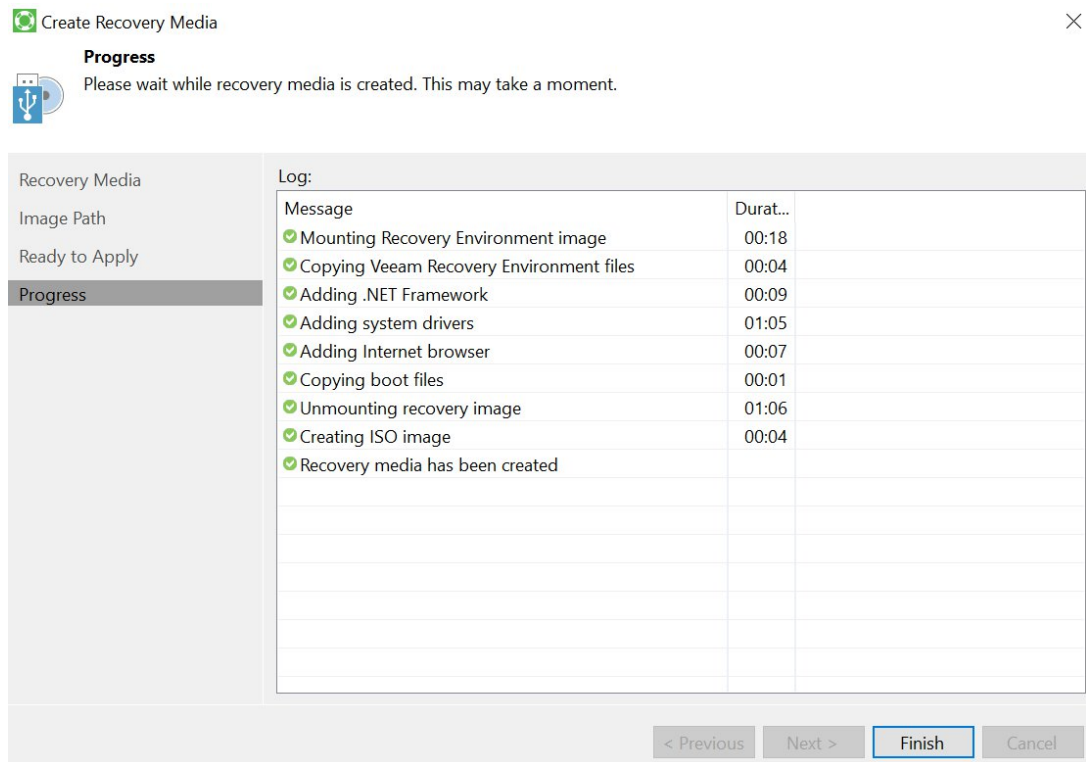


Рис. 3.32. Створення Recovery media.

Вставляємо створений завантажувальний носій у фізичний сервер та завантажуюмо його. Для цього заходимо в BIOS або UEFI сервера та змінюємо пріоритет завантаження на USB-накопичувач або диск із Veeam Recovery Media.

Після завантаження з відновлювального носія запускається Veeam Recovery Environment, який надає інструменти для відновлення системи (рис. 3.33).

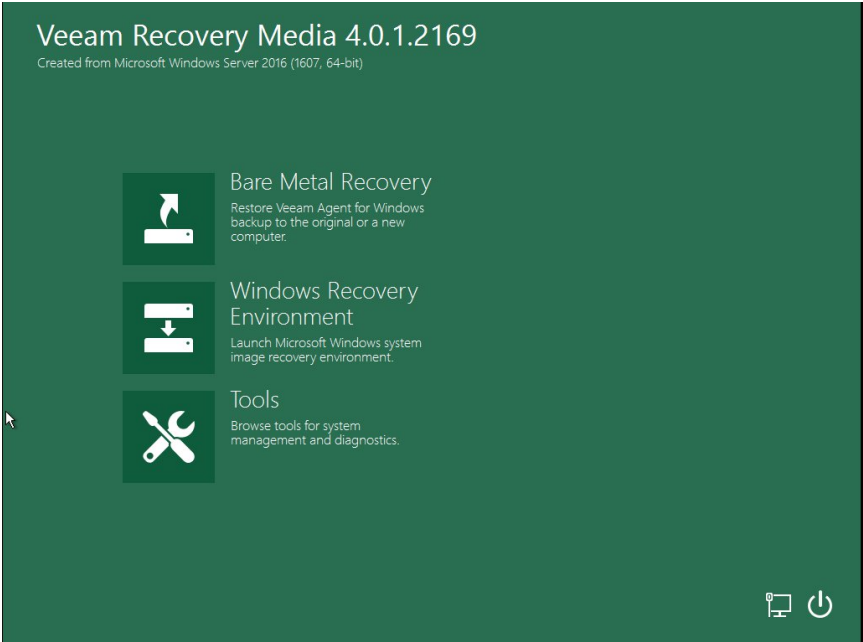


Рис. 3.33. Запуск Recovery media.

У Veeam Recovery Environment вибираємо опцію "Bare Metal Recovery" і вказуємо місце розташування резервної копії. Резервна копія може зберігатися на зовнішньому USB-накопичувачі, мережевому сховищі (наприклад, CIFS/NFS), або у Veeam Backup Repository (рис 3.34).

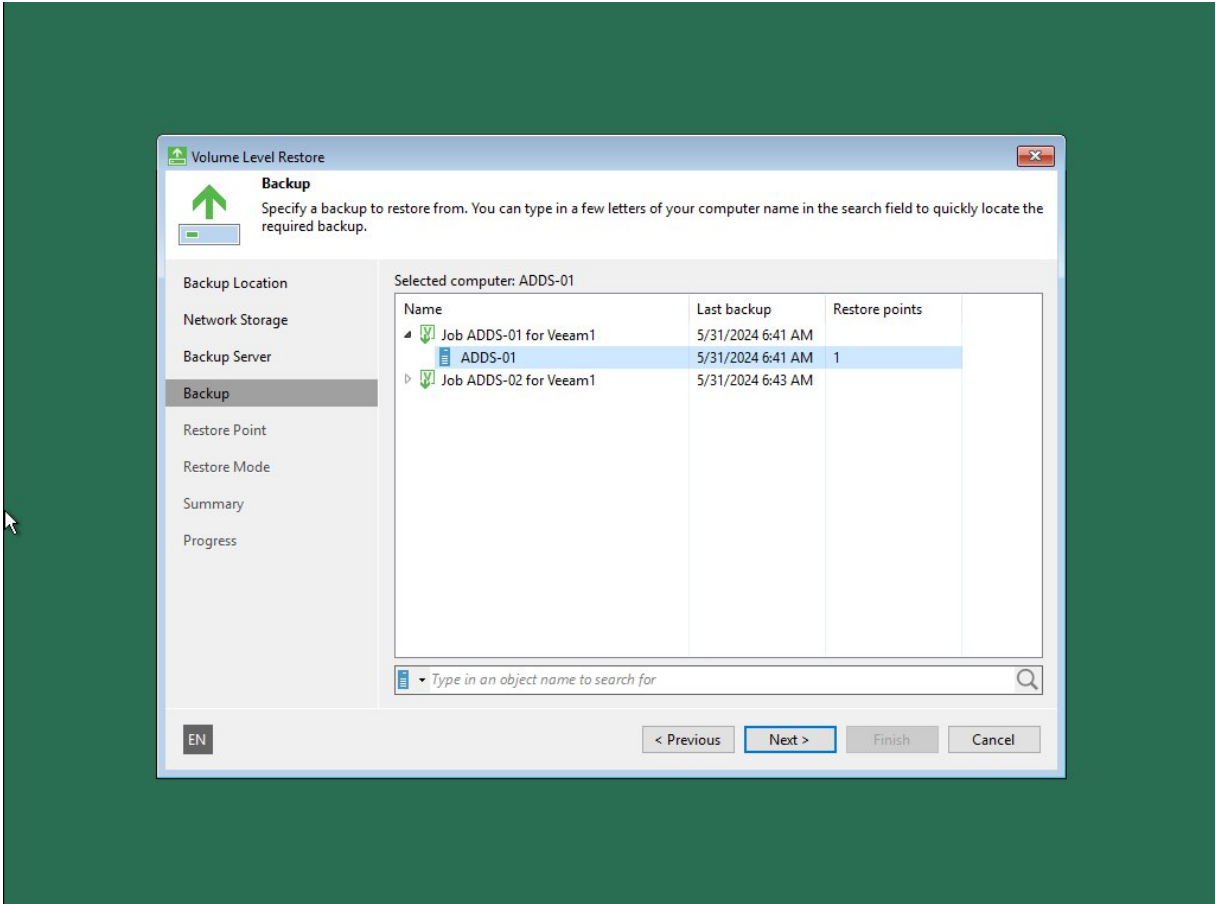


Рис. 3.34. Вибір резервної копії.

Вибираємо всю систему або окремі диски для відновлення. Для відновлення всього сервера вибираємо всі доступні диски. Підтверджуємо вибір та запускаємо процес відновлення. Veeam відновлює дані з резервної копії на сервер, включаючи операційну систему, додатки та всі налаштування (рис. 3.35).

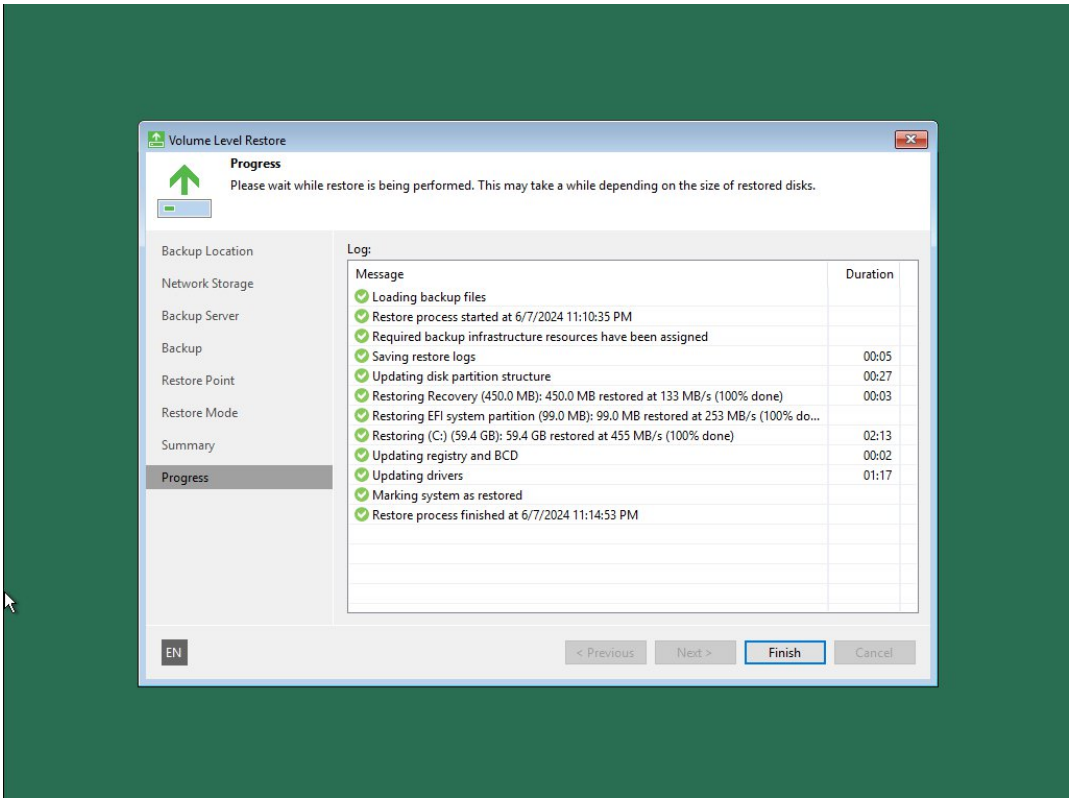


Рис. 3.35. Відновлення серверу з Veeam Backup and Replication серверу.

Після завершення процесу відновлення виймаємо відновлювальний носій і перезавантажуємо сервер. Сервер завантажується з відновленими даними, і система повертається до стану на момент створення резервної копії (рис. 3.36).

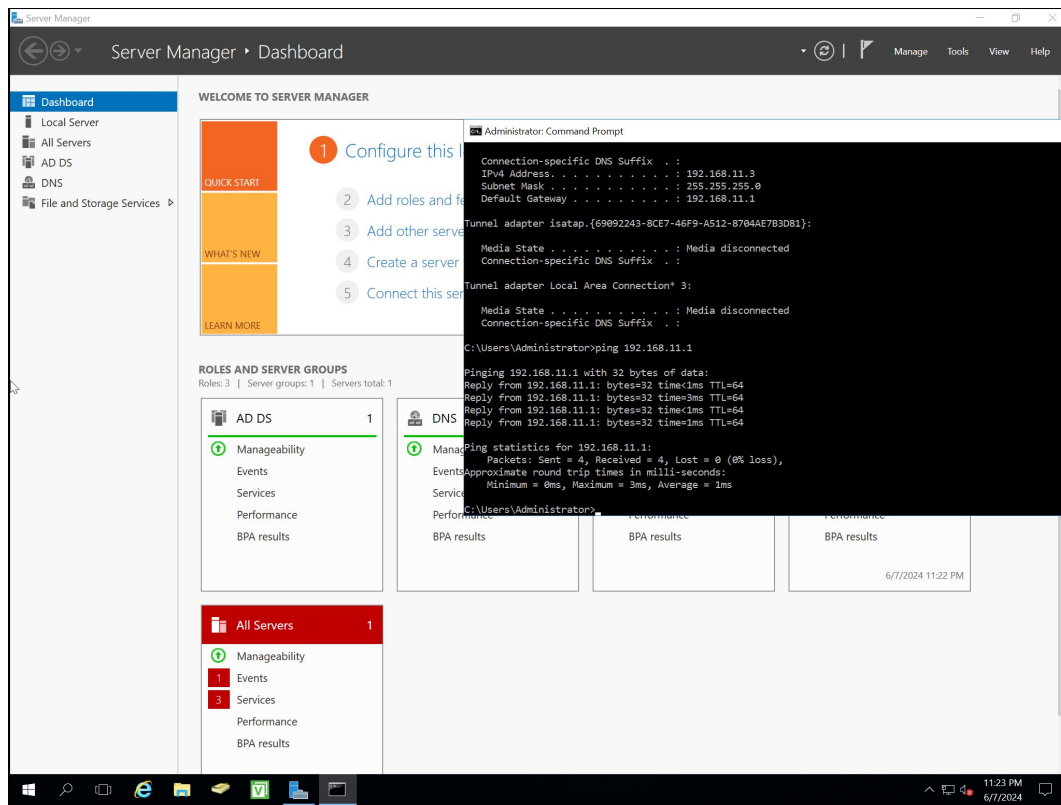


Рис. 3.36. Відновлений сервер.

Висновок до третього розділу

Третій розділ присвячений практичному аспекту – налаштуванню та тестуванню інфраструктури на базі Veeam Backup and Replication. Важливим етапом було проведення інсталяції програмного забезпечення та налаштування серверів резервного копіювання, що включало як фізичні, так і віртуальні середовища. Інтеграція Veeam Backup and Replication з Proxmox Backup Server дозволила досягти високого рівня надійності та доступності даних завдяки функціям дедуплікації, компресії та інкрементального резервного копіювання. В ході тестування резервних копій були перевірені різні сценарії відновлення даних, що підтвердило готовність інфраструктури до ефективного відновлення інформації у разі збоїв. Результати тестування показали, що система здатна забезпечити швидке відновлення даних та мінімізувати втрати інформації, що є критично важливим для підтримання безперервності бізнес-процесів. Цей розділ підтвердив високу надійність, ефективність та функціональність впровадженої системи резервного копіювання у корпоративному середовищі, забезпечуючи захист даних від втрат та швидке їх відновлення у разі необхідності.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У цій кваліфікаційній роботі ми здійснили всебічний аналіз та практичне впровадження системи резервного копіювання, що має критичне значення для забезпечення безперервності бізнес-процесів та захисту даних у корпоративних середовищах. Ми розглянули фундаментальні аспекти технології резервного копіювання, зокрема принципи та види резервного копіювання, методи відновлення даних, а також процеси, які дозволяють мінімізувати ризики втрати інформації. Проектування мережі резервного копіювання базувалося на виборі оптимального програмного та апаратного забезпечення. Окрема увага приділялась платформам віртуалізації, таким як ESXi, Hyper-V та VMware Workstation Pro, які інтегрувались у загальну інфраструктуру резервного копіювання. Налаштування серверів і мережних з'єднань дозволило створити надійну та ефективну систему, яка забезпечує стабільну роботу та швидке відновлення даних у разі збоїв.

Практична частина роботи зосередилася на інсталяції та налаштуванні Veeam Backup and Replication, що є провідним рішенням у сфері резервного копіювання. Інтеграція цього програмного забезпечення з Proxmox Backup Server та іншими компонентами інфраструктури дозволила досягти високого рівня захищеності даних, завдяки використанню сучасних методів дедуплікації, компресії та інкрементального резервного копіювання. Тестування показало, що система здатна забезпечити швидке та ефективне відновлення даних, мінімізуючи час простою бізнес-процесів.

Загалом, результати роботи підтверджують, що впроваджена система резервного копіювання відповідає високим вимогам надійності та ефективності, необхідним для сучасних корпоративних середовищ. Вона забезпечує захист даних від втрат, викликаних різноманітними факторами, та дозволяє швидко відновлювати інформацію, що є ключовим для підтримки стабільної роботи підприємства. Таким чином, виконані дослідження та впровадження підтвердили доцільність і ефективність обраних підходів та технологій для забезпечення резервного копіювання у корпоративних середовищах.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Офіційна документація Veeam Backup & Replication [Електронний ресурс]. – Режим доступу: <https://www.veeam.com/documentation-guides-datasheets.html?productId=8&version=product%3A8%2F221>
2. Microsoft Learn. Windows server 2016 Active Directory [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels>
3. Veeam Backup and Replication installation guide [Електронний ресурс]. – Режим доступу: https://helpcenter.veeam.com/docs/backup/qsg_vsphere/setup.html?ver=120
4. What Is Network Backup? [Електронний ресурс]. – Режим доступу: <https://www.solarwinds.com/resources/it-glossary/network-backup>
5. Network Disaster Recovery Plan [Електронний ресурс]. – Режим доступу: <https://www.comparitech.com/net-admin/network-disaster-recovery/>
6. Building an Effective Backup Strategy for an Organization [Електронний ресурс]. – Режим доступу: <https://www.nakivo.com/blog/how-to-build-a-backup-strategy-full-guide/>
7. Guide to Server Backups: Creating a Backup Strategy [Електронний ресурс]. – Режим доступу: <https://www.veeam.com/blog/server-backup-guide.html>
8. Proxmox installation guide [Електронний ресурс]. – Режим доступу: <https://phoenixnap.com/kb/install-proxmox>
9. Esxi installation guide [Електронний ресурс]. – Режим доступу: <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-93D0227B-E5ED-40B0-B8E2-71141A32EB00.html>
10. Hyper-V role on Windows Server [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server>
11. OMV guide [Електронний ресурс]. – Режим доступу: <https://docs.openmediavault.org/en/latest/installation/index.html>

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

12. Резервне копіювання та його види [Електронний ресурс]. – Режим доступу: <https://www.sim-networks.com/ukr/blog/backup-full-increment-differential>
13. Бекап, снапшот та реплікація [Електронний ресурс]. – Режим доступу: <https://gigacloud.ua/blog/navchannja/bekap-snapshot-ta-replikacija-scho-ce-i-v-chomu-riznicja>
14. Restoring Volumes from Veeam Agent Backups [Електронний ресурс]. – Режим доступу: https://helpcenter.veeam.com/docs/backup/cloud/cloud_connect_volume_restore.html?ver=120
15. Restoring infrastructure from scratch with Veeam [Електронний ресурс]. – Режим доступу: <https://www.veeam.com/blog/restoring-infrastructure-from-scratch-with-veeam.html>
16. Proxmox backup create [Електронний ресурс]. – Режим доступу: <https://linuxconfig.org/how-to-create-a-backup-with-proxmox-backup-client>
17. Creating jobs Veeam [Електронний ресурс]. – Режим доступу: https://helpcenter.veeam.com/docs/backup/vsphere/backup_job.html?ver=120
18. Backup and Restore proxmox [Електронний ресурс]. – Режим доступу: https://pve.proxmox.com/wiki/Backup_and_Restore

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

Шифрування у Veeam Backup and Replication

Шифрування під час передачі даних

Veeam використовує протокол SSL/TLS для шифрування даних під час передачі між компонентами інфраструктури резервного копіювання. Це забезпечує захист даних від несанкціонованого доступу під час їх передачі через мережу, зокрема між сервером резервного копіювання, проксі-серверами і репозиторіями.

Шифрування під час зберігання даних

Для захисту даних, що зберігаються в резервних копіях, Veeam Backup & Replication використовує шифрування на основі алгоритму AES (Advanced Encryption Standard) з довжиною ключа 256 біт. Це забезпечує високий рівень безпеки даних. Процес шифрування може бути налаштований на різних рівнях:

- **Резервні завдання (Backup Jobs).** Під час налаштування завдань резервного копіювання можна увімкнути шифрування даних. Шифрування буде застосовуватися до всіх створених резервних копій.
- **Репозиторії резервних копій.** Veeam дозволяє шифрувати дані безпосередньо в репозиторіях, де зберігаються резервні копії.

Керування ключами шифрування.

Veeam Backup & Replication використовує внутрішній механізм керування ключами шифрування. Ключі можуть бути створені і збережені безпосередньо в консолі Veeam. Для підвищення безпеки Veeam рекомендує зберігати ключі шифрування окремо від резервних копій.

Ключами шифрування можна управляти через консоль Veeam, де також можна змінювати ключі або видаляти їх за необхідністю. Це важливо для підтримання безпеки і управління доступом до даних.

Аутентифікація і контроль доступу

Всі операції з шифрування і розшифрування даних в Veeam Backup & Replication вимагають аутентифікації. Це гарантує, що лише авторизовані користувачі мають доступ до резервних копій. Контроль доступу здійснюється через систему ролей і прав доступу, що дозволяє гнучко управляти правами користувачів і груп.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

Практичне застосування шифрування

Налаштування шифрування резервного завдання. При створенні або редагуванні резервного завдання у Veeam Backup & Replication можна увімкнути шифрування даних у вкладці "Storage" (Сховище) та вказати пароль для шифрування.

Шифрування репозиторіїв. Шифрування можна увімкнути на рівні репозиторію, обравши відповідний параметр під час його створення або налаштування. Це забезпечує автоматичне шифрування всіх даних, що зберігаються в даному репозиторії.

		Дехтяр М.С.			ККІКБ.КР.Б – 123 – 06 – ПЗ	Арк.
		Головня О.С.				86
Змн.	Арк.	№ докум.	Підпис	Дата		