ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «АВТОМАТИЗОВАНА СИСТЕМА РЕЗЕРВНОГО КОПІЮВАННЯ У ЛОКАЛЬНИХ ХМАРНИХ СХОВИЩАХ»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми «Комп'ютерна інженерія»
(назва)

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

_____ *Данііл ХОТИНЕНКО*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач(ка) вищої освіти гр. КІД-42
Данііл ХОТИНЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Віталій ВОЛОХІН
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерна інженерія

Освітньо-професійна програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
«_____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Хотиненко Данііл Володимирович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Автоматизована система резервного копіювання у локальних хмарних сховищах»
керівник кваліфікаційної роботи: Віталій ВОЛОХІН, кандидат технічних наук, доцент,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025р. №56
2. Строк подання кваліфікаційної роботи «05» червня 2025р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, стандарти та протоколи резервного копіювання, архітектура локальних хмарних сховищ, методи автоматизації резервного копіювання, безпека та надійність збереження даних, тестування та порівняльний аналіз рішень для резервного копіювання.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
    1. Основи автоматизації резервного копіювання в локальному хмарному сховищі
    2. Проєктування систем автоматизації резервного копіювання
    3. Впровадження та перспективи масштабування локального хмарного сховища
5. Перелік ілюстративного матеріалу: *презентація*
    1. Мета, об'єкт, предмет дослідження
    2. Актуальність роботи
    3. Недоліки традиційних ручних та пропрієтарних рішень для резервного копіювання
    4. Особливість впровадження автоматизації резервного копіювання
    5. Архітектура автоматизованої системи резервного копіювання у локальне хмарне сховище
    6. Алгоритм роботи автоматизованої системи резервного копіювання у локальне хмарне сховище
    7. Демонстрація локального хмарного сховища Nextcloud
    8. Інструменти резервного копіювання: WebDAV, rsync, BorgBackup
    9. Демонстрація методу резервного копіювання через WebDAV і rsync з логуванням
    10. Демонстрація резервного копіювання з логуванням і email-сповіщенням

11. Демонстрація методу автоматизованого резервного копіювання через Cron Job
12. Порівняння автоматизованої системи резервного копіювання у локальному хмарному сховищі
13. Висновки
14. Публікації та апробація роботи

6. Дата видачі завдання «24» лютого 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.02-19.03.2025	
2	Обробка матеріалу	20.03-02.04.2025	
3	Розробка теоретичної частини	03.04-07.04.2025	
5	Проєктування систем автоматизації резервного копіювання	08.04-27.04.2025	
6	Впровадження та перспективи масштабування локального хмарного сховища	28.04-11.05.2025	
7	Висновки за результатами аналізу	12.05-15.05.2025	
8	Розробка презентації	16.05-26.05.2025	
9	Передзахист	27.05-29.05.2025	
10	Здача в деканат	30.05-05.06.2025	

Здобувач(ка) вищої освіти _____ Даніїл ХОТИНЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Віталій ВОЛОХІН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 89 стор., 112 рис., 3 табл., 31 джерел.

Мета роботи – оптимізація процесів резервного копіювання в локальних хмарних сховищах за рахунок використання методів автоматизації та відкритих програмних рішень.

Об'єкт дослідження – процеси резервного копіювання в локальних хмарних сховищах.

Предмет дослідження – методи та технології автоматизації резервного копіювання в локальних хмарних сховищах.

Короткий зміст роботи: У роботі розглянуто особливості автоматизації резервного копіювання в локальних хмарних сховищах як ефективну альтернативу традиційним ручним і пропрієтарним рішенням. Акцент зроблено на використанні інструментів з відкритим кодом, зокрема Nextcloud у поєднанні з WebDAV, rsync, BorgBackup та Cron Jobs. Описано архітектуру сховища, методи шифрування, дедуплікації та моніторингу, що забезпечують збереження даних без втручання користувача.

На основі практичного впровадження у віртуальному середовищі VMware проаналізовано ключові труднощі та переваги запропонованої системи. Порівняно з загальнодоступними сервісами, локальне рішення дозволяє краще контролювати доступ, підвищити безпеку та гнучко адаптувати систему під конкретні потреби організації.

КЛЮЧОВІ СЛОВА: РЕЗЕРВНЕ КОПІЮВАННЯ, АВТОМАТИЗАЦІЯ, ХМАРНЕ СХОВИЩЕ, БЕЗПЕКА, ДЕДУПЛІКАЦІЯ, ВІДНОВЛЕННЯ, ШИФРУВАННЯ, ЗБЕРЕЖЕННЯ ДАНИХ, ОПТИМІЗАЦІЯ, НАДІЙНІСТЬ, ХМАРНІ ТЕХНОЛОГІЇ.

ABSTRACT

Text part of the qualification work for the bachelor's degree: 89 pages, 112 figures, 3 tables, 31 sources.

The purpose of the work is to optimize backup processes in local cloud storage through the use of automation methods and open software solutions.

The object of the research is backup processes in local cloud storage.

The subject of the research is methods and technologies for automating backup in local cloud storage.

Summary of the work: The paper considers the features of automating backup in local cloud storage as an effective alternative to traditional manual and proprietary solutions. The emphasis is on the use of open source tools, in particular Nextcloud in combination with WebDAV, rsync, BorgBackup and Cron Jobs. The storage architecture, encryption, deduplication and monitoring methods are described, which ensure data preservation without user intervention.

Based on practical implementation in the VMware virtual environment, the key difficulties and advantages of the proposed system are analyzed. Compared to publicly available services, the local solution allows for better access control, increased security, and flexible adaptation of the system to the specific needs of the organization.

KEYWORDS: BACKUP, AUTOMATION, CLOUD STORAGE, SECURITY, DEDUPLICATION, RECOVERY, ENCRYPTION, DATA STORAGE, OPTIMIZATION, RELIABILITY, CLOUD TECHNOLOGIES.

ЗМІСТ

ВСТУП..... 9
РОЗДІЛ 1 ОСНОВИ АВТОМАТИЗАЦІЇ РЕЗЕРВНОГО КОПІЮВАННЯ В ЛОКАЛЬНОМУ ХМАРНОМУ СХОВИЩІ 10
1.1 Концепція автоматизованого резервного копіювання 10
1.2 Принципи та застосування локального хмарного сховища..... 17
1.3 Важливість автоматизації резервного копіювання..... 26
1.4 Виклики та перспективи автоматизації резервного копіювання. 31
РОЗДІЛ 2 ПРОЄКТУВАННЯ СИСТЕМ АВТОМАТИЗАЦІЇ РЕЗЕРВНОГО КОПІЮВАННЯ..... 35
2.1 Технології та інструменти для автоматизації резервного копіювання..... 35
2.2 Основні компоненти автоматизованої системи резервного копіювання 40
2.3 Стратегії оптимізації автоматизованої системи резервного копіювання..... 48
2.4 Розгортання локального хмарного сховища у віртуальному середовищі..... 54
РОЗДІЛ 3 ВПРОВАДЖЕННЯ ТА ПЕРСПЕКТИВИ МАСШТАБУВАННЯ ЛОКАЛЬНОГО ХМАРНОГО СХОВИЩА 67
3.1 Реалізація автоматизації резервного копіювання. 67
3.2 Потенційні труднощі та методи їх усунунення при розгортанні локального хмарного сховища у віртуалізованому середовищі..... 83
3.3 Рекомендації і перспективи впровадження 92
ВИСНОВКИ..... 97
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ……...……..98
Додаток А. Код сценарію автоматизації резервного копіювання в хмару через WebDAV і rsync з логуванням…….....101
Додаток Б. Код сценарію автоматизації резервного копіювання в хмару з логуванням і сповіщенням на email.…….....102
Додаток В. Код розгортання Nginx Proxy Manager зі сертифікацією Let`s Encrypt (через Docker Compose).……....103
Додаток Г. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація).…….....104

ВСТУП

Зберігання та керування даними стало ключовим елементом для стабільної роботи як приватних користувачів, так і підприємств. Збільшення обсягів інформації, що щодня генерується, призводить до зростання потреби у надійних, ефективних та зручних рішеннях для резервного копіювання. Особливо це стосується ситуацій, коли дані мають залишатися під повним контролем користувача, зберігаючись на локальній інфраструктурі, а не в публічних хмарних сервісах. У цьому контексті автоматизація резервного копіювання стає не розкішшю, а необхідністю.

Традиційні методи збереження даних, що базуються на ручному копіюванні або жорстко заданих сценаріях, часто не відповідають сучасним вимогам гнучкості, швидкості реагування та безперервності. Їх супроводжують ризики втрати важливої інформації через людський фактор, затримки у виконанні, або відсутність оновлених копій. Пропрієтарні рішення, хоча й спрощують деякі процеси, водночас обмежують користувача у свободі налаштувань, інтеграції та контролю над збереженими даними.

Зі зростанням інтересу до локальних хмарних середовищ все частіше з’являється потреба у впровадженні гнучких систем, які дозволяють забезпечити як централізоване зберігання, так і автоматизоване резервне копіювання з мінімальним втручанням. Власні рішення на основі відкритого програмного забезпечення дозволяють уникнути прив'язки до зовнішніх провайдерів, краще захистити конфіденційність інформації та ефективніше управляти наявними ресурсами.

Сучасні інструменти дають змогу реалізовувати локальні хмарні рішення із широкими можливостями доступу, синхронізації та збереження даних. Водночас виникає потреба в розумінні основних принципів побудови таких систем, їхньої архітектури, ключових компонентів і того, як саме автоматизація може підвищити надійність зберігання інформації, не ускладнюючи адміністрування.

РОЗДІЛ 1 ОСНОВИ АВТОМАТИЗАЦІЇ РЕЗЕРВНОГО КОПІЮВАННЯ В ЛОКАЛЬНОМУ ХМАРНОМУ СХОВИЩІ

1.1 Концепція автоматизованого резервного копіювання

З розвитком цифровізації обсяг інформації невпинно зростає, і важливо не тільки зберігати її, а й забезпечувати її захист та доступність у будь-який момент. Втрата даних може спричинити серйозні наслідки, тому необхідно використовувати ефективні методи збереження, серед яких особливу роль відіграє автоматизоване резервне копіювання. Його головне завдання – гарантувати безперервний доступ до важливої інформації, незалежно від можливих збоїв або втрат основного носія даних [1].

Резервне копіювання – це не просто дублювання файлів, а комплексний процес, що враховує відмовостійкість, доступність і безпеку даних. У випадках, коли інформація є критично важливою, її необхідно захищати від випадкового видалення, системних збоїв, кібератак та інших загроз. Використання автоматизованих систем резервного копіювання дозволяє уникнути людських похибок, адже всі процеси відбуваються без втручання користувача, відповідно до заданих алгоритмів і політик. Такі системи забезпечують не лише збереження інформації, а й її швидке відновлення у разі виникнення непередбачуваних ситуацій [1-2].

На відміну від ручного копіювання, яке вимагає регулярного втручання та контролю, автоматизовані рішення працюють на основі розкладів та заданих параметрів, що дозволяє системним адміністраторам та користувачам зосередитися на інших важливих завданнях, не турбуючись про те, що процес збереження даних буде пропущений або виконаний некоректно. Використання таких систем особливо актуальне для підприємств, що працюють із великими обсягами інформації, які постійно оновлюються. Наприклад, фінансові установи, медичні заклади, центри

обробки даних та інші організації, для яких втрата інформації може мати катастрофічні наслідки [2].

Автоматизовані системи резервного копіювання можуть бути реалізовані у різних середовищах. Одним із найпоширеніших рішень є хмарні технології, що дозволяють зберігати дані на віддалених серверах, забезпечуючи їх доступність у будь-який час. Водночас багато компаній обирають локальні хмарні сховища, що дозволяють контролювати збереження даних без залежності від сторонніх провайдерів. Такі рішення забезпечують високу швидкість доступу, контроль над інформацією та можливість розширення системи відповідно до потреб організації [1, 3].

Автоматизовані системи включають шифрування інформації, контроль доступу, багаторівневий розподіл копій та механізми відновлення після збоїв, що дозволяє мінімізувати ризики втрати або компрометації даних, особливо у випадках кібератак або технічних несправностей. У різних галузях існують нормативні вимоги, що регламентують обробку та збереження інформації – дотримання таких стандартів є особливо важливим для компаній, які працюють із конфіденційними даними, включаючи фінансові, юридичні та медичні організації.

До ключових міжнародних стандартів захисту даних належать (див. рис. 1.1) [3]:

— загальний регламент захисту даних (GDPR);
— закон про перенесення та підзвітність медичного страхування (HIPAA);
— стандарт безпеки даних платіжних карток (PCI-DSS);
— ISO/IEC 27001.



Рисунок 1.1 – Контроль відповідності щодо зберігання інформації: GDPR, HIPAA, PCI-DSS

Основні переваги автоматизації. Автоматизація резервного копіювання забезпечує низку ключових переваг, які значно покращують ефективність, надійність та безпеку процесів управління даними. Перехід від ручного резервного копіювання, яке потребує постійного контролю та втручання, до автоматизованих рішень дає змогу усунути людський фактор, зменшити ризики втрати даних, а також оптимізувати робочі процеси, звільнивши час для виконання більш стратегічних завдань. Використання таких систем гарантує послідовність і надійність, підвищує ефективність, забезпечує захист даних, аварійне відновлення, відповідність нормативним вимогам і загальну інформаційну безпеку (див. рис. 1.2) [3].

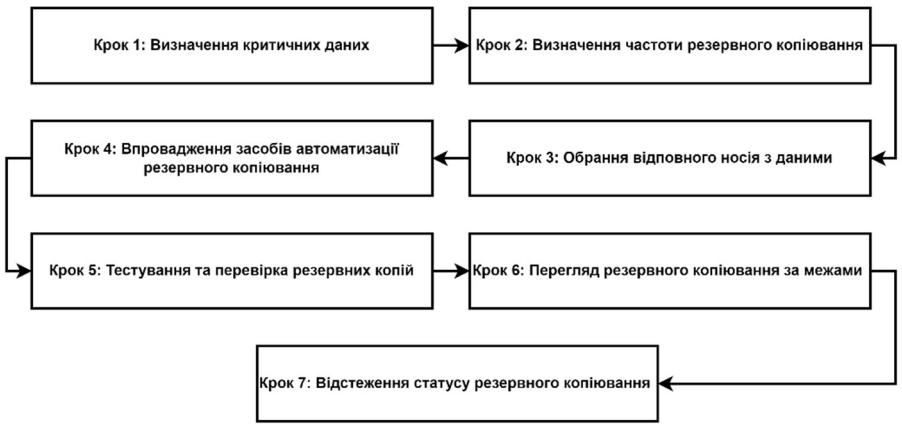


Рисунок 1.2 – Процес налагодження автоматизованого резервного копіювання

Однією з головних переваг автоматизованих систем резервного копіювання є їхня здатність забезпечувати стабільний і безперервний процес створення резервних копій без необхідності ручного втручання. У випадку ручного резервного копіювання завжди існує ризик помилки – можна забути зробити копію, зберегти її у неправильному місці або не включити всі необхідні файли. Автоматизація повністю усуває ці ризики, гарантуючи регулярне резервне копіювання за встановленим розкладом, що підтримує послідовну історію даних, до якої можна повернутися у будь-який момент. Крім того, системи автоматичного резервного копіювання зазвичай оснащені механізмами перевірки цілісності даних,

що дозволяє уникнути ситуацій, коли створені резервні копії виявляються пошкодженими або неповними (див. рис. 1.3) [3-4].

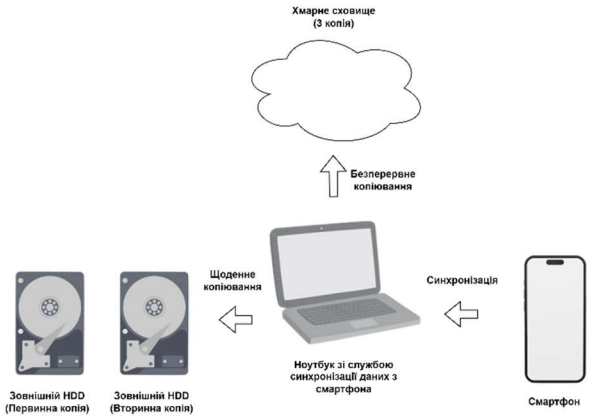


Рисунок 1.3 – Безперервне резервне копіювання зі інтегрованим механізмом перевірки цілосності даних

Надійність є ще одним критично важливим аспектом автоматизації, оскільки автоматизовані системи часто використовують розподілене зберігання та багаторівневу архітектуру, що дозволяє копіювати дані у кілька незалежних локацій, що запобігає їхній втраті у разі апаратного збою або інших форс-мажорних обставин. Багато сучасних рішень для резервного копіювання також включають перевірку даних на предмет коректності, використовуючи технології виправлення помилок, такі як ECC (Error-Correcting Code) (див. рис. 1.4), що особливо актуально для серверних систем, де навіть незначні пошкодження даних можуть призвести до серйозних проблем [5, 3-4].

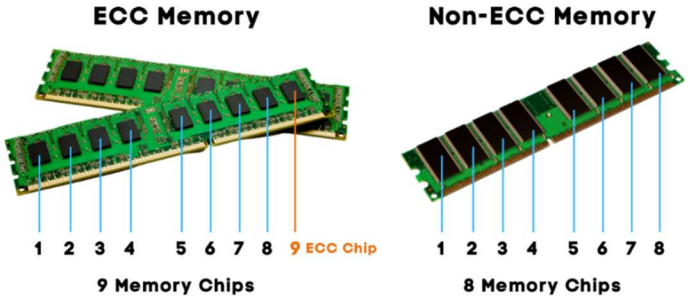


Рисунок 1.4 – Відмінність ECC та Non-ECC RAM: наявність додаткової мікросхеми у ECC RAM [5]

Ще одна вагома перевага автоматизації – це підвищення загальної ефективності роботи, оскільки зменшується навантаження на IT-персонал, що займається адмініструванням систем. Ручне резервне копіювання вимагає постійного моніторингу, а також значних ресурсів, що відволікає працівників від більш стратегічних завдань, пов’язаних з оптимізацією систем, підвищенням рівня безпеки та вдосконаленням бізнес-процесів. Автоматизовані системи резервного копіювання працюють у фоновому режимі, практично не впливаючи на продуктивність основних процесів, що особливо важливо у великих організаціях, де будь-які затримки можуть мати серйозні наслідки [3-4].

Окрім цього, багато сучасних рішень використовують інкрементне та диференціальне резервне копіювання, що дозволяє значно зменшити навантаження на систему. На відміну від повного резервного копіювання, яке дублює всю інформацію, ці методи копіюють лише нові або змінені файли, що дозволяє оптимізувати використання дискового простору, зменшити навантаження на процесор і мінімізувати використання пропускної здатності мережі. Завдяки цьому навіть під час активного резервного копіювання користувачі можуть продовжувати працювати без відчутного впливу на продуктивність системи, що є суттєвою перевагою для бізнесу (див. рис. 1.5) [6].

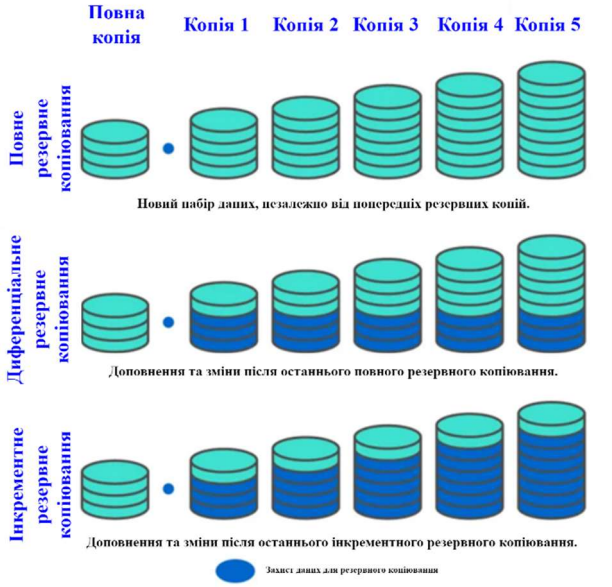


Рисунок 1.5 – Візуальне порівняння різних типів резервного копіювання

Автоматизація резервного копіювання забезпечує високий рівень захисту даних, оскільки втрата інформації може статися в будь-який момент і з різних причин. Людський фактор залишається однією з найбільш поширених причин втрати даних, коли працівник випадково видаляє важливу інформацію або неправильно копіює файли, що призводить до їх пошкодження. Також можливі збої під час передавання даних, що можуть спричинити втрату частини або навіть всієї інформації. Крім цього, загрозу можуть становити атаки зловмисного програмного забезпечення, збої в апаратному забезпеченні або зовнішні чинники, такі як стихійні лиха. Використання автоматизованих систем резервного копіювання дозволяє мінімізувати ці ризики, оскільки такі системи створюють додатковий рівень захисту, гарантують наявність безпечної копії даних та забезпечують можливість швидкого їх відновлення у будь-який момент (див. рис. 1.6) [3, 7].

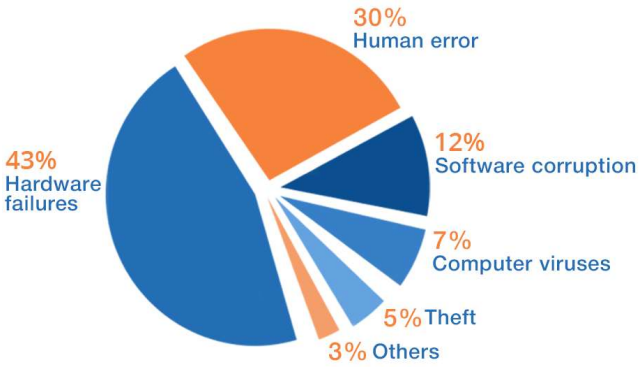


Рисунок 1.6 – Діаграма відповідності причин втрати даних [7]

Одна з найсерйозніших кіберзагроз сьогодення – програмне забезпечення-вимагач, яке може заблокувати доступ до даних або зашифрувати їх, вимагаючи викуп за розшифрування (див. рис. 1.7) [8]. Деякі види цього шкідливого програмного забезпечення навіть не здійснюють шифрування, а просто перешкоджають доступу до операційної системи, відображаючи банери з вимогами про сплату коштів. При цьому навіть після внесення викупу немає жодної гарантії, що доступ до даних буде відновлено. Автоматизовані системи резервного копіювання можуть значно зменшити вплив таких атак, оскільки вони зберігають

незмінні резервні копії, які захищені від несанкціонованих змін або видалень. У випадку атаки відновлення даних може бути здійснене без необхідності сплачувати викуп. До того ж, автоматизовані системи часто використовують шифрування даних, що робить їх захищеними навіть у разі компрометації сховища. Без спеціальних ключів розшифрування такі файли залишаються недоступними для зловмисників, що підвищує загальний рівень безпеки даних [8, 3-4].

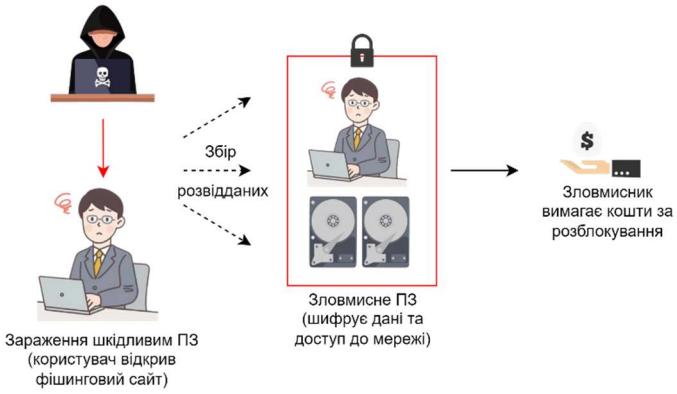


Рисунок 1.7 – Блокування традиційних незахищених систем шляхом проникнення зловмисного ПЗ

Ще однією важливою перевагою автоматизації є можливість аварійного відновлення даних. У разі значного збою, спричиненого апаратними проблемами, кібератаками або навіть стихійними лихами, швидке відновлення інформації стає критично важливим. Автоматизовані системи резервного копіювання дозволяють мінімізувати час простою та забезпечують ефективне відновлення інформації. Вони підтримують різні варіанти відновлення, включаючи повне відновлення системи, вибіркове відновлення окремих файлів або папок, а також відновлення даних на певний момент часу. Використовуючи історичні версії резервних копій, можна відновити лише необхідні файли без необхідності повного відновлення всієї системи, що значно економить ресурси. Деякі організації використовують географічно відокремлені резервні сховища, що захищає дані навіть у випадку локальних катастроф. Такий підхід, відомий як геонадмірність, гарантує можливість відновлення інформації навіть у найскладніших ситуаціях.



Рисунок 1.8 – Відновлення втрачених даних шляхом відновлення зі резервної копії

1.2 Принципи та застосування локального хмарного сховища

Локальні хмарні сховища забезпечують гнучкість загальнодоступних хмарних сервісів, одночасно надаючи повний контроль, безпеку та можливість гнучкого налаштування в межах власної інфраструктури. Одним із найпоширеніших рішень для цього є Nextcloud, який дозволяє організаціям та окремим користувачам розгортати приватне хмарне сховище на власних серверах (див. рис. 1.9) [9].

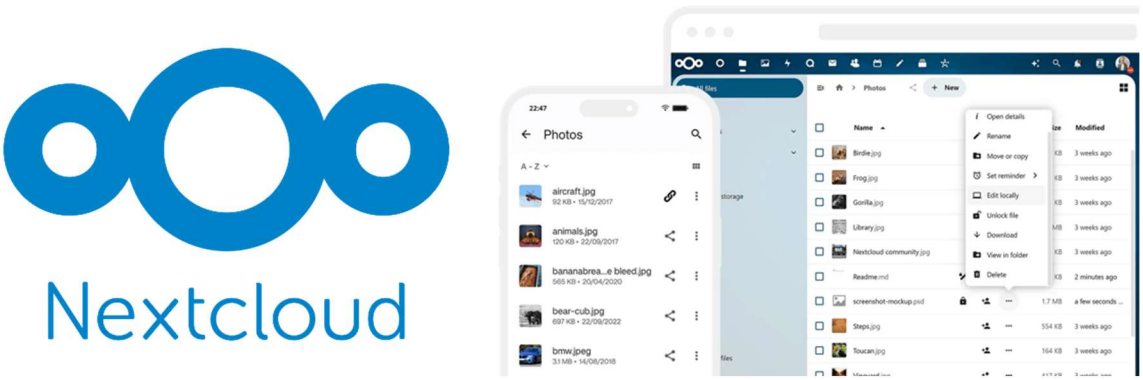


Рисунок 1.9 – Локальне хмарне сховище: Nextcloud

На відміну від традиційних методів зберігання файлів, Nextcloud пропонує централізоване керування даними, віддалений доступ з будь-якого пристрою та широку інтеграцію з іншими сервісами, що робить його значно більш гнучким рішенням у порівнянні з такими платформами, як Google Drive, Microsoft OneDrive чи Dropbox (див. рис. 1.10) [9].

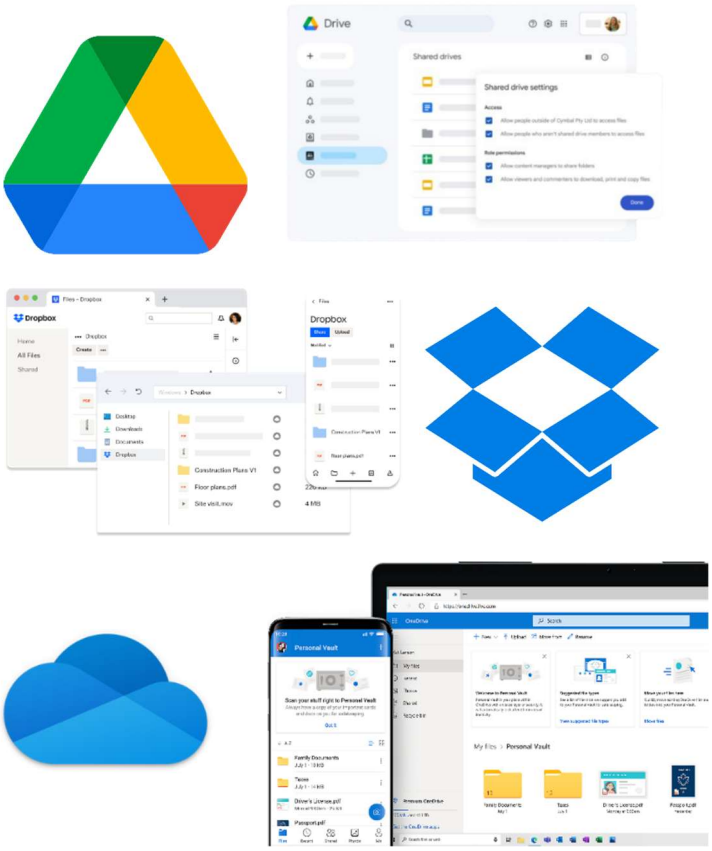


Рисунок 1.10 – Загальнодоступні хмарні сховища:
Google Drive, Dropbox, Microsoft OneDrive

Архітектура Nextcloud базується на моделі клієнт-сервер (див. рис. 1.11), де сервер розгортається на самокерованій інфраструктурі, наприклад, у домашній мережі, офісі чи центрі обробки даних, а клієнти взаємодіють із ним через настільні програми, мобільні пристрої або веб-інтерфейс. Така структура дозволяє зберігати, отримувати та синхронізувати файли з будь-якого пристрою без обмежень, які зазвичай накладають комерційні хмарні сервіси. Крім того, платформа підтримує багатокористувацьке середовище, що дає змогу співпрацювати над документами,

керувати доступом і правами користувачів, а також використовувати вбудовані механізми контролю версій, автоматичного резервного копіювання та наскрізного шифрування [9].

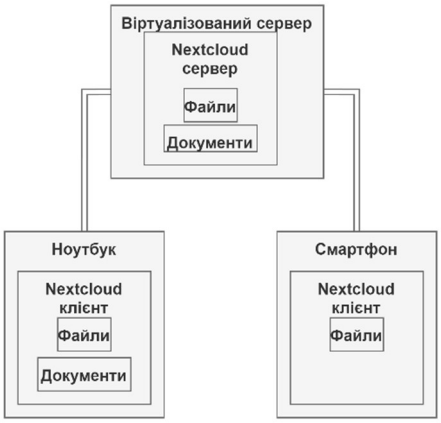


Рисунок 1.11 – Клієнт-серверна архітектура Nextcloud

Функціональність Nextcloud виходить за межі звичайного зберігання файлів завдяки інтеграції зі сторонніми застосунками. Наприклад, користувачі можуть увімкнути синхронізацію календарів, керування контактами, спільну роботу над документами через OnlyOffice або Collabora (див. рис. 1.12) [9-10].



Рисунок 1.12 – Рішення для роботи з документами з відкритим кодом: OnlyOffice та Collabora

Також проводити безпечні відеоконференції без залучення сторонніх сервісів (див. рис. 1.13). Такі можливості роблять Nextcloud потужною альтернативою загальнодоступним хмарним платформам, дозволяючи повністю контролювати свою інфраструктуру та уникати ризиків, пов'язаних із централізованими комерційними сховищами [9].

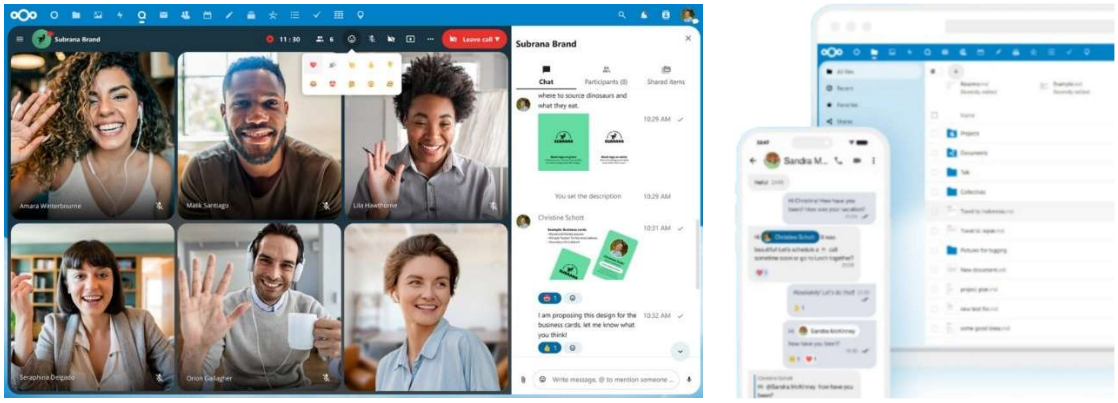


Рисунок 1.13 – Рішення для співпраці з відкритим кодом: Nextcloud Talk

Nextcloud у поєднанні з локальним серверним рішенням, таким як TrueNAS Scale, дозволяє створити високонадійну систему зберігання з підтримкою ZFS, дедуплікації та знімків даних, що забезпечує додатковий рівень безпеки та гнучкості (див. рис. 1.14). Використання таких платформ значно зменшує витрати, оскільки відсутні постійні платежі за ліцензування, а можливість масштабування не обмежується тарифними планами постачальників хмарних послуг [9, 11].

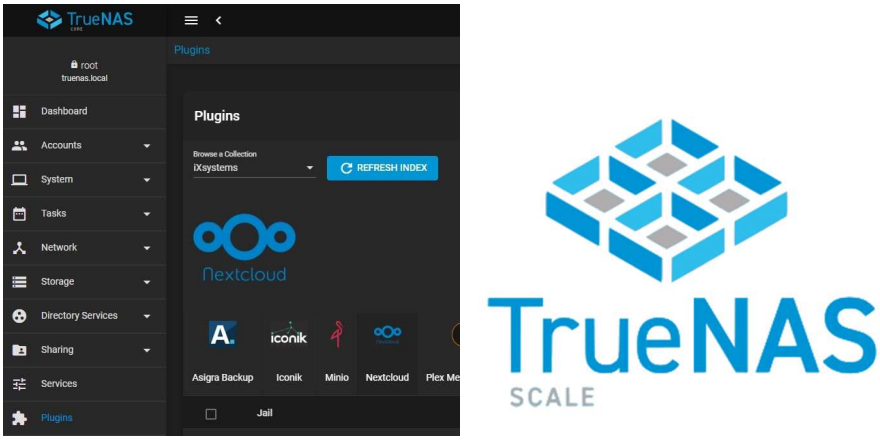


Рисунок 1.14 – Розміщення Nextcloud на локальному сервері TrueNAS Scale [11]

Локальне хмарне сховище проти загальнодоступних хмарних служб. Загальнодоступні хмарні служби, такі як Google Drive, Dropbox або OneDrive, забезпечують зручність і масштабованість, але мають значні компроміси щодо контролю над даними, конфіденційності та гнучкості (див. табл. 1.1) [12].

Таблиця 1.1 – Порівняння локального хмарного сховища із загальнодоступними хмарними рішеннями [12]

Особливість	**Загальнодоступні хмарні служби (Google Drive, Dropbox, OneDrive)**	**Локальне хмарне сховище (Nextcloud, автономні рішення)**
Контроль даних	Дані зберігаються на сторонніх серверах відповідно до політики постачальника	Повний контроль над політикою розміщення та зберігання даних.
Безпека та конфіденційність	Заходи шифрування та безпеки залежать від постачальника	Настроювані параметри безпеки, включаючи наскрізне шифрування
Гнучкість	Обмежена настройка; користувачі покладаються на попередньо встановлені функції	Можливість налаштування за допомогою плагінів та інтеграції
Відповідність	Норми щодо даних (GDPR, HIPAA) залежать від постачальника та регіону	Полегшене дотримання місцевих і галузевих правил
Витрати	На основі підписки; масштаб витрат із потребами зберігання	Одноразова вартість інфраструктури; менші довгострокові витрати

Якщо порівнювати локальне хмарне сховище, наприклад, Nextcloud, із публічними хмарами, можна виділити кілька ключових переваг. Публічні хмарні сервіси зберігають дані на сторонніх серверах відповідно до політики постачальника, що означає, що користувач не має повного контролю над розміщенням і безпекою своїх файлів. Локальне ж хмарне сховище, розгорнуте на власному сервері, надає можливість самостійно керувати всіма аспектами зберігання, включаючи налаштування безпеки, резервне копіювання та контроль доступу [9, 12].

Безпека та конфіденційність також залежать від постачальника у випадку загальнодоступних сервісів, тоді як Nextcloud дозволяє реалізувати наскрізне шифрування, керування доступом за ролями та двофакторну автентифікацію, що значно підвищує рівень захисту даних. Гнучкість публічних хмар обмежена, адже користувач змушений працювати з попередньо встановленими функціями та не має можливості значних модифікацій, тоді як локальне рішення дає можливість інтеграції з іншими інструментами, розширення за допомогою плагінів і повної кастомізації відповідно до власних потреб. Наприклад, Nextcloud підтримує інтеграцію з OnlyOffice, Collabora, системами управління завданнями, шифруванням та інструментами для відеоконференцій, що перетворює його на повноцінну платформу для співпраці [9-10, 12].

Відповідність вимогам регулювання також є важливим фактором. Загальнодоступні хмарні сервіси можуть змінювати політику обробки даних залежно від регіону або рішення компанії-постачальника, тоді як локальне хмарне сховище дозволяє гнучко підлаштовуватися під GDPR, HIPAA або інші галузеві стандарти, уникаючи ризиків, пов’язаних зі змінами умов обслуговування. Витрати на публічні хмарні сервіси базуються на підписці, що означає, що зі збільшенням обсягу зберігання зростає і вартість, а у випадку локального хмарного сховища є лише початкові витрати на інфраструктуру, після чого загальні витрати суттєво нижчі в довгостроковій перспективі [2-3, 9, 12].

Для підприємств, що працюють із конфіденційними даними, зокрема в охороні здоров'я, фінансах та державному секторі, рішення на базі Nextcloud та самохостингу є більш безпечною та відповідною альтернативою публічним хмарам. Повний контроль над даними усуває ризики несанкціонованого доступу, аналізу інформації постачальниками або втрати через зміну політики сервісу. Крім того, відсутність регулярної підписки робить таку модель економічно вигідною. Політики використання публічних хмар змінюються регулярно, що може призвести до непередбачуваних обмежень чи додаткових витрат, тоді як автономна модель локального хмарного сховища гарантує стабільність і передбачуваність роботи без залежності від сторонніх компаній. Наприклад, Google Drive або OneDrive можуть

змінювати умови зберігання, обмежуючи безкоштовний простір або змінюючи функціональність сервісу, що змушує користувачів пристосовуватися до нових умов або переходити на дорожчі підписки [9, 12].

Самохостинг на базі Nextcloud (див. рис. 1.15) дозволяє самостійно встановлювати та змінювати політики використання відповідно до власних потреб, що особливо важливо для організацій, які мають суворі вимоги до обробки даних. Гнучкість локального сховища відкриває можливості для повної кастомізації та інтеграції з іншими інструментами, зберігаючи при цьому всі права на дані без ризику їхнього аналізу чи використання третіми сторонами, що робить локальні хмарні рішення на базі відкритого коду надійнішою та довготривалою альтернативою загальнодоступним хмарним платформам, дозволяючи зменшити залежність від сторонніх компаній та мінімізувати витрати [9, 11].

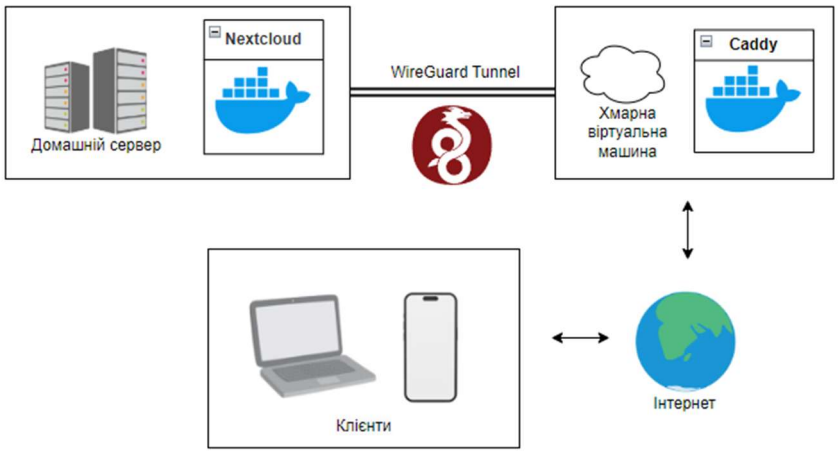


Рисунок 1.15 – Самохостинг Nextcloud зі використанням віртуалізації, контейнерезації та VPN-тунелювання

Доступ до локального хмарного сховища – WebDAV, API та інші механізми. Ключова перевага сучасних локальних хмарних рішень зберігання, таких як Nextcloud, полягає в підтримці множинних механізмів доступу, що забезпечує інтеграцію з різними платформами та програмами. Використання WebDAV (Web-based Distributed Authoring and Versioning) як широко розповсюдженого протоколу дозволяє монтувати Nextcloud як мережевий диск, надаючи прямий доступ до

файлів без необхідності відкривати веб-браузер (див. рис. 1.16). Таке рішення забезпечує плавну синхронізацію даних між локальними пристроями та хмарним сховищем, що робить його зручним інструментом для роботи з файлами в реальному часі без обмежень, характерних для багатьох публічних хмарних сервісів [9, 13].

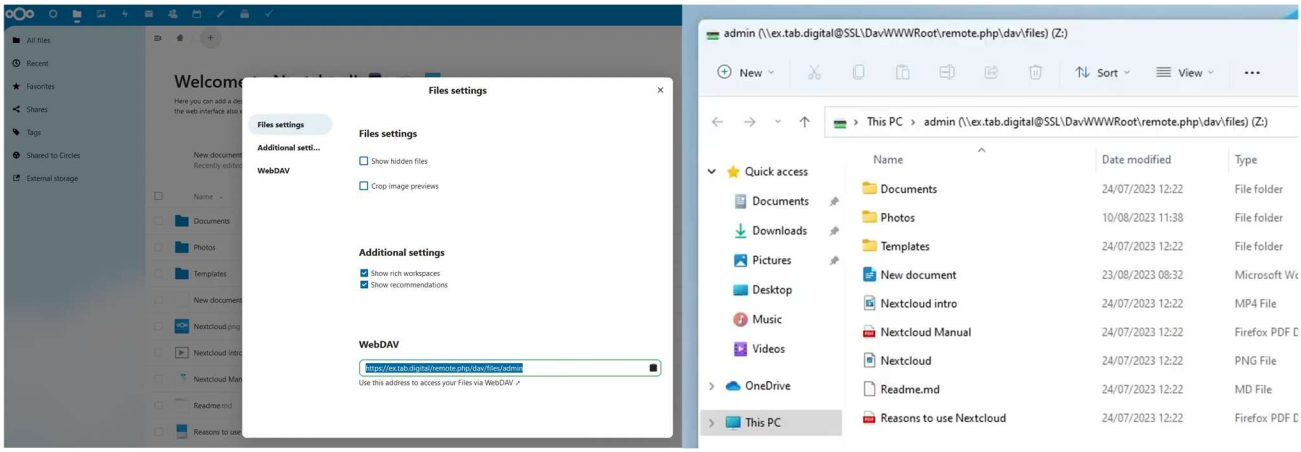


Рисунок 1.16 – Монтування локального сховища Nextcloud як мережевого диска: WebDAV

Окрім WebDAV, використання RESTful API у Nextcloud відкриває широкі можливості для автоматизації та інтеграції з іншими системами. Завдяки REST API, розробники можуть інтегрувати функціонал хмарного сховища у власні програми, автоматизувати завдання, створювати кастомізовані робочі процеси та розширювати можливості платформи відповідно до своїх потреб (див. рис. 1.17).

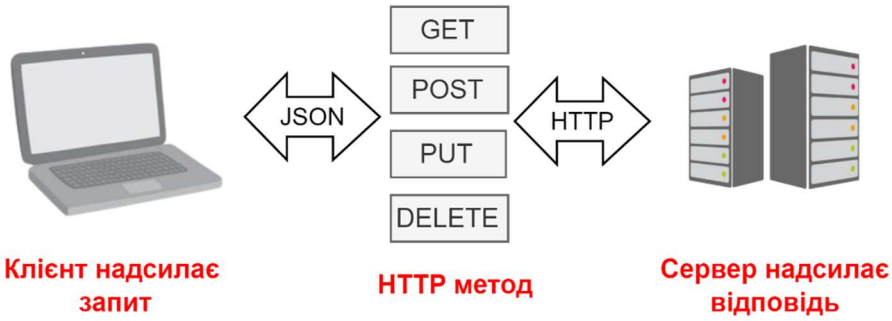


Рисунок 1.17 – Принцип роботи REST API у взаємодії між клієнтом та сервером у інтеграції власних ПЗ зі Nextcloud

Підтримка API дозволяє налаштовувати взаємодію між різними сервісами без необхідності прямого втручання у структуру Nextcloud, що робить його зручним для використання як у корпоративному середовищі, так і в особистому хостингу [9, 14].

Настільні та мобільні додатки для Windows, macOS, Linux, Android та iOS (див. рис. 1.18) забезпечують безперебійну синхронізацію файлів на всіх пристроях, дозволяючи користувачам отримувати доступ до даних у будь-якому місці. Використання локального хмарного сховища у такому форматі дозволяє не тільки централізовано керувати файлами, а й розширювати можливості співпраці.

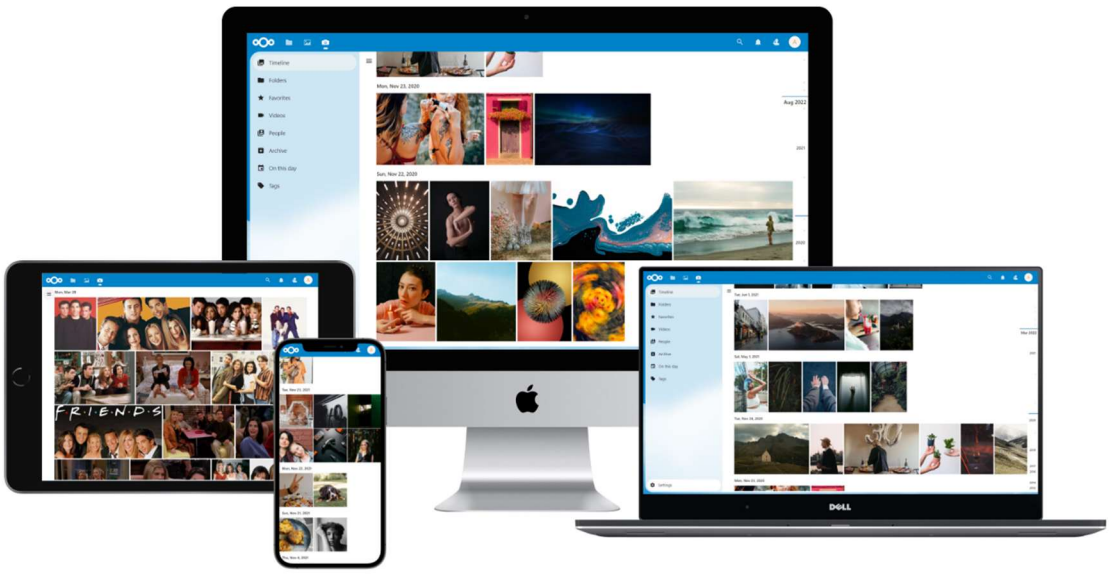


Рисунок 1.18 – Мультиплатформленість ПЗ Nextcloud:
Windows, Linux, macOS, Android, iOS

Функція Federated Cloud Sharing (див. рис. 1.19), що реалізована у Nextcloud, дозволяє об’єднувати кілька екземплярів хмари в єдину систему, уможливлюючи безпечний обмін файлами між різними організаціями або відокремленими інфраструктурними елементами без необхідності використовувати сторонні загальнодоступні сервіси [15, 9].

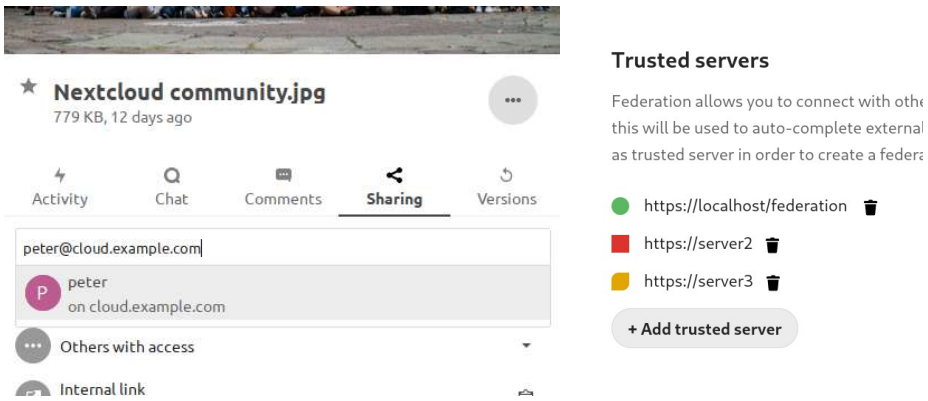


Рисунок 1.19 – Консолідація декількох екземплярів Nextcloud: функція Federated Cloud Sharing

Завдяки цьому Nextcloud може функціонувати як високодоступне, масштабоване та безпечне хмарне сховище, яке повністю відповідає вимогам як індивідуальних користувачів, так і підприємств. Поєднання повного контролю над даними, розширених можливостей безпеки, кастомізації, інтеграції та значної економії витрат у довгостроковій перспективі робить локальне хмарне сховище не просто альтернативою публічним хмарним сервісам, а значно ефективнішим та адаптивнішим рішенням для сучасних потреб цифрового середовища [9-15].

1.3 Важливість автоматизації резервного копіювання

Важливість автоматизації також полягає у швидкості відновлення даних. У випадку втрати або пошкодження інформації можна швидко повернути її у працездатний стан, що критично для багатьох галузей, таких як фінанси, медицина чи державний сектор. Усі ці фактори роблять автоматизацію резервного копіювання не просто зручною опцією, а необхідністю для безперебійного функціонування сучасних інформаційних систем [1-4].

Мінімізація ризиків втрати даних. Зазвичай втрата даних може призвести до серйозних наслідків для компанії, включаючи фінансові втрати, репутаційні

збитки, правові наслідки та збої в роботі системи, що впливає на процеси всередині організації [3-4, 7].

Причини цього можуть бути різними [7]:

— людський фактор;

— апаратні збої;

— пошкодження програмного забезпечення;

— кіберзагрози;

— стихійні лиха.

Одним із ключових способів зменшення ризику втрати даних є захист від випадкового видалення, що є найпоширенішою причиною втрати інформації через людський фактор. Співробітники можуть ненавмисно видалити важливі файли або не зберегти зміни, що призводить до незворотних наслідків у разі відсутності резервної копії. Автоматизована система резервного копіювання забезпечує постійне створення додаткових копій, що дозволяє відновити попередні версії файлів у разі помилки, що особливо важливо для корпоративних середовищ, де робота з великими обсягами інформації є критичною. Використання керування версіями дозволяє зберігати декілька станів одного документа, що дає змогу повернутися до будь-якої попередньої версії (див. рис. 1.20), які широко застосовуються у публічних хмарних сервісах, таких як Google Drive, Amazon S3 та Microsoft OneDrive, однак вони мають обмеження, тоді як локальні автоматизовані рішення резервного копіювання можуть працювати з будь-якими типами файлів та інфраструктурою [3-4, 7].

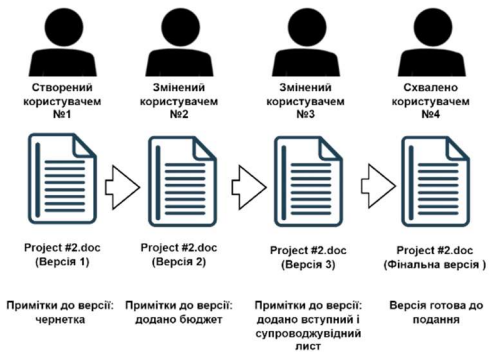


Рисунок 1.20 – Контроль версій на рівні документів: відкат до попередньої версії

Ще одним важливим способом мінімізації втрат є захист від апаратних збоїв. Втрата даних може відбуватися не лише через програмні помилки, але й через несправність обладнання – навіть найнадійніші накопичувачі, включаючи жорсткі диски (HDD), твердотільні накопичувачі (SSD) та RAID-масиви, мають обмежений термін служби та можуть вийти з ладу в будь-який момент, що призведе до потенційної втрати важливої інформації. Автоматизовані системи резервного копіювання створюють додатковий рівень безпеки, дозволяючи зберігати надлишкові копії даних у кількох місцях. Наприклад, використання RAID-масивів дає можливість підвищити відмовостійкість за рахунок збереження дубльованої інформації, що дозволяє відновити дані навіть у разі виходу з ладу одного з дисків (див. рис. 1.21) [3-4, 16].

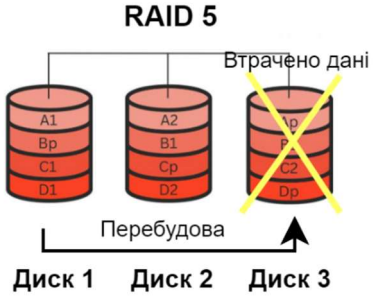


Рисунок 1.21 – Масив дисків у RAID 5: відновлення у разі втрати 1 диска

Окрім цього, загальноприйнятим підходом у резервному копіюванні є стратегія «3-2-1» (див. рис. 1.22), яка передбачає наявність трьох копій даних на двох різних носіях, одна з яких зберігається у віддаленому місці [3-4, 7].



Рисунок 1.22 – Стратегія надійного резервного копіювання 3-2-1

Автоматизована система резервного копіювання також може включати механізми моніторингу обладнання в реальному часі та сповіщення про можливі проблеми, що дозволяє вчасно вжити заходів та запобігти несподіваним збоям. Крім того, підтримка механізмів аварійного відновлення забезпечує швидке перемикання на резервні копії у разі виходу з ладу дисків або інших критичних компонентів системи [1-4, 6].

Оптимізація ресурсів і часу. У міру зростання обсягів даних керування ними стає дедалі важчим, а ризик втрати або некоректного копіювання збільшується.

Автоматизація резервного копіювання значно підвищує ефективність за рахунок [1-4]:

— зменшення ручного втручання;

— оптимізації продуктивності системи;

— звільнення IT-персоналу.

Традиційні методи резервного копіювання потребують значних витрат часу з боку IT-персоналу, адже вони передбачають ручне планування, ініціювання, контроль доступного місця для зберігання, видалення застарілих копій, перевірку цілісності та усунення помилок. Цей підхід не лише створює додаткове навантаження, а й підвищує ймовірність людських помилок, що може призвести до втрати критично важливої інформації. Впровадження автоматизованих систем резервного копіювання дозволяє усунути ці проблеми, зменшивши потребу в ручному втручанні та забезпечивши точність, регулярність і послідовність процесу Дані зберігаються за попередньо визначеним графіком, що усуває ризик пропущених копій через людський фактор (див. рис. 1.23) [2-3].

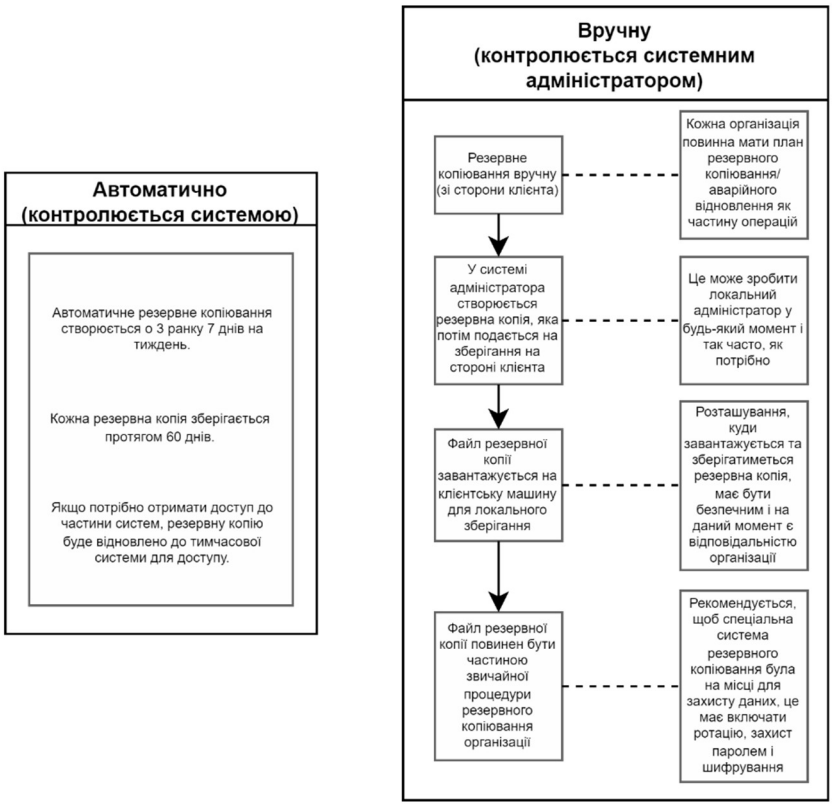


Рисунок 1.23 – Відмінність методів резервного копіювання:
ручне (ініціюється вручну) та автоматичне (за графіком)

Цим, автоматизація сприяє оптимізації продуктивності та зменшенню навантаження на систему – операції, що ініціюються резервним копіюванням, можуть споживати значні обчислювальні ресурси, особливо коли йдеться про великі обсяги даних. Якщо процес резервного копіювання запланований без урахування пікових навантажень, це може негативно вплинути на швидкодію критичних бізнес-додатків, уповільнити доступ до інформації та створити дискомфорт для користувачів. Автоматизовані системи дозволяють планувати виконання резервних копій у позаробочий час, що мінімізує вплив на продуктивність системи та не порушує бізнес-процеси, ба більше, використовуючи інкрементне або диференціальне над повним резервним копіюванням буде лише знижувати навантаження на ресурси, оскільки замість створення повних копій зберігаються лише змінені файли, що значно економить дисковий простір, зменшує використання обчислювальних потужностей і прискорює процес відновлення даних у разі потреби [2-3, 6].

1.4 Виклики автоматизації резервного копіювання в локальному хмарному сховищі

Автоматизація резервного копіювання в локальному хмарному сховищі відкриває широкі можливості для підвищення ефективності, але разом із тим створює унікальні проблеми, які необхідно вирішувати для забезпечення масштабованості, безпеки, відповідності нормативним вимогам та бездоганної інтеграції з наявною IT-інфраструктурою. На відміну від традиційних хмарних рішень, локальне хмарне сховище потребує більш детального контролю, оскільки організація бере на себе відповідальність за управління апаратними ресурсами, захист даних та підтримку взаємодії систем, що вимагає вирішення низки критичних проблем, які можна умовно розділити на три основні категорії [1-4]:

— масштабованість;
— обмеження сховища;
— забезпечення безпеки та відповідності даних;
— інтеграція з існуючою інфраструктурою.

Обмеження ємності зберігання та масштабованість. Одна з найбільших проблем у локальному хмарному сховищі – це забезпечення обробки зростаючих обсягів даних, зберігаючи при цьому економічну ефективність. На відміну від публічних хмарних сховищ, які можуть масштабуватися за вимогою, локальні рішення вимагають розширення фізичного обладнання, що створює додаткові виклики. Відповідальність за інфраструктуру та її розширення лежить безпосередньо на організації, що змушує враховувати як технічні, так і фінансові аспекти. Одним із критичних моментів є необхідність динамічного розширення сховища без переривання поточних операцій, що можливо завдяки впровадженню спеціалізованих рішень (див. рис. 1.24) [2-3].



Рисунок 1.24 – Труднощі у зберіганні та керуванні даними:
хмарне, мережеве та зовнішнє сховища

Масштабовані архітектури сховищ, такі як використання NAS або SAN, дозволяють розширювати обсяги сховища за потреби. Також ефективним підходом є гібридні рішення, які комбінують локальне та хмарне сховище, переміщуючи старі та менш важливі дані до зовнішніх хмарних ресурсів. Автоматизоване зберігання на рівнях також допомагає в оптимізації, оскільки дозволяє класифікувати дані на основі віку та частоти доступу, розміщуючи рідше використовувані файли у менш продуктивних, але більш містких сховищах. Важливим фактором залишається завчасне планування масштабованості, щоб уникнути необхідності дорогого оновлення інфраструктури, коли сховище досягне критичного рівня заповнення [3-4].

Забезпечення безпеки та відповідності даних. Будь-яке резервне копіювання повинно гарантувати захист інформації від несанкціонованого доступу, втрати або компрометації. Локальне хмарне сховище має певні переваги з точки зору контролю над даними, але також вимагає впровадження додаткових механізмів безпеки, таких як шифрування, управління доступом та аудит подій. Впровадження наскрізного шифрування даних допомагає запобігти витокам інформації навіть у разі фізичного доступу до носіїв. Однак ефективне шифрування потребує значних обчислювальних ресурсів, що може впливати на швидкість роботи системи, особливо якщо йдеться про великі сховища даних. Також важливим аспектом є відповідність нормативним вимогам, таким як GDPR, HIPAA або PCI-DSS, залежно від типу збережених даних. Виконання цих стандартів вимагає впровадження політик збереження, управління логами доступу та періодичного аудиту безпеки. У

деяких випадках доводиться створювати окремі ізольовані середовища для збереження конфіденційної інформації, що ускладнює загальну архітектуру системи (див. рис. 1.25) [1-4, 6].



Рисунок 1.25 – Труднощі у забезпеченні безпеки та відповідності: підвищення складний незахищений невпорядкований доступ та легкий захищений упорядкований доступ

Інтеграція з існуючою інфраструктурою. Будь-яке резервне копіювання повинно працювати у тісному взаємозв'язку з базами даних, корпоративними програмами, мережевими ресурсами та іншими критичними компонентами системи. У традиційних хмарних рішеннях інтеграція часто виконується через API або спеціалізовані сервіси, тоді як у локальному середовищі доводиться адаптувати систему під конкретні програмні рішення, що може спричиняти труднощі з підтримкою сумісності. Наприклад, деякі корпоративні додатки можуть не підтримувати нативні механізми резервного копіювання, що змушує впроваджувати додаткові скрипти та кастомізовані рішення для автоматизації процесу. Також проблеми можуть виникати при роботі з мережевими ресурсами, оскільки резервні копії можуть створювати додаткове навантаження на інфраструктуру, впливаючи на продуктивність інших систем. Для мінімізації таких ризиків необхідно використовувати спеціалізовані інструменти для балансування

навантаження, а також планувати резервне копіювання у періоди найменшої активності системи (див. рис. 1.26) [2-3, 11-12, 14].



Рисунок 1.26 – Труднощі у інтеграції у існуючу інфраструктуру: розгалдужнена Cloud-based та локальна інфраструктура

Віртуалізовані середовища, такі як VMware (віртуалізація), Docker (контейнерезація) чи Kubernetes (оркестрація контейнерів), вимагають додаткових механізмів для створення резервних копій та відновлення контейнерів або віртуальних машин у разі збою. Інструменти резервного копіювання повинні мати можливість інтегруватися з такими платформами, щоб забезпечувати швидке відновлення та мінімізувати час простою (див. рис. 1.27) [4, 14].

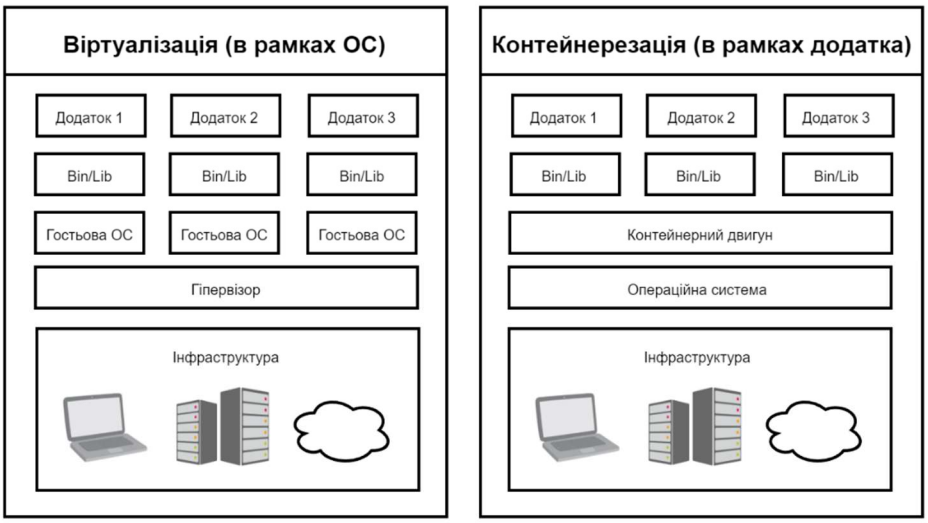


Рисунок 1.27 – Покращення використання існуючої інфраструктури: віртуалізація та контейнерезація

РОЗДІЛ 2 ПРОЄКТУВАННЯ СИСТЕМ АВТОМАТИЗАЦІЇ РЕЗЕРВНОГО КОПІЮВАННЯ

2.1 Технології та інструменти для автоматизації резервного копіювання

Автоматизація резервного копіювання базується на правильному поєднанні програмних рішень, інструментів синхронізації, механізмів безпеки та систем моніторингу. Побудова такої системи для хмарного сховища потребує оцінки різних технологій з урахуванням їхньої функціональності, простоти адміністрування, масштабованості та рівня захисту даних. Важливо враховувати не лише можливості Nextcloud, а й альтернативні рішення, такі як Syncthing, OwnCloud, Seafile та Pydio, щоб порівняти їхню ефективність у синхронізації даних, автоматизації резервного копіювання та безпеці.

Порівняння Nextcloud та альтернативних рішень. Кожна локальна хмарна система, яка використовується для самостійного зберігання даних, має унікальні особливості, що впливають на стратегію резервного копіювання. Деякі рішення орієнтовані переважно на синхронізацію файлів, інші забезпечують централізоване хмарне сховище з можливостями спільної роботи, а деякі поєднують обидва підходи. Серед найбільш популярних платформ, які можна розгорнути у власній інфраструктурі, варто розглянути п’ять рішень, що забезпечують високий рівень контролю та гнучкість налаштувань.

Nextcloud є автономним хмарним сховищем із відкритим кодом, яке підтримує синхронізацію файлів, спільний доступ та функції для колективної роботи. Резервне копіювання реалізується за допомогою WebDAV, BorgBackup та інших вбудованих механізмів керування версіями. Серед основних можливостей – підтримка інкрементного резервного копіювання, контроль версій та автоматичні знімки даних. Функції безпеки включають наскрізне шифрування, двофакторну аутентифікацію, контроль доступу та аудит подій. За рівнем масштабованості

підходить для малих і середніх підприємств, а також домашнього використання. Адміністрування здійснюється через веб-інтерфейс із широкими можливостями налаштувань, а оптимальний сценарій використання – організації, яким потрібна безпечна, гнучка та приватна хмара з інтеграцією у внутрішню IT-інфраструктуру (див. рис. 2.1) [2-3, 9, 12-15].

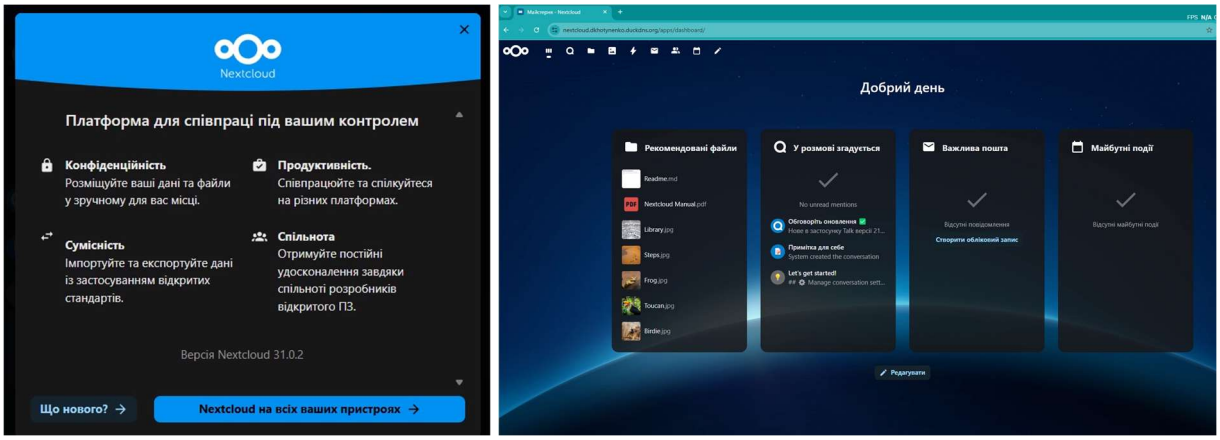


Рисунок 2.1 – Інтерфейс клієнт-серверного ПЗ Nextcloud

Syncthing пропонує однорангову синхронізацію файлів, що відрізняється від класичних систем резервного копіювання. Його можливості щодо збереження даних обмежені, оскільки він покладається на безперервну синхронізацію, а не на збереження резервних копій за розкладом. Захист реалізовано через шифрування TLS, контроль доступу та аутентифікацію, однак відсутня вбудована система керування версіями. За масштабованістю підходить для окремих користувачів та невеликих команд, але не забезпечує корпоративні функції. Адміністрування здійснюється через простий веб-інтерфейс, а основна сфера використання – користувачі, яким потрібна миттєва синхронізація файлів без використання централізованого сервера (див. рис. 2.2) [2-3, 17].

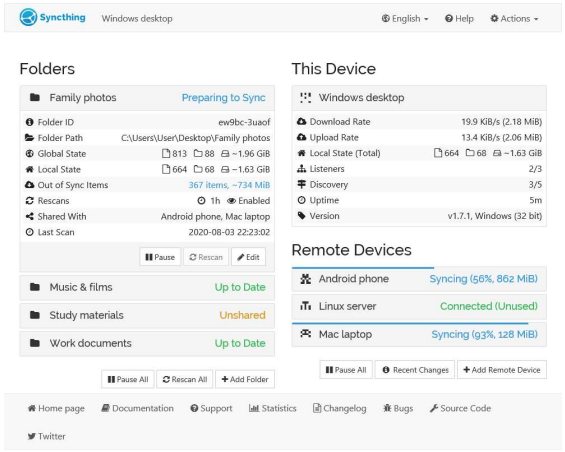


Рисунок 2.2 – Інтерфейс однорангової синхронізації файлів ПЗ Syncthing

OwnCloud є прямим конкурентом Nextcloud, пропонуючи аналогічні можливості зберігання, синхронізації та спільного використання файлів. Водночас йому бракує деяких розширених функцій безпеки та засобів колективної роботи. Резервне копіювання реалізується через WebDAV, а також шляхом експорту бази даних. Безпека забезпечується шифруванням, контролем доступу та двофакторною аутентифікацією, проте деякі функції доступні лише у платній версії. За масштабованістю підходить для малих і середніх підприємств, а адміністрування здійснюється через веб-інтерфейс, що має менше безкоштовних можливостей порівняно з Nextcloud. Використовується переважно організаціями, яким потрібне стабільне хмарне сховище без додаткових інструментів для спільної роботи (див. рис. 2.3) [2-3, 18].

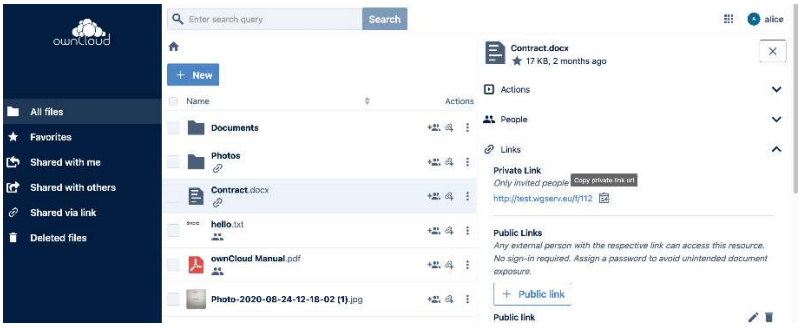


Рисунок 2.3 – Інтерфейс клієнт-серверного ПЗ OwnCloud

Seafile орієнтований на високу продуктивність і швидкість синхронізації даних, відрізняючись від Nextcloud обмеженим набором функцій для співпраці. Резервне копіювання реалізується через автоматичне керування версіями та дедуплікацію, що підвищує ефективність використання дискового простору. Захист включає наскрізне шифрування бібліотек файлів та контроль доступу. За масштабованістю підходить для малих і середніх підприємств, яким потрібна висока продуктивність при синхронізації даних. Адміністрування здійснюється через веб-інтерфейс із мінімальним використанням ресурсів, а основна сфера застосування – компанії, які цінують швидкість обміну файлами та вбудоване керування версіями (див.рис. 2.4) [2-3, 19].

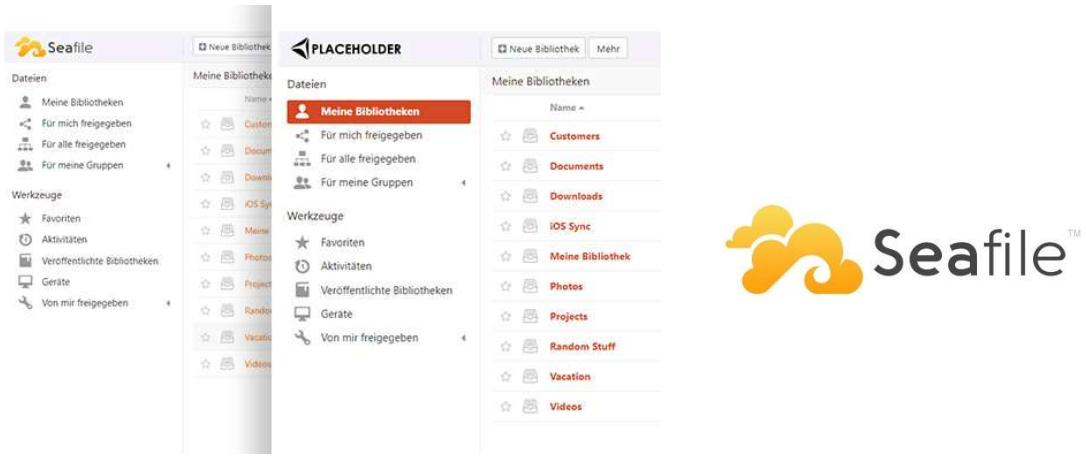


Рисунок 2.4 – Інтерфейс клієнт-серверного ПЗ Seafile

Pydio є корпоративною хмарною платформою, орієнтованою на безпеку та відповідність нормативним вимогам. На відміну від інших рішень, потребує більше ресурсів для роботи, проте забезпечує суворий контроль даних. Серед можливостей резервного копіювання – автоматичне збереження даних, хмарна синхронізація та управління життєвим циклом файлів. Захист включає відповідність GDPR, HIPAA та іншим стандартам безпеки, а за масштабованістю орієнтований на великі підприємства з жорсткими вимогами до безпеки. Адміністрування здійснюється через розширену адміністративну панель, а оптимальне використання – у корпоративних середовищах, де необхідне дотримання суворих стандартів захисту даних (див. рис. 2.5) [2-3, 20].

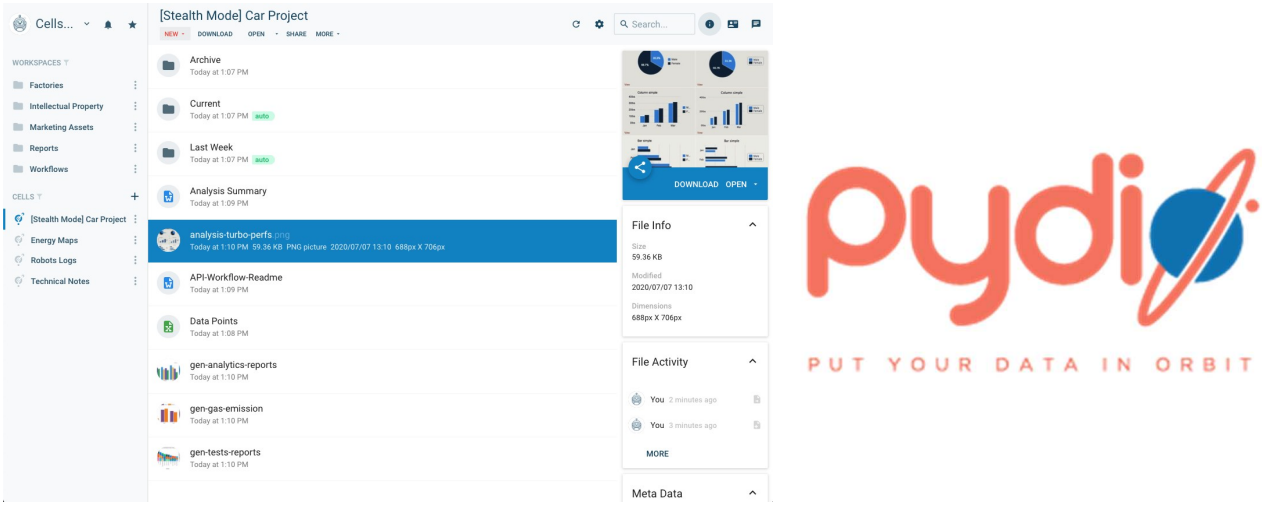


Рисунок 2.5 – Інтерфейс клієнт-серверного ПЗ Pydio

Вибір правильного рішення для резервного копіювання. Якщо розглядати, які переваги надаються у різних сценаріях, то для домашніх користувачів і малого бізнесу Nextcloud або OwnCloud пропонують більш зручний у використанні інтерфейс із вбудованим механізмом резервного копіювання та керування версіями, що робить їх зручними для невеликих інфраструктур [2-3, 9, 18].

Якщо пріоритетом є синхронізація файлів у реальному часі, Syncthing виступає легшим та більш оптимізованим рішенням, оскільки він спеціалізується саме на безперервному обміні файлами між пристроями без складних механізмів збереження попередніх версій. Для підприємств, які мають жорсткі вимоги до відповідності стандартам безпеки, Pydio може забезпечити кращий захист та контроль даних порівняно з іншими варіантами, завдяки розширеним можливостям керування доступом, аудитом подій та відповідності регуляторним нормам [2-3, 17, 20].

Якщо необхідна висока швидкість синхронізації разом із підтримкою дедуплікації, Seafile забезпечує ефективніше використання ресурсів і мінімізує дублювання файлів, що особливо корисно при роботі з великими обсягами даних. Проте, якщо розглядати універсальне рішення, яке може задовольнити більшість потреб, Nextcloud залишається найбільш гнучкою платформою завдяки широкому набору функцій, можливостям автоматизації резервного копіювання та потужним інструментам безпеки [2-3, 9, 19].

2.2 Основні компоненти автоматизованого резервного копіювання

Автоматизоване резервне копіювання у локальних хмарних системах зберігання, зокрема у Nextcloud, вимагає добре структурованого підходу до організації даних, їх обробки, моніторингу та безпеки. Поєднання цих аспектів дозволяє створити гнучку архітектуру, яка підтримує різні методи резервного копіювання, забезпечуючи цілісність інформації та швидке відновлення у разі збою. Nextcloud не лише зберігає файли користувачів, а й має можливості для автоматизації процесів резервного копіювання, управління версіями файлів, відновлення даних і забезпечення високого рівня безпеки. Ці особливості формують основу ефективної системи резервного копіювання, яку варто розглянути детальніше.

Структура файлів Nextcloud і методи доступу до файлів. Організація файлової системи Nextcloud базується на структурованих каталогах, у яких файли та папки кожного користувача зберігаються у визначеній директорії сервера. За замовчуванням шлях зберігання даних розташований у каталозі "/var/www/html/nextcloud/data/", де містяться підкаталоги користувачів, а також спільні файли та метадані щодо доступу (див. рис. 2.6).

```
dkhotynenko@nextcloud:~$ sudo ls -la /var/www/html/nextcloud/data
[sudo] password for dkhotynenko:
total 32
drwxrwx---  4 www-data www-data 4096 Apr  2 21:06 .
drwxr-xr-x 16 www-data www-data 4096 Apr  2 21:03 ..
drwxr-xr-x 11 www-data www-data 4096 Apr  2 21:12 appdata_oc82osujeodw
drwxr-xr-x  3 www-data www-data 4096 Apr  2 21:05 dkhotynenko
-rw-r--r--  1 www-data www-data  542 Apr  2 21:05 .htaccess
-rw-r--r--  1 www-data www-data    0 Apr  2 21:05 index.html
-rw-r--r--  1 www-data www-data   52 Apr  2 21:05 .ncdata
-rw-r-----  1 www-data www-data 6652 Apr  2 21:09 nextcloud.log
dkhotynenko@nextcloud:~$
```

Рисунок 2.6 – Структура домашньої директорії
локального хмарного сховища Nextcloud

Дозволи та інформація про файли зберігаються у базі даних, яка може бути MySQL, MariaDB або PostgreSQL, залежно від конфігурації під час встановлення.

Для забезпечення безперешкодного доступу до даних Nextcloud підтримує кілька механізмів взаємодії з файлами, що дозволяє адаптувати систему під різні потреби користувачів і забезпечити гнучке резервне копіювання (див. рис. 2.7).



Рисунок 2.7 – Бази даних, що працюють з Nextcloud:
MySQL, MariaDB або PostgreSQL

Основними методами доступу є веб-інтерфейс, який дозволяє користувачам завантажувати, переглядати та керувати файлами через браузер, WebDAV-протокол, що забезпечує можливість монтування Nextcloud як мережевого диска та прямий доступ до файлів на Windows, macOS та Linux без необхідності відкриття браузера, а також клієнти синхронізації для настільних і мобільних пристроїв, які автоматично оновлюють файли між локальним пристроєм та хмарним сховищем (див. рис. 2.8). Додатково використовується REST API, що забезпечує програмний доступ для інтеграції Nextcloud із зовнішніми додатками та автоматизації процесів резервного копіювання.

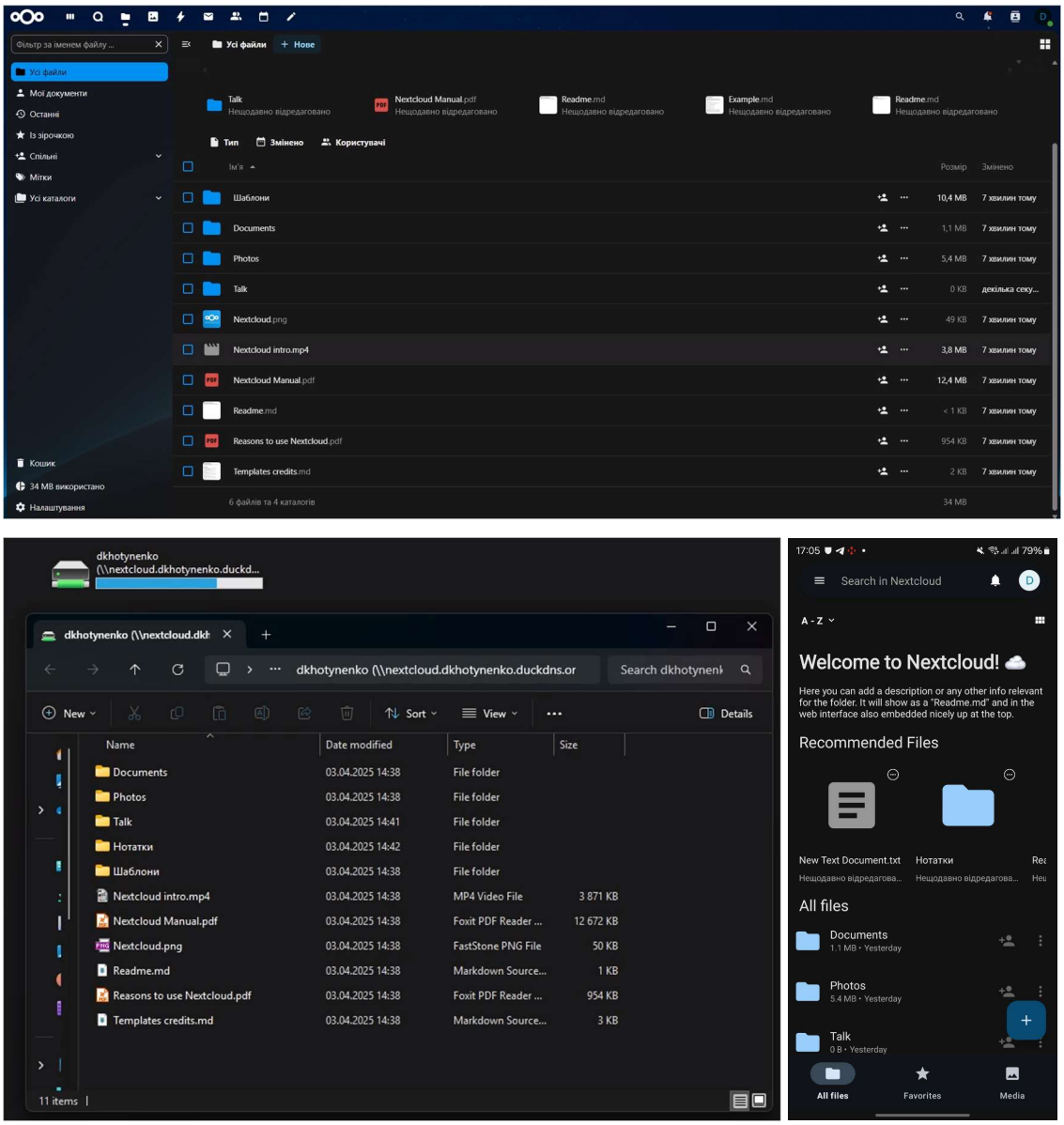


Рисунок 2.8 – Взаємодія з даними ПЗ Nextcloud:
веб-інтерфейс, мережевий диск, мобільний додаток

Важливим аспектом побудови ефективної системи резервного копіювання є розуміння того, що Nextcloud зберігає не лише файли, а й метадані, що містять дозволи, версії документів та спільні посилання. Тому резервні копії мають включати не тільки каталоги файлів, а й бази даних, у яких зберігається вся критично важлива інформація. Використання правильних механізмів доступу, а також реалізація автоматизованого резервного копіювання для файлів та баз даних дозволяє знизити ризики втрати даних і забезпечити високу надійність роботи локального хмарного сховища (див. рис. 2.9).

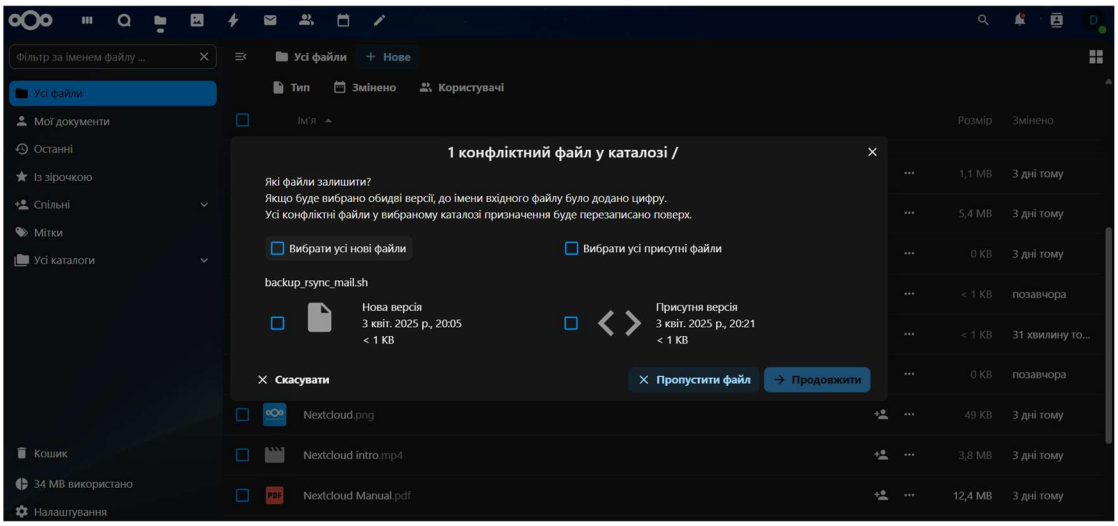


Рисунок 2.9 – Взаємодія з даними ПЗ Nextcloud:
надання спільного доступу та контроль версій

Автоматизація резервного копіювання у хмарній інфраструктурі Nextcloud дозволяє забезпечити стабільне збереження даних без необхідності постійного ручного втручання. Для цього використовуються різні інструменти та механізми планування, що дозволяють виконувати регулярне, поступове та інкрементальне резервне копіювання залежно від вимог конкретної системи. Вибір конкретного методу залежить від масштабів сховища, частоти оновлення файлів, доступних ресурсів і необхідності гнучкого відновлення даних у разі збою [1-4].

Інструменти автоматизації резервного копіювання – WebDAV для віддалених резервних копій. Одним із найпростіших способів автоматизованого доступу та резервного копіювання є WebDAV – протокол, який дозволяє монтувати Nextcloud як мережевий диск та здійснювати копіювання даних безпосередньо через файлову систему. Використовуючи WebDAV, можна організувати синхронізацію на клієнтських пристроях та налаштувати регулярне резервне копіювання через скрипти, що працюють у фоновому режимі. Завдяки підтримці WebDAV у більшості операційних систем та інструментів автоматизації цей метод є зручним для інтеграції з існуючими рішеннями резервного копіювання.

Перший сценарій рішення для резервного копіювання передбачає використання WebDAV для створення віддалених резервних копій, що дозволяє зберігати дані на зовнішньому сервері або іншому місці зберігання. Такий метод

особливо корисний у випадках, коли необхідно мати резервні копії в іншій фізичній локації для захисту від локальних збоїв або втрати даних. WebDAV добре інтегрується з автоматизованими сценаріями, що дозволяє налаштовувати заплановану синхронізацію без постійного ручного втручання (див. рис. 2.10) [3, 13, 21].

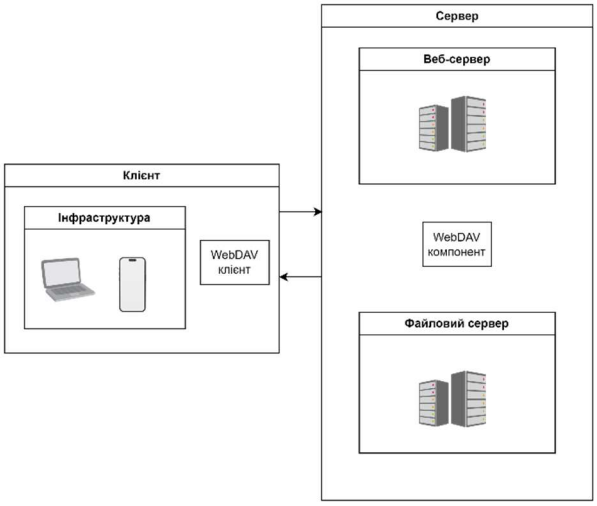


Рисунок 2.10 – Взаємодія з даними ПЗ Nextcloud:
принцип роботи протоколу WebDAV

Інструменти автоматизації резервного копіювання – rsync для локального та мережевого резервного копіювання. Для більш гнучкого та ефективного резервного копіювання часто використовується rsync – утиліта, що дозволяє створювати синхронізовані копії даних між локальним сервером та віддаленим сховищем. Вона підтримує інкрементальні оновлення, що означає копіювання лише змінених файлів, що значно зменшує навантаження на дисковий простір і ресурси сервера. Rsync дозволяє зберігати дані у їхньому оригінальному вигляді без додаткового архівування, що спрощує процес відновлення у разі втрати інформації. Rsync підтримує інкрементальне копіювання, тобто передає тільки змінені дані, що значно зменшує навантаження на мережу та дисковий простір. Цей інструмент використовується для локального або мережевого резервного копіювання, дозволяючи синхронізувати дані між сервером Nextcloud і зовнішнім сховищем (див. рис. 2.11) [3, 6, 22].

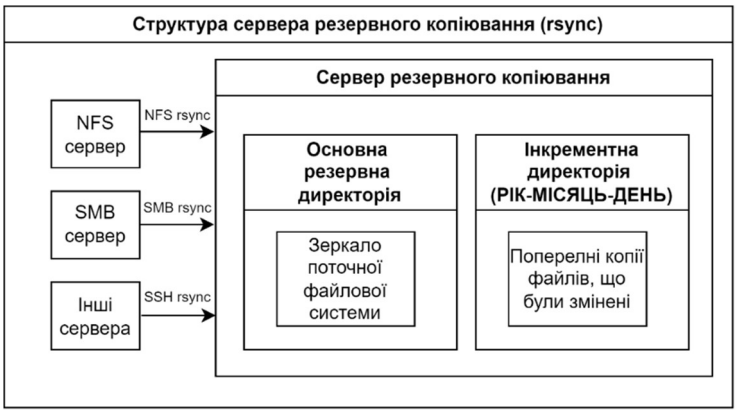


Рисунок 2.11 – Взаємодія з даними ПЗ Nextcloud:
принцип роботи rsync

Інструменти автоматизації резервного копіювання – BorgBackup для дедуплікованих, зашифрованих резервних копій. BorgBackup є одним із передових інструментів, що забезпечує дедуплікацію та шифрування, роблячи процес резервного копіювання більш безпечним і водночас ефективним у використанні дискового простору. Такий метод дозволяє значно зменшити обсяг резервних копій за рахунок збереження лише унікальних змінених блоків даних, що особливо корисно при великих обсягах інформації. Додатковий рівень безпеки забезпечується можливістю шифрування, що захищає резервні копії від несанкціонованого доступу (див. рис. 2.12) [3, 6, 23].

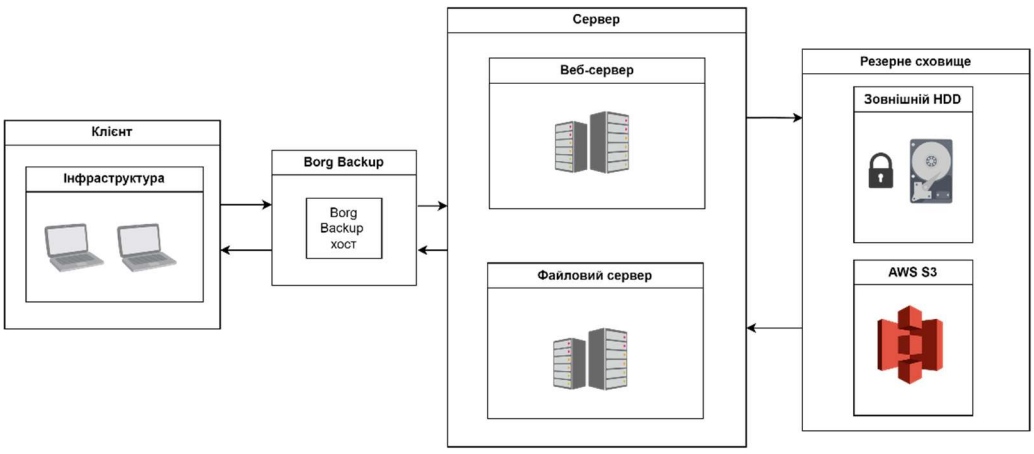


Рисунок 2.12 – Взаємодія з даними ПЗ Nextcloud:
принцип роботи BorgBackup

Інструменти автоматизації резервного копіювання – Cron Jobs для автоматизованого планування. Ще одним важливим механізмом автоматизації резервного копіювання є використання Cron Jobs, які дозволяють планувати резервне копіювання через заздалегідь визначені проміжки часу. Автоматизація цього процесу забезпечує стабільне та регулярне створення резервних копій без необхідності ручного втручання, що мінімізує ризик втрати даних у разі збою системи. Cron у Linux працює аналогічно Task Scheduler у Windows, дозволяючи виконувати завдання у визначений час або з певною періодичністю (див. рис. 2.13). [3, 24]

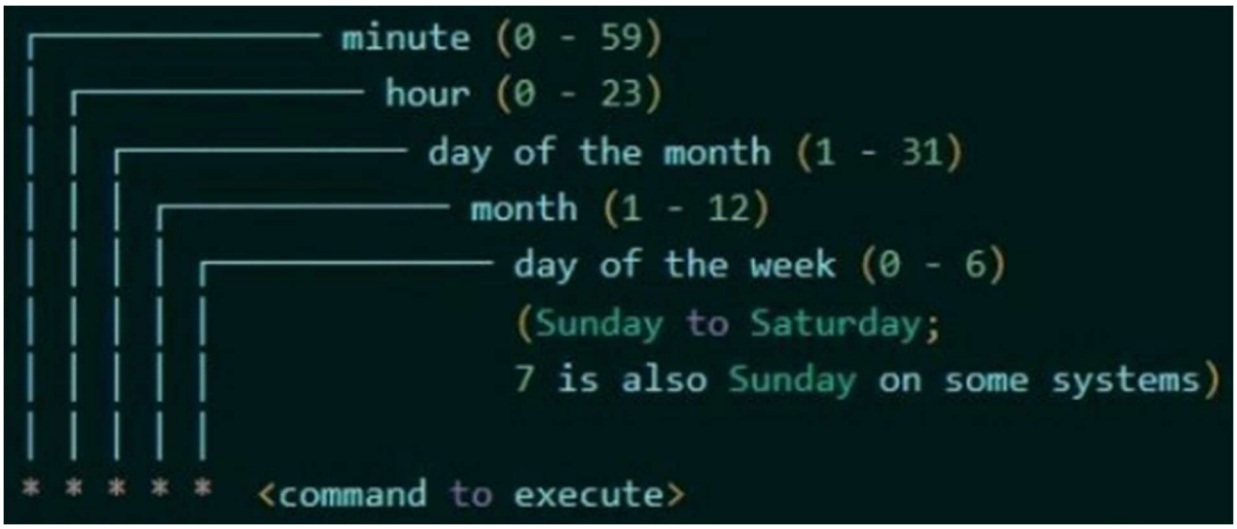


Рисунок 2.13 – Взаємодія з даними ПЗ Nextcloud:
принцип та можливості Cron Jobs

Використовуючи BorgBackup у поєднанні з Cron, можна реалізувати автоматичне резервне копіювання за розкладом, забезпечуючи постійну актуальність збережених даних [3, 23-24].

Використання Cron спрощує адміністрування резервних копій, оскільки можна налаштувати різні сценарії виконання – щоденне копіювання змінених файлів через rsync, створення архівів із BorgBackup раз на тиждень або навіть використання WebDAV для синхронізації даних між серверами кілька разів на день [3, 21-24] (див. рис. 2.14).

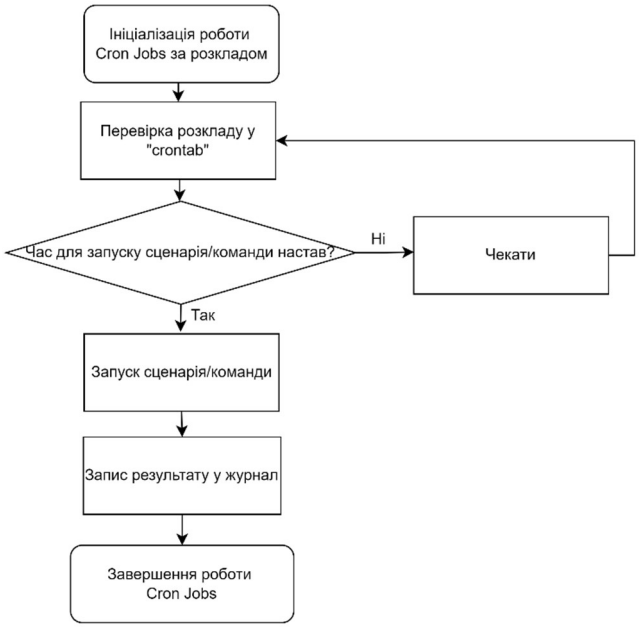


Рисунок 2.14 – Метод автоматизованого виконання сценаріїв резервного копіювання через Cron Job

У поєднанні зі всіма існуючими інструментами для резервного копіювання, було спроєктовано послідовну схему процесу автоматизованого резервного копіювання з використанням Cron, rsync, BorgBackup та WebDAV у середовищі Nextcloud (див. рис. 2.15).

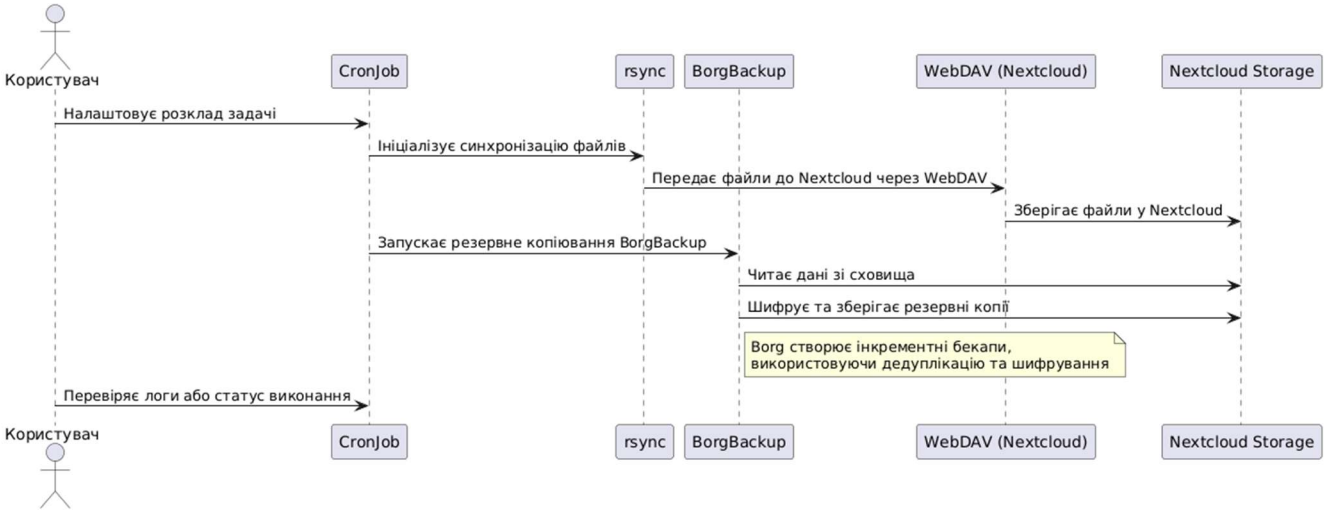


Рисунок 2.15 – Алгоритм автоматизованого резервного копіювання з використанням Cron, rsync, BorgBackup та WebDAV у локальне хмарне сховище Nextcloud

2.3 Стратегії оптимізації автоматизованої системи резервного копіювання

Визначившись із конкретним рішенням локального хмарного сховища, таким як Nextcloud, можна відразу помітити, що хоча він і має певну варіативність у створенні резервних копій завдяки контролю версій, синхронізації та базовим механізмам резервного копіювання, все ж потребує додаткової оптимізації для досягнення повної автоматизації. Використання Nextcloud як самостійної платформи локального хмарного сховища може бути ефективним, але для реалізації автоматизованої системи резервного копіювання часто розглядається комплексний підхід із використанням спеціалізованих платформ, таких як TrueNAS SCALE, яке є готовим рішенням із вбудованою підтримкою Nextcloud у вигляді плагіна (див. рис. 2.16) [1-4, 9, 11, 25].

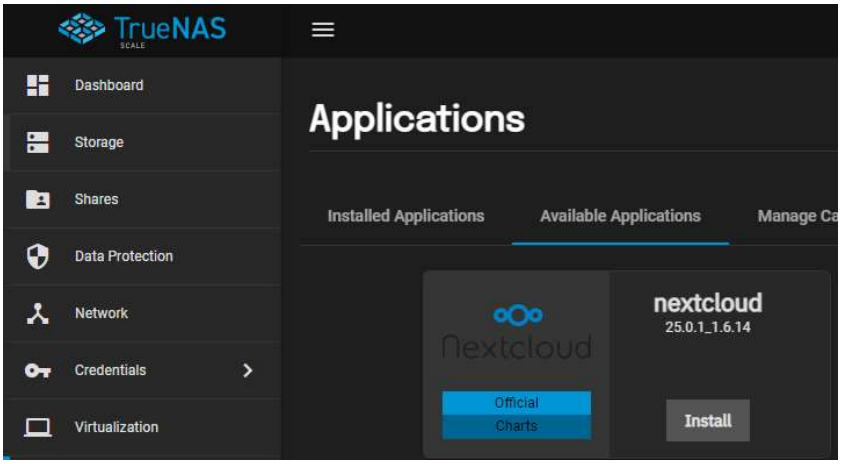


Рисунок 2.16 – Платформа для мережевого сховища TrueNAS: підтримка встановлення Nextcloud у якості додатка

Втім, замість використання сторонніх платформ можна піти іншим шляхом і реалізувати власні стратегії оптимізації, які дозволять Nextcloud виконувати функції повноцінної автоматизованої системи резервного копіювання. Впровадження дедуплікації, наскрізного шифрування, балансування навантаження та розподіленого зберігання значно підвищить ефективність локального хмарного

сховища та створить незалежну, добре налаштовану систему резервного копіювання, що дозволить використовувати гнучкість операційної системи Linux у поєднанні з веб-інтерфейсом Nextcloud для зручного керування та адміністрування.

Зменшення надлишкових копій файлів – дедуплікація даних. Дедуплікація даних як процес зменшення надлишкових копій файлів є важливим аспектом оптимізації сховищ, особливо в середовищі Nextcloud, який за замовчуванням орієнтований на версіювання, створюючи окремі копії файлів при кожній зміні. Усунення повторюваних копій дозволяє значно скоротити витрати на зберігання та оптимізувати використання ресурсів, замість багаторазового збереження однакових файлів система аналізує вміст, знаходить ідентичні блоки даних і зберігає лише унікальні екземпляри, що дозволяє суттєво зменшити споживання дискового простору та підвищити загальну ефективність резервного копіювання.

Оскільки Nextcloud за замовчуванням не має вбудованої підтримки дедуплікації, для її реалізації можна використовувати зовнішні рішення, такі як файлова система ZFS або Btrfs, які підтримують дедуплікацію на рівні блоків, BorgBackup, що виконує дедуплікацію на основі фрагментів даних, або rsync із жорсткими посиланнями, що дозволяє створювати додаткові резервні копії без фізичного дублювання файлів. Використання цих методів вже розглядалося в попередніх розділах, зокрема у контексті їх впровадження через команди Linux, що дозволяє налаштовувати дедуплікацію навіть без вбудованої підтримки в самому Nextcloud (див. рис. 2.17) [1-4, 6, 9, 11, 22-23].



Рисунок 2.17 – Доступні механізми для реалізації дедуплікації у середовищі Linux

Серед основних переваг дедуплікації можна виділити зменшення витрат на зберігання шляхом мінімізації зайнятого простору завдяки усуненню ідентичних файлів, що особливо важливо для резервного копіювання великих обсягів даних. Скорочення обсягу інформації, яку потрібно обробляти під час створення резервних копій, також оптимізує продуктивність цього процесу, зменшуючи навантаження на систему, прискорюючи операції резервного копіювання та відновлення, оскільки менша кількість унікальних даних значно зменшує час, необхідний для їхнього збереження та подальшого відновлення (див. рис. 2.18) [1-4, 6, 11].

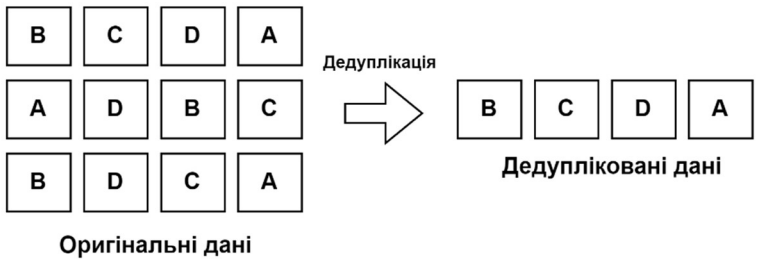


Рисунок 2.18 – Принцип роботи дедуплікації:
мінімізація даних через усунення ідентичних даних

Наскрізне шифрування та шифрування на стороні сервера – резервне шифрування. Шифрування відіграє важливу роль у захисті резервних копій файлів від несанкціонованого доступу, кібератак або фізичної крадіжки, і Nextcloud підтримує два основні підходи до його реалізації, на відміну від дедуплікації, яка вбудовано не передбачена. Один із цих методів — наскрізне шифрування, що передбачає шифрування файлів ще до їхнього виходу з клієнтського пристрою, забезпечуючи доступ до них лише для користувача, який володіє відповідним ключем, тобто фактично гарантує, що навіть сервер не матиме можливості переглядати їхній вміст. Інший підхід — шифрування на стороні сервера, коли файли зберігаються у відкритому вигляді під час передачі, а потім уже зашифровуються на сервері, що дозволяє керувати ключами централізовано (див. рис. 2.19) [2-3, 26].

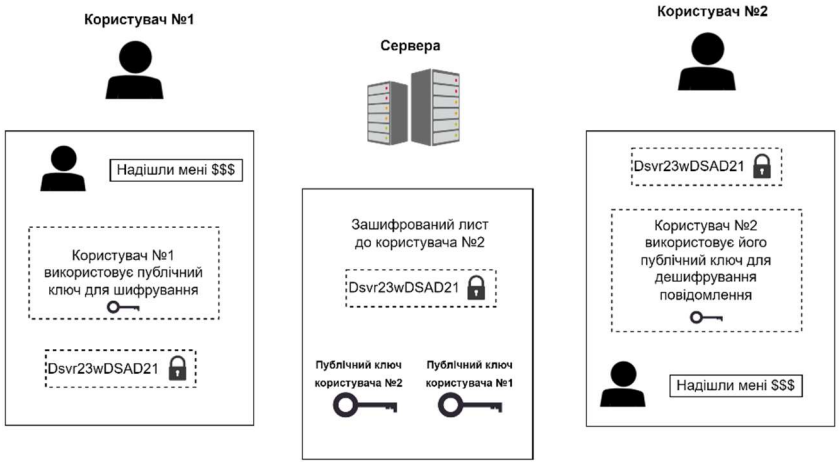


Рисунок 2.19 – Принцип роботи шифрування:
доступ до зашифрованих даних можна отримати, лише маючи ключ

Для наскрізного шифрування у Nextcloud реалізовано підтримку E2E Encryption через офіційні клієнти, однак перед використанням цього механізму необхідно активувати шифрування для конкретних папок вручну. Якщо ж мова йде про шифрування на стороні сервера, то тут використовується алгоритм AES-256, який є ефективним для захисту резервних копій, що зберігаються на зовнішніх носіях, таких як Amazon S3, NFS або CIFS. Додатково можна застосовувати шифрування GPG для додаткового захисту при збереженні резервних копій поза межами Nextcloud, що забезпечить ще вищий рівень безпеки (див. рис. 2.20) [26].



Рисунок 2.20 – Принцип роботи шифрування:
наскрізне шифрування AES-256

Захист резервних копій завдяки шифруванню не тільки запобігає несанкціонованому доступу до файлів, навіть у разі компрометації сховища, а й допомагає дотримуватися нормативних вимог щодо безпеки даних, таких як GDPR, HIPAA та інших міжнародних стандартів. Окрім цього, використання шифрування додає додатковий рівень безпеки при інтеграції Nextcloud із зовнішніми постачальниками хмарного зберігання, що дозволяє уникнути ситуацій, коли дані можуть опинитися в руках третіх осіб без належного захисту. У зв'язку з цим, шифрування варто розглядати не лише як частину резервного копіювання, а і як комплексний засіб захисту файлів на всіх етапах їхнього зберігання, передачі та відновлення [1, 3, 7, 9, 12, 15, 26].

Балансування навантаження та оптимізація роботи з великими обсягами даних. Nextcloud, як і будь-яке інше хмарне сховище, може стикатися з проблемами продуктивності при роботі з великими обсягами даних, особливо коли йдеться про резервне копіювання великих файлів або значної кількості дрібних об'єктів. У таких випадках можуть виникати затримки в роботі системи, повільне збереження файлів, підвищене навантаження на процесор і оперативну пам'ять сервера, а також перевантаження мережі через передачу значних обсягів резервних копій [2-3, 6].

Для вирішення цих проблем необхідно правильно балансувати навантаження, зокрема шляхом використання інкрементного або диференціального резервного копіювання замість створення повних копій щоразу, що дозволить зменшити обсяг передаваних і збережених даних, адже інкрементне копіювання зберігає лише зміни з моменту останнього резервного знімка, а диференційне — накопичує зміни з останнього повного копіювання, забезпечуючи баланс між швидкістю та ефективністю відновлення [3, 6].

Ще один метод оптимізації — розбиття великих файлів на частини, що нагадує підхід, який використовувався у старих файлообмінниках, коли файли архівували та ділили на менші сегменти для зручного завантаження. У випадку Nextcloud це реалізується за рахунок використання сховища файлів на основі фрагментів, що дозволяє завантажувати великі об'єкти невеликими блоками,

покращуючи швидкість передачі та зменшуючи використання пам’яті та процесорних ресурсів сервера [3, 6, 9, 23].

Додатково можна застосовувати автоматизоване планування резервного копіювання через Cron Jobs, що дозволяє уникнути перевантаження системи, виконуючи копіювання у непікові години, коли користувачі не працюють із даними, що також дає можливість розділяти завдання за частотою: для дрібних файлів резервне копіювання може відбуватися частіше, тоді як повне резервне копіювання виконуватиметься рідше, наприклад, раз на тиждень або за потреби [3, 6, 24].

Масштабування Nextcloud для великих розгортань – розподілене сховище. Розподілене сховище дозволяє Nextcloud масштабуватися на кількох серверах або інтегруватися із зовнішніми рішеннями для зберігання, що покращує резервування, надмірність, продуктивність та доступність. Одним із методів розподіленого сховища є створення кластера Nextcloud, що передбачає розгортання високої доступності, коли використовується два або більше серверів Nextcloud, підключених до спільного внутрішнього сховища, наприклад Ceph або Cluster FS. Такий підхід забезпечує захист від збоїв і запобігає простою навіть у разі виходу з ладу одного з серверів, а також балансування запитів користувачів між різними вузлами, що не дає перенавантажуватися окремим вузлам системи.

Крім створення кластера, можливий також варіант федерації Nextcloud, що дозволяє кільком незалежним екземплярам легко обмінюватися даними між собою, що є корисним для великих організацій, яким необхідні окремі кластери зберігання для різних відділів або регіональних підрозділів. Такий підхід покращує географічну надмірність і дозволяє розподіляти дані між різними локаціями, що відповідає стратегії 3-2-1, де передбачається зберігання трьох копій даних на двох різних носіях з однією резервною копією поза основним місцем розташування [3-4, 7, 9].

Nextcloud також підтримує інтеграцію з S3-сумісними сховищами, що працюють за принципом REST API і дозволяють підключати зовнішні рішення для зберігання, такі як Amazon S3, Wasabi, MinIO та інші подібні сервіси. Використання

S3 надає переваги у вигляді практично необмеженої масштабованості, що особливо важливо для великих обсягів резервного копіювання, а також автоматичного резервування та високої доступності. Крім цього, інтеграція з S3 дозволяє економічно вигідно організувати холодне зберігання даних для архівування, що є критично важливим для компаній, яким необхідно зберігати історичні дані, але без активного доступу до них (див. рис. 2.21) [9, 14].

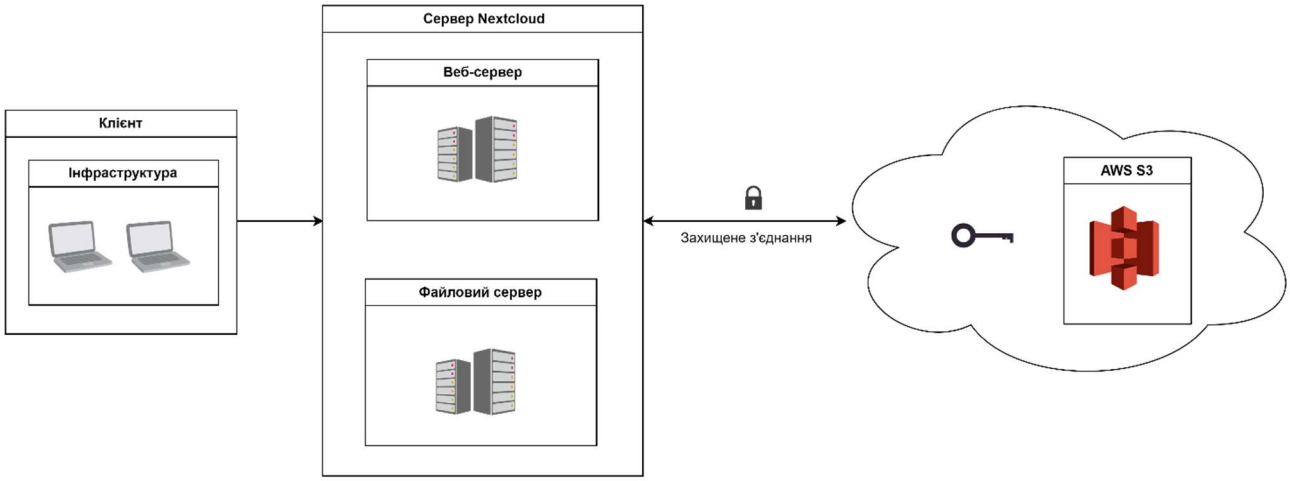


Рисунок 2.21 – Топологія розподіленого хмарного сховища Nextcloud на основі AWS S3

2.4 Розгортання локального хмарного сховища у віртуальному середовищі

Додаткові переваги розподіленого сховища включають високу доступність резервних копій, що запобігає втраті даних завдяки їхньому розміщенню у кількох місцях, а також зменшення затримок завдяки збереженню резервних копій ближче до кінцевих користувачів, що забезпечує не лише ефективний розподіл навантаження, а й значне покращення загальної продуктивності, що робить розподілене сховище оптимальним рішенням для масштабованих розгортань Nextcloud.

Переходячи до більш практичного аспекту, розгортання Nextcloud у віртуальному середовищі VMware дозволяє протестувати оптимізацію продуктивності, масштабованість і стабільність системи перед впровадженням у реальне середовище.

Процес встановлення Nextcloud у VMware включає кілька основних етапів (див. рис. 2.22):

— створення віртуальної машини з відповідною конфігурацією;

— встановлення операційної системи;

— налаштування необхідного середовища для роботи Nextcloud;

— оптимізація продуктивності;

— усунення можливих труднощів.

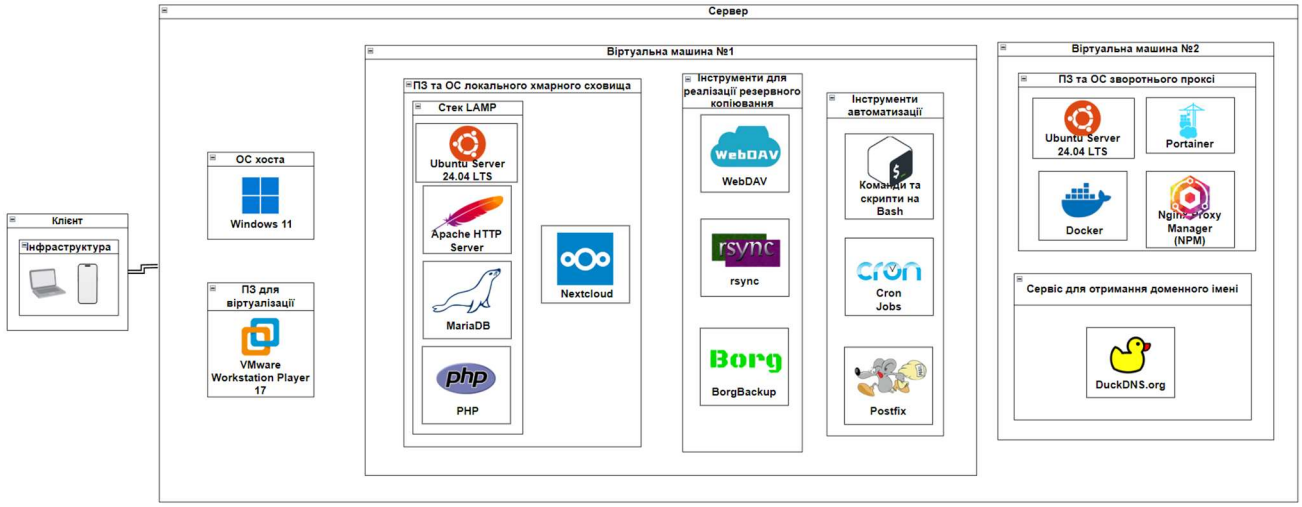


Рисунок 2.22 – Схема автоматизованої системи резервного копіювання у локальне хмарне сховище

Підготовка середовища для розгортання – Nextcloud. Для цього було використано віртуальне середовище на базі VMware, яке є популярним рішенням завдяки можливості ізоляції, масштабування та зручного керування ресурсами. Віртуальна машина також спрощує процес резервного копіювання та міграції між серверами, що додає додаткову гнучкість у налаштуванні системи. У цьому випадку для тестового розгортання Nextcloud було обрано VMware Workstation

Player як один із найпростіших і доступних варіантів, після чого необхідно було виконати підготовчі кроки для встановлення серверного середовища (див. рис. 2.23).

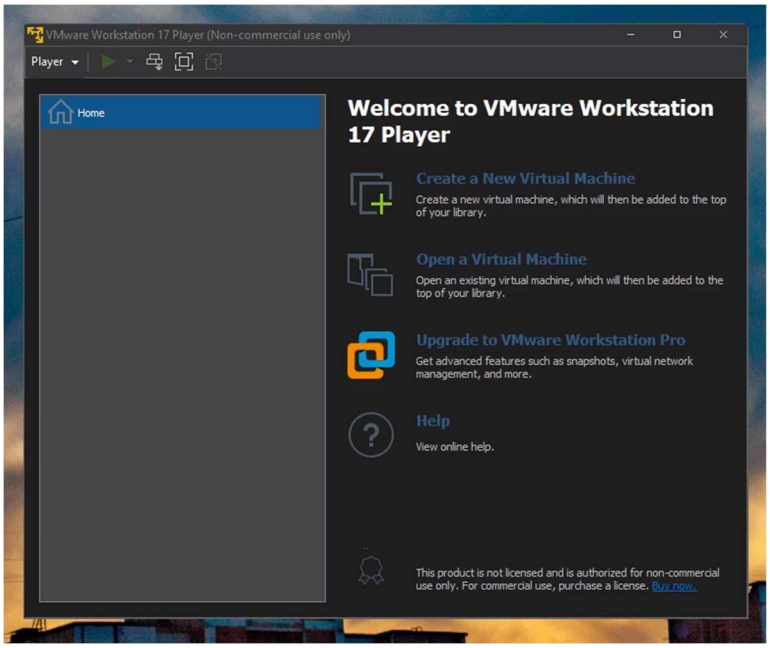


Рисунок 2.23 – Вибір віртуалізованого середовища для тестування: VMware Workstation 17 Player (гіпервізор 2-типу)

Перед встановленням Nextcloud було обрано відповідну операційну систему, і серед рекомендованих варіантів зупинилися на Ubuntu Server останньої стабільної версії, яка має широкий набір документації та добре підтримується спільнотою. Після цього віртуальна машина була створена з рекомендованими параметрами, зокрема з чотирма віртуальними ядрами процесора, 8 ГБ оперативної пам’яті, що хоча й перевищувало мінімальні вимоги, але забезпечувало достатню продуктивність для тестування, а також з 50 ГБ дискового простору для зберігання даних і перевірки роботи системи. Контролер дискової підсистеми був налаштований у режимі SCSI (LSI Logic), оскільки NVMe не був доступним у цьому випадку, а мережева карта була обрана VMXNET3, що є стандартним варіантом у VMware Workstation (див. рис. 2.24).

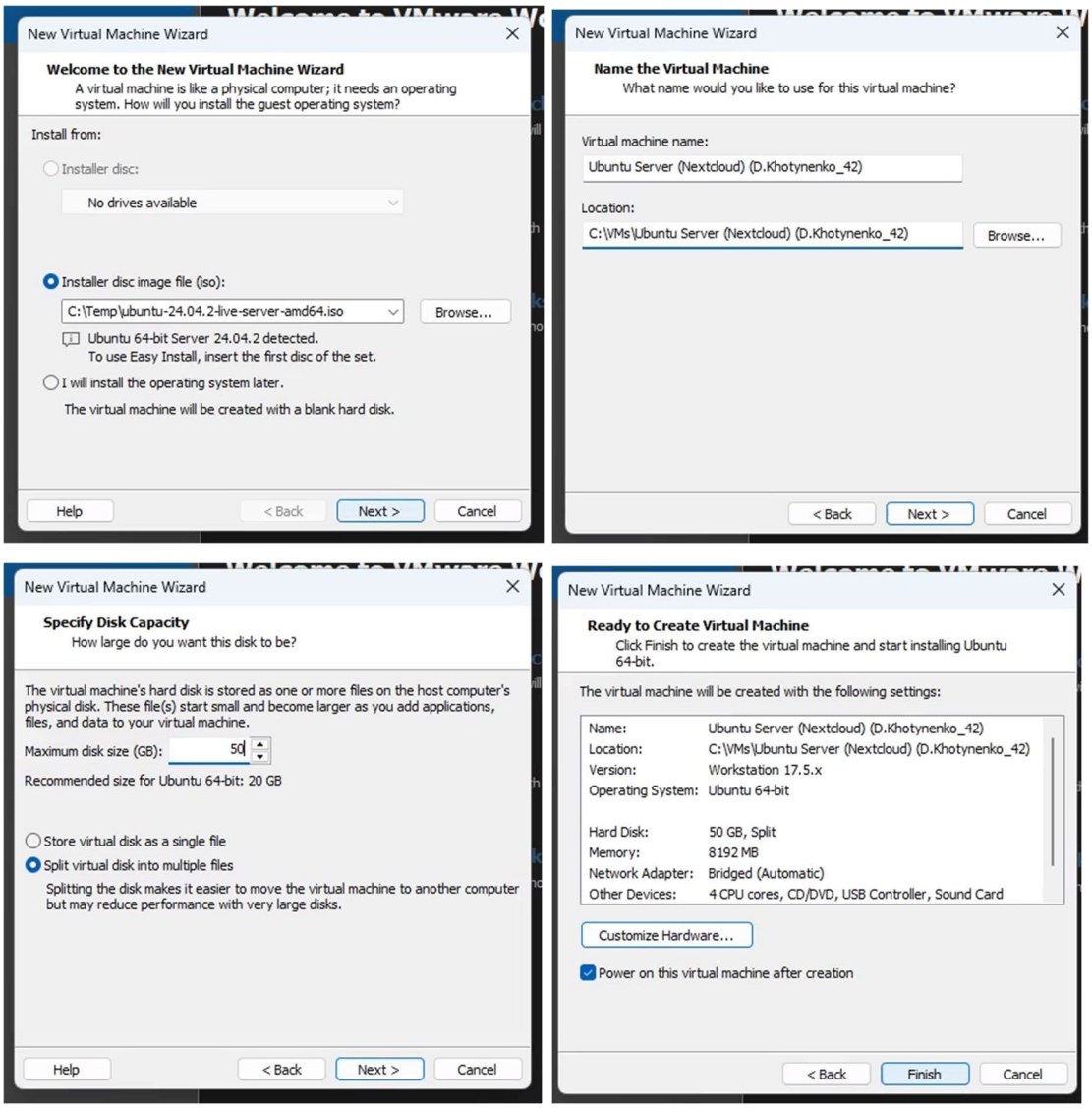


Рисунок 2.24 – Налаштування конфігурації віртуалізованого середовища:

Після створення віртуальної машини потрібно було підготувати образ Ubuntu Server, завантажити його та підключити до віртуальної машини для інсталяції. Під час створення або після створення віртуальної машини цей образ підключався у вигляді віртуального диска, після чого запускалася інсталяція операційної системи (див. рис. 2.25).

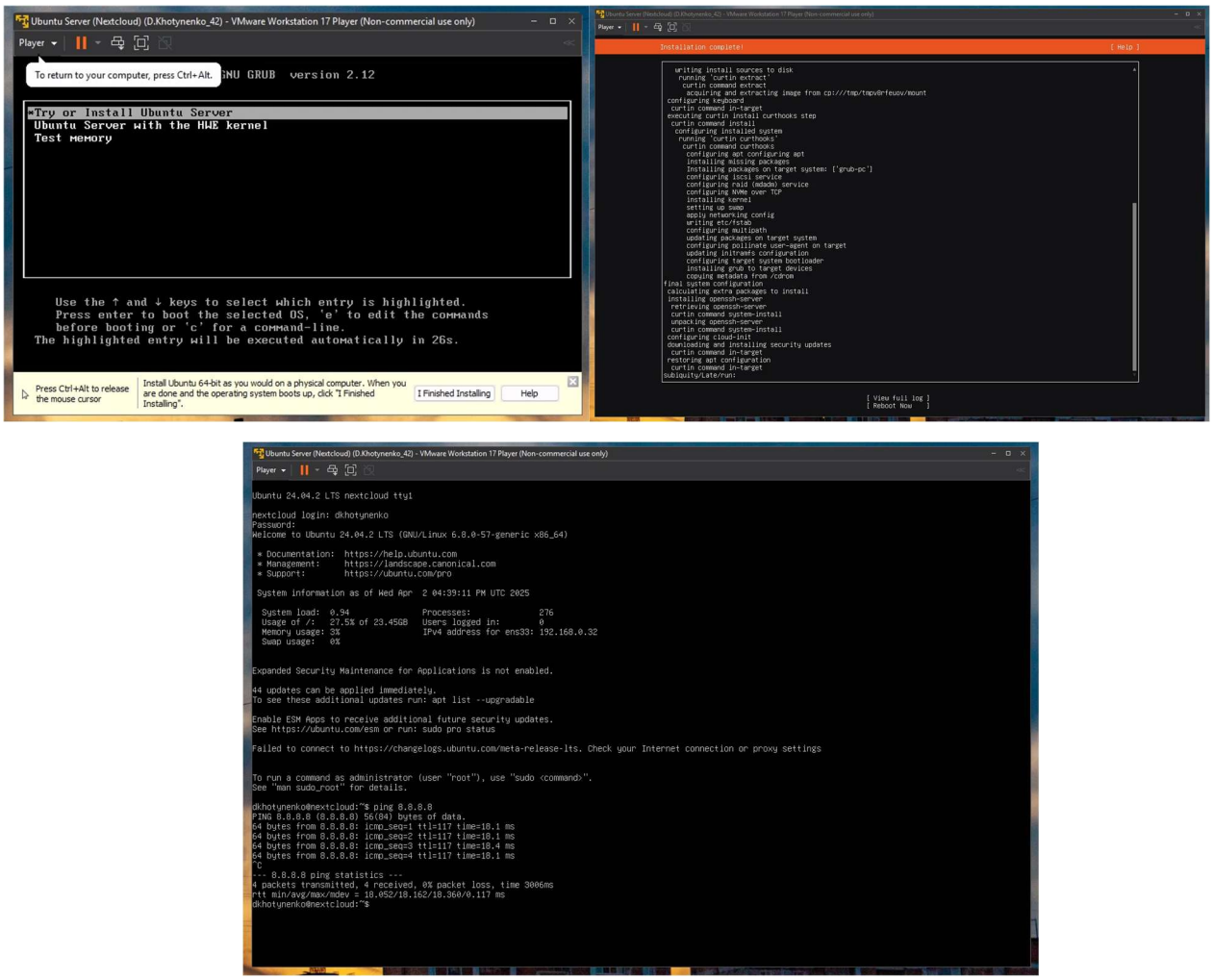


Рисунок 2.25 – Процес встановлення та ініціалізація Ubuntu Server у якості віртуалізованого сервера

Після завершення встановлення Ubuntu Server наступним кроком було підготувати середовище для роботи Nextcloud, що передбачало для початку оновлення інструментів до актуальної версії (див. рис. 2.26).

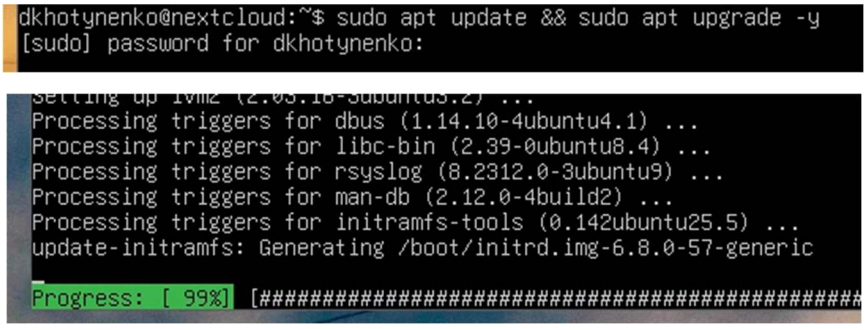


Рисунок 2.26 – Процес оновлення всіх інструментів Ubuntu Server до актуальної версії

Після оновлення, потрібно приступити до налаштування веб-сервера, бази даних та інтерпретатора PHP. Nextcloud може працювати на основі LAMP або LEMP стеків, де LAMP включає Apache, MySQL або MariaDB та PHP, а LEMP використовує Nginx замість Apache. У цьому випадку був обраний саме LAMP-стек. (див. рис. 2.26).

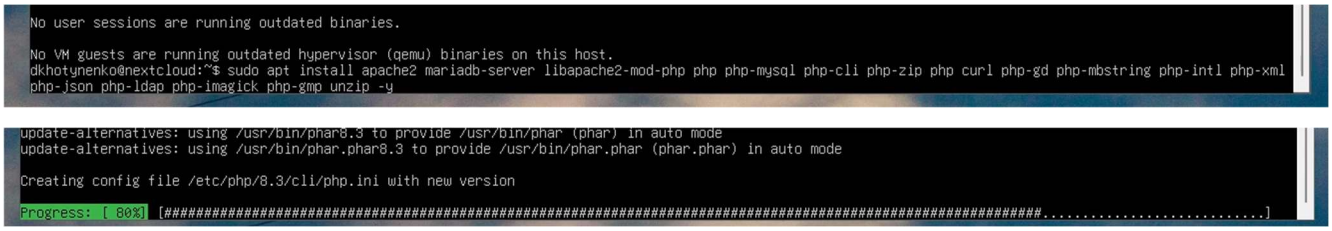


Рисунок 2.26 – Інтеграція LAMP-стека для роботи
зі локальним хмарним сховмищем

Перед цим також необхідно було перевірити конфігурацію мережі віртуальної машини, оскільки для коректної роботи Nextcloud важливо мати доступ до локальної або глобальної мережі. У віртуальних машинах VMware є кілька режимів підключення, серед яких Bridge, NAT та Host-Only. Режим Bridge дозволяє віртуальній машині отримати окрему IP-адресу в локальній мережі, що спрощує доступ з інших пристроїв, NAT забезпечує вихід у зовнішню мережу, але ускладнює доступ до віртуальної машини ззовні, а Host-Only створює ізольовану мережу, доступну лише для хостової системи. У цьому випадку був обраний режим Bridge, оскільки він найкраще підходив для тестування в локальній мережі, після чого можна було перевірити IP-адресу сервера в консолі після встановлення Ubuntu Server (див. рис. 2.27).

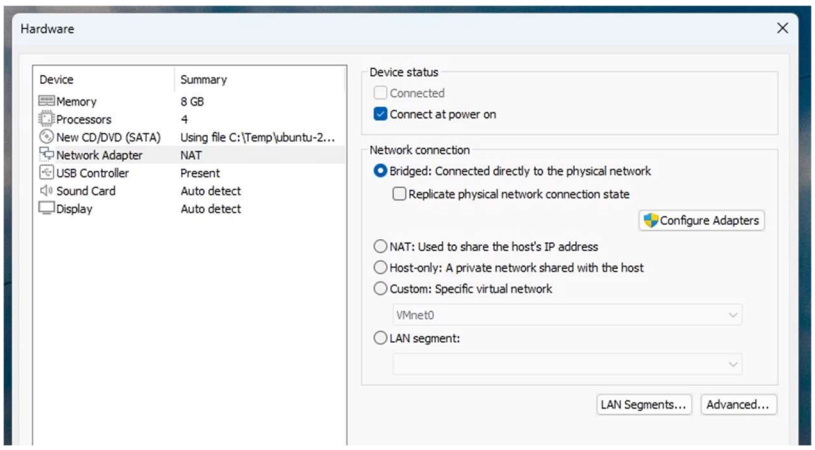


Рисунок 2.27 – Меню конфігурації VM:
обрано режим Bridge для роботи зі фізичним IP-адресом

Розміщення локального хмарного сховища у віртуальному середовищі – Nextcloud. Після підготовки середовища для роботи з Nextcloud і налаштування оптимізації резервного копіювання наступним кроком було встановлення самого Nextcloud (див. рис. 2.28).

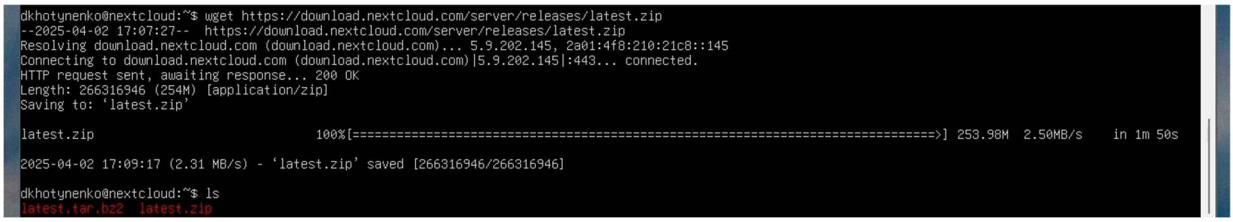


Рисунок 2.28 – Завантаження актуальної версії
локального хмарного сховища Nextcloud:

Після завантаження архів розпаковувався (див. рис. 2.29).

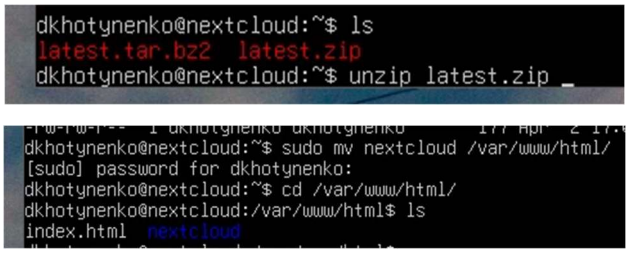


Рисунок 2.29 – Розпакування та переміщення вмісту архіву
зі локальним хмарним сховищем Nextcloud на сервері

Ці дії дозволяли отримати файли Nextcloud у правильному розташуванні для подальшого налаштування. Після цього потрібно було змінити права доступу до папки Nextcloud, щоб веб-сервер мав необхідні дозволи на її обробку (див. рис. 2.30).

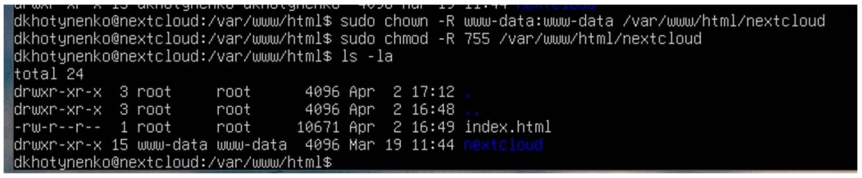


Рисунок 2.30 – Зміна правил доступу користувача та групи директорії Nextcloud

Після зміни прав доступу можна буде переходити до налаштування веб-сервера та бази даних. Першочергово створювалася база даних у MariaDB, для чого виконувався вхід до MariaDB під користувачем root (див. рис. 2.31).

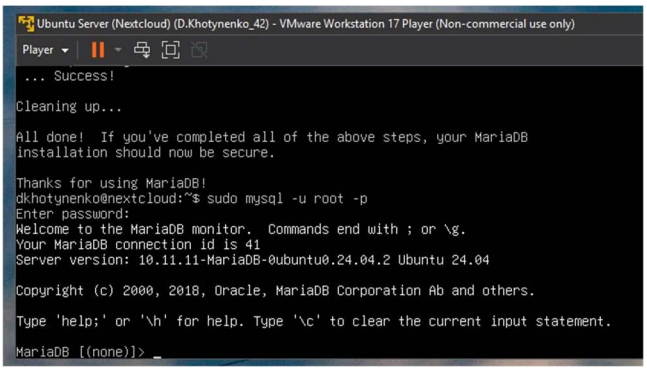


Рисунок 2.31 – Вхід до MariaDB

Далі виконувалися SQL-запити для створення бази даних та користувача з відповідними привілеями (див. рис. 2.32).

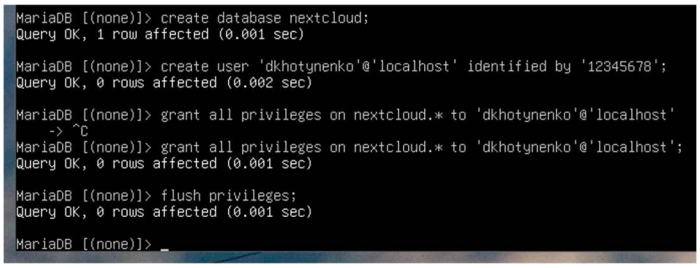


Рисунок 2.32 –Створення БД зі користувачем "nextcloud" та правами доступу

Після створення бази даних та налаштування користувача переходили до налаштування віртуального хоста Nginx, який використовувався у LAMP-стеку. Для цього відкривався конфігураційний файл для Apache командою (див. рис. 2.33).

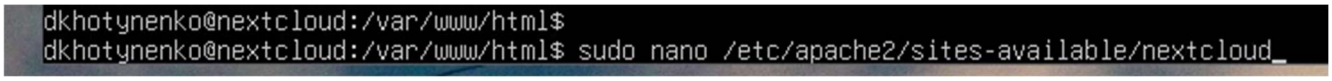


Рисунок 2.33 –Створення конфігураційного файлу "nextcloud" для Apache

У файл додавалися наступні параметри (див. рис. 2.34).

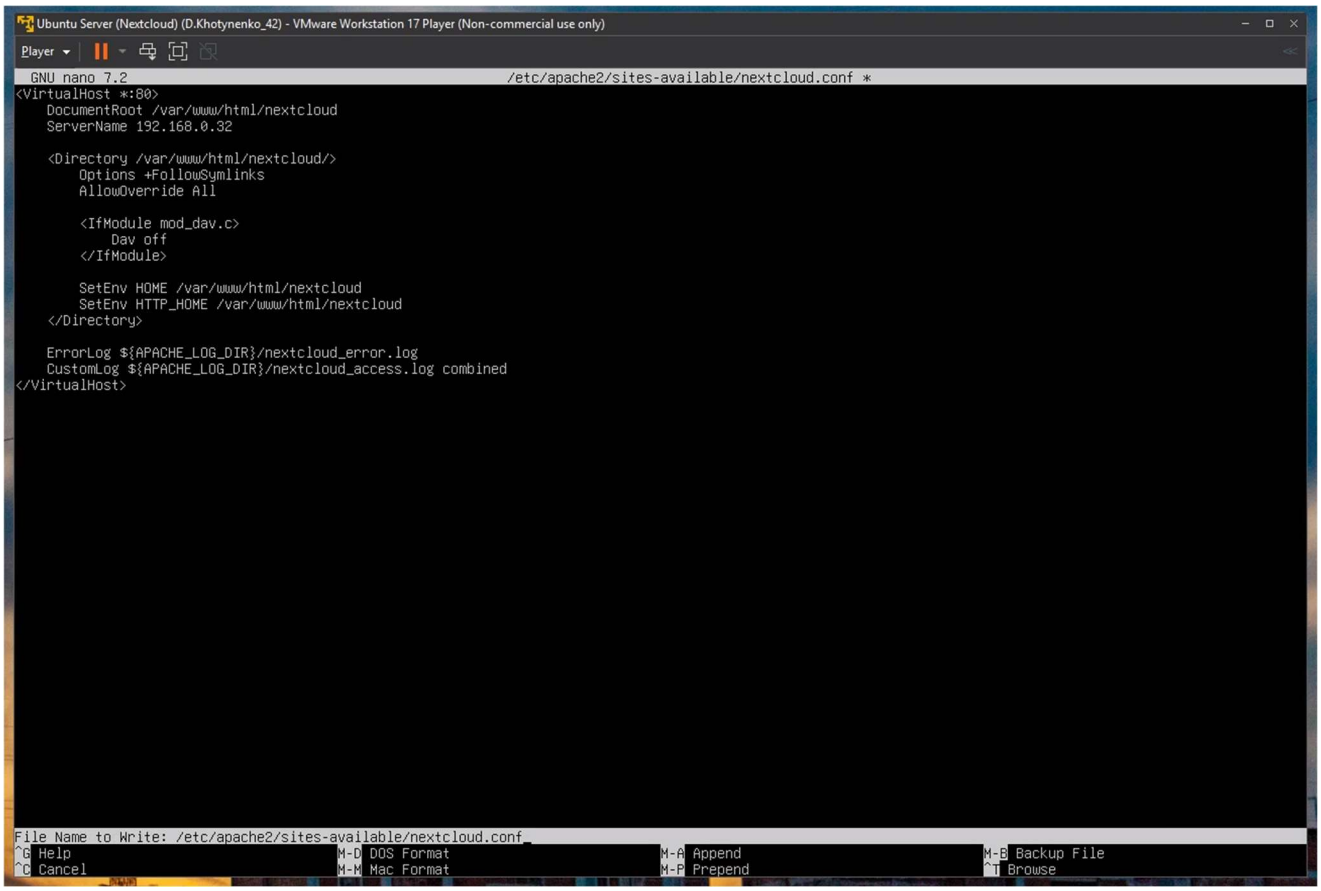


Рисунок 2.34 – Внесені параметри конфігураційного файлу "nextcloud" для Apache

Після збереження конфігураційного файлу сайт активовувався, а Apache перезапускався для застосування змін (див. рис. 2.35).

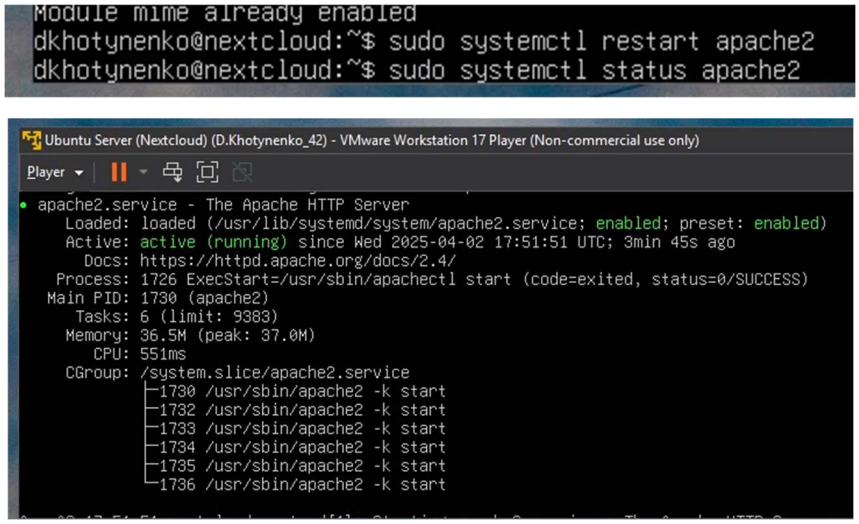


Рисунок 2.35 – Перезавантаження сервісу Apache для застосування змін

Після цих налаштувань Nextcloud можна було запускати через веб-інтерфейс, відкривши браузер і перейшовши за IP-адресою сервера "http://192.168.0.32/" (див. рис. 2.36).

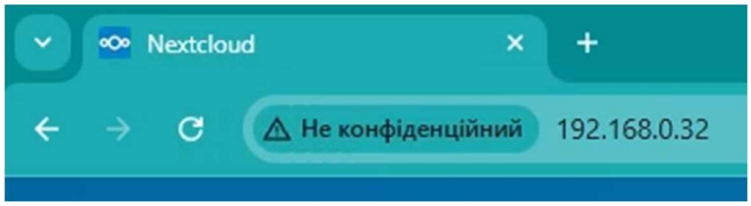


Рисунок 2.36 – Перехід за адресою сервера для перевірки працездатності Apache HTTP Сервера

При першому відкритті інтерфейсу Nextcloud пропонував створити адміністративний обліковий запис та ввести параметри бази даних, включаючи ім'я користувача nextcloud_user та його пароль (див. рис. 2.37).

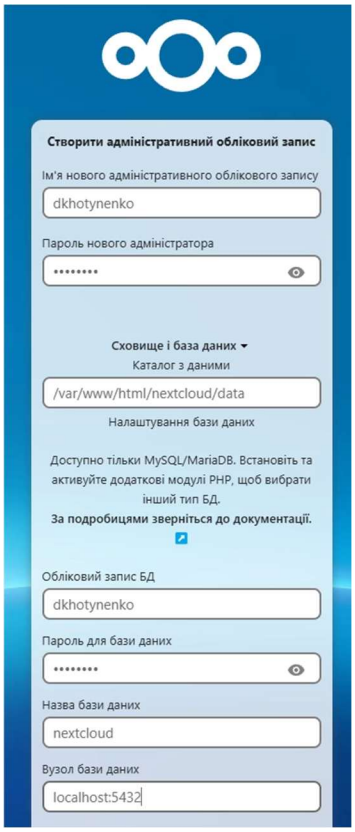


Рисунок 2.37 – Перше налаштування локального хмарного сховища Nextcloud

Після завершення цього етапу рекомендувалося встановити SSL-сертифікат Let's Encrypt для шифрованого з'єднання, що можна зробити за допомогою веб-сервіса DuckDNS та Nginx Proxy Manager (NPM).

Для реалізації надійності, був використаний попередньо налаштований робочий віртуальний сервер Ubuntu Server з Docker для роботи з контейнерами, на якому також увімкнено режим мережі Bridge, для використання фізичних IP-адресів. Управління контейнерами здійснюється за допомогою контейнера Portainer. (Додаток В)

Для отримання доменного імені використовувався веб-сервіс DuckDNS, де було створено для локального IP-адреса домен зі використанням субдоменів (див. рис. 2.38).

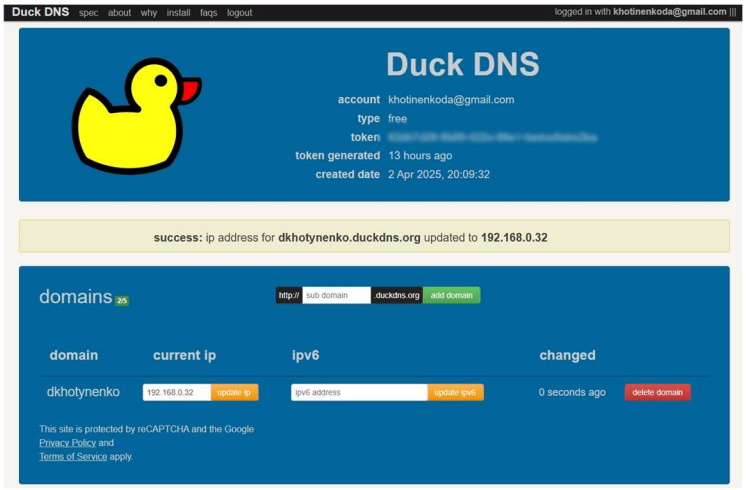


Рисунок 2.38 – Отримання безкоштовного доменного імені для роботи з під локальної мережі

Далі, через використання зворотнього проксі сервера NPM вводимо отриманий домен зі SSL сертифікатом Let`s Encrypt для роботи локального хмарного сховища зі захищеним протоколом HTTP (HTTPS) (див. рис. 2.39).

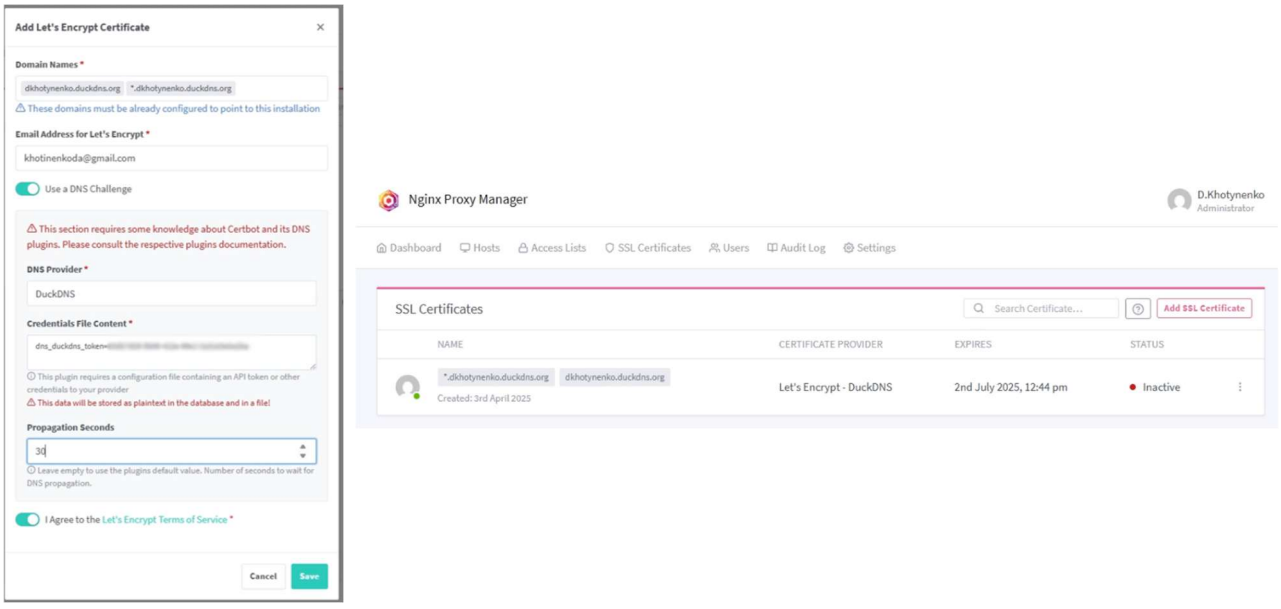


Рисунок 2.39 – Валідація нового Let`s Encrypt SSL сертифіката для роботи з протоколом HTTPS

Після активації SSL сертифікати у NPM, необхідно призначити субдомен з пула отриманого домена "dkhotynenko.duckdns.org" локальному IP-адресу сервера 192.168.0.32 по порту :80 (див. рис. 2.40).

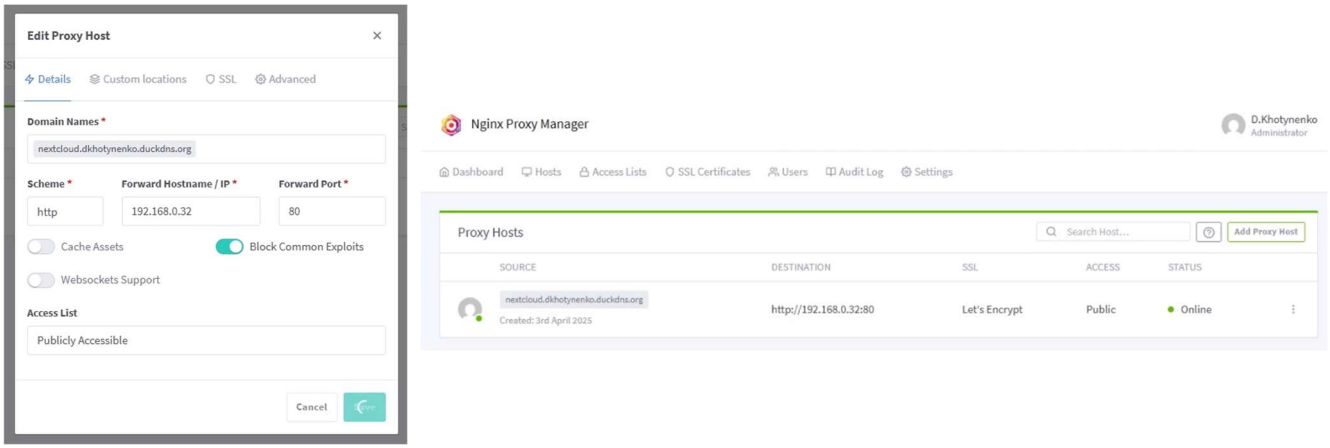


Рисунок 2.40 – Призначення субдомена "nextcloud " з пула отриманого домена "dkhotynenko.duckdns.org" локальному IP-адресу сервера 192.168.0.32 по порту :80

Завершуючи роботу над розгортанням локального хмарного сховища Nextcloud, перевіряємо роботу субдомена, вписавши "nextcloud.dkhotynenko.duckdns.org" замість IP адреса 192.168.0.32 по порту :80 (див. рис. 2.41).

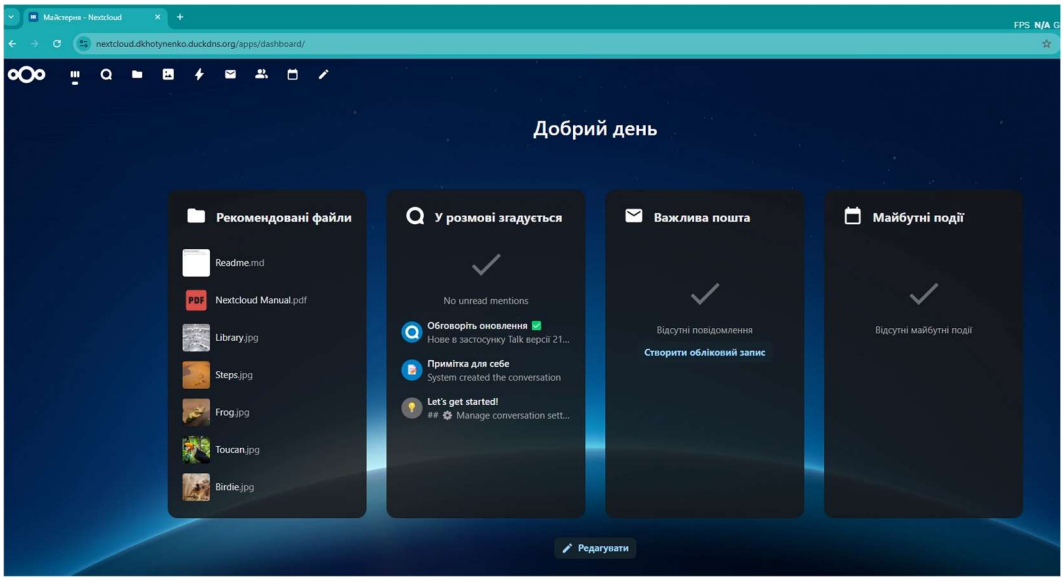


Рисунок 2.41 – Успішна робота по адресу "nextcloud.dkhotynenko.duckdns.org" через валідний SSL сертифікат Let`s Encrypt

РОЗДІЛ 3 ВПРОВАДЖЕННЯ ТА ПЕРСПЕКТИВИ МАСШТАБУВАННЯ ЛОКАЛЬНОГО ХМАРНОГО СХОВИЩА

3.1 Реалізація автоматизації резервного копіювання

Для того щоб створити систему автоматизації резервного копіювання на базі локального сховища Nextcloud, необхідно розглянути різні варіанти реалізації та протестувати кожен із них. Серед можливих рішень, що підтримуються Nextcloud, є WebDAV, rcync, BorgBackup та резервне копіювання на основі знімків файлової системи. Всі ці методи можуть бути використані для налаштування автоматичного резервного копіювання даних локального хмарного сховища, забезпечуючи гнучкість у виборі оптимальної стратегії збереження та відновлення інформації.

Налаштування автоматичного резервного копіювання локальних даних. Для захисту локальних файлів у локальному хмарному сховищі Nextcloud підтримується кілька методів резервного копіювання, таких як WebDAV, rcync та BorgBackup. Резервне копіювання через WebDAV забезпечує можливість монтування сховища як диска, що дозволяє планувати резервне копіювання з локальної системи. Для цього спочатку необхідно увімкнути WebDAV у Nextcloud, якщо він ще не активований, і це можна зробити у веб-застосунку Nextcloud, перейшовши до налаштувань і скопіювавши URL-адресу WebDAV (див. рис. 3.1).



Рисунок 3.1 – URL-адреса WebDAV для роботи без веб-інтерфейсу

Для монтування у Linux необхідно спершу встановити та налаштувати інструмент "davfs2" для роботи з WebDAV (див. рис. 3.2).

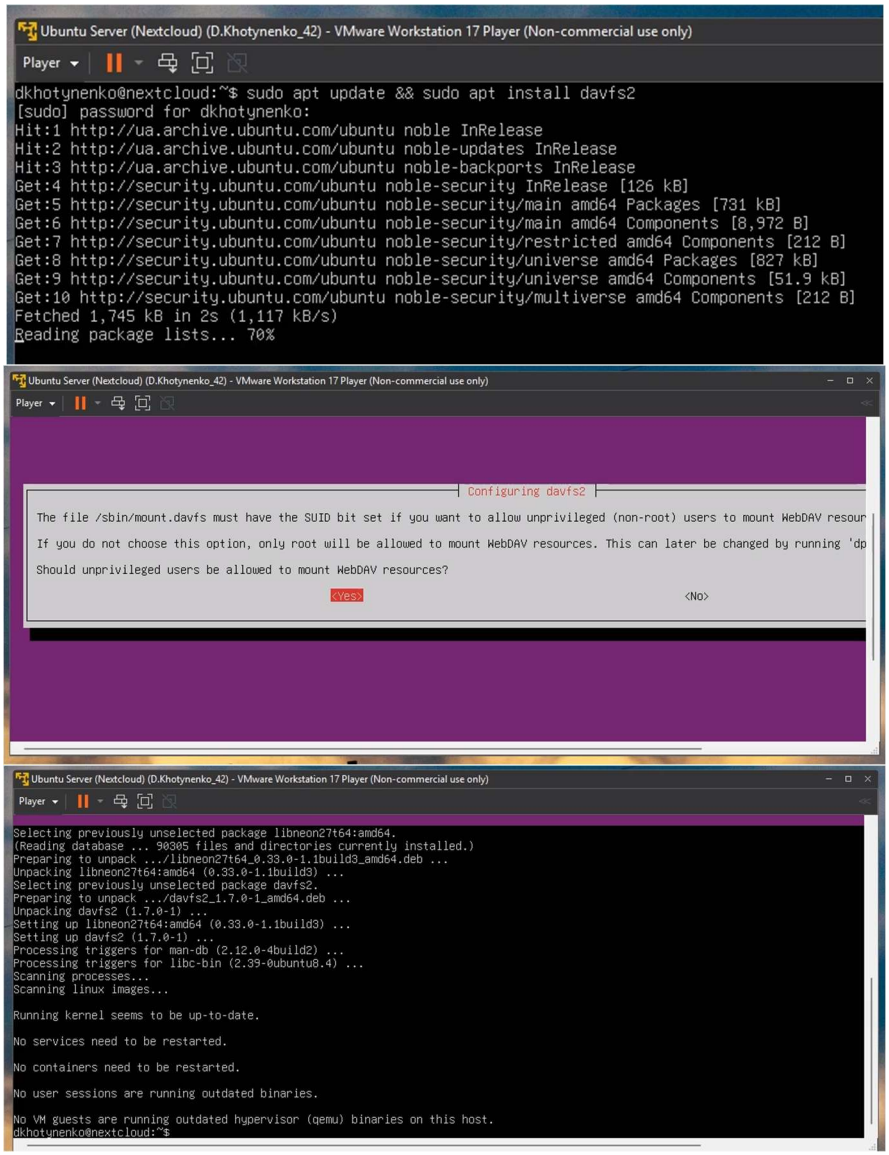


Рисунок 3.2 – Встановлення та налаштування інструмента для роботи з WebDAV у Linux

Після встановлення можливо приступати до монтування URL адреси мережевого диска у Linux. Для цього необхідно створити нову директорію та змонтувати у неї мережевий диск (див. рис. 3.3).

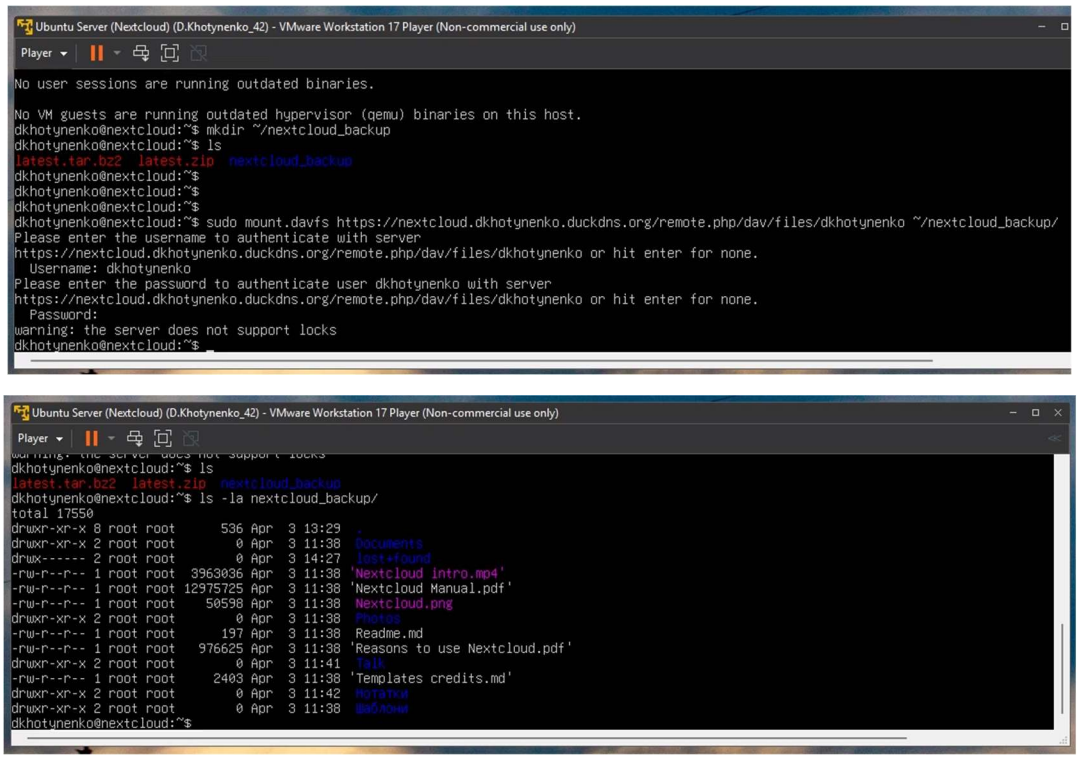


Рисунок 3.3 – Монтування мережевого диска у новостворену директорії для отримання прямого доступу до Nextcloud без веб-інтерфейсу у Linux

У Windows це можна зробити те саме через «Провідник файлів», натиснувши правою кнопкою миші на «Цей комп’ютер», вибравши «Додати мережеве розташування» та ввівши скопійовану URL-адресу WebDAV (див. рис. 3.4-3.5).

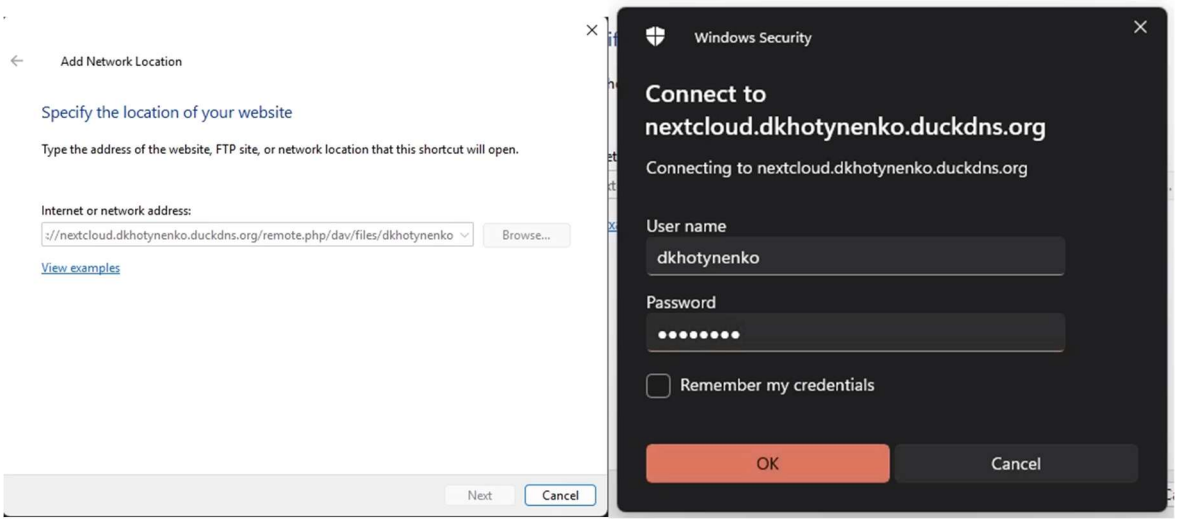


Рисунок 3.4 – Додавання мережевого диска у якості Nextcloud у Windows

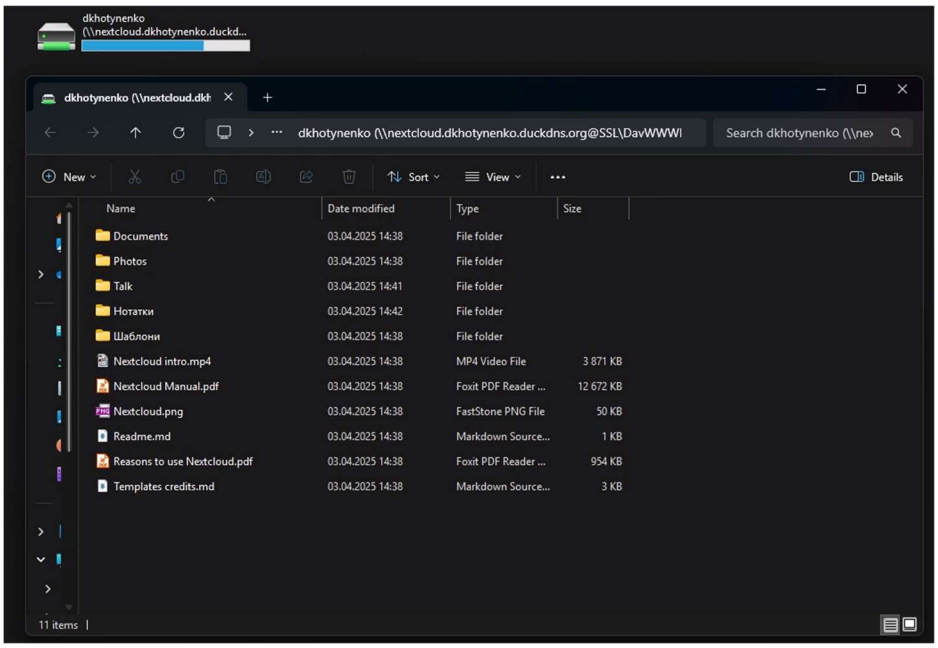


Рисунок 3.5 – Перевірка працездатності мережевого диска у якості Nextcloud у Windows

Після монтування Nextcloud у Linux або Windows можна автоматизувати резервне копіювання за допомогою завдання cron. Для цього створюється сценарій "backup_webdav.sh" (див. рис. 3.6-3.7). (Додаток А)

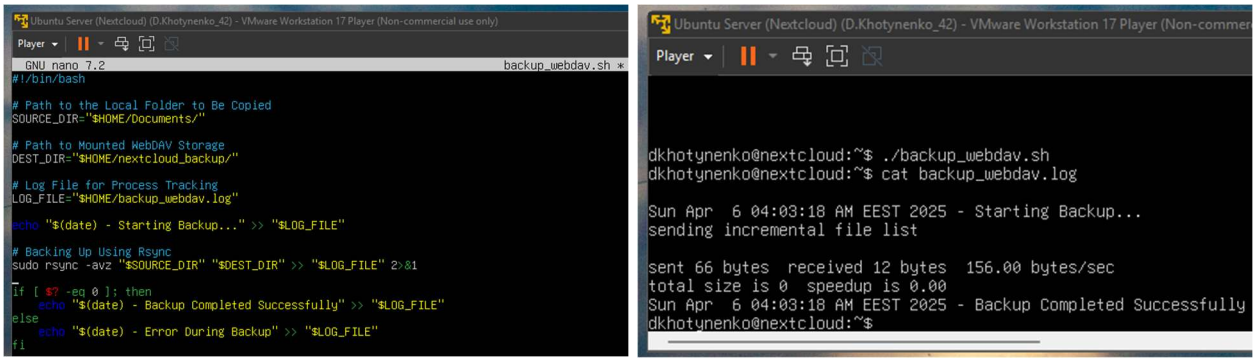


Рисунок 3.6 – Сценарій автоматизації резервного копіювання в хмару через WebDAV і rsync з логуванням

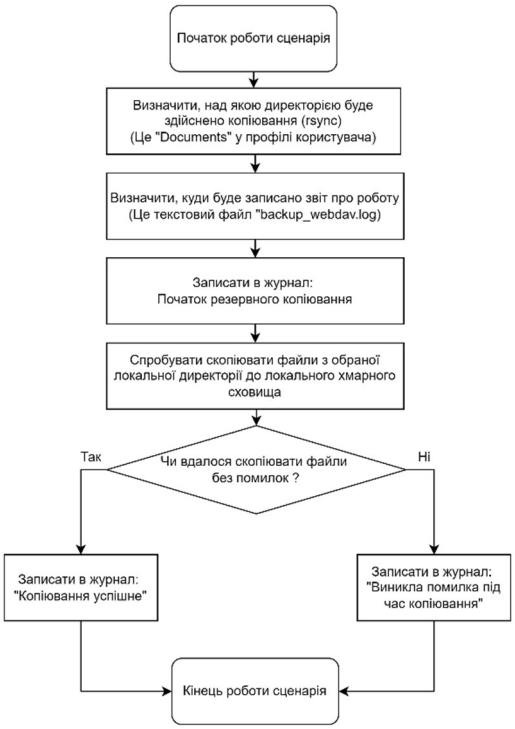


Рисунок 3.7 – Метод резервного копіювання у Nextcloud через WebDAV і rsync із логуванням

Далі, щоб автоматизувати завдання, необхідно через "crontab -e" реалізувати, наприклад щоденне резервне копіювання о 18:00 (див. рис. 3.8).

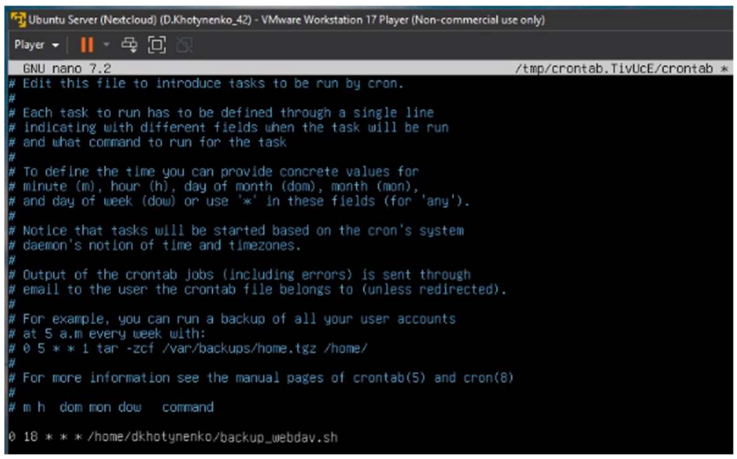


Рисунок 3.8 – Активація сценарія "backup_webdav.sh" через cron jobs: графік виконання – кожен день, о 18:00

Також у cron можна вписати команду, яка буде спрацьовувати, так, як і сценарій "backup_webdav.sh" (див. рис. 3.9).

```
0 19 * * * sudo rsync -avz /home/dkhotynenko/Documents/ /var/www/html/nextcloud/data/dkhotynenko/files/backup/
```

Рисунок 3.9 – Планування виконання команди "rsync…" через cron jobs

Ще один ефективний спосіб — використання BorgBackup, який дозволяє зменшити витрати на зберігання завдяки дедуплікації, оскільки зберігаються лише унікальні блоки файлів. Для початку встановлюється BorgBackup (див. рис. 3.10).

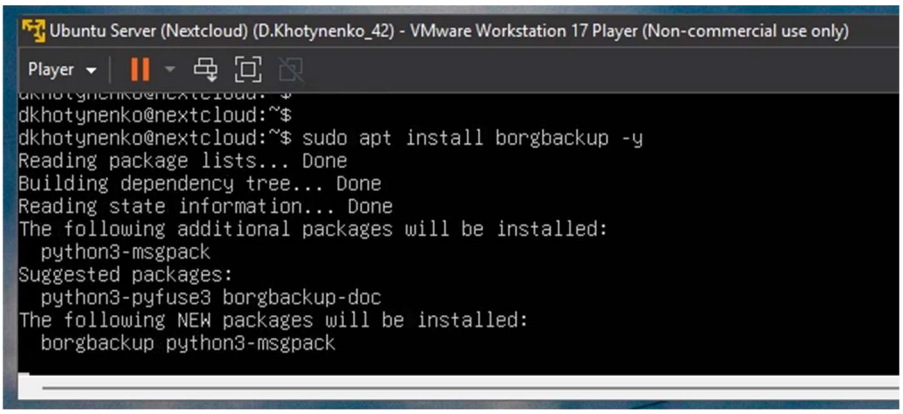


Рисунок 3.10 – Процес встановлення BorgBackup

Після встановлення необхідно створити та ініціалізувати сховище резервних копій (див. рис. 3.11).

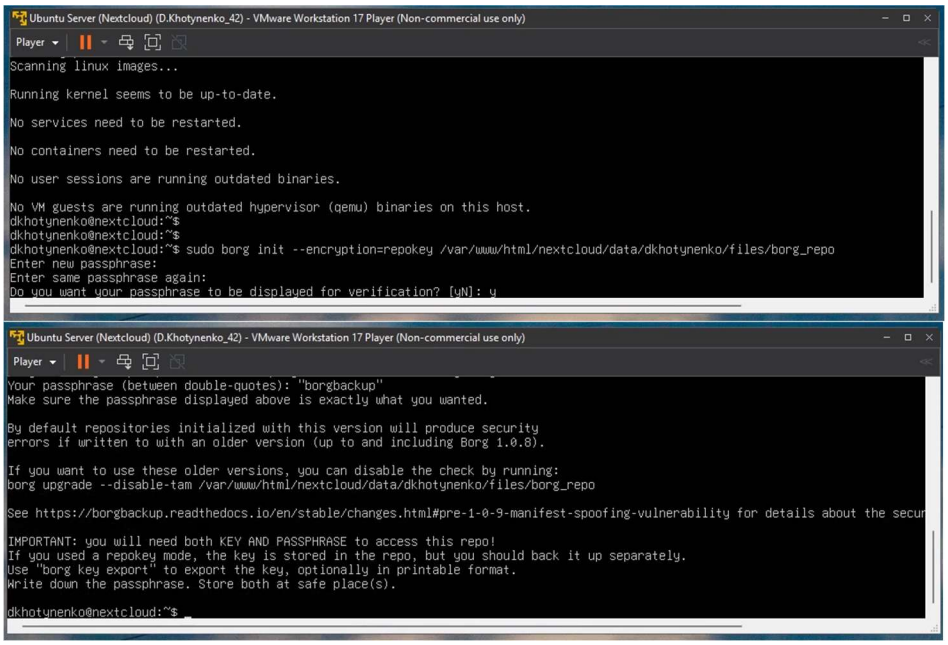


Рисунок 3.11 – Створення та ініціалізація сховища резервних копій BorgBackup

Далі запускається створення першої резервної копії та подальше інкрементне резервне копіювання (фрагменти змінених блоків структури файлової системи) (див. рис. 3.12).

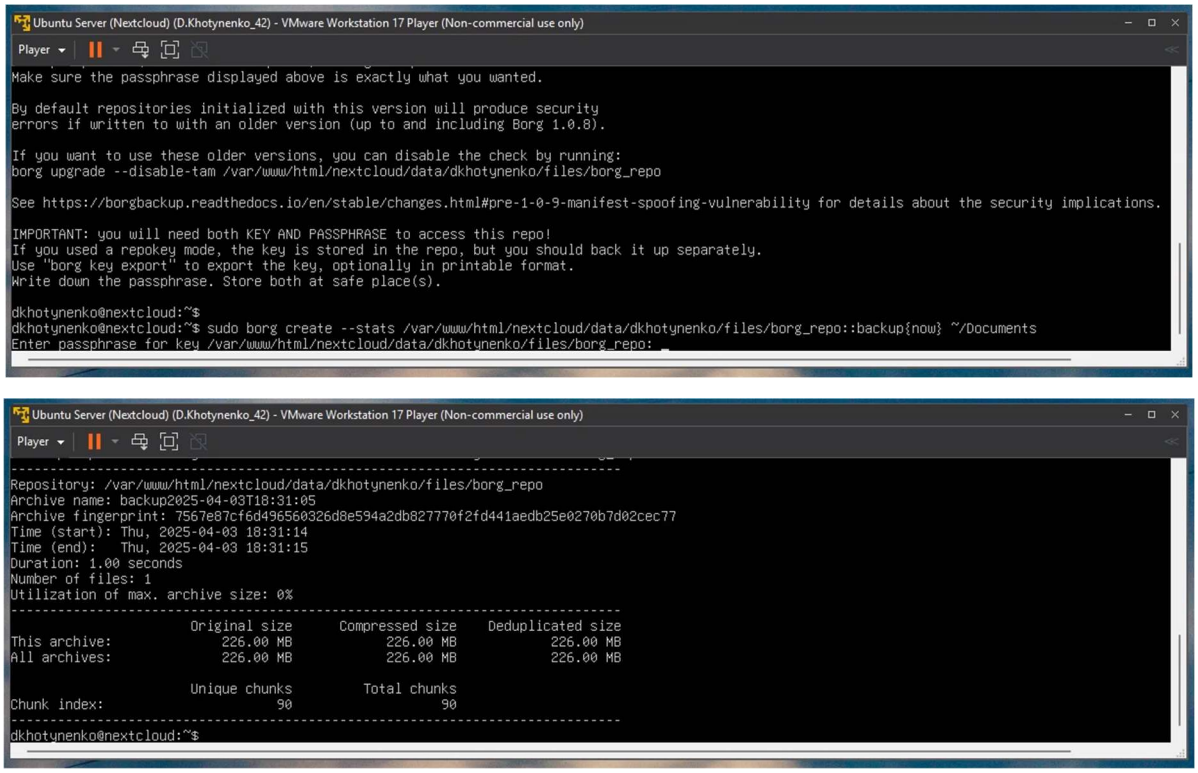


Рисунок 3.12 – Створення повної резервної копії через BorgBackup зі подальшим інкрементним резервним копіюванняс

Щоб автоматизувати процес подальшого інкрементного резервного копіювання, додається завдання cron для резервного копіювання, наприлад о 20:00 вечора (див. рис. 3.13).



Рисунок 3.13 – Активакція подальшого інкрементного резервного копіювання через BorgBackup

Моніторинг стану резервних копій за допомогою Logreader та інших інструментів. Крім забезпечення самого резервного копіювання необхідно гарантувати його надійність, що потребує моніторингу та ведення журналів.

Вбудовані в Nextcloud інструменти, такі як Logreader, дозволяють аналізувати журнали резервного копіювання, а також є можливість використовувати системні журнали Linux або сторонні рішення для глибшого аналізу та автоматичних сповіщень.

Logreader — це вбудований засіб перегляду журналів у Nextcloud, який допомагає виявляти помилки резервного копіювання або проблеми з синхронізацією. Якщо цей інструмент не увімкнений, необхідно перейти в панель адміністратора Nextcloud, вибрати «Налаштування адміністрування» → «Ведення журналу» та встановити прапорець напроти рівня журналу «Попередження та помилки», щоб зафіксувати потенційні збої резервного копіювання в майбутньому. Такий спосіб моніторингу дозволяє швидко знаходити проблеми без необхідності використання додаткового програмного забезпечення (див. рис. 3.14).

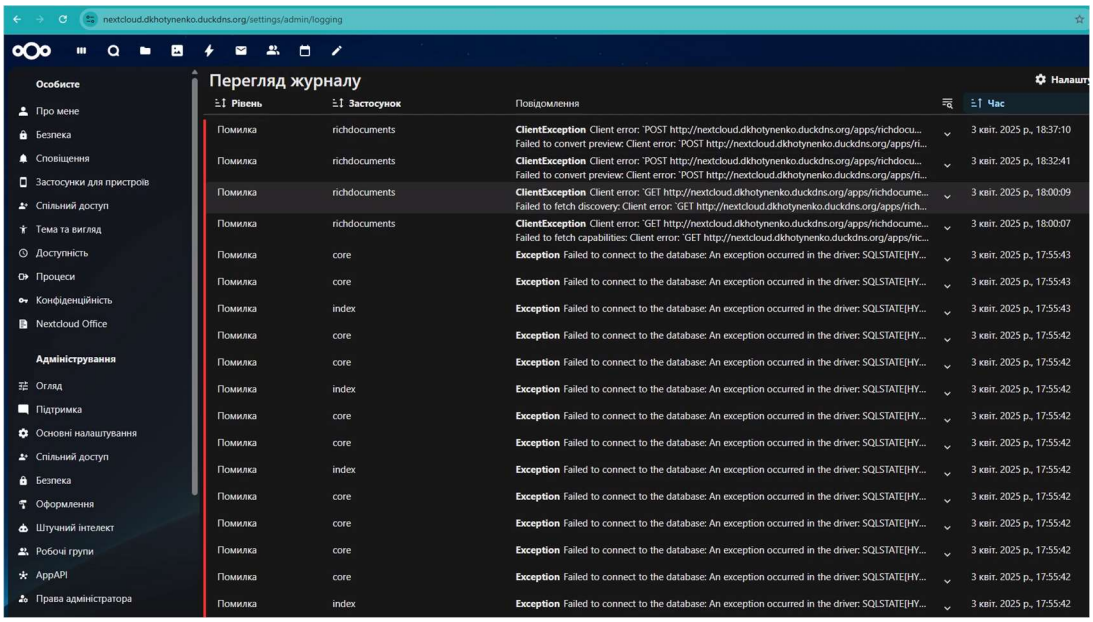


Рисунок 3.14 – Перегляд журналу Logreader у Nextcloud:
створення помилок неправильного доступу до мережевого диску

Крім вбудованих засобів можна використовувати зовнішній моніторинг за допомогою системних журналів Linux, які надають докладні звіти про можливі помилки. Наприклад, зручно переглядати журнал по резервному копіюванню через rsync за допомогою послідовності з команд (див. рис. 3.15).

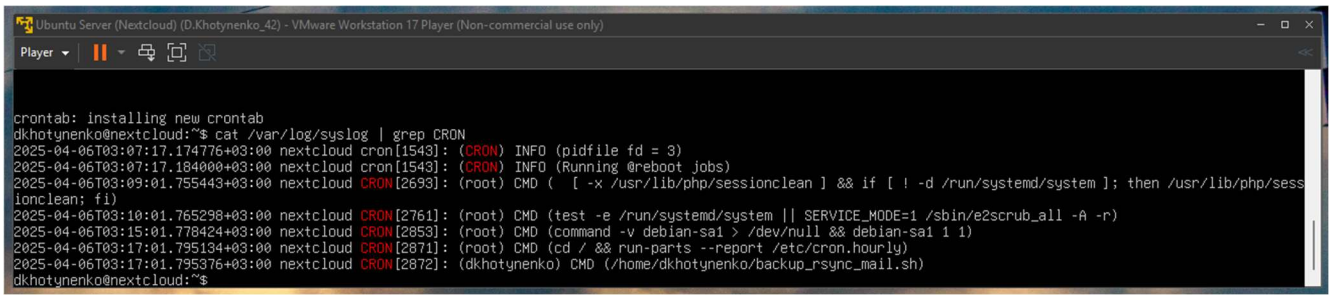


Рисунок 3.15 – Реалізація перегляду логів Cron Jobs про резервне копіювання rsync за допомогою "grep"

Ще одним зручним і унікальним варіантом стеження за станом резервного копіювання – відправка автоматичних сповіщень про збої резервного копіювання на електронну пошту. Для цього необхідно встановити інструмент "mailutils", налаштовуючи Postfix (див. рис. 3.16).

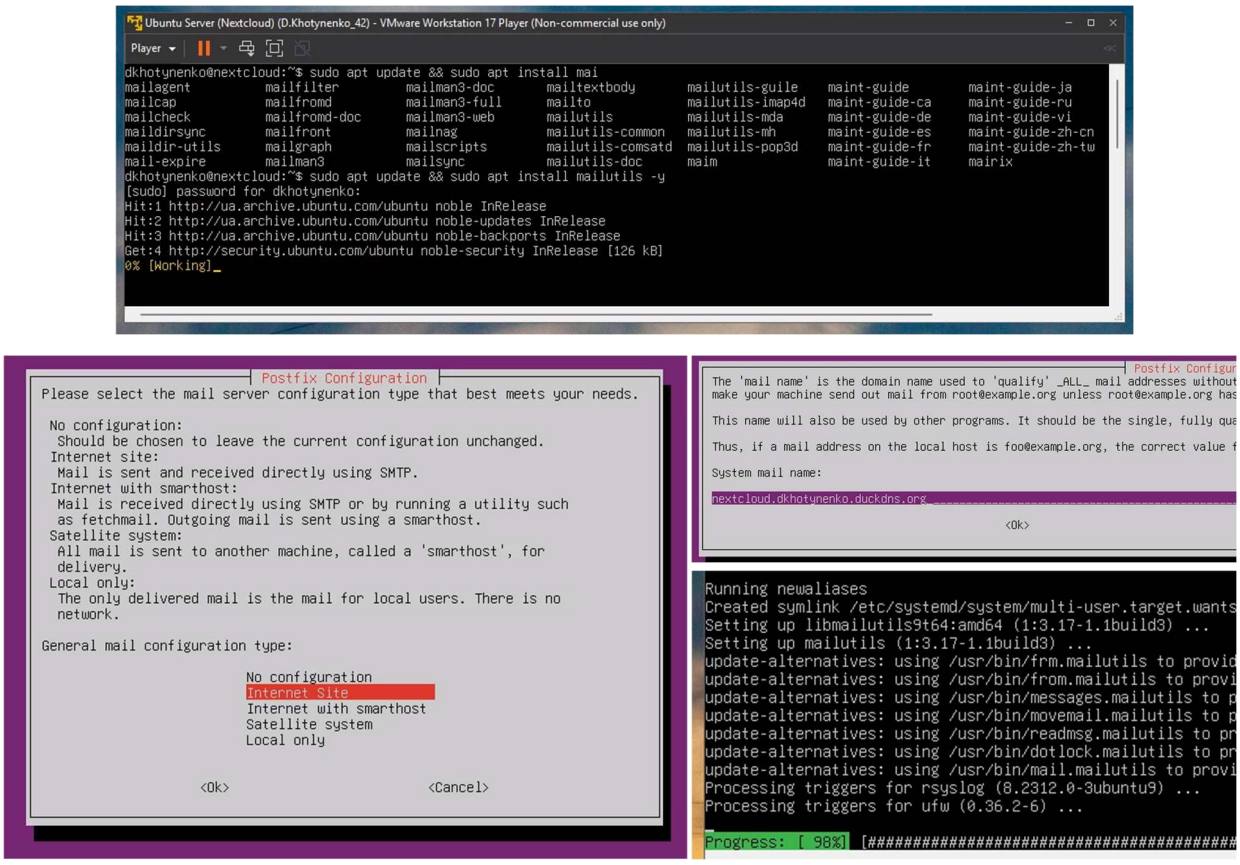


Рисунок 3.16 – Розгортання та налаштування інструменту для відправки повідомлень: Postfix

Для реалізації роботи з надсиланням листів на будь-яку електронну пошту, необхідно отримати пароль для використання протокола SMTP від домена gmail.com – пароль додатків (див. рис. 3.17).

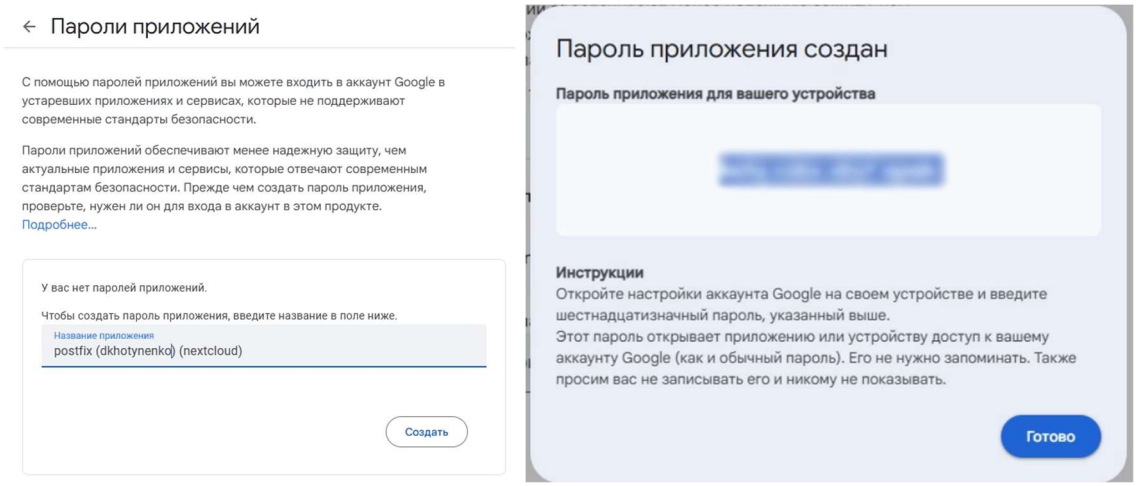


Рисунок 3.17 – Отримання пароля додатків від домена gmail.com для роботи зі SMTP протоколом

Далі необхідно ввести дані для "sasl_passwd", які будуть використовувати пароль електронної пошти під доменом gmail.com від її адресу через протокол SMTP (див. рис. 3.18).

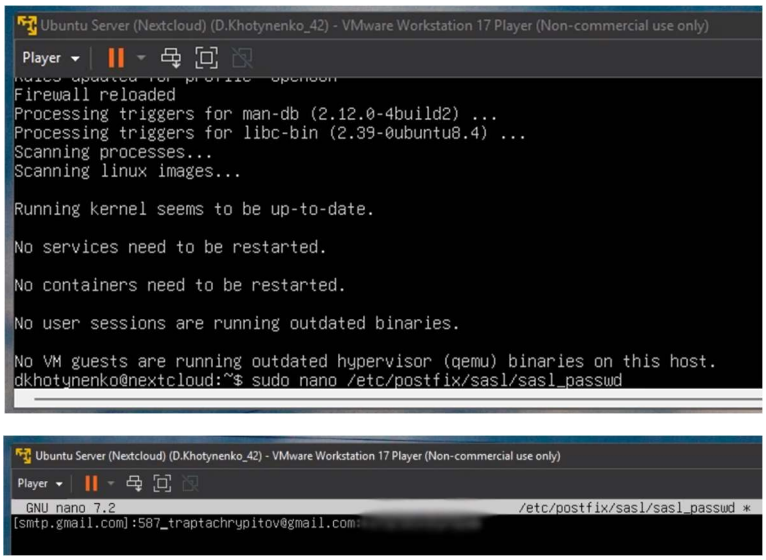


Рисунок 3.18 – Внесення унікального пароля додатків від домена електронної пошти gmail.com у файл "sasl_passwd"

Після присвоєння адресу та унікального пароля електронної пошти, від якої буде здійснювати пересилка листами через STMP протокол, також вкрай важливо налаштувати права доступу користувача та групи до файла "sasl_passwd та "sasl_passwd.db" (БД створюється першою командою на рис. 3.19) (див. рис. 3.19).

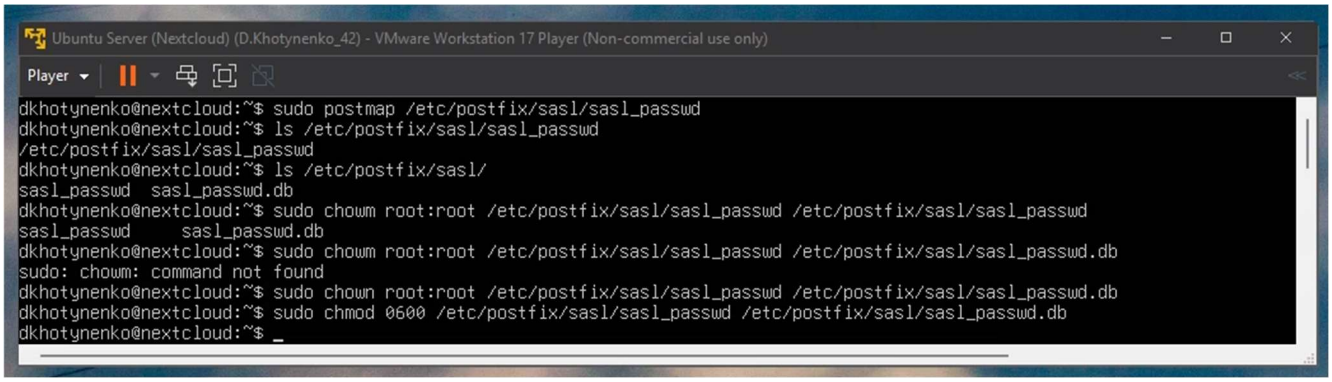


Рисунок 3.19 – Внесення унікального пароля додатків від домена електронної пошти gmail.com у файл "sasl_passwd"

Далі необхідно вписати необіхдні параметри у "main.cf" для завершення прив’язки реальної електронної пошти для роботи з розсилками (див. рис. 3.20).

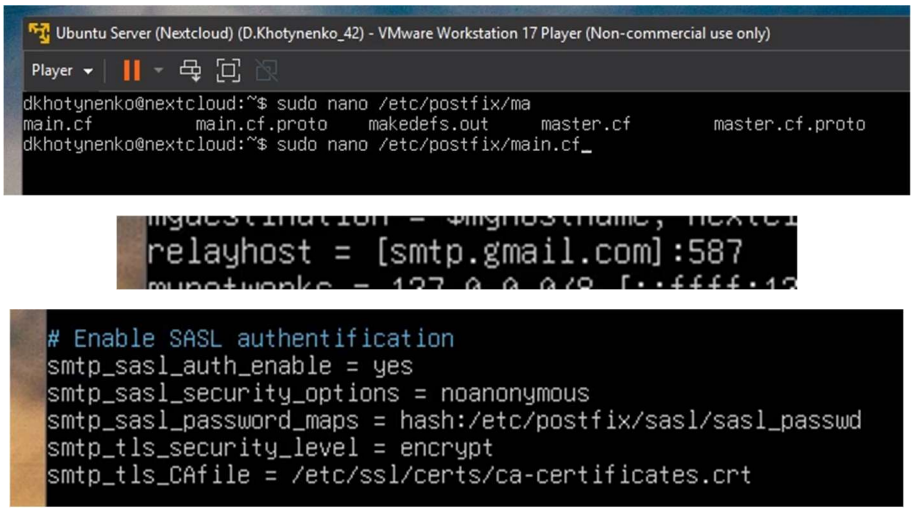


Рисунок 3.20 – Активація SASL аутентифікації для роботи служби зі розсилками

Для початку роботи зі розсилками, необхідно перезапустити службу "postfix" (див. рис. 3.21).

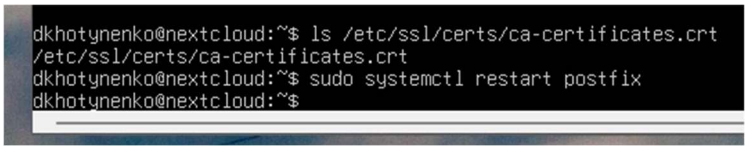


Рисунок 3.21 – Перезавантаження служби "postfix"

Тепер, за допомогою команди "sendmail" з’явилася можливість надсилати повідомлення на зі віртуалізованого сервера на будь-який електронний адрес (див. рис. 3.22).

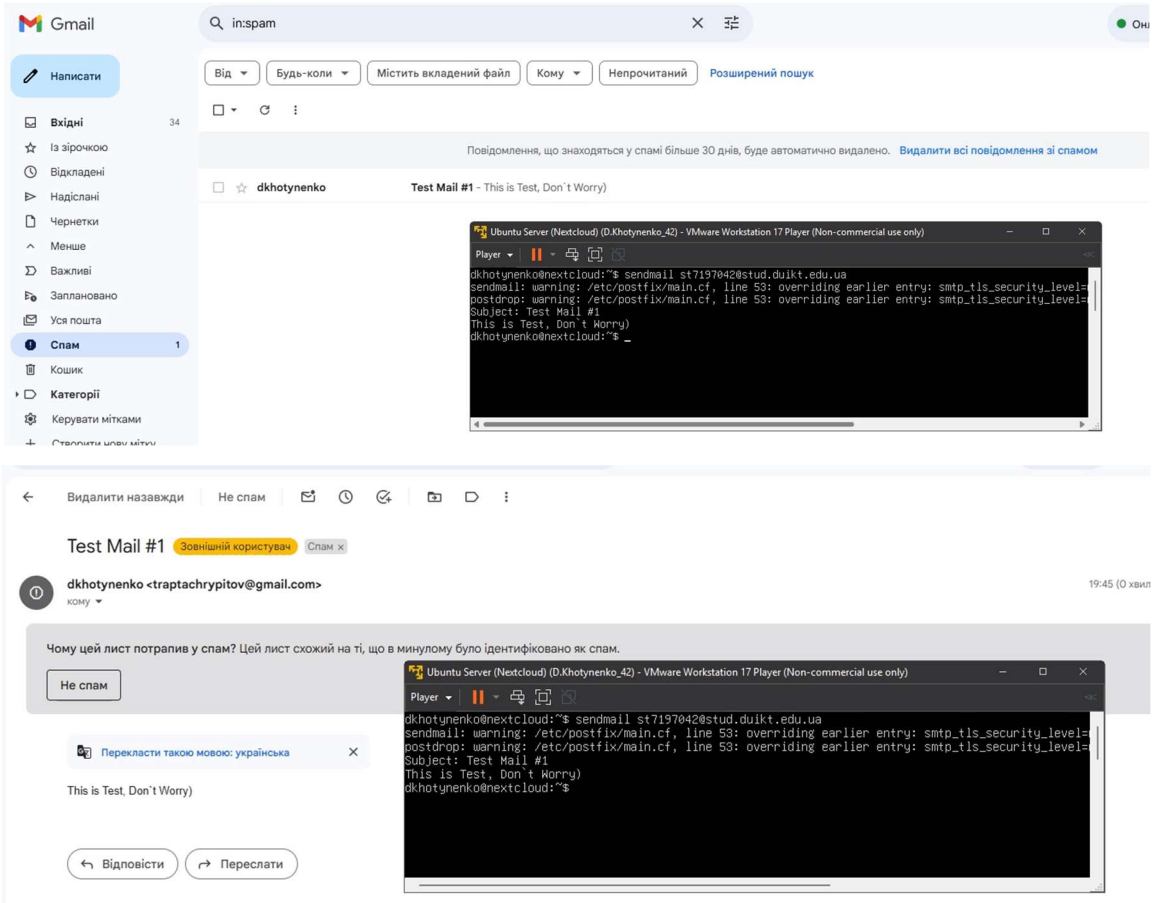


Рисунок 3.22 – Пробне надсилання листа зі віртуалізованого сервера через Postfix на існуючий електронний адрес

Таким чином, можна видозмінити сценарій резервного копіювання rsync, який пов’язаний зі "cron jobs", створивши автоматизоване резервне копіювання у локальне хмарне сховище (щоденно, о 21:00) зі створенням лог-файлу та надсиланням повідомлення адміністратору сервера у разі невдалої спроби резервного копіювання (навмисна помилка у сценарії (див. рис. 3.23)) (або ж також вдалої (див. рис. 3.24)) (див. рис. 3.25) (Додаток Б).

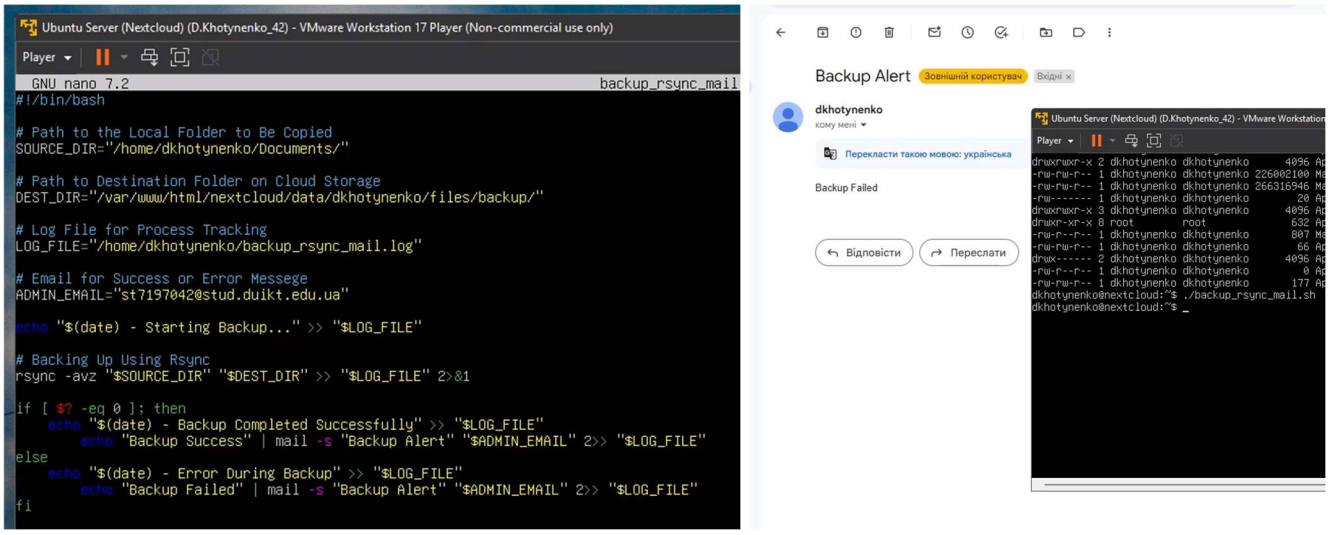


Рисунок 3.23 – Сценарій автоматизації резервного копіювання в хмару з логуванням і сповіщенням на email через Postfix (навмисно-невірний сценарій)

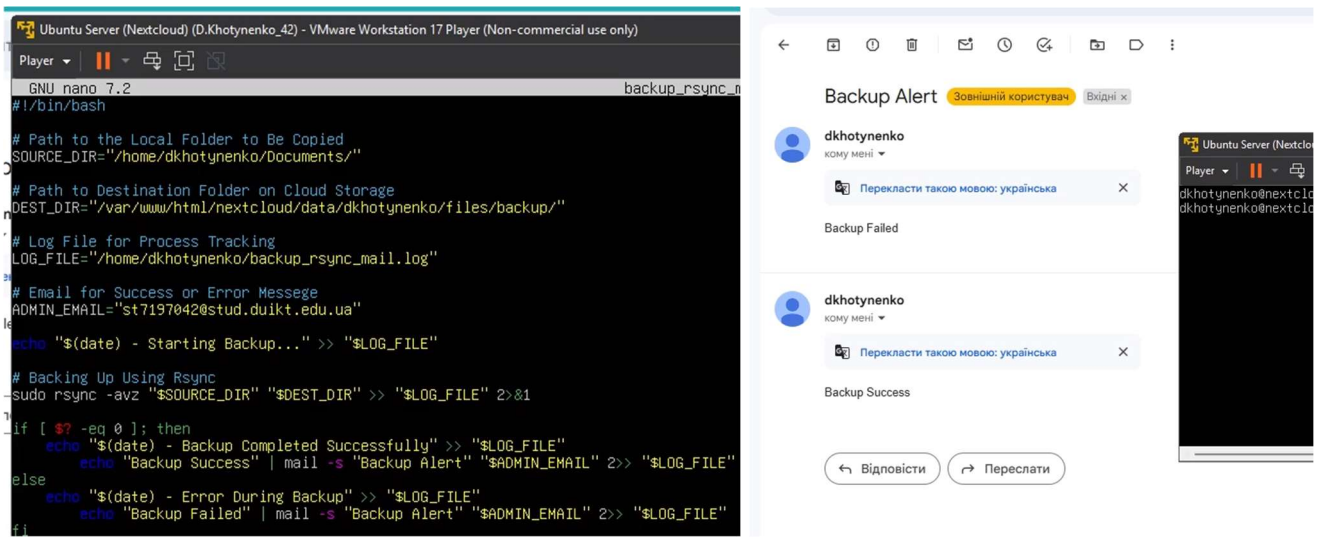


Рисунок 3.24 – Сценарій автоматизації резервного копіювання в хмару з логуванням і сповіщенням на email через Postfix (вірний сценарій)

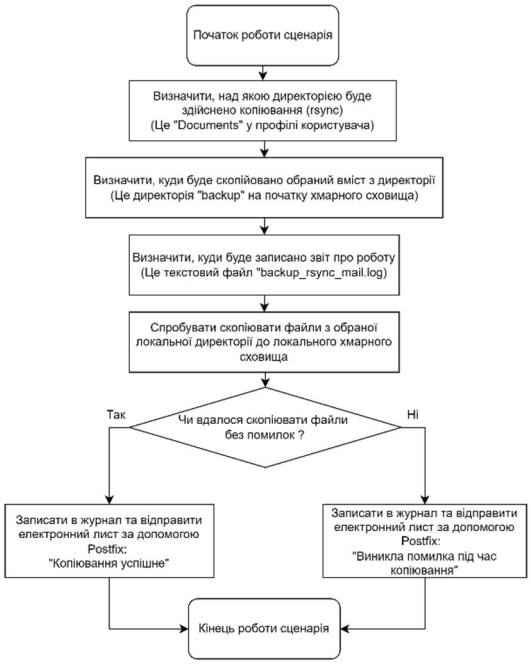


Рисунок 3.25 – Метод резервного копіювання з логуванням і email-сповіщенням у системі автоматизації резервного копіювання

Відновлення файлів із резервної копії. Аналіз швидкості та ефективності відновлення файлів із резервної копії є критично важливим для розуміння того, наскільки швидко можна повернути дані у разі втрати.

Для відновлення файлів із резервної копії WebDAV необхідно підключити сховище WebDAV та скопіювати файли назад (див. рис. 3.26).

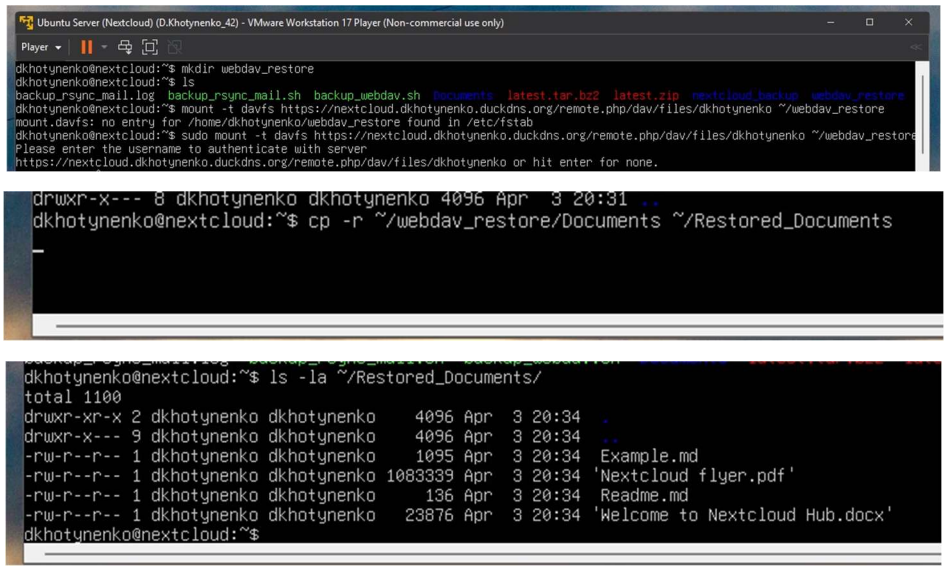


Рисунок 3.26 – Відновлення файлів зі резервної копії WebDAV

Для відновлення через rsync – подібно до відновлення у WebDAV (див. рис. 3.27).

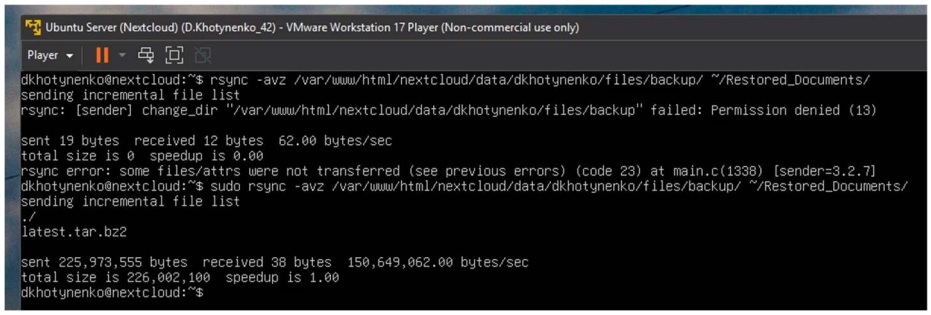


Рисунок 3.27 – Відновлення файлів зі резервної копії rsync

Використання BorgBackup для відновлення файлів передбачає спочатку перегляд списку доступних інкрементних резервних копій (див. рис. 3.28).

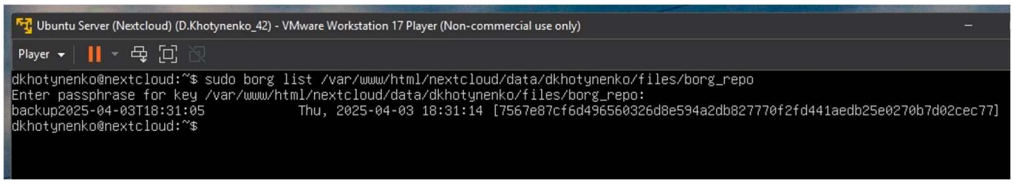


Рисунок 3.28 – Перегляд всіх інкрементних резервних копій, створених через BorgBackup

Після перегляду списку доступних резервних копій можна обрати останню та розпочати процес відновлення (див. рис. 3.29).

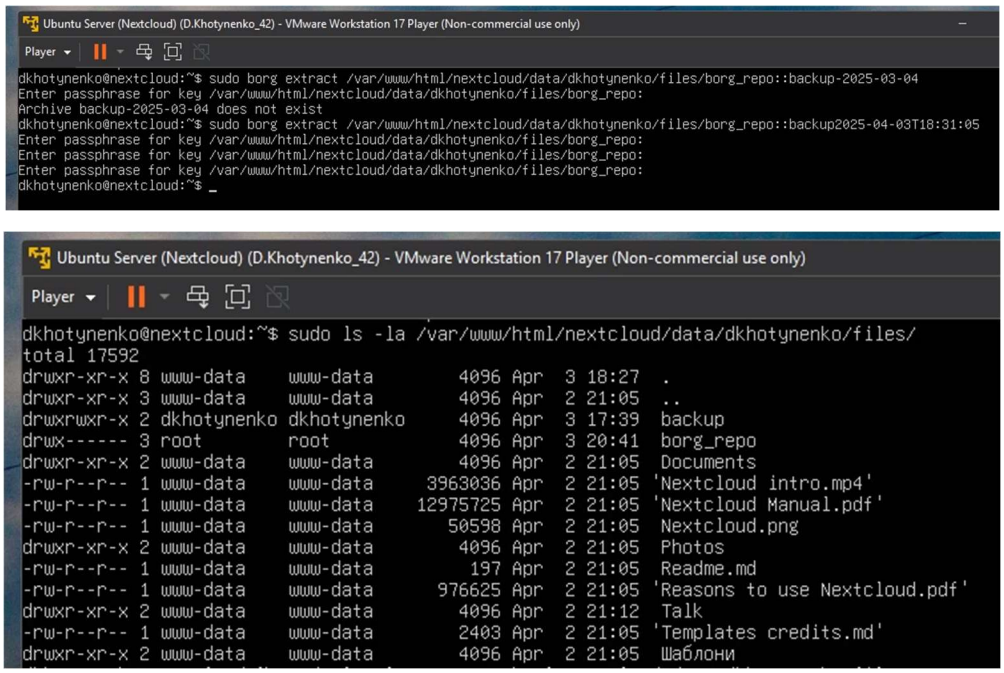


Рисунок 3.29 – Відновлення інкрементної резервної копії через BorgBackup

Таблиця 3.1 – Аналіз ефективності відновлення файлів із резервної копії (WebDAV, Rsync, BorgBackup)

Метод резервного копіювання	**Простота налаштування**	**Використання ресурсів сховища**	**Гнучкість відновлення**	**Особливості**
WebDAV	Висока (просте підключення як мережевого диска)	100% (зберігає всі файли без змін)	Обмежена (повне відновлення, без інкрементних копій)	Простий доступ через мережу, значне навантаження на сховище
Rsync	Середня (потрібна настройка сценаріїв або cron-завдань)	90% (зберігає повні копії + змінені файли)	Висока (відновлення окремих файлів та папок)	Передача лише змінених файлів, можливість синхронізації між серверами
BorgBackup	Низька (потрібні команди CLI та налаштування репозиторію)	40% (інкрементне збереження, дедуплікація)	Висока (відновлення будь-якої версії файлів)	Мінімальне навантаження на дисковий простір, шифрування резервних копій, швидке відновлення

З отриманих результатів можна зробити висновок, що найбільш ефективним методом резервного копіювання є BorgBackup, який забезпечив найшвидше відновлення файлів із найменшим навантаженням на систему. Rsync виявився компромісним варіантом, забезпечуючи баланс між продуктивністю та сумісністю, а WebDAV хоч і дозволяє легко підключати резервні копії як мережевий диск, потребує значно більше пам’яті та часу як на резервне копіювання, так і на відновлення.

Використання автоматизованого резервного копіювання через WebDAV, rsync або BorgBackup у поєднанні з Nextcloud дозволяє досягти високої надійності, а оптимізація стратегії резервного копіювання зменшує витрати пам’яті до 60%, що особливо важливо для ефективного використання ресурсів.

3.2 Потенційні труднощі та методи їх усунунення при розгортанні локального хмарного сховища у віртуалізованому середовищі

З тим як можна впровадити автоматизовану систему резервного копіювання у локальному хмарному сховищі, проблема таких не виникає, оскільки вони легко виправляються і навіть якщо існують, їх можна вирішити впровадивши той чи інший метод резервного копіювання, та й в принципі він має працювати плюс-мінус нормально. Але у випадку з тим, що використовувалося та розгорталося саме локальне хмарне сховище у віртуальній машині, а саме у віртуальній машині гіпервізора другого типу VMware Workstation Player, виникають певні нюанси, оскільки при цьому втрачається частина продуктивності порівняно з фізичним сервером або сервером, який працює на гіпервізорі першого типу.

Обмеження продуктивності через віртуалізацію. Хоча існують певні обмеження продуктивності через віртуалізацію, уникнути їх повністю неможливо, оскільки навіть при виділенні всіх ресурсів системи для Nextcloud у межах віртуальної машини або встановлення його безпосередньо на фізичний сервер,

повне використання цих ресурсів не завжди гарантується. Основна проблема полягає в тому, що гіпервізор другого типу, зокрема VMware Workstation Player, додає накладні витрати на продуктивність, через що вона буде нижчою порівняно з гіпервізором першого типу.

Перше значне обмеження стосується перевантаження центрального процесора, особливо якщо віртуальні ядра CPU розподілені неефективно. У разі роботи кількох віртуальних машин або виконання додаткових навантажень на хості, може виникати конкуренція за процесорні ресурси, що призводить до зниження продуктивності Nextcloud. Одним із варіантів вирішення є застосування CPU Pinning, що дозволяє закріпити певні фізичні ядра за конкретною віртуальною машиною, а також обмеження максимальної кількості віртуальних ядер, щоб уникнути надмірної конкуренції з іншими процесами (див. рис. 3.30) [9, 27].

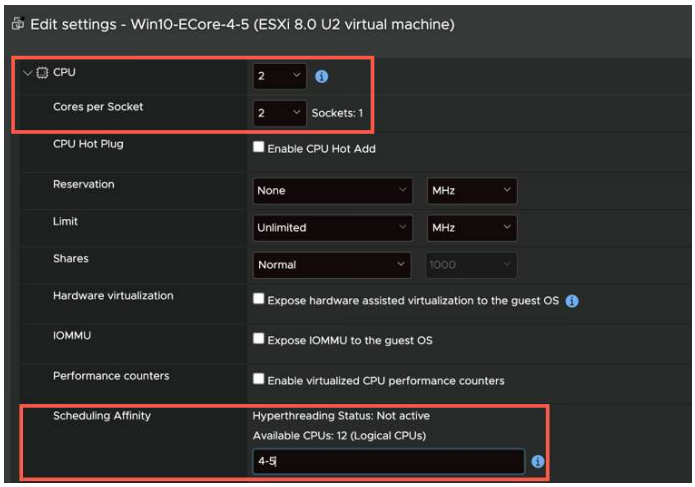


Рисунок 3.30 – Метод покращення роботи CPU через зафіксування окремих ядер (CPU Pinning) під окрему віртуальну машину [27]

Ще одним суттєвим фактором є недостатня кількість оперативної пам’яті, оскільки Nextcloud активно використовує її для кешування, обробки запитів та передачі файлів. У разі дефіциту пам’яті можуть спостерігатися зависання, уповільнення роботи або навіть аварійне завершення роботи сервісу. Для вирішення цієї проблеми варто налаштувати RAM Ballooning, що дозволить

динамічно розподіляти пам’ять між віртуальними машинами залежно від навантаження (див. рис. 3.31) [9, 28].

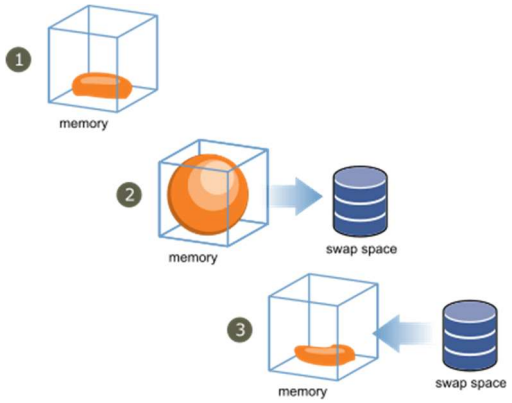


Рисунок 3.31 – Метод покращення роботи RAM через повертання невикористаної ОЗП (RAM Ballooning) [28]

Також доцільно впровадити оптимізацію кешування, встановивши APCu для PHP та додавши відповідний рядок у конфігураційний файл Nextcloud (див. рис. 3.32).



Рисунок 3.32 – Метод оптимізації кешування ОЗП через його очищення

Дискова підсистема також є потенційним вузьким місцем, особливо якщо використовується повільний HDD або навіть деякі SSD із низькою швидкістю запису. Додаткове навантаження може виникати при використанні мережевого зберігання, наприклад, через протокол SMB, оскільки він не оптимізований для роботи із файлами, що постійно змінюються та передаються між користувачами. У таких випадках найкращим рішенням буде використання NVMe-накопичувачів для

кешування та зберігання метаданих, що суттєво пришвидшить доступ до файлів. Основні дані можуть залишатися на HDD для зменшення витрат, але ZFS ARC Cache допоможе оптимізувати читання і прискорити роботу дискової підсистеми (див. рис. 3.33).

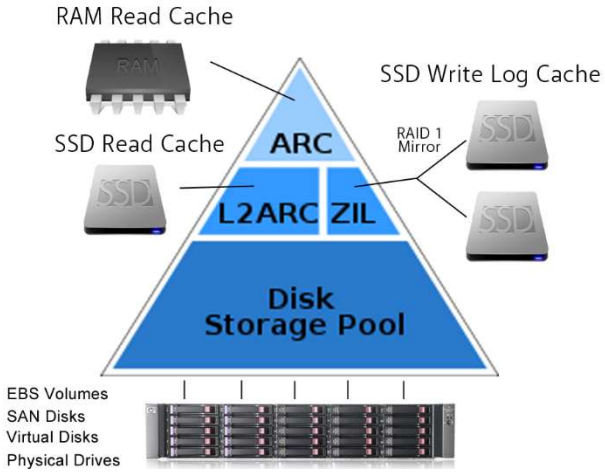


Рисунок 3.33 – Метод оптимізації читання з диску через ZFS ARC Cache [29]

Додатково можливе використання продуктивніших дискових контролерів у віртуальному середовищі, наприклад, VMware Paravirtual SCSI (PVSCSI) або ж VirtIO у випадку KVM/QEMU, що також сприятиме підвищенню швидкості обробки дискових операцій. Завдяки таким оптимізаціям можна зменшити негативний вплив віртуалізації на продуктивність і забезпечити стабільну роботу локального хмарного сховища навіть у межах гіпервізора другого типу.

Проблеми з мережею. Мережеві проблеми можуть виникати через некоректні налаштування доступу, вибір режиму мережі у віртуальному середовищі або неправильно налаштовані порти. Особливо це актуально при використанні VMware Workstation Player, коли потрібно забезпечити доступ до локального хмарного сховища та можливість його роботи у внутрішній мережі або навіть в інтернеті.

Якщо Nextcloud не виходить зробити доступним ззовні, потрібно використовувати режим мережевого моста (Bridged Mode), що дозволить отримати IP-адресу у локальній мережі (див. рис. 3.34).

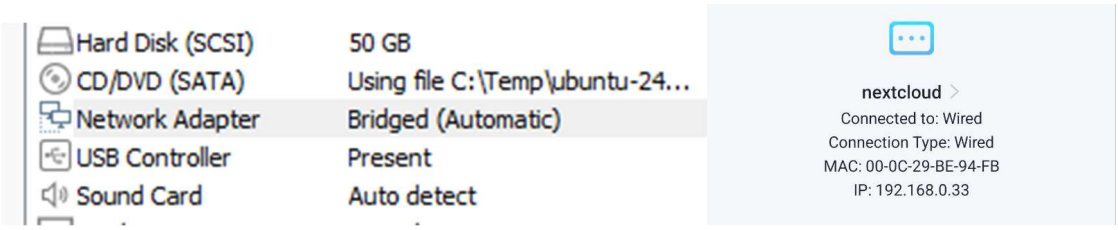


Рисунок 3.34 – Режим Bridge для використання внутрішніх фізичних локальних IP

Також важливо налаштувати статичну IP-адресу, оскільки при кожному перезавантаженні віртуальної машини або хоста маршрутизатор може видавати нову динамічну адресу, що призведе до постійних змін у конфігурації сервісів і потенційних збоїв у доступі. Для встановлення статичної IP-адреси в Linux необхідно відредагувати файл конфігурації мережі "/etc/netplan/00-installer-config.yaml" (див. рис. 3.35).

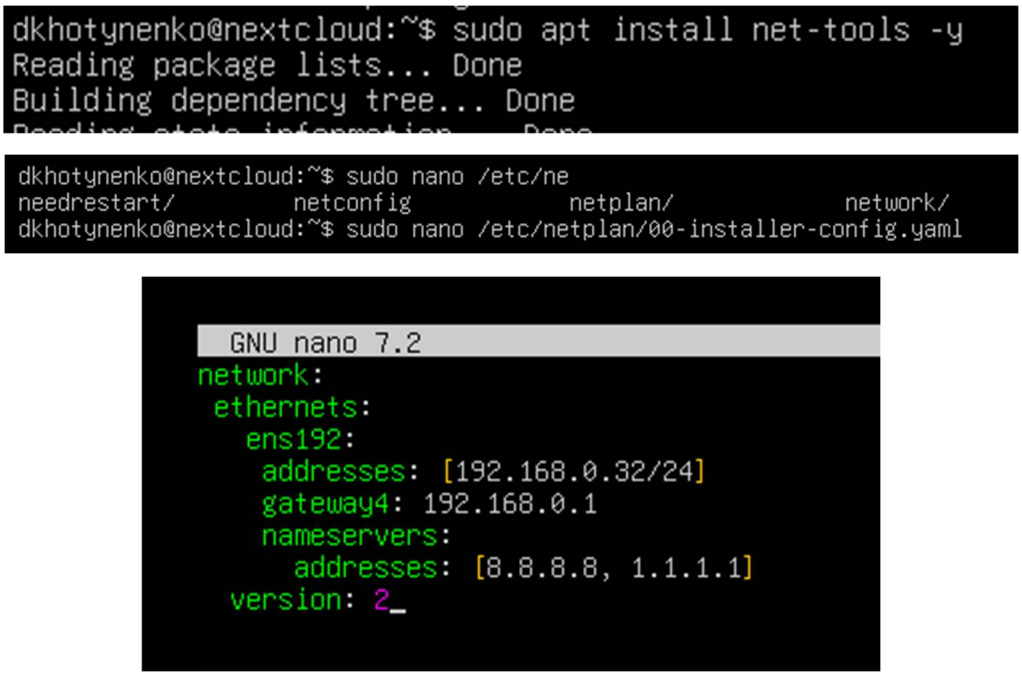


Рисунок 3.35 – Налаштування статичної IP адреси для уникнення зміни IP після перезавантаження

Після збереження змін слід застосувати нові налаштування командою "sudo netplan apply", що дозволить Nextcloud зберігати постійну IP-адресу та уникнути проблем з доступом після перезапуску (див. рис. 3.36).



Рисунок 3.36 – Застосування змін до мережевих налаштувань

Крім статичної адресації, можлива проблема з конфліктом портів, що часто виникає у віртуалізованих середовищах, коли одна IP-адреса використовується для кількох віртуальних машин або контейнерів. Якщо одна з машин вже зайняла стандартні веб-порти (80 або 443), то Nextcloud просто не зможе запустити свій веб-сервер, а відповідно, інтерфейс буде недоступним. Перевірити, чи зайняті порти іншими процесами, можна за допомогою команди "sudo netstat -tulnp" (див. рис. 3.37).

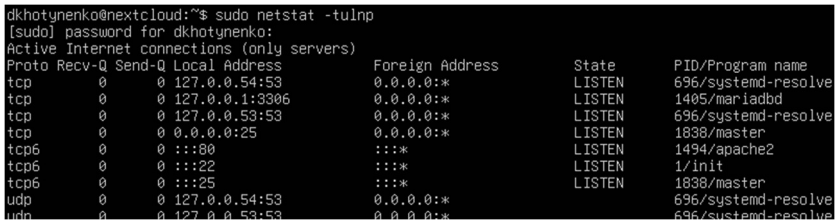


Рисунок 3.37 – Перевірка зайнятих портів перед розгортанням нового процесу

Якщо порти зайняті іншими віртуальними машинами або контейнерами, то можливі два варіанти вирішення. Перший — розподілити використання портів між різними машинами, якщо це можливо. Другий — використати реверс-проксі, що дозволить перенаправляти трафік відповідно до доменного імені або інших параметрів. У такій ситуації можна налаштувати Nginx як реверс-проксі, що особливо зручно, якщо Nextcloud вже встановлено з цим веб-сервером (див. рис. 3.38).



Рисунок 3.38 – Docker контейнери NPM (Nginx Proxy Manager)
для роботи з реверс-проксі

Ще однією причиною проблем з доступом може бути блокування мережевого трафіку файрволом, що може відбуватися через правила брандмауера, які забороняють доступ до певних портів або протоколів (див. рис. 3.39)

```
dkhotynenko@nextcloud:~$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)
dkhotynenko@nextcloud:~$ sudo ufw allow 433/tcp
Rule added
Rule added (v6)
dkhotynenko@nextcloud:~$ sudo ufw enable
Firewall is active and enabled on system startup
dkhotynenko@nextcloud:~$
```

Рисунок 3.39 – Зміна правил брандмауера у розблокуванні портів,
під якими працює Nextcloud

Після цього трафік на HTTP та HTTPS буде дозволений, що забезпечить стабільну роботу Nextcloud у мережі. Якщо після цих змін проблеми залишаються, варто перевірити налаштування маршрутизатора, зокрема NAT або Port Forwarding, якщо Nextcloud має бути доступний не лише у локальній мережі, а й з інтернету.

Управління сховищем. Nextcloud постійно зберігає дані у внутрішньому сховищі, а резервне копіювання безперервно створює резервні копії. Однією з основних проблем є обмежений дисковий простір, що може стати критичною перешкодою для роботи системи. Якщо вільне місце закінчиться, у логах почнуть з’являтися помилки про неможливість запуску певних служб, а після перезавантаження локального хмарного сховища або віртуальної машини Nextcloud може не запуститися взагалі, оскільки не матиме можливості створювати необхідні файли для роботи.

Рішенням може бути додавання нового диска до наявного пулу у VMware Workstation Player. Спершу потрібно створити новий віртуальний диск через налаштування Workstation Player (див. рис. 3.40).

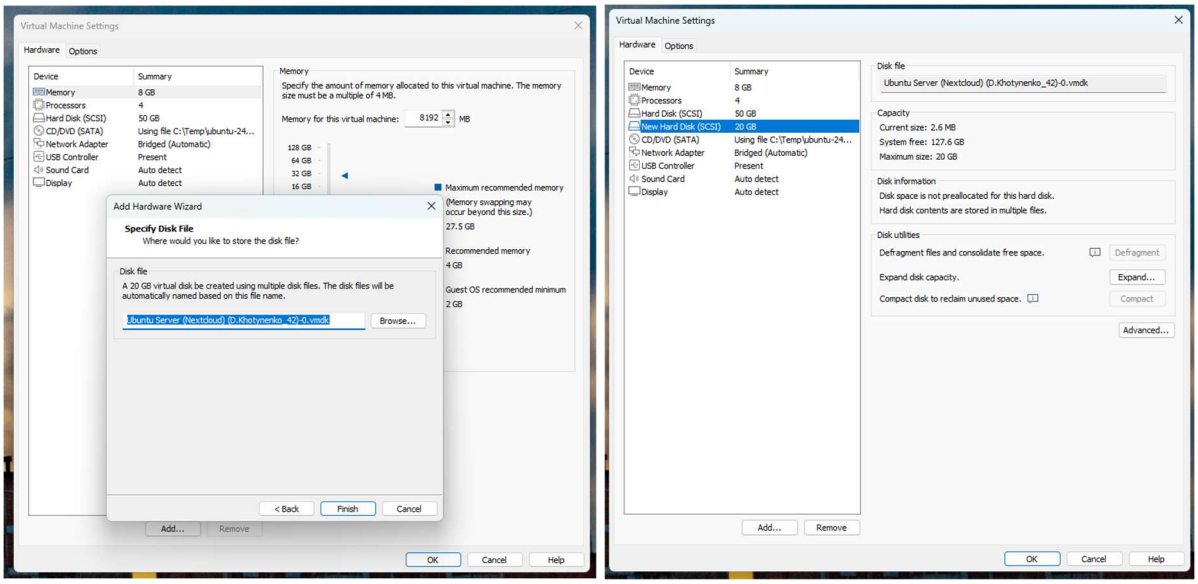


Рисунок 3.40 – Додавання нового динамічного віртуального SCSI диску до існуючої віртуальної машини у VMware Workstation Player

Після цього додати його до системи Linux та підключити до Nextcloud. Для цього спочатку необхідно ініціалізувати диск та створити на ньому файлову систему (див. рис. 3.41).

```
dkhotynenko@nextcloud:~$ lsblk
NAME                      MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda                         8:0    0  50G  0 disk
├─sda1                      8:1    0   1M  0 part
├─sda2                      8:2    0   2G  0 part /boot
└─sda3                      8:3    0  48G  0 part
  └─ubuntu--vg-ubuntu--lv 252:0    0  24G  0 lvm  /
sdb                         8:16   0  20G  0 disk
sr0                        11:0    1   3G  0 rom
dkhotynenko@nextcloud:~$ sudo gdisk /dev/sdb
GPT fdisk (gdisk) version 1.0.10

Partition table scan:
  MBR: not present
  BSD: not present
  APM: not present
  GPT: not present

Creating new GPT entries in memory.

Command (? for help): n
Partition number (1-128, default 1):
First sector (34-41943006, default = 2048) or {+-}size{KMGTP}:
Last sector (2048-41943006, default = 41940991) or {+-}size{KMGTP}:
Current type is 8300 (Linux filesystem)
Hex code or GUID (L to show codes, Enter = 8300):
Changed type of partition to 'Linux filesystem'

Command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!

Do you want to proceed? (Y/N): y
OK; writing new GUID partition table (GPT) to /dev/sdb.
The operation has completed successfully.
dkhotynenko@nextcloud:~$
```

Рисунок 3.41 – Ініціалізація нового диску та створення файлової системи

Далі його необхідно відформатувати у формат ext4 (див. рис. 3.42).

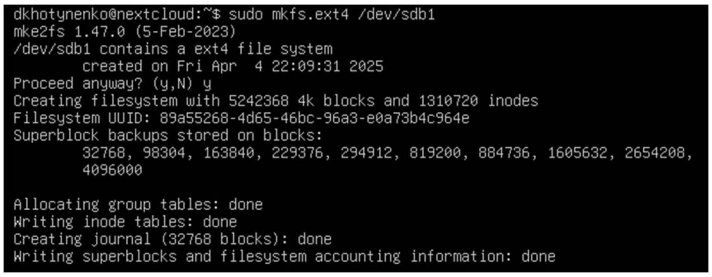


Рисунок 3.42 – Форматування нового розділу у формат ext4

Після чого змонтувати його у потрібну директорію (див. рис. 3.43).

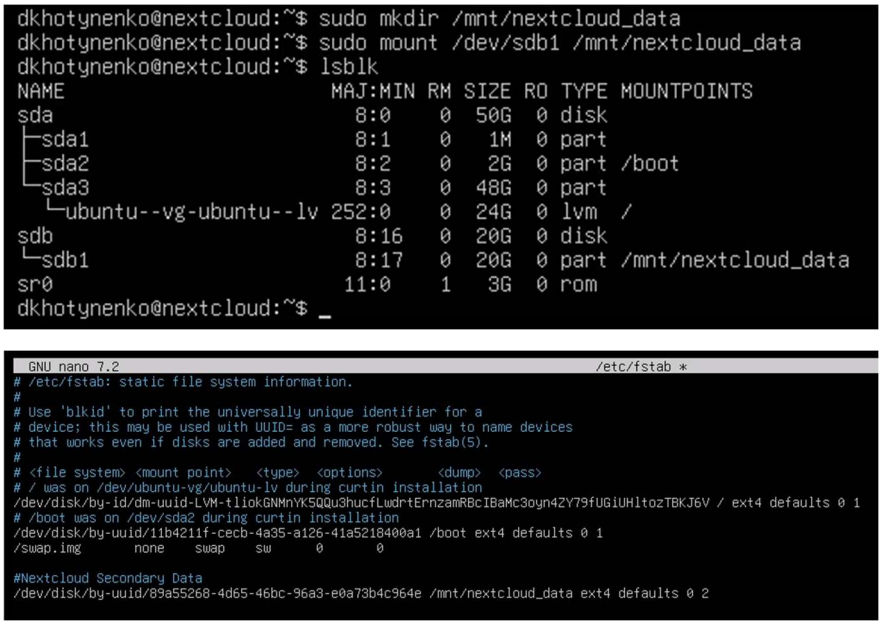


Рисунок 3.43 – Монтування нового розділа у потрібну директорію та прив’язка змонтованого диску після перезавантаження у "/etc/fstab/"

Альтернативним рішенням може бути використання хмарного S3-сховища для зберігання файлів, яке має практично необмежений масштабований простір, що дозволяє уникнути фізичних обмежень локального накопичувача, але водночас потребує правильної інтеграції з Nextcloud та налаштування відповідного з’єднання через API.

3.3 Рекомендації і перспективи впровадження

З огляду на запропоновану систему, можна зробити обґрунтовані висновки щодо доцільності впровадження локального хмарного сховища на базі Nextcloud з автоматизованою системою резервного копіювання. Застосування таких інструментів як WebDAV, rsync, BorgBackup та Cron Jobs дозволяє створити повністю контрольовану, гнучку, безпечну та недорогу альтернативу загальнодоступним сервісам, зокрема Google Drive, Dropbox чи Microsoft OneDrive.

Переваги локального рішення над загальнодоступними хмарами. Хоча популярні хмарні сервіси пропонують зручність і певну надійність, вони мають обмеження, особливо в контексті контролю над даними та безпеки. В публічних хмарах кінцевий користувач не має прямого контролю над місцем зберігання своїх файлів, політикою резервного копіювання чи безпосереднім адмініструванням сервера. У випадку критичних ситуацій або змін у політиці компанії-постачальника, дані можуть бути втрачені або заблоковані.

Локальне рішення на базі Nextcloud надає повний контроль над усіма аспектами інфраструктури: від розміщення файлів до налаштування безпеки, розкладу копіювання та моніторингу. Користувач сам визначає, які компоненти застосовувати, як розподіляти ресурси, де і як зберігати резервні копії — це критично важливо для організацій, що оперують чутливою або комерційно важливою інформацією.

На відміну від хмарних сервісів, де резервне копіювання часто є прихованою частиною інфраструктури, у Nextcloud резервне копіювання інтегрується вручну або через спеціалізовані інструменти. Наприклад, BorgBackup дозволяє реалізувати дедуплікацію, стиснення та шифрування даних на боці користувача, що підвищує захищеність і знижує обсяг збережених даних. У поєднанні з Cron Jobs та rsync, можна реалізувати ефективну інкрементальну систему резервного копіювання із розкладом, адаптованим до конкретних робочих навантажень.

Таблиця 3.2 – Порівняння запропонованої автоматизованої системи резервного копіювання у локальному хмарному сховищі

Критерій	**Nextcloud + WebDAV/rsync/Borg/Cron (запропоноване рішення)**	**Synology Hyper Backup**	**Veeam Backup & Replication**	**Seafile Pro**	**OwnCloud Enterprise**
Тип рішення	**Відкрите, модульне, кастомізоване**	Пропрієтарне, інтегроване	Пропрієтарне, орієнтоване на підприємства	Пропрієтарне/відкрите	Пропрієтарне
Контроль над системою	**Повний, з можливістю зміни всіх компонентів**	Частковий (в рамках екосистеми NAS)	Високий, але обмежений ліцензією	Середній	Середній
Гнучкість та розширюваність	**Висока (можливість додавання будь-яких сценаріїв і плагінів)**	Обмежена	Середня (через інтерфейс GUI)	Обмежена API	Обмежена
Механізми резервного копіювання	**rsync (інкрементальне), Borg (з дедуплікацією), Cron (планування)**	Інкрементальне, повне	Повне, інкрементальне, дедуплікація	Повне/інкрементальне	Повне/інкрементальне
Шифрування та безпека	**End-to-end, серверне, контроль доступу, аудит**	AES 256-біт, шифрування трафіку	AES, інтеграція з AD/LDAP	SSL/TLS, серверне	SSL/TLS, шифрування
Вартість	**Безкоштовне (крім інфраструктури)**	Обмежена безкоштовна версія	Висока вартість ліцензії	Платна Pro-версія	Комерційна ліцензія

Продовження таблиці 3.2 – Порівняння запропонованої автоматизованої системи резервного копіювання у локальному хмарному сховищі

Критерій	**Nextcloud + WebDAV/rsync/Borg/Cron (запропоноване рішення)**	**Synology Hyper Backup**	**Veeam Backup & Replication**	**Seafile Pro**	**OwnCloud Enterprise**
Автоматизація	**Повністю скриптована та налаштовується під будь-які потреби**	Через GUI, частково скриптується	Високий рівень через GUI	Середній рівень	Середній рівень
Моніторинг	**Logreader, email-сповіщення, кастомні скрипти**	Інтегрований	Інтегрований	Базовий	Базовий
Масштабованість	**Висока, завдяки кластеризації, federation, зовнішнім сховищам**	Обмежена пристроєм NAS	Висока	Обмежена	Відносно висока (в Enterprise)

Кластери та масштабованість як напрям подальшого розвитку. Із зростанням обсягу даних та потребою у високій доступності, особливо у виробничих або корпоративних середовищах, доцільним стає створення кластеризованих рішень на базі Nextcloud, що дозволить досягти як масштабованості, так і відмовостійкості: у разі збою одного з вузлів, інші можуть продовжити обслуговування користувачів або відновлення даних.

У цьому контексті варто виділити Nextcloud Federation — можливість з’єднувати кілька незалежних інстанцій Nextcloud у спільну екосистему з доступом до міжсерверного обміну даними, загального пошуку та централізованого управління користувачами, що відкриє шлях до побудови масштабованої децентралізованої хмари з гнучким керуванням та високим рівнем безпеки.

Окрему увагу в перспективі подальшого впровадження заслуговує використання сховищ на базі TrueNAS як елементів розширеного кластерного рішення. TrueNAS є потужною платформою для побудови мережевих сховищ з підтримкою ZFS, реплікації, резервного копіювання та вбудованої віртуалізації.

Інтеграція Nextcloud з TrueNAS через WebDAV або iSCSI може забезпечити розподілене, надійне і швидкодійне середовище з можливістю миттєвого масштабування.

У поєднанні з гіпервізорами першого типу (такими як Proxmox VE або VMware ESXi) така архітектура дозволяє не лише розгорнути кілька екземплярів Nextcloud у кластері, а й автоматизувати їх оновлення, балансування навантаження та відновлення після збоїв. На відміну від гіпервізорів другого типу (наприклад, VMware Workstation Player, що використовувався в цьому проєкті), гіпервізори першого типу працюють ближче до «заліза», що зменшує затримки, покращує ефективність та забезпечує вищу стабільність системи.

Рекомендації щодо впровадження в організаціях. Для малих і середніх підприємств, а також для освітніх та дослідницьких установ, впровадження Nextcloud з автоматизованим резервним копіюванням є оптимальним вибором за критеріями вартість/гнучкість/безпека.

Рекомендується наступна базова конфігурація:

— Nextcloud як основне сховище;
— BorgBackup з шифруванням і дедуплікацією для резервних копій;
— Cron Jobs для планування щоденного резервного копіювання;
— WebDAV або rsync для резервування на зовнішні носії чи інші сервери;
— Nextcloud Federation для інтеграції з іншими інстанціями у разі потреби масштабування;
— Моніторинг через Logreader, email-сповіщення, або інтеграція з Grafana/Prometheus.

Для середовищ, де важлива відмовостійкість, рекомендовано відразу передбачити кластеризацію з можливістю масштабування та додатково дослідити інтеграцію з TrueNAS або S3-сумісними сховищами, що відкриває потенціал для побудови приватної гібридної хмари.

Подальші дослідження у цьому напрямку мають бути зосереджені на:

1. Розробці кластерної архітектури на базі Nextcloud з розгортанням у Proxmox/ESXi.

2. Інтеграції AI-механізмів для прогнозування навантажень, аналізу файлів або автоматичного відновлення.

3. Тестуванні різних типів сховищ (TrueNAS, Ceph, MinIO) з точки зору швидкості, надійності, легкості інтеграції з Nextcloud.

4. Оптимізації продуктивності при зберіганні та обробці великих обсягів даних (відео, наукові архіви, резервні копії систем).

У підсумку, автоматизована система резервного копіювання у локальних хмарних сховищах на основі відкритого ПЗ не лише є ефективним способом резервного копіювання, але й стають основою побудови сучасної, масштабованої, безпечної цифрової інфраструктури незалежно від зовнішніх хмарних постачальників.

ВИСНОВКИ

У ході роботи було реалізовано локальне хмарне сховище на базі Nextcloud з автоматизованою системою резервного копіювання, що використовує WebDAV, rsync, BorgBackup і Cron Jobs, що забезпечило високу гнучкість управління даними, повний контроль над безпекою та можливість адаптації під конкретні потреби користувачів. Використання відкритого програмного забезпечення дозволило знизити витрати порівняно з комерційними хмарними сервісами.

Було протестовано процес розгортання та налагодження роботи Nextcloud у VMware Workstation Player, що продемонструвало його зручність для локального розгортання, але також виявило певні обмеження, зокрема щодо продуктивності та масштабованості. Виявлено, що для стабільної роботи з великими обсягами даних та високими навантаженнями доцільніше використовувати гіпервізори першого типу (Proxmox VE, VMware ESXi), що забезпечують кращу ефективність та відмовостійкість.

Перспективним напрямом розвитку є кластеризація Nextcloud з можливістю балансування навантаження та інтеграції з TrueNAS як мережевим сховищем, що дозволить підвищити надійність системи, зменшити ризик втрати даних та забезпечити масштабованість для підприємств різного рівня. Додатково можна досліджувати інтелектуальні алгоритми управління резервним копіюванням, які прогнозуватимуть навантаження та оптимізуватимуть ресурси.

Загалом, реалізоване рішення підтвердило, що локальні хмарні сховища є надійною та безпечною альтернативою публічним сервісам. Подальші дослідження можуть бути зосереджені на вдосконаленні автоматизації, підвищенні продуктивності та створенні повністю автономних кластерних систем, що відповідатимуть вимогам сучасного бізнесу та наукових установ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Edwards J. Choose the right automated backup system for your needs | TechTarget. Search Data Backup. URL: https://www.techtarget.com/searchdatabackup/tip/Choose-the-right-automated-backup-system-for-your-needs (дата звернення: 24.02.2025).
2. Automated vs manual backup: which to choose?. CloudAlly. URL: https://www.cloudally.com/blog/automated-vs-manual-backup-which-to-choose/ (дата звернення: 24.02.2025).
3. Automated backup: how it works & why to use it - adivi. Adivi Corporation. URL: https://adivi.com/blog/automated-backup/ (дата звернення: 25.02.2025).
4. Automated backup: how it works & why to use it | unitrends. Unitrends. URL: https://www.unitrends.com/blog/automated-backup/ (дата звернення: 27.02.2025).
5. What is ECC memory? The importance of ECC RAM in enterprise applications. Premio Inc. URL: https://premioinc.com/blogs/blog/what-is-ecc-memory-the-importance-of-ecc-ram-in-enterprise-applications (дата звернення: 28.02.2025).
6. Incremental vs differential backup - difference between data backup strategies - AWS. Amazon Web Services, Inc. URL: https://aws.amazon.com/compare/the-difference-between-incremental-differential-and-other-backups/#:~:text=A%20differential%20backup%20strategy%20only,changes%20since%20the%20last%20backup. (дата звернення: 01.03.2025).
7. The most common reasons for data loss -. - Professional Data Recovery & Backup Solution. URL: https://lostdata.com.sa/en/2021/06/07/the-most-common-reasons-for-data-loss/ (дата звернення: 02.03.2025).
8. What are the types of ransomware?. Akamai. URL: https://www.akamai.com/glossary/what-are-the-types-of-ransomware (дата звернення: 05.03.2025).
9. About nextcloud. Nextcloud. URL: https://nextcloud.com/about/ (дата звернення: 07.03.2025).
10. Collabora vs ONLYOFFICE. all mine!. URL: https://blog.jospoortvliet.com/2020/06/collabora-vs-onlyoffice.html (дата звернення: 09.03.2025).
11. JoshDW19. Blog - nextcloud and truenas collaborate to help you build your private cloud. TrueNAS Community. URL: https://www.truenas.com/community/threads/nextcloud-and-truenas-collaborate-to-help-you-build-your-private-cloud.95869/ (дата звернення: 11.03.2025).
12. Cloud storage comparison: google drive, onedrive, dropbox, & nextcloud -. Custom Development, Digital Marketing, & IT Services | CPS. URL: https://www.cpsmi.com/blog/cloud-storage-comparison-google-drive-onedrive-dropbox-nextcloud/ (дата звернення: 12.03.2025).
13. Accessing Nextcloud files using WebDAV – Nextcloud latest User Manual latest documentation. Nextcloud Documentation. URL:

https://docs.nextcloud.com/server/latest/user_manual/en/files/access_webdav.html (дата звернення: 13.03.2025).

14. Clients and Client APIs – Nextcloud latest Developer Manual latest documentation. Nextcloud Documentation. URL: https://docs.nextcloud.com/server/latest/developer_manual/client_apis/index.html (дата звернення: 15.03.2025).

15. Configuring federation sharing – nextcloud latest administration manual latest documentation. Nextcloud Documentation. URL: https://docs.nextcloud.com/server/latest/admin_manual/configuration_files/federated_cloud_sharing_configuration.html (дата звернення: 17.03.2025).

16. GeeksforGeeks. RAID (redundant arrays of independent disks) - geeksforgeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/raid-redundant-arrays-of-independent-disks/ (дата звернення: 18.03.2025).

17. An intro to the GUI – syncthing documentation. Welcome to Syncthing's documentation! – Syncthing documentation. URL: https://docs.syncthing.net/intro/gui.html (дата звернення: 21.03.2025).

18. Getting started: 6 efficient ways of sharing your folder (or file) - ownCloud. ownCloud. URL: https://owncloud.com/news/getting-started-sharing-6-ways/ (дата звернення: 27.03.2025).

19. Seafile - open source file sync and share software. Seafile - Open Source File Sync and Share Software. URL: https://www.seafile.com/en/features/ (дата звернення: 30.03.2025).

20. Pydio cells overview. Pydio. URL: https://pydio.com/en/pydio-cells/overview (дата звернення: 02.04.2025).

21. WebDAV. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/iis/configuration/system.webserver/webdav/ (дата звернення: 06.04.2025).

22. Rsync. linux.die.net. URL: https://linux.die.net/man/1/rsync (дата звернення: 08.04.2025).

23. Backup to (and restore from) the cloud with Borg and Rclone | Linux Things. Blog | Linux Things. URL: https://linuxthings.co.uk/blog/backup_to_the_cloud_with_borg_and_rclone (дата звернення: 12.04.2025).

24. Aduramimo. How to setup cronjobs for a Laravel project. DEV Community. URL: https://dev.to/dreywandowski/how-to-setup-cronjobs-for-a-laravel-project-2li2 (дата звернення: 15.04.2025).

25. How to Install Nextcloud on TrueNAS - WunderTech. WunderTech. URL: https://www.wundertech.net/how-to-install-nextcloud-on-truenas/ (дата звернення: 17.04.2025).

26. End-to-End encryption meaning, example & security. Wallarm | Advanced API Security. URL: https://www.wallarm.com/what/what-is-end-to-end-encryption (дата звернення: 25.04.2025).

27. Experimenting with ESXi CPU affinity and Intel Hybrid CPU Cores. WilliamLam.com. URL: https://williamlam.com/2024/01/experimenting-with-esxi-cpu-affinity-and-intel-hybrid-cpu-cores.html (дата звернення: 30.04.2025).

28. How memory (RAM) management works on VMware ESXi 6.7 - VMware - Tutorials. InformatiWeb Pro. URL: https://us.informatiweb-pro.net/virtualization/vmware/vmware-esxi-6-7-how-memory-ram-management-works.html (дата звернення: 02.05.2025).

29. Features Of ZFS - Technical Blogs from Sparksupport free complete details regarding ZFS for beginners & pro. Technical Blogs from Sparksupport. URL: https://sparksupport.com/blog/features-of-zfs-complete-guide-for-learners/ (дата звернення: 04.05.2025).

30. Хотиненко Д.В. Дослідження автоматизації резервного копіювання у локальних хмарних сховищах. «Проблеми комп'ютерної інженерії»: Науково-практ. конф., м.Київ, 3 грудня 2024 р. С.175-177.

31. Хотиненко Д.В., Волохін В.В. Автоматизація резервного копіювання у локальних хмарних інфраструктурах. «Сучасний стан та перспективи розвитку IoT» : VI Науково-техн. конф., м.Київ, 15 квітня 2025 р. (подано до публікації).

Додаток А

Код сценарію автоматизації резервного копіювання в хмару через WebDAV і rsync з логуванням

```
#!/bin/bash

# Path to the Local Folder to Be Copied
SOURCE_DIR="$HOME/Documents/"

# Path to Mounted WebDAV Storage
DEST_DIR="$HOME/nextcloud_backup/"

# Log File for Process Tracking
LOG_FILE="$HOME/backup_webdav.log"

echo "$(date) - Starting Backup..." >> "$LOG_FILE"

# Backing Up Using Rsync
rsync -avz "$SOURCE_DIR" "$DEST_DIR" >> "$LOG_FILE"
2>&1

if [ $? -eq 0 ]; then
    echo "$(date) - Backup Completed Successfully" >>
"$LOG_FILE"
else
    echo "$(date) - Error During Backup" >>
"$LOG_FILE"
fi
```

Додаток Б

Код сценарію автоматизації резервного копіювання в хмару з логуванням і сповіщенням на email

```
#!/bin/bash

# Path to the Local Folder to Be Copied
SOURCE_DIR="/home/dkhotynenko/Documents/"

# Path to Destination Folder on Cloud Storage
DEST_DIR="/var/www/html/nextcloud/data/dkhotynenko/fil
es/backup/"

# Log File for Process Tracking
LOG_FILE="/home/dkhotynenko/backup_rsync_mail.log"

# Email for Success or Error Messege
ADMIN_EMAIL="st7197042@stud.duikt.edu.ua"

echo "$(date) - Starting Backup..." >> "$LOG_FILE"

# Backing Up Using Rsync
rsync -avz "$SOURCE_DIR" "$DEST_DIR" >> "$LOG_FILE"
2>&1

if [ $? -eq 0 ]; then
    echo "$(date) - Backup Completed Successfully" >>
"$LOG_FILE"
    echo "Backup Success" | mail -s "Backup Alert"
"$ADMIN_EMAIL" 2>> "$LOG_FILE"
else
    echo "$(date) - Error During Backup" >>
"$LOG_FILE"
    echo "Backup Failed" | mail -s "Backup Alert"
"$ADMIN_EMAIL" 2>> "$LOG_FILE"
fi
```

Додаток В

Код розгортання Nginx Proxy Manager зі сертифікацією Let`s Encrypt (через Docker Compose)

```
version: '3'
services:
  app:
    image: 'jc21/nginx-proxy-manager:latest'
    ports:
      - '80:80'
      - '81:81'
      - '443:443'
    environment:
      DB_MYSQL_HOST: "db"
      DB_MYSQL_PORT: 3306
      DB_MYSQL_USER: "npm"
      DB_MYSQL_PASSWORD: "12345678"
      DB_MYSQL_NAME: "npm"
    volumes:
      - ./data:/data
      - ./letsencrypt:/etc/letsencrypt
  db:
    image: 'jc21/mariadb-aria:latest'
    environment:
      MYSQL_ROOT_PASSWORD: '12345678'
      MYSQL_DATABASE: 'npm'
      MYSQL_USER: 'npm'
      MYSQL_PASSWORD: '12345678'
    volumes:
      - ./mysql:/var/lib/mysql
```

Додаток Г

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра Комп'ютерної інженерії



КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавра

НА ТЕМУ: «АВТОМАТИЗОВАНА СИСТЕМА РЕЗЕРВНОГО КОПІЮВАННЯ У ЛОКАЛЬНИХ ХМАРНИХ СХОВИЩАХ»

Виконав студент групи КІД-42
Хотиненко Данііл Володимирович
Керівник дипломної роботи:
Волохін Віталій Васильович,
канд. техн. наук, доц.

Київ – 2025

Мета, об’єкт, предмет дослідження

Мета роботи – оптимізація процесів резервного копіювання в локальних хмарних сховищах за рахунок використання методів автоматизації та відкритих програмних рішень

Об’єкт дослідження – процеси резервного копіювання в локальних хмарних сховищах

Предмет дослідження – методи та технології автоматизації резервного копіювання в локальних хмарних сховищах

Актуальність роботи

У роботі розглянуто особливості автоматизації резервного копіювання в локальних хмарних сховищах як ефективну альтернативу традиційним ручним і пропрієтарним рішенням. Акцент зроблено на використанні інструментів з відкритим кодом, зокрема Nextcloud у поєднанні з WebDAV, rsync, BorgBackup та Cron Jobs. Описано архітектуру сховища, методи шифрування, дедуплікації та моніторингу, що забезпечують збереження даних без втручання користувача.

На основі практичного впровадження у віртуальному середовищі VMware проаналізовано ключові труднощі та переваги запропонованої системи. Порівняно з загальнодоступними сервісами, локальне рішення дозволяє краще контролювати доступ, підвищити безпеку та гнучко адаптувати систему під конкретні потреби організації.

Недоліки традиційних ручних та пропрієтарних рішень для резервного копіювання

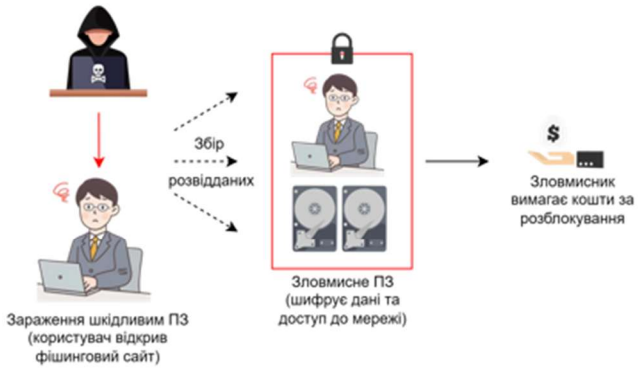


Рис. 1.7 – Блокування традиційних незахищених систем шляхом проникнення зловмисного ПЗ



Рис. 1.25 – Труднощі у забезпеченні безпеки та відповідності: підвищення складний незахищений невпорядкований доступ та легкий захищений упорядкований доступ



Рис. 1.24 – Труднощі у зберіганні та керуванні даними: хмарне, мережеве та зовнішнє сховища



Рис. 1.26 – Труднощі у інтеграції у існуючу інфраструктуру: розгалдужнена Cloud-based та локальна інфраструктура

Особливість впровадження автоматизації резервного копіювання



Рис. 1.2 – Процес налагодження автоматизованого резервного копіювання

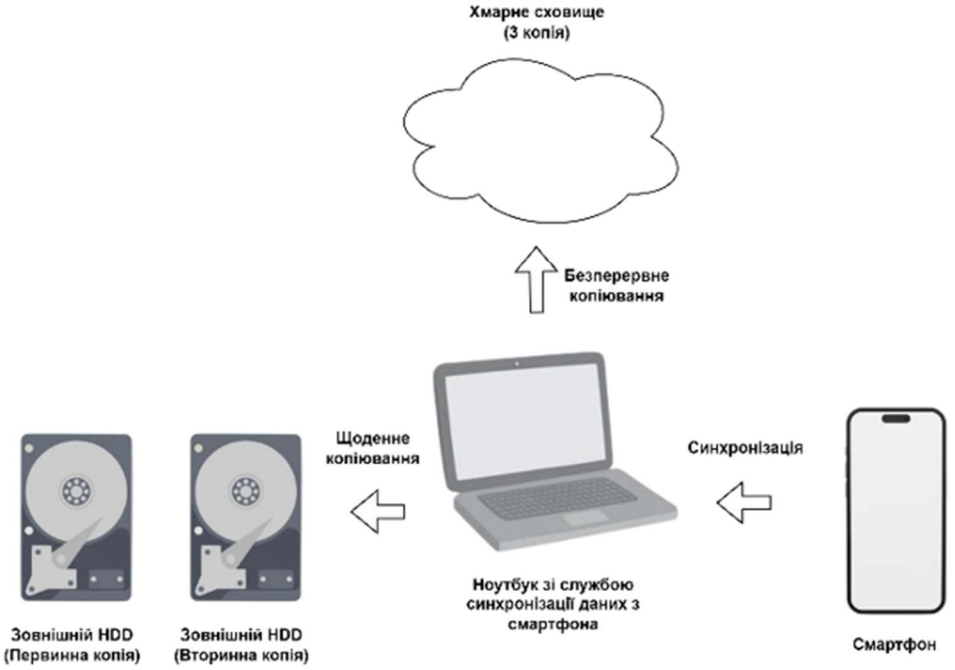


Рис. 1.3 – Безперервне резервне копіювання зі інтегрованим механізмом перевірки цілосності даних

Архітектура автоматизованої системи резервного копіювання у локальне хмарне сховище

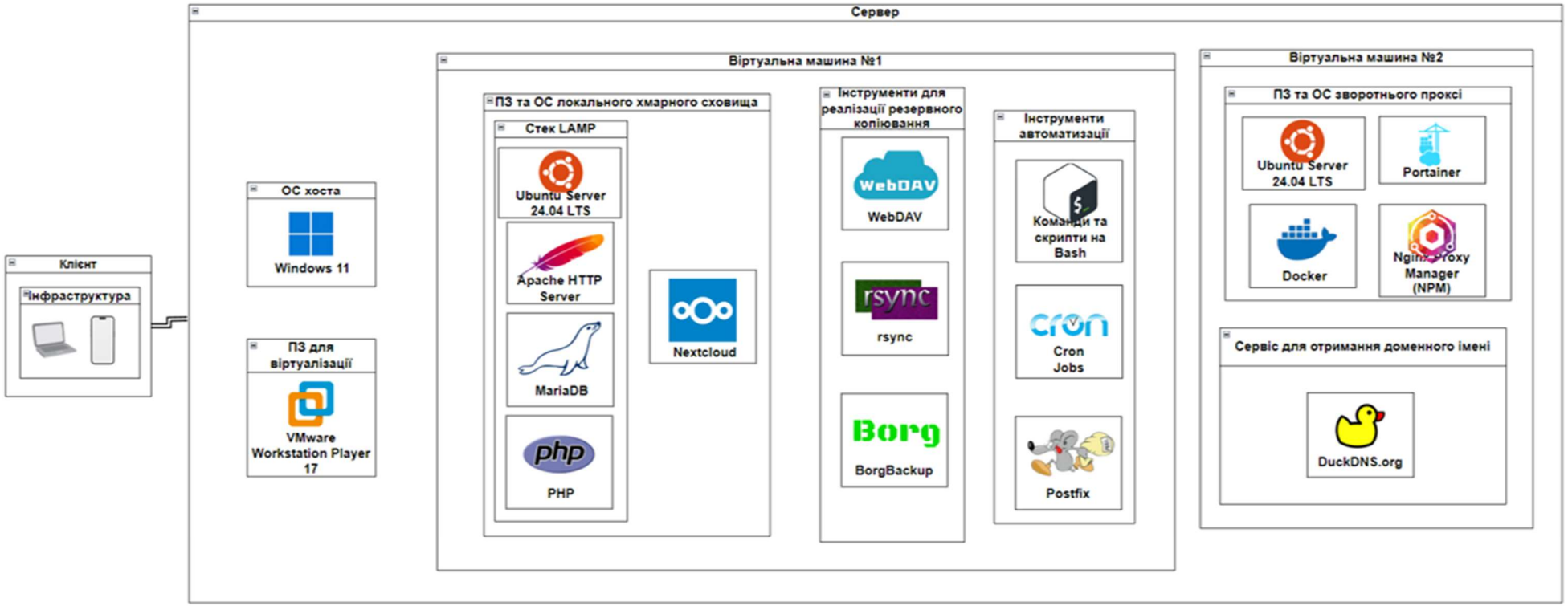


Рис. 2.22 – Схема автоматизованої системи резервного копіювання у локальне хмарне сховище

Алгоритм роботи автоматизованої системи резервного копіювання у локальне хмарне сховище

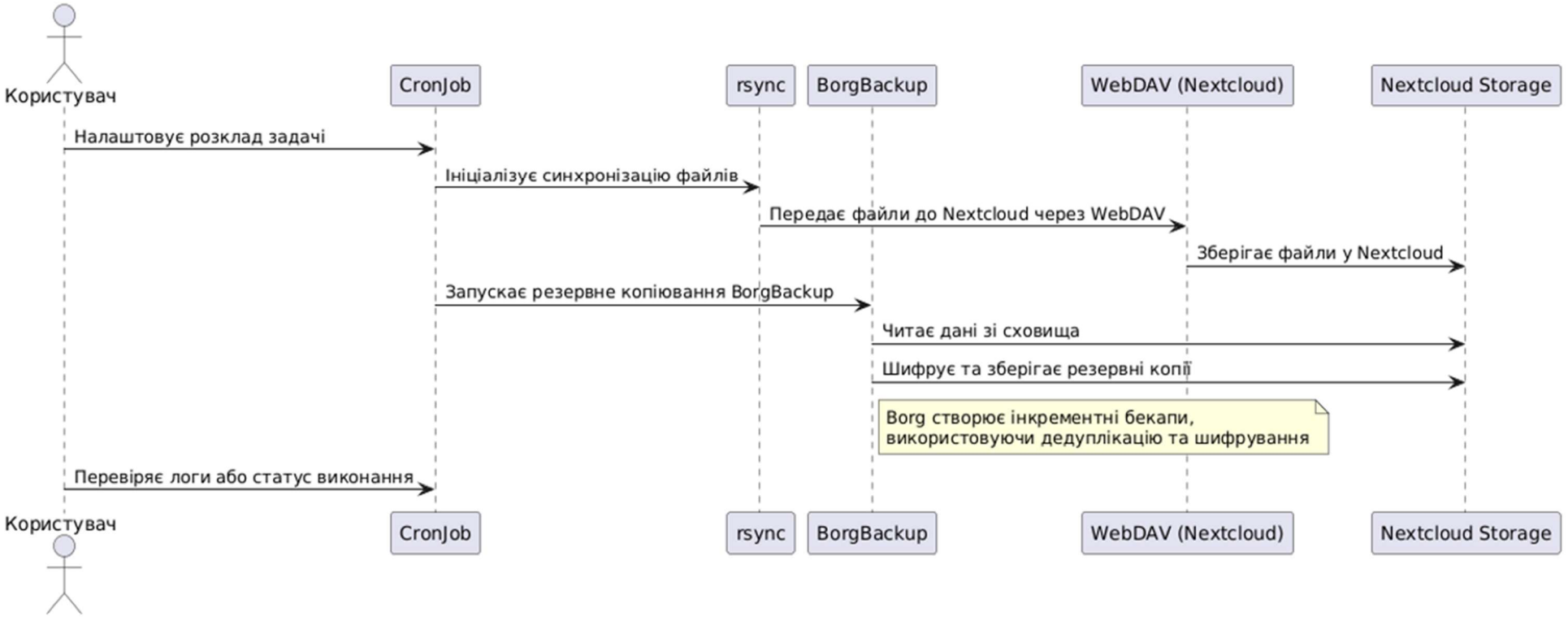
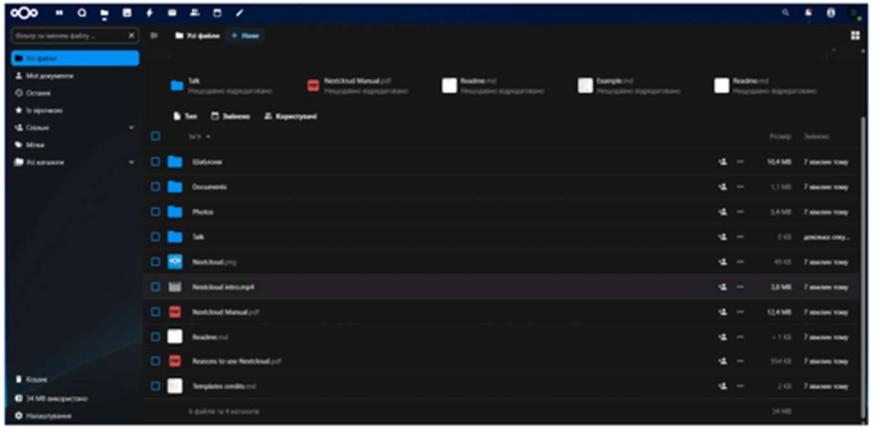


Рис. 2.15 – Алгоритм автоматизованого резервного копіювання з використанням Cron, rsync, BorgBackup та WebDAV у локальне хмарне сховище Nextcloud

Демонстрація локального хмарного сховища Nextcloud



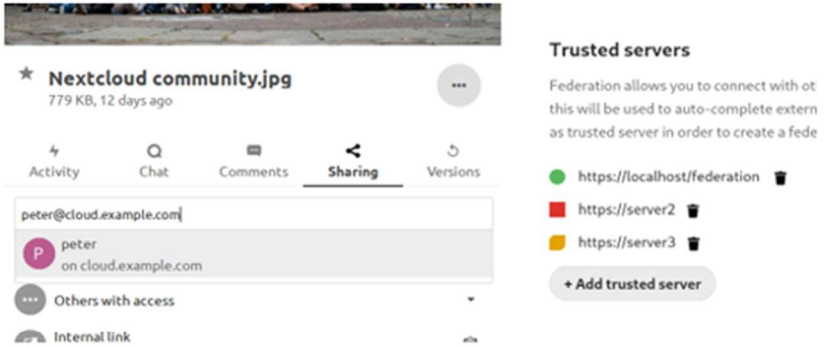


Рис. 1.19 – Консолідація декількох екземплярів Nextcloud: функція Federated Cloud Sharing

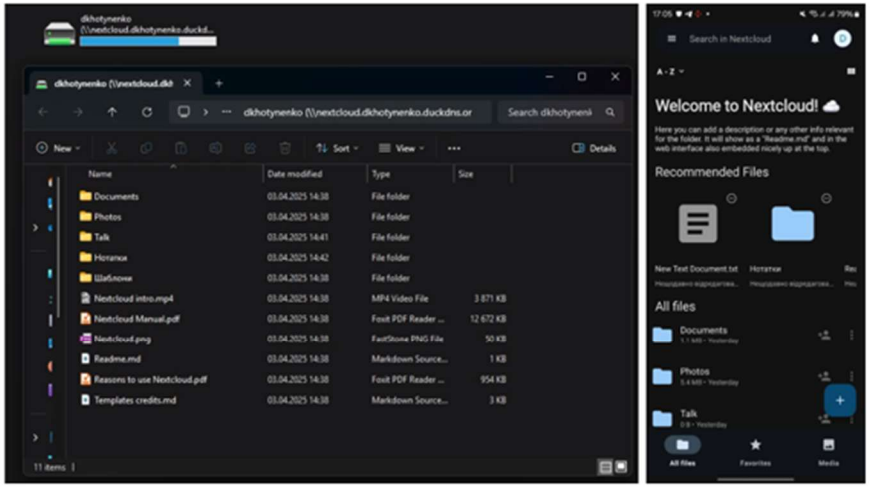


Рис. 2.8 – Взаємодія з даними ПЗ Nextcloud: веб-інтерфейс, мережевий диск, мобільний додаток

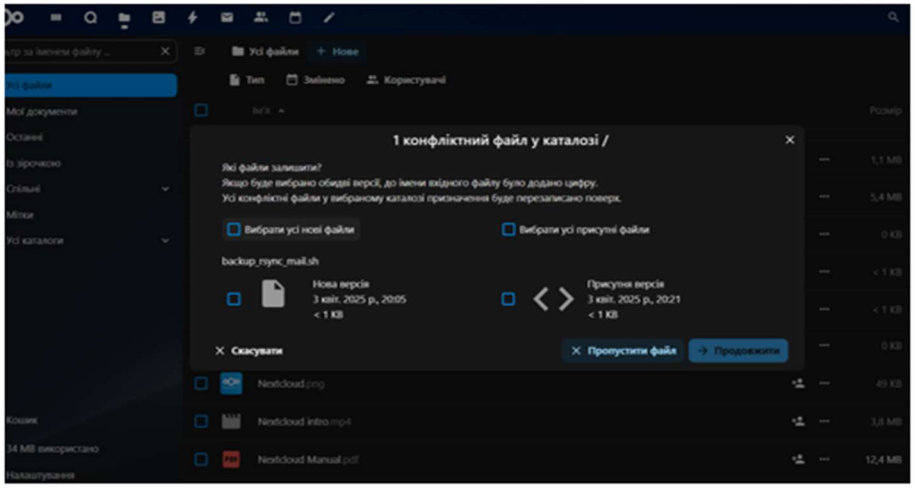


Рис 2.9 – Взаємодія з даними ПЗ Nextcloud: надання спільного доступу та контроль версій

Інструменти резервного копіювання: WebDAV, rsync, BorgBackup

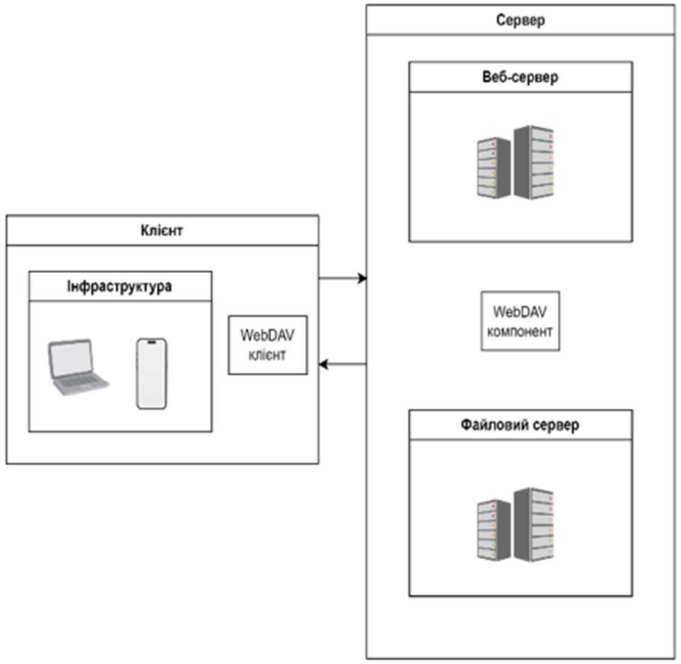


Рис. 2.10 – Взаємодія з даними ПЗ Nextcloud: принцип роботи протоколу WebDAV



Рис. 2.11 – Взаємодія з даними ПЗ Nextcloud: принцип роботи rsync

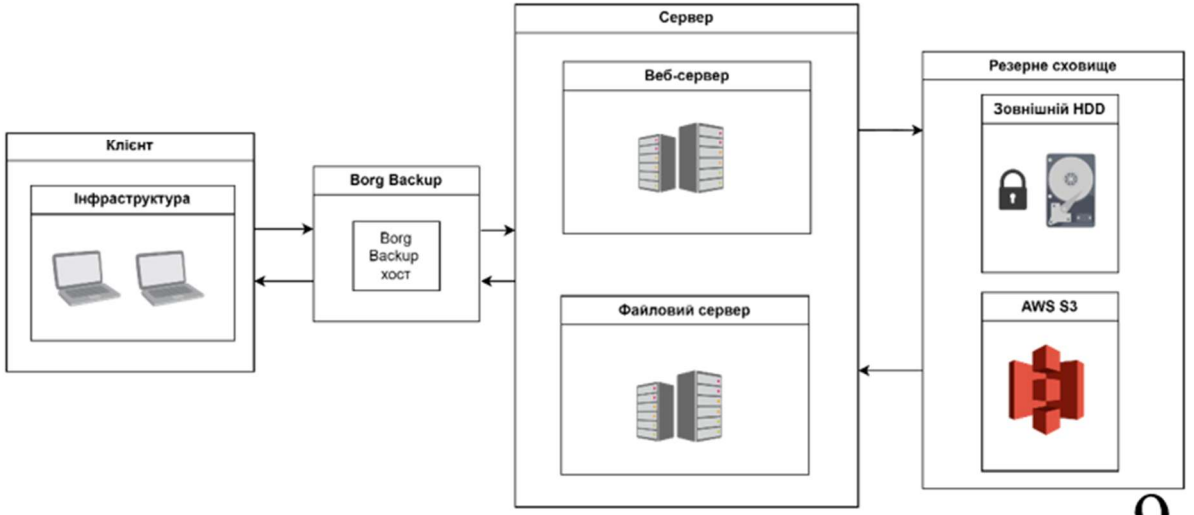


Рис. 2.12 – Взаємодія з даними ПЗ Nextcloud: принцип роботи BorgBackup

Демонстрація методу резервного копіювання через WebDAV і rsync з логуванням

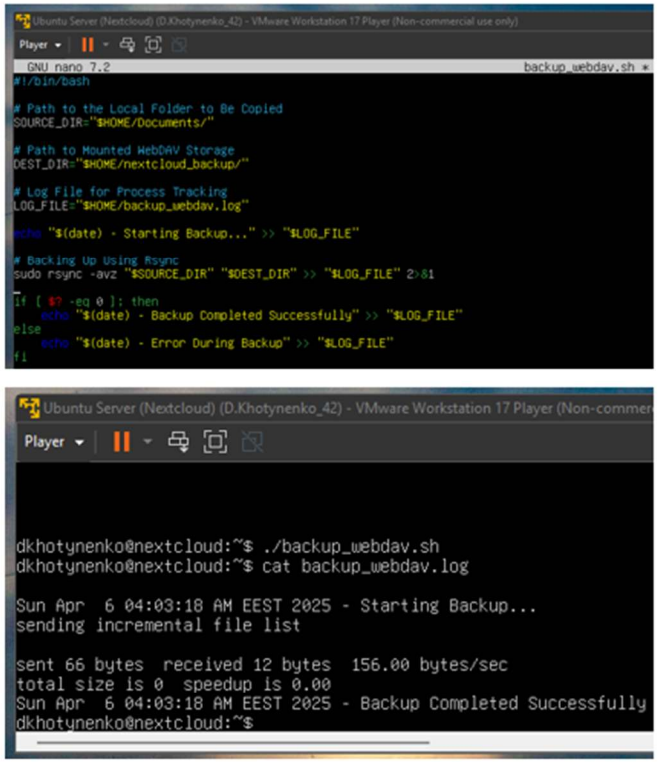


Рис. 3.6 – Сценарій автоматизації резервного копіювання в хмару через WebDAV і rsync з логуванням

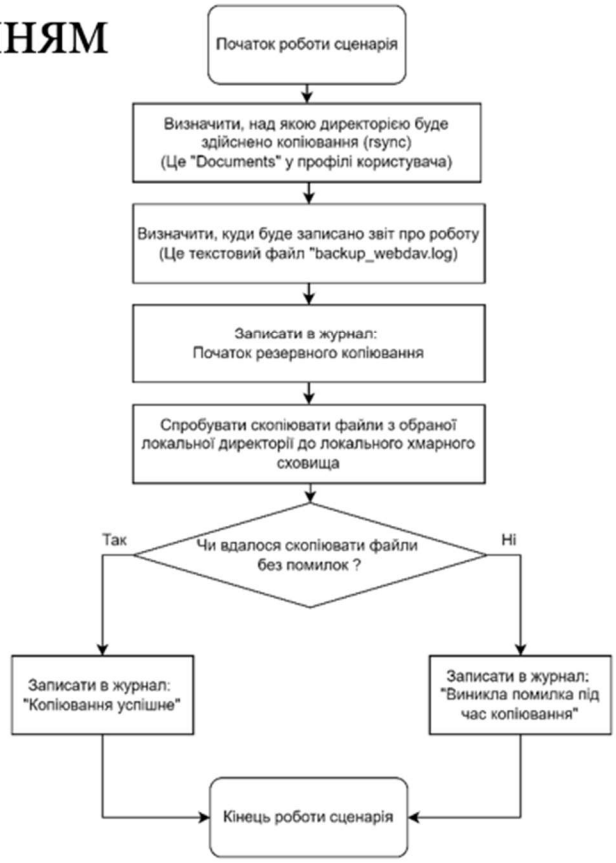


Рис. 3.7 – Метод резервного копіювання у Nextcloud через WebDAV і rsync із логуванням

Демонстрація резервного копіювання з логуванням і email-сповіщенням

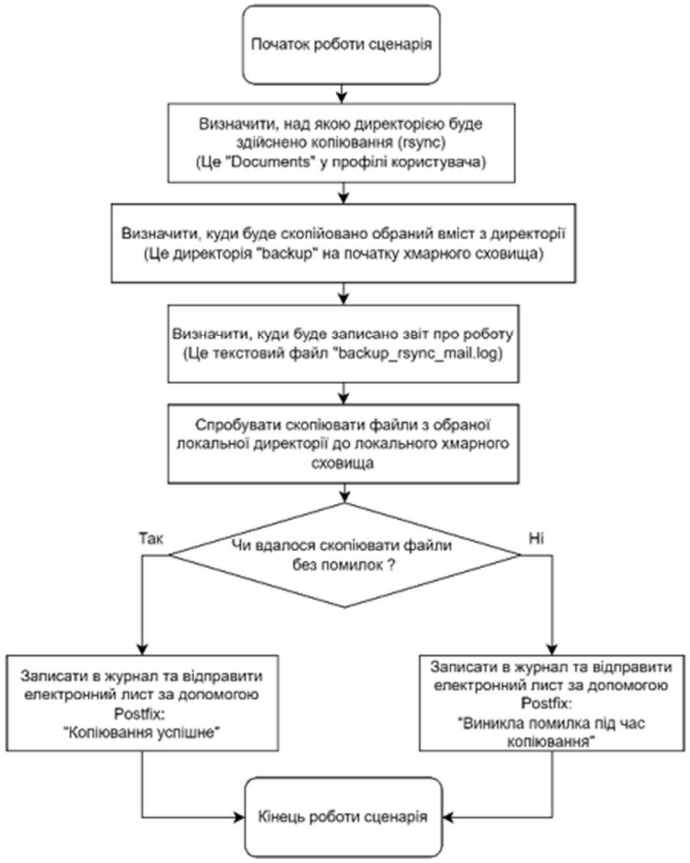


Рис. 3.25 – Метод резервного копіювання з логуванням і email-сповіщенням у системі автоматизації резервного копіювання

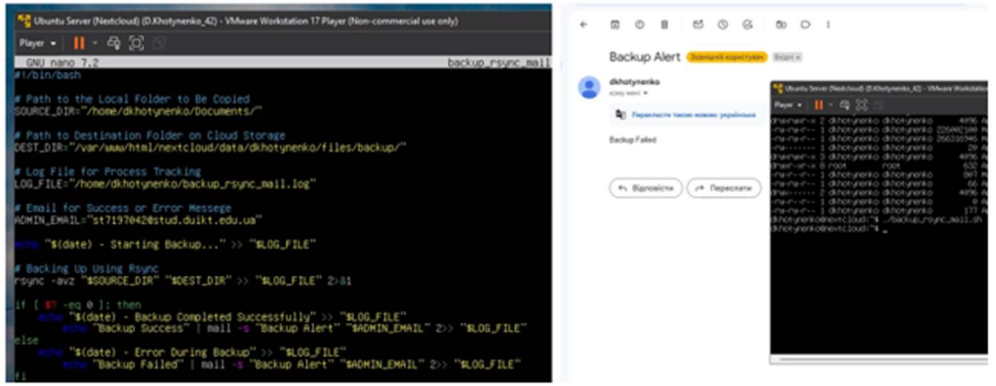


Рис. 3.23 – Сценарій автоматизації резервного копіювання в хмару з логуванням і сповіщенням на email через Postfix (навмисно-невірний сценарій)

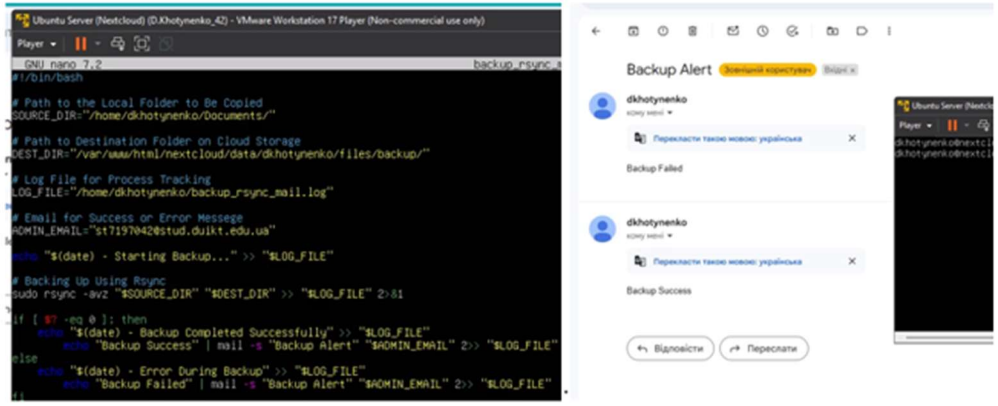


Рис. 3.24 – Сценарій автоматизації резервного копіювання в хмару з логуванням і сповіщенням на email через Postfix (вірний сценарій)

Демонстрація методу автоматизованого резервного копіювання через Cron Job

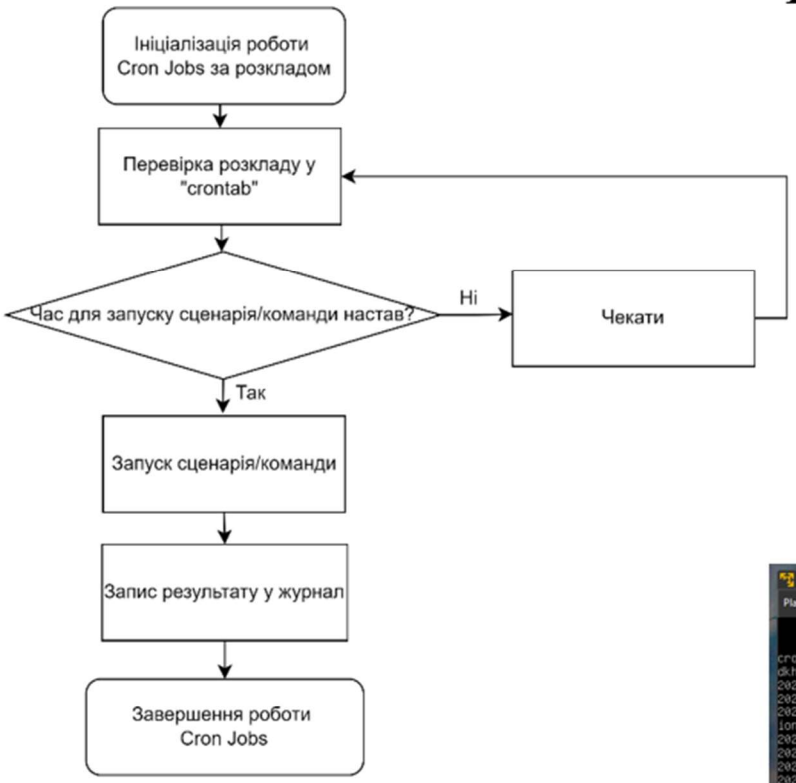


Рис. 2.14 – Метод автоматизованого виконання сценаріїв резервного копіювання через Cron Job

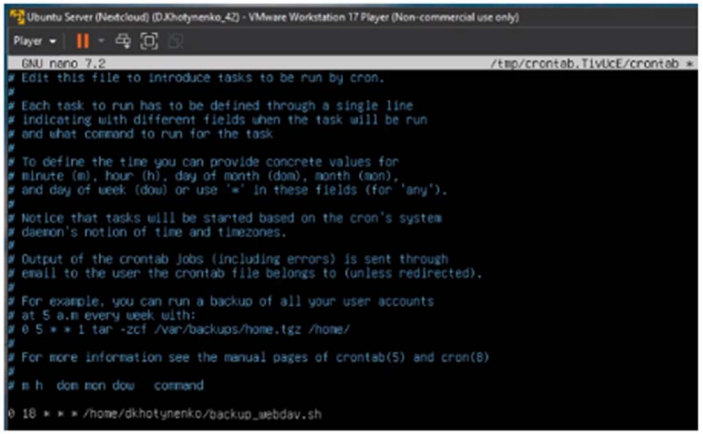


Рис. 3.8 – Активація сценарія "backup_webdav.sh" через cron jobs: графік виконання – кожен день, о 18:00

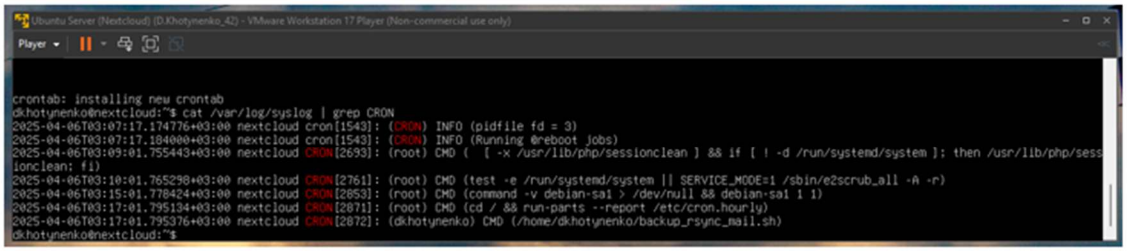


Рис. 3.15 – Реалізація перегляду логів Cron Jobs про резервне копіювання rsync за допомогою "grep"

Порівняння автоматизованої системи резервного копіювання у локальному хмарному сховищі

Табл. 3.2 – Порівняння запропонованої автоматизованої системи резервного копіювання у локальному хмарному сховищі

Критерій	**Nextcloud + WebDAV/rsync/Borg/Cron (запропоноване рішення)**	**Synology Hyper Backup**	**Veeam Backup & Replication**	**Seafile Pro**	**OwnCloud Enterprise**
Тип рішення	**Відкрите, модульне, кастомізоване**	Пропрієтарне, інтегроване	Пропрієтарне, орієнтоване на підприємства	Пропрієтарне/відкрите	Пропрієтарне
Контроль над системою	**Повний, з можливістю зміни всіх компонентів**	Частковий (в рамках екосистеми NAS)	Високий, але обмежений ліцензією	Середній	Середній
Гнучкість та розширюваність	**Висока (можливість додавання будь-яких сценаріїв і плагінів)**	Обмежена	Середня (через інтерфейс GUI)	Обмежена API	Обмежена
Механізми резервного копіювання	**rsync (інкрементальне), Borg (з дедуплікацією), Cron (планування)**	Інкрементальне, повне	Повне, інкрементальне, дедуплікація	Повне/інкрементальне	Повне/інкрементальне
Шифрування та безпека	**End-to-end, серверне, контроль доступу, аудит**	AES 256-біт, шифрування трафіку	AES, інтеграція з AD/LDAP	SSL/TLS, серверне	SSL/TLS, шифрування
Вартість	**Безкоштовне (крім інфраструктури)**	Обмежена безкоштовна версія	Висока вартість ліцензії	Платна Pro-версія	Комерційна ліцензія
Автоматизація	**Повністю скриптована та налаштовується під будь-які потреби**	Через GUI, частково скриптується	Високий рівень через GUI	Середній рівень	Середній рівень
Моніторинг	**Logreader, email-сповіщення, кастомні скрипти**	Інтегрований	Інтегрований	Базовий	Базовий
Масштабованість	**Висока, завдяки кластеризації, federation, зовнішнім сховищам**	Обмежена пристроєм NAS	Висока	Обмежена	Відносно висока (в Enterprise)

Висновки

У ході роботи було створено локальне хмарне сховище на базі Nextcloud з автоматизованою системою резервного копіювання, що поєднує WebDAV, rsync, BorgBackup і Cron Jobs. Рішення забезпечило гнучке управління даними, високу безпеку та адаптивність до потреб користувача, а використання відкритого ПЗ дозволило знизити витрати.

Розгортання у VMware Workstation Player продемонструвало зручність, але виявило обмеження щодо продуктивності. Для стабільної роботи з великими навантаженнями доцільніше використовувати гіпервізори першого типу. Перспективи розвитку включають кластеризацію, інтеграцію з TrueNAS і впровадження інтелектуального управління резервним копіюванням.

Публікації та апробація роботи

1. Хотиненко Д.В. Дослідження автоматизації резервного копіювання у локальних хмарних сховищах. «Проблеми комп'ютерної інженерії»: Науково-практ. конф., м.Київ, 3 грудня 2024 р. С.175-177.
2. Хотиненко Д.В., Волохін В.В. Автоматизація резервного копіювання у локальних хмарних інфраструктурах. «Сучасний стан та перспективи розвитку IoT» : VI Науково-техн. конф., м.Київ, 15 квітня 2025 р. (подано до публікації).