

Міністерство освіти і науки України
Державний заклад
«Луганський національний університет імені Тараса Шевченка»

Навчально-науковий інститут математики та інформаційних технологій
Кафедра інформаційних технологій та систем

Самотіс Сергій Іванович

Створення навчального середовища у VMware vCenter


кваліфікаційна робота

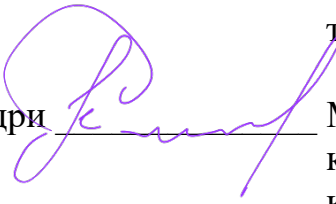
здобувача вищої освіти другого (магістерського) рівня

освітньої програми «Комп'ютерні мережі»

за спеціальністю 123 Комп'ютерна інженерія

Особистий підпис  Сергій САМОТИС

Науковий керівник  Геннадій МОГИЛЬНИЙ,
кандидат технічних наук, доцент
кафедри інформаційних технологій
та систем

Завідувач кафедри  Микола СЕМЕНОВ,
кандидат педагогічних наук, доцент
кафедри інформаційних технологій
та систем

АНОТАЦІЯ

Самотіс Сергій Іванович

Тема: Створення навчального середовища у VMware vCenter.

Спеціальність: 123 «Комп'ютерна інженерія»

Установа: ЛНУ імені Тараса Шевченка, 2026р.

Об'єкт дослідження: Процес організації хмарної інфраструктури та систем віртуалізації

Предмет дослідження: Методи та засоби розгортання навчального середовища на базі платформи VMware vCenter із забезпеченням захищеного доступу.

Метою роботи є підвищення ефективності практичної підготовки фахівців з комп'ютерних технологій шляхом проектування та реалізації навчального віртуалізованого середовища на базі платформи VMware vCenter із забезпеченням централізованого керування та захищеного доступу.

Результати роботи.

Проаналізовано сучасний стан технологій віртуалізації, та надано аналіз платформ VMware vSphere різних версій. Досліджено архітектурні особливості компонентів vSphere, зокрема гіпервізора ESXi та сервера керування vCenter, розроблено та обґрунтовано архітектуру навчального віртуалізованого середовища, інтегрованого з корпоративною службою каталогів Microsoft Active Directory, спроектовано та впроваджено модель контролю доступу (RBAC), адаптовану під специфіку навчального процесу

Ключові слова. Віртуальна система, ESX, vCenter, VMware vSphere операційна система, домен Microsoft, навчальний процес, навчальна лабораторія, рольова модель доступу.

ABSTRACT

Samotis Serhiy

Theme Creating a training environment in VMware vCenter.

Speciality: 123 "Computer Engineering"

Institution: Luhansk Taras Shevchenko National University (LTSNU), 2026.

The article of research: The process of organizing cloud infrastructure and virtualization systems

Subject of research: Methods and means of deploying a training environment based on the VMware vCenter platform with secure access.

The purpose of the work is to increase the efficiency of practical training of specialists in computer technologies by designing and implementing a training virtualized environment based on the VMware vCenter platform with centralized management and secure access.

Results of the work.

The current state of virtualization technologies is analyzed, and an analysis of VMware vSphere platforms of different versions is provided. The architectural features of vSphere components, in particular the ESXi hypervisor and the vCenter management server, are studied, the architecture of a training virtualized environment integrated with the corporate directory service Microsoft Active Directory is developed and substantiated, an access control model (RBAC) is designed and implemented, adapted to the specifics of the training process

Keywords. Virtual system, ESX, vCenter, VMware vSphere operating system, Microsoft domain, educational process, educational laboratory, role-based access model.

	Міністерство освіти і науки України
	Державний заклад «Луганський національний університет імені Тараса Шевченка»
Факультет (інститут)	Інститут математики та інформаційних технологій <small>(повна назва)</small>
Кафедра	Інформаційних технологій та систем <small>(повна назва)</small>
Галузь знань	12, Інформаційні технології <small>(код, назва)</small>
Напрямок підготовки (спеціальність)	123 «Комп'ютерна інженерія» <small>(код, назва)</small>

ЗАВДАННЯ
на кваліфікаційну роботу освітньо-кваліфікаційного рівня
« магістр »
(назва рівня)

Студенту	Самотісу Сергію Івановичу <small>(прізвище, ім'я, по батькові)</small>
Керівник кваліфікаційної роботи	Могильний Геннадій Анатолійович <small>(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)</small>

1. Тема роботи Створення навчального середовища у VMware vCenter

затверджена наказом по університету _____

2. Термін подання студентом закінченої роботи на кафедрі _____

3. Вихідні дані до роботи У результаті виконання роботи необхідно
дослідити типи та види віртуалізації, провести аналіз розвитку систем віртуалізації,
надати інформацію, щодо особливостей системи, розглянути особливості VMware
vSphere (Broadcom), запропонувати підходи до створення віртуального середовища
(визначаються кількісні або (та) якісні показники, яким повинен відповідати об'єкт розробки)

4. Зміст пояснювальної записки (перелік питань, що їх належить розробити)
Загальний аналіз систем віртуалізації, особливості архітектури та ліцензування
огляд гіпервізора VMware ESXi (vSphere), Огляд vSphere та компоненту vCenter
Аутентифікації у vCenter, безпеки, контроль доступу, створення середовища

(визначаються назви розділів або (та) перелік питань, які повинні увійти до тексту ПЗ)

5. Індивідуальний план виконання кваліфікаційної роботи

№	Заходи	Термін виконання
1.	Вибір теми роботи, вивчення наукової літератури, затвердження теми та керівника.	До 30 жовтня 2023
2.	Аналіз літературних джерел за темою роботи. Розробка ТЗ. Розробка та апробація методики дослідно-експериментальної роботи. Подання структури теоретичної частини роботи (пояснювальної записки) та плану експериментальних досліджень.	Другий тиждень жовтня 2024
3.	Робота над теоретичною частиною. Подання теоретичної частини роботи для першого читання керівником. Розробка методики тестування	До 1 грудня 2024
4.	Усунення зауважень, урахування рекомендацій керівника. Аналіз структури програмного забезпечення.	Перший тиждень грудня 2024
5.	Поетапний аналіз та обговорення результатів. Перевірка стану виконання роботи.	Перший тиждень грудня 2024
6.	Урахування рекомендацій керівника, усунення недоліків, підготовка варіанта роботи до передзахисту. Оформлення документації до проекту.	До 15 грудня 2024
7.	Попередній захист роботи на кафедрі.	За місяць до державної атестації
8.	Доопрацювання роботи з урахуванням рекомендацій після передзахисту. Розробка презентації. Підготовка графічних матеріалів. Перевірка на плагіат. Подання роботи науковому керівникові та рецензентові на підготовку відгуку та рецензії	За 10 днів до державної атестації
9.	Подання на кафедру остаточного варіанта роботи, з відгуком керівника і рецензена.	За 3 дні до державної атестації

ЗМІСТ

Вступ.....	9
Розділ 1. Загальний аналіз систем віртуалізації.....	13
1.1 Загальний аналіз рівнів корпоративного віртуального середовища	13
1.2 Перший рівень – серверна віртуалізація (Hypervisors);	15
VMware vSphere (Broadcom).....	16
Microsoft Hyper-V (Azure Stack HCI)	18
Proxmox VE / KVM-based рішення	19
Екосистема Xen (Citrix Hypervisor / XCP-ng).....	21
Рішення на базі OpenStack	23
Висновки по розділу	24
Розділ 2. Огляд архітектури та ліцензування	27
2.1 Огляд архітектури ліцензування VMware by Broadcom	27
Концептуальна трансформація корпоративної стратегії	27
Архітектура управління: vCenter Server	29
Мережева віртуалізація та безпека – NSX	30
Призупинення систем vSphere Standard та Essentials.....	30
Модернізація гіпервізора ESXi та вимоги до апаратної частини	31
Роль VMware Tanzu в сучасній інфраструктурі	31
Економічні аспекти експлуатації vSAN	31
Приблизний аналіз ліцензій – загальні цінові діапазони (MSRP)	32
2.2 Огляд архітектури ліцензування Omnisia Horizon	34
Концептуальна трансформація корпоративної стратегії	34
Основні компоненти Omnisia Horizon: Архітектурний рівень	35
Додаткові компоненти та інфраструктурне забезпечення.....	36
Глибока архітектура управління: On-Premise vs Cloud.....	38
Модернізація доставки додатків: Глибоке занурення в App Volumes	38
Перелік програмних компонентів за версіями та їх особливості	39
Компоненти, що потребують окремого ліцензування (Зовнішні покупки)	41

Приблизний аналіз ліцензій – загальні цінові діапазони.....	43
Розділ 3. Розгортання віртуального навчального середовища.....	46
3.1 Повний огляд гіпервізора VMware ESXi (vSphere)	46
Детальний огляд версій	48
Еволюція компонента ESXi	49
Послідовність встановлення (Step-by-Step)	53
Остаточне налаштування	54
3.2 Огляд vSphere – компонент vCenter	57
Архітектура та Версії.....	57
Розвиок архітектури (VCSA)	58
Вимоги до апаратної частини (Sizing)	61
Попередні вимоги (Prerequisites) до початку встановлення	61
Послідовність встановлення	62
3.3 Аутентифікації у vCenter – основа для корпоративного доступу.....	65
Аналіз vCenter Single Sign-On (SSO)	67
Джерела ідентифікації (Identity Sources)	68
Політики безпеки	70
Двофакторна аутентифікація (2FA)	71
3.4 Архітектура безпеки, контроль доступу – основа налаштування віртуального середовища	73
Управління доступом та Рольова Модель (Identity & Access Management)	74
Архітектура Дерев Інвентарю (Inventory Trees Model).....	76
Управління криптографічними ключами (Key Management & Encryption)	80
vSphere Trust Authority (vTA) та автоматизація.....	81
3.5 Опис створення віртуального навчального середовища.....	83
Головні ідея створення навчального середовища	83
Загальна послідовність дій створення віртуального навчального середовища	85
Опис процесу створення віртуального середовища.....	86

Висновки до розділу	98
Загальні висновки.....	100
Список літературних джерел	102
Додатки.....	106
Додаток А. Копії екранів процесу встановлення ESX 7	106
Додаток Б Копії екранів процесу налаштувань у ESXi 7.....	109
Додаток В. Копії екранів процесу встановлення vCenter 7	112

ВСТУП

В умовах стрімкої цифровізації та переходу бізнес-процесів у хмарні середовища, технології віртуалізації стали фундаментальною складовою сучасної ІТ-інфраструктури. На сьогоднішній день платформа VMware vSphere є де-факто промисловим стандартом у галузі корпоративної віртуалізації, забезпечуючи надійність, масштабованість та гнучкість управління ресурсами центрів обробки даних.

Актуальність дослідження зумовлена наявним розривом між теоретичною підготовкою фахівців у закладах вищої освіти та реальними потребами ринку праці. Роботодавці вимагають від випускників не лише знання архітектури віртуалізації, але й практичних навичок адміністрування, розгортання кластерів та управління віртуальними мережами. Проте розгортання фізичних лабораторних стендів для кожного студента є фінансово затратним та складним в обслуговуванні завданням.

Створення навчального середовища на базі VMware vCenter вирішує цю проблему, дозволяючи реалізувати концепцію хмарного навчального полігону. Критично важливою перевагою такого підходу є забезпечення повноцінного віддаленого доступу до лабораторних потужностей. В умовах поширення дистанційних та змішаних форм навчання, можливість працювати з інфраструктурою підприємства через веб-інтерфейс (vSphere Client) з будь-якої точки світу набуває особливого значення.

Використання vCenter Server дозволяє забезпечити безперервність навчального процесу: Студенти отримують цілодобовий доступ до навчального середовища незалежно від графіку роботи фізичних лабораторій університету, що сприяє самостійній роботі та глибшому засвоєнню матеріалу. Крім того, при певних налаштуваннях vCenter може гарантувати безпеку та ізоляцію: Виконання складних налаштувань відбувається у віртуальному просторі, що усуває ризики пошкодження основного обладнання, навіть при віддаленому підключенні через VPN або захищений шлюз.

З іншого боку vCenter дозволяє оптимізувати використання ресурсів за рахунок технології консолідації серверів ефективно розподіляти обчислювальні потужності між багатьма віддаленими користувачами одночасно.

Таким чином, розробка навчального середовища у VMware vCenter із можливостями керованого доступу є важливим науково-практичним завданням. Воно дозволяє адаптувати навчальний процес до сучасних викликів, забезпечуючи мобільність студентів та високу якість практичної підготовки.

Об'єкт дослідження: Процес організації хмарної інфраструктури та систем віртуалізації

Предмет дослідження: Методи та засоби розгортання навчального середовища на базі платформи VMware vCenter із забезпеченням захищеного доступу.

Метою роботи є підвищення ефективності практичної підготовки фахівців з комп'ютерних технологій шляхом проектування та реалізації навчального віртуалізованого середовища на базі платформи VMware vCenter із забезпеченням централізованого керування та захищеного доступу.

Для досягнення поставленої мети необхідно вирішити такі **завдання**:

1. Провести аналіз сучасних технологій віртуалізації, порівняти існуючі програмні рішення (гіпервізори 1-го та 2-го типів)
2. Провести аналіз сучасного стану процесу ліцензування VMware by Broadcom та Omnisia Horizon.
3. Дослідити архітектуру та функціональні можливості компонентів VMware vSphere, зокрема гіпервізора ESXi та сервера керування vCenter, а також визначити апаратні вимоги для їх розгортання.
4. Розробити архітектуру навчального середовища, спроектувати мережеву топологію та схему взаємодії компонентів, включаючи

інтеграцію з MS AD для організації безпечного підключення користувачів.

5. На засадах практичного використання кластера віртуалізації: встановити та хостів ESXi, інсталиувати архітектуру навчального середовища у vCenter Server Appliance (VCSA), налаштувати дата-центри, кластери та віртуальні мережі.

Методи дослідження. У роботі використано комплекс загальнонаукових та спеціальних методів:

- аналіз літературних джерел та документації – для вивчення стану проблеми та можливостей платформи VMware;
- системний аналіз – для проектування архітектури навчального середовища як цілісної системи;
- експериментальний метод – для практичного розгортання, налаштування та тестування працездатності системи у реальних умовах.

Інноваційна новизна одержаних результатів полягає в удосконаленні підходу до організації лабораторних практикумів з дисциплін адміністрування мереж шляхом інтеграції промислового рішення VMware vCenter у навчальний процес з адаптацією налаштувань безпеки та доступу під специфіку дистанційного навчання. Запропоновано модель доступу, що поєднує інформаційні ресурси інституту за допомогою використання Ms AD.

Практичне значення одержаних результатів. Розроблене навчальне середовище готове до впровадження у навчальний процес кафедри інформаційних технологій та систем. Воно дозволяє студентам набувати практичних навичок розгортання віртуальних машин, використання віртуальних комутаторів без ризику пошкодження основної інфраструктури інституту. Створена система може бути масштабована та використана для проведення курсів підвищення кваліфікації.

Робота складається з трьох розділів. У **першому розділі** проведено детальний огляд концепції віртуалізації, її типів та ролі в сучасній ІТ-індустрії. Зроблено огляд існуючих рівнів віртуалізації. Здійснено аналіз першого рівня віртуалізації, аналіз провідних платформ віртуалізації (VMware vSphere, Microsoft Hyper-V, Proxmox VE, Citrix Hypervisor) за критеріями функціональності та зручності адміністрування.

У **другому розділі** особливості структури та системи ліцензування основних складових навчального середовища. Описано особливості VMware by Broadcom, архітектура управління: vCenter Server, Основні компоненти Omnisia Horizon, Архітектурний рівень, додаткові компоненти та інфраструктурне забезпечення Omnisia Horizon

У **третьому розділі** розглянуто технічні характеристики та принципи роботи ключових компонентів обраної платформи. Детально описано архітектуру гіпервізора ESXi, роль сервера управління vCenter Server та його компонентів (Platform Services Controller). Визначено апаратні вимоги до серверного обладнання для забезпечення стабільної роботи навчального кластера. Наведено практична реалізація навчального середовища у VMware vCenter описано поетапний процес розгортання системи. Наведено алгоритм встановлення та базового налаштування гіпервізора ESXi, процес розгортання віртуального модуля vCenter Server Appliance (VCSA). Детально висвітлено процес створення основних структур навчального середовища.

РОЗДІЛ 1. ЗАГАЛЬНИЙ АНАЛІЗ СИСТЕМ ВІРТУАЛІЗАЦІЇ

1.1 Загальний аналіз рівнів корпоративного віртуального середовища

Період 2024–2026 років став не просто етапом еволюції, а поворотним моментом для індустрії корпоративної віртуалізації. Ринок, що десятиліттями функціонував в умовах технологічної гегемонії VMware, зіткнувся з тектонічними зрушеннями після поглинання компанії корпорацією Broadcom [1]. Ця подія стала каталізатором глобального перегляду ІТ-стратегій, змушуючи CIO (Chief Information Officers) переходити від тактики "працює — не чіпай" до стратегії активного управління ризиками.

Ключові фактори змін стратегії корпоративної віртуалізації та їхні наслідки (рис. 1.1):

1. Ліцензійний шок та TCO (Total Cost of Ownership): Скасування безстрокових (perpetual) ліцензій та примусовий перехід на модель передплати за ядрами процесора (per-core subscription) кардинально змінили фінансову модель ІТ. Для багатьох компаній це призвело до зростання операційних витрат (OPEX) на 300–500%. Бюджети, які раніше виділялися на цифрову трансформацію та інновації, тепер "з'їдаються" підтримкою існуючого статус-кво інфраструктури. Це створює "технічний борг" нового типу — фінансовий.

2. Консолідація продуктів та спрощення портфоліо: Примусове пакетування (bundling), коли клієнтам доводиться купувати повні стеки рішень (наприклад, VMware Cloud Foundation, що включає vSAN, NSX, Aria), навіть якщо їм потрібен лише базовий гіпервізор vSphere Standard, змусило бізнес шукати більш модульні альтернативи. Малий та середній бізнес, який раніше використовував безкоштовну версію ESXi Free (нині скасовану), опинився у вакуумі рішень.

3. Технологічний суверенітет та безпека: Компанії прагнуть зменшити залежність від закритих пропрієтарних екосистем (Vendor Lock-in).

Спостерігається виражений тренд на "репатріацію" даних із публічних хмар назад у локальні ЦОД (On-Premise) на базі Open Source рішень. Це дозволяє повернути повний контроль над SLA, фізичним розташуванням даних та політиками безпеки, що є критичним в умовах геополітичної нестабільності [8].

КЛЮЧОВІ ФАКТОРИ ЗМІН СТРАТЕГІЇ КОРПОРАТИВНОЇ ВІРТУАЛІЗАЦІЇ ТА ЇХНІ НАСЛІДКИ



Рис. 1.1 Фактори зміни стратегії

Поточний тренд — це побудова **гібридних, гетерогенних середовищ**, що поєднують локальні високопродуктивні кластери на базі KVM/Xen для постійних навантажень із гнучкістю публічних хмар для пікових навантажень (Cloud Bursting) та Disaster Recovery.

Відомо, що сучасна корпоративна інформаційна система складається з трьох рівнів віртуалізації (рис. 1.2):

- Рівень 1: Серверна віртуалізація (Hypervisors);
- Рівень 2: Віртуалізація робочих місць (VDI);
- Рівень 3: Контейнеризація (Modern Apps).

СУЧАСНА КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА: ТРИ РІВНІ ВІРТУАЛІЗАЦІЇ

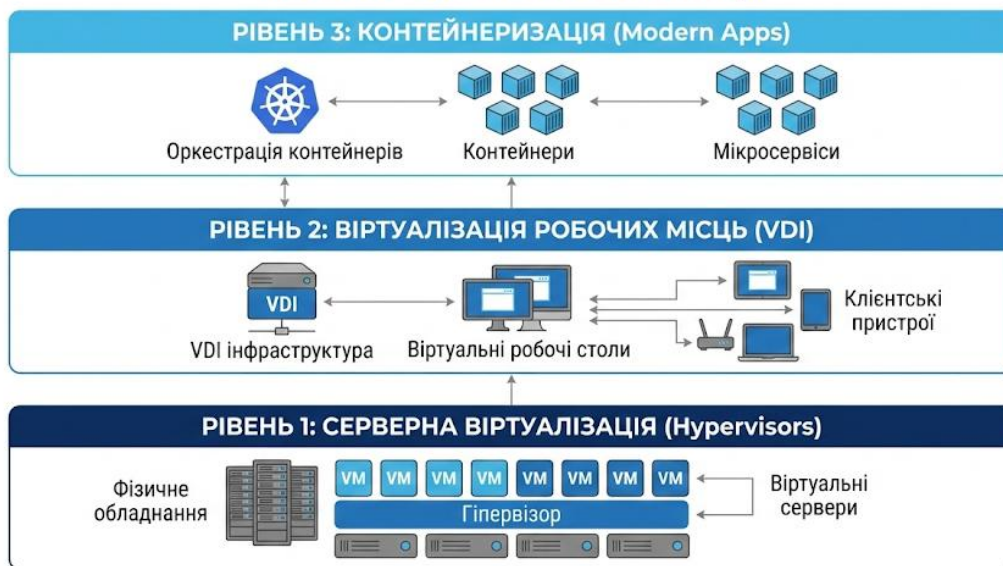


Рис. 1.2 Рівні віртуалізації

1.2 Перший рівень – серверна віртуалізація (Hypervisors);

Гіпервізор — це фундамент, що визначає не лише продуктивність обчислень, а й операційну модель роботи ІТ-відділу, вимоги до кваліфікації персоналу, сумісність із апаратним забезпеченням та стратегію резервного копіювання. В цей час існує декілька варіантів рішення для серверної віртуалізації (рис. 1.3):

- VMware vSphere (Broadcom);
- Microsoft Hyper-V (Azure Stack HCI);
- Proxmox VE / KVM-based рішення;
- Екосистема Xen (Citrix Hypervisor / XCP-ng);
- Рішення на базі OpenStack.



Рис.1.3 Серверна віртуалізація

VMware vSphere (Broadcom)

Традиційний лідер та стандарт "Enterprise" де-факто, на якому виросло ціле покоління системних адміністраторів та архітекторів [1] (рис.1.4).

Технічні переваги та унікальні можливості VMware vSphere (Broadcom):

- **DRS (Distributed Resource Scheduler)**: Неперевершений алгоритм балансування навантаження. Він не просто переміщує VM при нестачі ресурсів, а прогнозує навантаження, аналізує метрики CPU/RAM/Network у реальному часі, запобігаючи проблемі "шумних сусідів" (noisy neighbors) та забезпечуючи QoS (Quality of Service) для критичних додатків.
- **Екосистема та API**: Це головний "якір" платформи. 99% всіх систем резервного копіювання (Veeam, Commvault, Rubrik), моніторингу (Zabbix, Datadog, Dynatrace) та інформаційної безпеки розробляються та тестуються насамперед під vSphere. API VMware (VADP) — найбільш зрілий, стабільний та документований на ринку.
- **NSX**: Найпотужніша платформа програмно-визначених мереж (SDN) та мережевої безпеки. Вона дозволяє реалізувати мікросегментацію

(розподілений firewall на рівні vNIC кожної VM), що критично важливо для захисту від горизонтального переміщення (lateral movement) вірусів-шифрувальників всередині периметра.

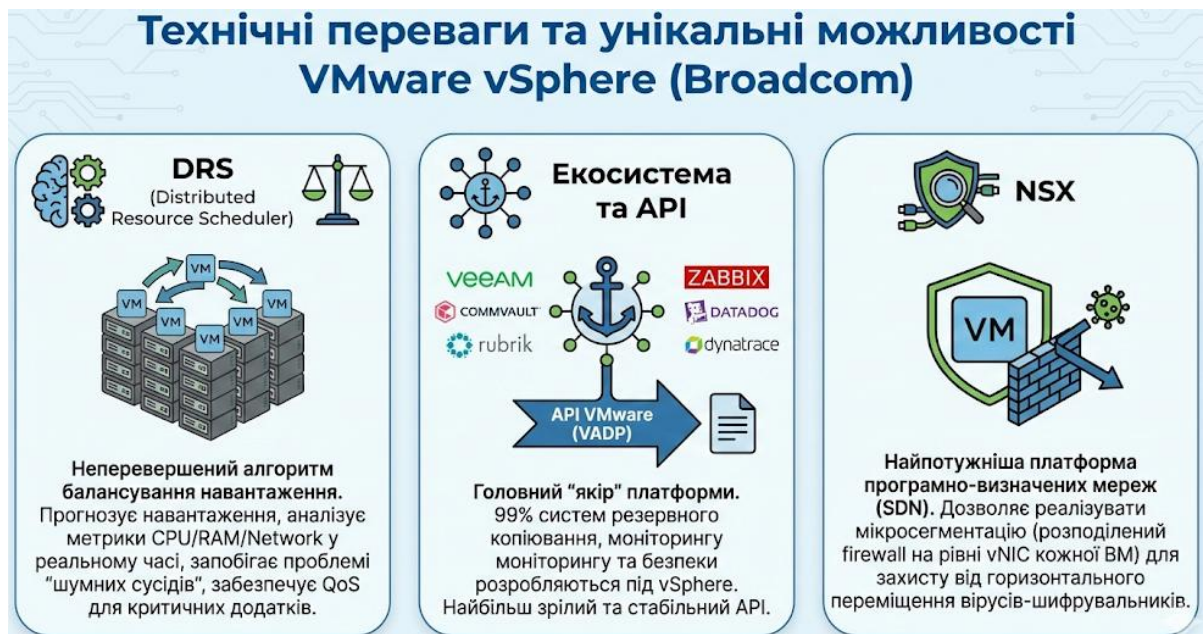


Рис. 1.4 Переваги VMware (Broadcom)

Однак слід відзначити, що повна непередбачуваність цінової політики та дорожньої карти розвитку для сегмента SMB (Small and Medium Business). Broadcom відкрито декларує фокус на топ-600 глобальних клієнтів. Середній бізнес фактично залишається з урізаною підтримкою через партнерську мережу, що підвищує ризики тривалих простоїв у разі складних архітектурних аварій (Level 3 Support issues).

Таким чином, VMware vSphere (Broadcom) Безальтернативний вибір для критичних систем Tier-1 (Банківський процесинг, ядро Телеком-операторів, АЕС, управління виробництвом, крупні державні структури), де вартість хвилини простою перевищує річну вартість ліцензій, а бюджети дозволяють ігнорувати зростання цін заради стабільності та передбачуваності.

Microsoft Hyper-V (Azure Stack HCI)

Сильне, зріле рішення для екосистем, історично побудованих навколо продуктів Microsoft (Windows Server, SQL Server, AD) [4]. Гіпервізор Type-1, що працює на рівні ядра Windows.

Архітектурні особливості та інтеграція рішень (рис.1.5) Microsoft Hyper-V (Azure Stack HCI):

- Єдиний стек керування: У зв'язці з Active Directory, Group Policy та System Center Virtual Machine Manager (SCVMM) керування тисячами ВМ стає рутинним завданням. Якщо у вас штат кваліфікованих Windows-адміністраторів, поріг входу мінімальний — не потрібно вивчати Linux, Bash або нові концепти керування.
- Storage Spaces Direct (S2D) та ReFS: Програмно-визначена СЗД від Microsoft. Дозволяє будувати гіперконвергентні кластери, використовуючи локальні диски. Використання файлової системи ReFS (Resilient File System) забезпечує прискорення операцій клонування блоків (Block Cloning), що миттєво створює VHDX файли. Однак технологія вибаглива до обладнання: вимагає RDMA-мережевих карт (RoCE або iWARP) та суворо сертифікованих NVMe накопичувачів.
- Azure Arc: Унікальна фішка гібридної стратегії. Дозволяє "натягнути" хмарну панель керування Azure на локальні сервери. Ви можете застосовувати хмарні політики безпеки (Azure Policy), моніторинг та керування оновленнями до "залізних" серверів у своєму локальному ЦОД.

В той же час сама система Management OS для рішень Microsoft вимагає регулярних оновлень та перезавантажень (Patch Tuesday), що ускладнює обслуговування кластерів порівняно з мікроядерними гіпервізорами (де оновлення часто не вимагають повного перезавантаження хоста). Підтримка

Linux значно покращилася, але все ще поступається нативним рішенням у плані продуктивності дискової підсистеми.

АРХІТЕКТУРНІ ОСОБЛИВОСТІ ТА ІНТЕГРАЦІЯ MICROSOFT HYPER-V (AZURE STACK HCI)

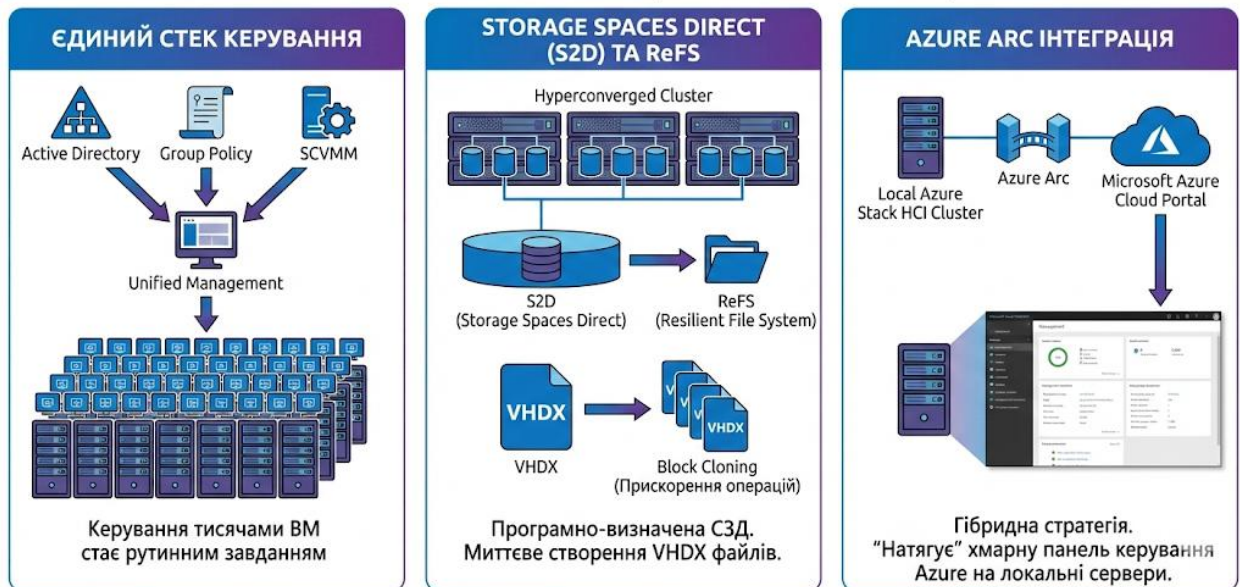


Рис. 1.5 особливості та інтеграція рішень Microsoft Hyper-V (Azure Stack HCI)

Таким чином, Microsoft Hyper-V (Azure Stack HCI) ідеально підходить для "Microsoft-shop" компаній та розподілених філіальних мереж (ROBO), що прагнуть безшовної гібридної моделі з хмарою Azure та хочуть уніфікувати інструменти керування.

Proxmox VE / KVM-based рішення

Головний бенефіціар поточного переділу ринку. Proxmox VE зробив гігантський ривок із нішевого продукту для ентузіастів у потужну Enterprise-платформу, здатну тримати навантаження рівня дата-центру [2].

Технологічні рішення та інновації Proxmox VE / KVM-based (рис. 1.6):

- KVM (Kernel-based Virtual Machine): Гіпервізор вбудований прямо в ядро Linux [7]. Це гарантує підтримку будь-якого новітнього "заліза" (процесори останніх поколінь, GPU для AI, SmartNICs) відразу після виходу драйверів у ядрі Linux (upstream), часто випереджаючи пропріетарні рішення на 6-12 місяців.

- ZFS & Ceph:
 - ZFS: Файлова система enterprise-рівня із вбудованим захистом цілісності даних (Check-summing), миттєвими знімками (COW Snapshots) та реплікацією. Ідеальна для надійних standalone-серверів.
 - Ceph (RBD): Повністю інтегрована розподілена об'єктна СЗД для кластерів. Забезпечує самовідновлення даних (Self-healing) та відсутність єдиної точки відмови. Вихід з ладу диска або цілого сервера не зупиняє сервіс, дані автоматично ребалансуються на здорові ноди [2].
- LXC (Linux Containers): Унікальна конкурентна перевага ("Killer feature"). Дозволяє запускати системні контейнери (практично без оверхеду на віртуалізацію ядра) поруч із "важкими" ВМ. Ідеально підходить для баз даних (PostgreSQL, MySQL) та веб-серверів, забезпечуючи near-metal продуктивність.
- Proxmox Backup Server (PBS): Революційне рішення з дедуплікацією на стороні клієнта. Дозволяє виконувати інкрементальні бекапи кожні 15 хвилин, передаючи мережею лише змінені блоки. Економія місця на бекапах досягає 20-50 разів, що кардинально знижує вимоги до обсягу сховища резервних копій.

Слід відзначити, що інтерфейс та UX суттєво відрізняються від звичного VMware vSphere Client. Немає повноцінного аналога DRS (автоматичне балансування ресурсів є, але воно базується на простіших метриках). Вимагає від команди адміністраторів базових навичок роботи в консолі Linux (bash, systemd, iproute2) для глибокої діагностики мережесх проблем або тонкого налаштування продуктивності (tuning).



Рис. 1.6 Технологічні рішення та інновації Proxmox VE / KVM-based

Таким чином, це основа безкоштовної віртуалізації. Найкраще співвідношення функціонал/ціна (TCO). Де-факто стандарт для проєктів імпортозаміщення, побудови приватних хмар з нуля та середовищ розробки, де важлива гнучкість та відсутність ліцензійних обмежень.

Екосистема Xen (Citrix Hypervisor / XCP-ng)

Технологія, перевірена часом та мільйонами інсталяцій у хмарах [6]. Xen використовує архітектуру мікроядра, що фундаментально відрізняє його від монолітного підходу KVM.

Існують наступні варіанти реалізації екосистеми Xen (рис. 1.7):

- Citrix Hypervisor: Комерційний продукт, який зараз розвивається вузькоспрямовано — для забезпечення найкращої роботи VDI рішень Citrix (оптимізація графічного стека, підтримка vGPU).
- XCP-ng (Xen Cloud Platform - next gen): Повністю відкритий форк, що активно підтримується спільнотою та компанією Vates. Позиціонується як "пряма заміна ESXi", фокусуючись на простоті міграції [3].

ВАРІАНТИ РЕАЛІЗАЦІЇ ЕКОСИСТЕМИ XEN

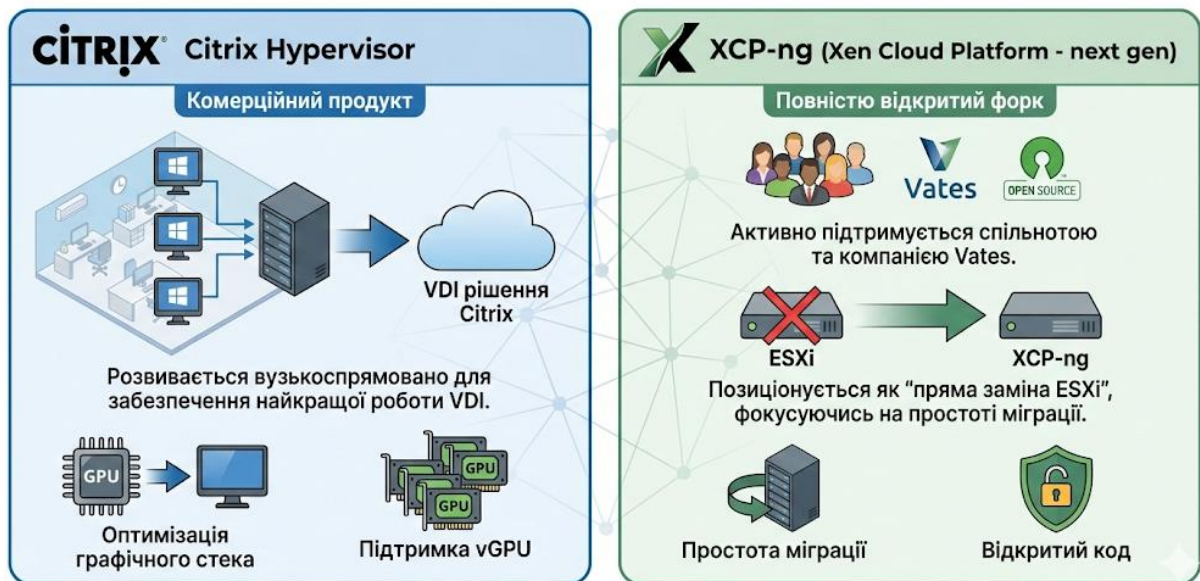


Рис.1.7 Варіанти реалізації екосистеми Xen

Аналіз Інтернет-джерел дозволив виявити ключові особливості Xen (рис. 1.8):

- **Безпека та Ізоляція (Dom0):** Драйвери обладнання та керуючий стек винесені у спеціальний привілейований домен (Dom0), ізольований від гіпервізора. Збій драйвера мережевої карти або контролера дисків рідше призводить до падіння всього хоста ("Purple Screen of Death"), ніж у монолітних ядрах.
- **Xen Orchestra (ХО):** Потужний веб-інтерфейс керування, який за логікою та зручністю часто перевершує Proxmox і є ідейно ближчим до vCenter. Вміє компілюватися з вихідних кодів (безкоштовно). Надає функції Enterprise-рівня: Continuous Replication (для Disaster Recovery з RPO близьким до нуля), візуалізацію "здоров'я" пулу, автоматичний патчинг хостів без простою (rolling pool update).

КЛЮЧОВІ ОСОБЛИВОСТІ XEN: БЕЗПЕКА, ІЗОЛЯЦІЯ ТА КЕРУВАННЯ

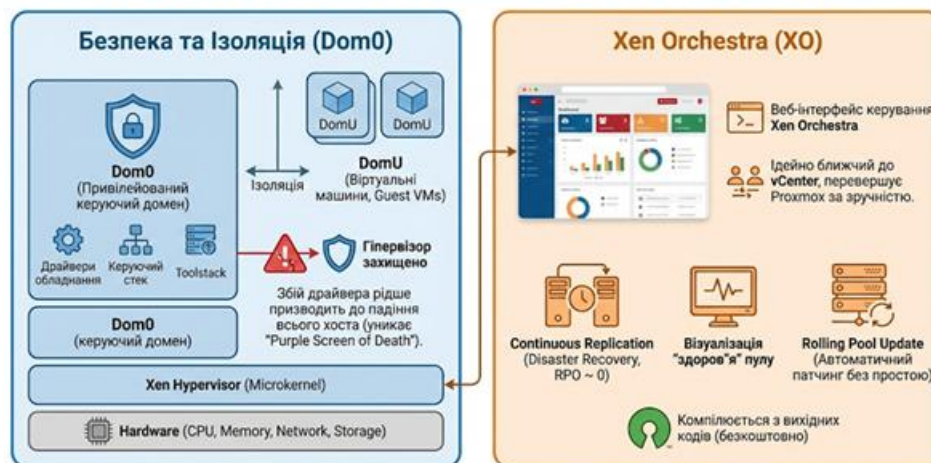


Рис.1.8 ключові особливості Xen

Порівняння з KVM: Xen складніший в адаптації під новітнє "геймерське" або нестандартне залізо (наприклад, Realtek NICs), оскільки список сумісності (HCL) суворіший. Однак на сертифікованому серверному обладнанні (HPE, Dell) він часто показує стабільнішу мережеву затримку та джиттер під високим навантаженням.

XCP-ng — це вибір "консервативних" адміністраторів VMware, які змушені мігрувати, але хочуть зберегти спокій. Це дозволяє залишити звичну парадигму керування "кластер-пул-хост" через зручний GUI, не занурюючись у нетрі Linux-адміністрування та конфігураційних файлів.

Рішення на базі OpenStack

Це не просто гіпервізор, а масштабна екосистема з десятків взаємопов'язаних модулів (Nova - обчислення, Neutron - мережа, Cinder - блокове сховище, Keystone - ідентифікація) для побудови повноцінної хмари "AWS у себе в ЦОД".

Реальність експлуатації: Надзвичайно складний в архітектурі, розгортанні та особливо оновленні (Upgrades між релізами). Вимагає наявності виділеної команди високооплачуваних DevOps/Python інженерів для підтримки життєвого циклу.

Таким чином, це рішення економічно виправдано лише для провайдерів публічних хмар, гіперскейлерів або найбільших держкорпорацій з тисячами хостів. Для звичайного корпоративного бізнесу — надмірна складність ("Overkill"), яка знищить рентабельність проєкту витратами на ФОП.

Висновки по розділу

Вибір платформи віртуалізації сьогодні перестав бути суто технічним питанням "яка кнопка зручніша" — це стратегічне бізнес-рішення, що впливає на виживання компанії в умовах цифрової економіки (рис.1.10).

- VMware залишається безперечним технологічним лідером ("золотий стандарт"), але свідомо трансформується у нішевий продукт для еліти [1]. Якщо ваш бізнес може дозволити собі кратне зростання ліцензійних платежів заради стабільності — залишайтеся, альтернативи за глибиною екосистеми все ще у ролі наздоганяючих.
- XCP-ng (Xen) — це "прихована перлина" ринку. Для адміністраторів, які звикли до логіки vCenter/Cluster, це найбільш безболісний та м'який шлях міграції у світ Open Source. Він стабільний, передбачуваний, має чудовий GUI і не вимагає перетворення команди системних адміністраторів на Linux-гуру.
- Proxmox (KVM) — це найпотужніший комбайн майбутнього. Якщо ваша команда готова інвестувати час у навчання і ви хочете отримати максимальну незалежність від вендорів, можливість використовувати змішане навантаження (VM + Контейнери LXC) та всю міць файлової системи ZFS — це найкращий вибір на горизонті найближчих 5-10 років.

Однак слід враховувати особливості поступового переходу. Не рекомендується провести міграцію методом "великого вибуху". Почніть із пілотного проєкту (PoC) на базі XCP-ng або Proxmox для некритичних сервісів

(середовища розробки, тестування, моніторинг), щоб реально оцінити готовність вашої команди до підтримки нової екосистеми та виявити вузькі місця в існуючому обладнанні.

Таким чином, загальну порівняльну характеристику можна надати таблицею 1.1.

Таблиця 1.1 Порівняльна матриця вибору (Decision Matrix)

Критерій	Enterprise (Банки, державні установи, ВПК)	Mid-Market (невелике виробництво)	Small/Startups (Малий бізнес, IT-компанії)
Ключовий фактор	Комплексна підтримка 24/7, Мінімізація ризиків	Зниження TCO (Total Cost of Ownership), Відхід від Vendor Lock-in, Оптимізація ресурсів	Швидкість запуску (Time-to-Market), Мінімальний поріг входу, Гнучкість (Agility)
Гіпервізор	VMware vSphere / Nutanix AHV	XCP-ng (Xen) / Proxmox VE / Hyper-V	Proxmox / Public Cloud (AWS/GCP/Azure)
СЗД (Storage)	High-End SAN (Huawei Dorado, NetApp, Pure Storage)	Software-Defined (VMware vSAN, Ceph, StarWind VSAN)	Локальні NVMe (ZFS) / Прості NAS (Synology/QNAP)
VDI	Citrix DaaS / VMware Horizon	Microsoft AVD / RDS / Termidesk	VPN + RDP / Web-based SaaS / Apache Guacamole
Контейнери	Red Hat OpenShift / VMware Tanzu	SUSE Rancher / Vanilla K8s	Managed K8s у хмарі / Docker Compose / Portainer

ВИБІР ПЛАТФОРМИ ВІРТУАЛІЗАЦІЇ

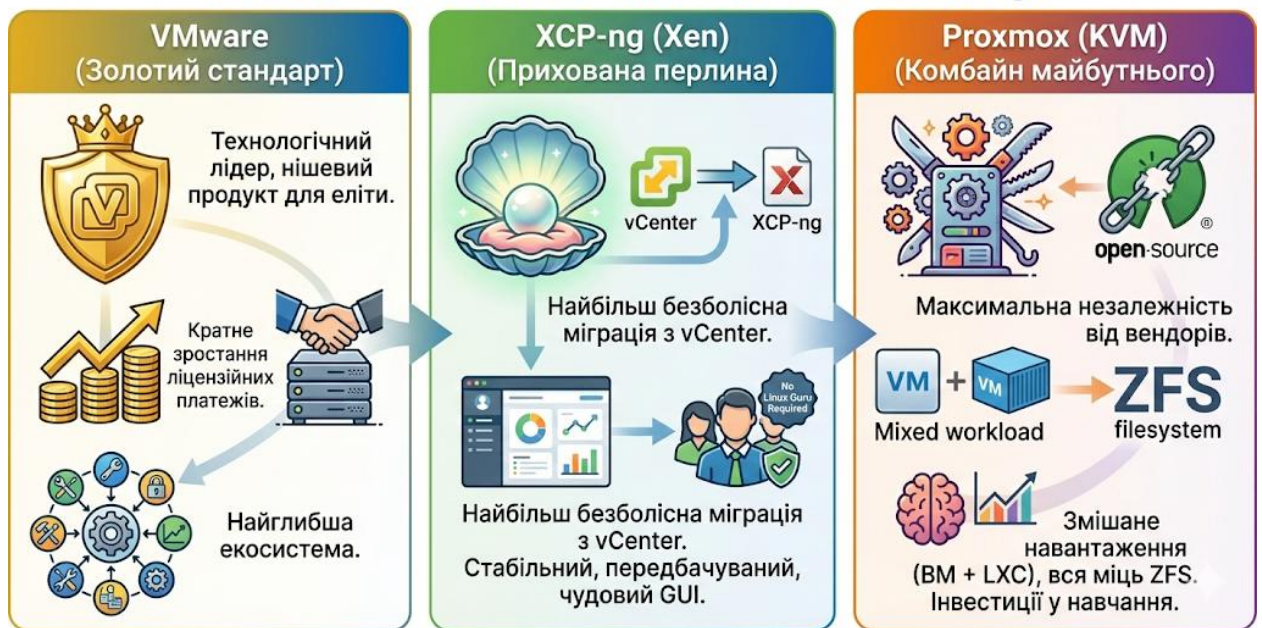


Рис.1.10 Вибір платформи віртуалізації

РОЗДІЛ 2. ОГЛЯД АРХІТЕКТУРИ ТА ЛІЦЕНЗУВАННЯ

2.1 Огляд архітектури ліцензування VMware by Broadcom

Концептуальна трансформація корпоративної стратегії

Придбання VMware корпорацією Broadcom ознаменувало фундаментальне зрушення у філософії дистрибуції корпоративного ПЗ[9]. Стратегія вендора переорієнтована з продажу розрізнених ліцензій на надання інтегрованих програмних стеків (Bundles). Це рішення спрямоване на глибоку стандартизацію ІТ-ландшафту замовників, що, на думку Broadcom, має знизити складність підтримки, проте на практиці це призводить до суттєвого зростання вартості володіння для малого та середнього сегментів [13].

Ключові положення оновленої політики (рис. 2.1):

1. Повний перехід на передплатну модель (Subscription-only): Продажі безстрокових (Perpetual) ліцензій та окремих контрактів на підтримку (SnS) офіційно припинені [10]. Таким чином, це мало суттєві *наслідки для бізнесу*: Перехід від капітальних витрат (CAPEX) до операційних (OPEX) вимагає перегляду фінансових циклів організації. Критичним аспектом є те, що після закінчення терміну дії передплати ПЗ може втратити функціональність управління («заморожування» консолі управління vCenter), що вимагає бездоганного дотримання термінів продовження.
2. Уніфікація метрик ліцензування: Ліцензування за ядрами (Per Core): Розрахунок вартості володіння тепер базується на кількості фізичних ядер процесорів [11]. Крім того було введено принцип мінімального порогу (16 ядер): Встановлено обов'язковий мінімум 16 ліцензій на один фізичний процесор (CPU). Це означає, що сервер із двома 8-ядерними процесорами буде ліцензуватися як 32-ядерна система. Дана політика робить економічно неефективною експлуатацію застарілого обладнання з низькою щільністю ядер та спонукає

замовників до оновлення серверного парку на сучасні багатоядерні рішення.

- Радикальна консолідація портфеля, переліку програмного забезпечення призвала до того, що лінійка з понад 50 відокремлених SKU (програмних додатків) була скорочена до двох ключових версій: **vSphere Foundation (VVF)** та **Cloud Foundation (VCF)** (табл. 21) [9], [11]. Це спрощує процес закупівлі для великих корпорацій, але позбавляє гнучкості тих, кому був потрібен лише специфічний функціонал.
- Поділ із Horizon (EUC):** Підрозділ End-User Computing виділено в незалежну компанію **Omnissa** [12]. Інтеграція між VMware та Horizon тепер будується на партнерських відносинах, що додає складності в управлінні контрактами та підтримці змішаних середовищ.

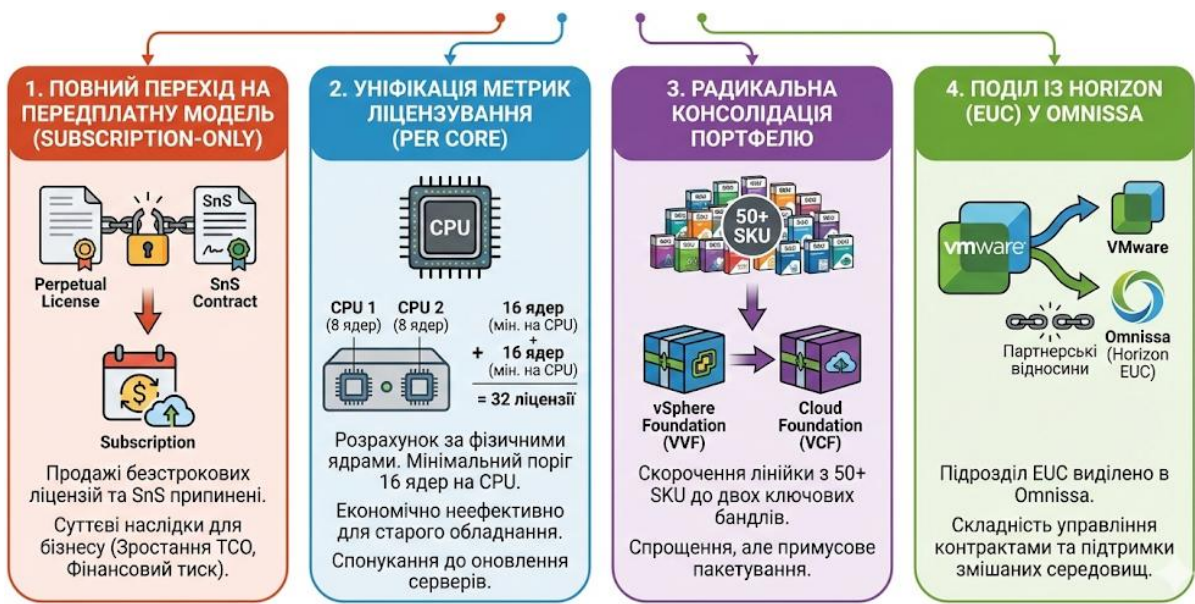


Рис. 2.1 Зміни в стратегії VMware (Broadcom)

Таблиця 2.1 Детальний аналіз пакетів VVF проти VCF [11]

Компонент	VMware vSphere Foundation (VVF)	VMware Cloud Foundation (VCF)
Склад	vSphere Enterprise Plus, vCenter Standard, Tanzu Kubernetes Grid	Весь функціонал VVF + NSX + Aria Suite Enterprise
Управління	Aria Operations (Advanced)	SDDC Manager (Повна автоматизація)
Квота vSAN	0.25 ТБ на ліцензоване ядро	1 ТБ на ліцензоване ядро

Архітектура управління: vCenter Server

У попередніх моделях vCenter Server представляв собою окремий актив, що вимагав значних витрат (особливо редакція Standard). У 2025 році vCenter фактично перейшов до розряду «допоміжної утиліти» [11] (рис.2.2).

- Уніфікація та інклюзивність: Ліцензія на vCenter Server Standard тепер інтегрована до складу обох основних передплат (VVF та VCF) без стягнення додаткової плати.
- Архітектурна свобода: Замовникам надається право на необмежене розгортання інстансів vCenter. Це дозволяє архітекторам проектувати топології з високим ступенем ізоляції або будувати відмовостійкі конфігурації з використанням Enhanced Linked Mode.
- Примусова рекомендації щодо відмовостійкості: Оскільки ліцензія більше не є стримуючим фактором, обов'язковим стандартом стає впровадження vCenter HA (High Availability).



Рис.2.2 Трансформування vCenter

Мережева віртуалізація та безпека – NSX

VMware NSX від Broadcom — це провідна платформа програмно-визначених мереж (SDN) та безпеки, яка дозволяє віртуалізувати мережеві функції (комутацію, маршрутизацію, брандмауери, балансувальники) у єдине логічне середовище, створюючи віртуальні мережі поверх фізичної інфраструктури для центрів обробки даних та хмар, забезпечуючи мікросегментацію, автоматизацію та керування з централізованої консолі. Після придбання VMware компанією Broadcom (<https://softprom.com/ua/vendor/vmware/product/vmware-nsx>) бренд зберігається, хоча назва NSX-T стала просто NSX.

Програмний стек NSX (раніше NSX-T) зазнав найбільш жорсткої консолідації. Тепер NSX став ексклюзивною перевагою тільки преміального сегмента ліцензій.

- Ексклюзивність NSX для VCF: Повноцінний функціонал мережевої віртуалізації доступний виключно в межах пакета VMware Cloud Foundation (VCF). Це рішення включає:
 - Distributed Firewall (DFW): Інструмент для реалізації мікросегментації та стратегії Zero Trust.
 - Advanced Load Balancer (ALB): Балансування трафіку на рівнях L4-L7.
 - Мережева абстракція (Overlay): Створення логічних мереж поверх фізичної інфраструктури.
- Наслідки для VVF: Пакет vSphere Foundation повністю позбавлений функцій NSX. Замовники, яким потрібна мікросегментація, змушені купувати повний стек VCF [14].

Призупинення систем vSphere Standard та Essentials

Раніше популярні редакції vSphere Standard та Essentials досягли стадії завершення життєвого циклу (EOL).

- Міграція з vSphere Standard: Дана редакція більше не постачається. Поточним користувачам Standard при продовженні пропонується перехід на VVF.
- Трансформація Essentials Plus: Традиційний набір для малого офісу трансформовано у спеціалізовану передплату **VVF з лімітом ядер**.

Модернізація гіпервізора ESXi та вимоги до апаратної частини

Гіпервізор ESXi 8.x/9.x став більш вимогливим до апаратної частини.

- Припинення підтримки безкоштовної версії: Корпорація офіційно завершила підтримку VMware vSphere Hypervisor (Free Edition) [10]. Легальний спосіб безкоштовного навчання у домашніх лабораторіях (Homelabs) видалено.
- Жорсткі вимоги до носіїв ОС: У нових версіях ESXi повністю припинена підтримка встановлення на SD-карти та USB-флешки. Для встановлення потрібні локальні SSD або NVMe накопичувачі (рекомендовано 128 ГБ+).

Роль VMware Tanzu в сучасній інфраструктурі

Контейнеризація стала невід'ємним атрибутом віртуалізації.

- **Інтеграція у VVF:** Дозволяє запускати кластери Kubernetes (TKG) всередині vCenter.
- **Tanzu Platform 10 (VCF):** Надає розширені можливості управління флотом кластерів (Fleet Management).

Економічні аспекти експлуатації vSAN

Перехід vSAN на об'ємне ліцензування (Capacity-based) вимагає перегляду архітектур [15].

- **Метрика ТБ (TiB):** Ліцензується сумарна «сира» (Raw) ємність дисків. При розрахунках Broadcom використовує двійкову систему (1024), де 1 терабайт дорівнює 1024 гігабайтам (технічно це тебібайт — TiB).

- **Оптимізація:** RAID-5/6 (Erasure Coding) стає економічно привабливішим за RAID-1.
- **Додаткові передплати: vSAN Capacity Add-on.** У випадках, коли фізична ємність дискової підсистеми перевищує обсяг, включений у базову ліцензію VVF/VCF, необхідне придбання додаткових ліцензій розширення (табл 2.2).
 1. Механізм активації: Ліцензії vSAN Capacity Add-on купуються за кількістю ТБ «сирої» ємності.
 2. Умови використання: Додаткова ємність ліцензується понад сумарний «безкоштовний» ліміт (Entitlement) на весь кластер.
 3. Відповідність термінів: Термін дії додаткової передплати на ємність має збігатися з терміном дії основної передплати на ядра.

Таблиця 2.2 Вартість vSAN Capacity Add-on (Додаткова ємність)

Період передплати	Орієнтовна ціна за 1 ТБ на рік (MSRP)	Примітка
1 рік	~\$25 - \$35	Тільки для короткострокового розширення
3 роки	~\$20 - \$28	Базовий корпоративний стандарт
5 років	~\$15 - \$22	Максимальна економія

Приблизний аналіз ліцензій – загальні цінові діапазони (MSRP)

Ціни вказані за одне ядро на рік за умови багаторічного контракту.

- **VVF:**
 - ~\$135 - \$160 / ядро на рік (при 3-річному контракті).
 - ~\$120 - \$145 / ядро на рік (при 5-річному контракті).
- **VCF:**
 - ~\$350 - \$400 / ядро на рік (при 3-річному контракті).
 - ~\$310 - \$360 / ядро на рік (при 5-річному контракті).
- **VVF Essentials Kit:**

- ~\$3,500 - \$4,500 за 3 роки (фікс. сборка 96 ядер).
- ~\$5,200 - \$6,800 за 5 років (фікс. сборка 96 ядер).

Таким чином, при виборі VMware by Broadcom треба враховувати

- Передплати на 3 та 5 років є пріоритетними. Для vSAN аддонів 5-річний контракт дає найбільш помітне зниження вартості за терабайт [5].
- Необхідно заздалегідь розраховувати RAW-ємність СХД. В інфраструктурах з високою щільністю зберігання (High Density) вартість vSAN Add-on може стати суттєвою частиною загального бюджету [7].
- **VVF Essentials Kit:** Обмежений жорстким лімітом у 96 ядер і не підтримує аддони на розширення vSAN ємності понад базові 0.25 ТБ на ядро [3].

Зведену інформацію можна представити у вигляді таблиці 2.3

Таблиця 2.3.Огляд ліцензій VMware (Broadcom)

Критерій	vSphere Foundation (VVF)	Cloud Foundation (VCF)	VVF Essentials Kit
Цільовий сегмент	Стандартні корпоративні ЦОД	Автоматизовані приватні хмари	Малий бізнес (до 3 хостів)
ESXi (Гіпервізор)	Enterprise Plus	Enterprise Plus	Essentials Plus
vCenter Server	Standard (Включено)	Standard (Включено)	Essentials (Включено)
Мережева безпека	Базова (VLAN/VDS)	Просунута (NSX/Мікросегментація)	Базова (VLAN/VDS)
NSX (Мережі та безпека)	Відсутній	Включений (Повний стек)	Відсутній
Tanzu (Kubernetes)	TKG (Runtime)	Tanzu Platform 10 (Full)	Відсутній
Автоматизація / Аналітика	Aria Operations (Logs/Diagnostics)	SDDC Manager / Aria Suite Ent.	Aria Operations (Logs/Diagnostics)
Ядра процесора	Мін. 16 ядер на CPU	Мін. 16 ядер на CPU	Макс. 96 ядер на комплект

Критерій	vSphere Foundation (VVF)	Cloud Foundation (VCF)	VVF Essentials Kit
Включений vSAN	0.25 ТБ на ліцензоване ядро	1 ТБ на ліцензоване ядро	0.25 ТБ на ліцензоване ядро
Дод. vSAN (Add-on)	~\$20-28/ТБ/рік (3р)	~\$20-28/ТБ/рік (3р)	Не передбачено
Ліцензування	Передплата за ядрами	Передплата за ядрами	Фіксована зборка
Економія при 5 роках	Висока (~20-25%)	Максимальна	Середня

2.2 Огляд архітектури ліцензування Omnissa Horizon

Концептуальна трансформація корпоративної стратегії

Після відокремлення підрозділу End-User Computing (EUC) від VMware та його остаточного придбання інвестиційною групою KKR у 2024 році [16], бренд Omnissa сформував власну стратегію, яка базується на ідеї "Автономного робочого простору" (Autonomous Workspace). Це не просто зміна назви, а стратегічне перепозиціонування Omnissa як "нейтрального" гравця, який прагне бути "Швейцарією" у світі EUC, забезпечуючи безшовну інтеграцію з будь-якими хмарами, гіпервізорами та пристроями [20].

Ключові положення оновленої політики та їх стратегічні наслідки:

- **Повна автономія (Standalone Entity):** Omnissa більше не залежить від дорожньої карти Broadcom. Це дає компанії можливість швидше адаптуватися до потреб ринку, не чекаючи на оновлення основного стека VMware. Прямим наслідком для замовників є розділення порталів підтримки: тепер усі дистрибутиви, документація та ліцензійні ключі знаходяться на платформі Omnissa Customer Connect [16].
- **Платформний підхід (Omnissa Platform):** Фокус зміщується на інтегрований стек, де Horizon (VDI) та Workspace ONE (UEM)

працюють як єдиний механізм. Система використовує машинне навчання для реалізації концепції Digital Employee Experience (DEX) — автоматичного виявлення аномалій у роботі сесій та їх виправлення без втручання адміністратора (Self-healing).

- **Subscription-First та Term-ліцензії:** Перехід на передплату є остаточним та безповоротним [18]. Це фундаментально змінює фінансовий ландшафт організації, перетворюючи одноразові інвестиції (CAPEX) на циклічні операційні витрати (OPEX). Важливо розуміти наслідки: після закінчення терміну підписки консоль управління Connection Server блокується, що унеможливорює створення нових сесій, хоча існуючі підключення можуть зберігатися протягом короткого "граційного" періоду.

Основні компоненти Omnisia Horizon: Архітектурний рівень

Для ефективного проектування VDI-інфраструктури необхідно розуміти функціональну взаємодію ключових модулів [17] (рис.2.3):

- **Horizon Connection Server:** Це "мозок" системи, що виконує роль брокера з'єднань. Він не лише автентифікує користувачів через AD/LDAP, а й динамічно призначає сесії, керує життєвим циклом віртуальних машин та контролює стан пулів десктопів.
- **Horizon Agent:** Встановлюється в "майстер-образ" операційної системи. Він забезпечує роботу протоколу **Blast Extreme**, який завдяки кодекам H.264/H.265 та адаптивному управлінню смугою пропускання дозволяє працювати навіть через нестабільні 3G/4G мережі з мінімальною затримкою.
- **Horizon Client:** Клієнтське ПЗ для Windows, macOS, iOS, Android та Chromebook. Забезпечує прокидання локальної периферії (сканерів, смарт-карт, принтерів) у віртуальне середовище.
- **Unified Access Gateway (UAG):** Спеціалізований Linux-аплайєнс у DMZ. Він реалізує концепцію **Per-App VPN** та виступає як захисний

бар'єр, що виключає необхідність використання громіздких VPN-клієнтів для віддаленого доступу.

- **App Volumes:** Інструмент для миттєвої доставки застосунків. Програми не встановлюються в ОС, а монтуються як віртуальні диски (VMDK) у момент входу користувача. Це дозволяє використовувати один "золотий образ" Windows для різних відділів (маркетинг, бухгалтерія, IT), просто підключаючи потрібні набори програм.
- **Dynamic Environment Manager (DEM):** Забезпечує "персоналізацію" неперсистентних столів. Навіть якщо віртуальна машина знищується після виходу, DEM зберігає всі налаштування браузерів, офісних програм та мапінг мережеских дисків, відновлюючи їх при наступному вході.

Omnissa Horizon: Архітектурний рівень

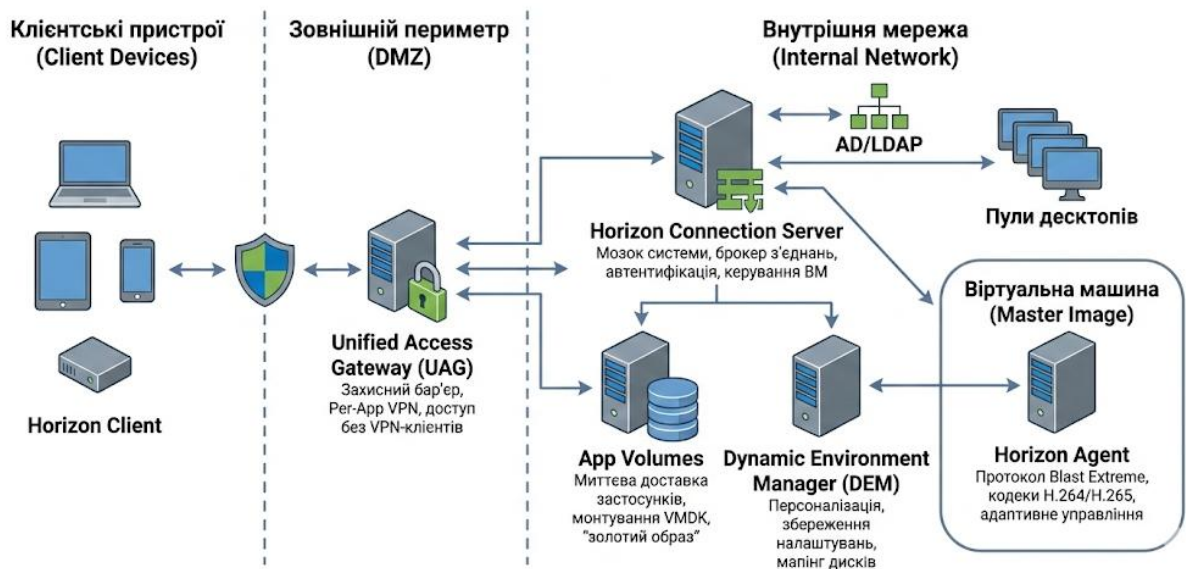


Рис. 2.3 Основні компоненти Omnissa Horizon

Додаткові компоненти та інфраструктурне забезпечення

Ці компоненти забезпечують стійкість та розширений функціонал VDI-середовища (рис. 2.4):

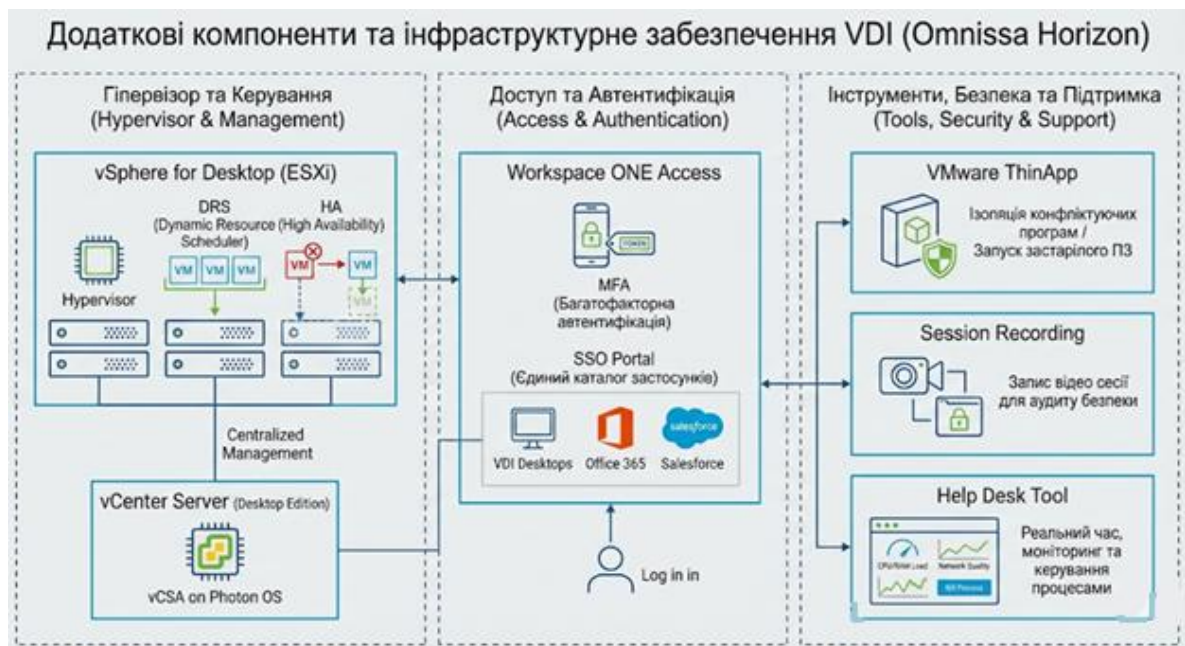


Рис. 2.4 Додаткові компоненти Horizon

- **vSphere for Desktop (ESXi):** Надає потужності гіпервізора спеціально для VDI. Включає DRS (Dynamic Resource Scheduler) для балансування навантаження між хостами та HA (High Availability) для автоматичного перезапуску VM у разі відмови обладнання. **Включено у більшість версій Horizon.**
- **vCenter Server (Desktop Edition):** Система управління всім кластером віртуалізації. У складі Horizon вона постачається як vCenter Server Appliance (vCSA) на базі Photon OS.
- **Workspace ONE Access:** Забезпечує багатофакторну автентифікацію (MFA) та єдиний каталог застосунків (SSO portal), де користувач бачить свої VDI-столи поруч із SaaS-додатками (Office 365, Salesforce).
- **VMware ThinApp:** Використовується для ізоляції конфліктуючих програм або запуску застарілого ПЗ у сучасних операційних системах.

- **Session Recording:** Критичний інструмент для фінансового та державного секторів, що дозволяє записувати відео кожної сесії для подальшого аудиту безпеки.
- **Help Desk Tool:** Надає службі підтримки можливість переглядати в реальному часі завантаження CPU/RAM клієнта, якість мережевого сигналу та "вбивати" завислі процеси без переривання всієї сесії.

Глибока архітектура управління: On-Premise vs Cloud

Omniissa пропонує два фундаментальні підходи до розгортання контрольної панелі [18]:

1. **Horizon Connection Server (On-Premise):** Повний контроль метаданих та трафіку всередині власного ЦОД. Це ідеально для організацій, що працюють за моделлю "Air-gapped" (без доступу до інтернету). Проте це вимагає від замовника самостійного забезпечення відмовостійкості баз даних SQL та серверів управління.
2. **Omniissa Horizon Cloud Service (Universal):** Це SaaS-рішення, де Omniissa бере на себе роль управління інфраструктурою. Ви отримуєте єдину консоль для управління десктопами в локальному ЦОД, а також у публічних хмарах (Azure, AWS, Google Cloud). Це дозволяє реалізувати сценарій **Bursting** — орендувати потужності в хмарі тільки під час пікових сезонних навантажень.

Модернізація доставки додатків: Глибоке занурення в App Volumes

Технологія App Volumes пройшла шлях від простого підключення дисків до концепції "**Apps on Demand**":

- **Прискорення входу:** Раніше всі додатки монтувалися під час входу в Windows, що затримувало появу робочого столу. Тепер додаток монтується тільки тоді, коли користувач натискає на його іконку. Це економить до 40% часу входу.

- **Writeable Volumes:** Це персональні віртуальні диски користувачів, які дозволяють встановлювати власні плагіни або програми. Це робить неперсистентні пули такими ж гнучкими, як і фізичні ПК, але зі збереженням централізованого управління.
- **Зниження витрат на Storage:** Оскільки програми не дублюються всередині кожної VM, вимоги до обсягу швидкої дискової пам'яті (SSD/NVMe) скорочуються у 3-5 разів.

Перелік програмних компонентів за версіями та їх особливості

1. Horizon Standard:
 - vSphere for Desktop & vCenter for Desktop: Повна інфраструктура віртуалізації.
 - Horizon Connection Server: Брокер з'єднань.
 - Unified Access Gateway (UAG): Безпечний шлюз.
 - Windows VDI: Підтримка віртуальних десктопів Windows.
 - Blast Extreme / PCoIP: Протоколи передачі даних.
2. Horizon Advanced (включає все з Standard +):
 - Published Apps (RDSH): Доставка окремих застосунків.
 - App Volumes (Standard): Динамічна доставка застосунків.
 - Dynamic Environment Manager (DEM) Standard: Керування профілями.
 - Instant Clones: Технологія миттєвого створення десктопів.
 - Workspace ONE Access: Портал застосунків та SSO.
3. Horizon Enterprise (включає все з Advanced +):
 - App Volumes Enterprise: Повний функціонал AppStacks.
 - DEM Enterprise: Розширені контекстні політики та Smart Policies.
 - Session Recording: Запис активності користувачів.
 - Help Desk Tool: Просунута технічна підтримка та аналітика.

- Linux VDI: Підтримка віртуальних десктопів на базі Linux.
- Skype/Teams Optimization: Спеціалізовані плагіни для відеозв'язку.

4. Horizon Universal (включає все з Enterprise +):

- Cloud Control Plane: Хмарна панель управління.
- Universal Broker: Єдиний брокер для гібридних середовищ.
- Hybrid Cloud Management: Керування On-prem, Azure, AWS та Google Cloud.
- DEEM (Digital Employee Experience Management): Просунута AI-аналітика досвіду користувачів.
- Universal Licensing: Можливість вільно переносити ліцензії між локальною інфраструктурою та хмарою.

Слід враховувати певні особливості Instant Clones та шлюзу UAG

Instant Clones — це технологія, що дозволяє клонувати пам'ять батьківської VM, створюючи "дитячу" машину за лічені секунди [17].

- Windows: Підтримка від Windows 10 до Windows Server 2025. Дозволяє реалізувати концепцію "Non-persistent VDI", де кожен користувач вранці отримує "свіжий" десктоп.
- Linux: Omnissa є лідером у підтримці Linux VDI (Ubuntu, RHEL, CentOS). Це дозволяє економити на ліцензіях Microsoft для розробників, надаючи їм потужні графічні столи на базі відкритого ПЗ [22].

Додатково Horizon дає ще декілька можливостей, тому, що у сучасному світі VDI неможливий без дотримання концепції нульової довіри [20]:

- Device Compliance: Перед наданням доступу шлюз UAG перевіряє стан пристрою (антивірус, версія ОС).
- Watermarking: У версії Enterprise доступна функція нанесення водяних знаків (ім'я користувача, IP) поверх відеосесії для запобігання витоку даних.

Особливістю варіантів поставки Horizon – співпраця з Broadcom та включення інфраструктурного компоненту: vSphere for Desktop (v4D)

OmniSSA зберігає унікальне OEM-партнерство з Broadcom [19], що є величезною перевагою для замовників.

Технічні нюанси та обмеження v4D:

- **Функціональний рівень:** Базується на **vSphere Enterprise Plus**, надаючи доступ до Distributed Switch (vDS) для складних мережевих конфігурацій та Host Profiles для стандартизації хостів.
- **Підтримка vGPU (NVIDIA):** v4D включає всі необхідні механізми для віртуалізації GPU. Це дозволяє одному потужному графічному процесору (наприклад, NVIDIA L40) обслуговувати до 32 інженерних робочих місць.
- **Обмеження використання:** Ліцензія дозволяє запускати на ESXi тільки VM, що безпосередньо стосуються Horizon (Connection Servers, UAG, App Volumes) та десктопи користувачів. **Заборонено** використовувати ці хости для запуску загальнокорпоративних серверів (Active Directory, SQL, Exchange тощо), якщо вони не виділені виключно під обслуговування VDI.

Компоненти, що потребують окремого ліцензування (Зовнішні покупки)

Це критичний розділ для бюджетування, оскільки OmniSSA не покриває 100% потреб VDI-проекту. Це має свою специфіку, на саме головне потребує придбання окремих ліцензій (табл. 2.4)

Таблиця 2.4. Додатковк ліцензування

Компонент	Вендор	Метрика	Чому купується окремо?
vSAN (Storage)	Broadcom	За обсягом (Per TiB)	Після зміни політики Broadcom, vSAN більше не входить у бандли Horizon. Його потрібно ліцензувати

Компонент	Вендор	Метрика	Чому купується окремо?
			окремо або використовувати класичні СЗД.
NSX (Network)	Broadcom	За ядрами (Per Core)	Необхідний для мікросегментації (захист кожної VM окремим фаєрволом). Це "золотий стандарт" безпеки VDI.
Windows OS	Microsoft	VDA або M365	OmniSSA не має права продавати ліцензії Microsoft. Для VDI потрібна спеціальна ліцензія Windows VDA або Microsoft 365 з правами віртуалізації.
NVIDIA vGPU	NVIDIA	За користувачам и	ПЗ для роботи графічних карт (vPC, vWS) ліцензується виключно через NVIDIA Enterprise [21].
SQL Server	Microsoft	Per Core / CAL	Потрібен для зберігання метаданих. Хоча Express версія безкоштовна, для великих інсталяцій потрібен SQL Standard/Enterprise.

Компоненти, що треба окремо придбати

Компонент	Власник	Тип ліцензії
 vSAN (Storage)	Broadcom	За обсягом (Per TiB)
 NSX (Network)	Broadcom	За ядрами (Per Core)
 Windows OS	Microsoft	VDA або M365
 NVIDIA vGPU	NVIDIA	За користувачами
 SQL Server	Microsoft	Per Core / CAL

Рис. 2.4 Компоненти з окремим ліцензуванням

Приблизний аналіз ліцензій – загальні цінові діапазони

Вибір метрики ліцензування напряду впливає на повернення інвестицій та особливості використання[18] (рис. 2.5):

- **Named User (NU):** Ліцензія закріплюється за обліковим записом у Active Directory. Користувач може підключатися до декількох десктопів одночасно. Цільова аудиторія: офісні співробітники, розробники.
- **Concurrent User (CCU):** Ліцензія рахується за активною сесією підключення. Це ідеально для кол-центрів, лікарень (позмінна робота), студентів. Дозволяє суттєво економити при великій кількості користувачів, що не працюють одночасно.

Слід враховувати, що Horizon поставляється у декількох типах. Перелік особливостей наведено у табл 2.5, а у табл 2.6 – перелік цен.

Таблиця 2.5 Перелік варіантів Horizon

Компонент	Horizon Standard	Horizon Advanced	Horizon Enterprise	Horizon Universal
vSphere / vCenter(vSphere for Desktop)	Включено	Включено	Включено	Опціональний Add-on
Доставка застосунків	Тільки VDI	VDI + RDSH	Повна автоматизація	Мультихмарна доставка
App Volumes	Відсутній	Включено (Standard)	Enterprise Edition	Включено
Instant Clones	Відсутні	Включено	Включено	Включено
Аналітика (DEEM)	Відсутня	Відсутня	Базова	Просунута (AI-driven)



Рис. 2.5 Типи ліцензій

Таблиця 2.6 Орієнтовна вартість передплати (MSRP на користувача):

Редакція	Тип метрики	1 рік (USD)	3 роки (Разом, USD)	5 років (Разом, USD)	Особливості використання
Standard	Named User (NU)	\$105 – \$130	\$270 – \$340	\$420 – \$530	Базовий VDI без RDSH та App Volumes.
Standard	Concurrent (CCU)	\$260 – \$320	\$680 – \$840	\$1,050 – \$1,300	Одночасні сесії для базових задач.
Advanced	Named User (NU)	\$150 – \$185	\$390 – \$480	\$600 – \$750	Додано RDSH та базовий App Volumes.
Advanced	Concurrent (CCU)	\$380 – \$460	\$980 – \$1,200	\$1,500 – \$1,850	Опimalьно для позмінної роботи з додатками.
Enterprise	Named User (NU)	\$210 – \$260	\$540 – \$690	\$850 – \$1,050	Повна автоматизація, Linux VDI, Session Recording.
Enterprise	Concurrent (CCU)	\$520 – \$680	\$1,350 – \$1,850	\$2,100 – \$2,800	Максимальний функціонал для змінної роботи.
Universal	Per User (SaaS)	\$260 – \$320	\$680 – \$840	\$1,050 – \$1,300	Мультихмарна підписка (On-prem + Azure/AWS).

Таким чином, перехід до Omnisia вимагає перегляду бюджетної стратегії, вибору систем оплати та ретельного вибору компонентів:

- True-up / True-down: Модель передплати дозволяє організаціям щорічно коригувати кількість ліцензій залежно від реального штату.

- ТСО: Підписка вже включає вартість Production Support 24/7 та доступ до всіх нових мажорних версій ПЗ. Це знижує загальні витрати на управління на 15-20% у довгостроковій перспективі [20].
- Особливості використання вбудованого vSphere for Desktop, щоб не платити Broadcom за ядра процесорів.
- Узгоджуйте ліцензії Microsoft та обов'язково перевірте наявність Microsoft SA або VDA для юридичної чистоти Windows-сесій.
- Переход на Instant Clones, скоротить потреби у Storage у 10 разів і спростить оновлення ПЗ.
- Обирайте ліцензію Universal для можливості швидкого розгортання резервного ЦОД в хмарі.

РОЗДІЛ 3. РОЗГОРТАННЯ ВІРТУАЛЬНОГО НАВЧАЛЬНОГО СЕРЕДОВИЩА

Загальна послідовність інсталювання VMware vSphere показана на рис.3.1. Ця послідовність використовується для всіх типів ліцензій.

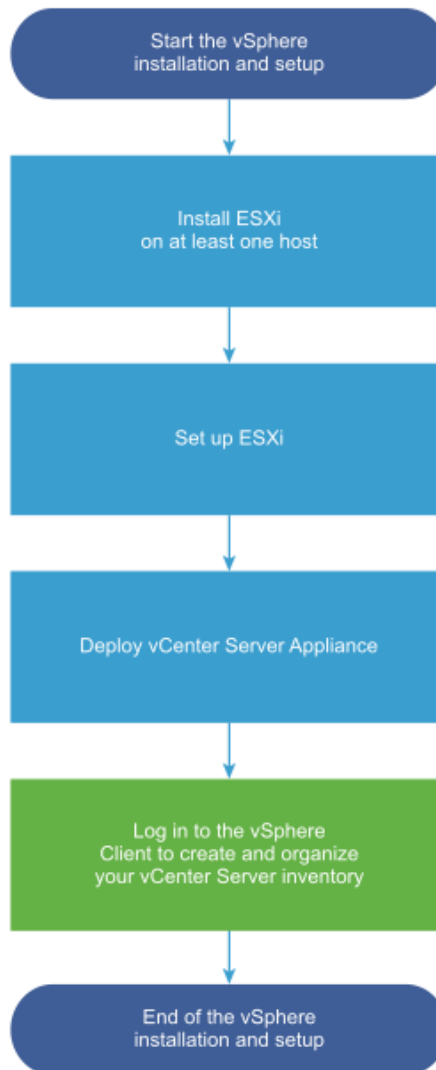


Рис. 3.1 Послідовність інсталювання

3.1 Повний огляд гіпервізора VMware ESXi (vSphere)

В попередньому розділі було наведено ґрунтовний аналіз сучасного програмного забезпечення та ліцензування від Broadcom. Таким чином, після

поглинання компанією Broadcom значна кількість ліцензій було скасовано. Тепер існують два основні пакети передплати та один додатковий.

- VMware Cloud Foundation (VCF) — "Все включено"
- VMware vSphere Foundation (VVF) — "Основна віртуалізація"
- vSphere Standard / Essentials Plus. Збережені тільки для найменших

До кожного типу ліцензії входить компонент ESX – самий нижній шар програмного забезпечення. **Компонент ESXi 7 – перший базовий елемент пропонуємого навчального середовища** (рис. 3.2). З цього компоненту починається всі процеси розгортання цієї системи. (ESXi 7 vs 8 vs 9).

Таблиця 3.1 Зведена таблиця порівняння версій

Характеристика	ESXi 7.0	ESXi 8.0	ESXi 9.0
Статус (2026)	EGS (End of General Support)	Mainstream (Стабільна)	Latest (Найновіша)
Модель драйверів	Native Only (vmklinux видалено)	Native + DPU Support	Native + Enhanced Offload
Завантажувальний диск	USB/SD допустимі (але ненадійні)	USB/SD Deprecated (потрібен дод. диск)	NVMe/SSD Обов'язковий (USB блокується)
Управління конфігом	Host Profiles (XML)	Configuration Profiles (JSON)	VCF Configuration Integration
Підтримка DPU (SmartNIC)	Ні	Так (Project Monterey, v1)	Так (Gen 2, повне розвантаження NSX/vSAN)
Максимум vGPU	Обмежена підтримка MIG	Покращена робота з Multi-Instance GPU	AI/ML Optimization (Shared Pass-Through)
Ліцензування	Perpetual (ключі) & Subscription	Переважно Subscription	Тільки Subscription (Cores)
TPM 2.0	Підтримується (Optional)	Рекомендується	Обов'язковий (Enforced Secure Boot)

Характеристика	ESXi 7.0	ESXi 8.0	ESXi 9.0
Життєвий цикл (LCM)	Baselines (VUM) & Images	Images (vLCM) пріоритетні	Тільки Images (Baselines видалені)



Рис. 3.2 ESXi – базовий компонент навчального середовища

Детальний огляд версій

Загальний огляд версій надано на рис 3.3.

VMware vSphere 9.0 (ESXi 9.0) — "Cloud Native Core"

- Реліз: Червень 2025.
- Архітектура: Ядро гіпервізора перероблено для роботи як "вузла" (Node) у складі VCF. Автономна робота можлива, але функціонал управління сильно зміщений у бік SDDC Manager [25].
- Storage Stack: Впроваджено новий протокол для роботи з NVMe-over-Fabrics, що знижує latency на 30% порівняно з ESXi 8.0.

VMware vSphere 8.0 (ESXi 8.0) — "Hardware Evolution"

- Реліз: Жовтень 2022.
- Project Monterey: Перша версія, що дозволила виносити мережеві служби (NSX) та служби зберігання (vSAN) на DPU (Data Processing Unit — SmartNIC), розвантажуючи основний CPU.

- **Config Store:** Перехід від монолітних файлів конфігурації до структурованої бази даних на хості, керованої через API.

VMware vSphere 7.0 (ESXi 7.0) — "Kubernetes Era"

- Реліз: Квітень 2020 (Підтримка закінчилася у 2025).
- Спадщина: Ця версія "вбила" старі драйвери (vmklinux), через що безліч старого обладнання перестало працювати. Також тут з'явилися vSphere with Tanzu (інтегрований K8s).

ЕВОЛЮЦІЯ ВЕРСІЙ VMWARE ESXi: ВІД KUBERNETES ДО CLOUD NATIVE

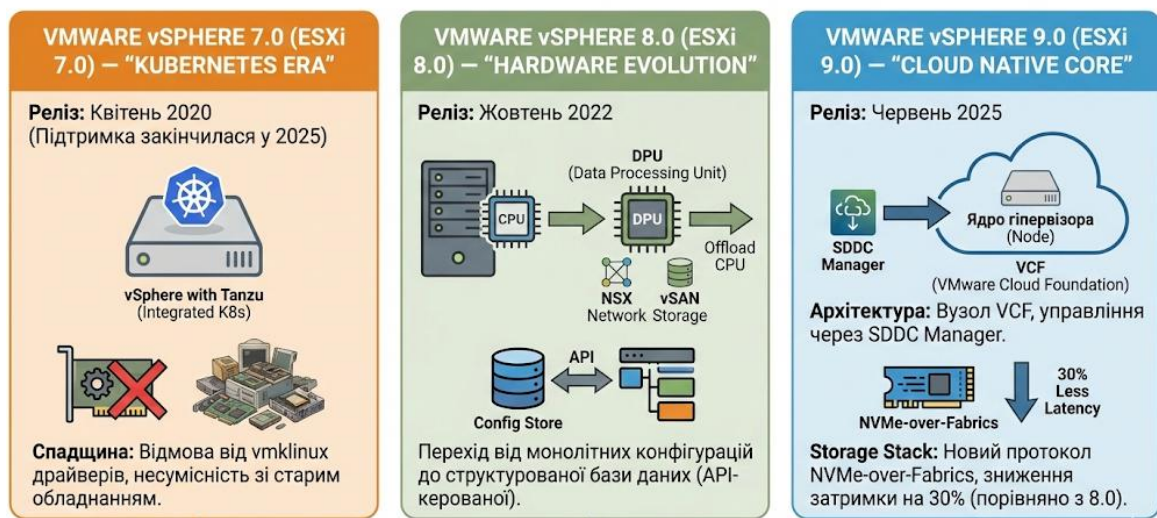


Рис. 3.3 Огляд версій ESX

Еволюція компонента ESXi

Сучасному інженеру важливо розуміти, що знаходиться у певних версіях, щоб правильно діагностувати проблеми [25].

Від Host Profiles до Configuration Profiles

- **Було (ESXi 7.0):** Host Profiles. Великоваговий механізм, що працює поверх vCenter. Часто викликав помилки "Compliance check failed" через дрібниці.
- **Стало (ESXi 8.0/9.0):** vSphere Configuration Profiles.
 - Конфігурація зберігається у вигляді JSON-документа.
 - Працює на рівні кластера (Cluster-level configuration).

- Якщо хост "дрейфує" від конфігу, ESXi може виправити це автоматично при перезавантаженні, не вимагаючи ручного "Remediate".

Зміна структури завантажувальних розділів

У старих версіях (6.x/7.0) розділи були фіксованими та маленькими. У 8.0+ введена динамічна розмітка:

- System Boot: Завантажувач (EFI).
- Boot Banks (0 і 1): Сама ОС (гіпервізор).
- ESX-OSData: Величезний розділ (мін. 32GB, рек. 128GB+), що об'єднує старі розділи Locker, Scratch та Core Dump. Саме цей розділ вбиває SD-карти кількістю операцій запису (IOPS). Тому USB-флешки більше не підходять для встановлення.

Вимоги до апаратної частини (Hardware Requirements)

Нижче наведено детальний розбір вимог за версіями (рис. 3.4).



Рис.3.4 Аналіз вимог до апаратної частини

Процесор (CPU). Усі версії вимагають 64-бітну архітектуру x86, увімкнені в BIOS інструкції NX/XD (Execute Disable Bit) та підтримку віртуалізації (Intel VT-x / AMD RVI).

- ESXi 7.0:
 - Мінімальні вимоги: 2 фізичних ядра.
 - Підтримувані сімейства: Широкий спектр legacy-обладнання.
 - Intel: Xeon E5-2600 v1/v2 (Sandy Bridge, Ivy Bridge), Xeon E3, Core i7-4xxx.
 - AMD: Opteron 4000/6000 Series.

Нюанс: Це остання версія, "терпима" до процесорів 2012-2015 років випуску.

- ESXi 8.0:
 - a. Жорстке відсікання: Безліч процесорів, підтримуваних у 7.0, оголошені EOL.
 - b. Видалено підтримку: Intel Sandy Bridge, Ivy Bridge та частково Haswell.
 - c. Рекомендований мінімум:
 - i. Intel: Xeon Scalable (Skylake/Cascade Lake) і новіші.
 - ii. AMD: EPYC 7000 Series (Naples/Rome).
- ESXi 9.0:
 - a. Сучасний стандарт: Вимагає CPU з підтримкою розширених інструкцій для шифрування та AI.
 - b. Приблизний зріз: Процесори, випущені після 2019-2020 року.
 - c. Увага: Якщо при встановленні на старий CPU 8.0 видавав Warning (який можна було обійти прапором allowLegacyCPU), то 9.0 гарантовано зупинить встановлення (PSOD або Fatal Error).

Оперативна пам'ять (RAM)

- ESXi 7.0:

- a. Технічний мінімум для встановлення: 4 ГБ (неофіційно), 8 ГБ (офіційно).
 - b. Рекомендовано для продакшену: 12 ГБ+.
- ESXi 8.0 / 9.0:
 - a. Технічний мінімум інсталятора: 8 ГБ (встановлення може пройти, але служби не стартують).
 - b. Реальний мінімум (VCF/vCenter agent): **12-16 ГБ** тільки для гіпервізора.
 - c. Рекомендовано: 64 ГБ і вище, оскільки сучасні служби (nsx-opsagent, vsan-health) споживають значно більше пам'яті.

Завантажувальні носії (Storage) — Еволюція вимог

Найкритичніша зміна для інженерів, які звикли ставити ESXi на флешки.

- ESXi 7.0:
 - a. Допустимо: Встановлення на USB-флешки та SD-карти високої якості (8GB+).
 - b. Застереження: Вже у версії 7.0 U2 з'явилися попередження про деградацію SD-карт через частий запис логів.
- ESXi 8.0:
 - a. Статус: Використання USB/SD як *єдиного* завантажувального пристрою — Deprecated (Застаріло).
 - b. Вимога: Якщо ви завантажуєтеся з USB, ви зобов'язані надати локальний HDD/SSD диск мінімум на 32 ГБ для розділу ESX-OSData. Без цього диска ви отримаєте попередження про персистентність логів.
- ESXi 9.0:
 - a. Заборонено: Завантаження з SD-карт та USB-флешок у режимі Boot-Only блокується або робить систему Unsupported.

- b. Стандарт: M.2 NVMe SSD (мінімум 32 ГБ, краще 64+ ГБ) або SATADOM.

Мережа (Network)

- ESXi 7.0: Повна відмова від драйверів vmklinux. Старі карти (наприклад, Realtek 8168 або древні Intel PRO/1000), які працювали в 6.7, перестали визначатися.
- ESXi 8.0 / 9.0:
 - a. **HCL Strict Mode:** Використовуйте тільки серверні адаптери (Intel X710/E810, Mellanox ConnectX-5/6, Broadcom).
 - b. **Швидкість:** Рекомендується мінімум 10GbE. 1GbE допустимий тільки для управління (Mgmt), але не для трафіку vSAN/vMotion/NSX у сучасних кластерах.

Послідовність встановлення (Step-by-Step)

Підготовка

- Перевірка HCL: Критично важлива для ESXi 9.0. Звіртеся з офіційним списком сумісності [26].
- Образ: Завантажуйте ISO ESXi 9.0 з порталу Broadcom [26]. Настійно рекомендується Custom Image від вендора (Dell, HPE, Lenovo).
- UEFI: Режим Legacy BIOS (CSM) не рекомендований і може не підтримуватися на новому залізі. Вмикайте чистий UEFI + Secure Boot.

Процес встановлення (Console), та особливості налаштування

Копії екранів процесу встановлення наведено у додатку А

1. Завантаження з ISO (через iDRAC/iLO).
2. Welcome Screen: Enter.
3. EULA: F11.
4. Disk Selection:
 - ESXi 9.0 проведе сувору перевірку диска. Якщо диск "зношений" (SMART) або не підходить за типом, встановлення може перерватися.

- При оновленні (Upgrade) з 7.0 на 9.0 переконайтеся, що розмітка диска сумісна. Прямий апгрейд з 6.7 неможливий.
5. Layout & Password: Вибір розкладки та встановлення пароля root.
 6. Install: F11.
 7. Reboot: Перезавантаження.

Первинне налаштування (DCUI)

1. Мережа (F2 -> Configure Management Network):
 - Призначте Static IP, Mask, Gateway.
 - IPv6: Якщо не використовується, рекомендується вимкнути (вимагає перезавантаження), хоча VCF 9.0 активно просуває IPv6.
2. DNS/Hostname: Обов'язково коректний FQDN та DNS-записи (A та PTR). Без цього не встане vCenter 9.0.
3. Troubleshooting: Увімкніть SSH тільки на час налаштування.

Особливості

vSphere Lifecycle Manager (vLCM) У версії 9.0 vLCM — єдиний правильний спосіб управління оновленнями.

- Використовуються **Images** (Образи кластера).
- Baseline (старий метод через VUM) остаточно йде в минуле.

Certificate Management. У 9.0 посилено роботу з сертифікатами. Самопідписані сертифікати (Self-signed) браузері та суміжні системи блокують агресивніше. Плануйте інтеграцію з корпоративним СА.

Через нові драйвери (особливо мережеві стеки під DPU) можливі "дитячі хвороби" на ранніх зборки 9.0. Завжди перевіряйте наявність патчів (Patch 01/02) відразу після встановлення GA версії.

Остаточне налаштування

Після встановлення буде доступним основний компонентт налаштувань ESXi – доступ через браузер на адресу мережевого адаптеру, що налаштовано (при інсталюванні на Management. В межах цієї роботи не будемо розглядати ці етапи. На рисунка 3.5 -3.8 показан зовнішній вигляд певних особливостей

версії 7, але різних зборок у Додатку Б наведено інші копії екрану налаштувань.

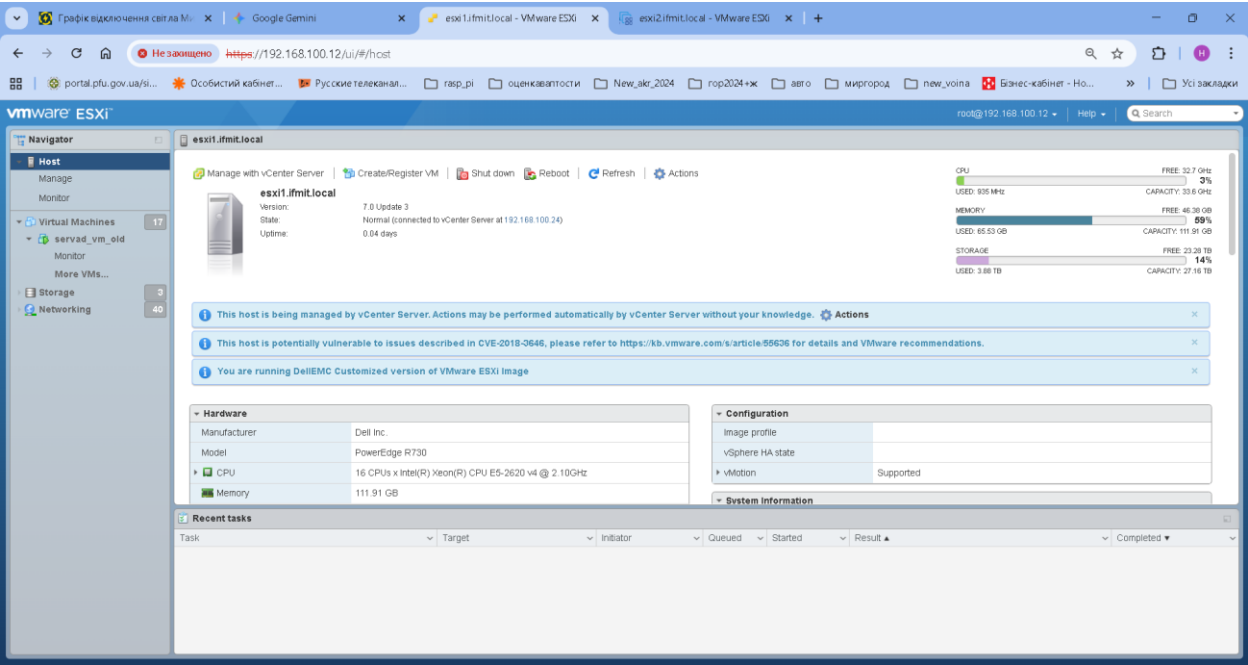


Рис. 3.5 Параметри Хоста (зборка 1)

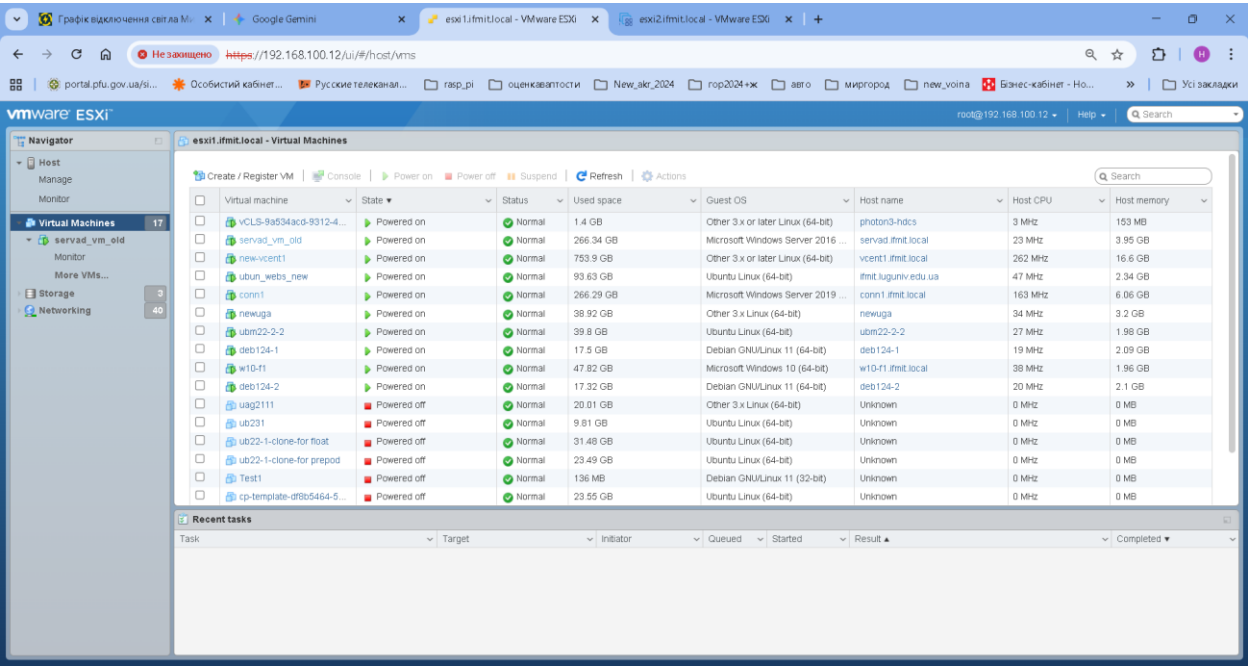


Рис. 3.6 Параметри віртуальних машин (зборка 1)

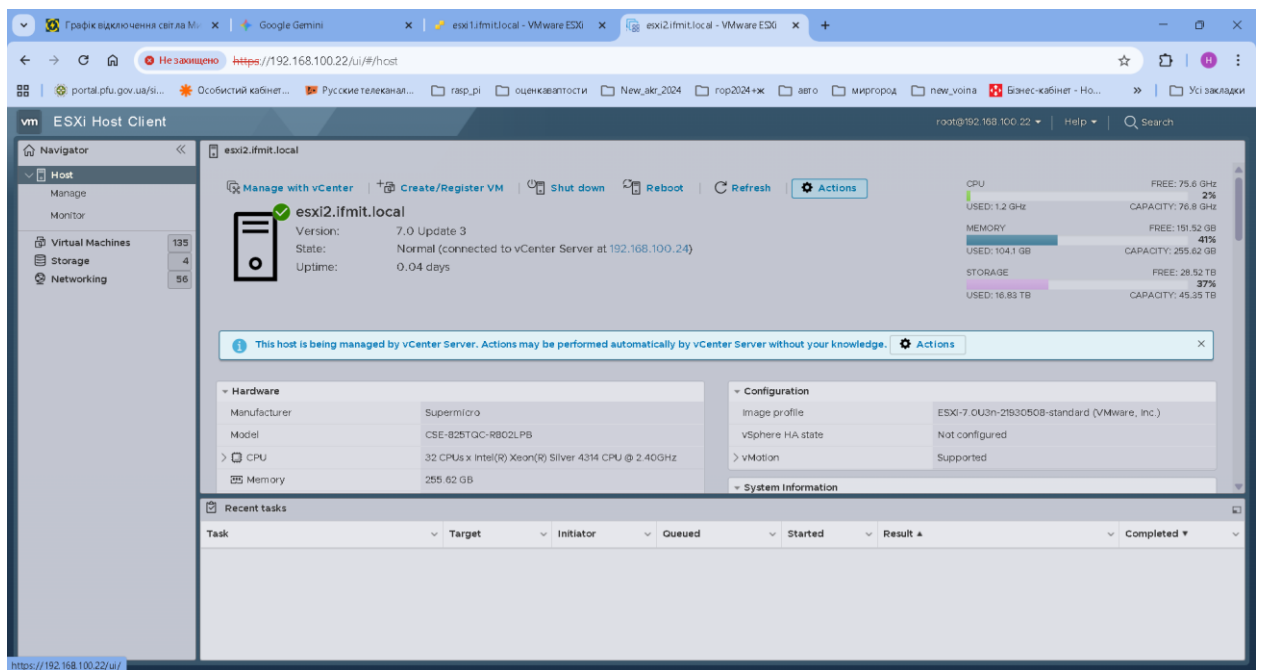


Рис. 3.7 Параметри Хоста (зборка 2)

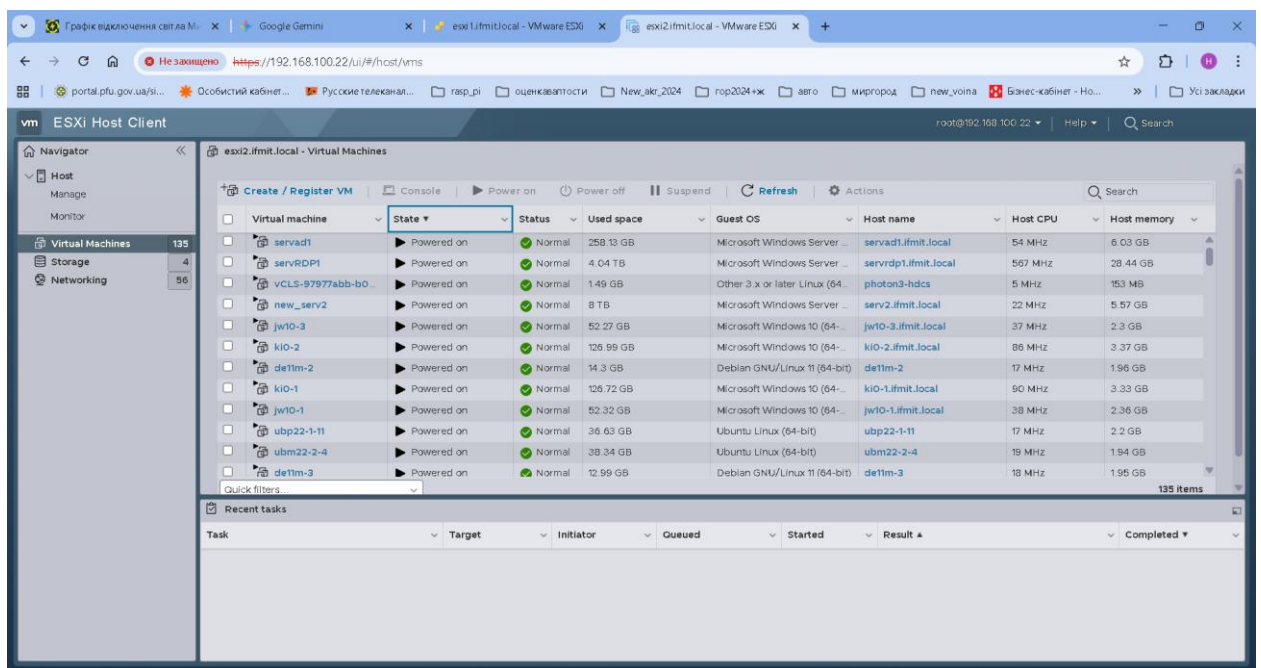


Рис. 3.8 Параметри віртуальних машин (зборка 2)

3.2 Огляд vSphere – компонент vCenter

vCenter Server — це централізована платформа управління інфраструктурою VMware vSphere. Це ключовий компонент, без якого неможливі кластеризація (HA, DRS), розподілений комутатор (vDS), vMotion та управління життєвим циклом (Lifecycle Manager). vCenter Server – це другий базовий компонент навчального середовища. vCenter Server - це основний компонент для створення навчального середовища (рис. 3.10).

- vCenter Server 7.x
- vCenter Server 8.x
- vCenter Server / VCF 9 (The Future / New Standard)

Розглянемо основні особливості цих версій.



Рис.3.10 Версії та особливості vCenter Server

Архітектура та Версії

На даний момент у корпоративному секторі зустрічаються три гілки. Важливо розуміти їхній статус в екосистемі Broadcom:

vCenter Server 7.x

- Статус: Mature / End of Support Approaching.
- Особливості: Остання версія, яка масово використовувалася до поглинання Broadcom.

- Архітектура: Прибрано зовнішній PSC, перехід на чисте використання vCenter Server Appliance (VCSA).
- Ризики: Підтримка закінчується (EOS у 2025 році), рекомендується планувати міграцію.

vCenter Server 8.x

- Статус: Current Mainstream (Актуальна).
- Особливості: Впровадження архітектури vSphere Distributed Services Engine (робота з DPU).
- Покращення: Значно перероблено DRS та vMotion (Unified Data Transport).
- Інтеграція: Повна підтримка хмарних консолей та аддонів VVF/VCF.

vCenter Server / VCF 9 (The Future / New Standard)

- Статус: Unified Platform (VCF 9).
- Контекст: Broadcom анонсувала VCF 9 як єдину платформу, покликану усунути розрізненість версій (раніше vCenter міг бути 8.0, NSX 4.1, SDDC Mgr 5.1).
- Мета: "Дев'ятка" спрямована на створення єдиного уніфікованого продукту, де vCenter стає менш помітним "під капотом" загальної хмарної платформи.
- Фокус:
 - a. **Native Cyber Resilience:** Посилена безпека "з коробки".
 - b. **Private AI:** Глибока інтеграція інструментів для запуску ШІ-навантажень.
 - c. **Спрощення:** Єдина консоль управління та API для всіх компонентів (Compute, Network, Storage).

Розвиок архітектури (VCSA)

Загальний огляд процесу розвитку архітестури vCenter наведено на рис. 3.11.

- ОС: Раніше vCenter можна було ставити на Windows Server. Зараз це виключно vCenter Server Appliance (VCSA) на базі пропрієтарної ОС VMware Photon OS (Linux).
- Database: Вбудована PostgreSQL (vPostgres). Підтримка зовнішніх баз даних (Oracle/MS SQL) повністю припинена.
- PSC (Platform Services Controller). У версіях 7.0 та вище концепцію зовнішнього (External) PSC повністю видалено. Тепер використовується виключно архітектура Embedded PSC (вбудований у VCSA), що спрощує топологію та усуває проблеми реплікації між контролерами. [27], [28], [29]. Призначення PSC – об'єднує загальні служби інфраструктури, забезпечуючи безпеку та управління доступом. Ключові компоненти PSC:
 - a. vCenter Single Sign-On (SSO): Служба аутентифікації (STS), що дозволяє входити в різні компоненти vSphere (vCenter, NSX, Aria) під одним обліковим записом.
 - b. VMware Certificate Authority (VMCA): Кореневий центр сертифікації, що видає сертифікати для хостів ESXi та сервісів vCenter.
 - c. Licensing Service: Централізоване управління ліцензійними ключами.
 - d. Lookup Service: Реєстр служб, що дозволяє компонентам vSphere знаходити один одного.
 - e. VMware Directory Service (vmdir): Служба каталогів (LDAP) для домену SSO (за замовчуванням vsphere.local).

Еволюція архітектури VMware vCenter (VCSA)

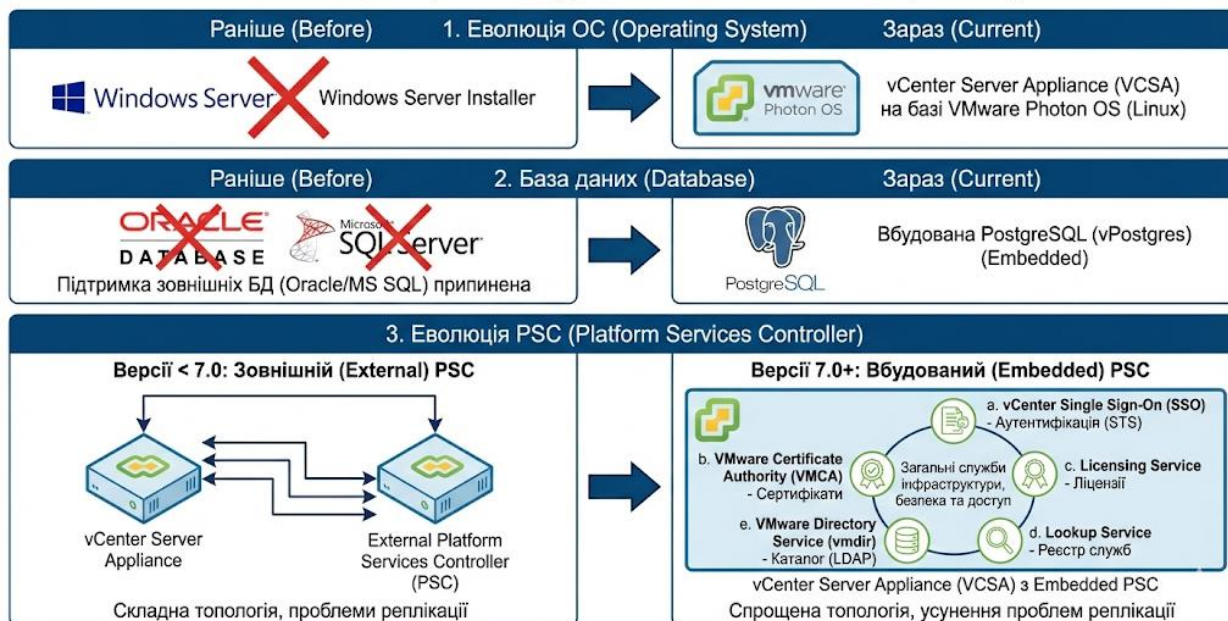


Рис. 3.11 Розвиток архітектури vCenter

Слід враховувати сумісність версій ESX та vCenter. У таблиці 3.2 наведено перлік сумісних версій

Таблиця 3.2 Матриця сумісності (Interoperability Matrix)

Версія vCenter Server	Підтримувані версії ESXi	Коментар інженера
vCenter 9.0	ESXi 9.0 ESXi 8.0 U3	Підтримка ESXi 7.0 та старіших повністю вилучена. Перед апгрейдом vCenter до 9.0 переконайтеся, що всі хости мінімум версії 8.0 U3.
vCenter 8.0	ESXi 8.0 ESXi 7.0 ESXi 6.7 (до EOL)	Найбільш універсальна версія для перехідного періоду. Дозволяє керувати змішаним кластером під час міграції.
vCenter 7.0	ESXi 7.0 ESXi 6.7 ESXi 6.5	Не підтримує ESXi 8.0. Якщо ви купили новий сервер з ESXi 8.0, ви не зможете підключити його до старого vCenter.

Вимоги до апаратної частини (Sizing)

Сайзинг vCenter критично важливий. Нестача RAM призведе до падіння служб (особливо vmware-vpxd та vsphere-ui). Ресурси вибираються під час встановлення. Вимоги до vCenter Server 8.0 / 9.0 (Актуальні) наведені у табл 3.3 , а до vCenter Server 7.0 у таблиці 3. 4

Таблиця 3.3 Параметри vCenter Server 8.0 / 9.0

Розмір (Size)	vCPU	RAM (GB)	Storage (GB)*	Хостів	ВМ	Примітка
Tiny	2	14	599	До 10	До 100	Lab / Small ROBO
Small	4	19	653	До 100	До 1000	Малий продакшн
Medium	8	28	856	До 400	До 4000	Стандартний Enterprise
Large	16	37	1290	До 1000	До 10 000	Великі ЦОД
X-Large	24	58	1993	До 2000	До 35 000	Масштаб провайдера

Таблиця 3.3 Параметри vCenter Server 7

Розмір (Size)	vCPU	RAM (GB)	Storage (GB)*	Хостів	ВМ	Примітка
Tiny	2	12	415	До 10	До 100	Lab / Test
Small	4	19	480	До 100	До 1000	Production
Medium	8	28	700	До 400	До 4000	Production
Large	16	37	1060	До 1000	До 10 000	Production
X-Large	24	56	1800	До 2000	До 35 000	High Load

Попередні вимоги (Prerequisites) до початку встановлення

Це найважливіший етап. 90% проблем зі встановленням трапляються через ігнорування цих пунктів.

1. DNS (Domain Name System):

- **Обов'язково:** Створити А-запис (Forward) та PTR-запис (Reverse) для майбутнього vCenter на DNS-сервері.

- *Приклад:* vcsa.corp.local -> 192.168.1.10 та 192.168.1.10 -> vcsa.corp.local.
- Інсталятор перевірить вирішення імен. Якщо PTR немає — встановлення впаде на 2-му етапі.

2. NTP (Time Sync):

- Час на хості ESXi, де буде розгорнуто vCenter, має бути синхронізовано.
- Розбіжність часу викличе помилку аутентифікації SSO.

3. Мережа:

- Статична IP-адреса для vCenter.
- Доступність шлюзу та DNS з підмережі управління (Management Network).

Послідовність встановлення

Встановлення vCenter 8.0/9.0 відбувається методом "Installer з клієнтської машини" (Windows/Mac/Linux) на цільовий хост ESXi. Перелік копій екрану процесу встановлення vCenter 7 наведено у Додатку В

Процес розділений на **два етапи (Stage 1 та Stage 2)**.

Підготовка

1. Завантажте ISO-образ з порталу Broadcom Support (потрібна активна передплата VVF/VCF).
2. Змонтуйте ISO на робочій станції інженера.
3. Запустіть installer.exe з папки vcsa-ui-installer\win32.

Stage 1: Deployment (Розгортання OVF)

На цьому етапі на ESXi просто копіюються бінарні файли та створюється віртуальна машина.

1. Target ESXi: Вкажіть IP хоста ESXi, логін root та пароль.
2. VM Settings: Ім'я VM (в інвентарі ESXi) та пароль root для самої Photon OS.
3. Deployment Size: Виберіть розмір (Tiny/Small...) залежно від запланованого навантаження.

4. Datastore: Виберіть сховище. Рекомендується включити "Thin Disk Mode" (Тонкий диск) для економії місця, якщо це не високонавантажений Tier-1 сторадж.
5. Network Settings: Введіть IP, Mask, Gateway, DNS та FQDN (обов'язково FQDN, якщо є DNS).
6. *Запуск*: Інсталятор залле OVF-шаблон на хост і увімкне VM.

Stage 2: Configuration (Налаштування сервісів)

Після успішного деплою починається налаштування "нутрошів".

1. Time Sync: Синхронізація з NTP серверами (рекомендується) або з хостом ESXi.
2. SSO Configuration (Single Sign-On):
 - Створення нового домену SSO. Стандарт: vsphere.local.
 - Створення пароля для administrator@vsphere.local (це головний "God-mode" акаунт).
3. CEIP: Участь у програмі покращення (зазвичай відключають у закритих контурах).
4. *Фіналізація*: Система застосує налаштування, запустить служби, створить базу даних.

Після того, як веб-інтерфейс (<https://<fqdn-vcenter>>) став доступним:

1. **Ліцензування**:
 - Зайти в Administration -> Licenses. Ввести ключі для vCenter та хостів ESXi.
 - *Увага*: У нових версіях VCF ключі можуть пушитися через Cloud Gateway, але локальне введення все ще працює для VVF/Standard.
2. **Identity Sources**:
 - Підключення до Active Directory (LDAP або Integrated Windows Auth). Додавання груп адміністраторів AD до полі Administrators у vCenter.
3. **Створення ієрархії**:

- Datacenter -> Cluster -> Add Hosts.
- Налаштування EVC (Enhanced vMotion Compatibility), якщо процесори хостів різних поколінь.

4. vCenter HA (High Availability):

- Архітектура vCenter HA передбачає створення трьох нод: Active, Passive, Witness.
- Вимагає окремої мережі (vCenter HA Network) з latency менше 10ms.

5. Резервне копювання (Backup):

- vCenter (VCSA) має вбудований механізм бекапу (File-Based Backup).
- Налаштовується у VAMI інтерфейсі (<https://<fqdn-vcenter>:5480>).
- Бекап робиться за протоколами (SFTP, NFS, SMB, HTTPS) на зовнішній сервер. Снепшоти ВМ vCenter як метод бекапу не рекомендуються для довгострокового зберігання через базу даних.

Після встановлення використовуємо ВЕБ сторінку за адресом, що вказана при встановленні vCenter. Приклади сторінок показано на рисунках 3.12 – 3.14

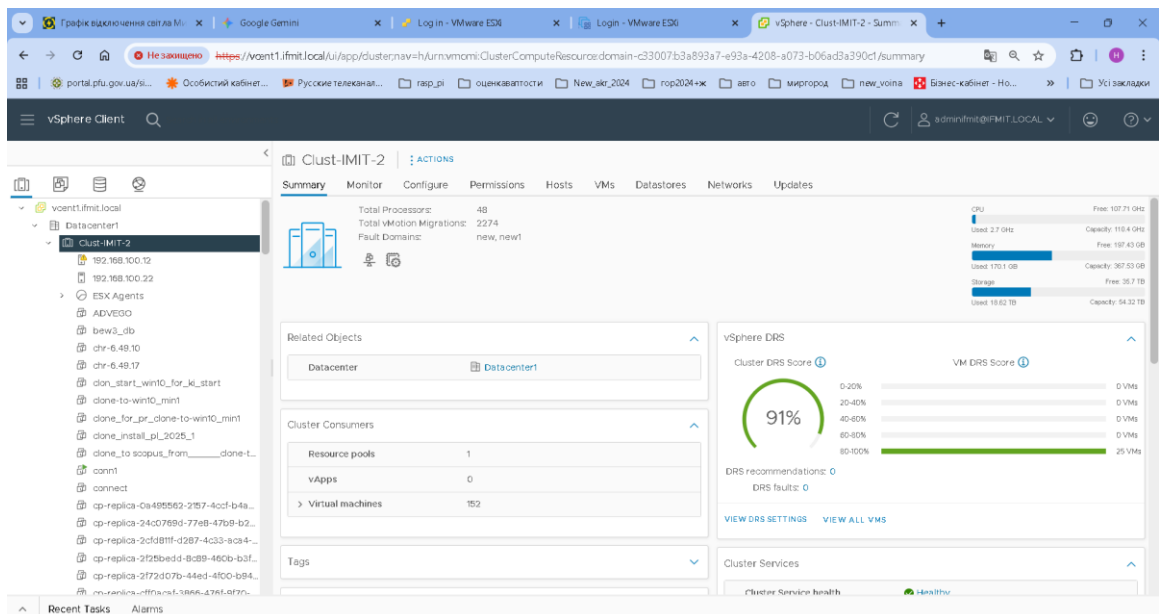


Рис.3.12 Параметри vCenter

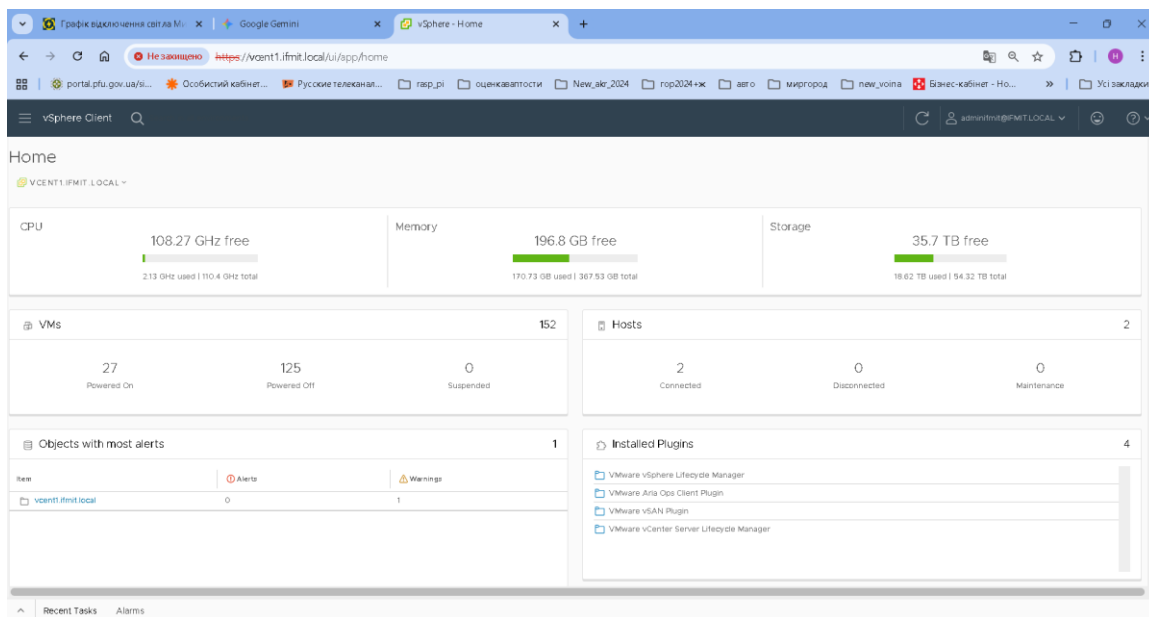


Рис.3.13 Параметри vCenter

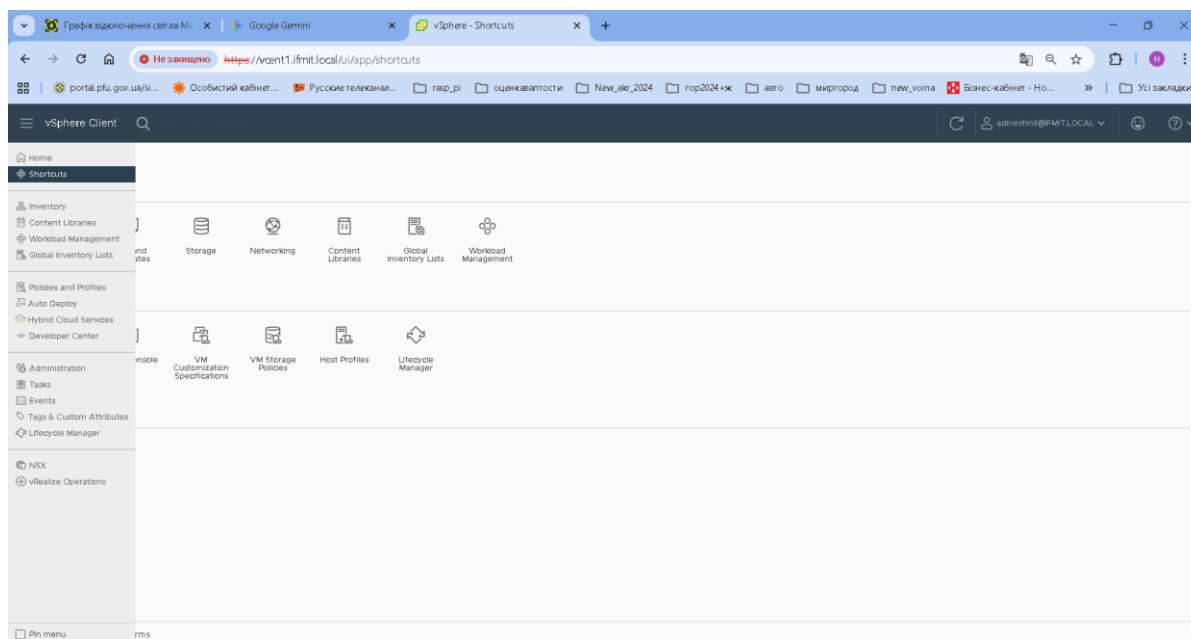


Рис.3.14 Параметри vCenter

3.3 Аутентифікації у vCenter – основа для корпоративного доступу

При аналізі системи аутентифікації використовувався детальний опис наведений у [23]. Встановлено, що у версії vSphere 7.0 відбулися

фундаментальні зміни в архітектурі сервісів аутентифікації, спрямовані на спрощення топології та зниження експлуатаційних витрат. Ключовим моментом є повна та остаточна відмова від концепції зовнішніх контролерів служб платформи (External Platform Services Controller — PSC).

Починаючи з vSphere 7.0, розгортання нового vCenter Server або оновлення до цієї версії передбачає використання виключно **вбудованого (embedded)** Platform Services Controller.

- Спрощення топології: Раніше адміністраторам доводилося керувати складними топологіями з реплікацією між зовнішніми вузлами PSC, які часто вимагали балансувальників навантаження. У vSphere 7.0 усі сервіси (SSO, ліцензування, сертифікати) працюють всередині одного віртуального модуля (appliance), що виключає мережеві затримки між компонентами управління та аутентифікації.
- Відсутність підтримки External PSC: Інсталятор vSphere 7.0 більше не надає можливості розгортання зовнішнього PSC. Будь-яка спроба розгорнути нову інсталяцію включатиме вбудований PSC за замовчуванням.

Для середовищ, що оновлюються з версій 6.5 або 6.7, де використовувалися зовнішні PSC, процес оновлення включає обов'язкову міграцію.

- Автоматична конвергенція: Під час оновлення (Upgrade) інсталятор автоматично виявляє зовнішню топологію та виконує процес конвергенції (Converge). Функціонал зовнішнього PSC переноситься всередину оновлюваного vCenter Server Appliance (VCSA), а старий зовнішній вузол PSC виводиться з експлуатації (decommission).
- vCenter Server Converge Tool: У попередніх версіях (6.7 U1+) це була окрема утиліта CLI/GUI. У версії 7.0 логіка конвергенції вбудована безпосередньо в процес оновлення, що знижує ризик людської помилки.

Аналіз vCenter Single Sign-On (SSO)

vCenter Single Sign-On (SSO) залишається центральним шлюзом аутентифікації, але його внутрішня логіка та можливості інтеграції були розширені. SSO забезпечує не просто вхід користувача, а створює безпечний домен довіри для всіх рішень VMware (vCenter, NSX-T, vRealize/Aria).

Взаємодія компонентів відбувається наступним чином:

- **Security Token Service (STS):** Серце системи SSO. STS діє як провайдер ідентифікації, випускаючи токени SAML 2.0. Ці токени підписуються сертифікатом STS (STS Signing Certificate), валідність якого є критичною для функціонування всього середовища. Якщо цей сертифікат втрачає чинність, доступ до vCenter втрачається повністю.
- **Administration Server:** Надає API та інтерфейс для конфігурування SSO. Саме через цей компонент адміністратори керують політиками паролів та джерелами ідентифікації.
- **vCenter Lookup Service:** Служба каталогу сервісів. Коли ви встановлюєте, наприклад, Site Recovery Manager (SRM) або NSX, вони реєструються в Lookup Service, щоб vCenter знав їхні endpoint'и. Це критично важливий компонент для взаємодії "Machine-to-Machine".

Під час інсталяції створюється локальний домен (за замовчуванням vsphere.local).

- **Administrator@vsphere.local:** Обліковий запис "суперкористувача". На відміну від root (адміністратор OS Photon), цей користувач керує прикладним рівнем віртуалізації.
- **System Domain User Groups:** У vSphere 7.0 попередньо встановлено багато сервісних груп (наприклад, *DCAdmins*, *ComponentManager.Administrators*), членство в яких надає права на виконання специфічних системних викликів. Модифікація цих груп

вручну не рекомендується, за винятком додавання адміністраторів до групи *Administrators*.

Джерела ідентифікації (Identity Sources)

Для інтеграції з корпоративними службами каталогів vCenter 7.0 підтримує кілька механізмів, при цьому спостерігається явний зсув у бік федеративних сервісів.

Identity Provider Federation (Ключове нововведення v7)

Це найбільш значуща зміна в аутентифікації vSphere 7.0.

- Принцип роботи (OAuth2 / OIDC): Замість того, щоб vCenter сам перевіряв логін і пароль (як у LDAP/IWA), він перенаправляє користувача на зовнішній провайдер (наприклад, Microsoft ADFS). Користувач вводить пароль на сторінці ADFS, проходить там MFA, і vCenter отримує лише підписаний токен доступу (Identity Token).
- Переваги безпеки: vCenter Server ніколи не бачить і не обробляє паролі користувачів AD. Це зменшує поверхню атаки та виключає ризик компрометації облікових даних через логи vCenter.
- Реалізація MFA: Оскільки аутентифікація відбувається на стороні IdP (ADFS), ви можете використовувати будь-які методи MFA, налаштовані у вашому корпоративному середовищі (Azure MFA, Duo, Okta через ADFS), без необхідності встановлювати додаткові плагіни у vCenter.

Традиційні методи (Legacy)

1. Active Directory (Integrated Windows Authentication - IWA):

- Дозволяє vCenter приєднатися до домену AD як комп'ютерний об'єкт (SPN).
- *Важливо:* Хоча IWA підтримується у vSphere 7.0, VMware оголосила цей метод застарілим (deprecated) на користь федерації та LDAPS, оскільки IWA складний у діагностиці та залежить від протоколів SMB/RPC.

2. Active Directory over LDAP / OpenLDAP:

- Пряме підключення до LDAP-каталогу.
- *Безпека:* Настійно рекомендується використовувати **LDAPS (LDAP over SSL)**. У vSphere 7.0 посилено вимоги до перевірки сертифікатів контролерів домену при налаштуванні LDAPS.

Управління сертифікатами

vCenter 7.0 надає гнучку модель управління SSL-сертифікатами, засновану на службі **VECS (VMware Endpoint Certificate Store)**. Правильний вибір режиму управління сертифікатами є критичним для стабільності системи.

VMware Certificate Authority (VMCA) як Root CA

У кожен vCenter вбудовано власний центр сертифікації (VMCA).

- Автоматизація: При додаванні хоста ESXi в інвентар, vCenter автоматично замінює самопідписаний сертифікат хоста на новий, підписаний VMCA. Це забезпечує ланцюжок довіри всередині кластера.
- Термін дії: За замовчуванням сертифікати, що видаються VMCA, мають тривалий термін дії, але адміністратор може ініціювати їх перевипуск через CLI або GUI.

Розглянемо різноманітні режими роботи

- Fully Managed (Повністю керований):
 - а. *Суть:* Використовується "з коробки". VMCA підписує все.
 - б. *Плюси:* Нульові витрати на адміністрування при додаванні хостів.
 - в. *Мінуси:* Браузери адміністраторів видаватимуть помилку "Not Secure", доки кореневий сертифікат VMCA не буде додано до довірених на робочих станціях.
- Hybrid Mode (Гібридний режим — Best Practice):

- a. *Суть:* Замінюється **тільки** сертифікат, що відповідає за веб-інтерфейс (Machine SSL Certificate), на сертифікат від корпоративного CA (Microsoft CA, GlobalSign тощо). Внутрішні сертифікати (Solution User Certificates) залишаються під управлінням VMCA.
- b. *Чому це найкращий вибір:* Це усуває помилки SSL у браузері, але не змушує адміністратора вручну оновлювати десятки внутрішніх сертифікатів сервісів vSphere, що часто призводило до збоїв у попередніх версіях.
- Custom Mode (Користувачський режим):
 - a. *Суть:* Повна заміна всіх сертифікатів (включаючи внутрішні сервіси) на зовнішні.
 - b. *Ризики:* Метод вкрай трудомісткий. Помилка в одному сертифікаті може призвести до недоступності vCenter. Рекомендується лише для організацій з найжорсткішими вимогами Compliance (наприклад, військові стандарти), де використання самопідписаних CA заборонено.

Основним інструментом є утиліта командного рядка, доступна через SSH:

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

Вона пропонує меню з 8 опцій, що покриває всі сценарії: від заміни Machine SSL (Опція 1) до повної регенерації всіх сертифікатів VMCA у разі компрометації або закінчення терміну дії (Опція 4 або 8).

Політики безпеки

У рамках SSO адміністратори можуть налаштовувати політики, що впливають на безпеку сесій та облікових записів.

Політики паролів та блокувань, це:

- *Складність:* Налаштування вимог до паролів для локальних користувачів (довжина, спецсимволи).

- Lockout Policy: Критично важлива для захисту від Brute-force атак. Дозволяє задати кількість невдалих спроб входу та час автоматичного розблокування.

Політики часу життя токенів (Token Lifetime). Ці налаштування часто ігноруються, але вони важливі для безпеки та інтеграцій:

- Clock Tolerance: Допустима різниця в часі між клієнтом та сервером.
- Maximum Token Lifetime: Максимальний час життя SAML-токена. За замовчуванням 8 годин. Це означає, що навіть при активній роботі сесія може закінчитися, якщо не налаштовано оновлення (Renewable).
- Renewable Lifetime: Період, протягом якого токен може бути оновлений без повторного введення пароля. Це впливає на UX адміністраторів та роботу скриптів автоматизації, що використовують сесійні токени.

Двофакторна аутентифікація (2FA)

vCenter 7 відходить від пропрієтарних методів у бік відкритих стандартів.

1. Smart Card (PIV/CAC): Широко використовується в держсекторі. Вимагає наявності кард-рідерів та інфраструктури PKI. vCenter зіставляє сертифікат на смарт-картці з користувачем в AD (через UPN або SAN).
2. RSA SecurID: Нативна інтеграція. Вимагає наявності сервера RSA Authentication Manager. Користувач вводить PIN + Token Code під час входу. Це надійний, але застарілий метод порівняно з хмарними MFA.
3. Federation (AD FS) — Сучасний стандарт MFA:
 - Як згадувалося в розділі Identity Sources, це **єдиний** спосіб використовувати сучасні методи аутентифікації (Push-сповіщення, біометрія телефону, FIDO2 ключі) з vCenter.
 - vCenter не "знає" про те, який другий фактор використовувався; він просто довіряє твердженню (Claim) від ADFS, що користувач успішно пройшов перевірку.

Таким чином, необхідно врахувати наступне:

1. При плануванні впровадження vCenter 7.0 повністю виключіть з дизайну зовнішні PSC. Використовуйте вбудовану архітектуру з увімкненим VCHA (vCenter HA), якщо потрібна висока доступність, оскільки це більше не вимагає зовнішніх балансувальників.
2. Для корпоративних середовищ (Enterprise) перехід на Identity Provider Federation є пріоритетним. Це не тільки спрощує реалізацію MFA, але й готує інфраструктуру до майбутніх оновлень, де підтримка Legacy-протоколів (IWA) може бути припинена.
3. Використовуйте Гібридний режим (Hybrid) як золотий стандарт. Замініть сертифікат Machine SSL на довірений корпоративний, щоб забезпечити "зелений замок" у браузері, але залиште управління внутрішніми сертифікатами (Solution Users, ESXi hosts) за VMCA. Це забезпечить баланс між безпекою та операційною стійкістю.
4. Моніторинг: Впровадьте моніторинг терміну дії STS-сертифіката. Його закінчення не видно у звичайному інтерфейсі "Certificate Management", але призводить до повної непрацездатності входу в систему (рис.3.15).

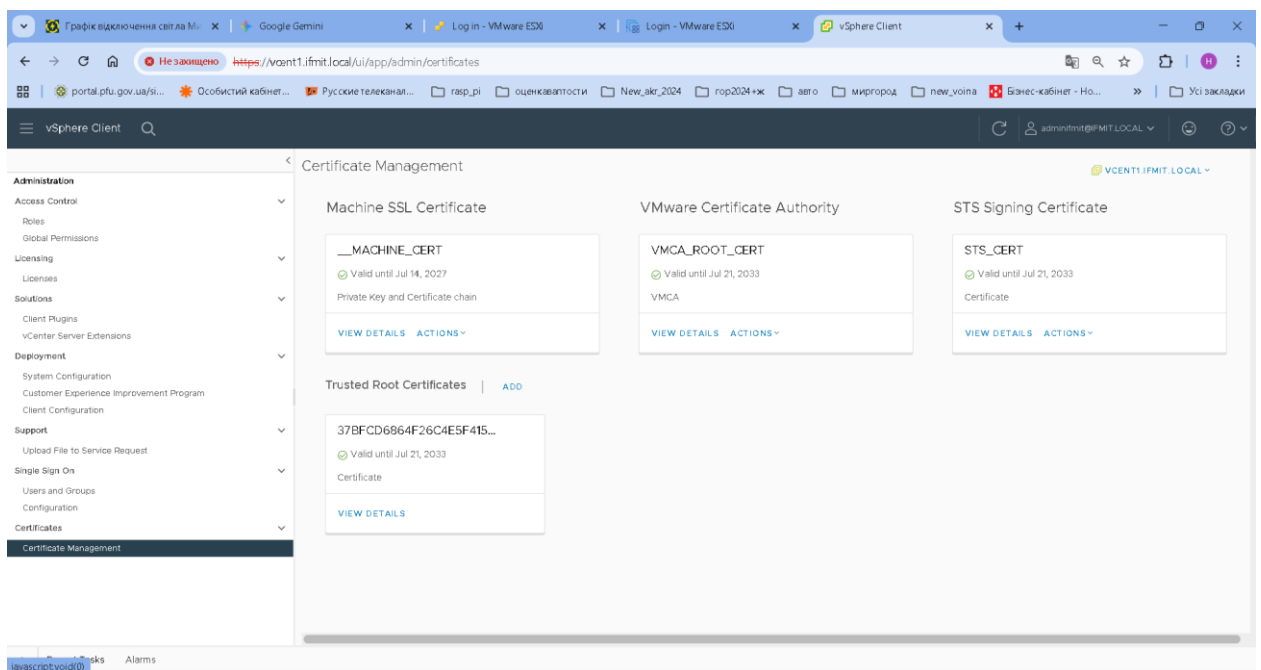


Рис. 3.16 Сертифікати

3.4 Архітектура безпеки, контроль доступу – основа налаштування віртуального середовища

З виходом платформи vSphere 7.0 корпорація VMware здійснила не просто оновлення функціоналу, а стратегічний перехід до концепції «Вбудованої безпеки» (Intrinsic Security). Ця парадигма передбачає фундаментальну відмову від використання накладених (агентських або периметральних) засобів захисту як основного бар'єру на користь механізмів, інтегрованих безпосередньо в ядро гіпервізора ESXi та керуючі компоненти інфраструктури vCenter.

У контексті vCenter Server спостерігається трансформація моделі довіри. Традиційний підхід, де внутрішня мережа управління вважалася «чистою зоною», більше не є релевантним через зростання векторів атак (lateral movement). Здійснюється міграція до моделі «Нульової довіри» (Zero Trust), яка постулює необхідність безперервної верифікації легітимності кожного компонента інфраструктури — від хостів віртуалізації та віртуальних машин до кінцевих користувачів та сервісних облікових записів.

Ключовими факторами цієї трансформації є:

- Демократизація криптографічного захисту: Впровадження механізму vSphere Native Key Provider (NKP), що усуває фінансові та архітектурні бар'єри для шифрування даних. Це перетворює шифрування з опції "для обраних" на гігієнічний стандарт.
- Апаратна верифікація цілісності: Перехід від програмної перевірки до апаратної атестації за допомогою технології Trusted Platform Module (TPM) 2.0. Це дозволяє гарантувати незмінність коду гіпервізора ще до завантаження операційної системи.

Проведемо аналіз архітектурних змін, дослідження взаємозв'язків між об'єктами та формалізовані рекомендації щодо конфігурації підсистем безпеки у промислових середовищах експлуатації.

Управління доступом та Рольова Модель (Identity & Access Management)

Підсистема розмежування доступу в vCenter 7 базується на ієрархічній моделі рольового управління (Role-Based Access Control — RBAC). Коректна конфігурація цього компонента є критичною умовою забезпечення цілісності та конфіденційності даних, оскільки 80% інцидентів безпеки у віртуальних середовищах пов'язані саме з помилками конфігурації прав доступу, а не з вразливостями програмного коду.

Структурний аналіз Рольової Моделі

Архітектура безпеки будується на суворому взаємозв'язку трьох фундаментальних сутностей: **Суб'єкт** — **Роль** — **Об'єкт**. Глибоке розуміння їх взаємодії необхідне для побудови захищеного контуру управління та уникнення ефекту «надлишкових привілеїв» (рис. 3.17).

Підсистема розмежування доступу vCenter 7: Модель RBAC



Рис.3.17 Структура Ролей vCenter

Суб'єкти доступу (Subjects)

Суб'єктами доступу виступають сутності, що ініціюють запит на виконання операції.

1. Користувачі та Групи:

- *Локальні суб'єкти:* Облікові записи в домені vsphere.local. Їх використання має бути зведене до мінімуму (переважно для аварійного доступу "break-glass", коли зовнішні служби недоступні).
- *Зовнішні суб'єкти:* Користувачі з AD/LDAP або федеративні провайдери (IDP).
- *Рекомендація:* Категорично рекомендується призначення привілеїв виключно на рівні **Груп**. Призначення прав індивідуальним користувачам робить аудит безпеки неможливим у масштабах підприємства та ускладнює процедуру відкликання прав при звільненні співробітника.

2. Сервісні акаунти:

- Окрему увагу слід приділити сервісним обліковим записам (для систем резервного копіювання, моніторингу, автоматизації). Для них не діє принцип MFA, тому паролі та політики та обмеження прав мають бути максимально жорсткими.

Класифікація Ролей (Roles). Роль у vSphere — це не просто набір прав, це визначення функціонального профілю.

• Системні ролі (System Roles):

- *Administrator:* Надає повний контроль, включаючи керування правами доступу. Використання цієї ролі для щоденних операцій є грубим порушенням безпеки.
- *Read-Only:* Забезпечує можливість моніторингу. Важливо розуміти, що ця роль дозволяє переглядати конфігурацію мережі та сховищ, що може бути використано зловмисником для розвідки (Reconnaissance).

- *No Access*: Блокуюча роль. Використовується для створення "сліпих зон". Наприклад, адміністратори продуктивного середовища не повинні навіть бачити об'єкти середовища розробки або секретного проєкту.
- **Шаблонні ролі (Sample Roles):**
 - Містять попередньо сконфігуровані набори прав (наприклад, Virtual Machine Power User).
 - *Ризик*: При оновленні vCenter ці ролі можуть бути перезаписані вендором до значень за замовчуванням. Тому їх використання в "чистому" вигляді заборонено в Production-середовищах. Завжди клонуйте шаблон у нову роль (наприклад, CORP_VM_PowerUser).
- **Користувацькі ролі (Custom Roles):**
 - Дозволяють реалізувати принцип найменших привілеїв (Least Privilege). Створюються шляхом вибору конкретних атомарних операцій (понад 500 доступних привілеїв).

Архітектура Дерев Інвентарю (Inventory Trees Model)

Це найбільш складний і часто неправильно зрозумілий аспект vSphere. Ключовою концептуальною помилкою є сприйняття vCenter як єдиного ієрархічного дерева. Фактично, vCenter керує чотирма паралельними вимірами (деревами) об'єктів, які перетинаються лише на кореневому рівні — об'єкті Datacenter (Дата-центр) (Рис.3.18).

1. Hosts and Clusters (Хости та Кластери): Відображає фізичні обчислювальні ресурси.
2. VMs and Templates (ВМ та Шаблони): Логічна організація робочих навантажень.
3. Storage (Сховища): Ієрархія систем зберігання (Datastores, Datastore Clusters).
4. Networking (Мережі): Ієрархія віртуальної комутації (DVS, Port Groups).

Архітектура Дерев Інвентуру vCenter

vCenter керує чотирма паралельними вимимими об'єктами

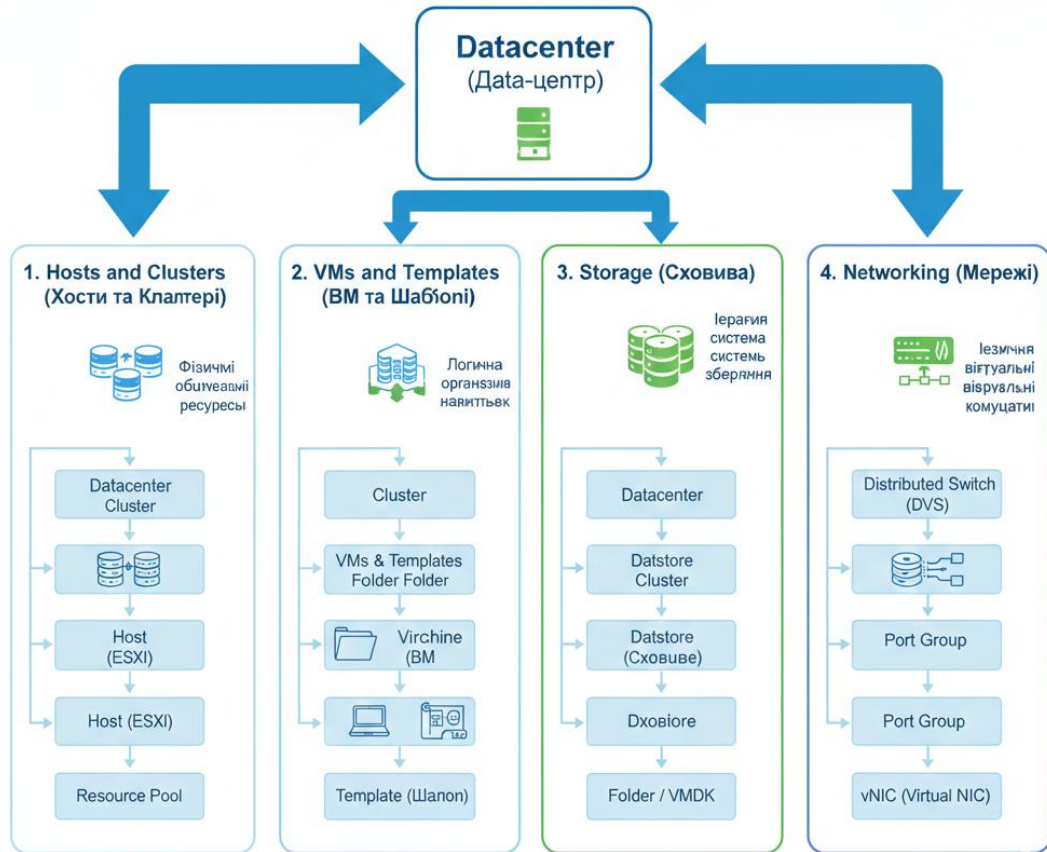


Рис.3.18 Древа інвентуру vCenter

Критичні наслідки для безпеки:

Призначення прав в одному дереві ніколи автоматично не поширюється на об'єкти в інших деревах, навіть якщо логічно вони пов'язані.

- *Приклад:* Якщо ви створите папку "Project X" у поданні *VMs and Templates* і надасте користувачеві права адміністратора на цю папку, він зможе керувати ВМ. Однак, він не побачить датасторів, на яких лежать диски цих ВМ, і мереж, до яких вони підключені, оскільки це об'єкти інших дерев.

Деталізована логіка призначення ролей за типами об'єктів

Розглянемо специфіку призначення прав, щоб уникнути ситуацій "фантомного доступу" або блокування легітимних операцій.

А. Об'єкти: Каталоги (Folders) — Контейнеризація доступу

Каталоги у vSphere є суворо типізованими. Ви не можете змішувати об'єкти різних типів в одній папці.

- Стратегія: Для ізоляції департаменту (Multi-tenancy) необхідно створити дзеркальну структуру папок у всіх чотирьох деревах: Папка ВМ "HR", Папка Мереж "HR", Папка Сховищ "HR".
- Помилка: Призначення ролі тільки на папку ВМ призведе до того, що адміністратор зможе вмикати ВМ, але не зможе створити нову ВМ, оскільки не матиме прав на вибір мережі (Network.Assign) та диску (Datastore.AllocateSpace).

Б. Об'єкти: Хости та Кластери (Hosts & Clusters) — Проблема міграції
Хост ESXi часто сприймається як контейнер для ВМ, але в динамічній інфраструктурі це хибне уявлення.

- Специфіка DRS: Віртуальні машини постійно мігрують між хостами завдяки технології DRS (Distributed Resource Scheduler).
- Ризик: Якщо ви призначите права користувачеві на конкретний хост ESXi-01, то після автоматичної міграції ВМ на хост ESXi-02 користувач миттєво втратить доступ до управління цією машиною.
- Рішення: Точкою призначення прав має бути Кластер або Пул Ресурсів. Це забезпечує безперервність доступу незалежно від фізичного розміщення навантаження.

В. Об'єкти: Мережі — Двостороннє рукошлякування

Призначення прав на мережу є найскладнішим аспектом через механізм перевірки прав з двох сторін.

- Механізм: При спробі підключити ВМ до порт-групи, vCenter перевіряє права в двох місцях:
 - а. На об'єкті ВМ: чи має користувач право змінювати налаштування (VirtualMachine.Config.EditDevice).
 - б. На об'єкті Мережа: чи має користувач право призначати цю мережу (Network.Assign).

- Типова помилка: Адміністратор надає повні права на VM, але забуває надати права на порт-групу. Результат: помилка "Permission to assign network denied".
- Рекомендація: Створюйте спеціальну роль Network Consumer (тільки право Assign) і призначайте її на папки з мережами для відповідних груп користувачів.

Г. Об'єкти: Сховища (Datastores) — Management Plane vs Data Plane

- Два рівні доступу:
 - a. Management Plane: Операції з самим LUN/NFS (форматування, розширення, перейменування). Вимагає адміністративних прав.
 - b. Data Plane: Використання дискового простору віртуальними машинами.
- Логіка провіжнінгу: Щоб створити віртуальний диск, користувачеві необхідний привілей Datastore.AllocateSpace. Без цього права створення снапшотів або нових VM буде неможливим, навіть за наявності повних прав на саму VM.
- Рекомендація: Використовуйте Кластери Сховищ (Datastore Clusters). Це дозволяє абстрагуватися від конкретних LUN і дозволити Storage DRS балансувати навантаження, не порушуючи модель доступу користувача.

Принцип релевантності та область дії (Relevance & Scope)

Важливим нюансом є те, що vCenter не виконує семантичну перевірку "здорового глузду" при призначенні прав.

- Проблема: Система дозволить призначити роль з правами керування мережевим комутатором (Distributed Switch) на об'єкт "Віртуальна машина".
- Результат: Це право буде "мертвим". Воно ніколи не спрацює, тому що об'єкт VM не має дочірніх об'єктів типу "Комутатор".

- Висновок: Створення універсальних "Супер-ролей" (які містять права на все) і призначення їх на нижні рівні ієрархії (на конкретну VM) є поганою практикою. Це захаращує базу даних прав і створює ілюзію доступу.
- Best Practice: Ролі мають бути контекстними (VM_Admin, Network_Admin, Storage_User) і призначатися на відповідні типи об'єктів.

Компонент vCenter Single Sign-On (SSO) перетворився на повноцінний Security Token Service (STS).

- Федеративна ідентифікація (Identity Federation): У версії vSphere 7 VMware зміщує фокус з прямої інтеграції AD на використання федерації (OIDC/OAuth2) через AD FS.
- Застарілі протоколи: Метод *Integrated Windows Authentication (IWA)*, який вимагав приєднання vCenter до домену AD, офіційно оголошено застарілим (deprecated). Він створює жорстку залежність від доступності контролерів домену та має відомі вразливості.

Управління криптографічними ключами (Key Management & Encryption)

Впровадження вдосконалених механізмів шифрування у vSphere 7.0 вирішує проблему фізичної безпеки даних (Data at Rest).

vSphere Native Key Provider (NKP) це революційна зміна в архітектурі. До виходу 7-ї версії шифрування вимагало наявності зовнішнього апаратного або програмного KMS (Key Management Server), що коштувало дорого і було складно в обслуговуванні.

- Архітектура NKP: vCenter Server сам стає генератором ключів. Він створює Key Derivation Key (KDK). Цей кореневий секрет реплікується на всі хости ESXi в кластері в захищеному вигляді. Хости використовують його для генерації ключів шифрування даних (DEK) для кожної VM.

- **Відмовостійкість:** Навіть якщо vCenter Server вийде з ладу, хости ESXi зможуть продовжувати роботу зашифрованих VM та перезавантажувати їх, оскільки KDK закешований у TPM модуль хоста або в захищену пам'ять. Однак, без vCenter неможливо буде створити нові зашифровані VM.

Шифрування віртуальних машин (VM Encryption)

- **Технологія VAIO (vSphere APIs for I/O Filtering):** Шифрування відбувається на льоту перед записом на диск. Це означає, що система зберігання даних (Storage Array) "бачить" лише зашифрований потік даних. Як Наслідок - функції дедуплікації та компресії на стороні Сховища (Storage) стають неефективними, оскільки зашифровані дані мають високу ентропію і не стискаються. Це слід враховувати при плануванні ємності (Capacity Planning).
- **Політики зберігання (SPBM):** Активація шифрування здійснюється через профілі. Це дозволяє зашифрувати працюючу VM без простою (Live Encryption), просто змінивши її політику.

vSphere Trust Authority (vTA) та автоматизація

vTA — це наступний крок після Secure Boot. Це механізм, який гарантує, що ваші секретні дані обробляються лише на "чистому" обладнанні.

- **Архітектура ізоляції:** Створюється жорсткий поділ на два класи обладнання:
 - a. **Trust Authority Cluster (Керуючий):** "Елітна" група хостів, які зберігають ключі шифрування.
 - b. **Trusted Cluster (Робочий):** Хости, які виконують навантаження.
- **Процес Атестації:** При завантаженні робочий хост створює криптографічний зліпок свого стану (хеші BIOS, завантажувача, ядра, драйверів) за допомогою TPM модуля. Цей звіт надсилається в Керуючий кластер.

- a. Якщо звіт збігається з еталоном ("Золотим образом"), хост отримує ключі шифрування.
- b. Якщо виявлено найменшу розбіжність (наприклад, інсталювано непідписаний драйвер або руткіт), хост вважається скомпрометованим. vTA **відмовляє** у видачі ключів. Зашифровані ВМ на цьому хості не запускатимуться, що унеможливило витік даних.

Безпека в масштабі неможлива без автоматизації. Ручні налаштування схильні до людських помилок (Configuration Drift).

- Модуль PowerCLI VMware.VimAutomation.Security:
 - a. Надає командлети для повного управління життєвим циклом НКР.
 - b. Дозволяє проводити аудит відповідності: наприклад, скрипт може щодня перевіряти, чи всі ВМ у папці "Finance" мають політику шифрування, і автоматично виправляти відхилення.
 - c. *Масові операції*: Set-VMEncryptionKey дозволяє виконати Deep Rekey (зміну ключа даних) для тисяч ВМ однією командою, що вручну зробити неможливо.

Таким чином, платформа vCenter Server 7.0 надає безпрецедентний за потужністю інструментарій забезпечення інформаційної безпеки, який раніше був доступний лише у спеціалізованих захищених середовищах. Демократизація технологій шифрування через Native Key Provider знижує поріг впровадження засобів захисту даних, а вдосконалена рольова модель дозволяє будувати гранулярні політики доступу.

Проте, технологія сама по собі не гарантує безпеки. Ефективність впровадження цих інструментів знаходиться в прямій залежності від якості організаційних заходів: коректного проєктування архітектури дерев

інвентарю, розуміння моделі загроз та суворої дисципліни управління криптографічними ключами. Перехід на vSphere 7.0 вимагає від команди експлуатації не лише технічних навичок, але й зміни мислення в бік концепції Zero Trust.

3.5 Опис створення віртуального навчального середовища

Результати аналізу підсистем безпеки VMware vSphere 7.0, проведеного у попередньому розділі, формують фундамент для практичної побудови захищеного контуру віртуальної лабораторії. Встановлено, що хоча впровадження **Native Key Provider (NKP)** і спрощує захист даних у стані спокою, виключаючи залежність від високовартісних зовнішніх KMS, головним архітектурним викликом залишається організація логічного доступу.

Ключова проблема, що потребує вирішення у цьому розділі, полягає у особливості рольової моделі vCenter Server. На відміну від класичних плоских систем, vSphere оперує чотирма ізольованими ієрархіями об'єктів (хости, віртуальні машини, сховища та мережі). Права, призначені в одній ієрархії, не успадковуються в інших, що створює ризики конфігураційних розривів. Особливої уваги потребує механізм призначення мережевих інтерфейсів, який вимагає перехресних прав у різних деревах інвентарю, а також специфіка роботи DRS, що унеможлиблює прив'язку прав до конкретних фізичних хостів.

Головні ідея створення навчального середовища

Грунтуючись на виявлених ризиках та принципі **Zero Trust**, далі буде розроблено деталізовану систему доступу. Основний акцент буде зроблено на відмові від стандартних ролей на користь користувацьких (Custom Roles), що дозволить нівелювати конфлікти між «деревами» інвентарю та забезпечити

безпечну роботу сервісних груп в умовах динамічної міграції віртуальних машин.

Таким, чином, **головна ідея, створення навчального віртуального середовища** полягає у виборі, розробці та призначенні певних нестандартних ролей на певні об'єкти програмного компоненту vCenter.

Пропонується віртуальну лабораторію розташувати у вбудованих, додаткових об'єктах (рис.3.19):

- – **Каталог Віртуальних машин та шаблонів**
- – **Каталог мереж та свічів**
- – **Додаткові налаштування для хостів та сховищ.**



Рис.3.19 Структура віртуального середовища

Каталог (каталоги) віртуальних машин та шаблонів призначено створення студентами (здобувачами освіти) тренувальних віртуальних машин по параметрам, що контролює викладач

Каталог мереж та свічів призначення для розташування викладачем певних віртуальних свічів (мереж), що використовуються здобувачами освіти

для створення окремого мережевого середовища. В залежності від завдання є можливість надати слухачам освіти можливість створення певних мереж (груп портів). Однак накопичений досвід свідчить, що достатньо створити ці мережі та надати слухачам **доступ тільки на читання**. Фактично це означає, що слухачі освіти мають можливість використати певні ізольовані мережі, і таким чином, отримати при виконанні лабораторних робіт свою, **особисту мережу**, яка не конфліктує з іншими мережами у всій інформаційній системі.

Загальна послідовність дій створення віртуального навчального середовища

Для виконання умов, необхідних для створення навчального середовища необхідно виконати наступні кроки (рис. 3.20):

- 1 Приєднати компонент vCenter до Microsoft AD
2. Створити додаткові групи у Microsoft AD на сервері, контролері AD.
- 3 Створити додаткові каталоги віртуальних машин для розташування віртуальних машин слухачів.
- 4 Створити додаткові каталоги для віртуальних мереж для використання віртуального середовища
- 5 Розташувати початкові віртуальні машини для студентів у каталозі .
- 6 Розробити Ролі для налаштування обмежень процесів створення віртуальних машин, використання або створення мереж, використання хостів або кластеру, використання певних сховищ (дисків).
- 7 Призначити певні Ролі для певних груп Ms AD на каталоги для збереження віртуальних машин.
- 8 Призначити певні Ролі для певних груп Ms AD на каталоги для віртуальних мереж та створити ці віртуальні мережі.
- 9 Призначити певні Ролі для певних груп Ms AD на необхідні сховища.
- 10 Призначити певні Ролі для певних груп Ms AD на хости або кластер.



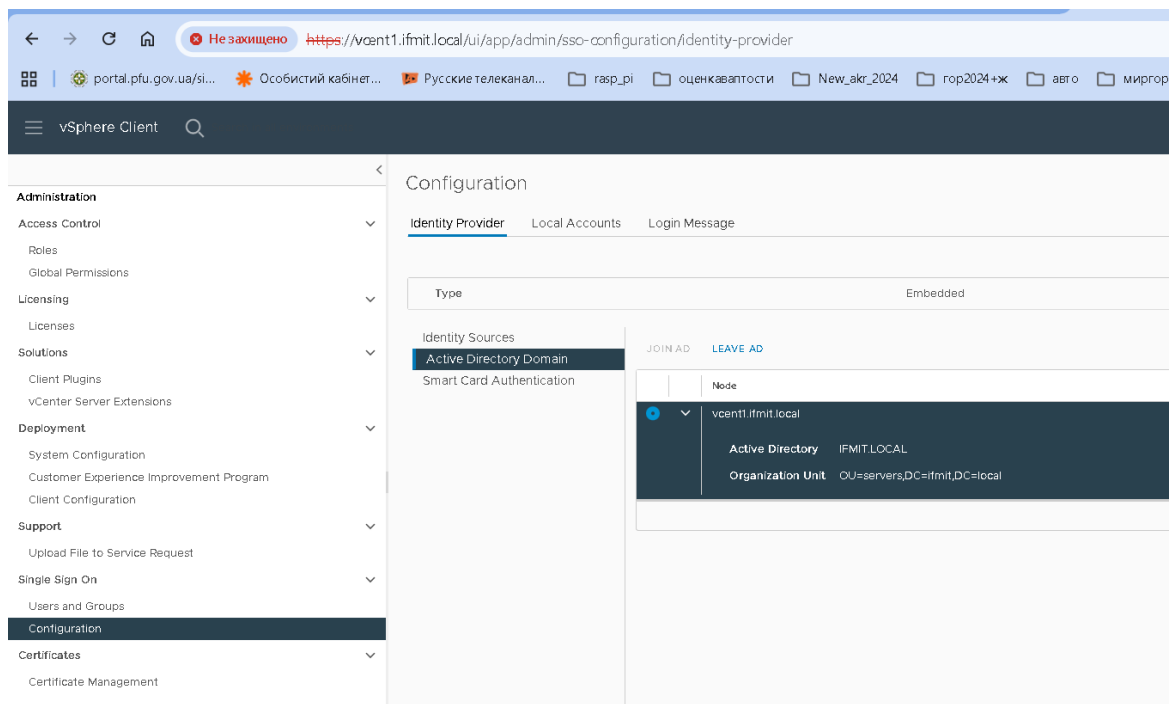
Рис.3.20 Послідовність створення навчального середовища

Опис процесу створення віртуального середовища

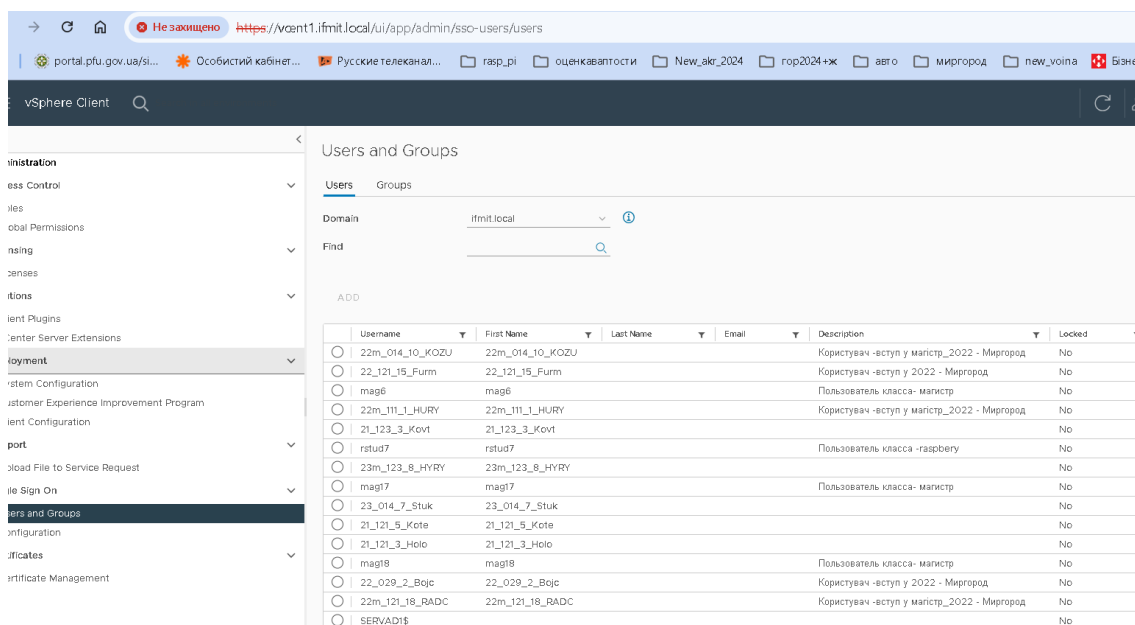
1 Приєднання до Microsoft AD. Потрібно знати пароль адміністратора Microsoft AD (рис. 3.21а б). У компоненті vCenter обираємо Системне меню Administration -> Configuration -> Active Directory Domain. Після такої дії vCenter буде «бачити» користувачів та групи з Active Directory Domain.

2. Створення додаткових групи у Microsoft AD на сервері, контролері AD.

Зайти на сервер Microsoft. Запустити додаток «Диспетчер Серверів». У цьому додатку обрати «засоби» -> «Користувачі та комп'ютери» (рис.3.22 та 3.23). На цьому етапі треба спланувати пати та кількість доступів.



a)



б

Рис. 3.21 Приєднання до AD

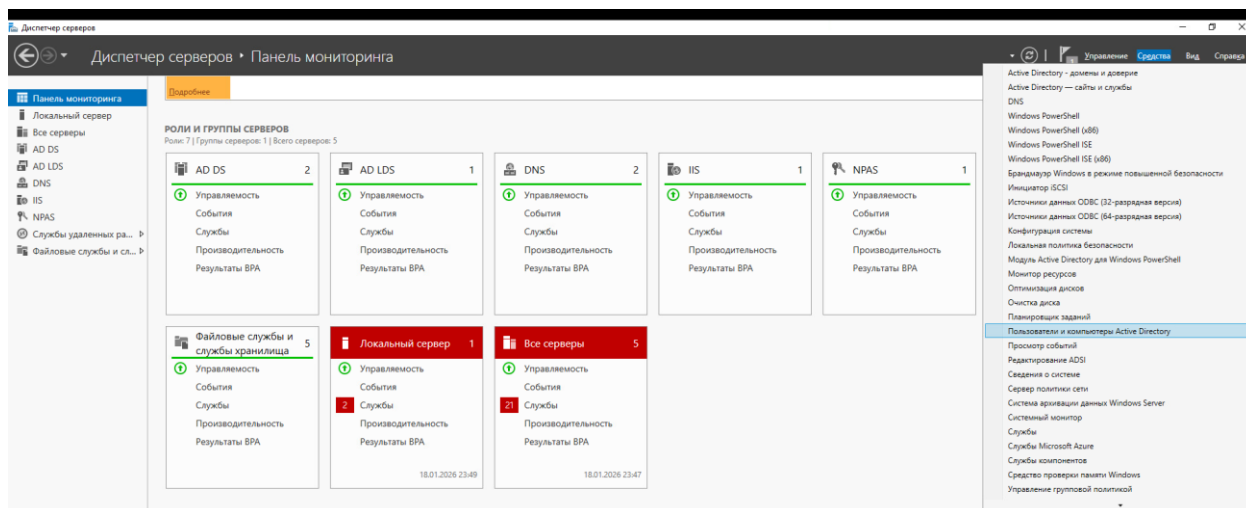


Рис. 3.22 Диспетчер серверів

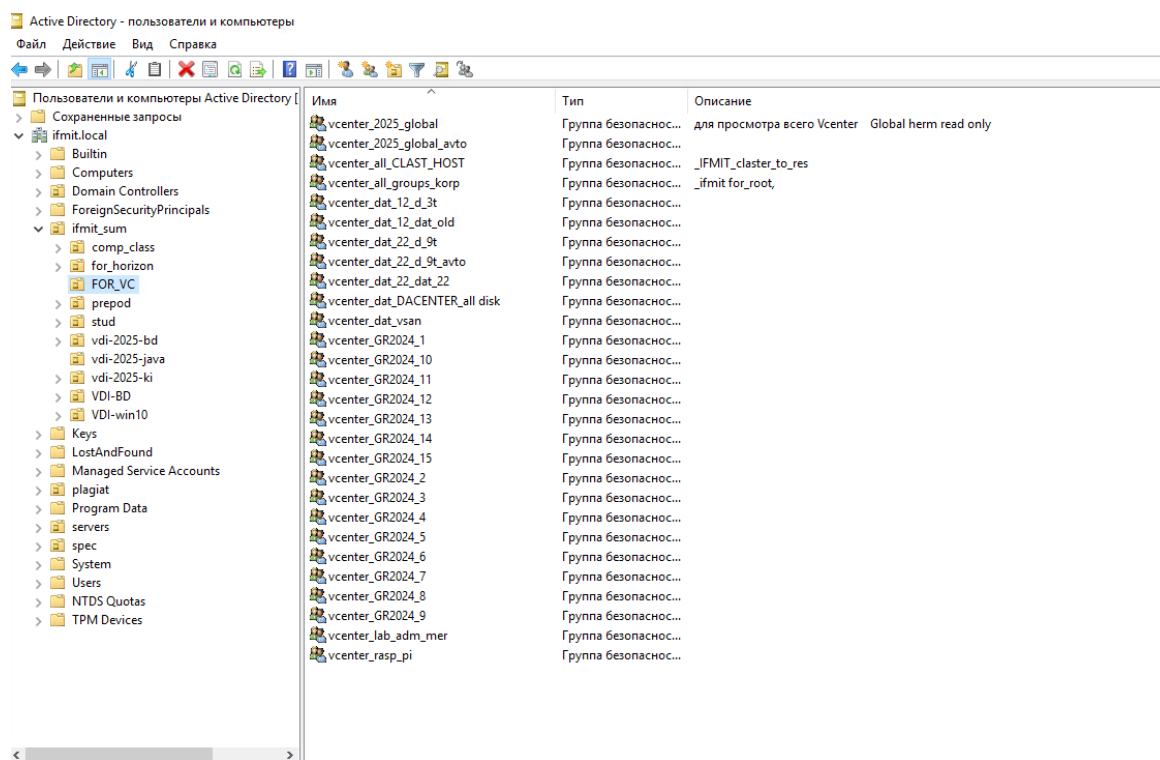


Рис. 3.23 Группы Ms AD для навчального середовища

Усі інші процеси створення віртуального середовища виконуємо у компоненті **vCenter** у різноманітних структурах. Для переходу з однієї структури до іншої використовуємо системне меню, підменю Shortcuts (рис. 3.24)

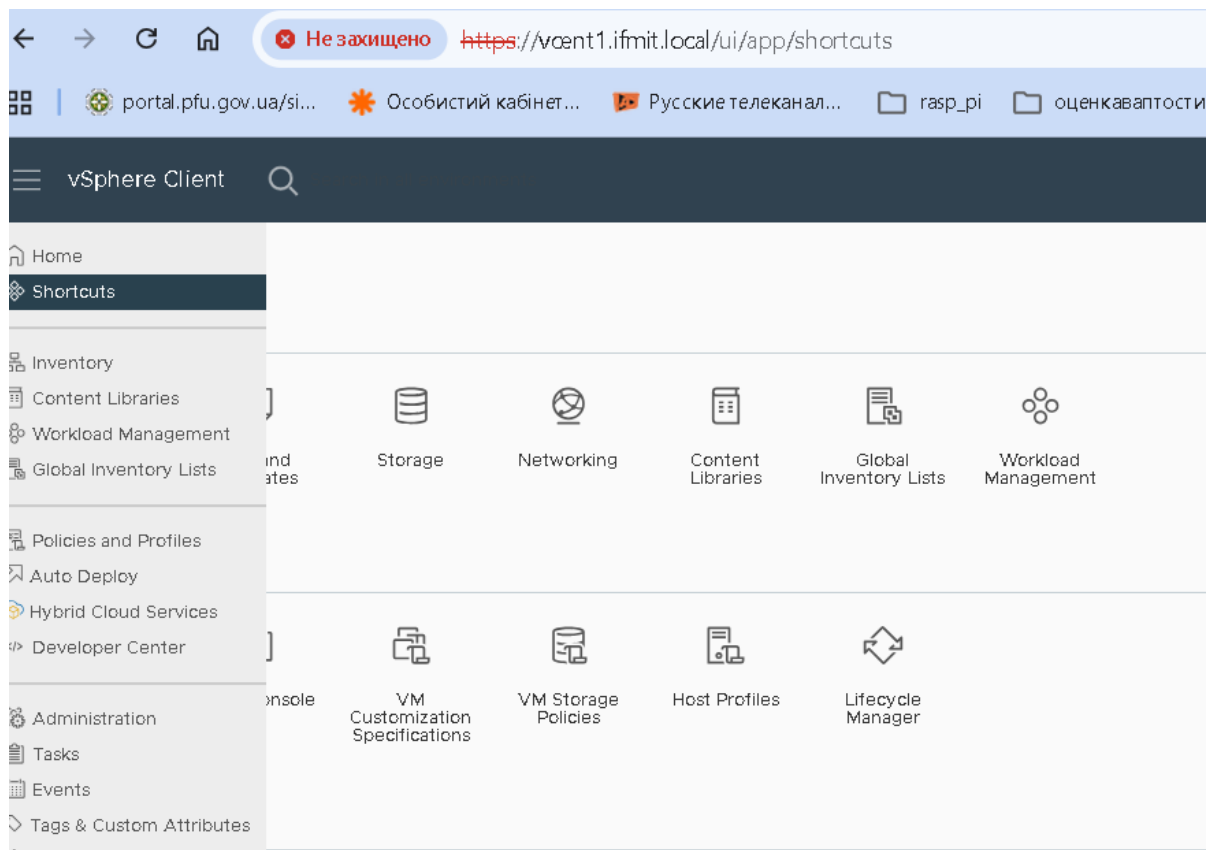


рис.3.24 Перехід по структурам: системне меню, підменю Shortcuts

3 Створення додаткових каталогів віртуальних машин для розташування віртуальних (тренувальних) машин слухачів. Спочатку переходимо системне меню, підменю Shortcuts розділ Virtuals.... Створення віртуального середовища робимо у головному каталозі За допомогою команд: Action -> Create new folder. В межах експериментального розгортання було створено кореневий каталог віртуального середовища (lab_corp_mer) та підкаталоги для певних груп користувачів (GR2024_??) де вони мають право створювати свої віртуальні машини (рис. 3.25).

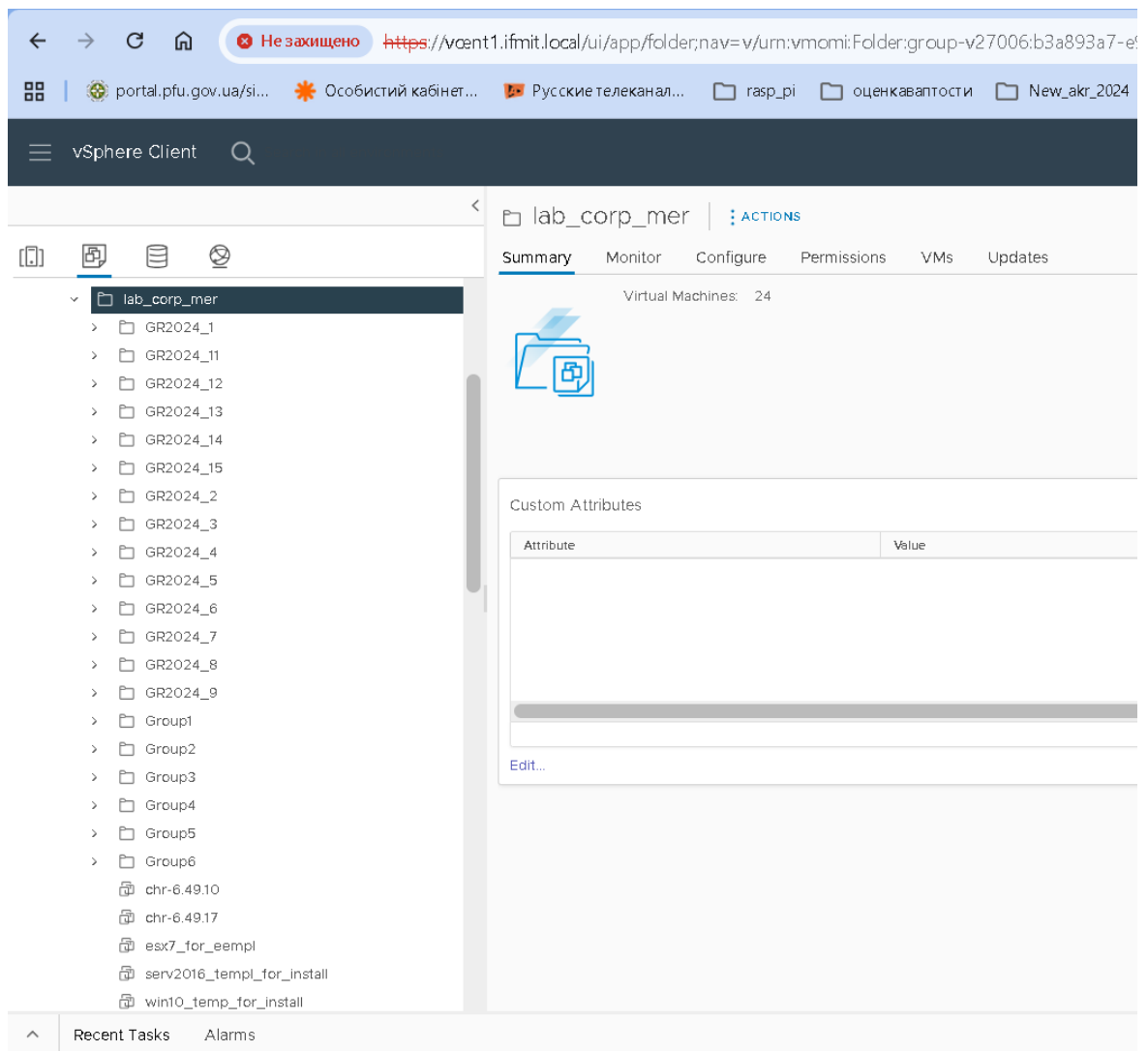


Рис. 3.25 Структура віртуального середовища для збереження тренувальних машин слухачів,

4 Створення додаткових каталогів для віртуальних мереж для використання віртуального середовища. Спочатку переходимо системне меню, підменю Shortcuts розділ Networking. За допомогою команд: Action -> Create new folder. В межах експериментального розгортання було створено кореневий каталог віртуального середовища (net_folder_for_lab) та підкаталоги для певних груп користувачів (GR2024_??) де вони мають право створювати свої віртуальні машини (рис. 3.26)

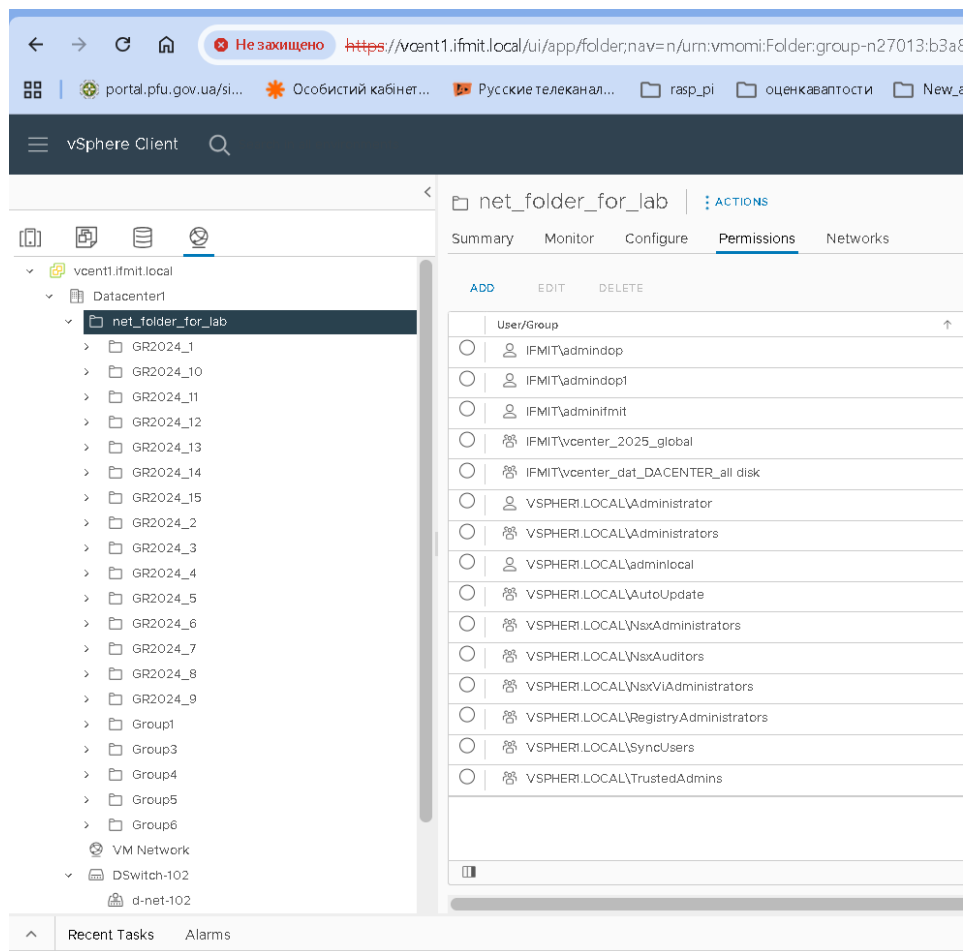


Рис. 3.26 Структура віртуальне середовища для збереження тренувальних машин слухачів,

5 Розташувати початкові віртуальні машини для студентів у каталозі. У даному випадку всі початкові віртуальні машини – машини які студенти беруть за основу для подальшого використання розташовуємо у корневому каталозі віртуального середовища – lab_corp_mer (Дивись нижню частину рис.3.25).

6 Розробка Ролей для налаштування обмежень процесів створення віртуальних машин, використання або створення мереж, використання хостів або кластеру, використання певних сховищ (дисків).

Створення певних ролей робиться у системному меню, підменю Administration (рис. 3.27)

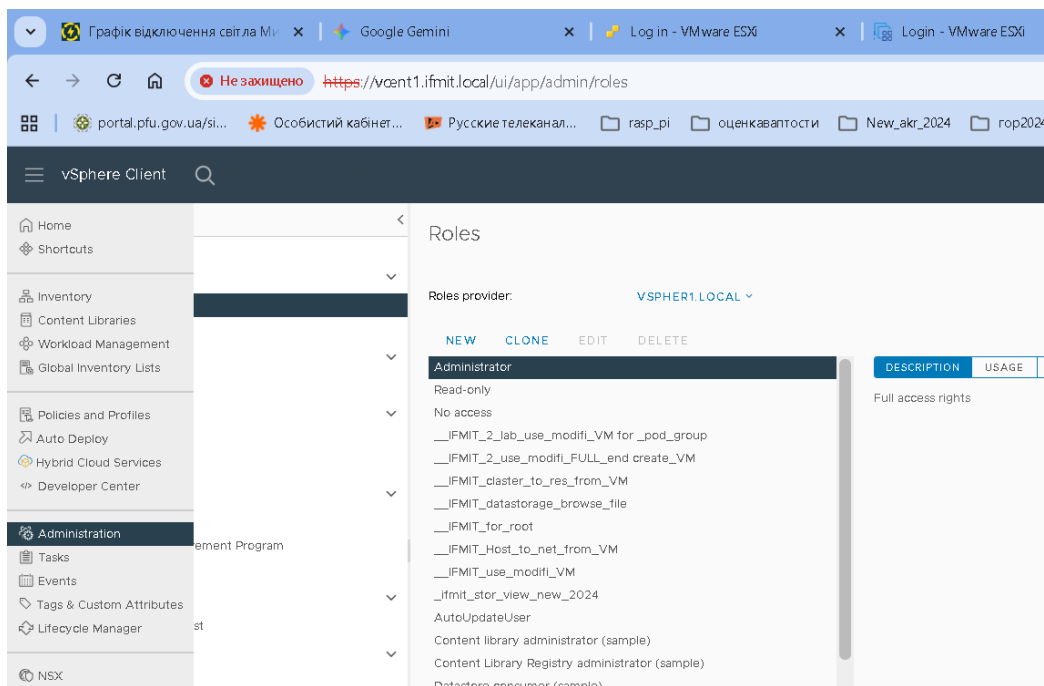


Рис. 3.27 Меню Administration

Після цього обираємо меню Roles та додаємо певну Роль (рис.3.28)

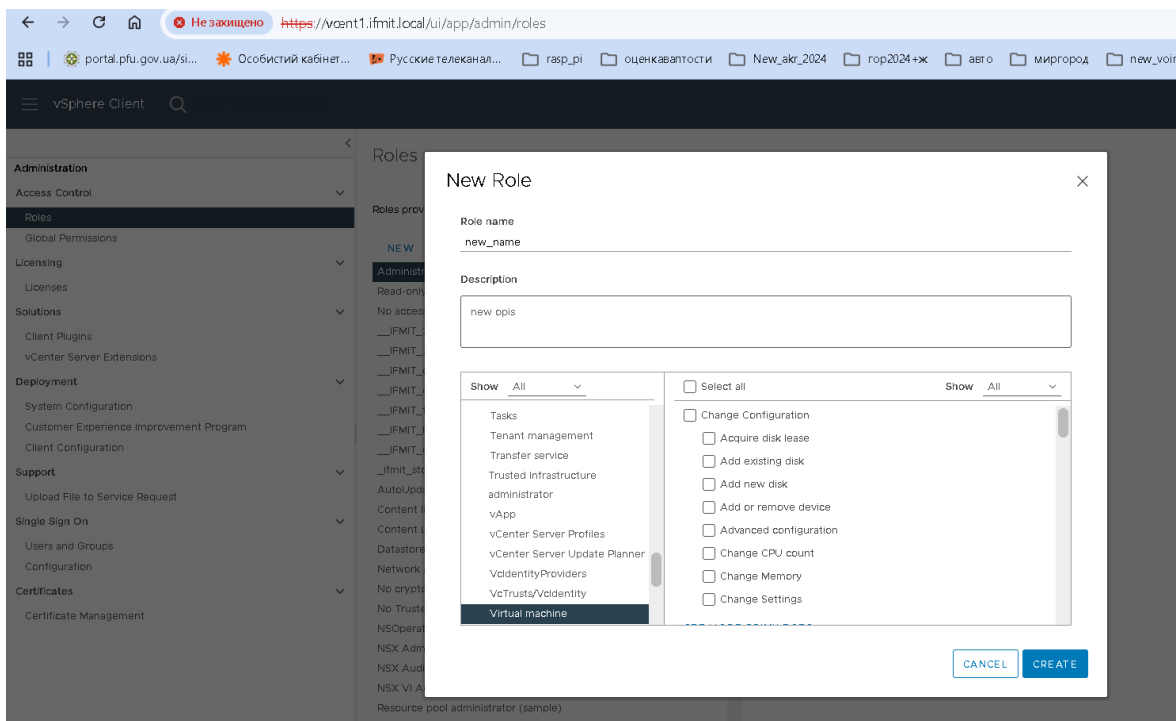


Рис. 3.28 Додавання Ролей.

Це самий головний процес налаштування. Він потребує особливої уваги. Слід враховувати ідеологію vCenter, враховувати різні типи Дерев (див. рис.3.18) та призначати певні ролі. В деяких випадках налаштування обмежень може не мати ні якого сенсу для певних об'єктів. В цілому було створено 5 ролей.

Роль на кореневий каталог віртуальних машин (**lab_for_corp_mer**) віртуального середовища з обмеженнями – ТІЛЬКИ ЧИТАННЯ та можливість КЛОНУВАТИ створені викладачем початкові віртуальні машини (крок 5). Можливість створення віртуальних машин на цьому рівні ЗАБОРОНЕНО

На підкаталоги для студентів (**GR2024_??**) надана можливість створення віртуальних машин ТІЛЬКИ МЕТОДОМ КЛОНУВАННЯ. Створення віртуальних машин іншими засобами – ЗАБОРОНЕНО. Крім того ЗАБОРОНЕНО змінювати параметри віртуальних машин (обсяг диску, процесор, ОЗУ та інші).

Окрему роль створюємо для використання певного сховища (диску) надаємо можливість ЧИТАННЯ каталогів та файлів цього диску.

Окрему роль створюємо для використання ресурсів хоста. Надаємо можливість ЧИТАННЯ ресурсів

Окрему роль створюємо для читання мереж.

Перелік Ролей показано на рисунку 3.29-3.31. Всі вони починаються з назви «**_____IFMIT**»

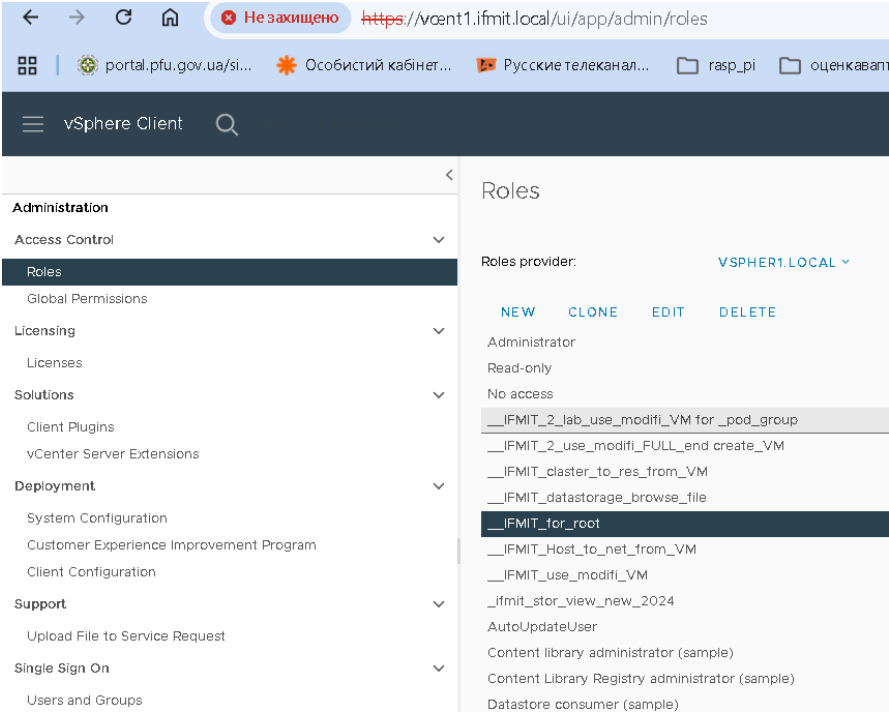


Рис. 3.29. Перелік Ролей віртуального середовища

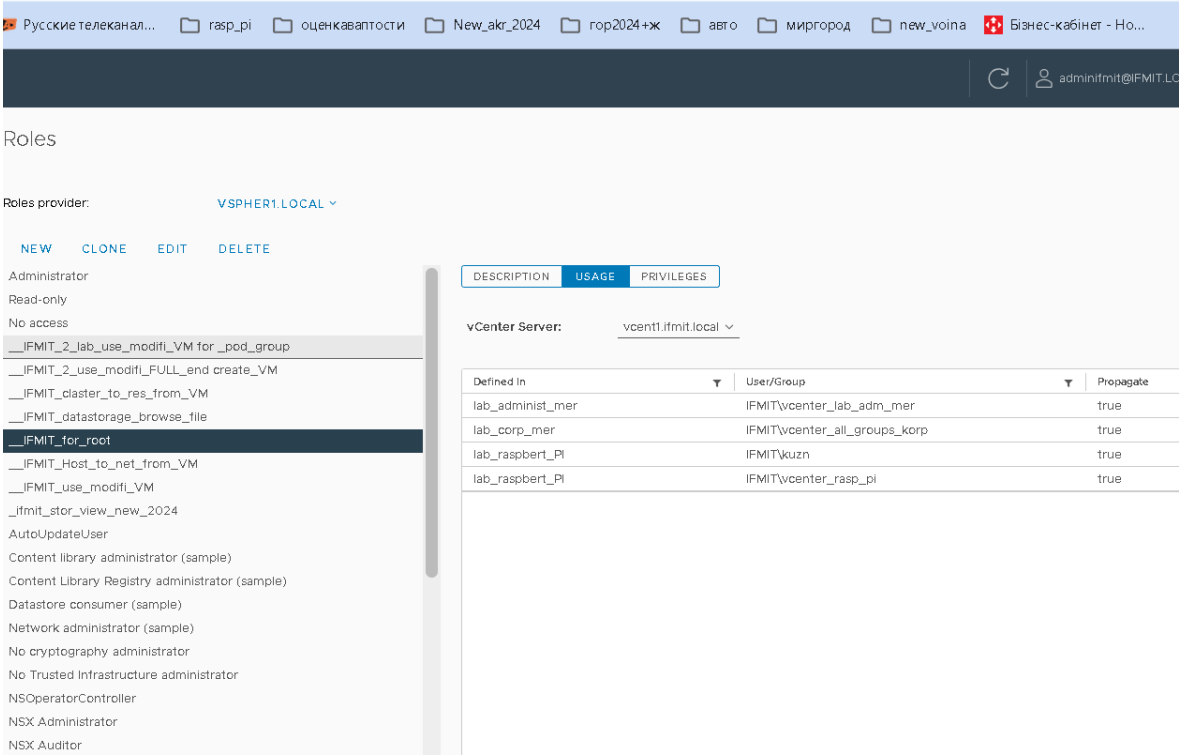


Рис. 3.30. Перелік кому призначена Роль

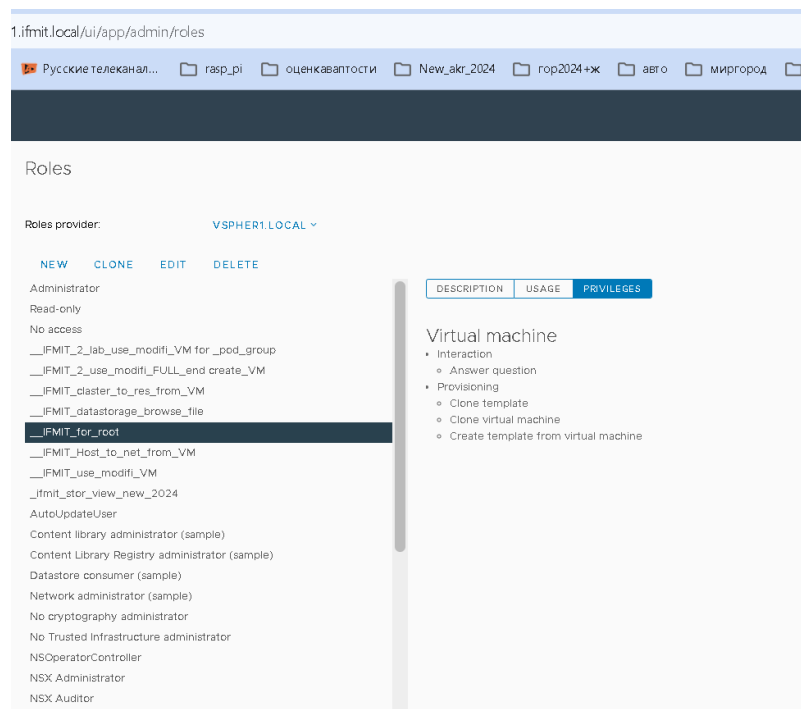


Рис. 3.31 . Перелік властивостей Ролі

7-10 Призначення певних Ролей для певних груп Ms AD на каталоги для збереження віртуальних машин. Для цього переходимо на певний каталог віртуального середовища (або диск, мережу, хост). Обираємо вкладку Permission та команду ADD. Та обираємо певну групу користувачів AD та певну передньо створену Роль (рис. 3.32)

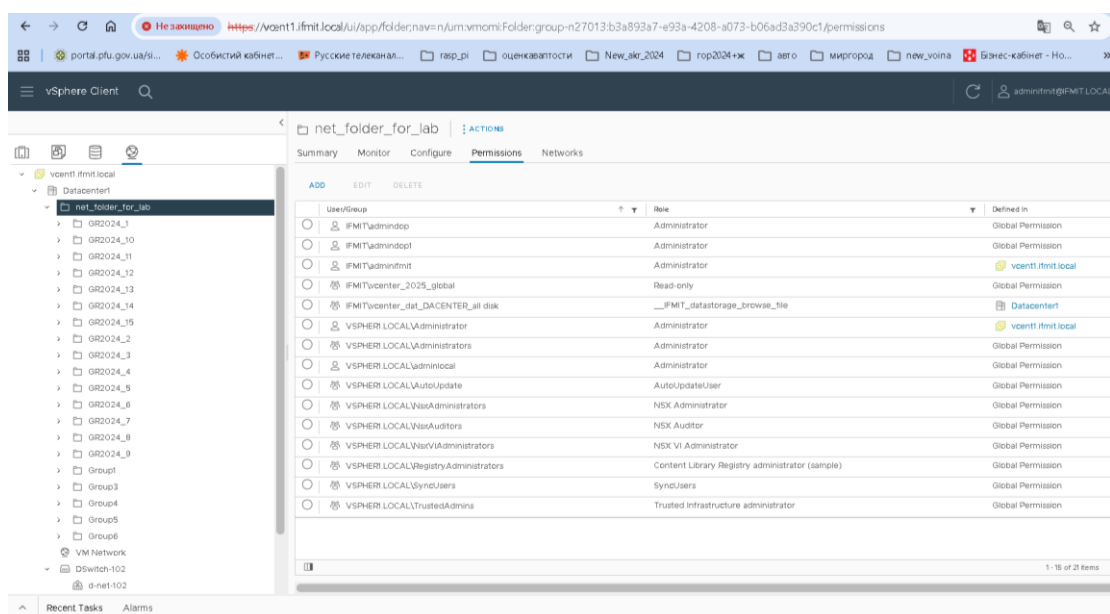


Рис.3.32 Призначення Ролі

На рис. 3.33-3.34 показано результат налаштувань віртуального середовища за рахунок призначення Ролей

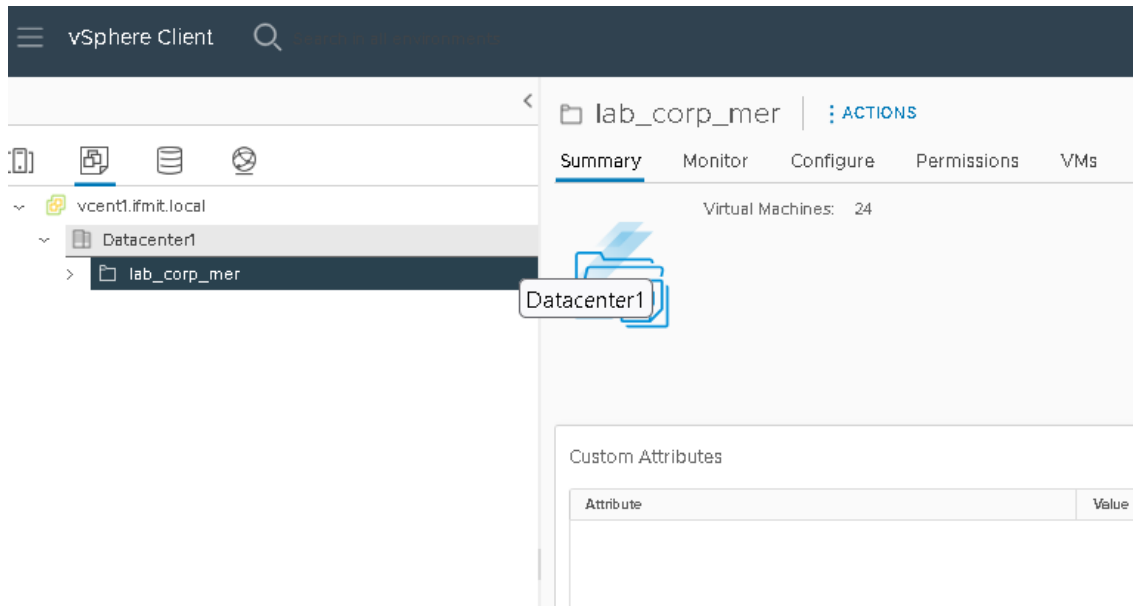


Рис. 3.33 Обмеження на перегляд інших об'єктів поза межами навчального середовища

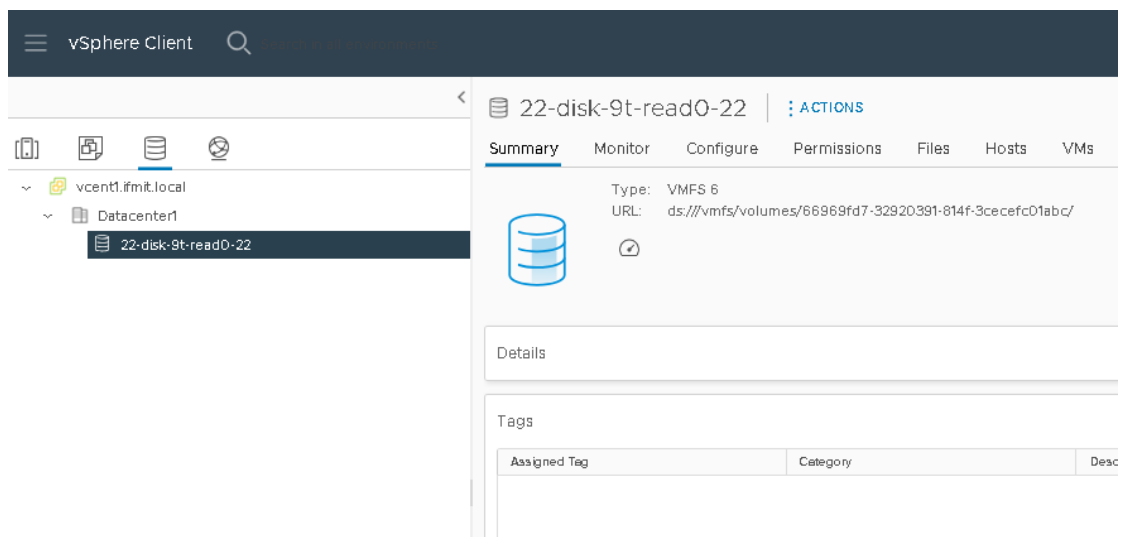


Рис. 3.34 Обмеження на перегляд накопичувачів (дисків)

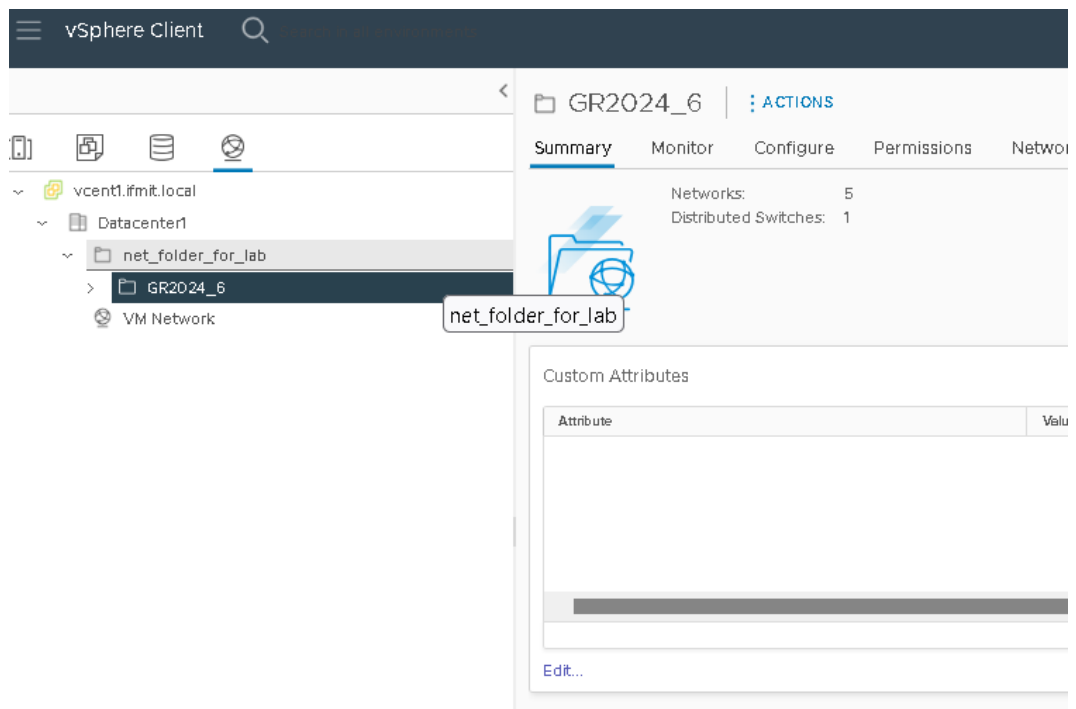


Рис. 3 35 Обмеження на використання мереж

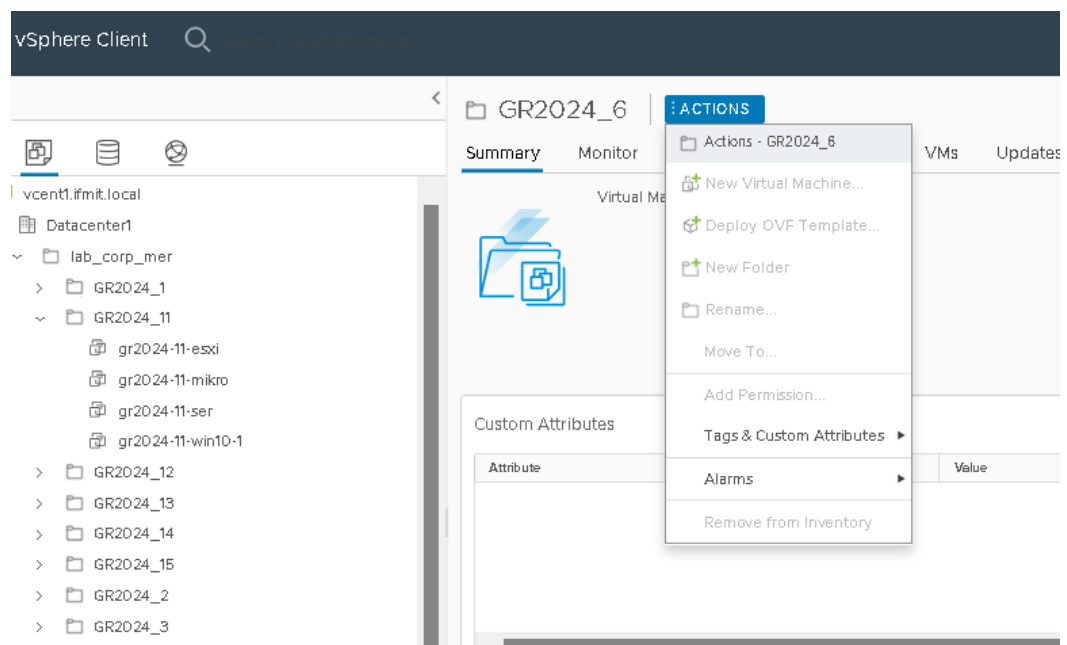


Рис 3. 36 Обмеження на можливість створення віртуальної машини

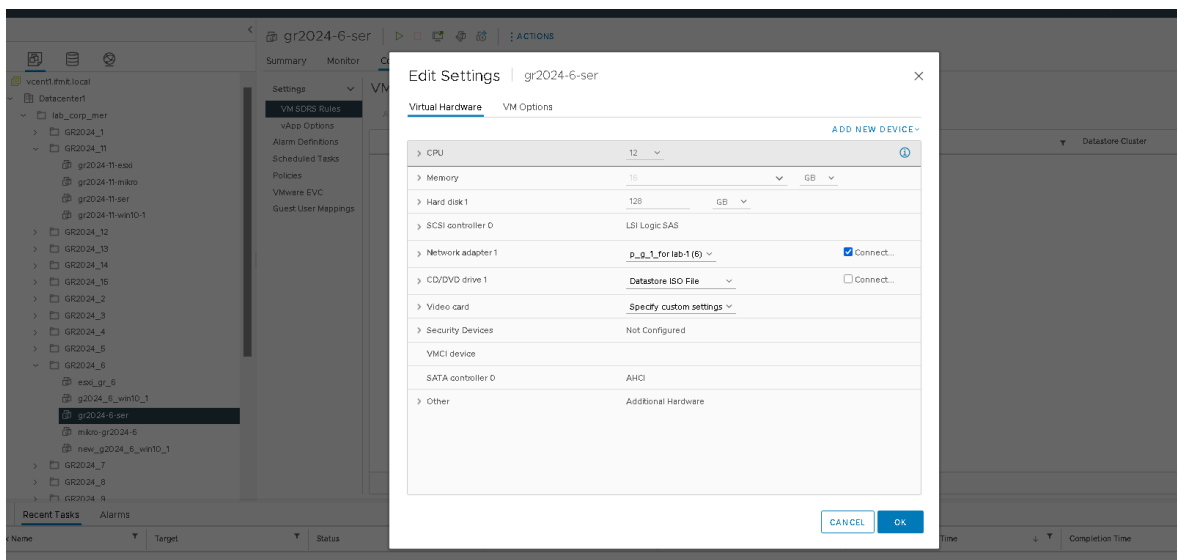


Рис. 3. 37 Обмеження на можливість змінити властивості віртуальної машини

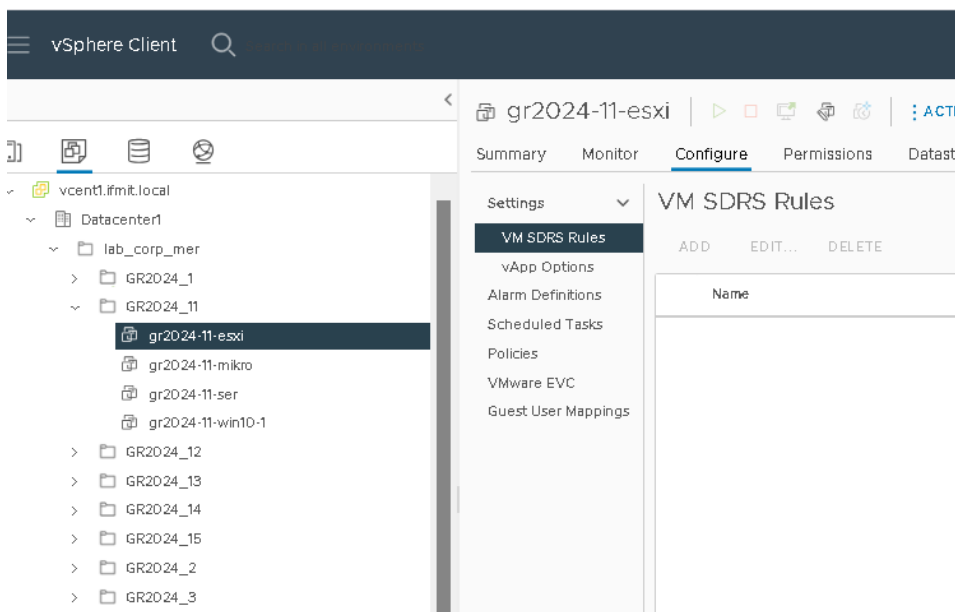


Рис. 3. 38 Обмеження на можливість запускати віртуальні машини інших студентів

Висновки до розділу

Підсумовуючи результати третього розділу, слід зазначити, що наведено ґрунтовний опис процесу розгортання віртуальної інфраструктури на базі VMware vSphere. Ключовою особливістю розгорнутого середовища є його адаптація під багатокористувацьку модель навчання, де гіпервізор ESXi та

система vCenter Server виступають не лише технічним фундаментом, а й керованим дидактичним простором. Це досягається шляхом глибокої ієрархічної структуризації інвентарю, де використання спеціалізованих папок (Folders) дозволяє логічно ізолювати ресурси окремих навчальних груп та індивідуальних проєктів у межах єдиного апаратного комплексу.

Створення навчального середовища ґрунтується на конфігурації моделі управління доступом (RBAC), яка враховує специфіку навчальних сценаріїв. На відміну від стандартних корпоративних налаштувань, тут основний акцент зміщено на створення «пісочниць-каталогів» для студентів, що забезпечується шляхом жорсткого обмеження прав на рівні віртуальних машин, мереж інтерфейсів та сховищ даних. Така детермінація прав доступу гарантує неможливість деструктивного впливу на загальну інфраструктуру або результати роботи інших учасників навчального процесу, зберігаючи при цьому достатній рівень автономії для виконання складних лабораторних завдань.

Таким чином, сформована віртуальна лабораторія є високотехнологічним освітнім інструментом, який поєднує в собі промислову надійність із гнучкістю, необхідною для засвоєння професійних компетенцій у сфері системного адміністрування та хмарних технологій.

ЗАГАЛЬНІ ВИСНОВКИ

Дійсно сучасна ІТ-інфраструктура базується на технологіях віртуалізації, підготовка кваліфікованих фахівців потребує наявності потужного та гнучкого інструментарію для відпрацювання практичних навичок

На основі проведеного дослідження, викладеного у кваліфікаційній роботі, сформовано такі загальні висновки, що підсумовують результати проектування та розгортання навчального середовища у VMware vCenter:

1. Проаналізовано сучасний стан технологій віртуалізації, що дозволило визначити платформу VMware vSphere як провідний промисловий стандарт, який забезпечує необхідну надійність та масштабованість для корпоративних та навчальних центрів обробки даних. Встановлено, що попри суттєві зміни у стратегії ліцензування після поглинання компанії корпорацією Broadcom (перехід на модель передплати та консолідація продуктів у пакети VVF та VCF), VMware залишається найбільш функціональним рішенням для підготовки фахівців з комп'ютерної інженерії.

2. Досліджено архітектурні особливості компонентів vSphere, зокрема гіпервізора ESXi та сервера керування vCenter. Аналіз еволюції ESXi показав перехід до суворіших апаратних вимог (відмова від драйверів vmklinux, обов'язковість TPM 2.0 та швидкісних носіїв ОС), а трансформація vCenter Server у віртуальний модуль VCSA на базі Photon OS дозволила спростити топологію управління завдяки вбудованому Platform Services Controller (PSC).

3. Розроблено та обґрунтовано архітектуру навчального віртуалізованого середовища, інтегрованого з корпоративною службою каталогів Microsoft Active Directory. Це дозволило реалізувати централізовану аутентифікацію та забезпечити прозоре управління доступом для різних

категорій користувачів (викладачів та студентів) через використання доменних груп.

4. Спроектовано та впроваджено модель контролю доступу (RBAC), адаптовану під специфіку навчального процесу. Шляхом створення користувацьких ролей та ієрархічної структури папок (Folders) у чотирьох деревах інвентарю vCenter було сформовано ізольовані зони для студентів. Це гарантує можливість виконання складних лабораторних завдань, включаючи клонування віртуальних машин та налаштування мереж, без ризику пошкодження основної інфраструктури закладу вищої освіти.

5. Запропонований підхід до організації лабораторних практикумів дозволяє ефективно розподіляти обчислювальні потужності між користувачами, забезпечуючи високу якість практичної підготовки фахівців в умовах дистанційного та змішаного навчання.

Таким чином, мету роботи — підвищення ефективності практичної підготовки фахівців шляхом створення захищеного віртуалізованого середовища — повністю досягнуто.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. VMware vSphere Product Line. [Електронний ресурс] URL: <https://www.google.com/search?q=https://www.vmware.com/products/vsphere> (дата звернення: 12.11.2025).
2. Proxmox VE Administration Guide. [Електронний ресурс] URL: https://pve.proxmox.com/wiki/Main_Page (дата звернення: 12.11.2025).
3. XCP-ng Documentation. [Електронний ресурс] URL: <https://xcp-ng.org/docs/> (дата звернення: 12.11.2025).
4. Azure Stack HCI Solution Overview. [Електронний ресурс] URL: <https://learn.microsoft.com/en-us/azure-stack/hci/overview> (дата звернення: 12.11.2025).
5. Citrix Tech Zone - HDX Graphics. [Електронний ресурс] URL: <https://www.google.com/search?q=https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/graphics/hdx-graphics.html> (дата звернення: 12.11.2025).
6. The definitive guide to the Xen Hypervisor architecture. [Електронний ресурс] URL: https://wiki.xenproject.org/wiki/Xen_Project_Software_Overview (дата звернення: 12.11.2025).
7. Kernel Based Virtual Machine (KVM) main page. [Електронний ресурс] URL: https://www.linux-kvm.org/page/Main_Page (дата звернення: 12.11.2025).
8. CNCF Kubernetes Landscape. [Електронний ресурс] URL: <https://www.cncf.io/> (дата звернення: 12.11.2025).
9. Broadcom Completes Acquisition of VMware; Briefs on New Strategy and Portfolio Simplification. [Електронний ресурс] URL:

- <https://www.google.com/search?q=https://www.broadcom.com/company/news/financial/broadcom-completes-acquisition-vmware> (дата звернення: 12.11.2025).
10. End of Availability of Perpetual Licensing and SaaS Subscriptions for VMware Products. [Електронний ресурс] URL: <https://kb.vmware.com/s/article/96065> (дата звернення: 12.11.2025).
11. VMware Cloud Foundation 9 Licensing and Product Packaging Guide. [Електронний ресурс] URL: <https://www.google.com/search?q=https://docs.vmware.com/en/VMware-Cloud-Foundation/services/vcf-licensing-guide/> (дата звернення: 12.11.2025).
12. Transitioning Horizon to Omnisia: Licensing Integration Guide. [Електронний ресурс] URL: <https://www.google.com/search?q=https://www.omnisia.com/resources/horizon-transition-guide> (дата звернення: 12.11.2025).
13. IDC Market Analysis: The Virtualization Landscape Post-Broadcom. [Електронний ресурс] URL: <https://www.google.com/search?q=https://www.idc.com/research/post-broadcom-vmware-strategy> (дата звернення: 12.11.2025).
14. Gartner: How to Navigate VMware Licensing Changes. [Електронний ресурс] URL: <https://www.google.com/search?q=https://www.gartner.com/en/documents/vmware-licensing-strategy-2025> (дата звернення: 12.11.2025).
15. VMware vSAN Licensing Whitepaper: Raw Capacity vs. Licensed Entitlement. [Електронний ресурс] URL: <https://www.google.com/search?q=https://core.vmware.com/resource/vsan-licensing-guide> (дата звернення: 12.11.2025).
16. Omnisia: KKR Completes Acquisition of VMware's EUC Division. [Електронний ресурс] URL:

- <https://www.google.com/search?q=https://www.omnissa.com/news/kkr-completes-acquisition> (дата звернення: 12.11.2025).
17. Horizon 8 Documentation: Installation and Configuration Guide. [Електронний ресурс] URL: <https://www.google.com/search?q=https://docs.omnissa.com/bundle/horizon-installation/> (дата звернення: 12.11.2025).
18. Omnissa TechZone: Horizon Subscription Licensing FAQ. [Електронний ресурс] URL: <https://www.google.com/search?q=https://techzone.omnissa.com/resource/horizon-licensing-faq> (дата звернення: 12.11.2025).
19. Broadcom-Omnissa Strategic OEM Partnership Agreement. [Електронний ресурс] URL: <https://www.google.com/search?q=https://www.broadcom.com/legal/oem-agreements/omnissa> (дата звернення: 12.11.2025).
20. Gartner Magic Quadrant for Desktop as a Service (DaaS) 2025. [Електронний ресурс] URL: <https://www.google.com/search?q=https://www.gartner.com/en/documents/daas-market-analysis> (дата звернення: 12.11.2025).
21. NVIDIA Virtual GPU (vGPU) Software Licensing Guide. [Електронний ресурс] URL: <https://docs.nvidia.com/grid/gpus-supported-by-vgpu.html> (дата звернення: 12.11.2025).
22. IDC MarketScape: Worldwide Virtual Client Computing 2025 Vendor Assessment. [Електронний ресурс] URL: <https://www.google.com/search?q=https://www.idc.com/getdoc.jsp%3FcontainerId%3DUS51234525> (дата звернення: 12.11.2025).
23. vmware-vsphere-7-0 [Електронний ресурс] URL: <https://techdocs.broadcom.com/content/dam/broadcom/techdocs/us/en/pdf/vmware/vsphere/vsphere/vmware-vsphere-7-0.pdf> (дата звернення: 13.11.2025).

24. VMware Cloud Foundation. [Электронный ресурс] URL: <https://www.vmware.com/products/cloud-infrastructure/vmware-cloud-foundation> (дата звернения: 18.11.2025)
25. VMware vSphere Documentation. [Электронный ресурс] URL: <https://techdocs.broadcom.com/us/en/vmware-cis/vsphere.html> (дата звернения: 18.11.2025)
26. Broadcom Support Portal. [Электронный ресурс] URL: <https://support.broadcom.com/> (дата звернения: 18.11.2025)
27. VMware vCenter Server Installation and Setup [Электронный ресурс] // Broadcom TechDocs. – Режим доступа: <https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0.html> (дата звернения: 18.10.2025).
28. Broadcom Delivers the Modern Private Cloud with VMware Cloud Foundation 9.0 [Электронный ресурс] // Broadcom Newsroom. – Режим доступа: <https://news.broadcom.com/releases/vmware-cloud-foundation-9-0> (дата звернения: 18.10.2025).
29. VMware vSphere 8.0 Release Notes [Электронный ресурс] // Broadcom TechDocs. – Режим доступа: <https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/release-notes/vmware-vsphere-80-release-notes.html> (дата звернения: 18.10.2025).

ДОДАТКИ

Додаток А. Копії екранів процесу встановлення ESX 7

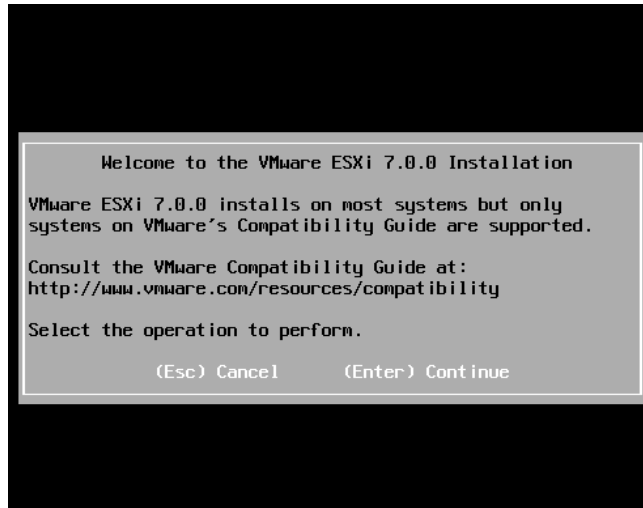


Рис.А.1

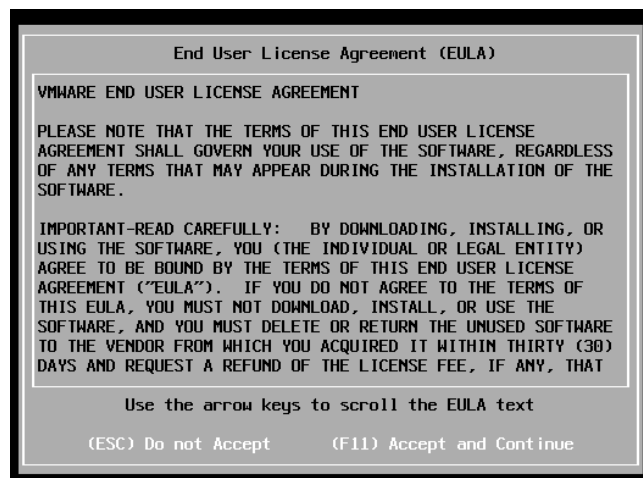


Рис.А.2

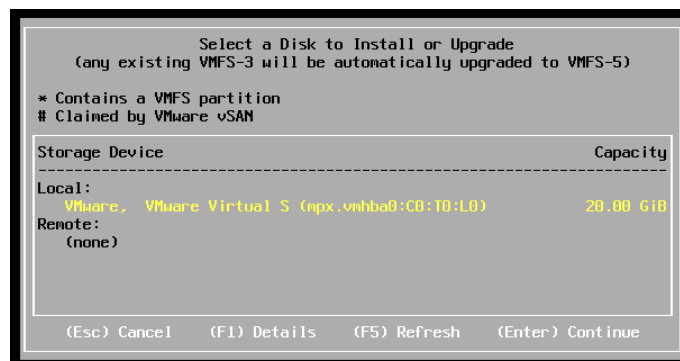


Рис.А.3



Рис.А.4

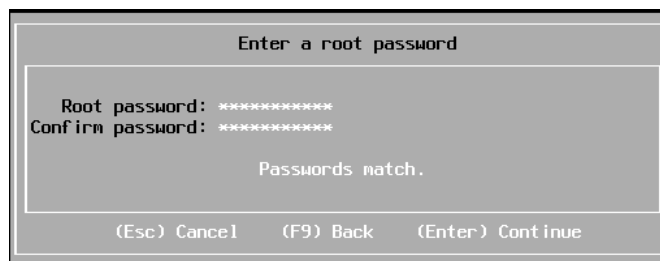


Рис.А.5

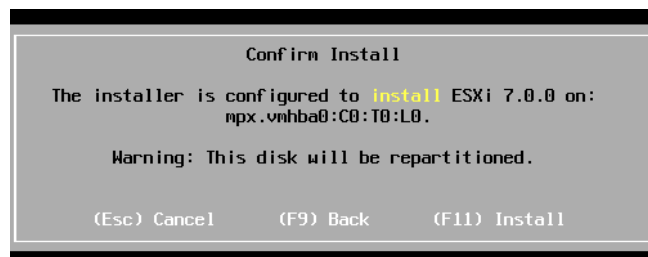


Рис.А.6

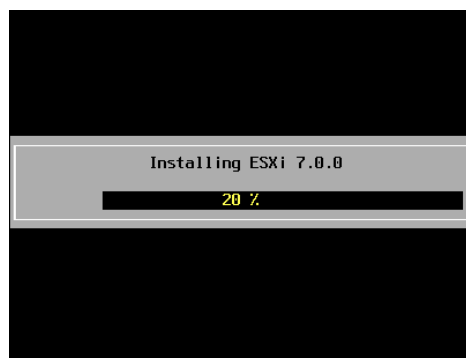


Рис.А.7

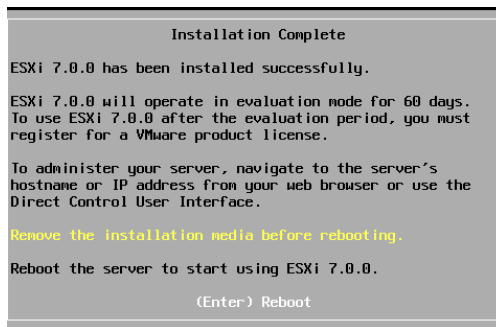


Рис.А.8

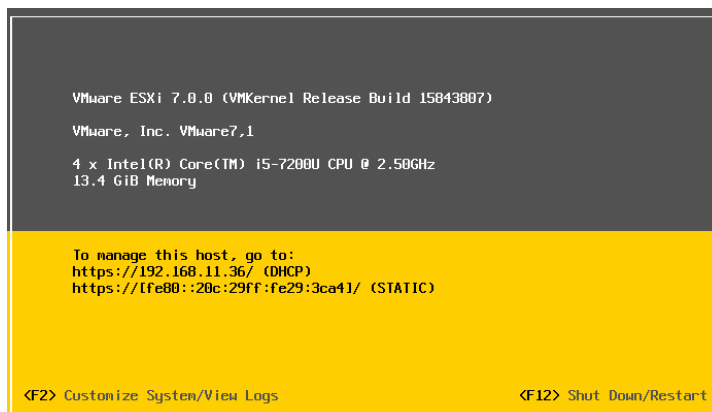


Рис.А.9

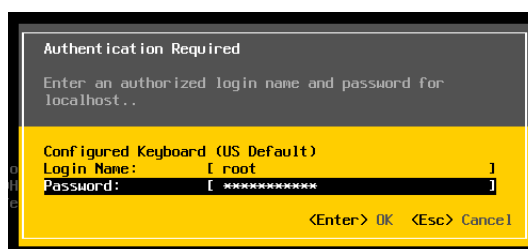


Рис.А.10

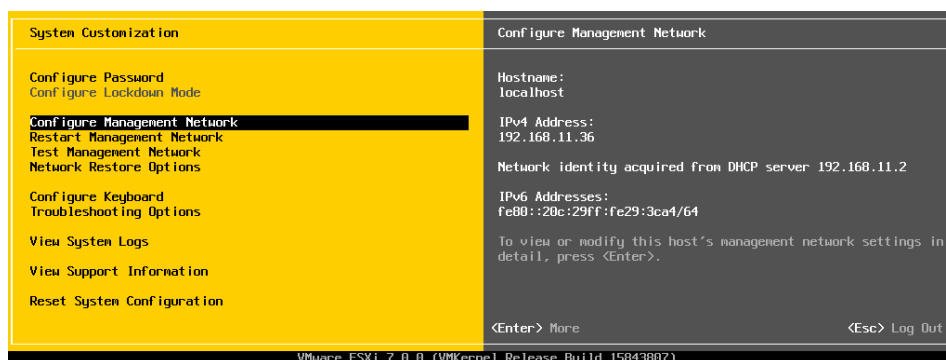


Рис.А.11

Додаток Б Копії екранів процесу налаштувань у ESXi 7

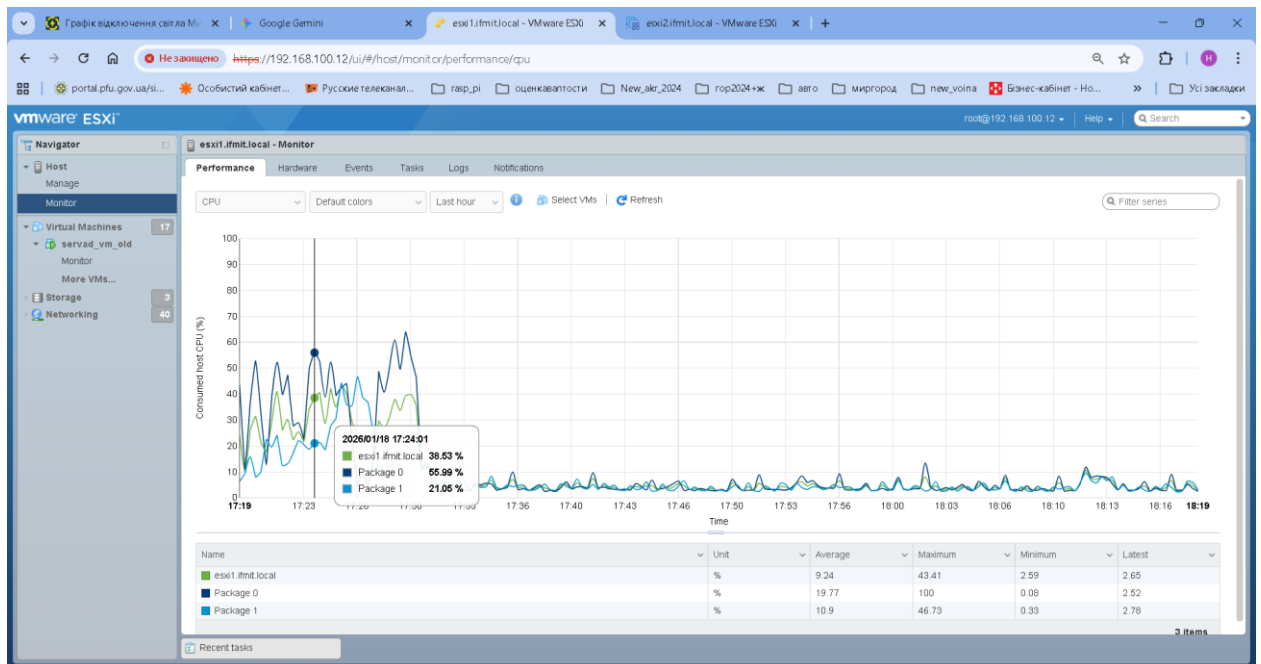


Рис. Б.1

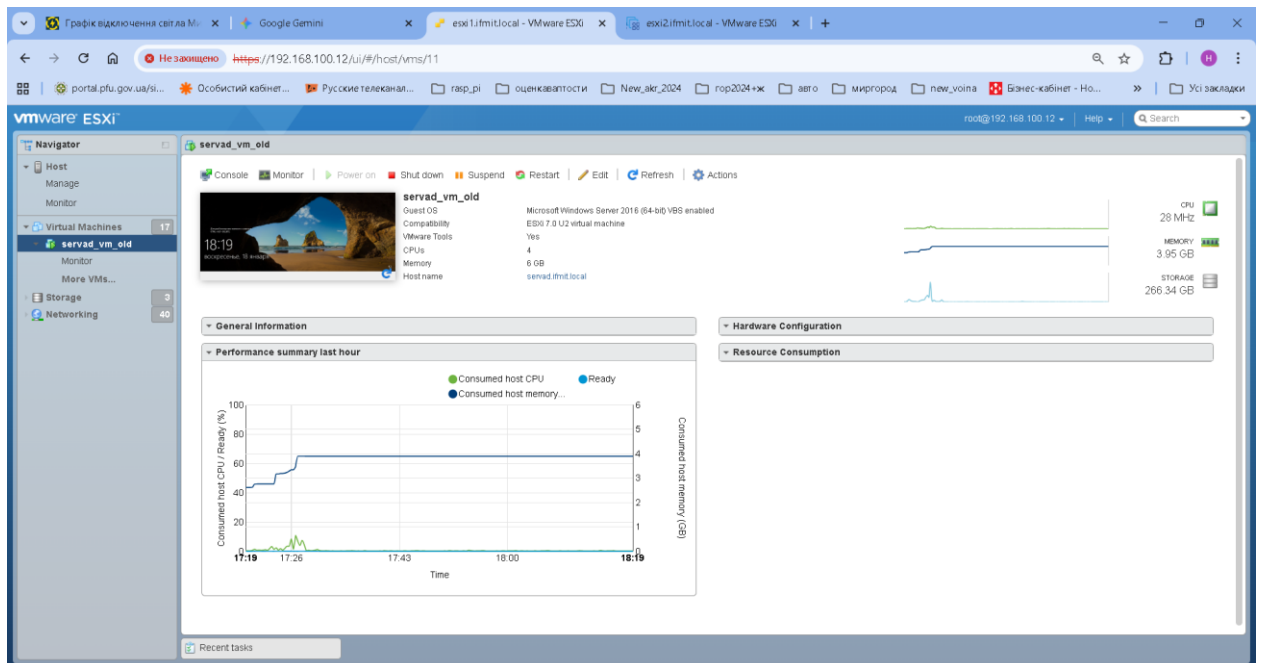


Рис. Б.2

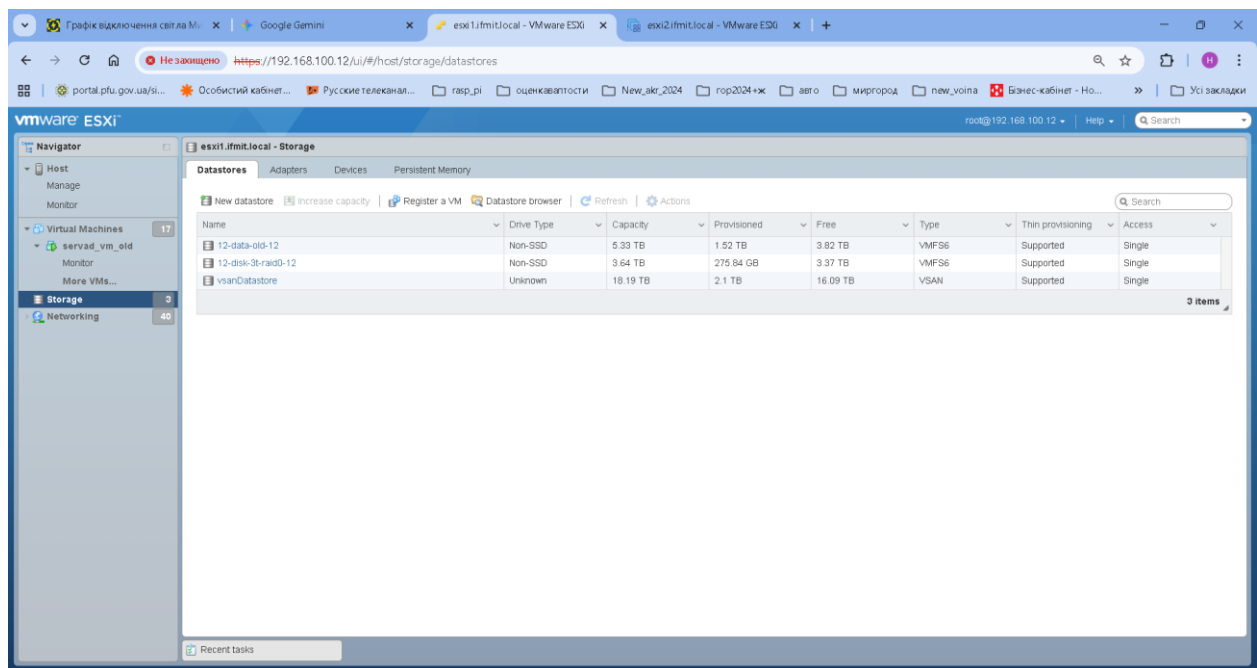


Рис. Б.3

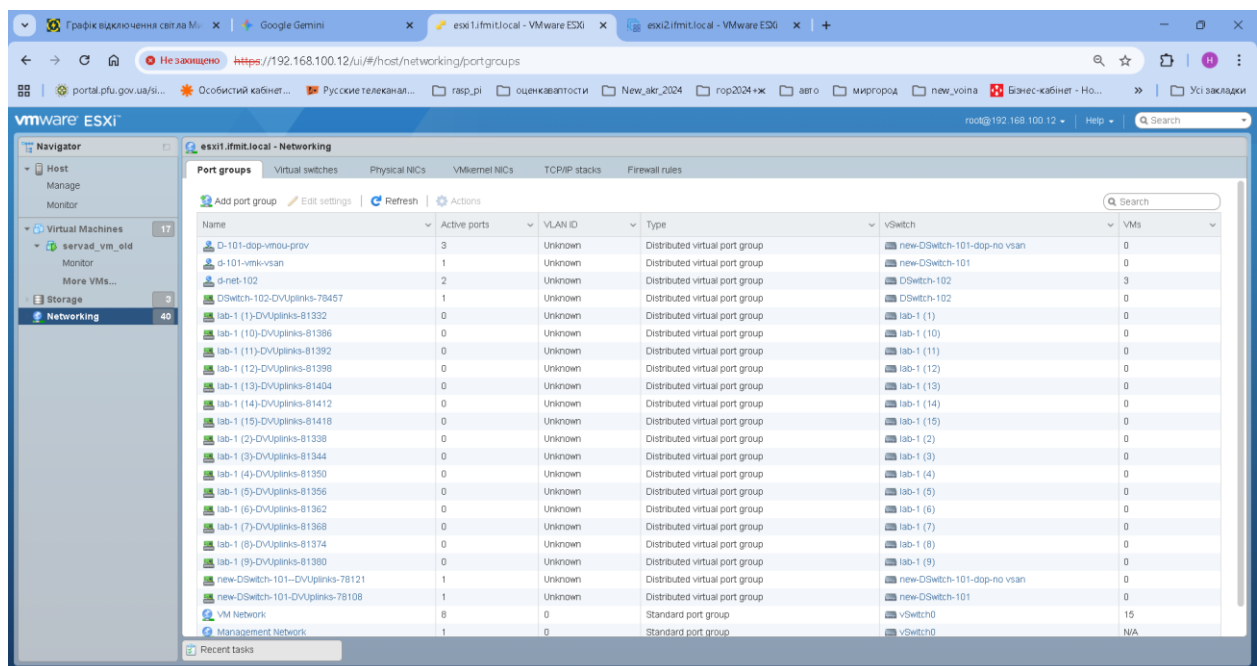


Рис. Б.4

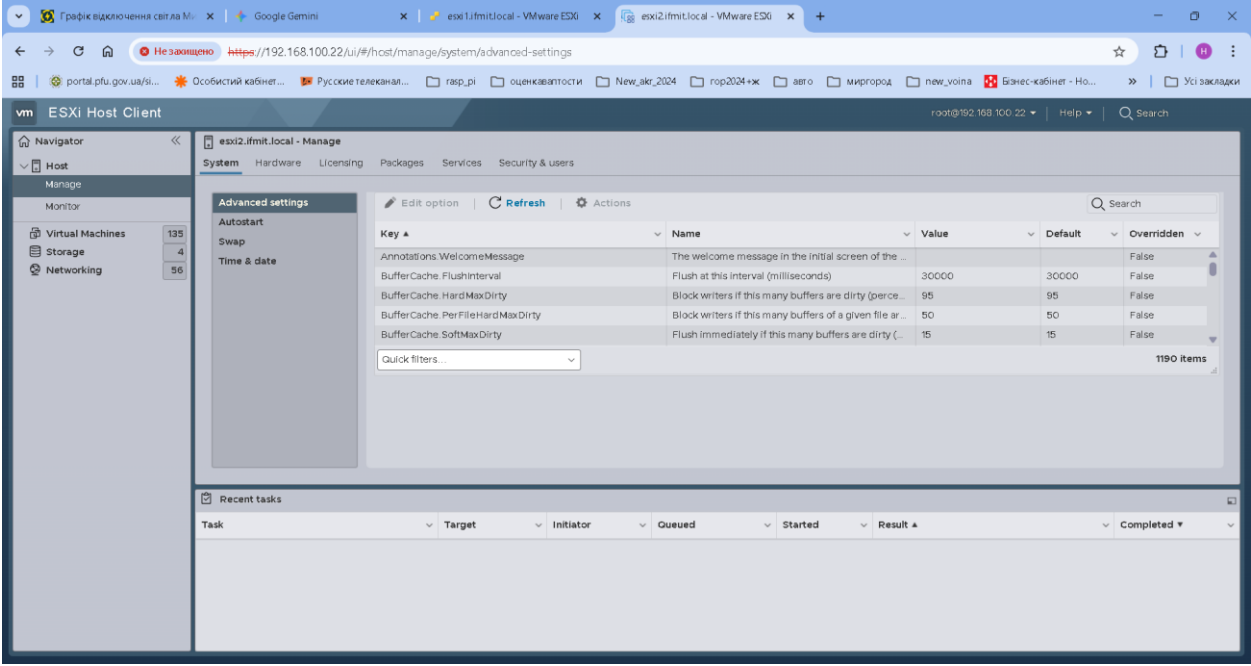


Рис. Б.5

Додаток В. Копії екранів процесу встановлення vCenter 7

Для установки vCenter 7.0 зберігаємо завантажений ISO на керуюче середовищем vSphere машину з Windows в D:\Install\VMware\VMware vSphere 7\VMware vCenter 7. Далі монтуємо ISO-образ як віртуальний диск DVD на комп'ютері, з якого здійснюється підключення до ESXi-хостів, або витягуємо вміст у каталог користувача. Переходимо в каталог " *vcsa-ui-installer\win32* " і запускаємо " *installer.exe* " (у випадку з Linux шукаємо каталог " *vcsa-ui-installer/lin64* "). Натискаємо «Install» для встановлення нового vCenter Server:

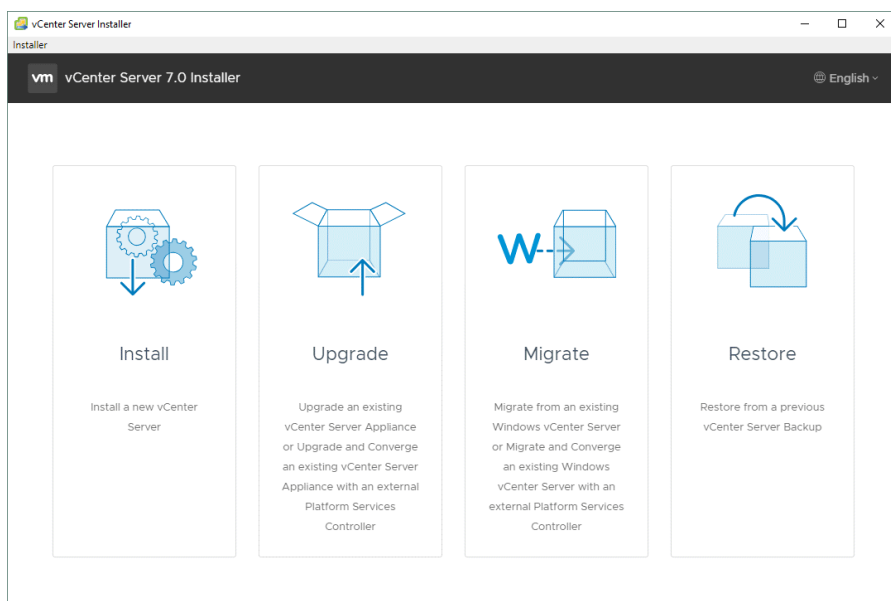


Рис. В.1

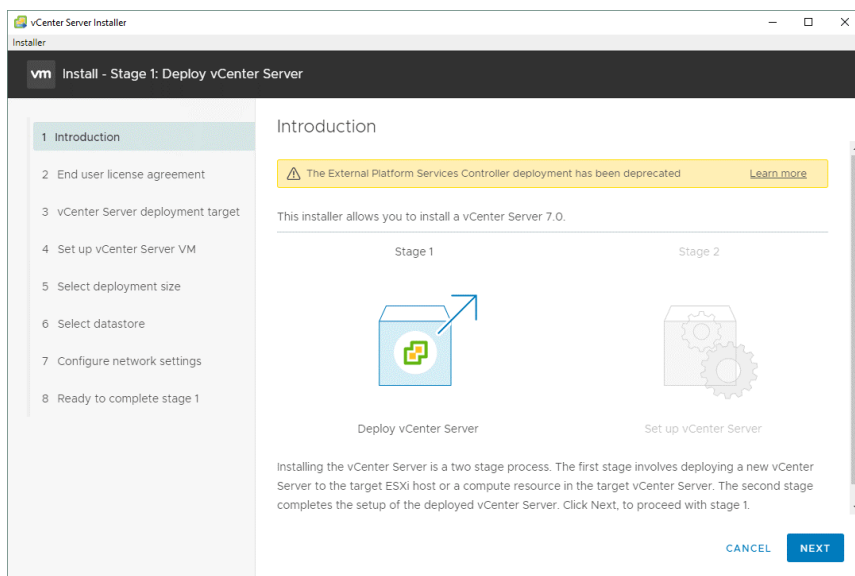


Рис. В.2

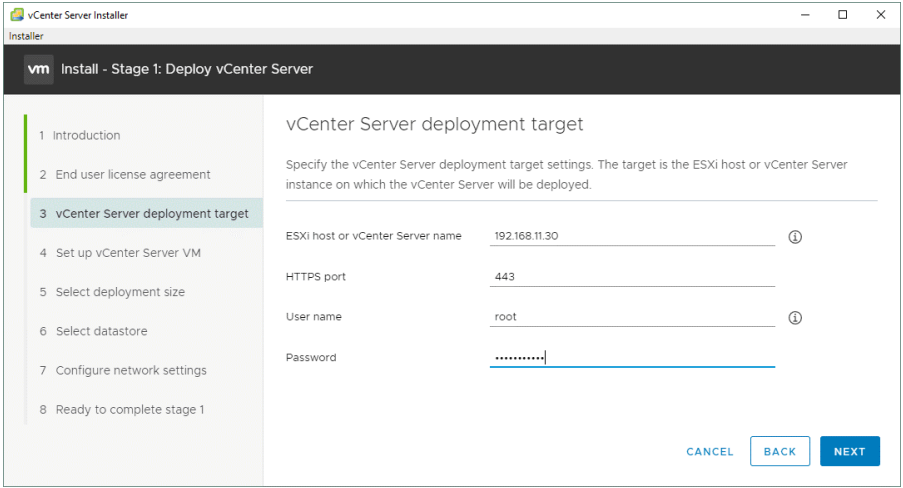


Рис. В.3

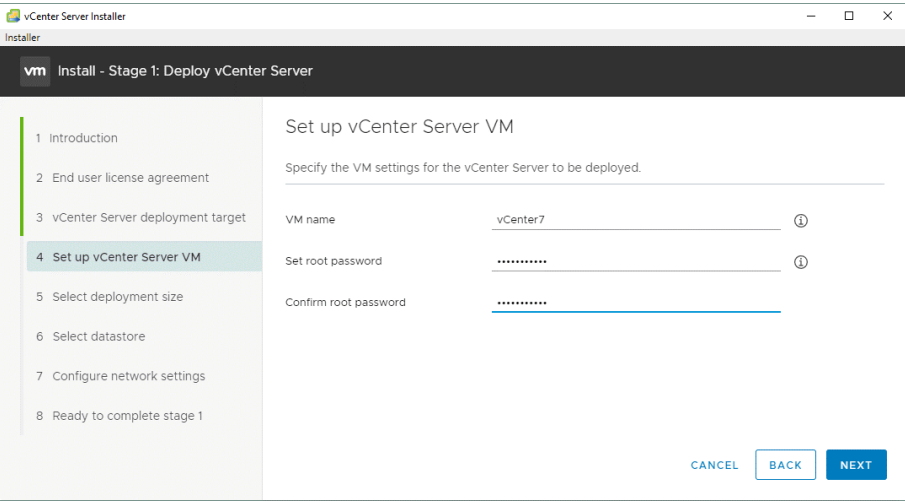


Рис. В.4

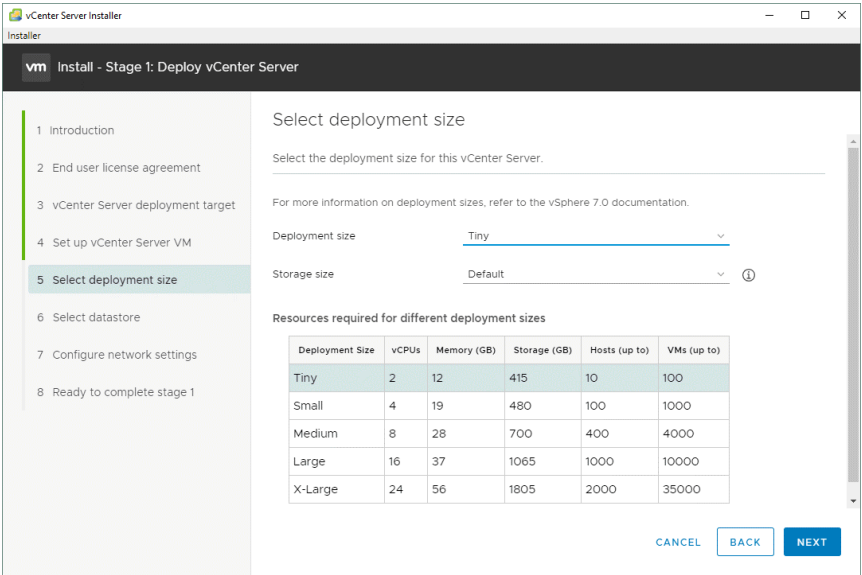


Рис. В.5

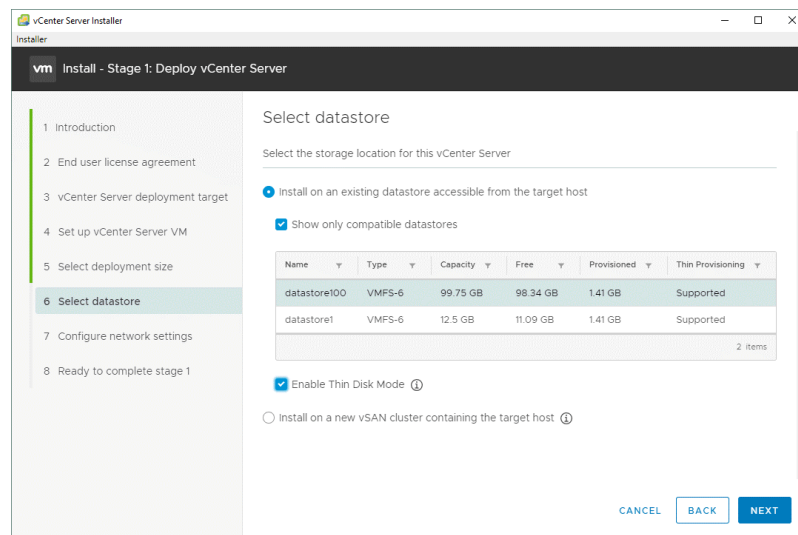


Рис. В.6

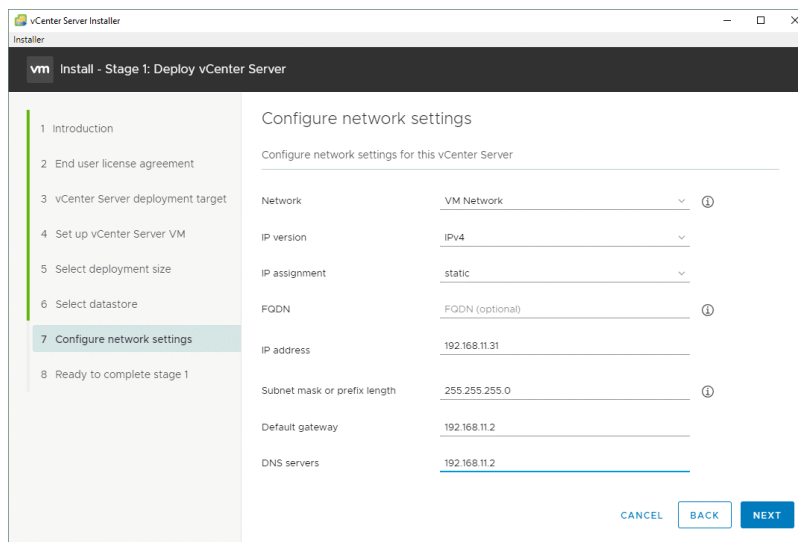


Рис. В.7

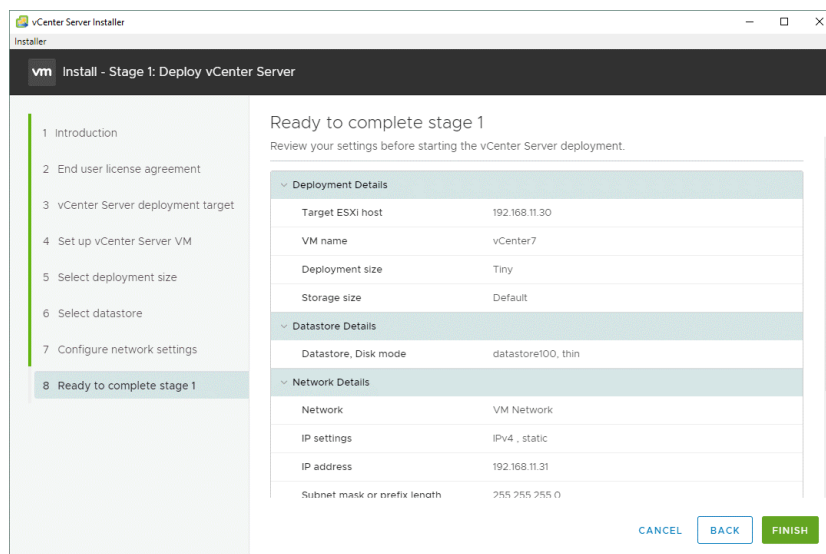


Рис. В.8

vm

Install - Stage 2: Set Up vCenter Server

1 Introduction

2 vCenter Server configuration

3 SSO configuration

4 Configure CEIP

5 Ready to complete

vCenter Server configuration

Time synchronization mode

Synchronize time with the ESXi ho

SSH access

Enabled

CANCEL

BACK

NEXT

Рис. В.9

vm

Install - Stage 2: Set Up vCenter Server

1 Introduction

2 vCenter Server configuration

3 SSO configuration

4 Configure CEIP

5 Ready to complete

SSO configuration

Create a new SSO domain

Single Sign-On domain name

vsphere.local

Single Sign-On user name

administrator

Single Sign-On password

.....

Confirm password

.....

Join an existing SSO domain

PSC

vCenter

CANCEL

BACK

NEXT

Рис. В.10

vm

Install - Stage 2: Set Up vCenter Server

1 Introduction

2 vCenter Server configuration

3 SSO configuration

4 Configure CEIP

5 Ready to complete

Configure CEIP

Join the VMware Customer Experience Improvement Program

Participating in VMware's Customer Experience Improvement Program ("CEIP") enables VMware to provide you with a proactive, reliable, and consistent vSphere environment and experience. Examples of such enhancements can be seen in the following features:

- vSphere Health
- vSAN Online Health
- vCenter Server Update Planner
- vSAN Performance Analytics
- Host Hardware Compatibility
- vSAN Support Insight

CEIP collects configuration, feature usage, and performance information. No personally identifiable information is collected. All data is sanitized and obfuscated prior to being received by VMware.

For additional information on CEIP and the data collected, please see VMware's

Join the VMware's Customer Experience Improvement Program (CEIP)

CANCEL

BACK

NEXT

Рис. В.11

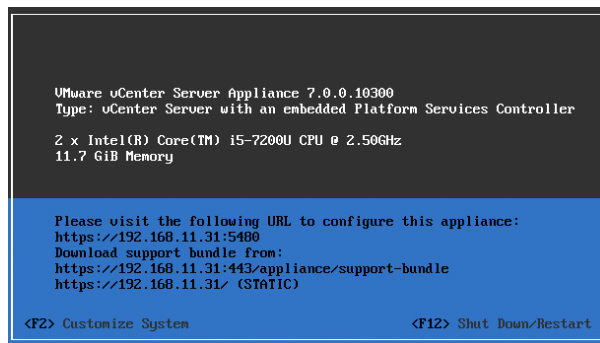


Рис. В.12

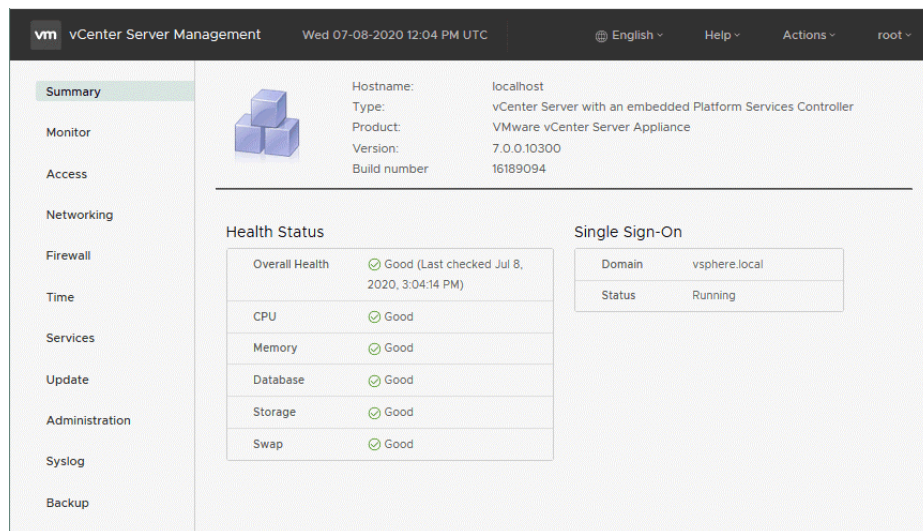


Рис. В.13