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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проєкт публічного веб-порталу організації з керуванням через Active Directory»

Виконав: студент 4-го курсу групи КІ-21-1
спеціальності 123 «Комп'ютерна інженерія»
_____ Владислав ЖЕРЕБЧУК
Керівник: доцент кафедри КІ та КБ, к.т.н.
_____ Юрій БРОДСЬКИЙ
Рецензент: професор кафедри КІ та КБ, д.т.н., с.н.с.
_____ Сергій КОВБАСЮК

Житомир – 2025

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу бакалавра

Студент: Жеребчук Владислав Сергійович

Тема роботи: «Проєкт публічного веб-порталу організації з керуванням через Active Directory»

затверджена Наказом університету від 3 березня 2025 р. № 79/с

Термін здачі студентом закінченої роботи 9 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження): Предметом дослідження є технології веб-розробки, служби Active Directory, механізми автентифікації LDAP, а також засоби розгортання та адміністрування веб-порталів у середовищі Windows Server.

Об'єктом дослідження є інформаційна інфраструктура організації, зокрема процес керування доступом до веб-ресурсів у корпоративному середовищі.

Обладнання та програмне забезпечення:

1. Засіб віртуалізації Oracle VirtualBox
2. Операційні системи Windows Server 2019, Windows 10
3. Доменні служби Microsoft, зокрема Active Directory, IIS
4. Система моніторингу PRTG Network Monitor

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Фальковський І.Г.	01.04.2025	01.04.2025
2	Фальковський І.Г.	01.04.2025	01.04.2025
3	Фальковський І.Г.	01.04.2025	01.04.2025

Студент _____ Владислав ЖЕРЕБЧУК
Керівник _____ Юрій БРОДСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	
2	Аналіз отриманого завдання	05.03.2025	
3	Аналіз літературних джерел	20.03.25-23.03.2025	
4	Постановка задачі дослідження	25.03.2025-30.03.2025	
5	Вибір засобів реалізації	01.04.2025-14.04.2025	
6	Проектування мережі	15.04.2025-10.04.2025	
7	Налаштування і відлагодження проекту	10.05.2025-25.05.2025	
8	Перевірка працездатності	26.05.2025-30.05.2025	
9	Написання пояснювальної записки	30.05.2025-09.06.2025	
10	Захист	19.06.2025	

Студент _____ Владислав ЖЕРЕБЧУК

Керівник _____ Юрій БРОДСЬКИЙ

АНОТАЦІЯ

У кваліфікаційній роботі розглянуто проєкт створення публічного веб-порталу організації з підтримкою автентифікації користувачів через службу Active Directory. Метою роботи було забезпечення централізованого керування доступом до інформаційних ресурсів у межах корпоративної мережі з використанням LDAP-протоколу.

У процесі реалізації було спроєктовано і впроваджено доменну інфраструктуру на базі Windows Server, налаштовано служби та засоби моніторингу PRTG Network Monitor. Розгорнуто веб-портал на базі CMS WordPress, інтегрований з Active Directory. Реалізовано механізм розмежування доступу до вмісту сайту на основі ролей користувачів: неавторизовані відвідувачі мають доступ лише до публічних сторінок, користувачі AD — до внутрішніх розділів, адміністратори — до розширених можливостей керування.

Пояснювальна записка містить 65 сторінок, включає 73 рисунки, 3 таблиці. Список використаних джерел налічує 21 найменувань.

Ключові слова: ACTIVE DIRECTORY, LDAP, ВЕБ-ПОРТАЛ, WORDPRESS, АВТЕНТИФІКАЦІЯ, ІНФРАСТРУКТУРА, СИСТЕМА МОНІТОРИНГУ, PRTG.

ANNOTATION

This bachelor’s qualification work presents a project for developing a public web portal for an organization with user authentication support via Active Directory. The aim of the work was to implement centralized access control to information resources within a corporate network using the LDAP protocol.

During the implementation, a domain infrastructure based on Windows Server was designed and deployed. Core services and the PRTG Network Monitor system were configured. The web portal, developed using the WordPress CMS, was integrated with Active Directory. A role-based access control mechanism was implemented: unauthenticated visitors have access only to public pages, AD users can access internal sections, and administrators are granted extended management capabilities.

The explanatory report consists of 65 pages, includes 73 figures and 3 tables. The list of references contains 21 sources.

Keywords: ACTIVE DIRECTORY, LDAP, WEB PORTAL, WORDPRESS, AUTHENTICATION, INFRASTRUCTURE, MONITORING SYSTEM, PRTG.

ЗМІСТ

ВСТУП 8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНОЇ МЕРЕЖІ З ЦЕНТРАЛІЗОВАНИМ КЕРУВАННЯМ ДОСТУПОМ 9
1.1. Архітектура корпоративної мережі на основі Active Directory 9
1.2. Протокол LDAP як засіб автентифікації користувачів 13
1.3. Побудова веб-порталу у корпоративній мережі 15
1.4. Системи моніторингу корпоративної мережі 19
РОЗДІЛ 2. ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА СТРУКТУРИ ДОМЕНУ 25
2.1. Загальна концепція, логіка роботи та взаємодія компонентів системи 25
2.2. Логічна модель доменної інфраструктури 27
2.3. Вибір обладнання та програмного забезпечення 28
2.4. Адресна схема і топологія мережі 29
РОЗДІЛ 3. НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ПРОЕКТУ 32
3.1. Налаштування доменних служб Active Directory 32
3.2. Встановлення системи моніторингу мережі 39
3.3. Розгортання веб-порталу 43
3.4. Тестування комп'ютерної мережі та налаштованих сервісів 55
ВИСНОВКИ 62
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 63
ДОДАТКИ 66

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

AD – Active Directory

IIS – Internet Information Services

LDAP – Lightweight Directory Access Protocol

CA – Certificate Authority

CMS – Content Management System

DHCP – Dynamic Host Configuration Protocol

GPO – Groups Policy Object

DNS – Domain Name System

СУБД – Система управління базами даних

DC – Domain Controller

URL – Uniform Resource Locator

ВСТУП

Актуальність теми. У сучасних організаціях ефективне управління IT-інфраструктурою, зокрема доступом користувачів до ресурсів, є критично важливим. Використання служби Active Directory дозволяє централізовано керувати обліковими записами, політиками безпеки та доступом до інформаційних систем. Одним із актуальних напрямків є розробка публічних веб-порталів, які забезпечують як відкритий доступ до інформації, так і обмежений доступ до внутрішніх сервісів за допомогою корпоративної автентифікації. Реалізація такого підходу поєднує переваги веб-технологій із безпекою та централізованим управлінням, що є особливо актуальним для навчальних закладів, державних і приватних організацій.

Метою кваліфікаційної роботи є створення публічного веб-порталу організації з інтеграцією в інфраструктуру Active Directory для забезпечення автентифікації користувачів через LDAP та централізованого керування доступом до інформаційних ресурсів.

Визначена мета обумовлює такі завдання:

- Налаштувати інфраструктуру домену Active Directory;
- Реалізувати веб-портал організації на основі CMS WordPress із розгортанням на IIS;
- Забезпечити автентифікацію користувачів веб-порталу через LDAP Active Directory;
- Налаштувати моніторинг стану інфраструктури для контролю роботи сервісів;
- Провести тестування функціональності порталу та взаємодії з доменом.

Об’єктом дослідження є інформаційна інфраструктура організації, зокрема процес керування доступом до веб-ресурсів у корпоративному середовищі.

Предметом дослідження є технології веб-розробки, служби Active Directory, механізми автентифікації LDAP, а також засоби розгортання та адміністрування веб-порталів у середовищі Windows Server.

У процесі виконання кваліфікаційної роботи було розроблено проект публічного веб-порталу організації з автентифікацією користувачів через службу Active Directory, що дозволяє здійснювати захищений доступ до внутрішніх сервісів на основі доменних облікових записів.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНОЇ МЕРЕЖІ З ЦЕНТРАЛІЗОВАНИМ КЕРУВАННЯМ ДОСТУПОМ

1.1. Архітектура корпоративної мережі на основі Active Directory

Доменна інфраструктура є основою централізованого управління комп'ютерними ресурсами в корпоративному середовищі. У контексті Windows Server вона реалізується за допомогою служби Active Directory Domain Services (AD DS) — ієрархічної системи, що дозволяє ефективно зберігати і керувати інформацією про об'єкти мережі (користувачів, комп'ютери, принтери тощо) та керувати доступом до ресурсів.

Однією з найпоширеніших реалізацій доменної інфраструктури в корпоративному середовищі є служба каталогів Active Directory Domain Services (AD DS), яка входить до складу ОС Windows Server. Active Directory організовує інформацію у вигляді «об'єктів» — це можуть бути будь-які ресурси мережі, зокрема комп'ютери, користувацькі облікові записи, контакти, групи, організаційні одиниці чи спільні папки. Кожен об'єкт має унікальне ім'я та набір атрибутів, які допомагають точно його ідентифікувати. Уся ця інформація зберігається в спеціалізованому структурованому сховищі, яке забезпечує швидку обробку запитів і масштабованість. Завдяки цьому користувачі та програми можуть легко знаходити й використовувати необхідні дані [1]. Завдяки Active Directory реалізується автентифікація користувачів та пристроїв, авторизація доступу до ресурсів, а також реплікація змін між серверами в межах домену або організації.

Структура домену в Active Directory має чітку ієрархію. Найвищим рівнем є ліс (англ. Forest) — логічна структура, яка об'єднує одну або кілька доменних структур зі спільною конфігурацією, схемою об'єктів та глобальним каталогом. У межах лісу домени можуть автоматично довіряти один одному, що забезпечує взаємну автентифікацію та взаємодію між об'єктами. Ліс може містити кілька доменів, які утворюють дерево доменів, проте в невеликих мережах зазвичай достатньо одного домену.

Наступним рівнем ієрархії є домен — базова адміністративна одиниця, яка визначає межі політик безпеки та керування. Домен має унікальне ім'я, зазвичай у форматі DNS, наприклад: uniwork.net. У межах домену зберігаються всі об'єкти — облікові записи користувачів, комп'ютерів, групи, принтери тощо. Домен є єдиною точкою автентифікації для користувачів і пристроїв, а адміністрування здійснюється за допомогою одного або кількох серверів — контролерів домену.

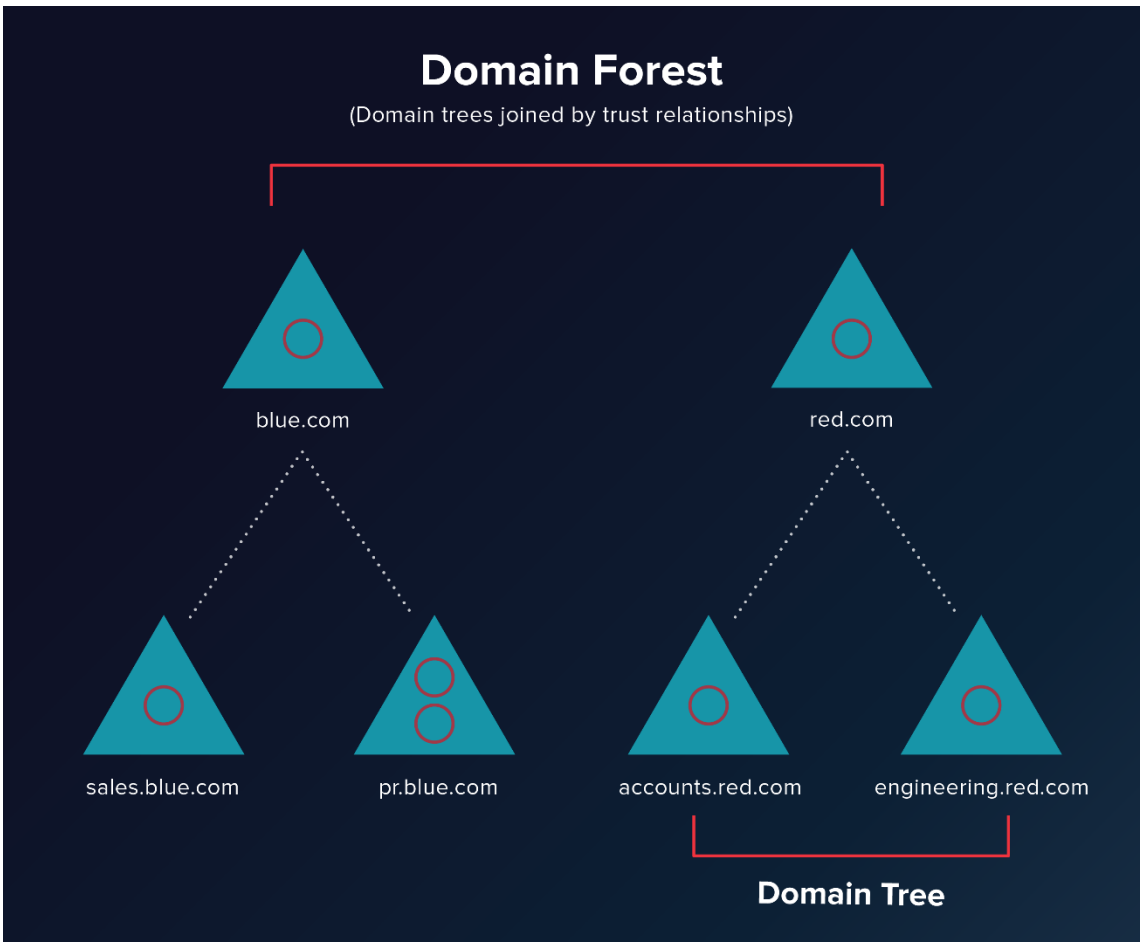


Рисунок 1.1.1 – Приклад організації структури лісу

Контролер домену — це сервер, на якому встановлено роль AD DS. Він відповідає за обробку запитів автентифікації, застосування групових політик, підтримку структури каталогів, а також за синхронізацію змін з іншими контролерами домену. У великих або критично важливих середовищах зазвичай використовується два або більше контролерів для забезпечення відмовостійкості та балансування навантаження.

Контролер домену містить копію бази даних AD DS. На кожному контролері домену існує копія сховища даних. База даних AD DS використовує технологію баз

даних Microsoft Jet і зберігає інформацію про каталог у файлі Ntds.dit і пов'язаних з ним журналах. За замовчуванням ці файли зберігаються у папці C:\Windows\NTDS.

У межах одного домену для структурування об'єктів використовуються організаційні одиниці (OU). Це логічні підрозділи, які можуть відображати реальну організаційну структуру установи: наприклад, відділи, факультети або філії. Організаційні одиниці дозволяють не лише впорядковувати об'єкти, а й делегувати адміністративні повноваження та застосовувати локальні групові політики.

Безпека вбудована в AD DS за рахунок інтеграції з автентифікацією входу та механізмами контролю доступу до об'єктів каталогу. Завдяки єдиному імені користувача та паролю адміністратори можуть централізовано управляти даними й структурою каталогу в усій мережі, а авторизовані користувачі мають змогу отримувати доступ до ресурсів незалежно від свого місцезнаходження. Використання політик для адміністрування значно спрощує керування навіть великими і складними мережами.

Серед ключових компонентів AD DS:

- Схема — набір правил, що визначає типи об'єктів і атрибутів у каталозі, обмеження на їх використання та формат імен.
- Глобальний каталог — містить відомості про всі об'єкти каталогу, дозволяючи здійснювати пошук даних незалежно від того, в якому домені вони зберігаються.
- Механізм запитів та індексування — забезпечує можливість для користувачів і програм знаходити об'єкти й їх властивості або розміщувати їх у каталозі.
- Служба реплікації — відповідає за поширення даних каталогу по всій мережі. Усі контролери домену в межах одного домену беруть участь у реплікації, зберігаючи повну копію каталогічної інформації для свого домену. Будь-які зміни автоматично поширюються на всі контролери домену [2].

Управління користувачами в домені передбачає створення облікових записів, налаштування атрибутів, призначення ролей і забезпечення доступу до ресурсів відповідно до повноважень. Для спрощення адміністрування користувачі можуть

об’єднуватися в групи. Групи бувають двох типів: групи безпеки, які використовуються для призначення дозволів, та групи розсилки — для організації електронної пошти.

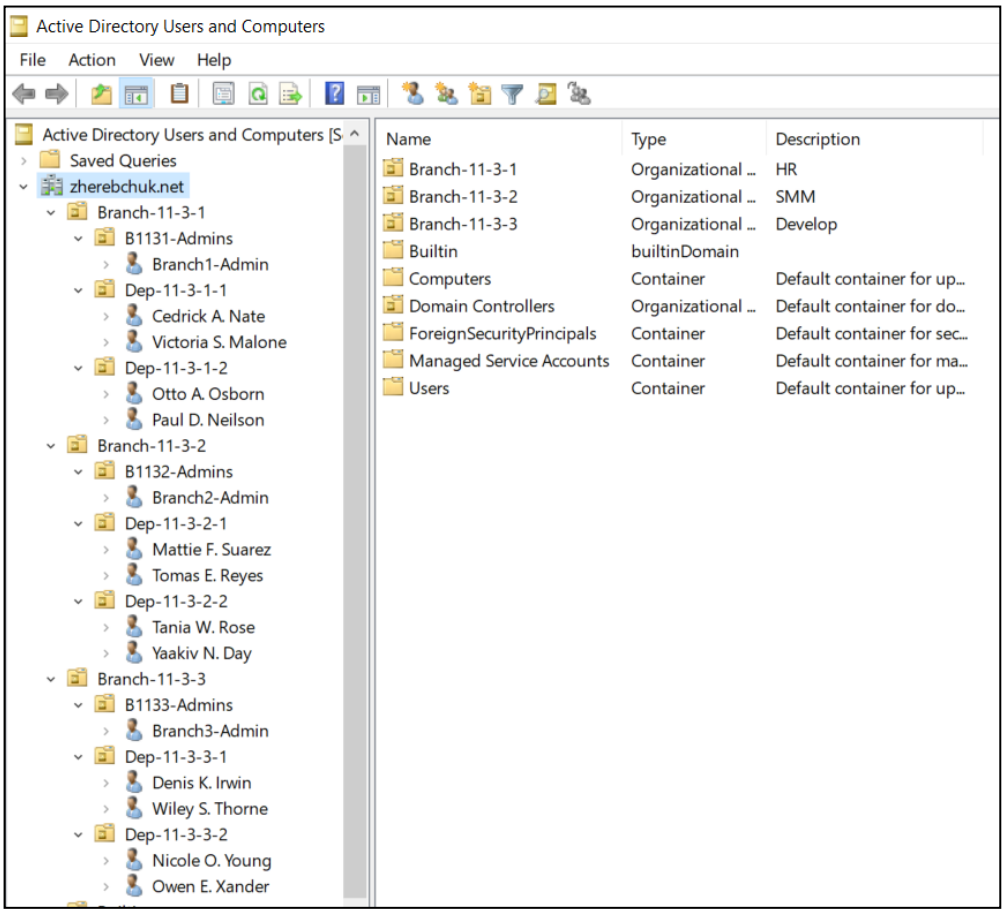


Рисунок 1.1.2 – Домен у Active Directory

Одним з основних інструментів централізованого управління є групові політики (Group Policy Objects, GPO). Вони дозволяють автоматизовано застосовувати конфігурації безпеки, обмеження, інтерфейсні налаштування та інші параметри до користувачів і пристроїв. Групові політики можуть застосовуватися на рівні сайту, домену або OU, що забезпечує гнучкість та адаптивність при побудові системи адміністрування.

Наявність доменної інфраструктури спрощує адміністрування великої кількості комп’ютерів, дозволяє централізовано оновлювати політики, забезпечує підвищений рівень контролю безпеки, а також є основою для інтеграції з іншими сервісами.

1.2. Протокол LDAP як засіб автентифікації користувачів

У сучасних інформаційних системах важливу роль відіграє механізм автентифікації, що дозволяє перевірити особу користувача перед наданням доступу до ресурсів. Одним з найпоширеніших і стандартних протоколів автентифікації у корпоративному середовищі є LDAP (Lightweight Directory Access Protocol) — полегшений протокол доступу до служби каталогів, який ґрунтується на моделі клієнт-сервер.

LDAP — це відкритий стандарт, розроблений як спрощений варіант складнішого протоколу DAP, що входив до складу стандарту X.500[3][19]. Його головна перевага — легкість впровадження, масштабованість і підтримка більшістю операційних систем і застосунків, зокрема серверів автентифікації, електронної пошти, систем моніторингу, корпоративних порталів тощо.

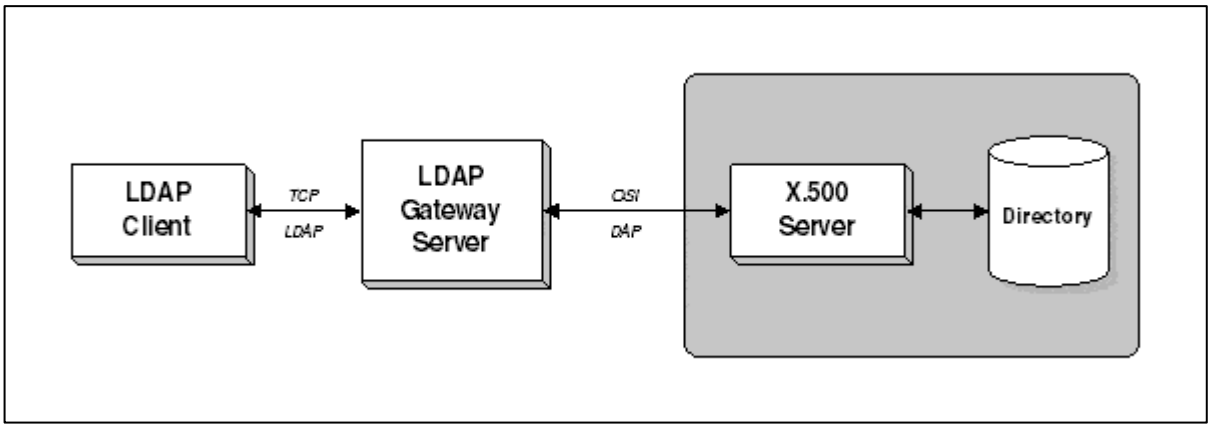


Рисунок 1.2.1 – Механізм автентифікації через LDAP

Фактично, клієнт надсилає запит на отримання інформації з бази даних LDAP разом зі своїми обліковими даними на сервер LDAP. Сервер, у свою чергу, перевіряє ці дані, звіряючи їх з основною ідентифікаційною інформацією користувача, що вже зберігається у системі. Якщо передані облікові дані збігаються з тими, що пов’язані з відповідним записом у базі, клієнт отримує доступ до потрібної інформації — наприклад, атрибутів користувача, членства в групах чи інших пов’язаних даних. У випадку невідповідності даних сервер блокує доступ і запит не виконується [4]. Запити можуть бути як простими (пошук конкретного користувача за іменем), так і складними (вибірка всіх об’єктів певного типу в межах заданої гілки каталогу).

Розглянемо приклад запиту на пошук користувача «John Doe». Сервер LDAP працює з деревом інформації про каталог (DIT), яке представляє собою ієрархічну структуру записів. Кожен із них має унікальне розташування в цьому дереві, визначене повним іменем (DN), наприклад:

CN=John Doe, OU=IT, DC=uniwork, DC=net.

Тут CN означає Common Name (ім'я об'єкта), OU — Organizational Unit, а DC — Domain Component. LDAP-запити формуються з урахуванням цієї структури, що дозволяє гнучко та точно здійснювати пошук та автентифікацію об'єктів.

Це ім'я (Distinguished Name) точно визначає місце запису в ієрархії. Сервер LDAP швидко обходить структуру DIT, щоб знайти потрібного користувача та пов'язану з ним інформацію. Така організація забезпечує не лише порядок, а й ефективний доступ до даних у чітко структурованій формі [5].

Нижче наведено основні операції, які виконує LDAP:

Прив'язка (Bind) — автентифікація користувача на сервері LDAP, наприклад, під час входу в систему на початку дня.

Пошук (Search) — пошук записів за заданими критеріями, наприклад, знаходження користувача в Outlook або Skype для бізнесу.

Додавання (Add) — створення нових облікових записів чи ролей в Active Directory.

Зміна (Modify) — редагування властивостей існуючих об'єктів у каталозі.

Видалення (Delete) — повне видалення запису користувача з Active Directory.

Крім DN, важливу роль відіграють атрибути LDAP-об'єктів. Наприклад, об'єкт користувача в Active Directory може мати такі атрибути: sAMAccountName (ім'я входу в систему), userPrincipalName (UPN), mail (електронна пошта), memberOf (членство у групах), givenName, sn (прізвище) тощо. Сторонні системи, наприклад веб-портали або інші сервіси, можуть використовувати ці атрибути для авторизації, надання доступу, персоналізації тощо.

Таблиця 1.1 – Типові атрибути LDAP-об'єктів користувача

Атрибут	**Призначення**	**Приклад значення**
sAMAccountName	Ім'я користувача для входу	j.doe
userPrincipalName	Повне ім'я користувача	j.doe@uniwork.net

mail	Email-адреса користувача	j.doe@uniwork.net
memberOf	Групи, до яких входить користувач	CN=IT,OU=Staff,…

LDAP-автентифікація у зовнішніх застосунках реалізується через підключення до AD-серверу за відомими параметрами (адреса, порт, база пошуку) та виконанням bind-запиту. У процесі bind-запиту система намагається “зв’язати” ім’я користувача (DN або UPN) із паролем. Якщо облікові дані дійсні, сервер відповідає успішно, і користувач вважається автентифікованим. У більшості випадків LDAP-підключення виконується на порт 389 (незахищене з’єднання) або 636 (через SSL/TLS) [5].

Веб-системи, які підтримують LDAP, можуть бути налаштовані на використання Active Directory як джерела автентифікації. У цьому випадку користувач вводить свої доменні облікові дані, які передаються на LDAP-сервер для перевірки. Це дозволяє уникнути дублювання облікових записів, забезпечити централізовану безпеку та спростити адміністрування.

1.3. Побудова веб-порталу у корпоративній мережі

Веб-портали стали невід’ємною частиною цифрової інфраструктури сучасних організацій, забезпечуючи зручний доступ до сервісів, обмін інформацією та ефективну взаємодію між користувачами. Залежно від призначення, такі портали можуть бути публічними або внутрішніми (корпоративними). Публічні портали зазвичай орієнтовані на зовнішніх користувачів: клієнтів, студентів, партнерів, громадськість. Вони надають доступ до загальної інформації, новин, сервісів подання заявок тощо. Натомість внутрішні портали слугують інструментом організації внутрішніх процесів: доступу до документів, календарів, систем моніторингу, внутрішніх оголошень, обліку тощо.

У межах корпоративної мережі побудова веб-порталу потребує використання стабільної та керованої серверної платформи. Одним із найрозповсюдженіших рішень для розгортання веб-додатків у середовищі Windows є служба IIS (Internet Information Services). Веб-сервер IIS входить до складу ОС Windows Server і забез-

печує повний набір функціональних можливостей для хостингу сайтів, веб-додатків та служб. Він підтримує основні протоколи (HTTP, HTTPS, FTP), має вбудовані механізми безпеки, засоби керування сертифікатами, розширювану архітектуру на основі модулів, а також інтеграцію з .NET і PowerShell [6]. Існують також сторонні утиліти для запуску IIS на Linux та macOS, але це часто забезпечує меншу стабільність та низьку продуктивність. Для адміністраторів доступна графічна консоль, яка полегшує налаштування сайтів, віртуальних каталогів, прав доступу, модулів обробки запитів тощо.

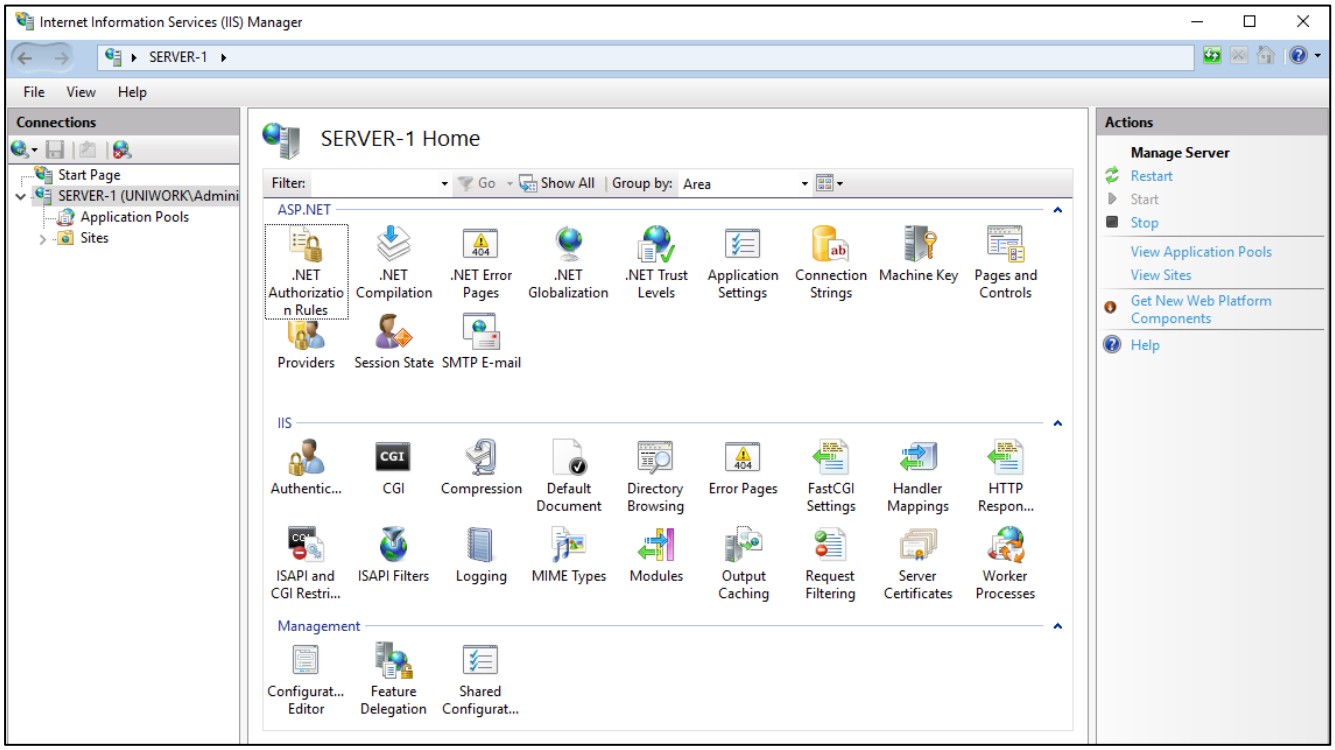


Рисунок 1.3.1 – Графічний інтерфейс IIS

Ось основні способи використання сервера Microsoft IIS у сучасних IT-середовищах [7]:

- Хостинг веб-сайтів — IIS виконує функції сервера додатків і здатен розміщувати корпоративні веб-сайти, веб-додатки та служби WCF. Близько 30% веб-ресурсів у світі працюють саме на цій платформі.
- Фільтрація запитів — сервер надає модуль для виявлення та блокування потенційно небезпечних клієнтських запитів. Фільтрація може здійснюватися за такими параметрами, як тип файлу, довжина URL або максимальний розмір переданого рядка.

- Ведення журналів — IIS збирає докладну інформацію про роботу сервера і сайтів, зокрема дані про навантаження, продуктивність і збої. Аналіз логів дає змогу оперативно виявляти та усувати технічні проблеми.
- Інтеграція з .NET — платформа IIS має вбудовану підтримку Microsoft .NET, що дає змогу розробникам ефективно створювати, розгортати й адмініструвати веб-додатки на основі ASP.NET.

Важливим етапом є вибір системи управління контентом (CMS). Хоча більшість популярних CMS спочатку розроблялись під Linux-середовище, значна частина з них може бути успішно встановлена й функціонувати під Windows за умови наявності відповідного веб-сервера, інтерпретатора мови та СУБД.

Серед найпоширеніших рішень для Windows-середовища доцільно розглянути WordPress, Joomla та OrchardCore.

Таблиця 1.2 – Порівняння CMS

Характеристика	**WordPress**	**Joomla**	**OrchardCore**
Платформа	PHP / MySQL	PHP / MySQL	ASP.NET Core / SQL Server
Середовище	Кросплатформенне	Кросплатформенне	Оптимізоване для Windows
Простота використання	Висока	Середня	Низька (вимагає знань .NET)
Гнучкість	Висока (через плагіни)	Висока	Дуже висока
Призначення	Публічні сайти, блоги	Корпоративні сайти	Внутрішні портали, інтегровані рішення
Спільнота та підтримка	Найбільша	Велика	Помірна (активна у .NET середовищі)

WordPress є найбільш популярною CMS у світі, яка завдяки своїй відкритості, простоті інтерфейсу та великій спільноті розробників набула широкого поширення не лише в блогах. Попри те, що WordPress працює на PHP та зазвичай використовується на веб-серверах Apache або Nginx, він також повністю сумісний із Windows-сервером IIS. Наявність великої кількості розширень, зокрема плагінів LDAP-автентифікації, робить WordPress привабливим варіантом для організацій, які потребують швидкого та масштабованого розгортання порталу [8].

Joomla — ще одна відкрита CMS на основі PHP, яка підтримує багаторівневу систему доступу, шаблони, модулі та розширення. На відміну від WordPress, вона спочатку орієнтована на більш складні проєкти з ієрархічною структурою контенту та багатьма користувачами. Joomla має вбудовану підтримку LDAP-автентифікації, яка активується через стандартний плагін, що полегшує її інтеграцію у середовища з централізованою службою каталогів. Також Joomla більш гнучка з точки зору конфігурації, однак потребує більше часу на налаштування [9].

OrchardCore — це сучасна CMS, яка побудована на технології ASP.NET Core і призначена для роботи саме у Windows-середовищі. Вона має модульну архітектуру, розроблену з урахуванням принципів безпеки, продуктивності та масштабованості. OrchardCore підтримує використання Razor Pages, Liquid Templates, API-first структуру та повну інтеграцію з Microsoft Identity, що дозволяє реалізувати складні сценарії автентифікації через LDAP, Azure AD або OAuth2 [10]. На відміну від WordPress і Joomla, OrchardCore орієнтована на розробників і може вимагати програмування для розширення функціоналу.

З огляду на порівняльні характеристики трьох розглянутих CMS, для реалізації веб-порталу в межах цього проєкту було обрано WordPress. Основним аргументом на його користь стала наявність найбільшої екосистеми плагінів, зокрема розширень для LDAP-автентифікації, які дозволяють не лише перевіряти облікові дані користувача, а й автоматично створювати локальні облікові записи на основі записів у Active Directory. Крім того, WordPress відзначається найпростішим процесом налаштування, що дозволяє швидко розгорнути портал без потреби у глибоких технічних знаннях.

На відміну від нього, Joomla має складнішу архітектуру й потребує більше часу на початкову конфігурацію. Хоча в неї і є вбудований модуль LDAP-автентифікації, він не підтримує автоматичне створення користувачів, що суттєво ускладнює інтеграцію з Active Directory у динамічному середовищі. OrchardCore, попри сучасну архітектуру та глибоку інтеграцію з .NET-середовищем, виявився надто складним у налаштуванні і має обмежену кількість доступних модулів, що не дозволяє реалізувати функціонал без значного програмного доопрацювання.

Інтеграція систем управління контентом (CMS) зі службами каталогів за протоколом авторизації дозволяє забезпечити єдину точку автентифікації для користувачів і, відповідно, зменшити кількість облікових записів, які потрібно адмініструвати. Усі облікові дані зберігаються централізовано в каталозі (наприклад, Active Directory або OpenLDAP), а CMS лише виконує перевірку введеного логіна й пароля.

1.4. Системи моніторингу корпоративної мережі

У процесі розгортання інформаційної системи особливу увагу слід приділяти не лише її побудові, а й подальшому моніторингу роботи компонентів, їх доступності, продуктивності та стабільності. Система моніторингу дозволяє виявляти проблеми на ранніх етапах, зменшувати час простою сервісів, контролювати навантаження на сервери, мережеві пристрої та служби, а також забезпечує прозорість роботи всієї мережевої інфраструктури.

У корпоративному середовищі система моніторингу зазвичай повинна охоплювати як серверну частину (контролери домену, файлові сервери, веб-сервери), так і мережеві пристрої (маршрутизатори, комутатори), а також відображати стан служб (DNS, DHCP, LDAP, HTTP тощо). Крім цього, вона має забезпечувати сповіщення про критичні події, можливість збору статистики й побудови графіків навантаження [11].

У межах реалізованого проєкту було обрано систему PRTG Network Monitor, яка відома своєю простотою у впровадженні, гнучким інтерфейсом та широкою функціональністю. Це комерційне рішення, яке розповсюджується німецькою компанією Paessler і дозволяє моніторити практично будь-який аспект IT-інфраструктури. PRTG підтримує велику кількість протоколів і технологій: SNMP, WMI, NetFlow, ICMP, LDAP, HTTP, SSL, SQL-запити, Active Directory тощо. Після встановлення система автоматично сканує мережу, додає відомі пристрої та служби, і починає збір даних у режимі реального часу.

Однією з переваг PRTG є інтуїтивно зрозумілий веб-інтерфейс із можливістю створення дашбордів, налаштування попереджень, перегляду історичних даних,

формування PDF-звітів тощо. Система дозволяє адміністратору визначати порогові значення, за перевищення яких буде надіслане повідомлення поштою або іншим каналом. Важливою особливістю є можливість моніторингу LDAP-автентифікації та взаємодії з Active Directory — що є актуальним у контексті інтеграції з веб-порталом та службами домену [12].

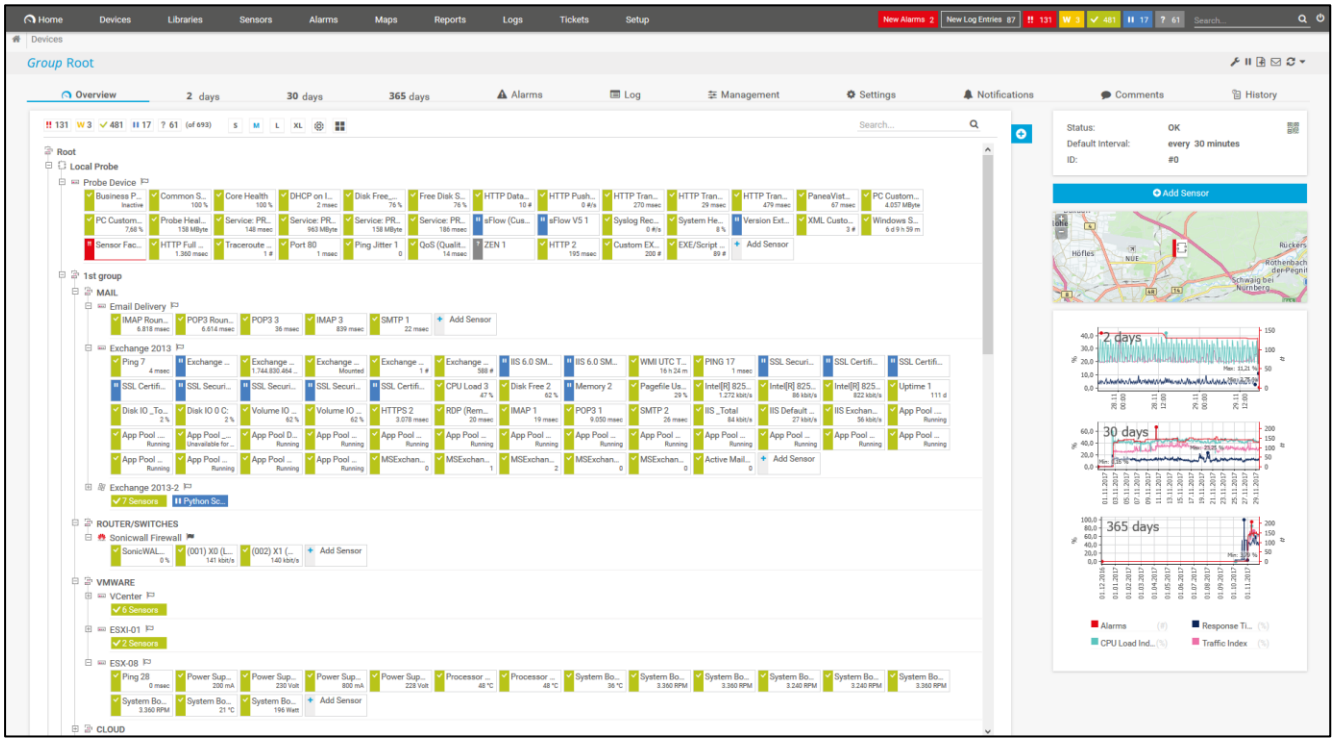


Рисунок 1.4.1 – Деревоподібний вигляд стану пристроїв моніторингу PRTG

Разом із тим, існують інші системи моніторингу, з якими варто порівняти PRTG:

Zabbix

Zabbix — це потужна система моніторингу з відкритим вихідним кодом, що дозволяє відслідковувати стан серверів, мережевих пристроїв, віртуалізації, додатків та сервісів у реальному часі. Zabbix підтримує великий набір протоколів (SNMP, ICMP, JMX, IPMI, HTTPS, SSH) і дозволяє створювати індивідуальні шаблони моніторингу [13].

Система має клієнт-серверну архітектуру: Zabbix Server відповідає за збір даних і генерацію подій, а Zabbix Agent — встановлюється на моніторингових хостах для передачі локальної інформації (завантаження CPU, обсяг оперативної пам’яті,

логів тощо). Також Zabbix дозволяє працювати з агентами без встановлення — через SNMP або IPMI.

Веб-інтерфейс Zabbix є гнучким і дозволяє створювати графіки, карти, тригери та звіти. Є підтримка сценаріїв реагування, наприклад, надсилання email або запуск скрипту при настанні події. Для більш складних середовищ доступні паралельний облік SLA, підтримка HA-кластерів, розширена рольова модель користувачів та централізоване управління.

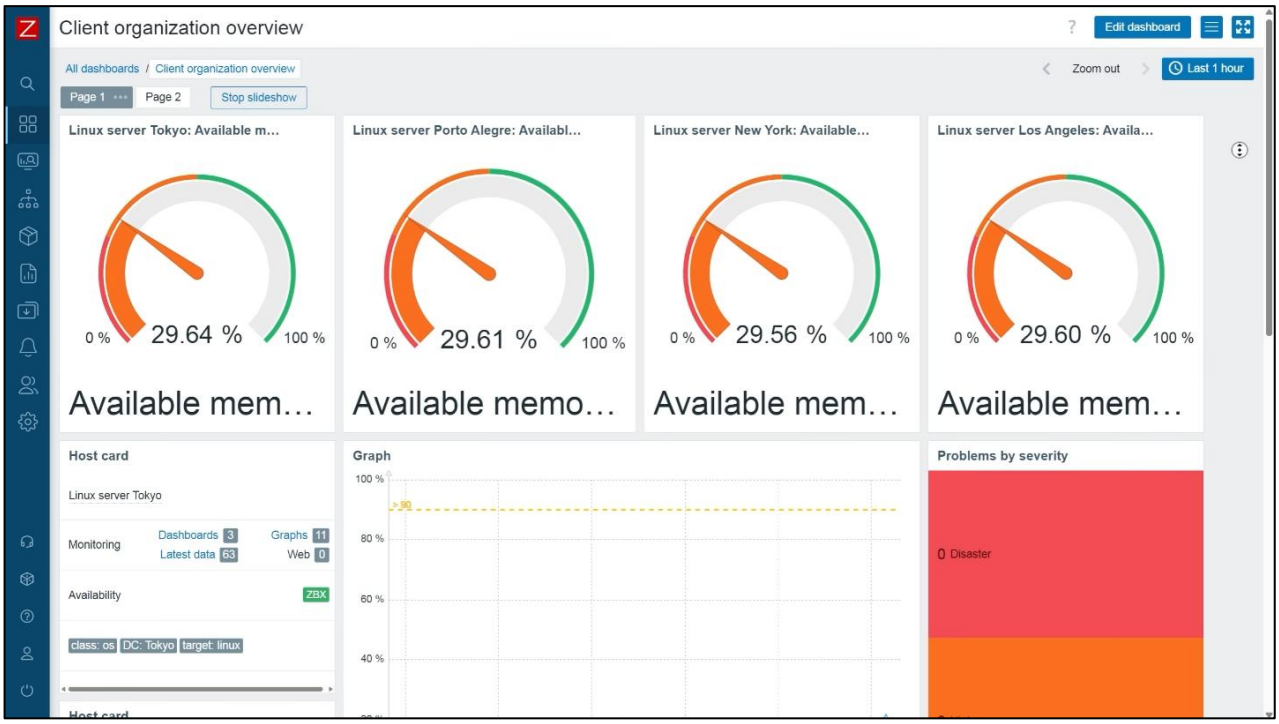


Рисунок 1.4.2 – Дашборд веб-інтерфейсу Zabbix

Недоліком Zabbix є висока складність первинного налаштування та потреба в базових навичках адміністрування Unix-подібних систем, оскільки типовий сервер Zabbix розгортається саме на Linux. Проте для великих, розподілених мереж із високими вимогами до кастомізації — це один із найкращих безкоштовних інструментів.

Nagios Core

Nagios Core — одна з перших систем моніторингу, яка стала стандартом у галузі завдяки своїй стабільності, відкритості та гнучкості. Система має модульну архітектуру, що дозволяє розширювати функціональність через плагіни. Базовий Nagios здатен моніторити сервіси, пристрої та хости шляхом виконання команд або скриптів, які повертають статус об'єкта [14].

Рисунок 1.4.3 – Веб-інтерфейс NagiosCore

Основні переваги Nagios — це велика кількість готових плагінів та активна спільнота. З його допомогою можна перевіряти доступність мережевих вузлів, порти, використання ресурсів, наявність оновлень тощо. За допомогою конфігураційних файлів адміністратор налаштовує сценарії моніторингу, відправлення повідомлень, логіку реагування на збої.

Однак недоліком є відсутність сучасного веб-інтерфейсу в базовій версії, що ускладнює візуалізацію. Саме тому більшість користувачів використовують сторонні розширення: Nagios XI (комерційна версія з GUI), Centreon, Thruk або NConf. Усі ці надбудови полегшують управління, але вимагають додаткових зусиль на налаштування.

Nagios добре підходить для невеликих і середніх проєктів, де потрібна стабільність та прозора логіка перевірок, однак у великих середовищах його конфігурація може стати надто складною.

SolarWinds Network Performance Monitor (NPM)

SolarWinds NPM — це потужне, комерційне рішення, орієнтоване на великі підприємства з високими вимогами до доступності, SLA і розширеної аналітики. Система забезпечує глибокий рівень моніторингу: від базових мережевих перевірок до аналізу трафіку, затримок, утрат пакетів та залежностей між сервісами.

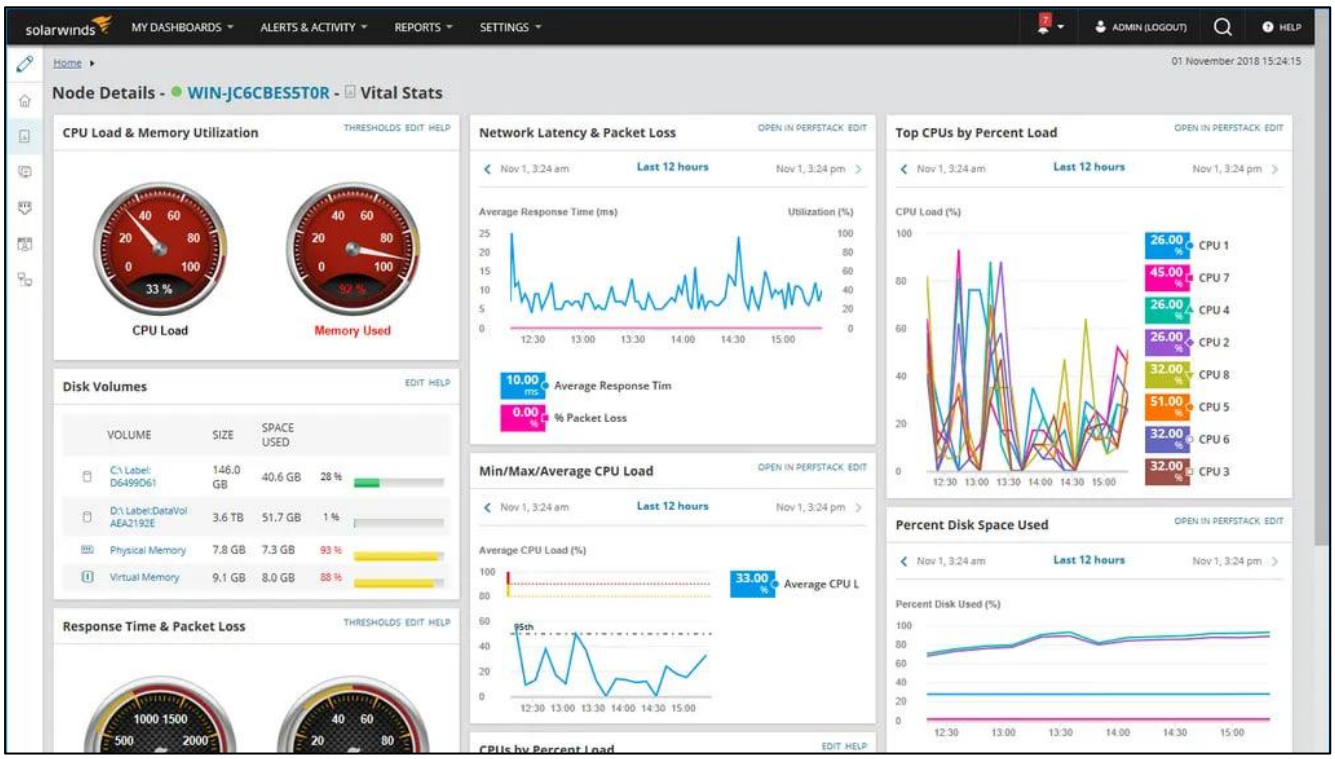


Рисунок 1.4.4 – Дашборд Network Perfomance Monitor

SolarWinds підтримує автоматичне виявлення пристроїв у мережі, побудову топології, графіки продуктивності та повну історію всіх інцидентів. Система орієнтована передусім на інфраструктури з десятками або сотнями вузлів, де потрібна комплексна картина роботи мережі. Особливостями SolarWinds є:

- Підтримка інтеграції з Active Directory;
- Розширене управління ролями;
- Створення SLA-звітів та аналітики;
- Висока масштабованість;
- Глибока інтеграція з іншими модулями SolarWinds (IPAM, NetFlow Analyzer, Server & Application Monitor).

Недоліком цієї системи є висока вартість ліцензування, особливо у великих розгортаннях.

У порівнянні з цими системами, PRTG демонструє найкраще співвідношення функціональності, простоти розгортання та підтримки Windows-інфраструктури. Особливо важливо, що вона не потребує окремих Linux-серверів або глибокого знання командного рядка, що робить її зручною для використання в середовищі, орієнтованому на служби Active Directory. Крім того, в умовах навчального проєкту

або середніх організацій PRTG можна використовувати у безкоштовній версії з обмеженням до 100 сенсорів, чого зазвичай цілком достатньо.

Висновки до першого розділу

У першому розділі було розглянуто теоретичні засади побудови корпоративної інформаційної системи з централізованим керуванням доступом. Було проаналізовано структуру доменної інфраструктури на основі служби Active Directory Domain Services, яка забезпечує ієрархічне зберігання даних про об'єкти мережі, їх автентифікацію, авторизацію та централізоване адміністрування. Особливу увагу приділено ключовим компонентам AD DS — лісу, доменам, організаційним одиницям, контролерам домену, а також механізмам реплікації, пошуку та керування доступом за допомогою групових політик (GPO).

Розглянуто принципи роботи протоколу LDAP, що використовується для забезпечення автентифікації користувачів у службі каталогів. Його підтримка в зовнішніх інформаційних системах, зокрема веб-порталах, дозволяє уніфікувати керування обліковими записами та уникнути дублювання даних, що значно підвищує рівень безпеки та спрощує адміністрування.

У межах побудови веб-порталу в корпоративному середовищі проведено огляд і порівняння найбільш поширених систем управління контентом (CMS): WordPress, Joomla та OrchardCore. За результатами аналізу було обґрунтовано вибір WordPress як найбільш оптимального рішення для реалізації проєкту — з огляду на простоту встановлення, підтримку LDAP-автентифікації та широку екосистему розширень.

Також було розглянуто питання моніторингу інфраструктури корпоративної мережі. Проаналізовано можливості систем PRTG Network Monitor, Zabbix, Nagios Core та SolarWinds NPM. Серед них для реалізації обрано PRTG як систему, що поєднує простоту впровадження, підтримку всіх ключових мережевих протоколів, зручний графічний інтерфейс і тісну інтеграцію з Windows-середовищем. Моніторинг дозволяє виявляти потенційні збої в роботі доменної інфраструктури, веб-порталу та служб безпеки, що є важливою складовою підтримки стабільності та надійності системи.

РОЗДІЛ 2. ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА СТРУКТУРИ ДОМЕНУ

2.1. Загальна концепція, логіка роботи та взаємодія компонентів системи

Інформаційна система, що розробляється, призначена для побудови корпоративного веб-порталу з підтримкою централізованої автентифікації користувачів на основі служби каталогів. Її структура передбачає поєднання публічно доступних інформаційних ресурсів із внутрішніми розділами з обмеженим доступом, призначеними для авторизованих користувачів. Таким чином, система виконує роль інтерфейсу між корпоративною мережею та зовнішнім або частково відкритим інтернет-середовищем.

Проєктована система побудована за принципом централізованого керування доступом, у якому служба каталогів (LDAP/Active Directory) виступає єдиним джерелом автентифікації. Облікові записи користувачів, правила доступу, ролі та групи зберігаються в каталозі, а веб-портал лише виконує перевірку автентичності під час входу. Такий підхід дозволяє зменшити кількість точок керування безпекою, мінімізувати дублювання облікових записів та підвищити загальний рівень захисту даних.

Система реалізується в умовах ізольованого віртуального середовища на базі VirtualBox, що дає змогу змоделювати мережу з контролером домену, веб-сервером та робочими станціями. Центральною частиною є домен uniwork.net, у межах якого створено користувачів, організаційні одиниці (OU), групові політики та інші елементи інфраструктури.

З точки зору інформаційної архітектури, до складу системи входять такі компоненти:

- Сервер контролера домену з роллю AD DS, який зберігає каталог облікових записів;
- Веб-сервер із CMS WordPress, що працює під керуванням IIS;
- LDAP-інтерфейс між CMS і AD, реалізований за допомогою плагіна;
- Система моніторингу PRTG, яка контролює стан усіх ключових служб.

Взаємодія CMS із LDAP-службою

Одним із ключових технічних рішень у проєкті є інтеграція веб-порталу WordPress із LDAP-службою, що реалізована через плагін miniOrange LDAP Login. Після встановлення плагіна адміністратор налаштовує підключення до серверу каталогу, вказуючи адресу, порт, DN бази пошуку, дані привілейованого користувача (bind-user), та правила пошуку користувача (наприклад, за атрибутом sAMAccountName).

Під час спроби входу користувача до системи, CMS передає введені логін і пароль на LDAP-сервер. Якщо облікові дані відповідають запису в каталозі, користувач автоматично отримує доступ до внутрішніх сторінок сайту. У випадку, якщо локального запису WordPress ще не існує, плагін автоматично створює його на основі даних з LDAP. Такий механізм забезпечує не лише автентифікацію, а й синхронізацію користувачів між системами.

Окремі розділи сайту можуть бути обмежені для неавторизованих користувачів. Це реалізується за допомогою CMS або розширень, які перевіряють стан сесії WordPress та ролі, призначені на основі груп користувача в LDAP. Таким чином, можна реалізувати градацію доступу, наприклад: студенти, співробітники, адміністратори.

Типові сценарії використання системи

Сценарій 1: Вхід користувача до веб-порталу. Користувач відкриває веб-сайт і натискає кнопку "Увійти". Вводить свій доменний логін і пароль. CMS виконує bind-запит до LDAP-серверу. У разі успішної автентифікації, користувач перенаправляється до внутрішньої сторінки з персоналізованим контентом.

Сценарій 2: Обмеження доступу до розділу. Користувач переходить за прямим посиланням на сторінку моніторингу (/monitoring). Система перевіряє статус автентифікації. Якщо користувач не увійшов — його перенаправляють на форму входу. Якщо він автентифікований, але не входить до потрібної LDAP-групи, відображається повідомлення "Доступ заборонено".

Сценарій 3: Автоматичне створення облікового запису. Новий працівник організації вперше входить на сайт за допомогою свого логіна AD. Плагін автоматично створює локального користувача WordPress, призначає роль (наприклад, "працівник") та дозволяє доступ до внутрішнього порталу.

Переваги інтегрованого підходу

Інтеграція CMS з LDAP-службою надає одразу кілька стратегічних переваг:

-єдина точка керування обліковими записами – усі логіни й паролі зберігаються централізовано.

-підвищена безпека – завдяки уніфікації автентифікації й обмеженню доступу.

-спрощене адміністрування – не потрібно створювати окремі акаунти у CMS.

-масштабованість – можна легко адаптувати під більшу кількість користувачів або інші сервіси.

2.2. Логічна модель доменної інфраструктури

Доменна структура в проєктованій системі побудована відповідно до моделі централізованого управління користувачами й ресурсами. Логічна модель базується на домені uniwork.net, у межах якого реалізовано ієрархічну систему організаційних одиниць (OU) та облікових записів користувачів.

Кожна OU відповідає певному підрозділу чи групі користувачів. Наприклад, OU-1, OU-2, OU-3 — це логічні області, які містять групи та користувачів відповідних відділів (dep1-admin, dep2-gcs, dep3-alo тощо). Така структура дозволяє застосовувати групові політики (GPO) диференційовано, залежно від ролі користувача в організації.

Користувачі організовані відповідно до функціональних ролей — адміністративний персонал (depX-admin), спеціалісти (depX-ckl, depX-gcs) тощо.

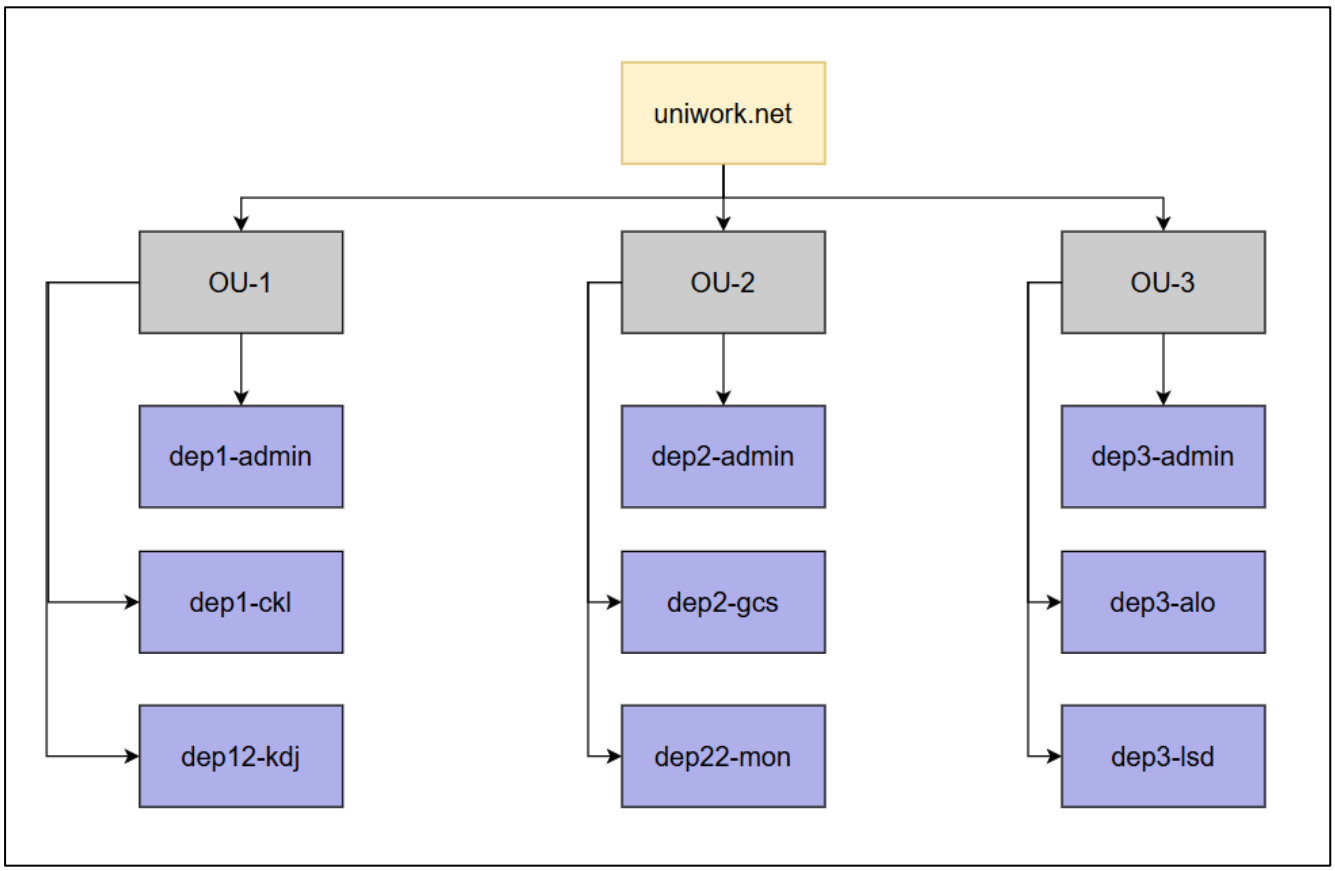


Рисунок 2.2.1 – Ієрархічна модель OU та груп у домені uniwork.net

Така структура забезпечує масштабованість, зручність адміністрування та повну підтримку механізмів групових політик на рівні користувача або OU.

2.3. Вибір обладнання та програмного забезпечення

Для реалізації порталу було обрано веб-стек на основі CMS WordPress, що працює під керуванням IIS на платформі Windows Server, з використанням PHP і MySQL. Такий вибір зумовлений високою сумісністю WordPress із розширеннями LDAP, зручністю адміністрування, активною спільнотою підтримки та простотою інтеграції з інфраструктурою Windows. Використання IIS забезпечує прямий зв’язок із службами Active Directory, а розгортання на Windows Server спрощує конфігурування безпеки, мережевих політик та моніторингу системи.

Для практичної побудови проекту використано гіпервізор Oracle VirtualBox версії 7.1.8.

На Server-1 встановлено операційну систему Windows Server 2019 Standard (Desktop Experience) з 64-бітною розрядністю. Виділено 6 процесорних ядер, 4 ГБ оперативної пам’яті та 50 ГБ постійної.

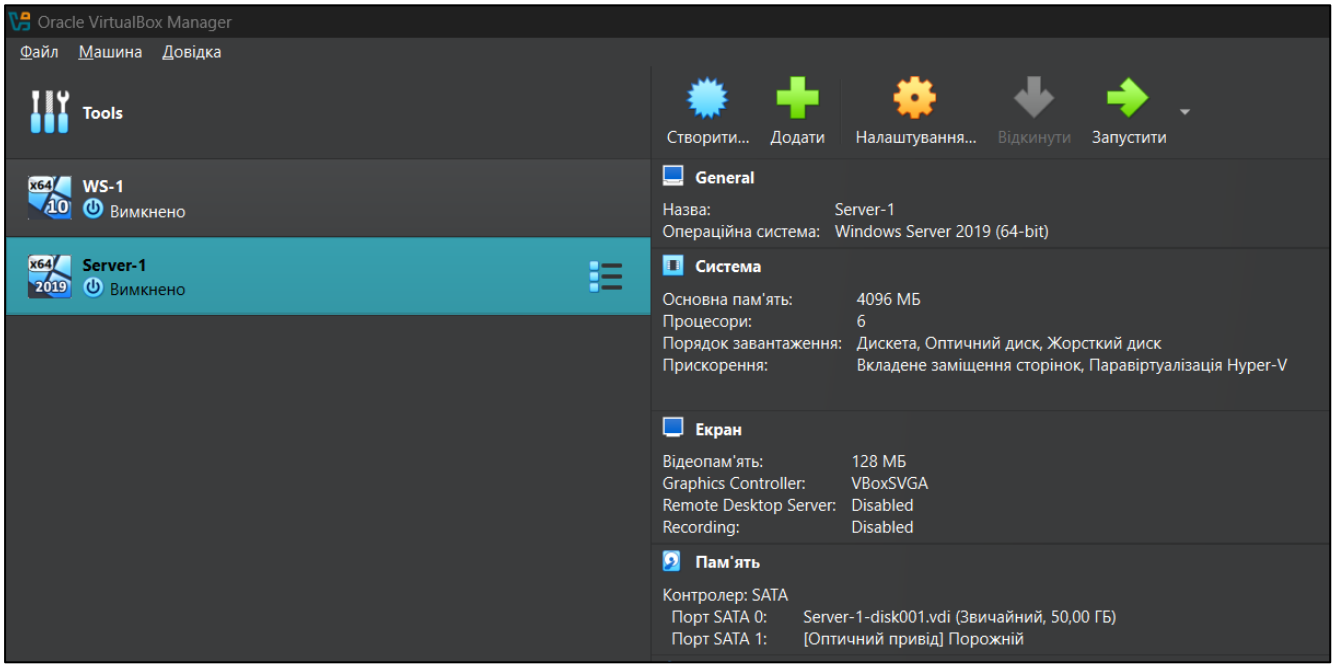


Рисунок 2.3.1 – Фізичні ресурси виділені для Server-1

На віртуальну машину WS-1, яка виконує роль робочої станції, встановлено 64-бітну версію Windows 10. Для робочих станцій виділено 3 процесорних ядра, 3 ГБ оперативної та 40 ГБ постійної пам’яті.

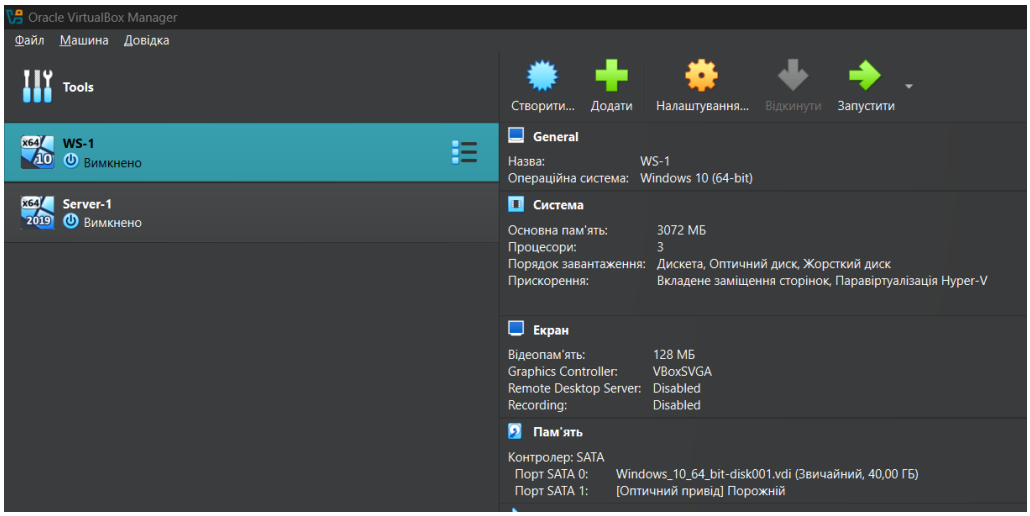


Рисунок 2.3.2 – Фізичні ресурси виділені для WS-1

2.4. Адресна схема і топологія мережі

Мережа, у межах якої реалізовано систему, має просту модель з єдиною підмережею IPv4 з використанням підмережі 192.168.1.0/24. Усі пристрої підключені до одного комутатора (SW-1) та зв’язані через маршрутизатор (R-1), який виконує роль шлюзу за замовчуванням. Сервер домену має статичну IP-адресу, а клієнтська станція отримує адресу динамічно через службу DHCP.

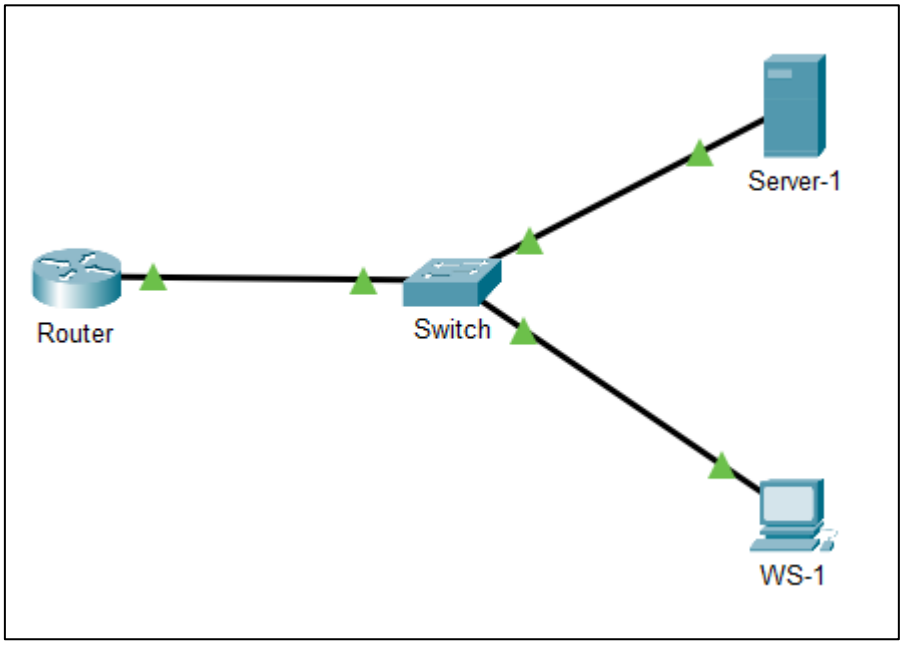


Рисунок 2.4.1 – Спроектована топологія мережі

Таблиця 2.1 – Схема IP-адресації в мережі

Пристрій	Інтерфейс	Шлюз	IP-адреса
Мережа	-	-	192.168.1.0/24
R-1	Fa0/0	-	192.168.1.1
SW-1	VLAN 1	192.168.1.1	192.168.1.2
Serv-1 (Windows)	NIC	192.168.1.1	192.168.1.3
WS-1	NIC	192.168.1.1	DHCP

Щоб надати пристроям доступ до Інтернету, було створено й налаштовано мережу NAT відповідно до обраної адресації.

Рисунок 2.4.2 – Мережа NAT

Висновки до другого розділу

У межах другого розділу було здійснено проєктування корпоративної інформаційної системи, що поєднує функції публічного веб-порталу з централізованим

керуванням автентифікацією користувачів. Визначено загальну концепцію системи, згідно з якою основними її компонентами є доменна служба каталогу, система керування контентом (CMS), а також система моніторингу.

Побудовано логічну структуру домену uniwork.net, що охоплює ієрархічну систему організаційних одиниць (OU), облікові записи користувачів і групи безпеки. Така структура забезпечує масштабованість, централізоване управління доступом, а також можливість реалізації гнучких групових політик на основі ролей користувачів.

Розроблено топологію мережі з урахуванням принципів ізоляції й логічного поділу на компоненти — маршрутизатор, комутатор, контролер домену та робоча станція. Для забезпечення зручного і безпечного тестування всі елементи інфраструктури розгорнуто у віртуальному середовищі VirtualBox.

Обґрунтовано вибір програмного забезпечення: Windows Server 2019 для розгортання служби Active Directory, WordPress як базової CMS, плагіна LDAP Login для інтеграції з каталогом користувачів, а також системи моніторингу PRTG Network Monitor для нагляду за станом мережі та серверів. Враховано ресурси віртуальних машин, їхні функціональні ролі та вимоги до взаємодії.

Інтеграція CMS з LDAP реалізована на рівні логіки системи, а також змодельовано типові сценарії взаємодії користувачів із порталом. Це забезпечує єдину точку входу, спрощене адміністрування та чіткий контроль над доступом до внутрішніх ресурсів.

РОЗДІЛ 3. НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ПРОЕКТУ

3.1. Налаштування доменних служб Active Directory

Для початку необхідно налаштувати IP-адресацію та імена хостів пристроїв.

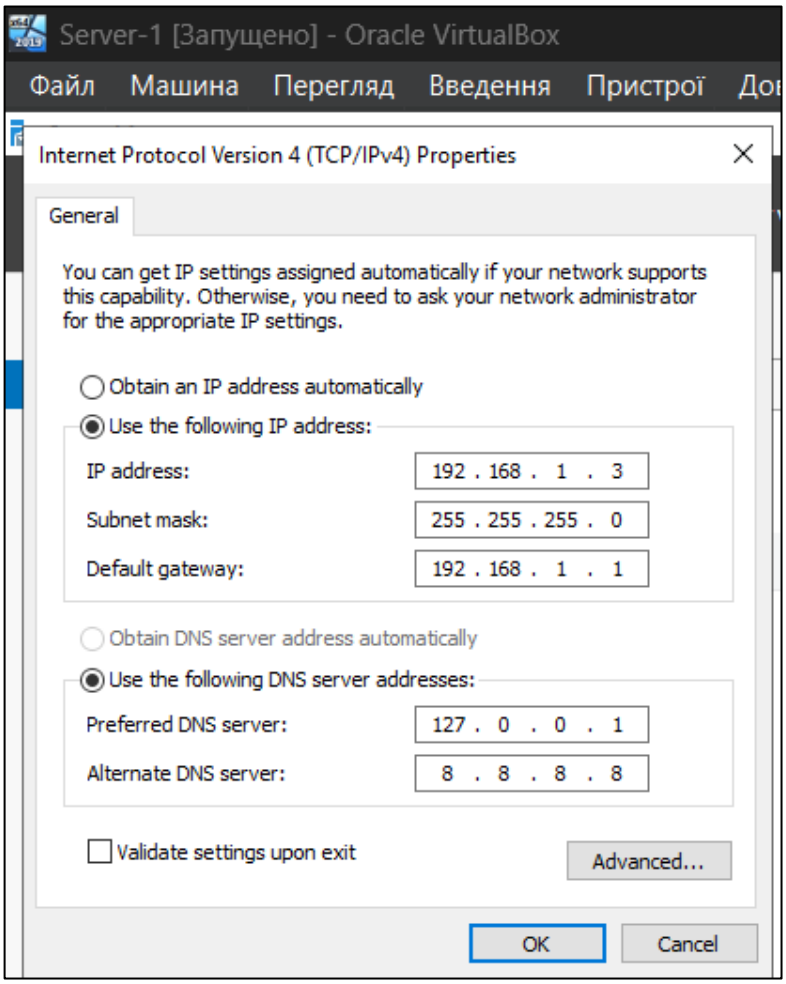


Рисунок 3.1.1 – Налаштування IP-адресації Server-1

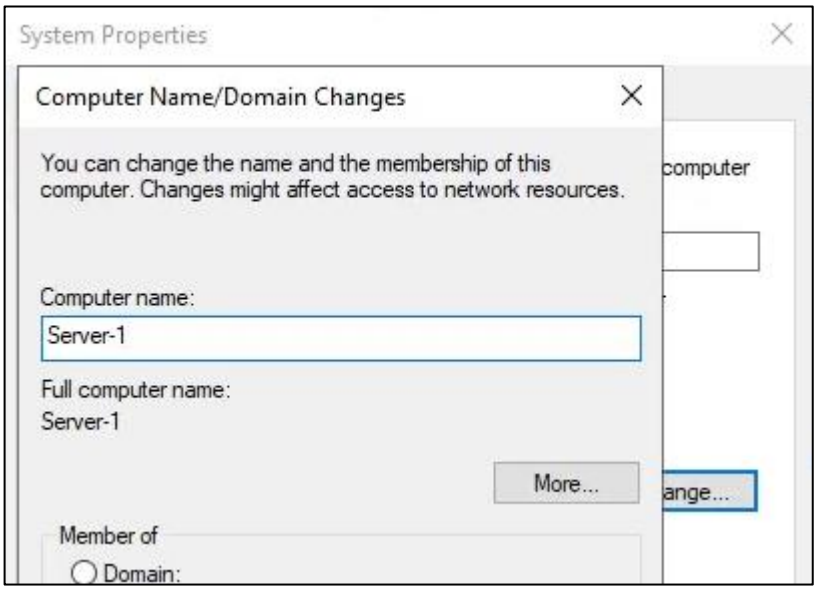


Рисунок 3.1.2 – Зміна хостнейму Server-1

Встановлюємо необхідні ролі для сервера:

- Active Directory Domain Services
- DHCP Server та DNS Server
- Web Server

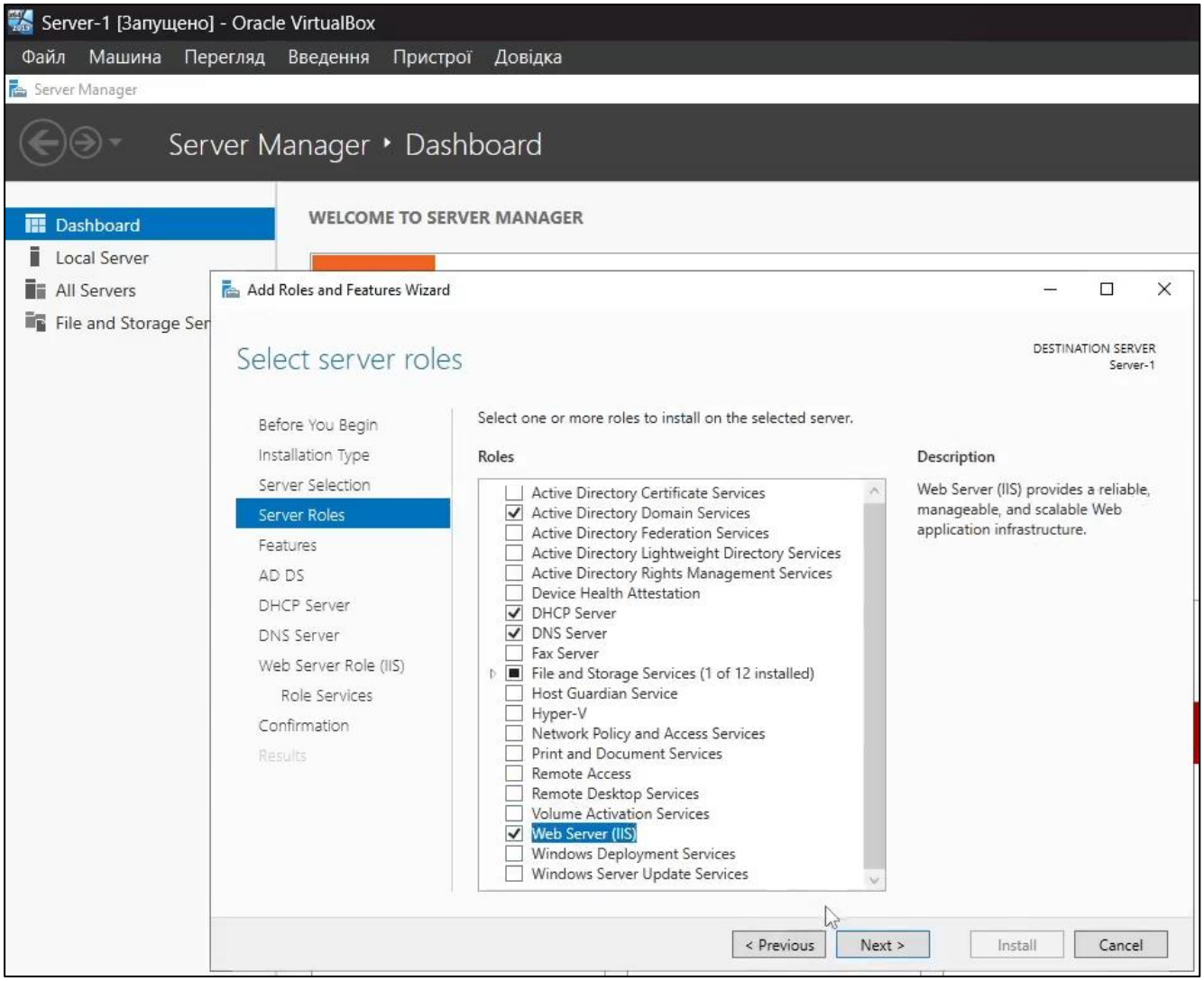


Рисунок 3.1.3 – Встановлення необхідних служб

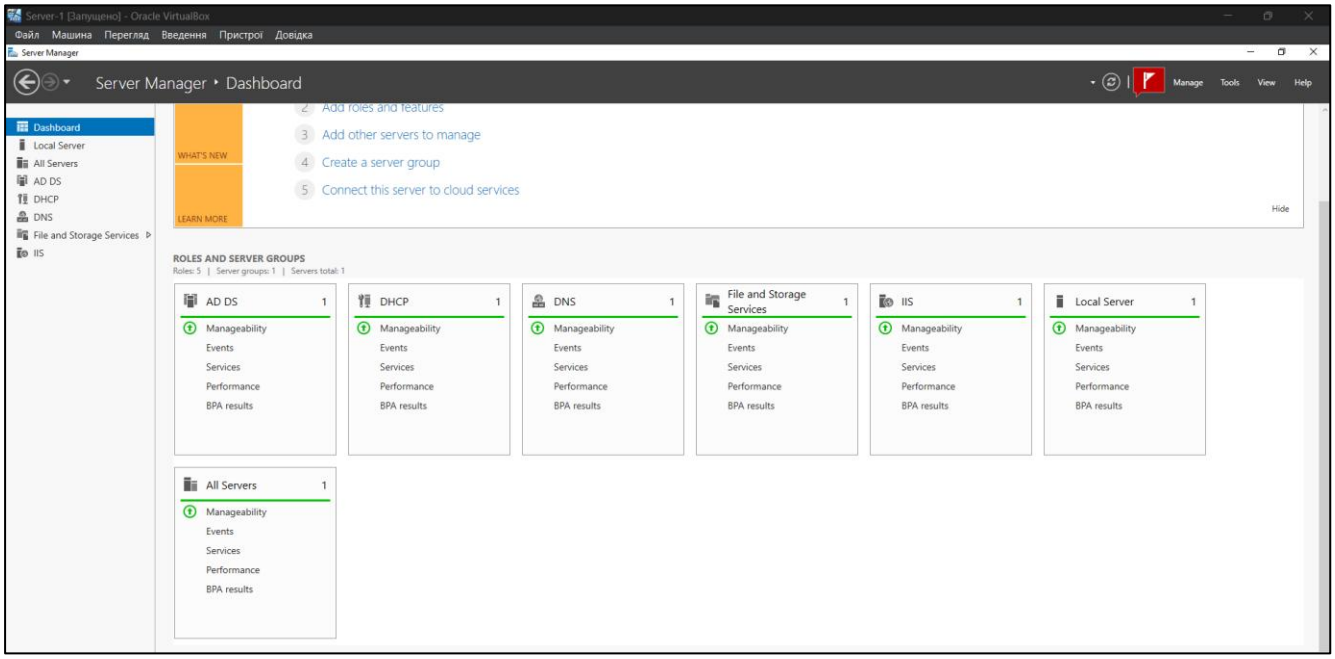


Рисунок 3.1.4 – Дашборд із встановленими ролями на сервері

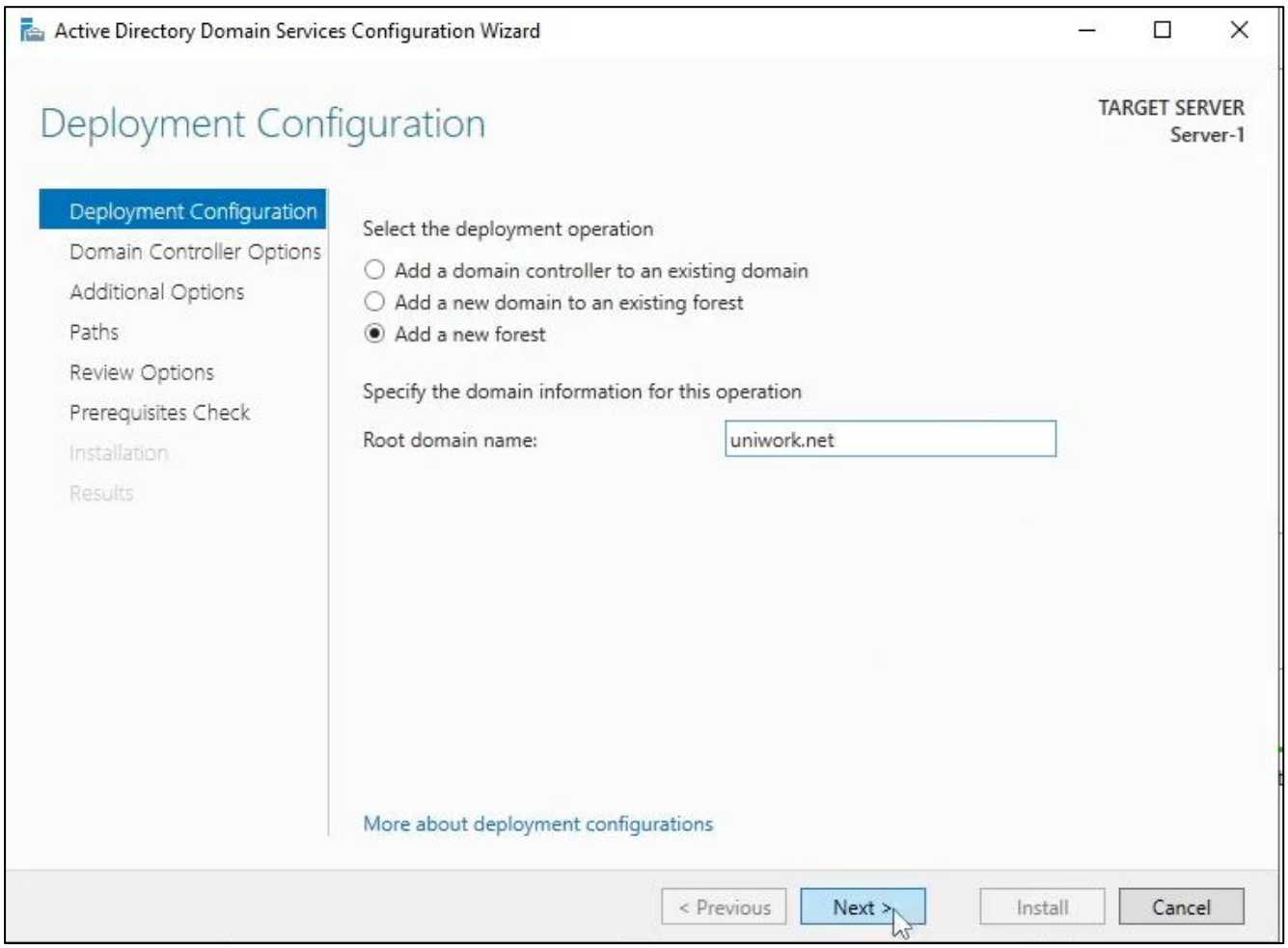


Рисунок 3.1.5 – Створення і конфігурація домену

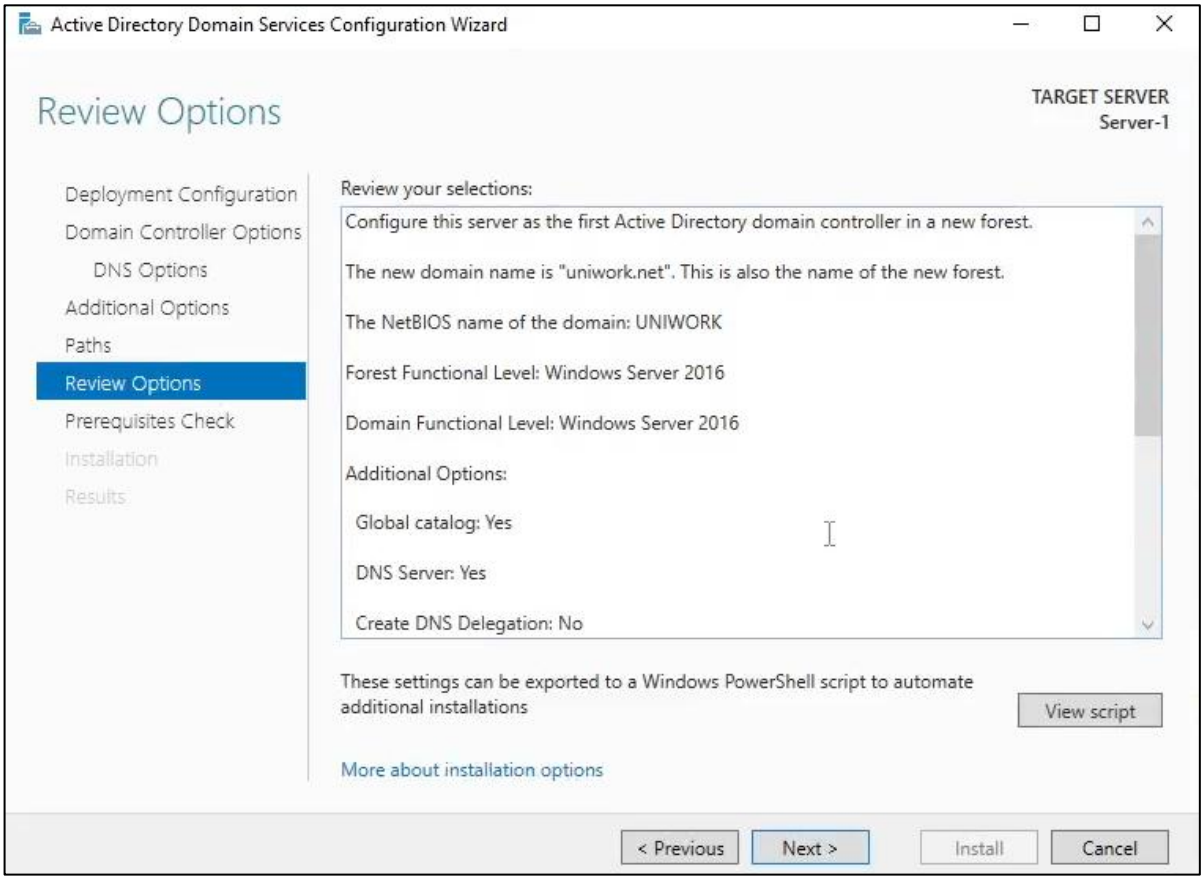


Рисунок 3.1.6 – Обрані параметри конфігурації

Вхід у ролі адміністратора домену здійснюється під повним доменним іменем UNWORK\Administrator. Цей користувач має повний контроль над доменною інфраструктурою і логікою роботи.

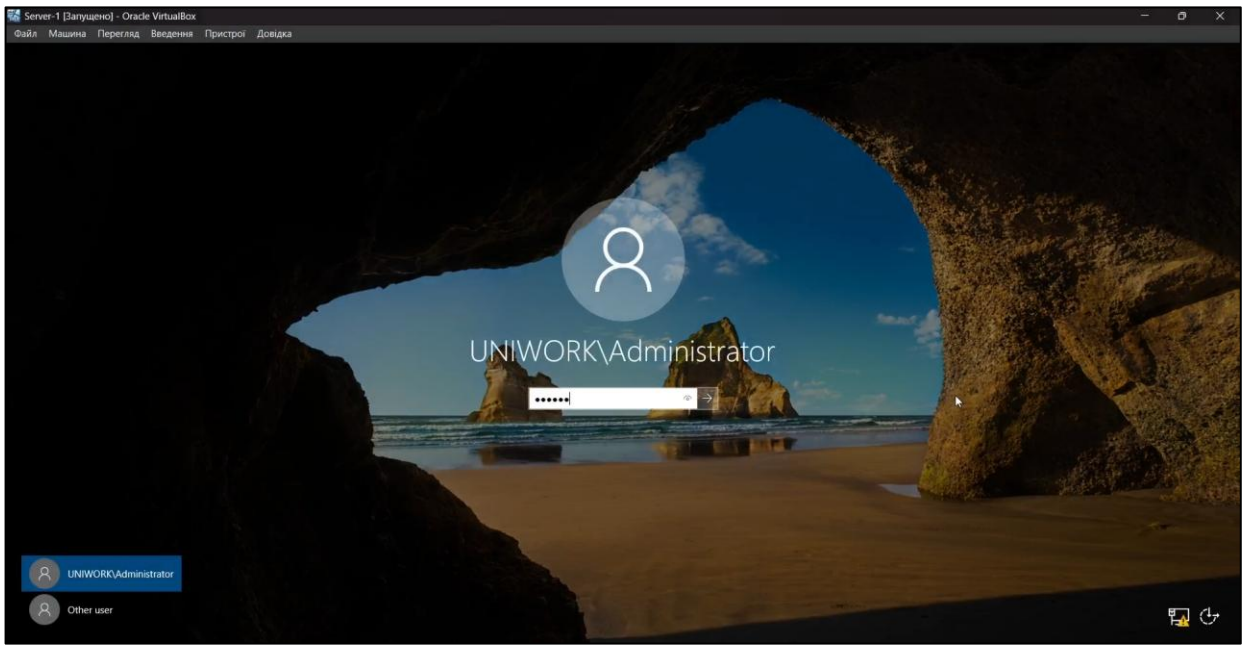


Рисунок 3.1.7 – Авторизація на Server-1

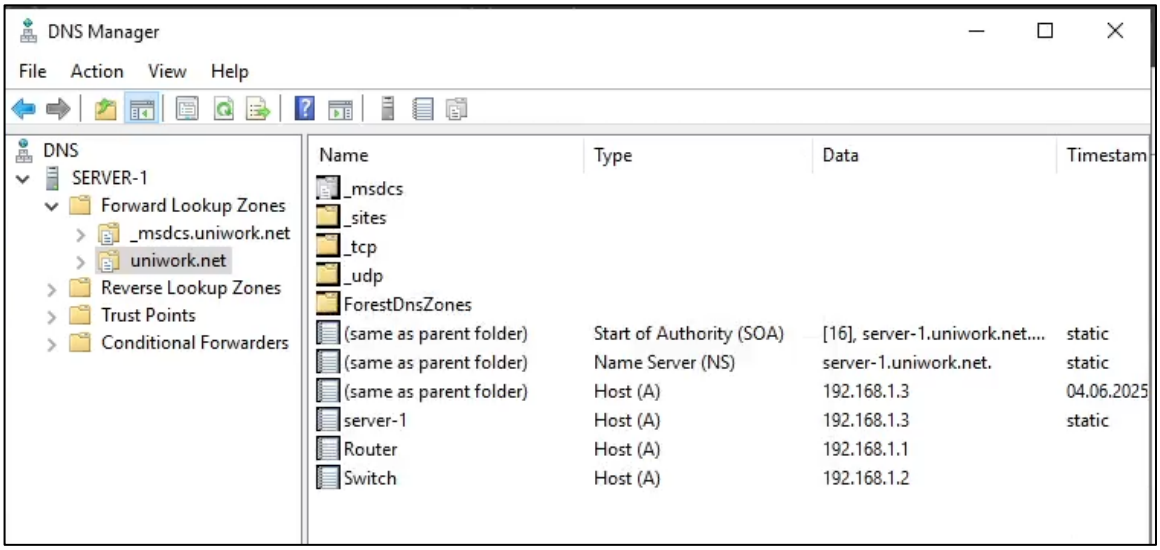


Рисунок 3.1.8 – Зона прямого перегляду DNS домену

Для того, щоб робочі станції автоматично отримували IP-адреси, налаштовуємо DHCP

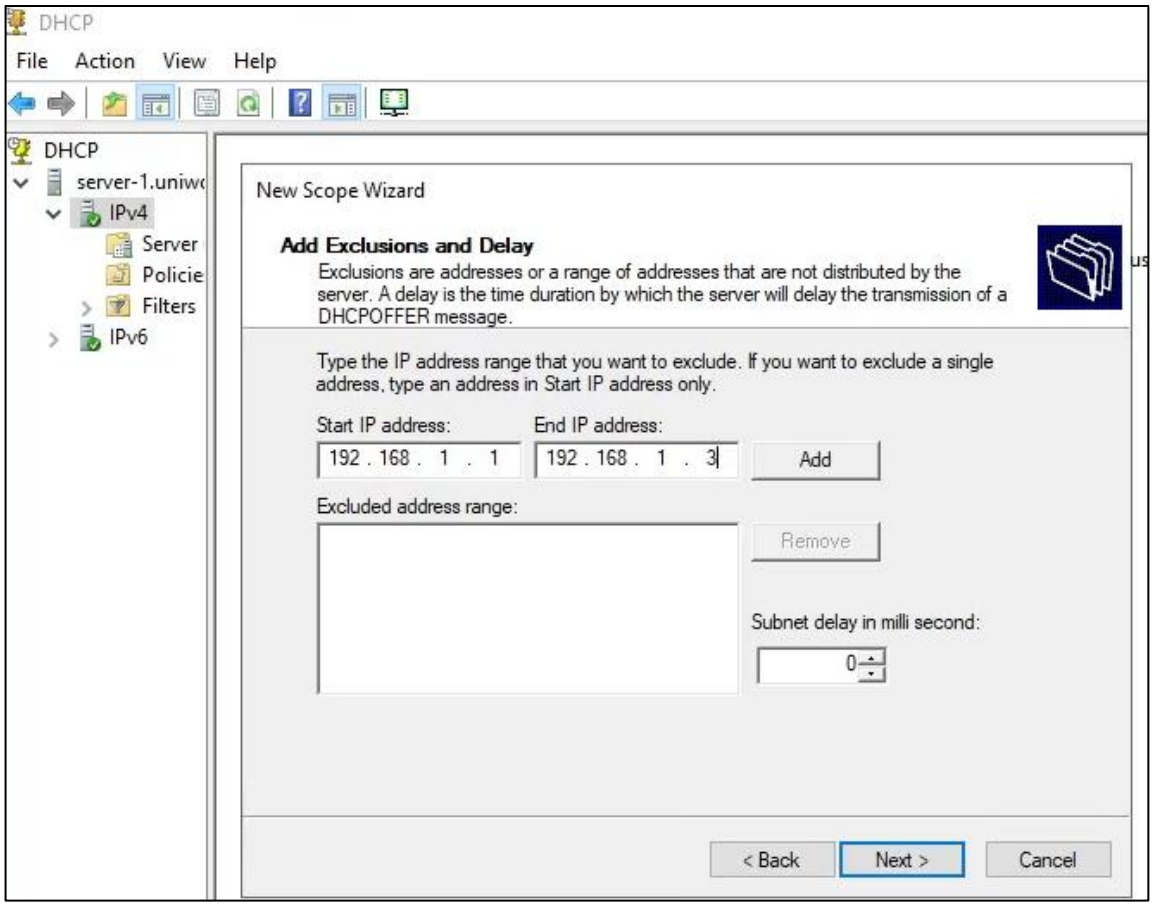


Рисунок 3.1.9 – Діапазон адрес DHCP

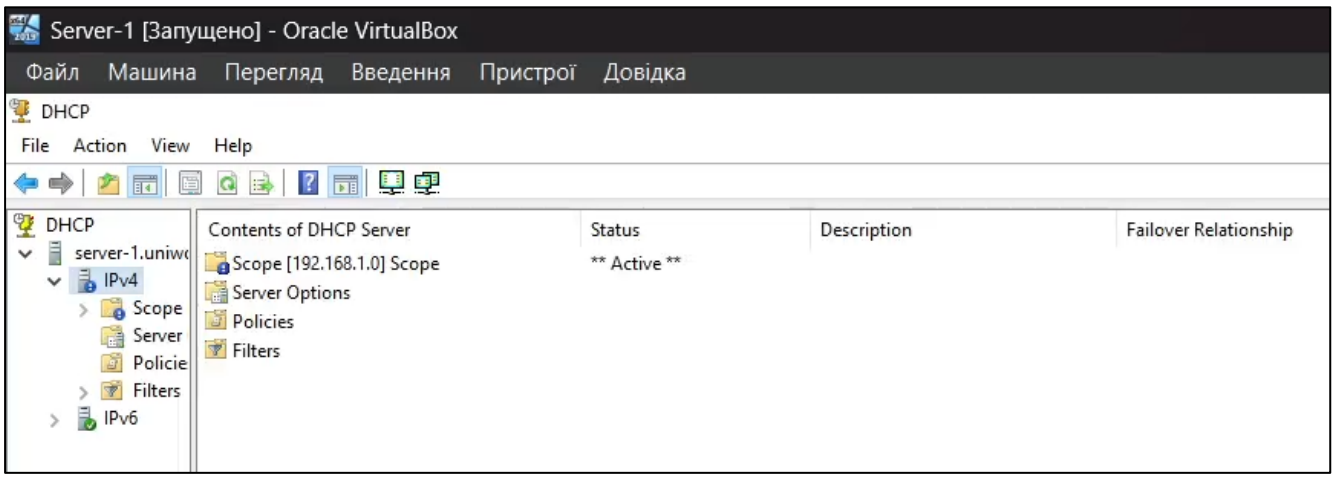


Рисунок 3.1.10 – Створений DHCP пул

Для ефективного управління й розподілу користувачів використовуємо організаційні одиниці. Відповідно до структури домену uniwork.net, в них створюємо користувачів.

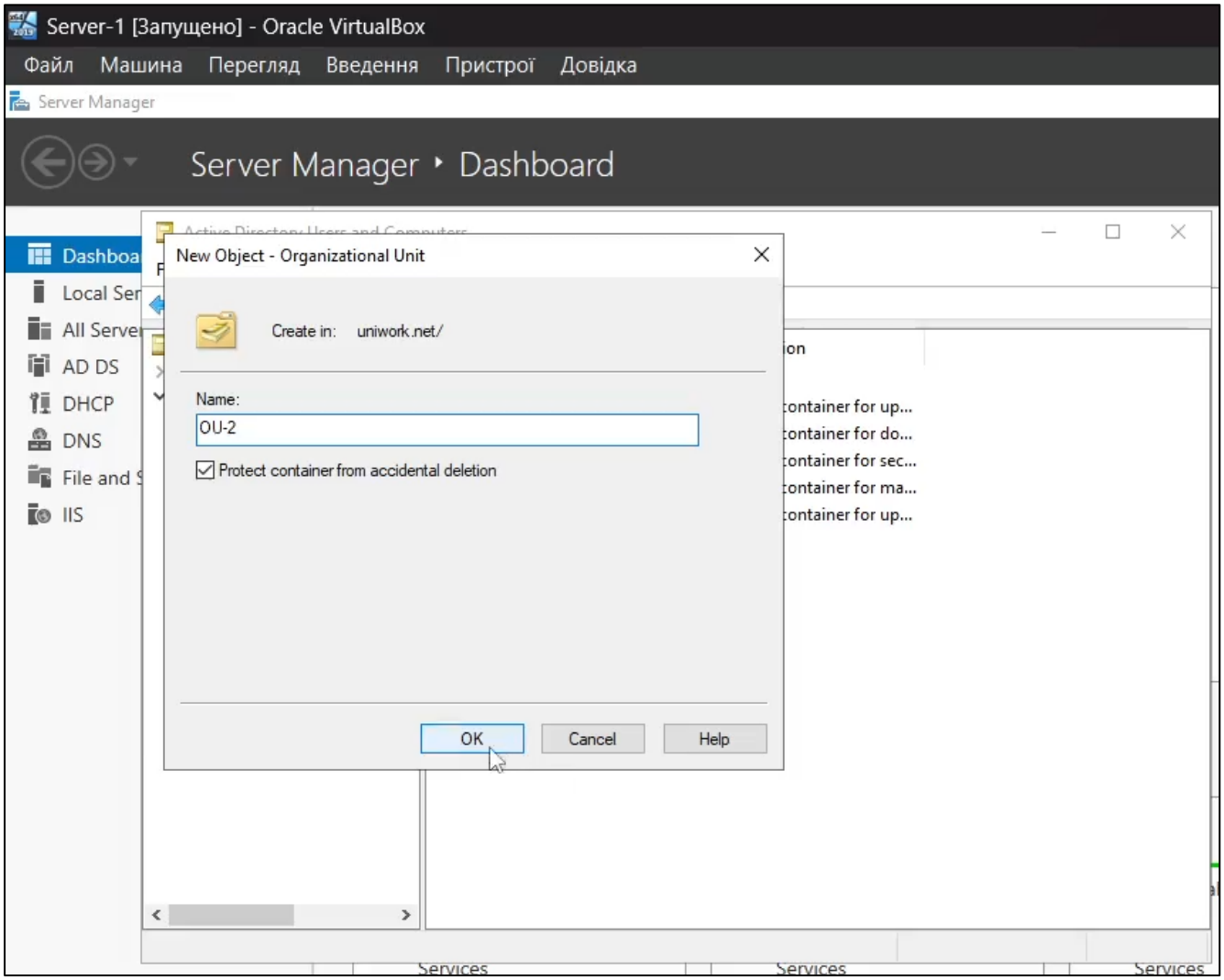


Рисунок 3.1.11 – Створення організаційної одиниці OU-2

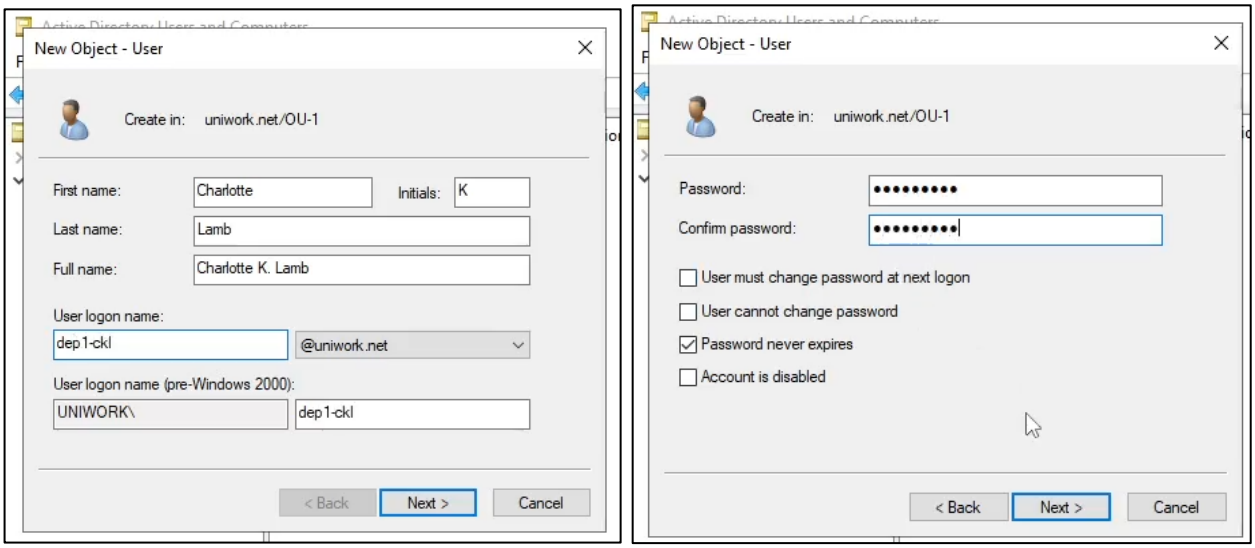


Рисунок 3.1.12 – Створення користувача

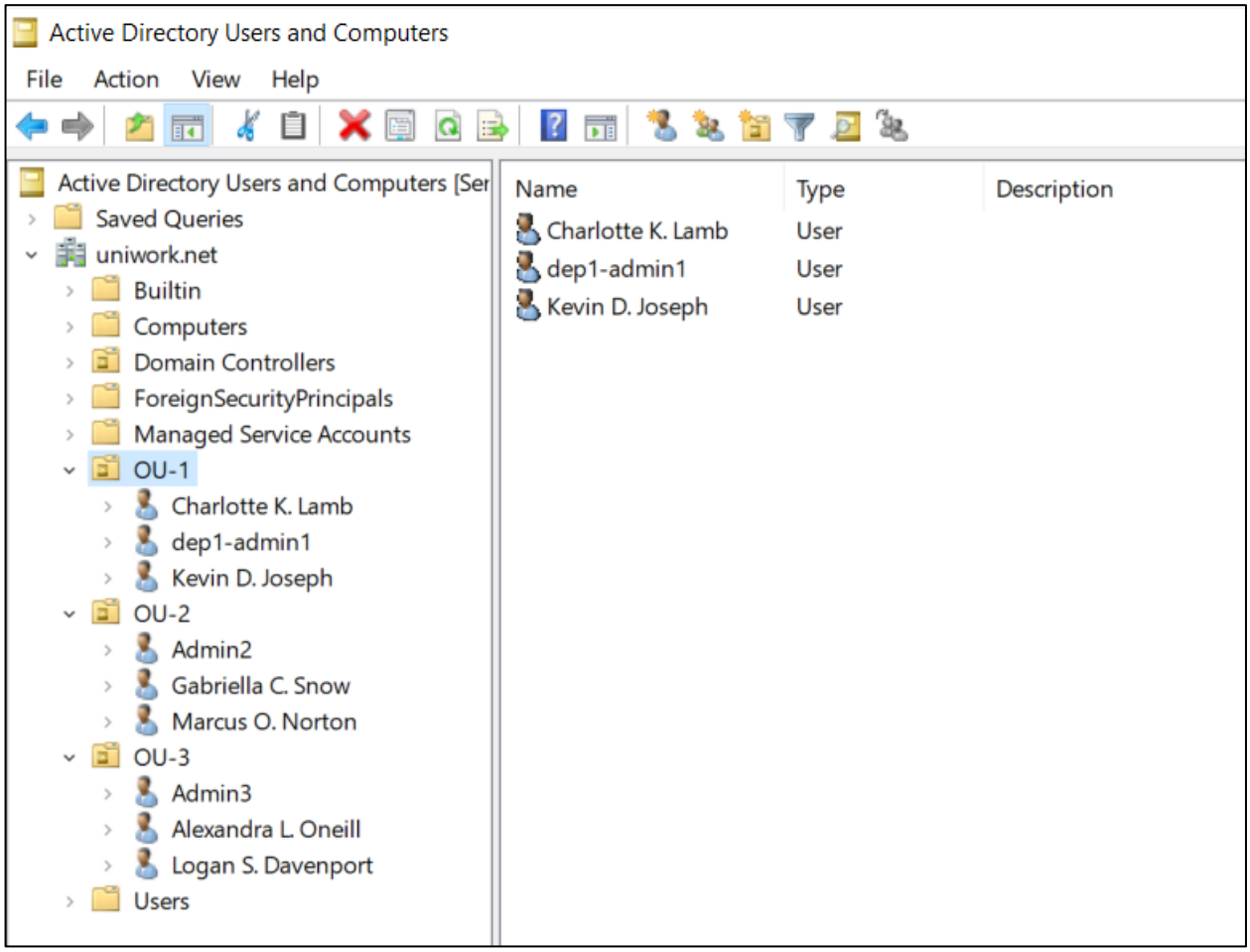


Рисунок 3.1.13 – Створена структура домену і користувачів

3.2. Встановлення системи моніторингу мережі

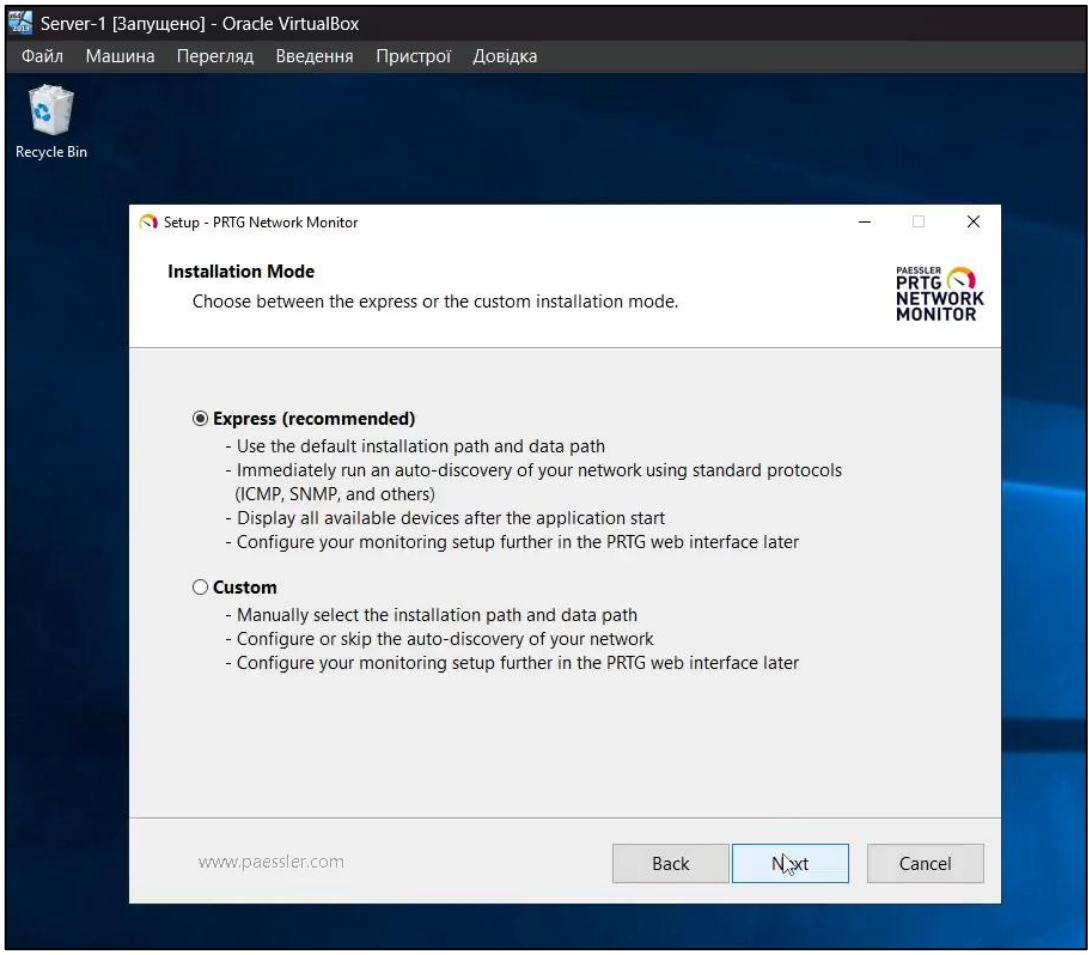


Рисунок 3.2.1 – Процес інсталяції PRTG

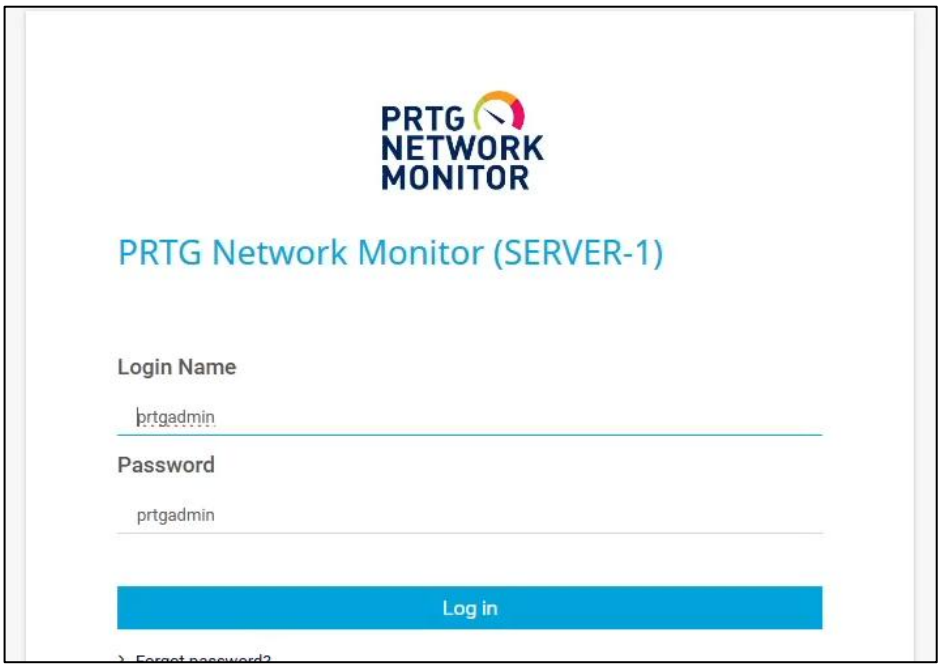


Рисунок 3.2.2 – Авторизація до веб-інтерфейсу PRTG Network Monitor

Меню веб-інтерфейсу надає доступ до всіх інструментів, які надає моніторингова служба. На головній сторінці зведено інформацію про всі сенсори й поточні критичні проблеми. Залежно від рівня важливості вони позначені різними кольорами, наприклад зелений – добре, а червоний – несправність.

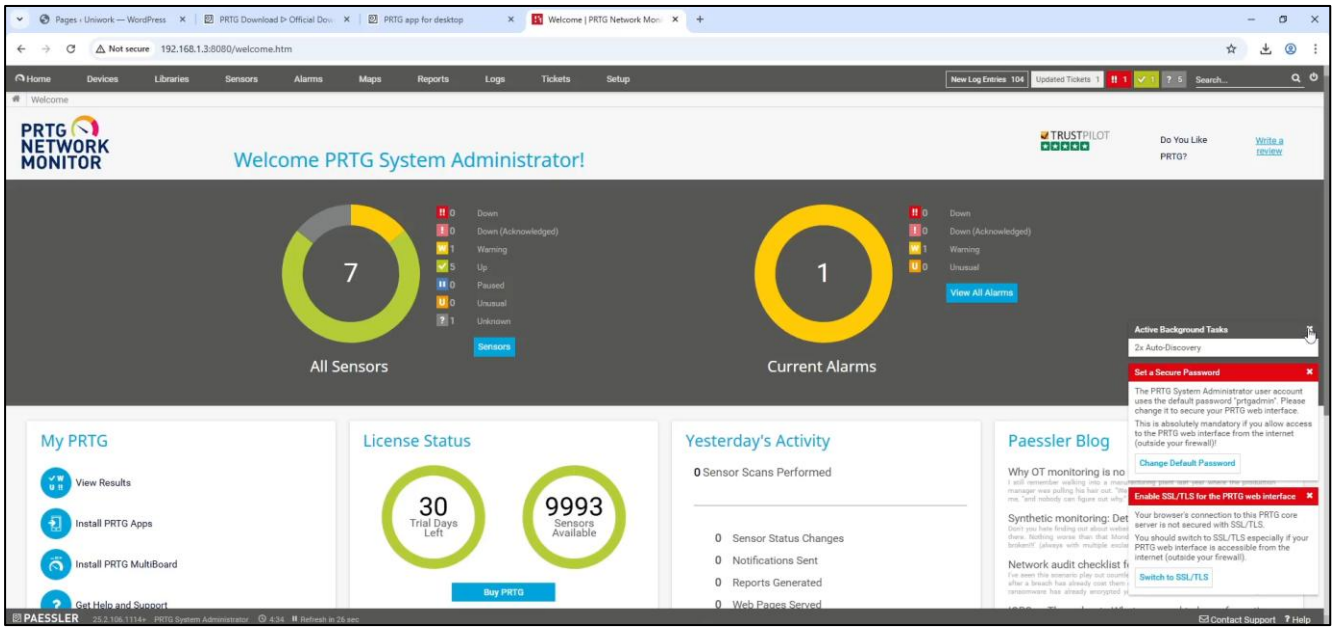


Рисунок 3.2.3 – Головна сторінка системи моніторингу

Для роботи необхідно додати пристрої, стан яких потребує моніторингу. Для пристрою додаються сенсори, які відповідають певним метрикам. Для ручного додавання пристрою ми вказуємо його ім’я та адресу для ідентифікації.

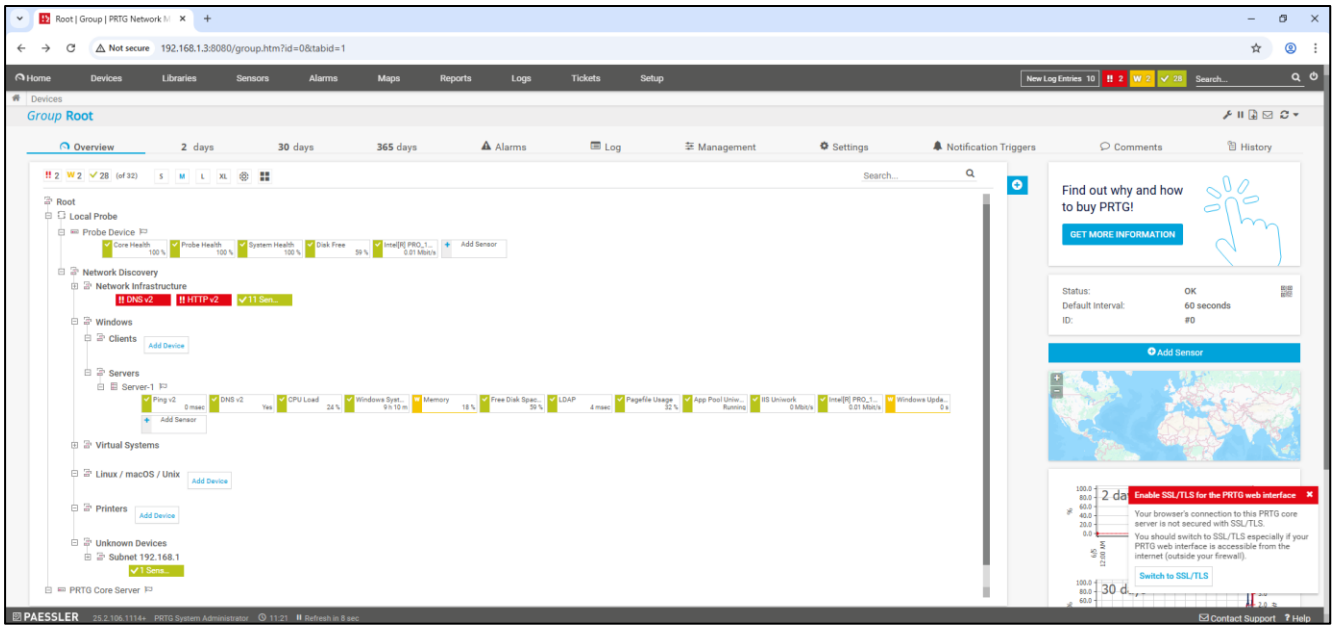


Рисунок 3.2.4 – Меню пристроїв

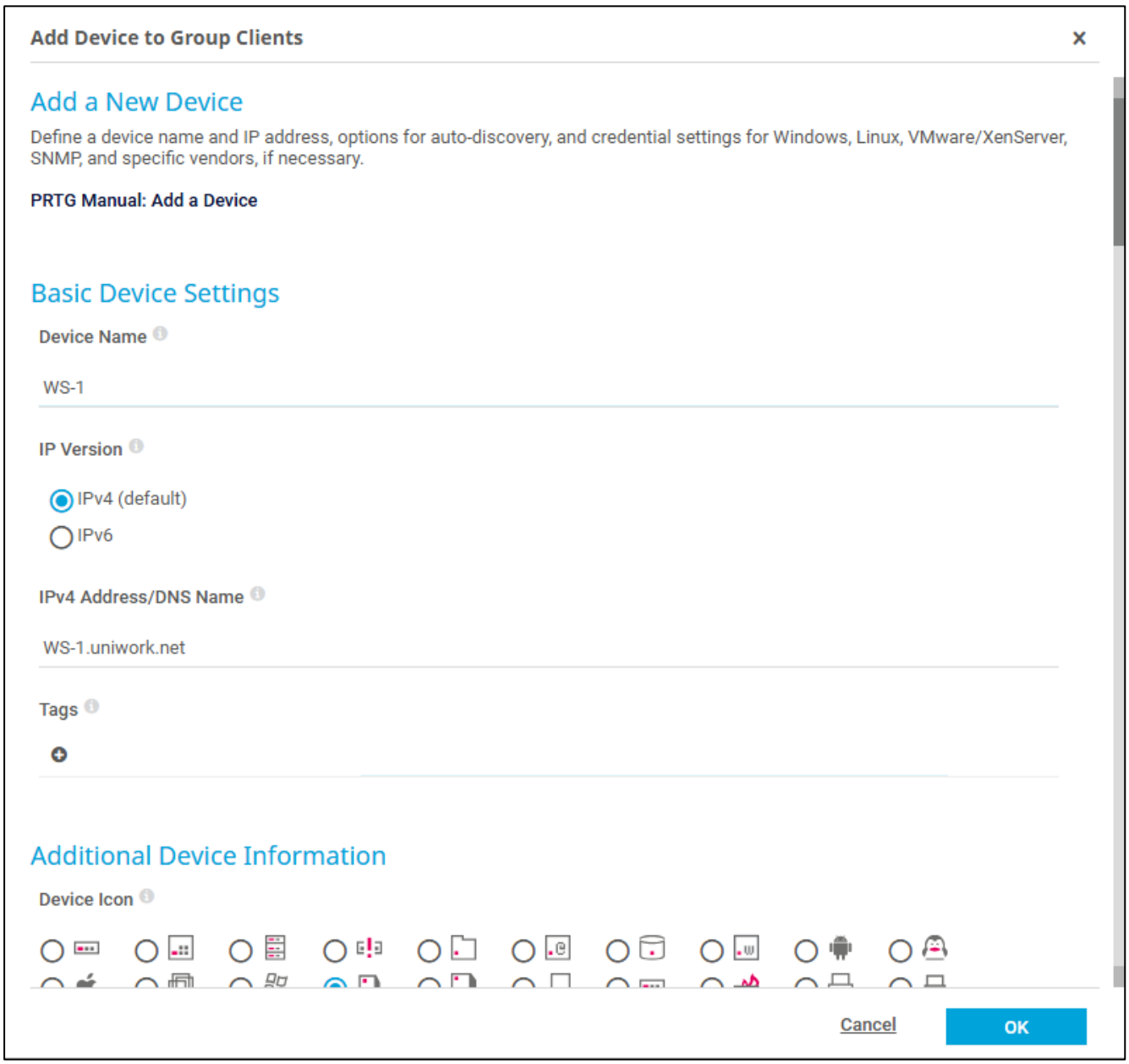


Рисунок 3.2.5 – Додавання пристрою

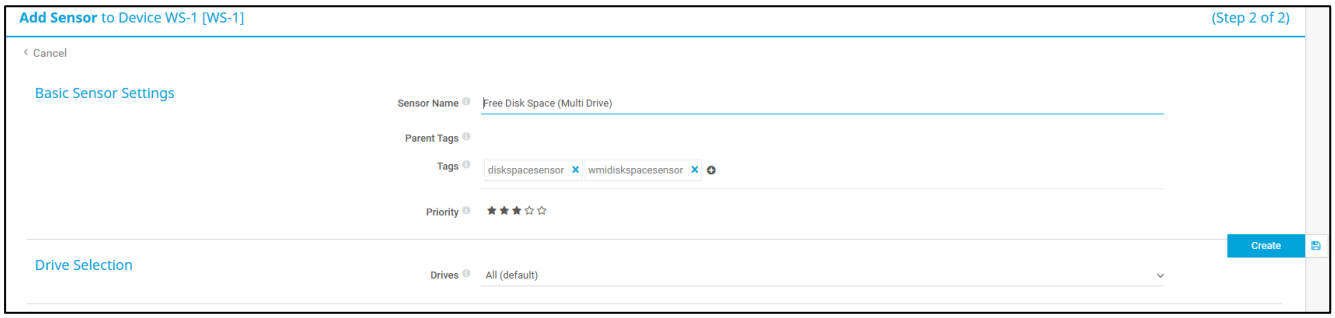


Рисунок 3.2.6 – Додавання сенсора

В меню Alarms відображено всі сенсори, що потребують уваги або вже повідомляють про проблему.

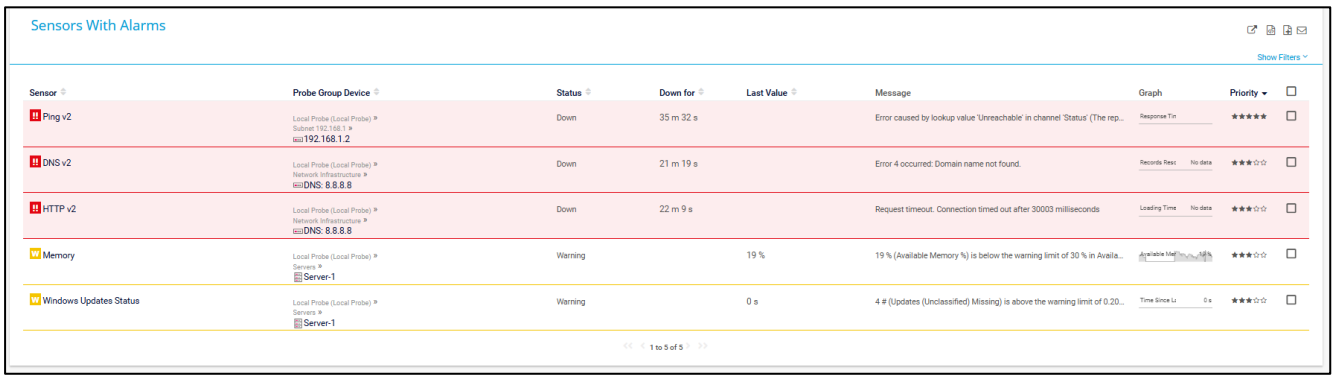


Рисунок 3.2.7 – Меню Sensors with Alarms

На сторінці Log Entries записуються всі події, зміни станів, попередження з вказанням дати й часу, що дозволяє адміністратору швидко знаходити й визначати послідовність подій і їх наслідки.

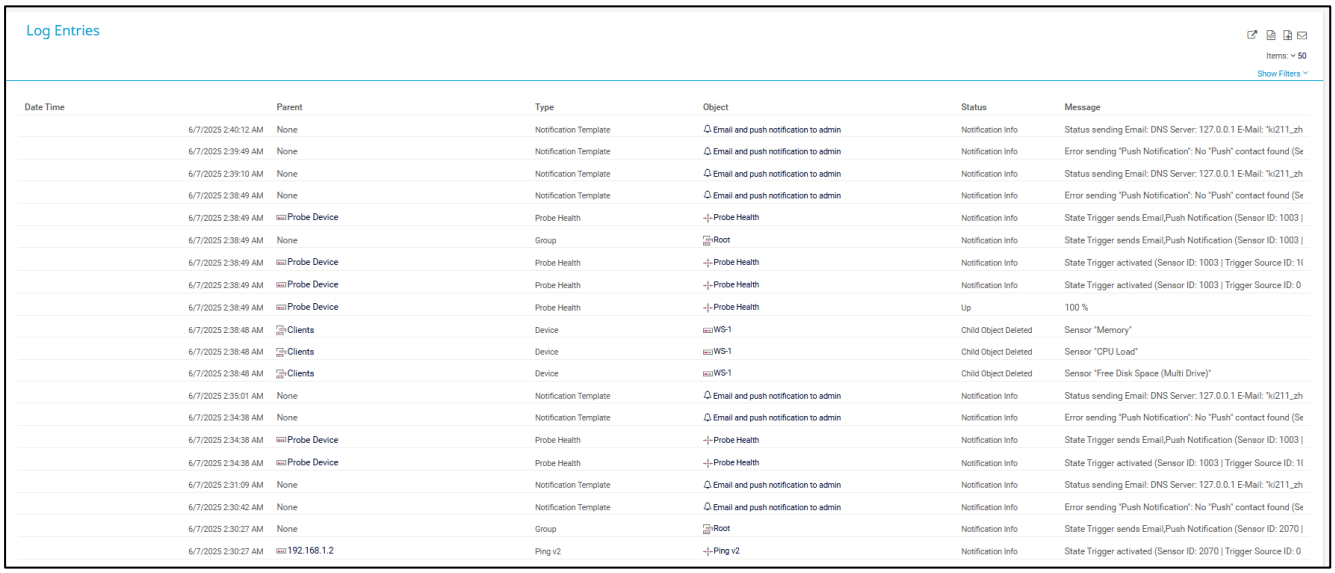


Рисунок 3.2.8 – Меню Log Entries

Інструмент Maps у PRTG Network Monitor дозволяє створювати мережеві карти, що слугують способом представлення даних у вигляді налаштовуваних дашбордів. Він забезпечує відображення статусу пристроїв, де кожен елемент карти показує поточний стан сенсорів, графіки та таблиці даних, а також пропонує кастомізацію через додавання іконок, фонових зображень та HTML-елементів. Карти можуть бути публічно доступними через URL, що дозволяє їх використовувати для спільного перегляду, а їх автоматичне оновлення гарантує актуальність даних у режимі реального часу.

Було створено дашборд для моніторингу мережі, включаючи відстеження продуктивності пристроїв (завантаження процесора, пам’ять, трафік), аналіз інцидентів через сповіщення про помилки та попередження, а також інтерактивні графіки та історичні дані для прогнозування можливих збоїв.

Рисунок 3.2.9 – Меню Maps. Створений дашборд

3.3. Розгортання веб-порталу

Для розгортання веб-порталу необхідно попередньо виконати певні налаштування і встановити необхідні програмні інструменти. Встановлюємо СУБД MySQL та MySQL Workbench для зручної взаємодії з базами даних.

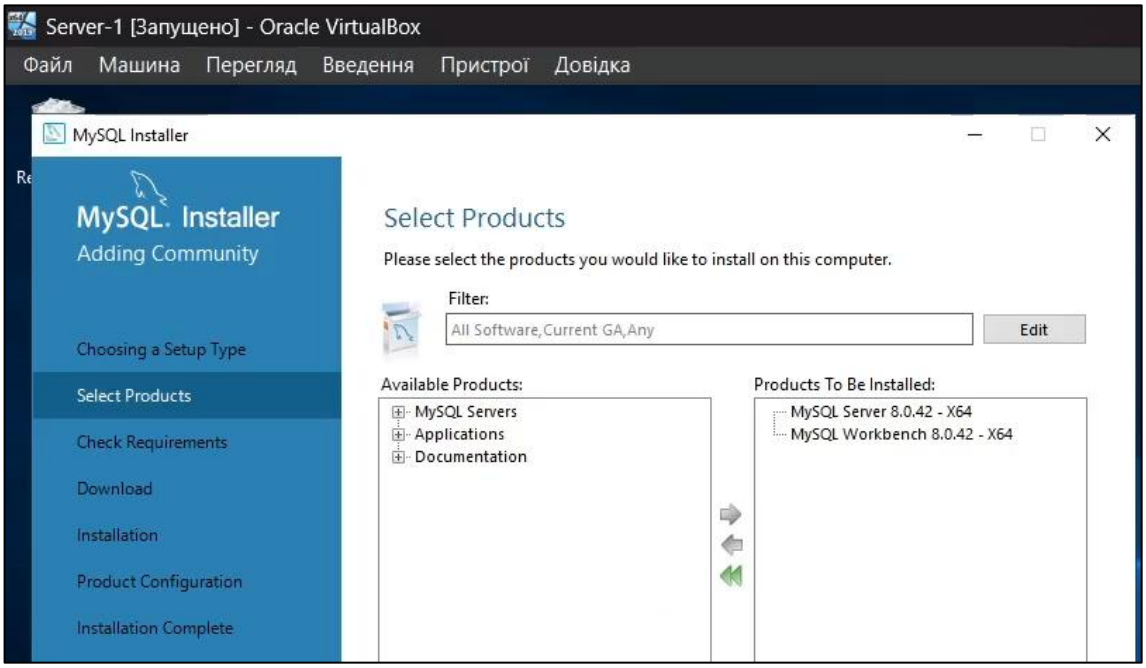


Рисунок 3.3.1 – Процес встановлення

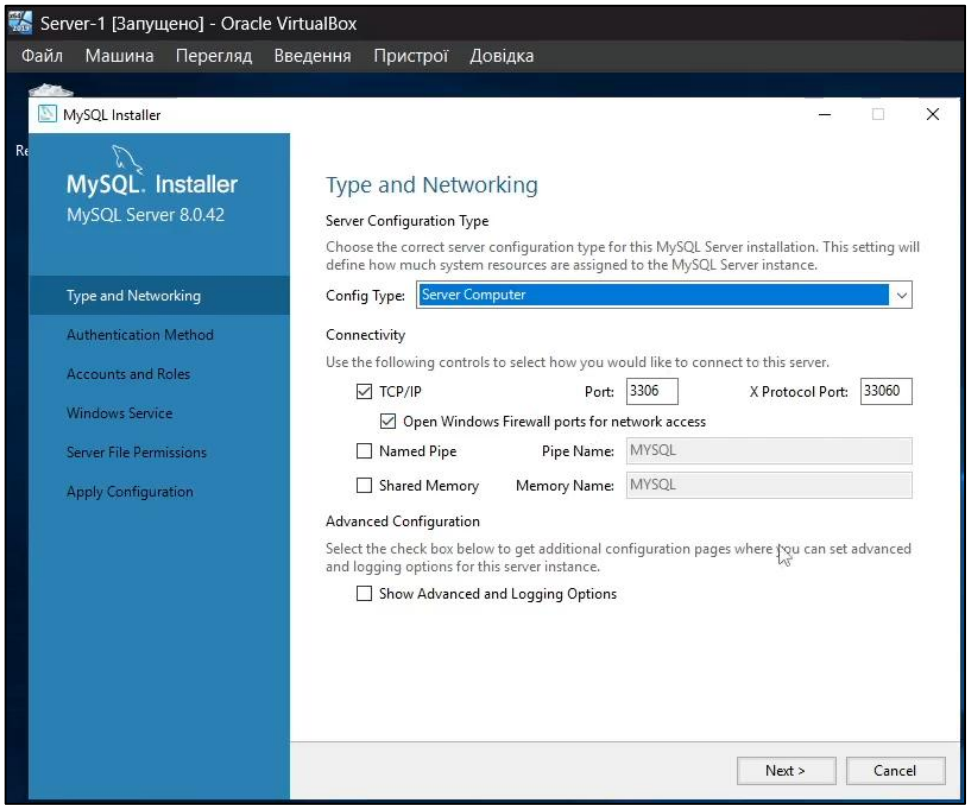


Рисунок 3.3.2 – Параметри конфігурації

Окрім кореневого користувача, створюємо також окремого користувача wpuser для веб-порталу.

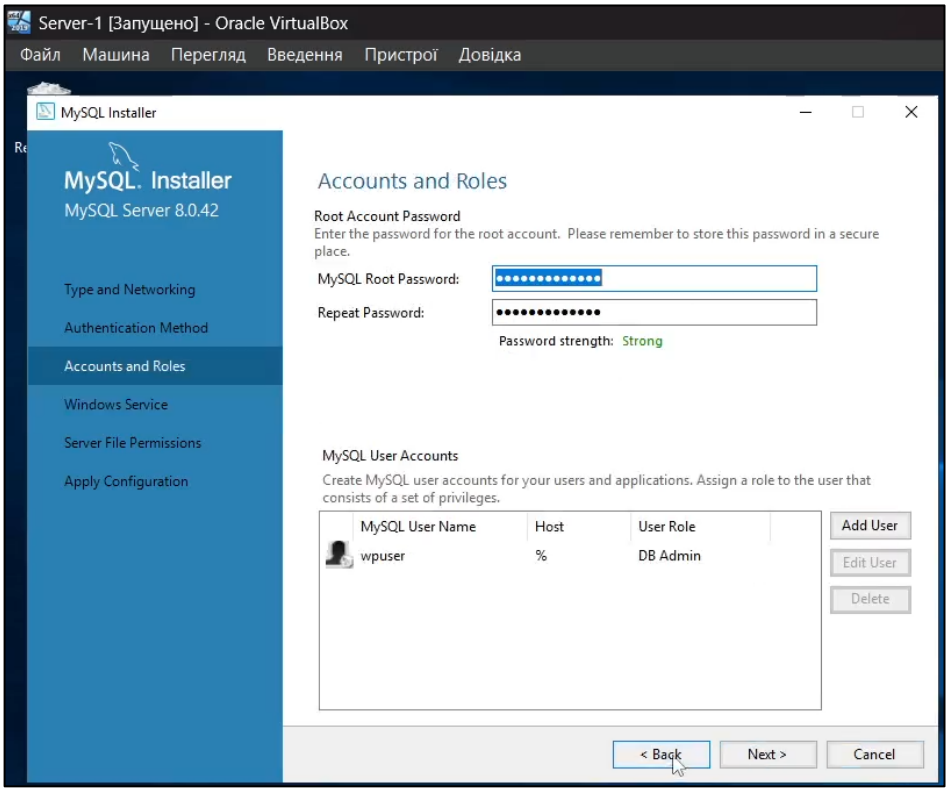


Рисунок 3.3.3 – Користувачі MySQL

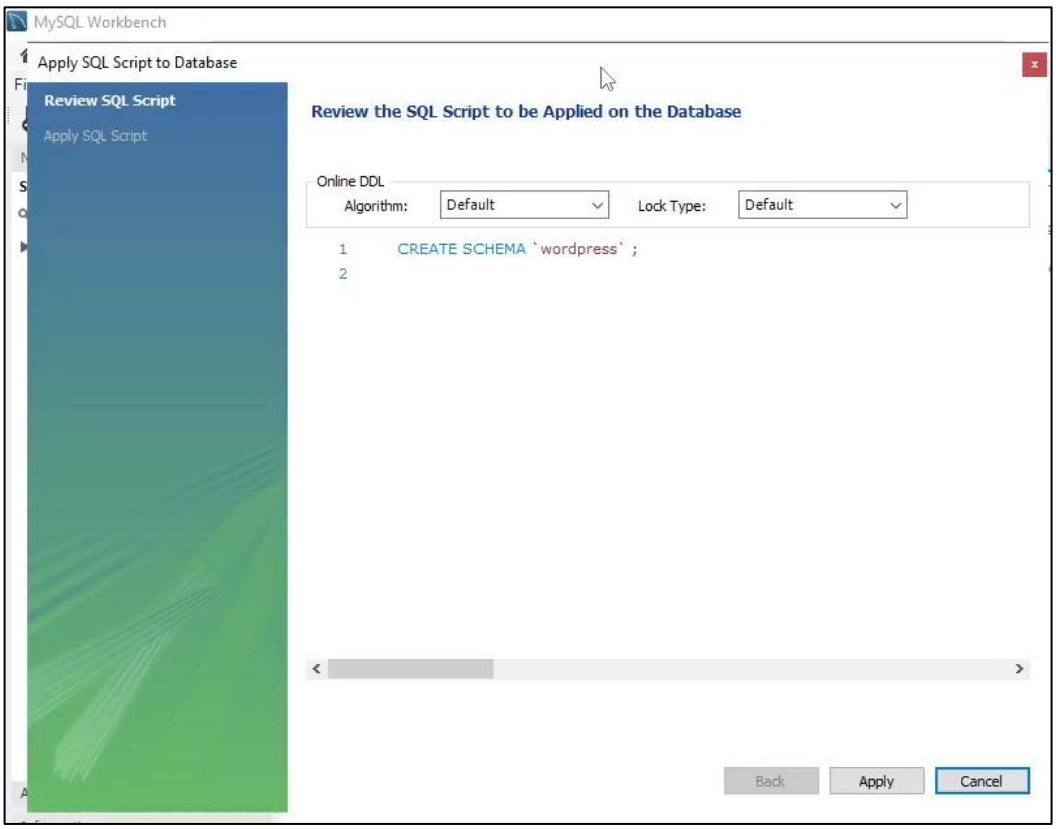


Рисунок 3.3.4 – Створення бази даних wordpress

Для WordPress необхідним програмним рушієм є PHP, тож за допомогою модуля для PowerShell, встановлюємо його і необхідні розширення. Далі в конфігураційному файлі php.ini розкоментовуємо або додаємо рядки для решти вже встановлених розширень, щоб їх увімкнути.

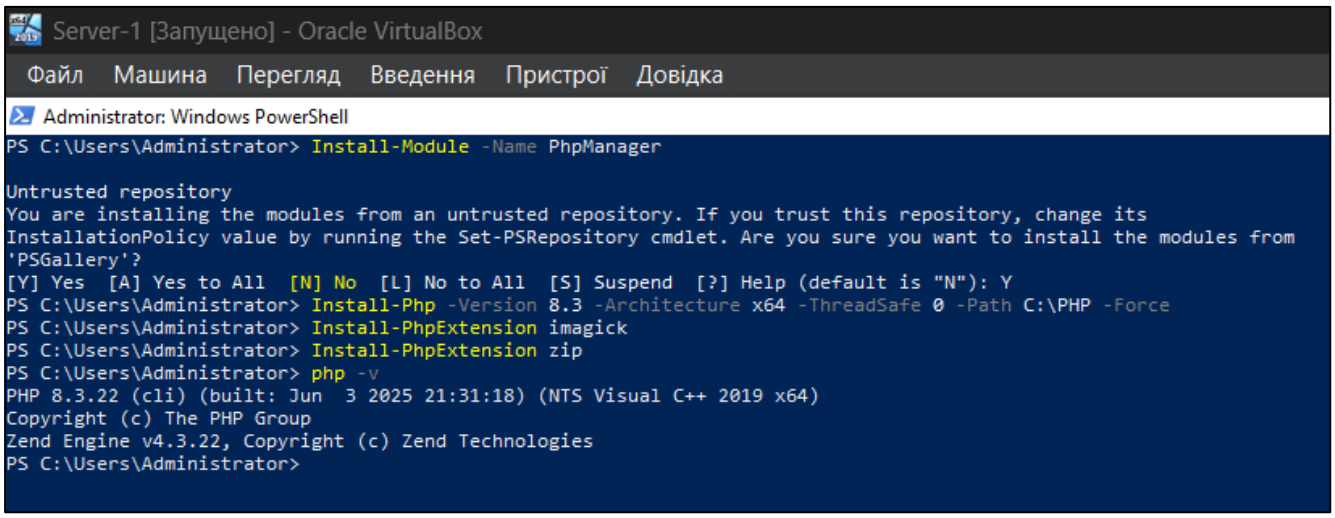


Рисунок 3.3.5 – Встановлення PHP за допомогою PhpManager

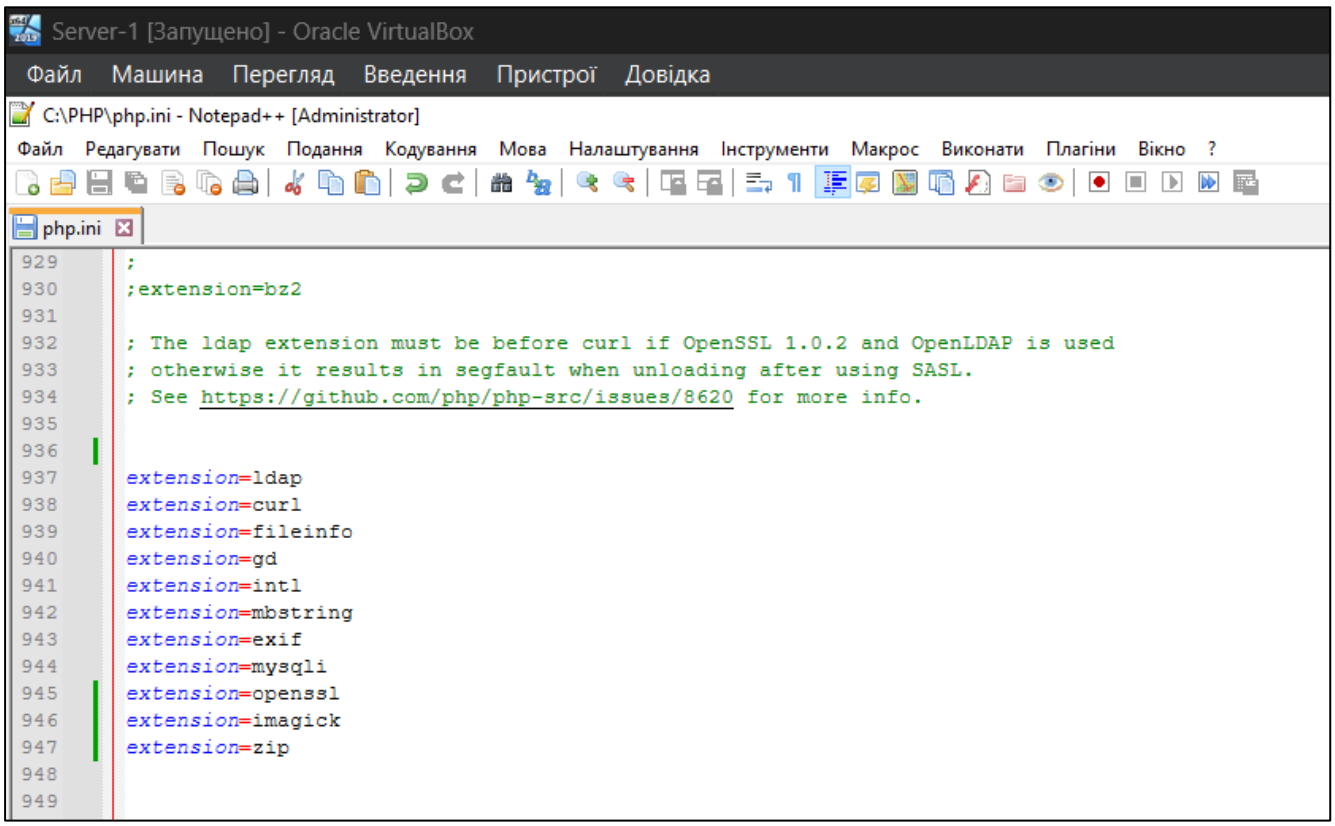


Рисунок 3.3.6 – Конфігураційний файл php.ini

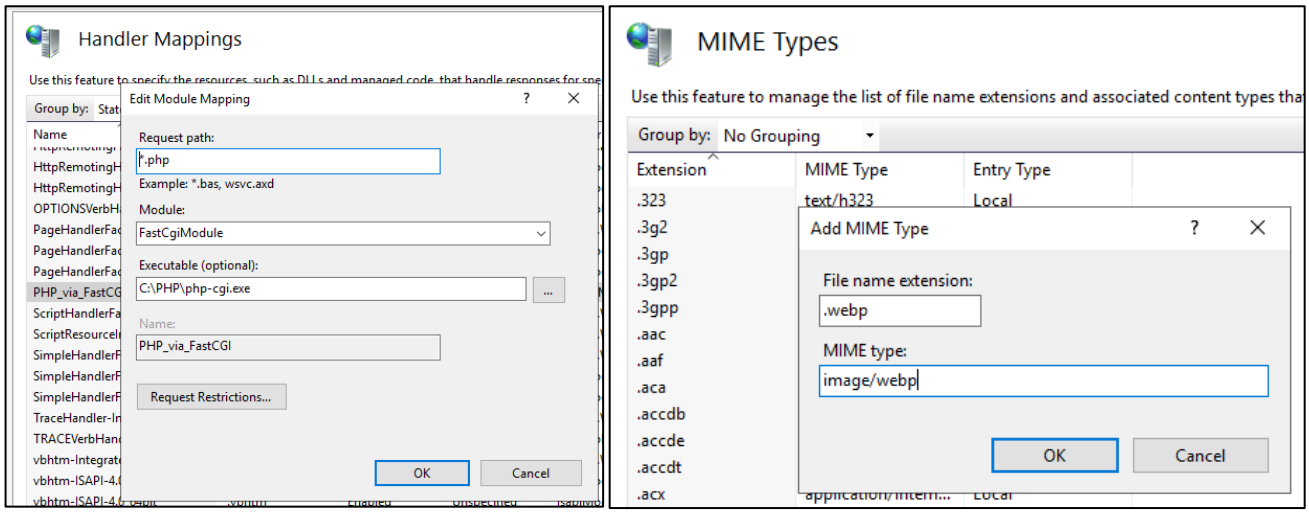


Рисунок 3.3.7 – Додавання обробника FastCGI і розширення webp

Засобами IIS створюємо сайт з назвою організації Uniwork. Фізичний шлях вказуємо до папки wordpress, в яку було скопійовано вміст архіву з офіційного сайту WordPress.org. В якості типу підключення обираємо https і використовуємо SSL сертифікат підписаний локальним центром сертифікації (Додаток А).

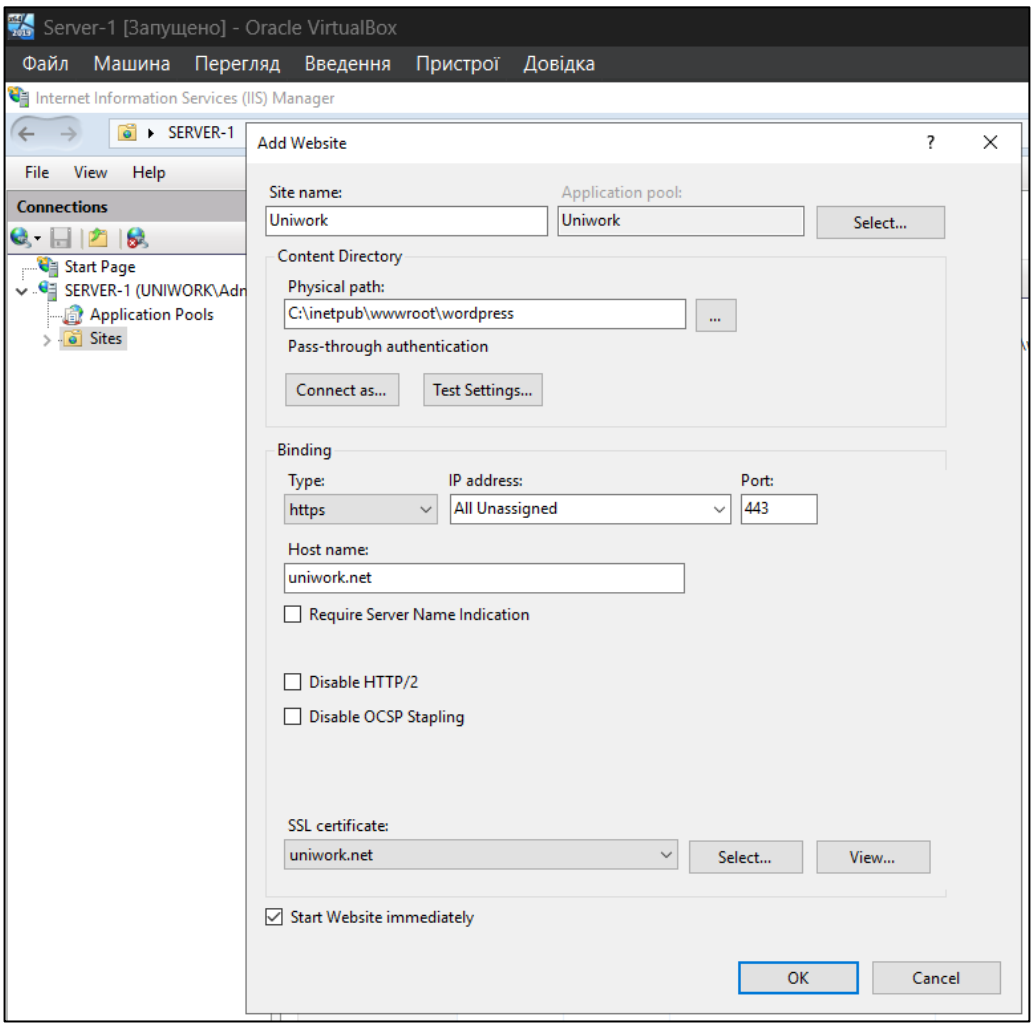


Рисунок 3.3.8 – Створення сайту в IIS Manager

Тепер сайт доступний за посиланням https://uniwork.net і його потрібно підключити до БД wordpress. Вказуємо назву сайту і користувача-адміністратора.

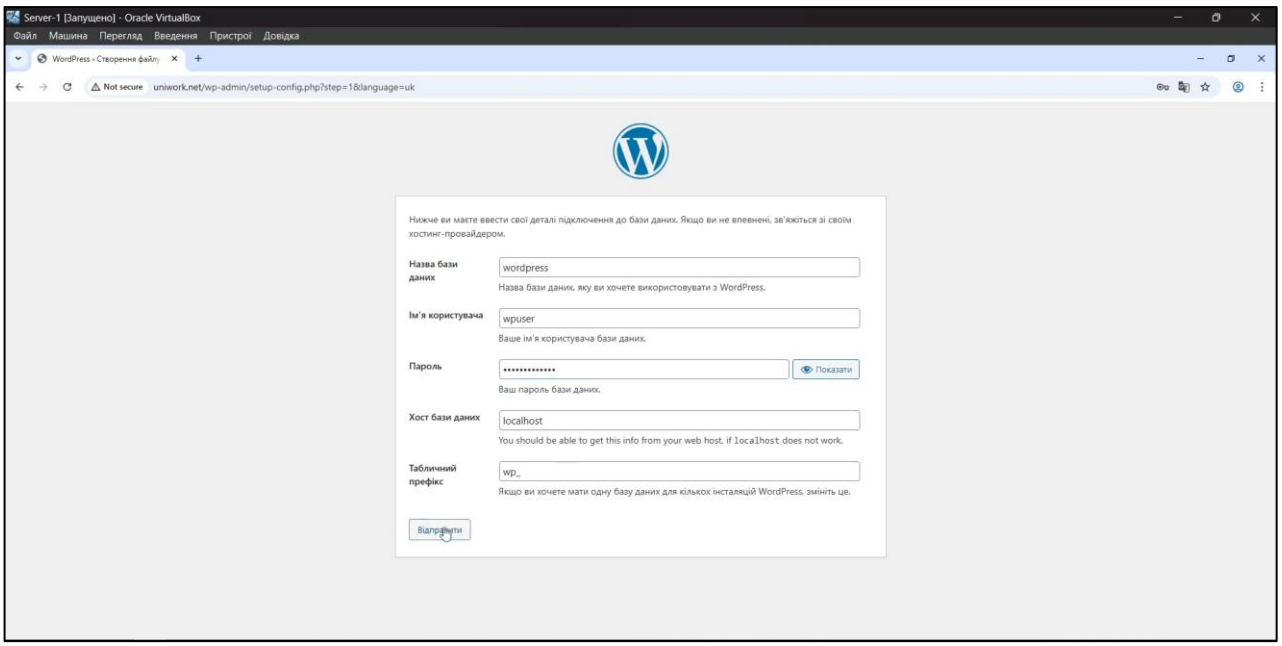


Рисунок 3.3.9 – Підключення до БД

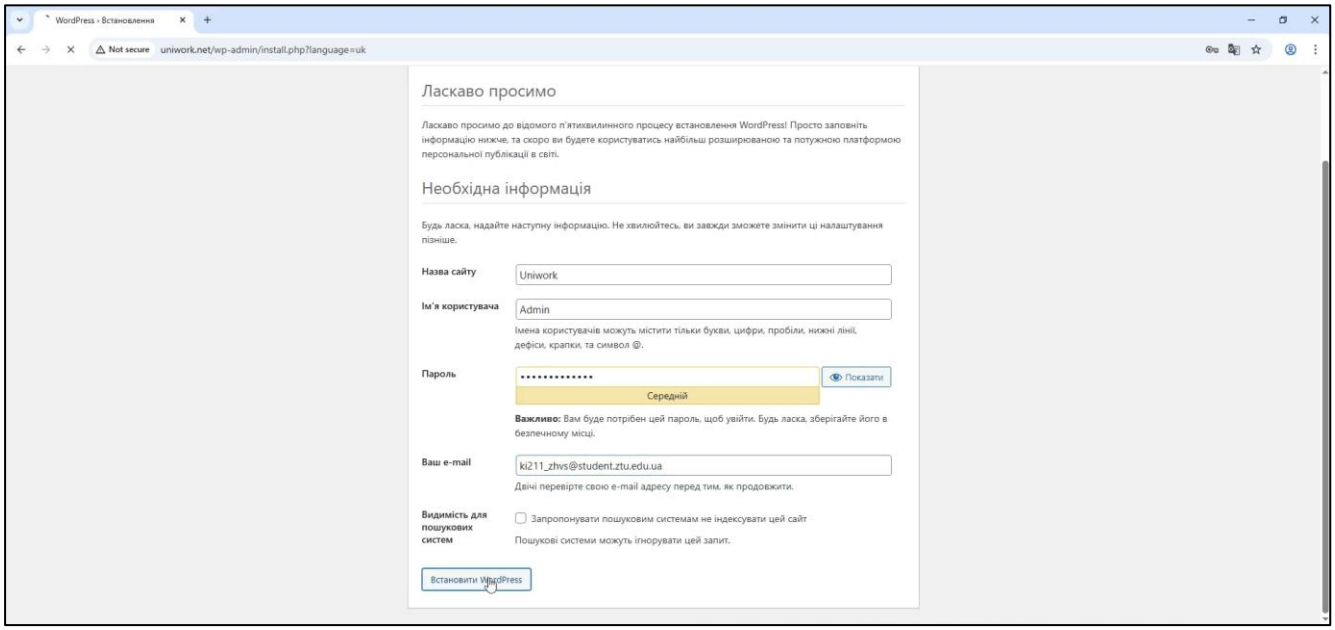


Рисунок 3.3.10 – Встановлення WordPress

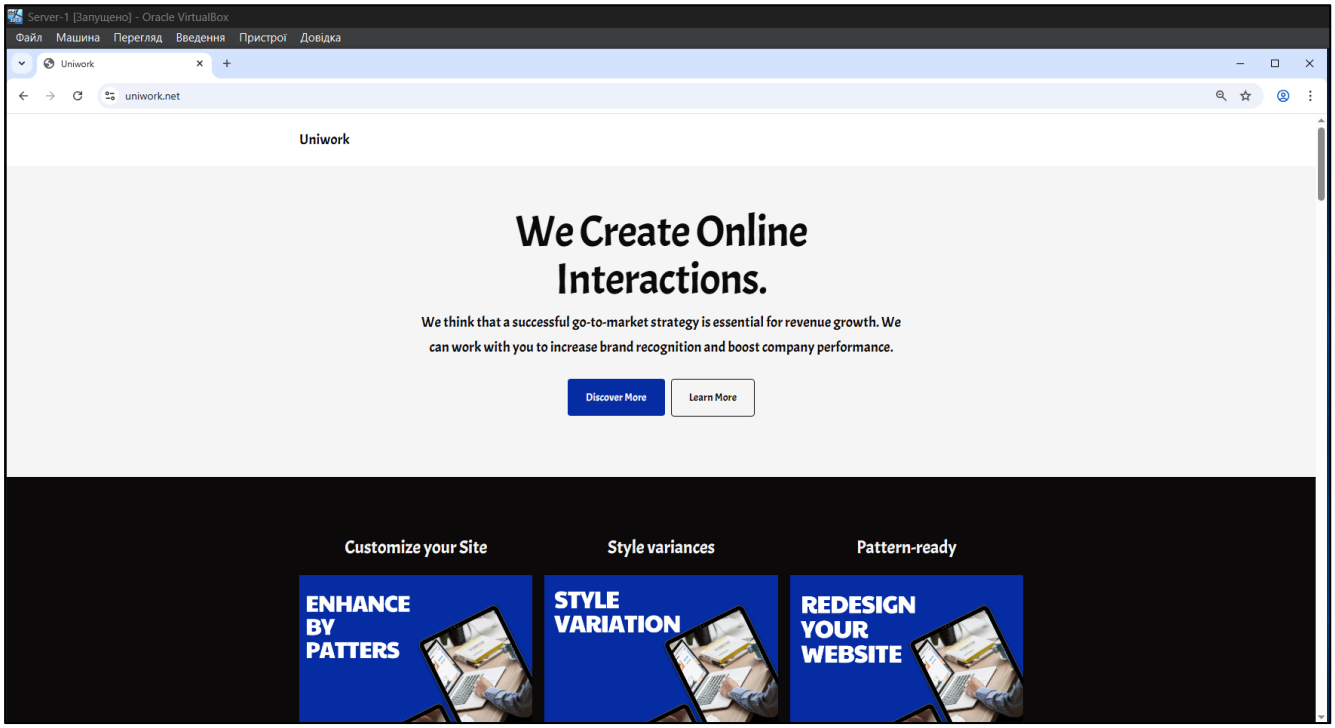


Рисунок 3.3.11 – Головна сторінка сайту uniwork.net

Далі встановлюємо необхідні плагіни, а саме:

- W3 Total Cache для оптимізації швидкодії сайту
- LDAP by miniOrange для інтеграції користувачів AD
- Contact Form 7 та Flamingo для форми зворотнього зв'язку й перегляду отриманих повідомлень відповідно
- Capabilities для створення ролей і обмеження доступу до елементів веб-сайту

- Restrictions для заборони доступу і розмежування прав перегляду сторінок

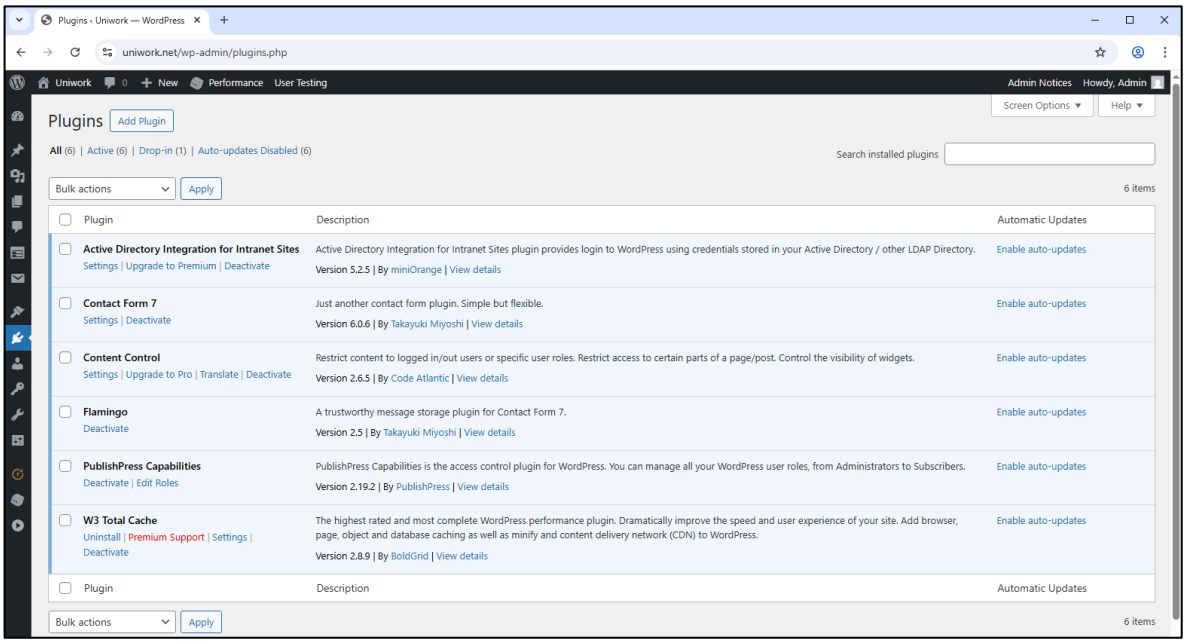


Рисунок 3.3.12 – Встановлені плагіни

Створюємо сторінки, кожна з яких буде мати різні рівні доступу для користувачів.

На сторінку Contact Us додаємо елемент із плагіну Contact Form 7 і вказуємо форму за замовчуванням Contact Form 1.

На сторінку Monitoring додаємо блок HTML-коду, який ми отримали в PRTG Network Monitor. В ньому міститься посилання на створений дашборд (Рис. 3.2.9).

На сторінку Schedule таблицю з розкладом і завданнями для працівників організації.

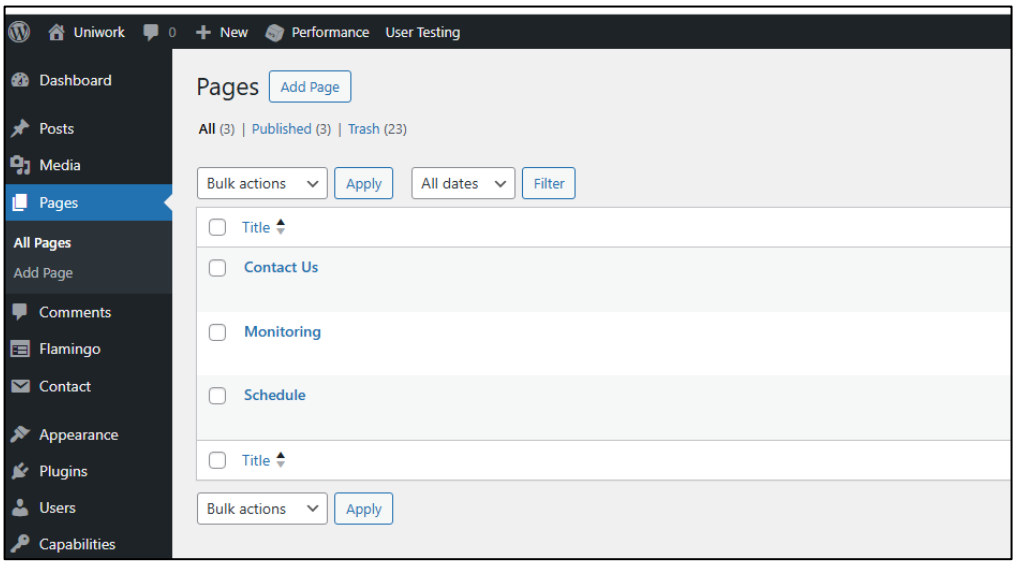


Рисунок 3.3.13 – Створені сторінки

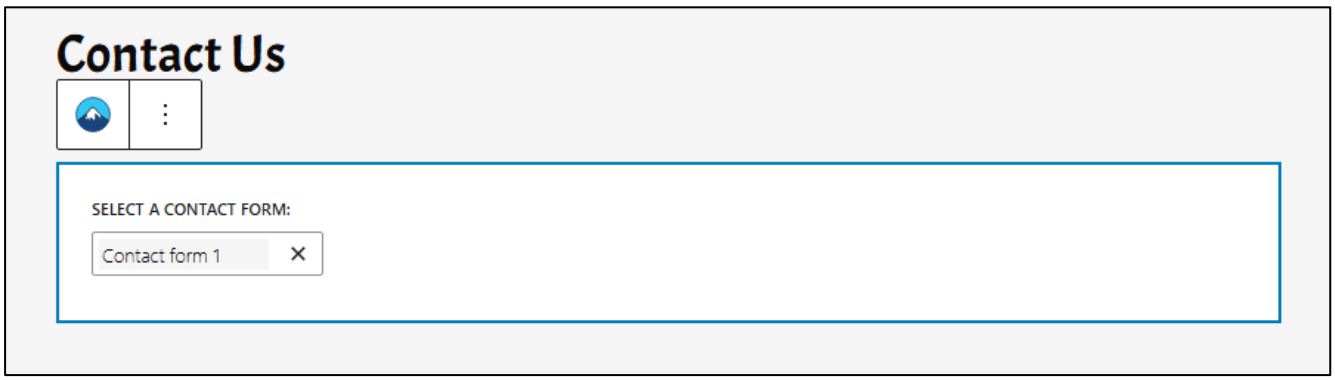
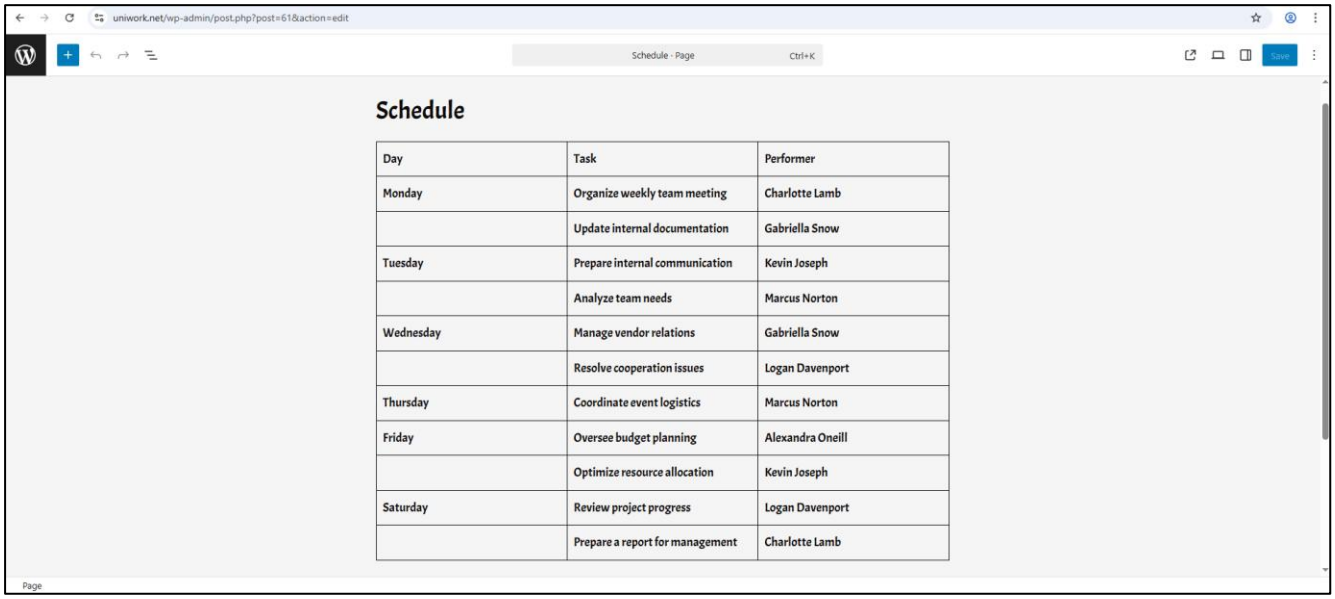


Рисунок 3.3.14 – Сторінка Contact Us

Рисунок 3.3.15 – Сторінка Monitoring



Day	Task	Performer
Monday	Organize weekly team meeting	Charlotte Lamb
	Update internal documentation	Gabriella Snow
Tuesday	Prepare internal communication	Kevin Joseph
	Analyze team needs	Marcus Norton
Wednesday	Manage vendor relations	Gabriella Snow
	Resolve cooperation issues	Logan Davenport
Thursday	Coordinate event logistics	Marcus Norton
Friday	Oversee budget planning	Alexandra Oneill
	Optimize resource allocation	Kevin Joseph
Saturday	Review project progress	Logan Davenport
	Prepare a report for management	Charlotte Lamb

Рисунок 3.3.16 – Сторінка Schedule

Засобами плагіну Capabilities створюємо окрему роль adUser для користувачів Active Directory. В навігаційній панелі для неавторизованих користувачів залишаємо посилання лише на сторінки зворотнього зв'язку і авторизації. Для користувачів ролі adUser, окрім двох попередніх, буде також доступне посилання на сторінку з розкладом.

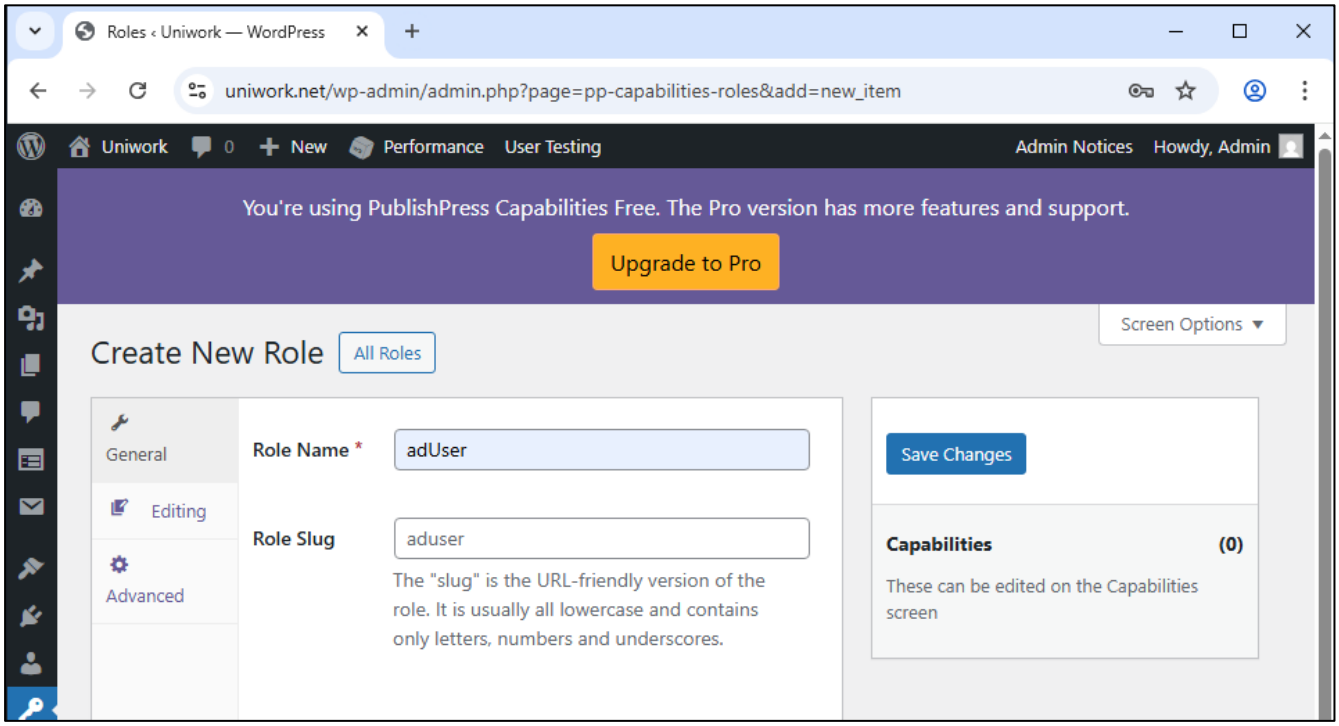


Рисунок 3.3.17 – Створення нової ролі adUser

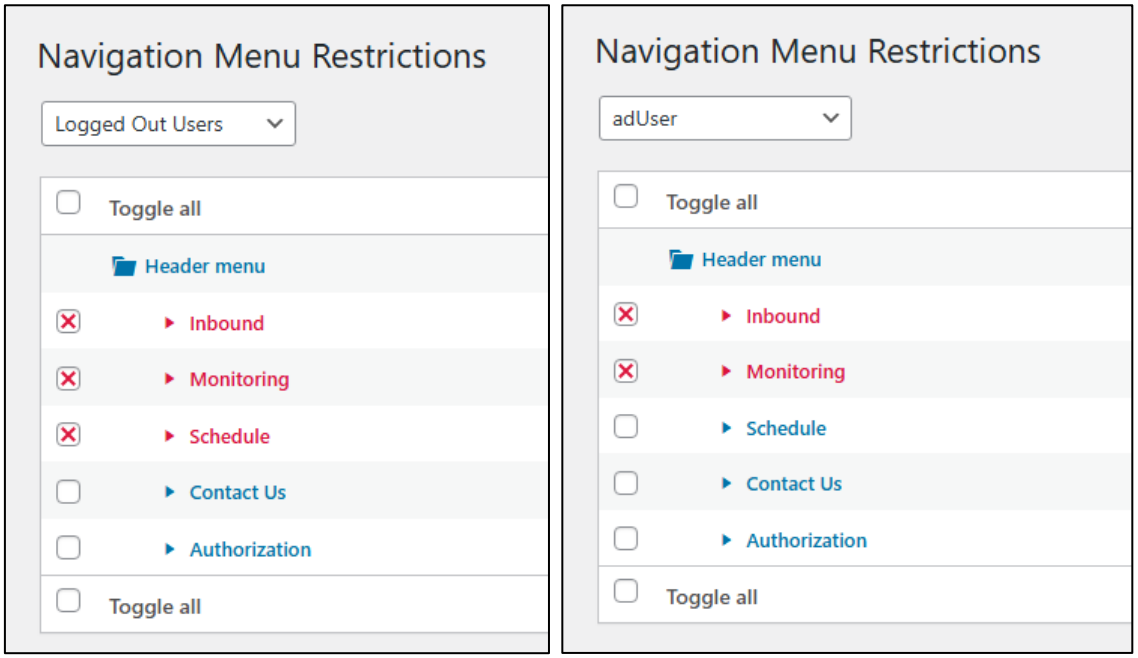


Рисунок 3.3.18 – Обмеження доступу до навігаційної панелі

Наступним кроком є обмеження доступу до контенту, на основі ролей. Для цього, використовуючи плагін Restrictions, створюємо правила доступу до певних сторінок.

Для сторінки Schedule використовуємо метод Matching, тобто відповідність певній ролі. Обираємо користувачів Admin та adUser. Аналогічним способом надаємо доступ до сторінки Monitoring, але лише для користувача Admin.

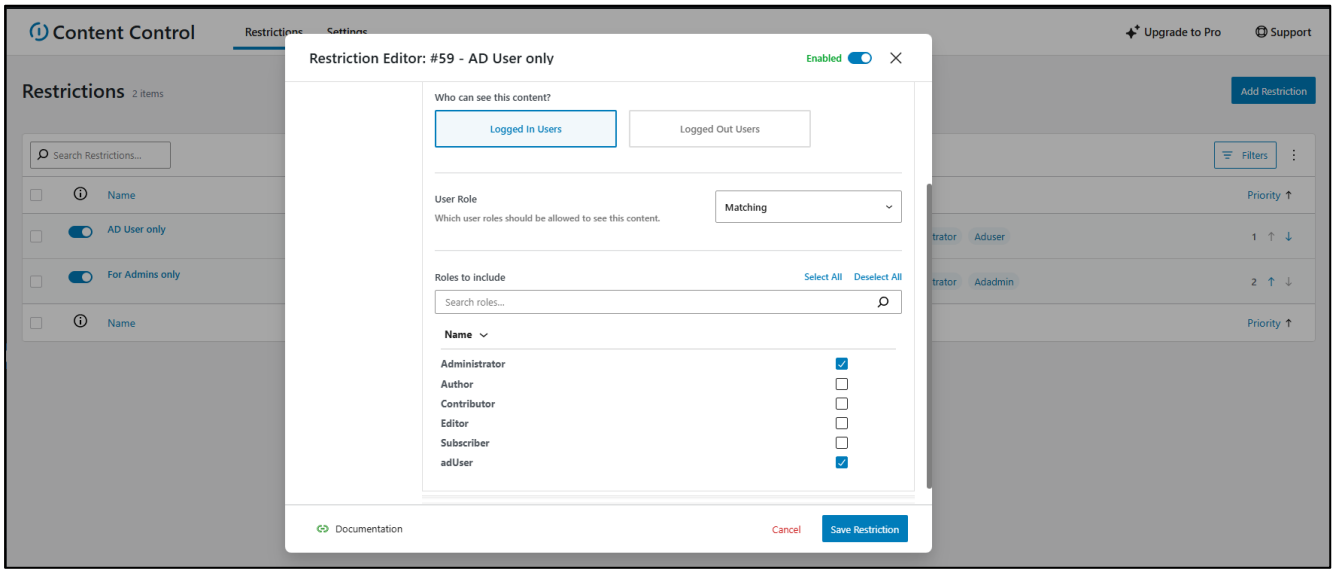


Рисунок 3.3.19 – Створення нового обмеження “AD User only”

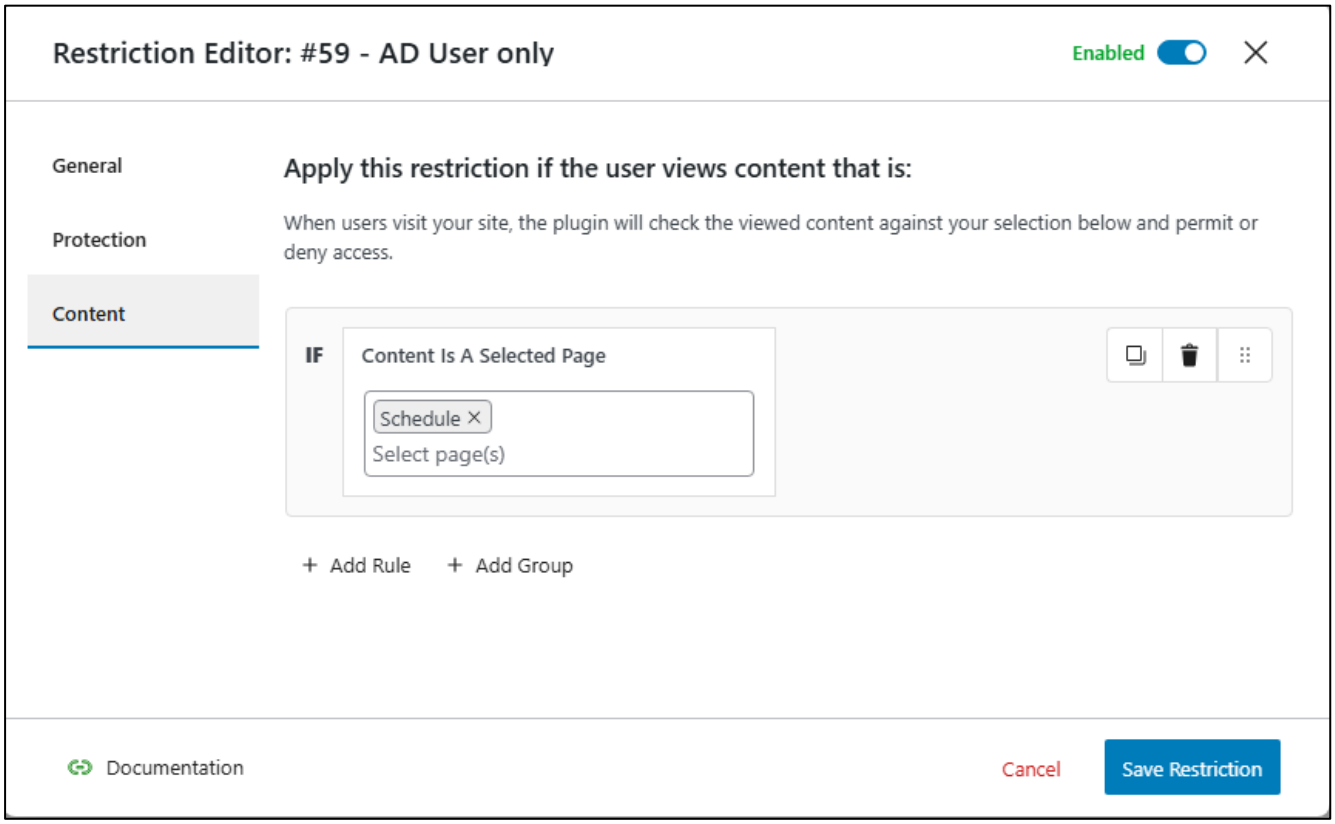


Рисунок 3.3.20 – Вибір контенту до якого застосовується обмеження

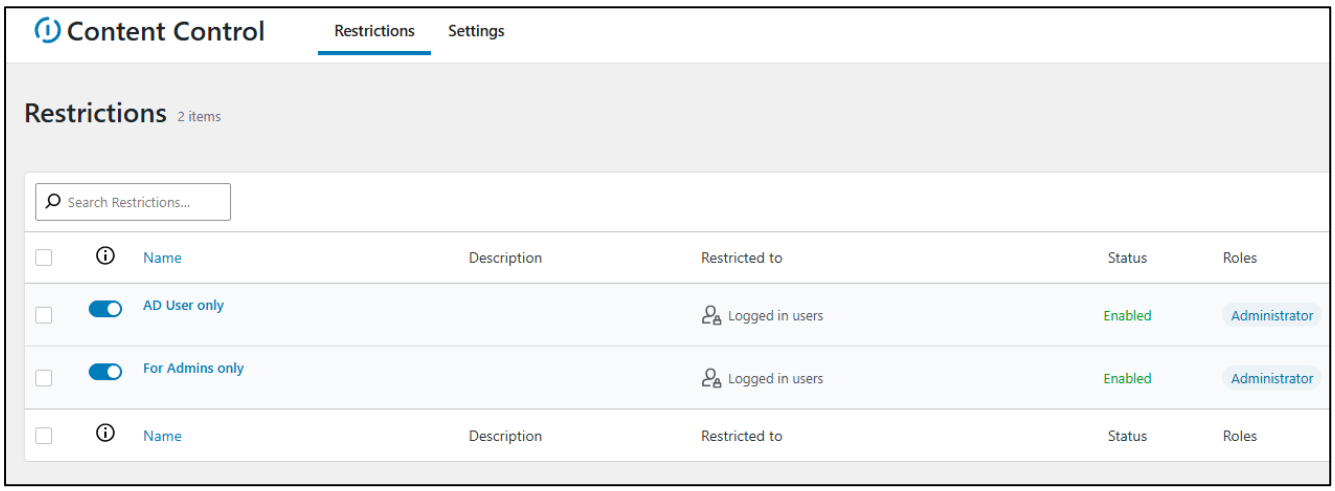


Рисунок 3.3.21 – Створені правила доступу

Накінець налаштовуємо LDAP автентифікацію. В полі Directory Service обираємо Microsoft Active Directory. Вказуємо адресу серверу автентифікації, а саме Server-1, порт залишаємо незмінним. Вводимо облікові дані службового аккаунту ldapreader створеного спеціально для зчитування атрибутів користувачів домену.

Обираємо в якості області пошуку домен uniwork.net, а також атрибут sAMAccountName, який буде використовуватися в якості логіна.

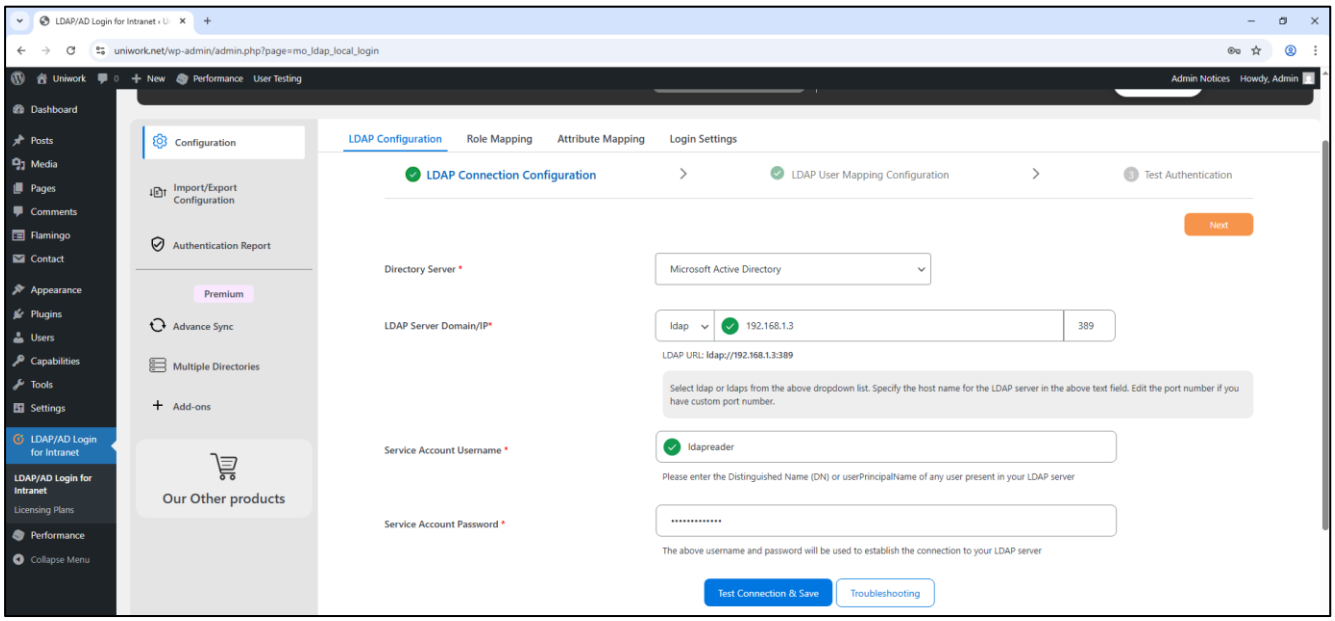


Рисунок 3.3.22 – Конфігурація LDAP плагіна

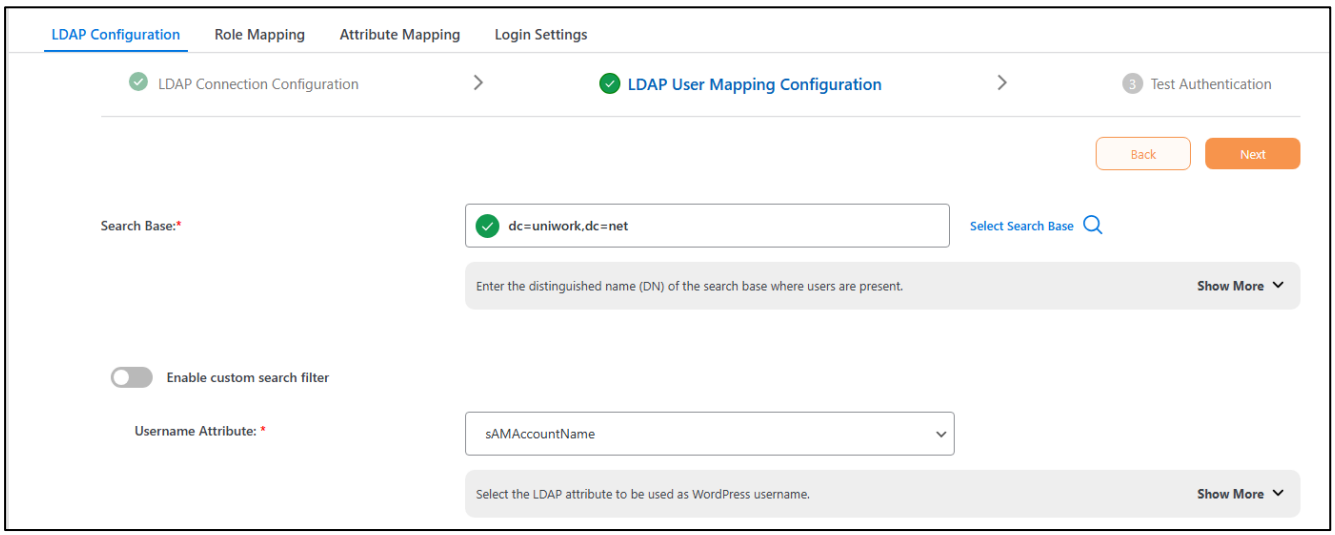


Рисунок 3.3.23 – Конфігурація LDAP плагіна

Призначаємо роль adUser усім користувачам, які успішно пройшли автентифікацію.

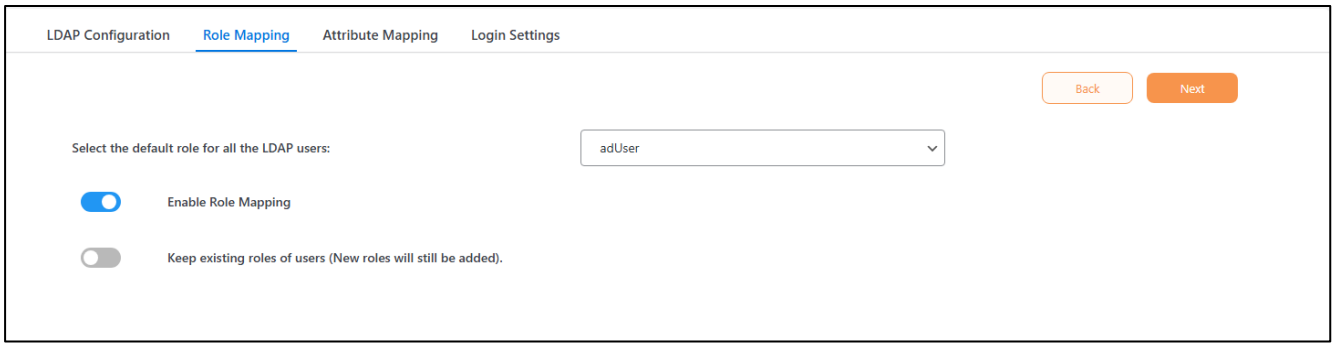


Рисунок 3.3.24 – Налаштування Role Mapping

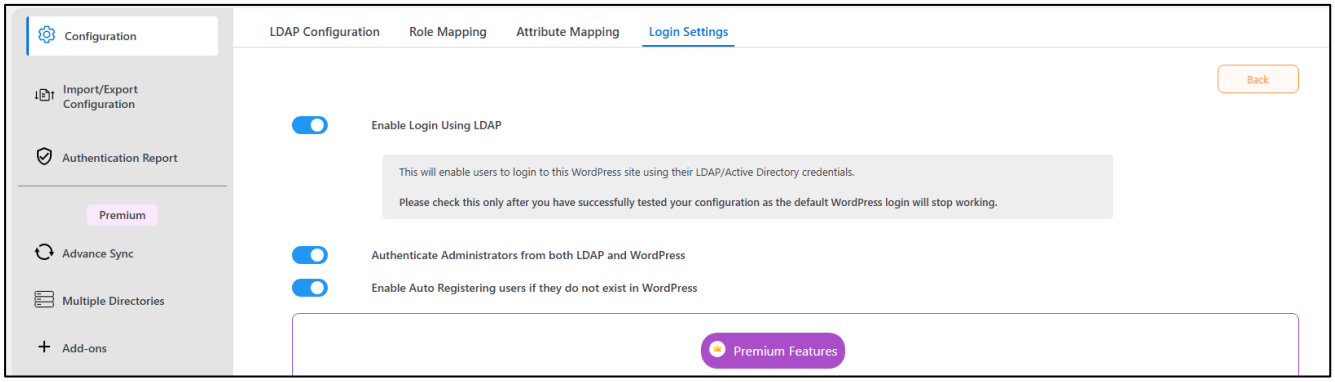


Рисунок 3.3.25 – Увімкнення LDAP як способу входу

3.4. Тестування комп'ютерної мережі та налаштованих сервісів

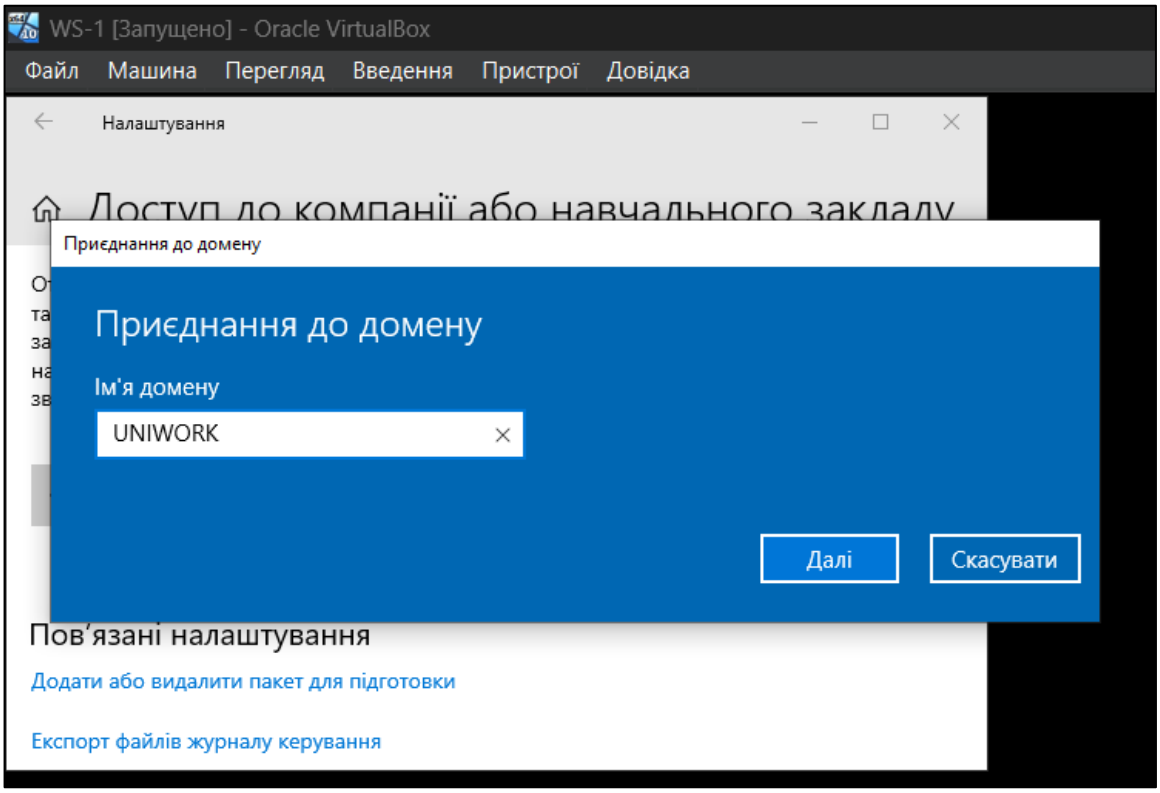


Рисунок 3.4.1 – Додавання робочої станції в домен

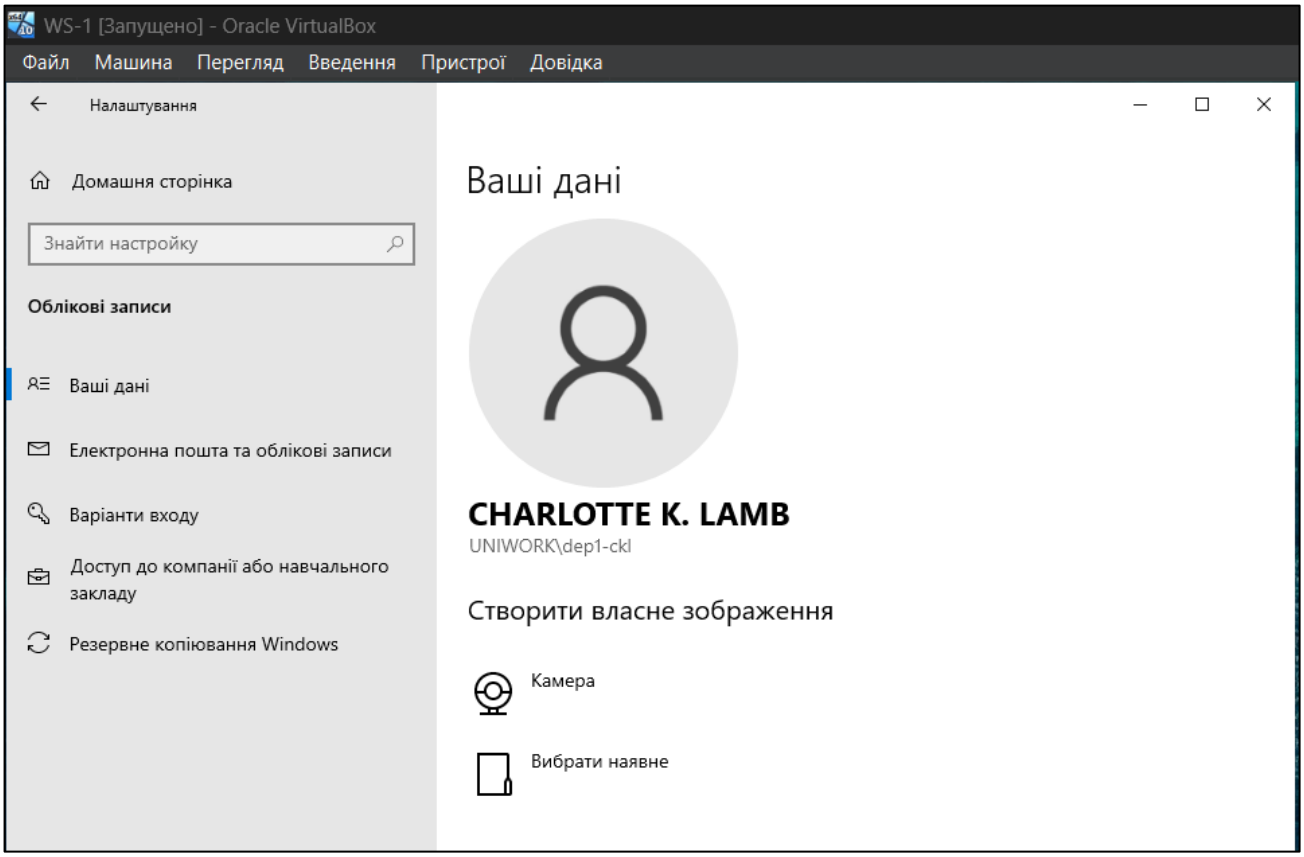


Рисунок 3.4.2 – Вхід з робочої станції під обліковими даними користувача AD

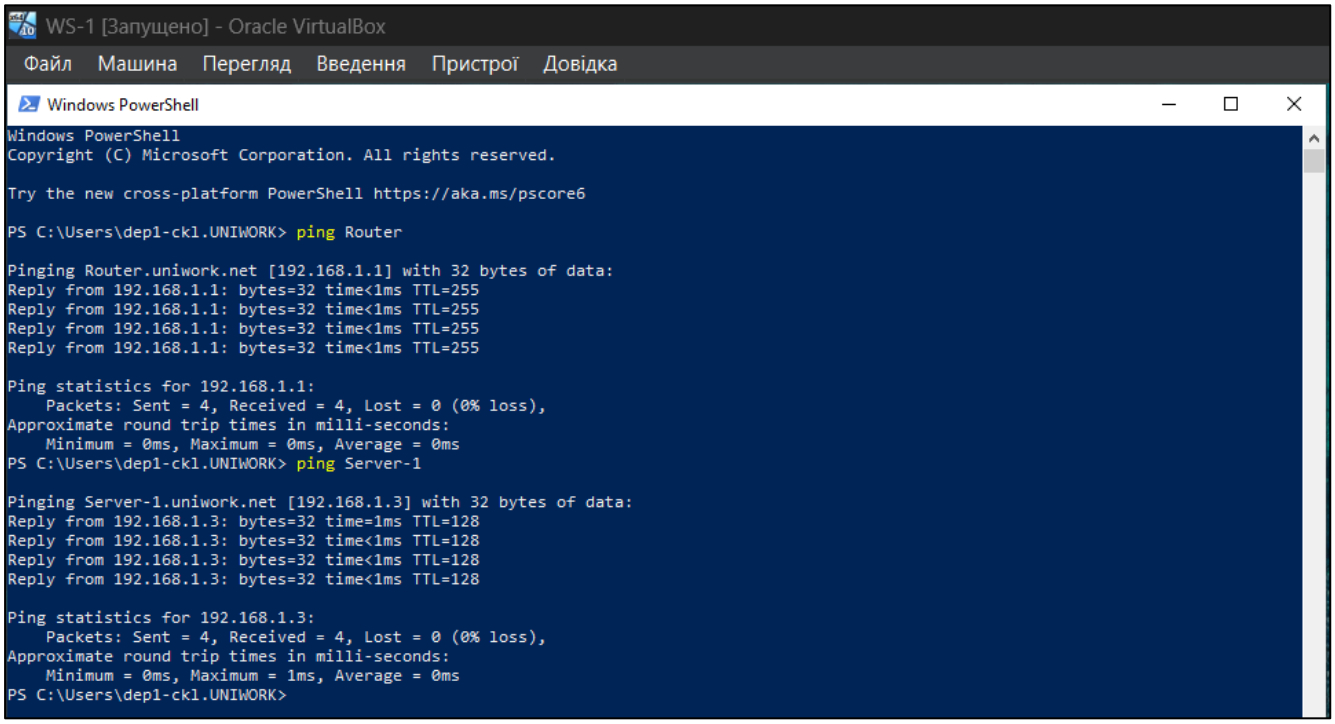


Рисунок 3.4.3 – Перевірка зв’язку

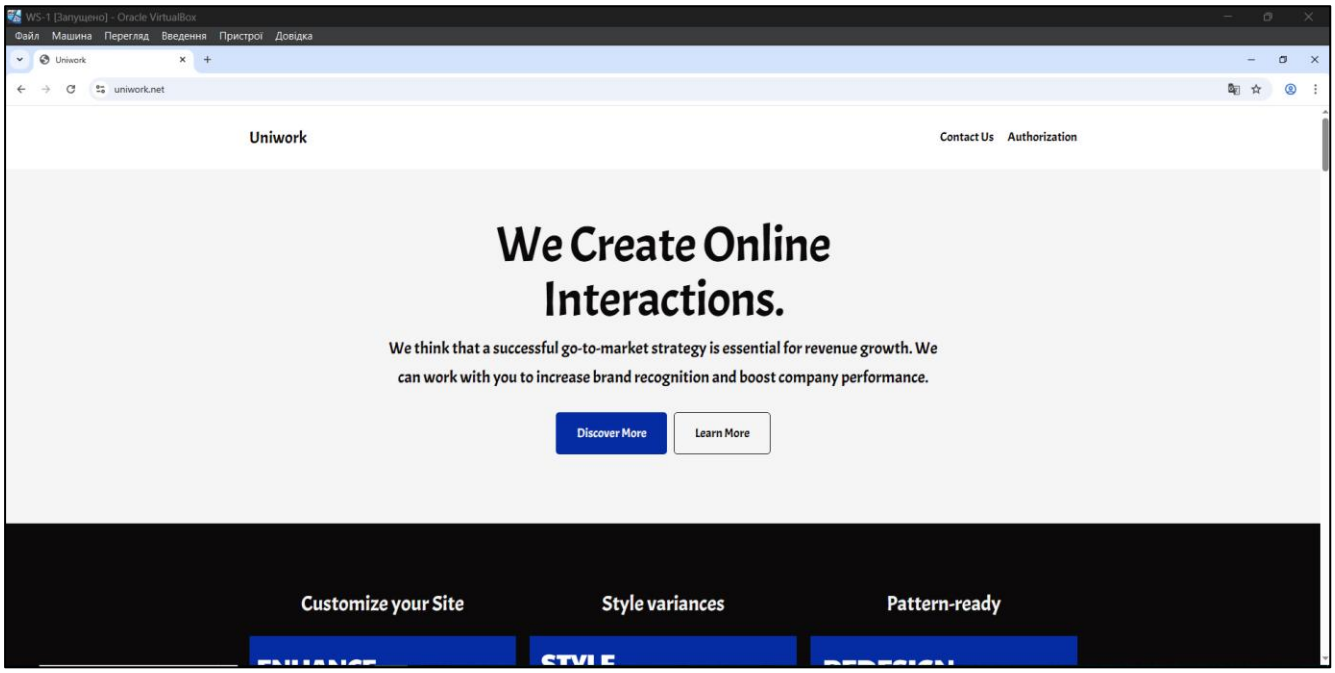


Рисунок 3.4.4 – Вигляд сайту в ролі неавторизованого користувача

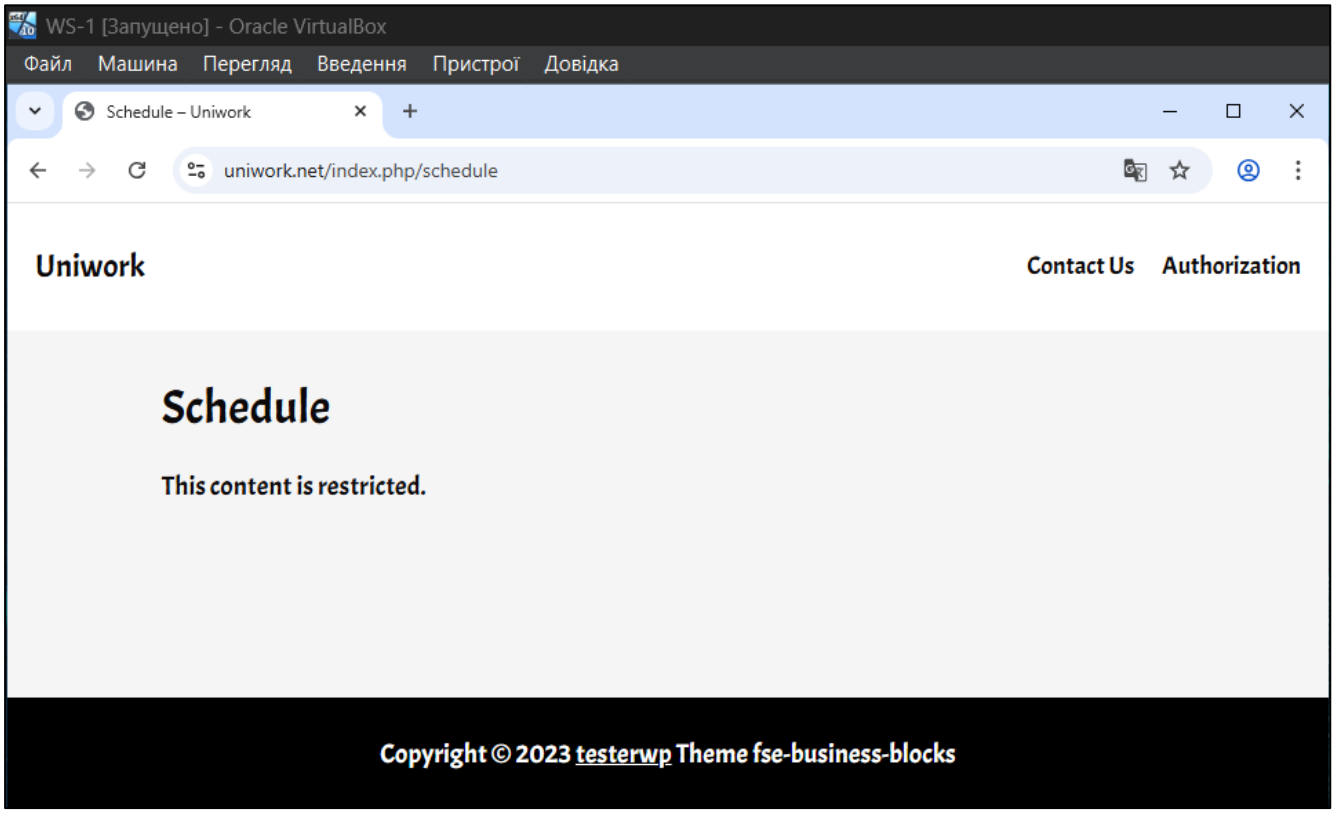


Рисунок 3.4.5 – Сторінка Schedule без прав доступу

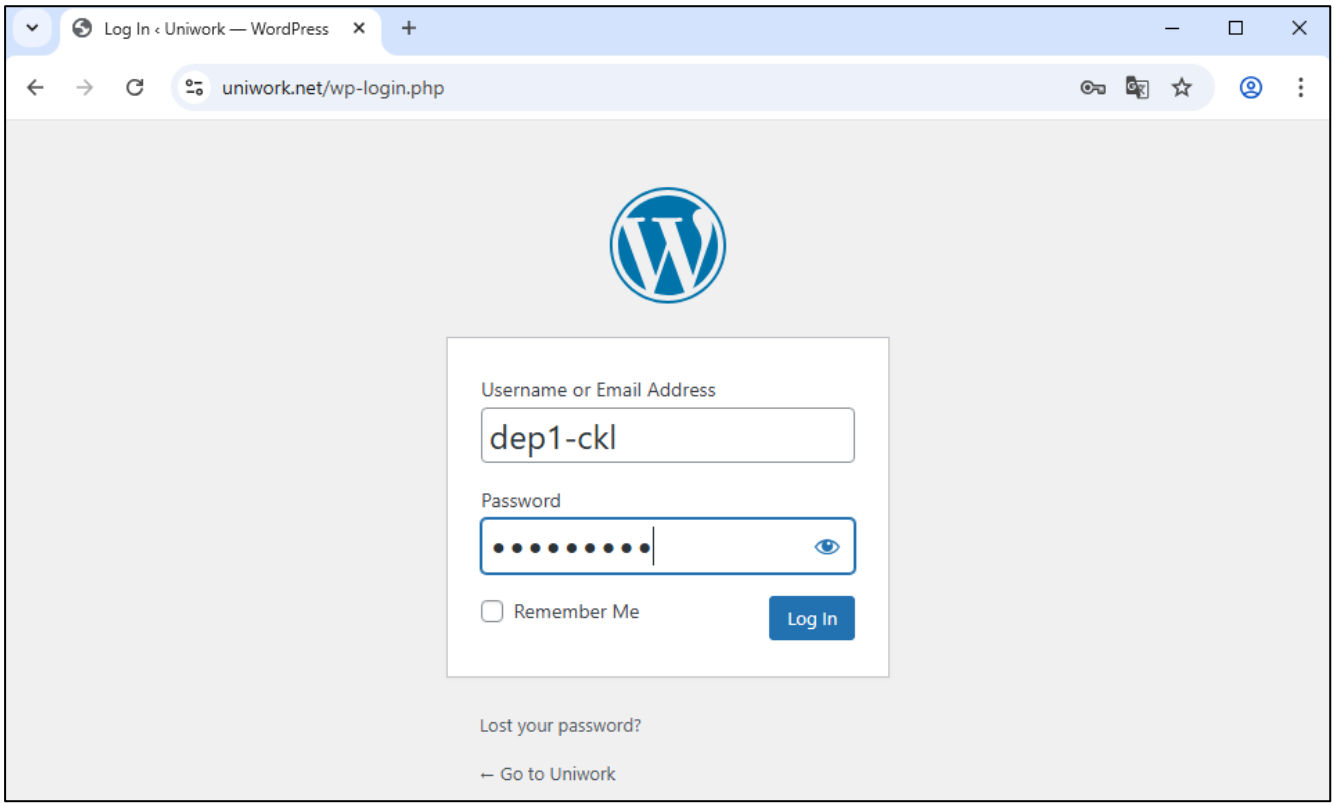


Рисунок 3.4.6 – Авторизація на сайті за допомогою облікового запису AD

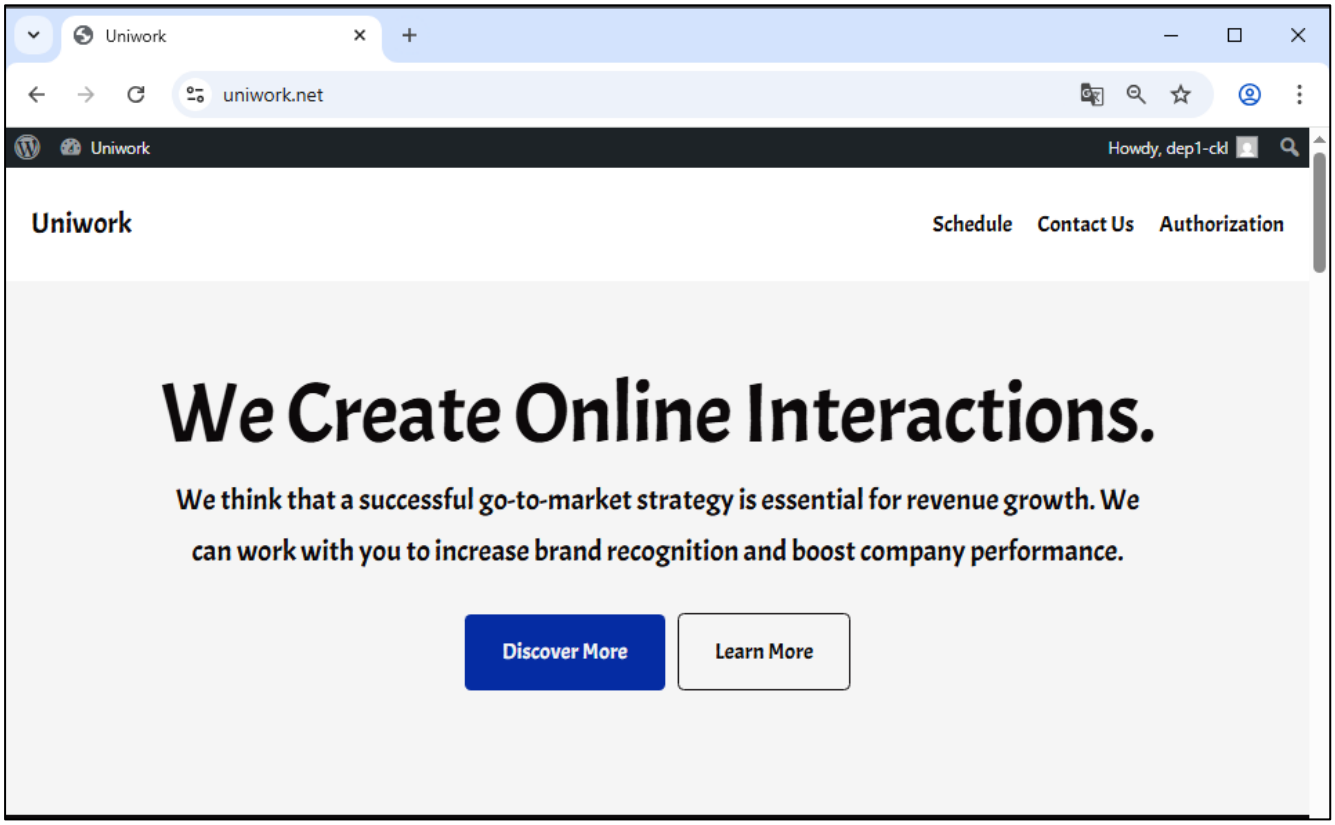


Рисунок 3.4.7 – Вигляд сайту в ролі авторизованого користувача AD

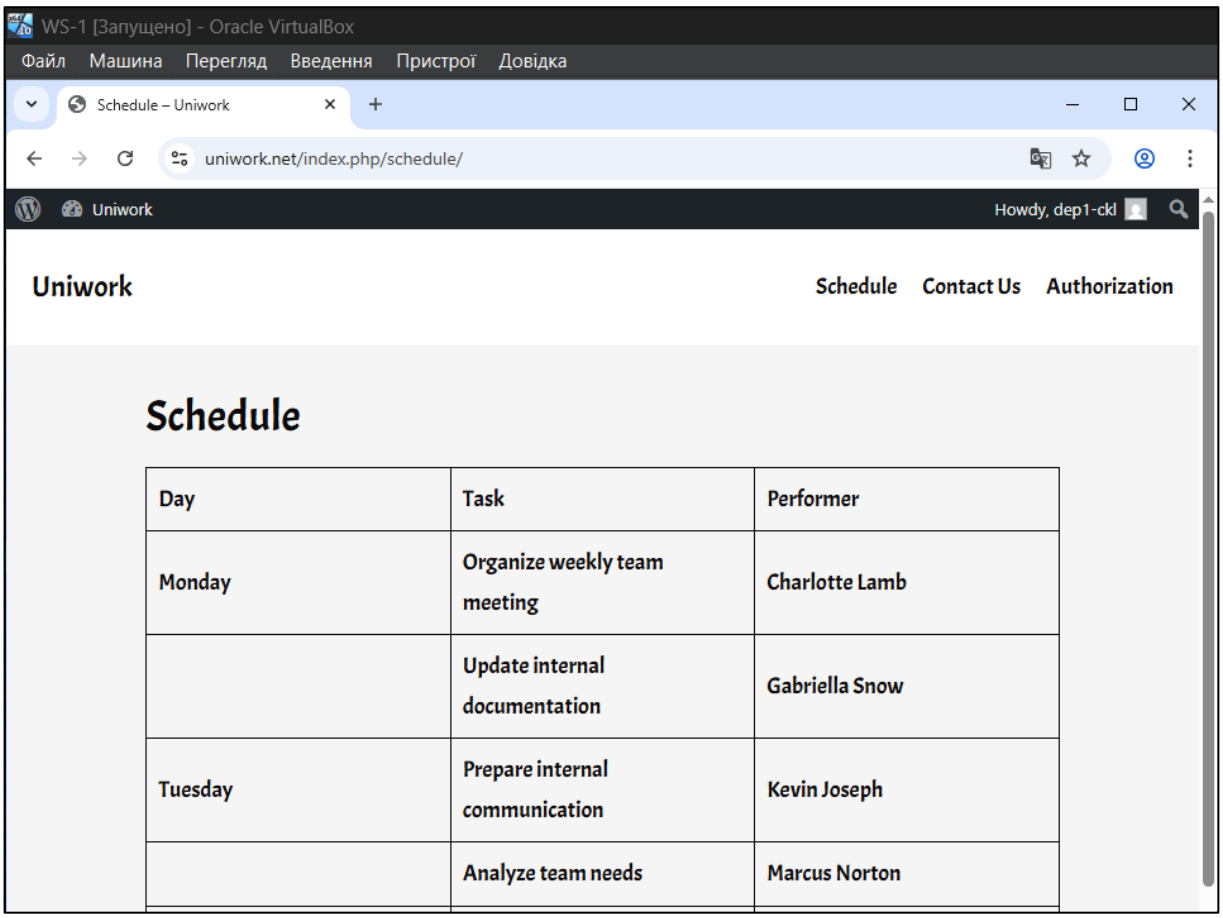


Рисунок 3.4.8 – Перегляд сторінки Schedule в ролі авторизованого користувача

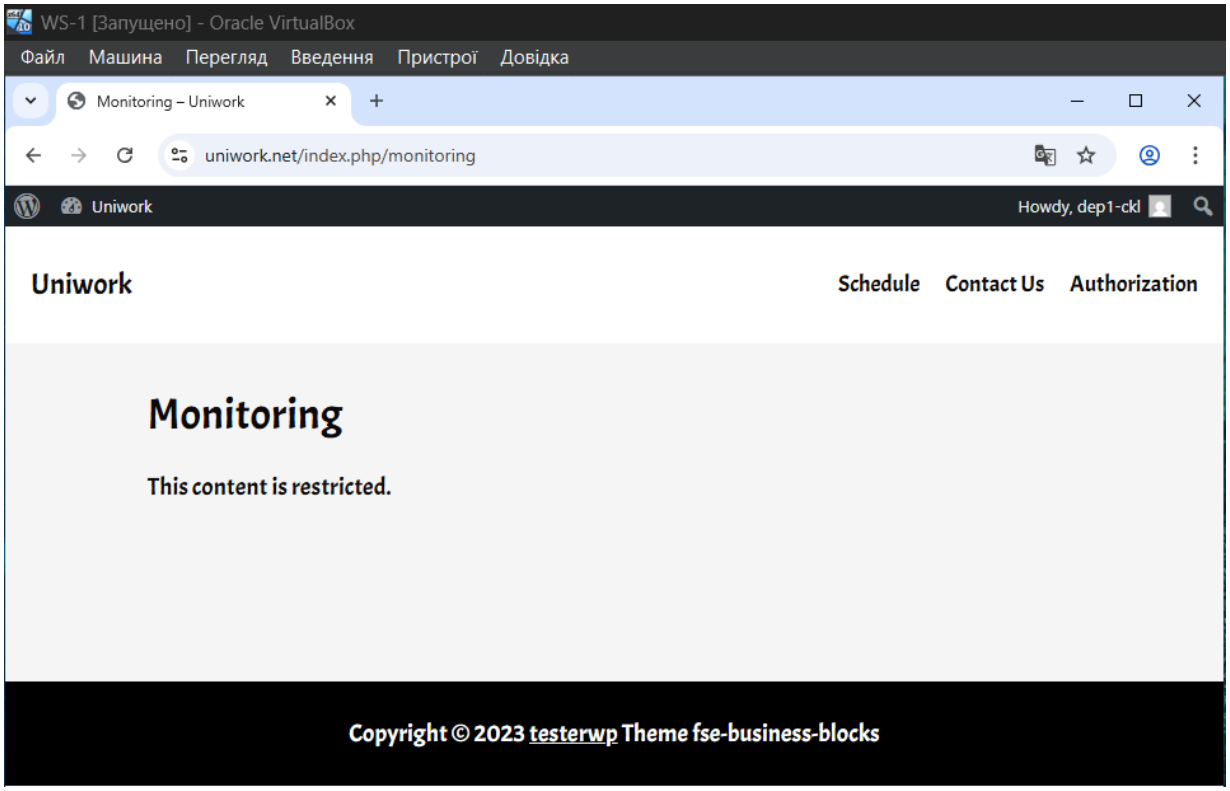


Рисунок 3.4.9 – Перегляд сторінки Monitoring

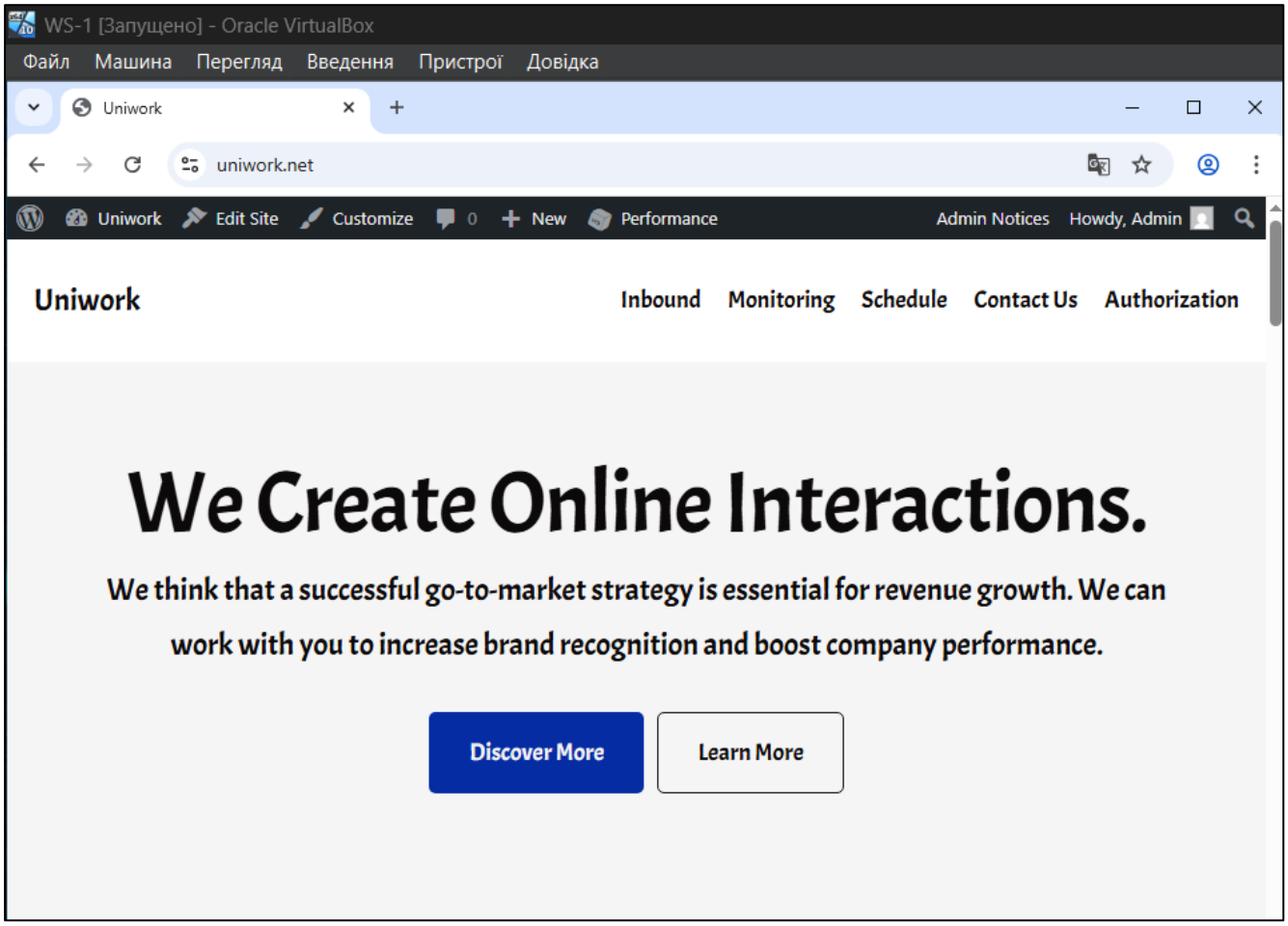


Рисунок 3.4.10 – Вигляд сайту в ролі Admin

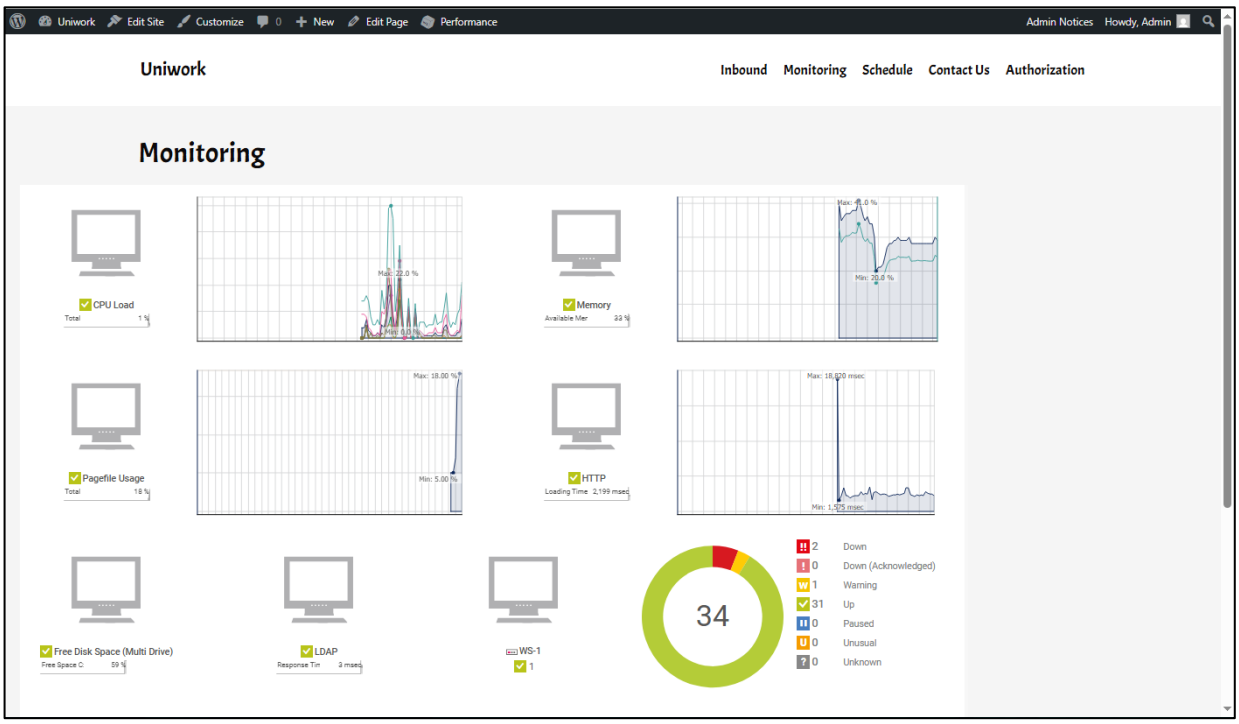


Рисунок 3.4.11 – Сторінка Monitoring

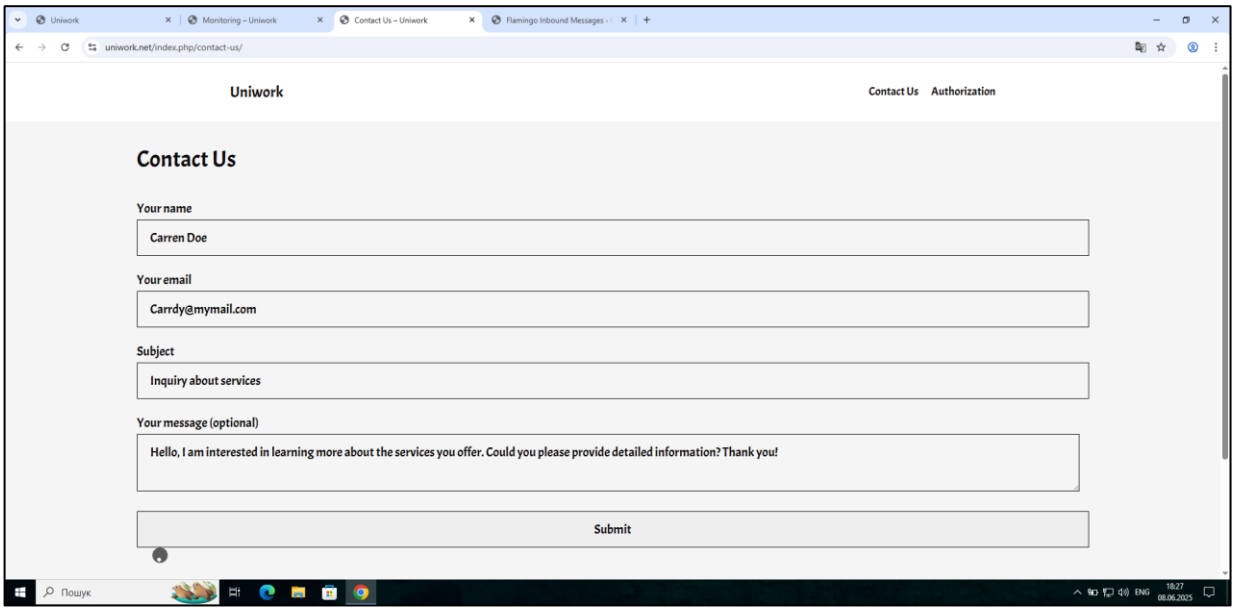


Рисунок 3.4.12 – Сторінка для контакту

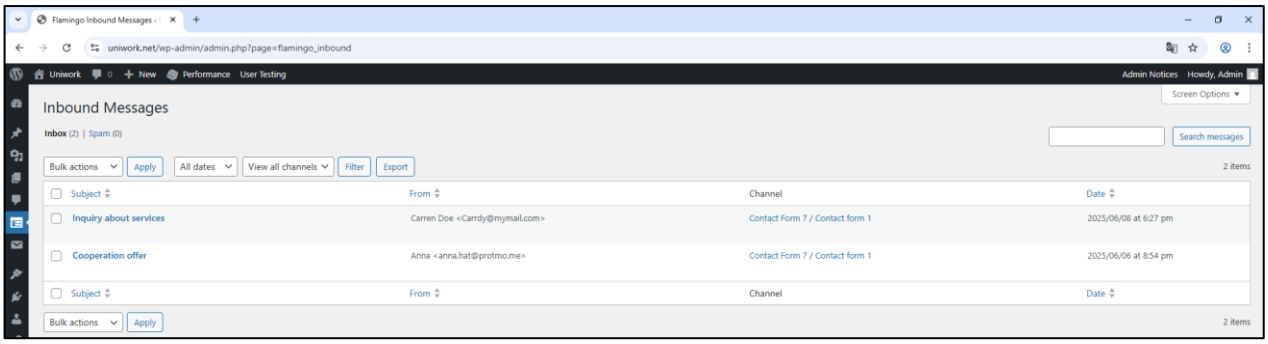


Рисунок 3.4.13 – Перегляд отриманих повідомлень від користувачів

Висновки до третього розділу

У третьому розділі було реалізовано практичну частину проєкту, яка включає налаштування доменної інфраструктури, розгортання служби моніторингу, створення публічного веб-порталу та проведення тестування всіх компонентів.

Насамперед було налаштовано сервер Windows Server 2019 з ролями Active Directory, DNS, DHCP та IIS, що забезпечило основу для створення доменної структури з організаційними одиницями та обліковими записами. Далі була встановлена система моніторингу PRTG Network Monitor, яка успішно інтегрувалась у середовище та дозволила в режимі реального часу контролювати стан інфраструктури.

Особливу увагу було приділено налаштуванню веб-порталу на базі CMS WordPress із підтримкою автентифікації користувачів через LDAP-протокол. В результаті реалізовано інтеграцію з Active Directory, автоматичне створення локальних облікових записів WordPress на основі доменних даних, а також механізми обмеження доступу до вмісту сайту відповідно до ролей користувачів. Створено типові сценарії використання порталу, що підтвердили працездатність і ефективність розробленої системи.

Проведене тестування показало коректну взаємодію всіх компонентів: доменна інфраструктура працює стабільно, LDAP-автентифікація реалізована успішно, а контроль доступу до сторінок порталу здійснюється відповідно до заданих політик безпеки.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було повністю досягнуто поставлену мету — створення публічного веб-порталу організації з централізованим керуванням доступом на основі служби Active Directory. Реалізовано доменну інфраструктуру на платформі Windows Server з логічною структурою облікових записів, організаційних одиниць і групових політик.

Веб-портал, побудований на базі CMS WordPress, інтегровано з Active Directory за допомогою LDAP-протоколу. Це забезпечило єдину точку автентифікації користувачів, автоматичне створення облікових записів WordPress на основі доменних даних, а також гнучке розмежування доступу до вмісту порталу відповідно до ролей користувачів. Для контролю працездатності інфраструктури було впроваджено систему моніторингу PRTG Network Monitor з відображенням критичних подій у режимі реального часу.

Проведене тестування підтвердило правильність налаштувань і стабільну взаємодію всіх компонентів. Запропоноване рішення демонструє ефективність поєднання сучасних веб-технологій із централізованим управлінням у доменному середовищі, а також може бути адаптоване для потреб навчальних закладів, державних і приватних організацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What Is Active Directory? (AD) - Definition, Benefits & More | Proofpoint AU [Електронний ресурс] // Proofpoint. – Режим доступу: https://www.proofpoint.com/au/threat-reference/active-directory.
2. Active Directory Domain Services overview [Електронний ресурс] // Microsoft Learn: Build skills that open doors in your career. – Режим доступу: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview.
3. Lightweight Directory Access Protocol (LDAP) - NETWORK ENCYCLOPEDIA [Електронний ресурс] // NETWORK ENCYCLOPEDIA. – Режим доступу: https://networkencyclopedia.com/lightweight-directory-access-protocol-ldap/.
4. Що таке автентифікація LDAP? [Електронний ресурс] // Hideez. – Режим доступу: https://hideez.bakotech.com/ua/ldap-saml.
5. Mikac E. LDAP Port 389 vs 636 [Електронний ресурс] / Erik Mikac // CBT Nuggets. – Режим доступу: https://www.cbtnuggets.com/blog/technology/networking/ldap-port-389-vs-636.
6. Як встановити та налаштувати IIS - [Електронний ресурс] // HostZealot. – Режим доступу: https://www.hostzealot.com.ua/blog/how-to/yak-vstanoviti-ta-nalashtuvati-iis.
7. What Is IIS and How Does It Work? - IT Glossary | SolarWinds [Електронний ресурс] // SolarWinds. – Режим доступу: https://www.solarwinds.com/resources/it-glossary/iis-server.
8. Інструмент створення блогів, платформа для публікацій і CMS [Електронний ресурс] // WordPress.org Україна. – Режим доступу: https://uk.wordpress.org/.
9. Joomla! - Content Management System to build websites & apps [Електронний ресурс] // Joomla!. – Режим доступу: https://www.joomla.org/about-joomla.html.
10. Orchard Core Documentation [Електронний ресурс] // Orchard Core Documentation. – Режим доступу: https://docs.orchardcore.net/en/latest/.

11. Serdyukov O. Огляд безкоштовних програм моніторингу серверів [Електронний ресурс] / Oleg Serdyukov // United DC. – Режим доступу: https://unit-eddc.net.ua/news/i/net-monitoring/?srsltid=AfmBOory9w9UovGTj-9Rw7z2Qo5ofC5GQWhx337lWPN-y8D09XHyog7y.
12. PRTG Network Monitor – All-in-one network monitoring tool [Електронний ресурс] // Paessler - The Monitoring Experts. – Режим доступу: https://www.paessler.com/prtg/prtg-network-monitor.
13. Zabbix: Що це і як ним користуватися [Електронний ресурс] // ALexHost SRL. – Режим доступу: https://alexhost.com/uk/faq/zabbix-what-it-is-and-how-to-use-it/.
14. About Nagios Core · Nagios Core Documentation [Електронний ресурс] // Nagios Enterprises. – Режим доступу: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/about.html.
15. LDAP Login For Intranet Sites | WordPress LDAP Plugin [Електронний ресурс] // Plugins - miniOrange. – Режим доступу: https://plugins.miniorange.com/wordpress-ldap-login-intranet-sites.
16. Vacca J. R. Computer and Information Security Handbook / John R. Vacca. – [Б. м.] : Elsevier Science & Technology Books, 2017. – 1280 с.
17. Active Directory Administration Cookbook: Actionable, Proven Solutions to Identity Management and Authentication on Servers and in the Cloud. – [Б. м.] : Packt Publishing, Limited, 2019. – 620 с.
18. Burge S. How to Use LDAP for WordPress User Accounts [Електронний ресурс] / Steve Burge // PublishPress. – Режим доступу: https://publishpress.com/blog/wordpress-sso/wordpress-ldap/.
19. Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map [Електронний ресурс] / ред. K. Zeilenga. – [Б. м.] : RFC Editor, 2006. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc4510.
20. Порівняння WordPress vs Joomla: що краще для вашого сайту [Електронний ресурс] // Wonder Web. – Режим доступу: https://wonder-web.com.ua/blog/porivnyannya-wordpress-vs-joomla-scho-krasche-dlya-vashogo-saytu/.

21. Shahriar H. LDAP Vulnerability Detection in Web Applications [Електронний ресурс] / Hossain Shahriar, // International Journal of Secure Software Engineering. – 2017. – Т. 8, № 4. – С. 31–50. – Режим доступу: https://doi.org/10.4018/ijsse.2017100102.

ДОДАТКИ

Додаток А
Створення локального центру сертифікації

Server-1 [Запущено] - Oracle VirtualBox

Файл Машина Перегляд Введення Пристрої Довідка

Administrator: C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\LocalCA>mkdir certs,crl,newcerts,private

C:\LocalCA>type nul > C:\LocalCA\index.txt

C:\LocalCA>echo 1000 > C:\LocalCA\serial

C:\LocalCA>_
```

C:\LocalCA\openssl.cnf - Notepad++ [Administrator]

Файл Редагувати Пошук Подання Кодування Мова Налаштування Інструменти Макрос Виконати Плагіни Вікно ?

php.ini openssl.cnf

```
[ ca ]
default_ca = CA_default

[ CA_default ]
dir = C:/LocalCA
database = $dir/index.txt
new_certs_dir = $dir/newcerts
certificate = $dir/cacert.pem
serial = $dir/serial
private_key = $dir/private/cakey.pem
default_days = 3650
default_md = sha256
policy = policy_loose
x509_extensions = v3_ca

[ policy_loose ]
commonName = supplied

[ req ]
default_bits = 2048
prompt = no
default_md = sha256
distinguished_name = dn

[ dn ]
C = UA
ST = Zhytomyr
L = Zhytomyr
O = Uniwork
OU = IT
CN = Uniwork Local CA

[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign
```

Server-1 [Запущено] - Oracle VirtualBox

Файл Машина Перегляд Введення Пристрої Довідка

C:\LocalCA\uniwork.cnf - Notepad++ [Administrator]

Файл Редагувати Пошук Подання Кодування Мова Налаштування Інструменти Макрос Виконати Плагіни Вікно ?

php.ini | openssl.cnf | uniwork.cnf

```
[ req ]
default_bits = 2048
prompt = no
default_md = sha256
distinguished_name = dn
req_extensions = req_ext

[ dn ]
C = UA
ST = Zhytomyr
L = Zhytomyr
O = Uniwork
OU = Web
CN = uniwork.net

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = uniwork.net
DNS.2 = www.uniwork.net
```

Server-1 [Запущено] - Oracle VirtualBox

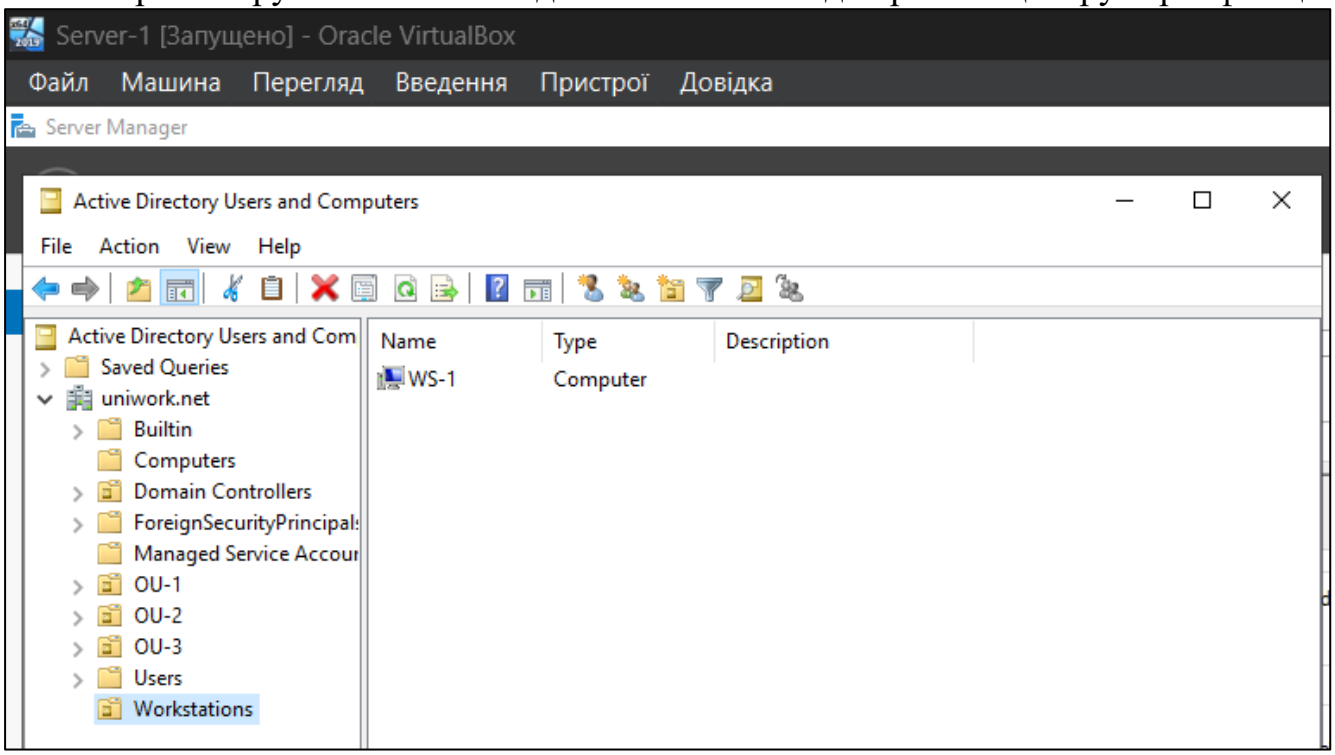
Файл Машина Перегляд Введення Пристрої Довідка

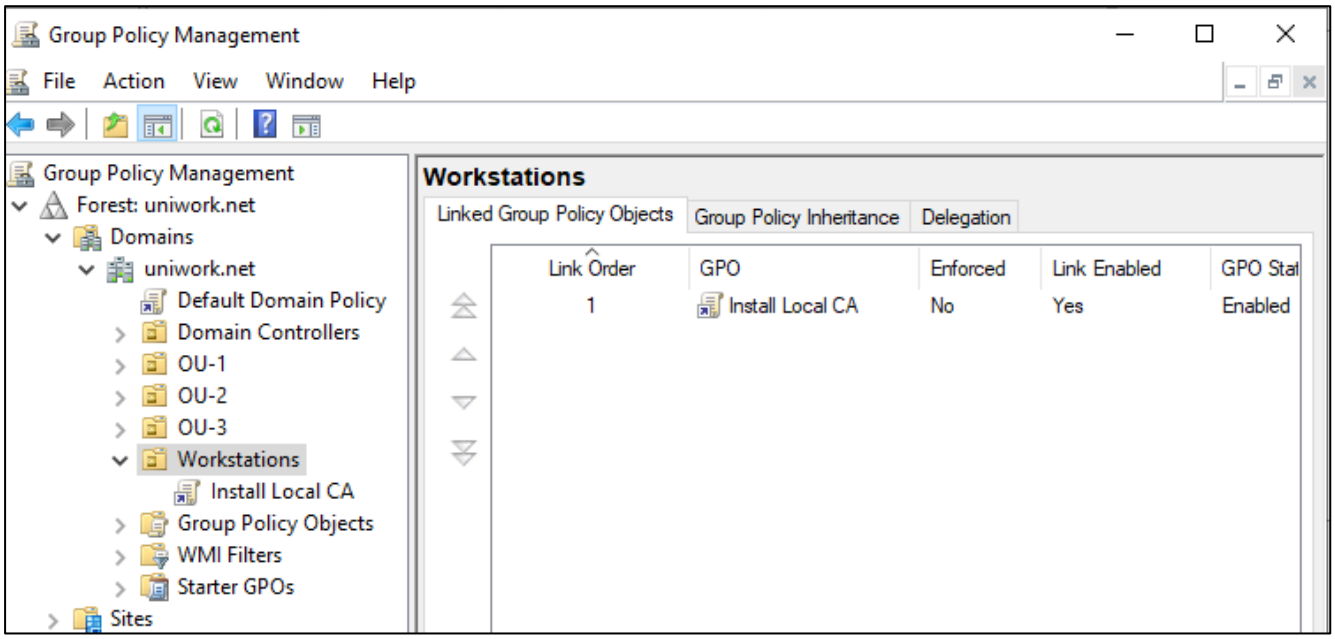
Administrator: C:\Windows\System32\cmd.exe

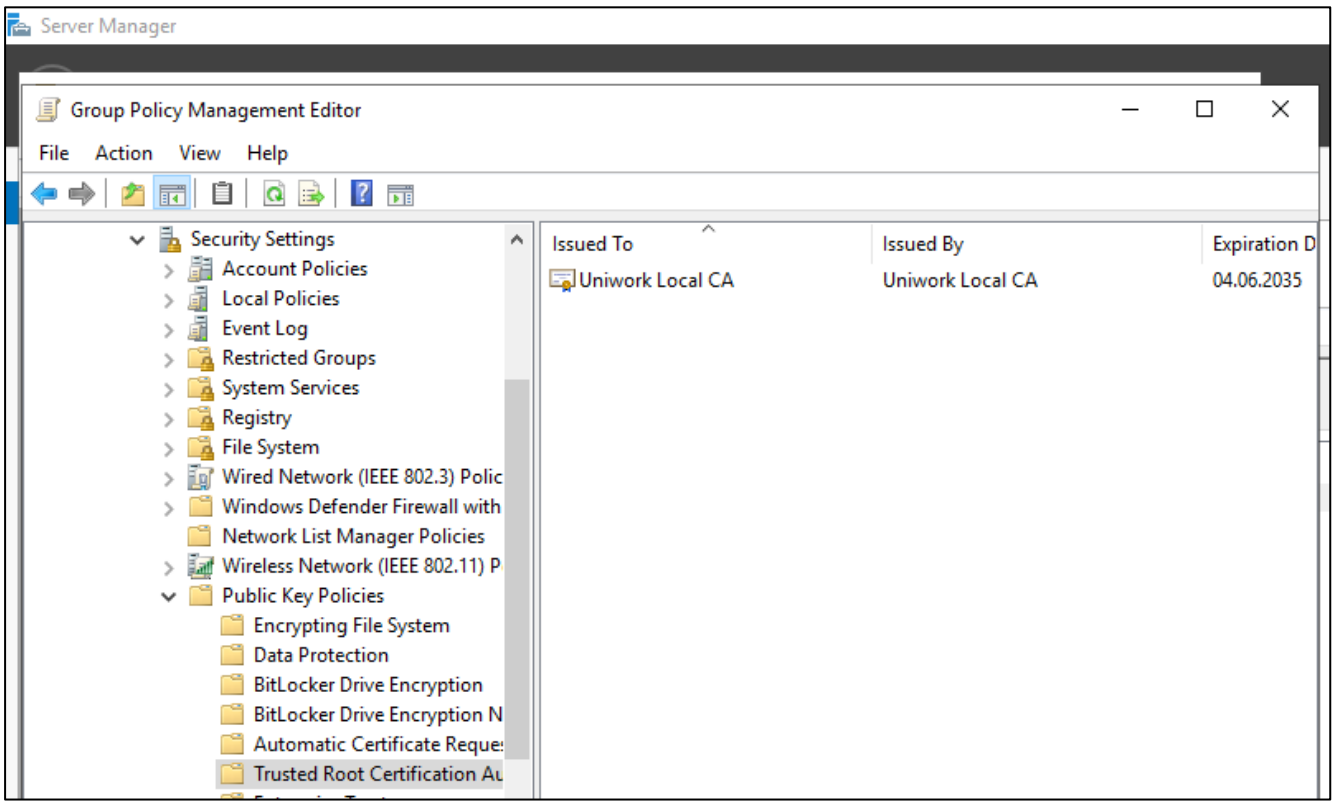
```
C:\LocalCA>openssl genrsa -out C:\LocalCA\private\cakey.pem 4096

C:\LocalCA>openssl req -config C:\LocalCA\openssl.cnf -key C:\LocalCA\private\cakey.pem -new -x509 -days 3650 -sha256 -out C:\LocalCA\cacert.pem

C:\LocalCA>
C:\LocalCA>openssl genrsa -out C:\LocalCA\uniwork.key 2048

C:\LocalCA>openssl req -new -key C:\LocalCA\uniwork.key -out C:\LocalCA\uniwork.csr -config C:\LocalCA\uniwork.cnf

C:\LocalCA>openssl x509 -req -in C:\LocalCA\uniwork.csr -CA C:\LocalCA\cacert.pem -CAkey C:\LocalCA\private\cakey.pem -CAcreateserial -out C:\Local
CA\uniwork.crt -days 825 -sha256 -extfile C:\LocalCA\uniwork.cnf -extensions req_ext
Certificate request self-signature ok
subject=C=UA, ST=Zhytomyr, L=Zhytomyr, O=Uniwork, OU=Web, CN=uniwork.net

C:\LocalCA>openssl pkcs12 -export -out uniwork.pfx -inkey uniwork.key -in uniwork.crt -certfile cacert.pem
Enter Export Password:
Verifying - Enter Export Password:

C:\LocalCA>_
```

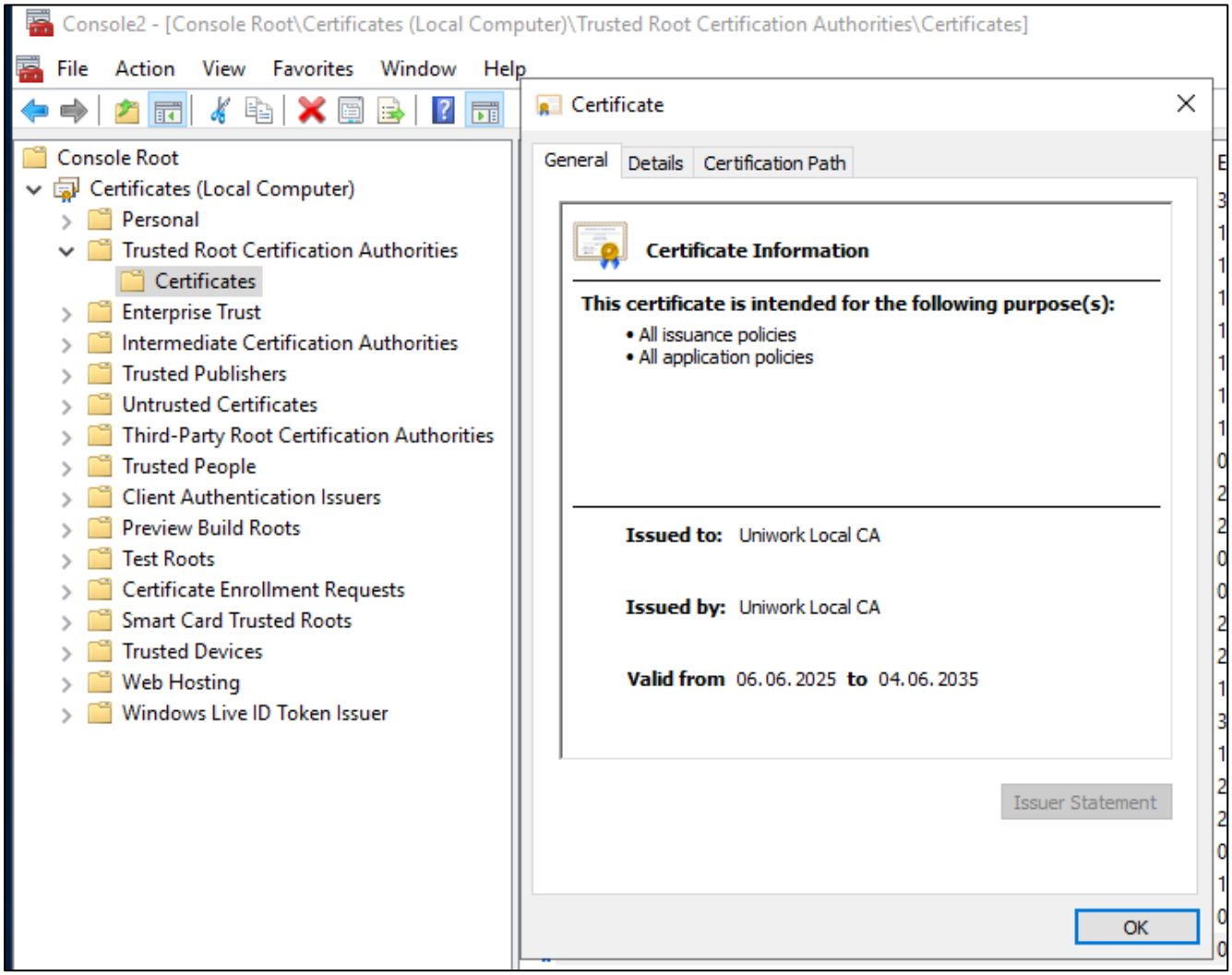
Додаток Б

Створення групової політики для встановлення довіреного центру сертифікації






Server Manager
Group Policy Management Editor
File Action View Help
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Polic
Windows Defender Firewall with
Network List Manager Policies
Wireless Network (IEEE 802.11) P
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption N
Automatic Certificate Reque
Trusted Root Certification Au
Issued To
Issued By
Expiration D
Uniwork Local CA
Uniwork Local CA
04.06.2035


Console2 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Issuer
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: Uniwork Local CA
Issued by: Uniwork Local CA
Valid from 06.06.2025 to 04.06.2035
Issuer Statement
OK

Додаток В
Права доступу користувачів

	Головна сторінка	Contact Us	Schedule	Monitoring
Admin	+	+	+	+
adUser	+	+	+	–
Публічний доступ	+	+	–	–