МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

І. М. Гаркуша

АДМІНІСТРУВАННЯ ОПЕРАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Методичні рекомендації до виконання лабораторних робіт
для здобувачів ступеня бакалавра освітньо-професійної програми
«Інформаційні системи та технології»
спеціальності 126 Інформаційні системи та технології

Дніпро
НТУ «ДП»
2025

Гаркуша І. М.

Адміністрування операційних систем та мереж [Електронний ресурс] : методичні рекомендації до виконання лабораторних робіт для здобувачів ступеня бакалавра освітньо-професійної програми «Інформаційні системи та технології» спеціальності 126 Інформаційні системи та технології / І. М. Гаркуша ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2025. – 61 с.

Автор
І. М. Гаркуша, канд. техн. наук, доц.

Затверджено науково-методичною комісією спеціальності F6 Інформаційні системи і технології (126 Інформаційні системи та технології) (протокол № 7 від 30.06.2025) за поданням кафедри інформаційних технологій та комп'ютерної інженерії (протокол № 17 від 30.06.2025).

Надані теоретичні відомості та практичні завдання, а також рекомендації щодо їх виконання. Поданий перелік рекомендованих джерел.

Орієнтовано на активізацію навчальної діяльності здобувачів ступеня бакалавра спеціальності 126 Інформаційні системи та технології, закріплення практичних навичок у засвоєнні дисципліни «Адміністрування операційних систем та мереж».

Відповідальний за випуск завідувач кафедри інформаційних технологій та комп'ютерної інженерії В. В. Гнатушенко, д-р техн. наук, проф.

ЗМІСТ

ВСТУП

Сучасний світ інформаційних технологій (IT) базується на рішеннях, які пов’язані з комп’ютерними мережами. Вони виступають інструментом комунікації бізнесу та обміну інформації. Тому значна увага в організаціях приділяється процесам, які пов’язані з ефективним, захищеним та надійним використанням різноманітних апаратно-програмних інформаційних систем користувачами, адмініструванням операційних середовищ та мережевого обладнання, адмініструванням користувачів та їх різноманітних ресурсів.

Множина сучасних серверних операційних систем (ОС) в організаціях для управління комп’ютерами та користувачами за декілька десятиліть вже майже склалася. На ринку сучасного серверного сегменту домінують GNU/Linux-сумісні ОС, серед яких можна виділити Ubuntu Server, Debian, Red Hat Enterprise Linux Server та сумісні рішення на його основі, рішення на базі openSUSE. Також в корпоративному сегменті активно використовуються рішення на базі MS Windows Server.

Методичні рекомендації до виконання робіт з практикуму є частиною курсу «Адміністрування операційних систем та мереж», який викладається в Національному технічному університеті «Дніпровська політехніка» здобувачам освітньо-професійної програми “Інформаційні системи та технології” першого (бакалаврського) рівня вищої освіти спеціальності 126 Інформаційні системи та технології у п’ятому семестрі третього курсу навчання.

Методичні рекомендації пропонують виконання шести лабораторних робіт. Роботи передбачають активне використання технологій віртуалізації на базі інструменту Oracle VirtualBox (або подібного за необхідності). В ході виконання робіт розглядаються питання встановлення та базового налаштування серверних ОС MS Windows Server (варіанти з GUI та Core), Ubuntu Server, а також питання налаштування мережевого екрану на базі рішень ОС IPFire, питання розгортання та підготовки Web-серверу Apache2.

Основна мета робіт – формування компетентностей щодо застосування процесів адміністрування в MS Windows Server, GNU/Linux-сумісних ОС та мереж під їх керуванням. Окрім встановлення, роботи передбачають набуття знань щодо використання певних засобів автоматизації на базі скриптових мов, отримання знань про певні команди налаштування серверної та клієнтської частин ОС при роботі з мережами, використання мережевих екранів.

Наприкінці методичних рекомендацій містяться критерії оцінювання та перелік рекомендованих сучасних літературних джерел.

Робота №1.
Встановлення та налаштування MS Windows Server з GUI

Мета роботи: встановити на віртуальну машину MS Windows Server з графічною оболонкою та виконати основні налаштування AD DS. Ознайомитися з процесом налаштування.

Теоретично-практична частина

Розглянемо послідовність встановлення та налаштувань MS Windows Server на прикладі версії 2025. Передбачається, що на хостовій машині встановлений продукт віртуалізації Oracle VirtualBox (для MS Windows або GNU/Linux-сумісних ОС) або UTM (для платформи Apple macOS).

Встановлення MS Windows Server відбувається з офіційного ISO-образу компанії Microsoft, період функціонування якого обмежений терміном у 180 діб.

Офіційний ISO-образ із MS Windows Server можна завантажити або з офіційного серверу Microsoft, або із внутрішньої хмари дистанційного курсу.

Для встановлення MS Windows Server 2025 оберіть файл:

```
26100.1742.240906-0331.ge_release_svc_refresh_SERVER_EVAL_x64FRE_en-us.iso
```

Для встановлення MS Windows Server 2019 (у разі, якщо встановлення 2025 версії неможливо з технічних обставин) оберіть файл:

```
17763.379.190312-0539.rs5_release_svc_refresh_SERVER_EVAL_x64FRE_en-us.iso
```

Встановлення в Oracle VirtualBox робити у режимі *Skip Unattended Installation*. Назва віртуальної машини, наприклад: *Windows_Server_2025_GUI*.

При створенні віртуальної машини потрібно подбати про хоча б два процесорних ядра та 4096 Гб оперативної пам’яті для розгортання MS Windows Server. Також перед встановленням увімкнути опцію процесора PAE/NX, увімкнути опцію використання кешу контролером введення/виведення хосту. Всі інші опції для Oracle VirtualBox можна залишити за замовченням.

При встановленні MS Windows Server 2025 врахувати опції:

– Time and currency format: Ukrainian (Ukraine);

– Keyboard or input method: US;

– I would like to: Install Windows Server; відмітьте опцію: “I agree everything ...”;

– Select Image: Windows Server 2025 Standard Evaluation (Desktop Experience) – обрання варіанту із графічним інтерфейсом користувача (із GUI – **G**raphical **U**ser **I**nterface);

– Select location to install Windows Server: Create Partition, обрати: Disk 0 Partition 2.

Після виконання цих кроків, розпочніть встановлення, натиснувши на кнопку *Install*.

Після перезавантаження, очікуйте перших кроків налаштування (це займає певний час). ISO-диск залишайте. Завантаження здійснюйте не з ISO-образу, а вже з віртуального диску.

Після повторного перезавантаження, вкажіть складний, комплексний пароль для користувача із ім'ям *Administrator*. Наприклад:

```
#123&456ms
```

та натисніть на кнопку *Finish*. Після процедури встановлення ОС розблокуйте екран входу в систему комбінацією швидких клавіш Host+Del (або використайте меню вікна VirtualBox – *Введення \ Клавіатура \ Вставити Ctrl+Alt+Del)* та здійсніть вхід (логін) у систему під вбудованим обліковим записом *Administrator*.

При відкритті вікна *Send diagnostic data to Microsoft*, натисніть кнопку *Accept*. У підсумку буде здійснено вхід у систему та автоматично відкриється засіб *Server Manager* (рис. 1.1).

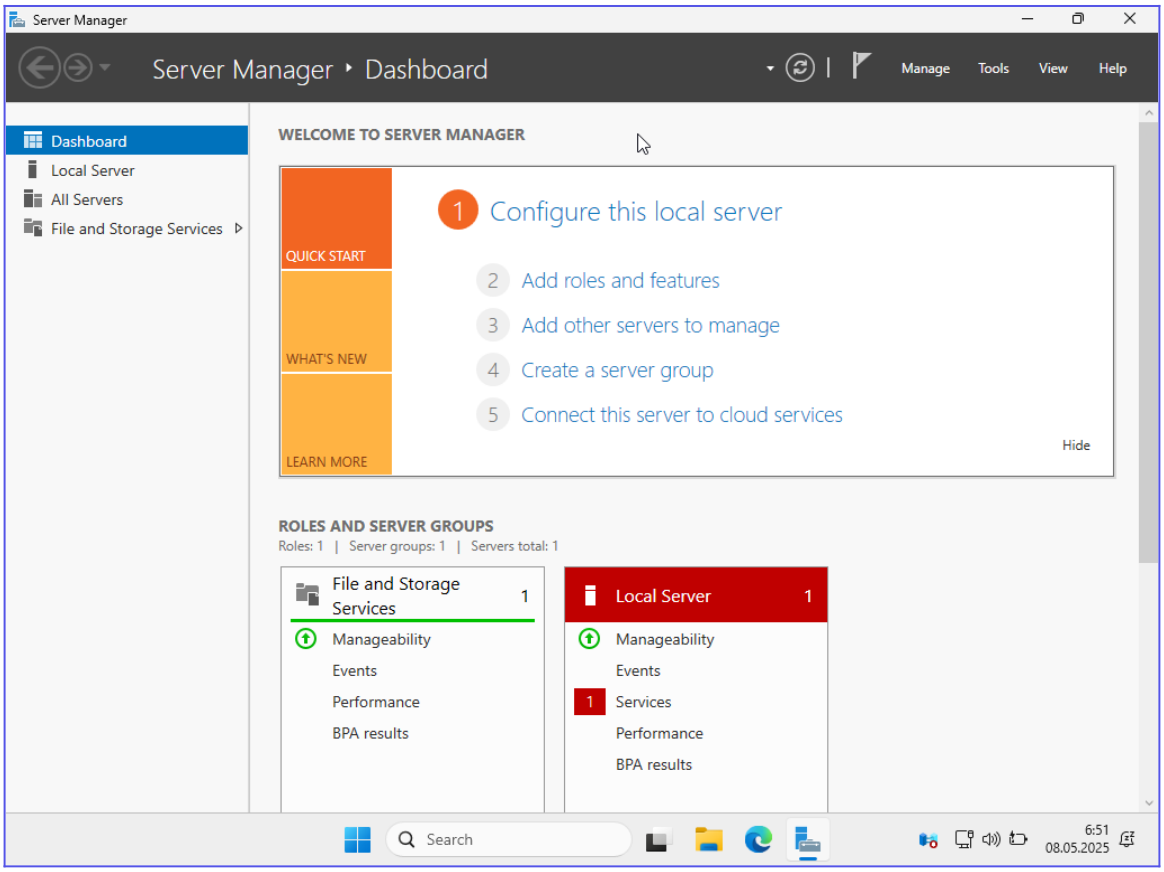


Рис. 1.1. Вікно *Server Manager* при першому вході в ОС MS Windows Server

Встановіть гостьові доповнення Oracle VirtualBox через пункт меню *Пристрої \ Встановити гостьові доповнення* (рис. 1.2). Після встановлення та перезавантаження повинна з'явитися можливість зміни розрізнення екрану MS Windows Server.

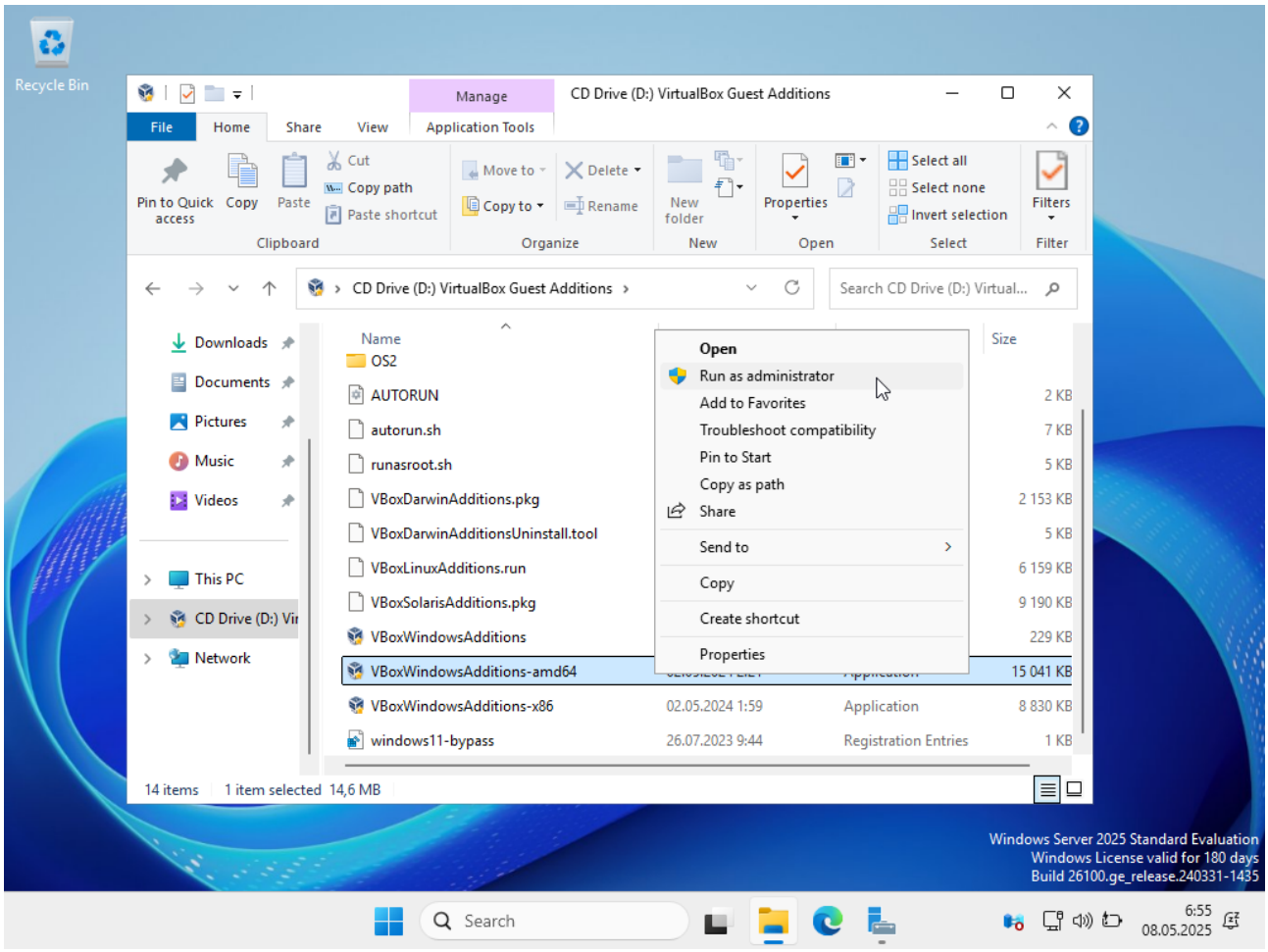


Рис. 1.2. Встановлення гостьових доповнень Oracle VirtualBox

Натисніть праву кнопку миші на кнопці *Start* та оберіть пункт меню *Settings*. У вікні налаштувань оберіть *Windows Update* та з налаштувань основної частини вікна в *Pause updates* вкажіть період оновлень: *Extend for 4 weeks*.

У вікні налаштувань оберіть *Time & language*. В основній частині вікна натисніть на *Time zone*. У списку *Time zone* нижче, оберіть часову зону: *UTC+02:00 Helsinki, Kyiv, Riga... .*

Підготуємо сервер до встановлення *Active Directory Domain Services* (AD DS).

Перейменуємо гостьову систему. У вікні *Settings* оберіть *System* та трошки нижче назви системи за замовченням натисніть на посилання *Rename*.

У вікні перейменування задайте нове ім’я для комп’ютера, наприклад, **PDC** (скорочення від **P**rimary **D**omain **C**ontroller – основний контролер домену) та натисніть кнопку *Next* і далі на кнопку *Restart now.*

Після перезавантаження, завершіть роботу сервера та поверніться до налаштувань встановленої віртуальної машини в Oracle VirtualBox. Оберіть опції мережі, приєднайте мережевий адаптер до внутрішньої мережі (ім’я: **intnet**) та закрийте вікно налаштувань віртуальної машини.

Виконайте запуск Windows Server. Після логіну, відкрийте вікно *Settings*, оберіть пункт *Network & internet* та групу налаштувань *Ethernet*.

В пункті *IP assignment* натисніть кнопку *Edit* та змініть налаштування IPv4 адреси мережевого інтерфейсу: оберіть варіант *manual*, увімкніть IPv4 та в якості IP-адреси вкажіть адресу 10.0.0.1, а в якості маски підмережі: 255.255.255.0. Натисніть на кнопку *Save* та закрийте вікно налаштувань. Можна перевірити налаштування мережевого інтерфейсу командою *ipconfig* (рис. 1.3). Зверніть увагу, що з часом всі служби сервера стартують (рис. 1.3) – відсутні червоні повідомлення. Сервер працює в режимі локального автономного серверу.

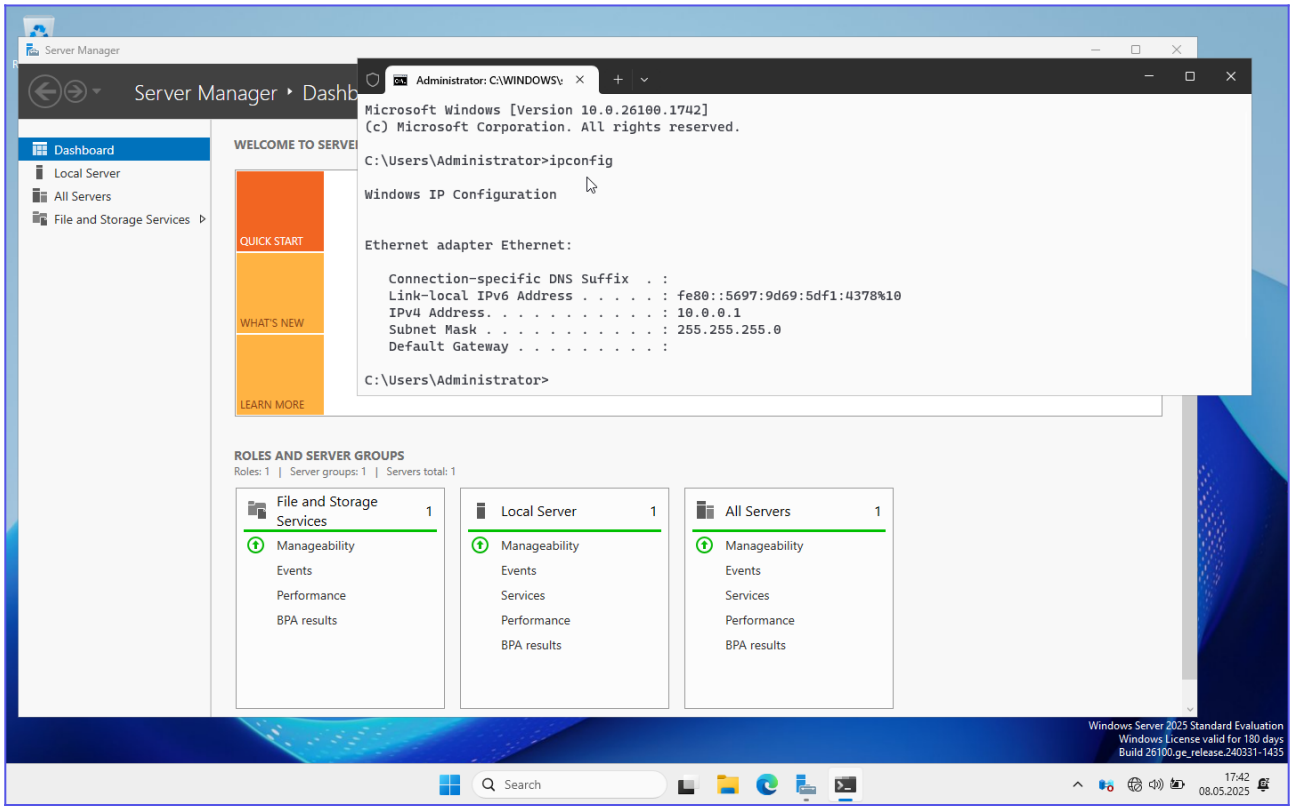


Рис. 1.3. Перевірка налаштувань мережевого інтерфейсу

В частині вікна *Dashboard* програми *Server Manager*, натисніть на пункт *Add roles and features* (додавання ролей та особливостей). У помічнику обрання ролей та особливостей з опціями за замовчуванням, оберіть крок *Server Roles*

(кроки помічника відмічаються справа) та відмітьте опції *Active Directory Domain Services* (натисніть на кнопку *Add Features* для підтвердження), оберіть опцію встановлення *DNS Server* (натисніть на кнопку *Add Features* для підтвердження), натисніть на кнопку *Next*. Пропустіть крок обрання додаткових особливостей (натисніть *Next*).

Погодьтеся з наступним кроком помічника-майстра щодо встановлення AD DS ролі (натисніть *Next*). Погодьтеся з наступним кроком щодо встановлення служби DNS на сервері (натисніть *Next*).

Відмітьте опції щодо дозволу на автоматичне перезавантаження – *Restart the destination server automatically if required* та натисніть на кнопку *Install*. В процесі встановлення ролей, помічник повідомить, що адміністратор може закрите його вікно та дивитися сповіщення за спеціальною кнопкою із прапорцем у верхній правій частині вікна *Server Manager*. З часом буде надіслано сповіщення щодо можливості надання цьому серверу статусу контролера домену (рис. 1.4).

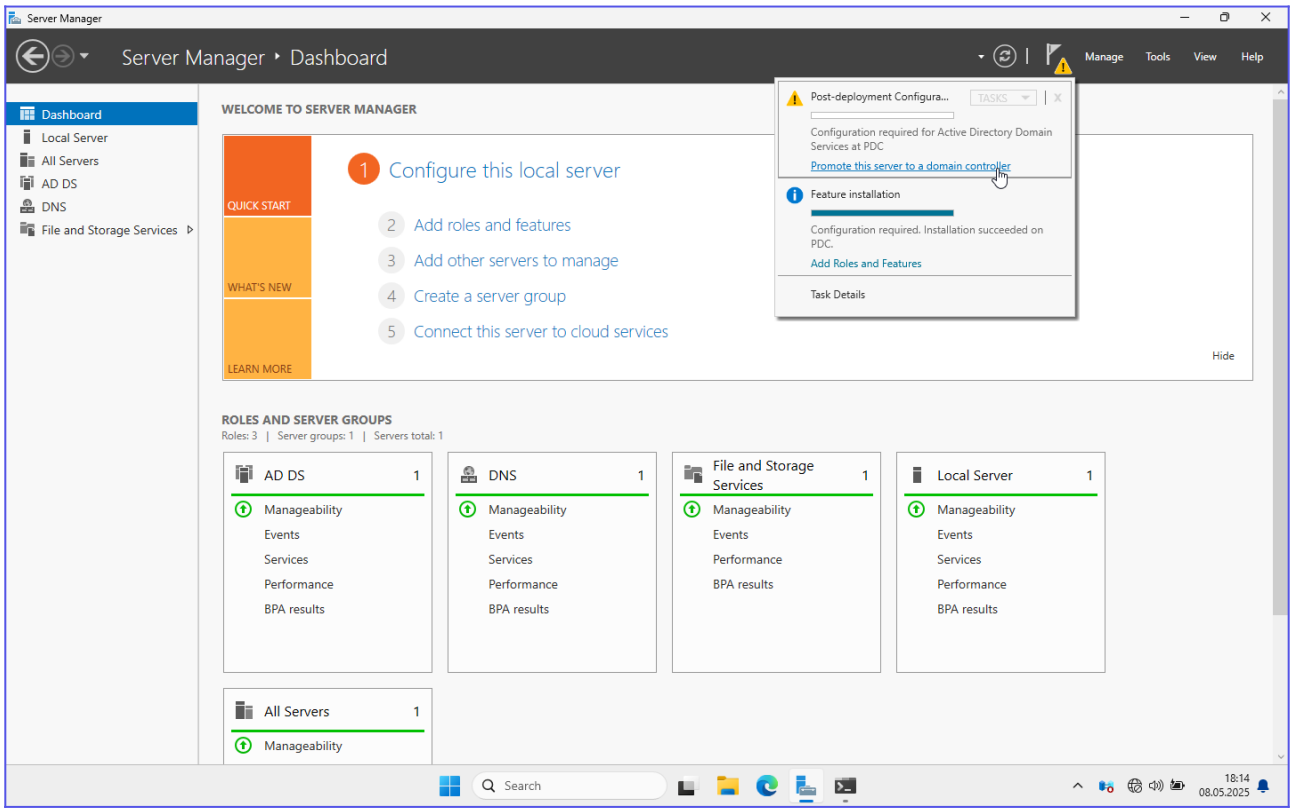


Рис. 1.4. Повідомлення щодо надання серверу статусу контролера домену

При обранні цього пункту повідомлення відкривається вікно помічника для подальшого конфігурування. Будуть надані три можливості створення контролера домену з врахуванням:

– додавання цього контролера до наявного домену;

– додавання нового домену до наявного лісу доменів (ієрархічної множини доменів);

– додавання в новий ліс.

Тобто, якщо контролер домену створюється у мережі вперше і до нього ніякого іншого контролера не існувало і відповідно не існувало домену чи відсутня ієрархія у вигляді лісу, то тоді обирається третій варіант. Далі обов'язково потрібно вказати *Root domain name* у формі символьного доменного імені ієрархічної структури. Наприклад:

```
mydomain.org
```

Далі потрібно вказати та підтвердити пароль для сервісу режиму відновлення служб каталогів.

На наступному кроці можна проігнорувати сповіщення, щодо DNS, оскільки сервер з вказаними налаштуваннями мережі не буде бачити DNS верхнього рівня.

В якості NetBIOS-імені буде задано скорочене ім'я: *MYDOMAIN*, з яким можна погодитися.

На наступному кроці помічника конфігурування будуть вказані каталоги з розташуванням бази даних AD DS. Це дуже важливі каталоги й адміністратор обов'язково повинен знати їх розташування.

На передзавершальному кроці помічник налаштування надає можливість зберегти всі вказані значення опцій конфігурування в окремому скрипті мовою Windows PowerShell. За бажанням адміністратор може зберегти цей скрипт для власних потреб (кнопка *View script*).

Після натискання на кнопку *Next* йде перевірка налаштувань, по завершенню якої стане доступна кнопка *Install*. Після натискання на неї розпочинається процес створення та налаштування контролера домену та AD DS. На цьому етапі нічого відмінити вже не можна. Після перезавантаження сервер набуває статусу контролера домену із відповідними можливостями. Процес переведення серверу в статус контролера домену буде займати певний час.

Вхід в систему буде містити назву домену. Наприклад, вхід під обліковим записом адміністратора домену: `MYDOMAIN\Administrator`.

Після встановлення AD DS та контролера домену, можна перейти до виконання подальших налаштувань, наприклад, сервера DNS.

Завдання

Використовуючи знання, які отримані з лекцій та з теоретично-практичної частини роботи, виконати встановлення MS Windows Server 2025 в середовищі Oracle VirtualBox (або у подібному, наприклад, UTM для платформи Apple macOS із врахуванням її особливостей конфігурування). У разі технічної неможливості встановлення версії MS Windows Server 2025, в якості альтернативи, можна обрати для встановлення версію MS Windows Server 2019. В якості імені сервера обрати ім'я *PDC* та мережеві налаштування, що були описані в теоретично-практичній частині роботи.

Примітка: у разі виконання роботи в комп'ютерному класі, потрібно з'ясувати у викладача, в який каталог виконувати збереження віртуальної машини із всіма її файлами. Це робиться обов'язково, оскільки профілі звичайних користувачів в комп'ютерних класах мають гостьові властивості (тобто налаштовані віртуальні машини після завершення роботи будуть втрачені). Для подальшого збереження створених віртуальних машин викладач відводить спеціальний каталог.

Після встановлення MS Windows Server, виконати розгортання служб AD DS та DNS нового домену у новому лісі. В якості імені домену обрати ім'я *mydomain.org*.

Використовуючи матеріали лекцій, після завершення налаштування AD DS, за допомогою утиліти *Active Directory Users and Computers*, створити користувача домену із ім'ям *student*.

Відобразити у звіті основні кроки налаштування ОС. Продемонструвати викладачу результати налаштувань. Правила оформлення звіту подані у додатку А.

Робота №2.
Встановлення та налаштування MS Windows Server Core

Мета роботи: встановити на віртуальну машину MS Windows Server у варіанті Core (без графічної оболонки) та розгорнути на ньому DNS-сервер та резервний контролер домену. Підключити в домен робочу станцію на базі ОС MS Windows.

Теоретично-практична частина

При встановленні MS Windows Server в Oracle VirtualBox використовуйте схожі початкові налаштування віртуальної машини за виключенням: кількість пам'яті для функціонування віртуальної машини: 2048 Мб, налаштування мережі – приєднайте мережевий адаптер до внутрішньої мережі (ім'я: **intnet**).

На початку встановлення MS Windows Server, на етапі *Select Image*, оберіть редакцію: *Windows Server 2025 Standard Evaluation* – встановлення варіанту Core серверу без графічного інтерфейсу користувача (без GUI). Всі інші налаштування аналогічні тим, що були розглянуті в роботі №1.

Після перезавантаження, задайте пароль користувача *Administrator* у вікні із текстовим інтерфейсом користувача (TUI – Text User Interface).

На етапі запиту *Send Diagnostic data to Microsoft*, оберіть *Required*.

Далі буде запущена утиліта конфігурування серверу *SConfig* (Server Configuration) – рис. 2.1.

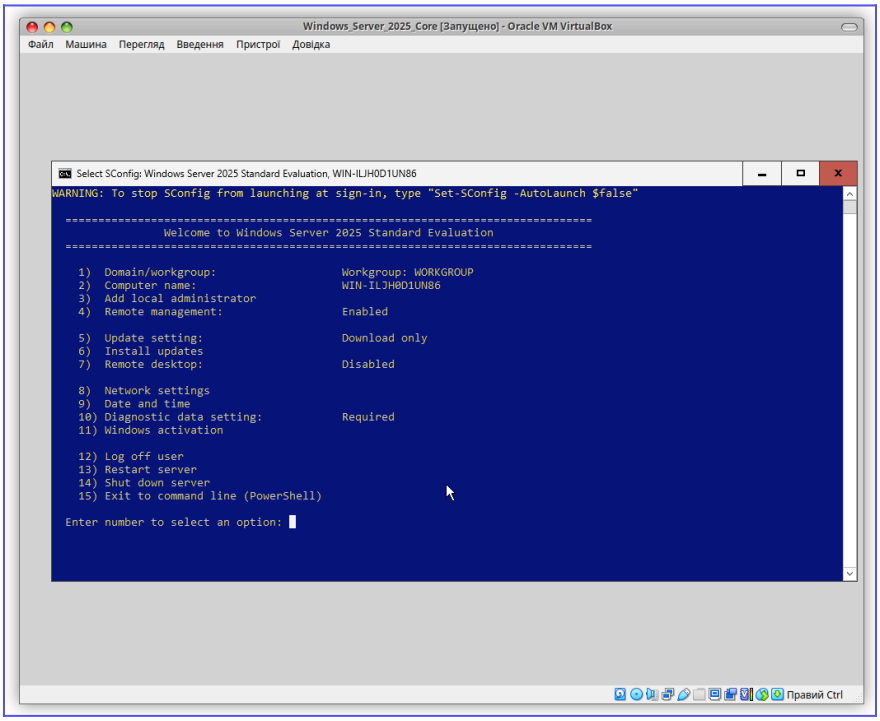


Рис. 2.1. Конфігурування MS Windows Server Core через *SConfig* (кольорова палітра змінена)

Введіть у рядку *Enter number to select an option* значення 2 (*Computer Name*). На запит *Enter new computer name*, введіть ***srv2*** та натисніть на клавішу *Enter*. Виконайте перезавантаження. Після перезавантаження та входу в систему, у 2025 версії серверу у варіанті Core автоматично запуститься *SConfig*.

Далі введіть значення 8 (*Network Settings*). Введіть індекс мережевого адаптеру (наприклад, 4) та далі оберіть опцію 1 (*Set network adapter address*). Далі на запит *(D)HCP or (S)tatic IP address*, введіть S. Якщо IP-адреса серверу з роботи №1 була задана як 10.0.0.1 з маскою 255.255.255.0, то введіть IP-адресу 10.0.0.2 та натисніть на *Enter*. Введіть відповідну маску підмережі – 255.255.255.0, натисніть на *Enter*. Введіть IP-адресу шлюзу за замовченням – 10.0.0.1 та натисніть на *Enter* (буде змінена у наступній роботі). Якщо все гаразд з налаштуваннями, *SConfig* виведе відповідні повідомлення. Натисніть *Enter* для продовження.

Наступним пунктом для конфігурування, серед пунктів налаштування мережі, оберіть 2 (*Set DNS servers*). На запит *Enter* 1*st DNS server*, введіть 10.0.0.1 та натисніть на *Enter*. На запит *Enter* 2*nd DNS server*, введіть 10.0.0.2 та натисніть на *Enter*. На запит *Enter* 3*rd DNS server* – натисніть на *Enter* та повторно на *Enter* для переходу до підменю налаштування мережі.

У рядку *Enter selection* натисніть на *Enter* для переходу у головне меню *SConfig*. Далі введіть значення 13 (*Restart server*) та підтвердіть перезавантаження.

Після логіну в систему під адміністратором, вийдіть із засобу *SConfig*, обравши пункт 15 (*Exit to command line*) та у командному рядку Windows PowerShell введіть команду (регістр символів не має значення):

```
Set-SConfig -AutoLaunch $false
```

Команда вимкне можливість запускати *SConfig* автоматично при кожному вході в систему під адміністратором.

Запустіть віртуальну машину із сервером, який був встановлений у роботі №1. Після його запуску, перейдіть в командний рядок хосту *SRV2* та виконайте перевірку мережевого з’єднання командою:

```
ping 10.0.0.1
```

Зверніть увагу, що *ping* для MS Windows Server Core за замовченням заблокований, тобто команда `ping 10.0.0.2` з серверу *PDC* нічого не дасть – порт для ICMP Echo на *SRV2* за замовченням закритий.

Приєднаємо сервер *SRV2* до домену *mydomain.org*. Для цього виконайте у командному рядку *SRV2* команду:

```
sconfig
```

Оберіть для конфігурування пункт 1 (*Domain/workgroup*).

На запит *Join (D)omain or (W)orkgroup*, введіть D та натисніть *Enter*. Далі введіть ім'я домену: *mydomain.org* та знов натисніть на *Enter*. На запит *Specify an authorized domain\user*, введіть ім'я адміністратора домену: *mydomain\administrator* та натисніть *Enter*. Далі введіть пароль адміністратора домену. Підтвердіть перезавантаження. У разі запиту на введення нового імені комп'ютера – натисніть *Enter*.

Оберіть пункт 13 (*Restart Server*) для виконання перезавантаження.

Виконайте вхід від адміністратора домену в оточення MS Windows Server з GUI. Скористайтеся меню *Tools* програми *Server Manager* та відкрийте інструмент *Active Directory Users and Computers*. Переконайтеся, що у гілці *Computers* з'явився хост *SRV2* (рис. 2.2).

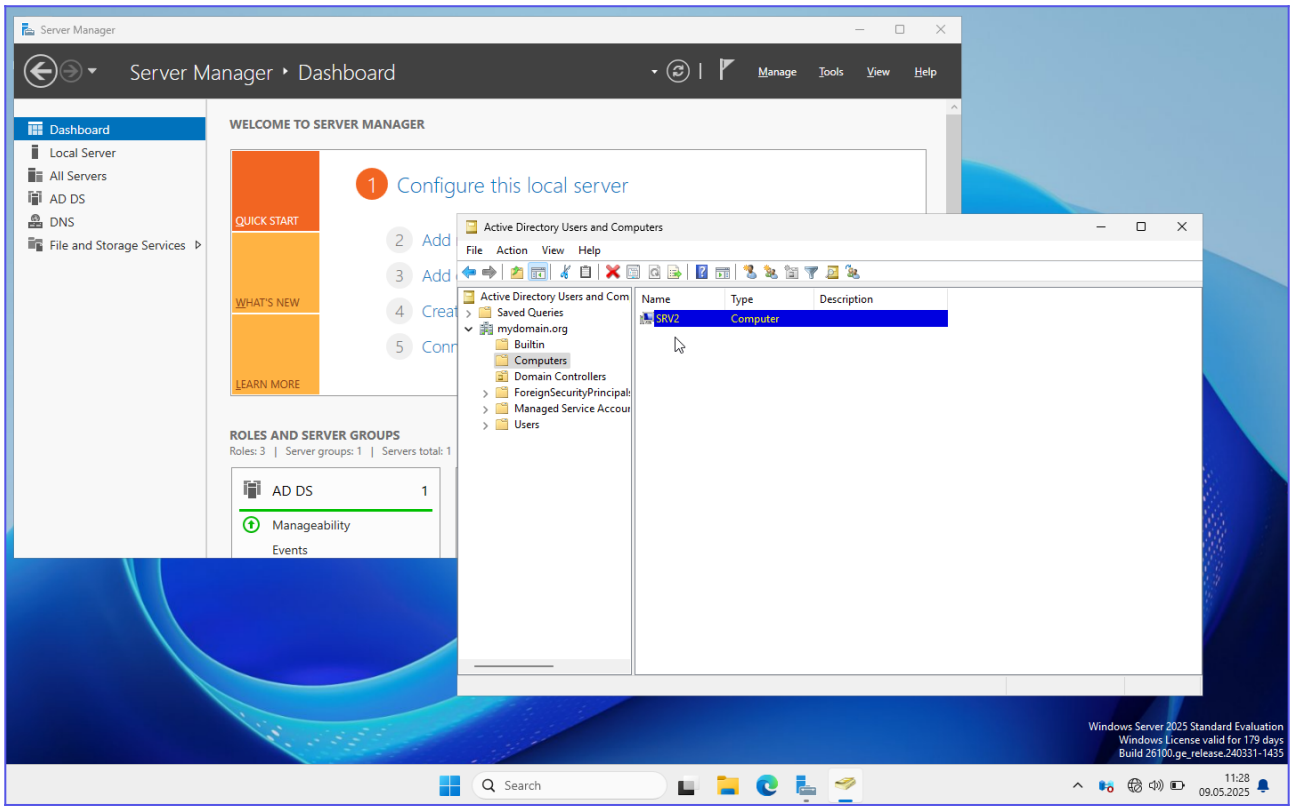


Рис. 2.2. Результат додавання в домен комп'ютера з ім'ям *SRV2*

Додамо можливість віддаленого конфігурування MS Windows Server Core через засіб *Server Manager*.

Перейдіть до *Server Manager* та натисніть праву кнопку миші на пункті *All Servers*. Оберіть пункт меню *Add Servers* (рис. 2.3).

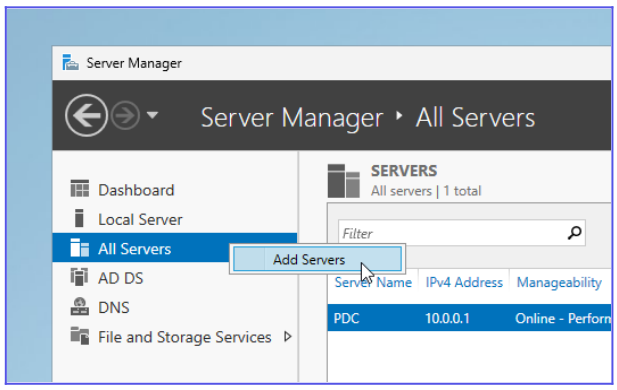


Рис. 2.3. Пункт меню додавання серверу до списку серверів

В діалоговому вікні додавання серверу, в полі *Name (CN)* введіть *srv2* та натисніть кнопку *Find Now*. Після появи *srv2* у списку, оберіть його та натисніть на кнопку із зображенням стрілки вправо для додавання у список. Після цього натисніть на кнопку OK та дочекайтеся завершення процедури додавання у список серверів.

Відкрийте контекстне меню *SRV2* зі списку серверів та оберіть пункт меню *Add Roles and Features* (рис. 2.4). Оберіть та виконайте встановлення на Core-сервері служб AD DS та DNS.

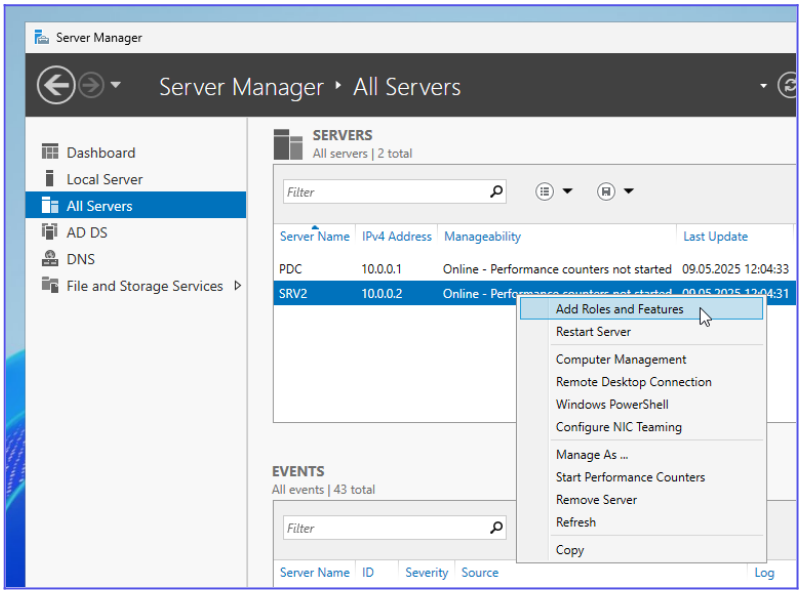


Рис. 2.4. Контекстне меню із пунктами віддаленого управління вибраним сервером

Слідкуйте за станом прапорця у правій верхній частині *Server Manager* та натисніть, коли буде сповіщення для SRV2, на посилання *Promote this server to a domain controller.*

В процесі встановлення, оберіть варіант *Add a domain controller to an existing domain*. При цьому потрібно скористатися кнопкою *Change*, щоб вказати користувача із повноваженнями адміністратора.

Виконайте наступні кроки так, як і в роботі №1. Тільки на кроці, де потрібно вказати з якого контролеру домену треба виконувати реплікацію (*Replicate from*), оберіть *PDC.mydomain.org*.

Після завершення процедури встановлення, дочекатися перезавантаження *SRV2* та процедури виконання налаштування (*Applying computer settings*) на ньому.

Зверніть увагу, що стала відпрацьовувати команда `ping 10.0.0.2` для *SRV2* від *PDC*, оскільки із встановленням серверу стали доступні певні служби, які потребують відкриття протоколу ICMP Echo, наприклад, *File and Printer Sharing*.

Також зверніть увагу на те, що в *Active Directory Users and Computers*, сервер *SRV2* перейшов у гілку *Domain Controllers* (рис. 2.5).

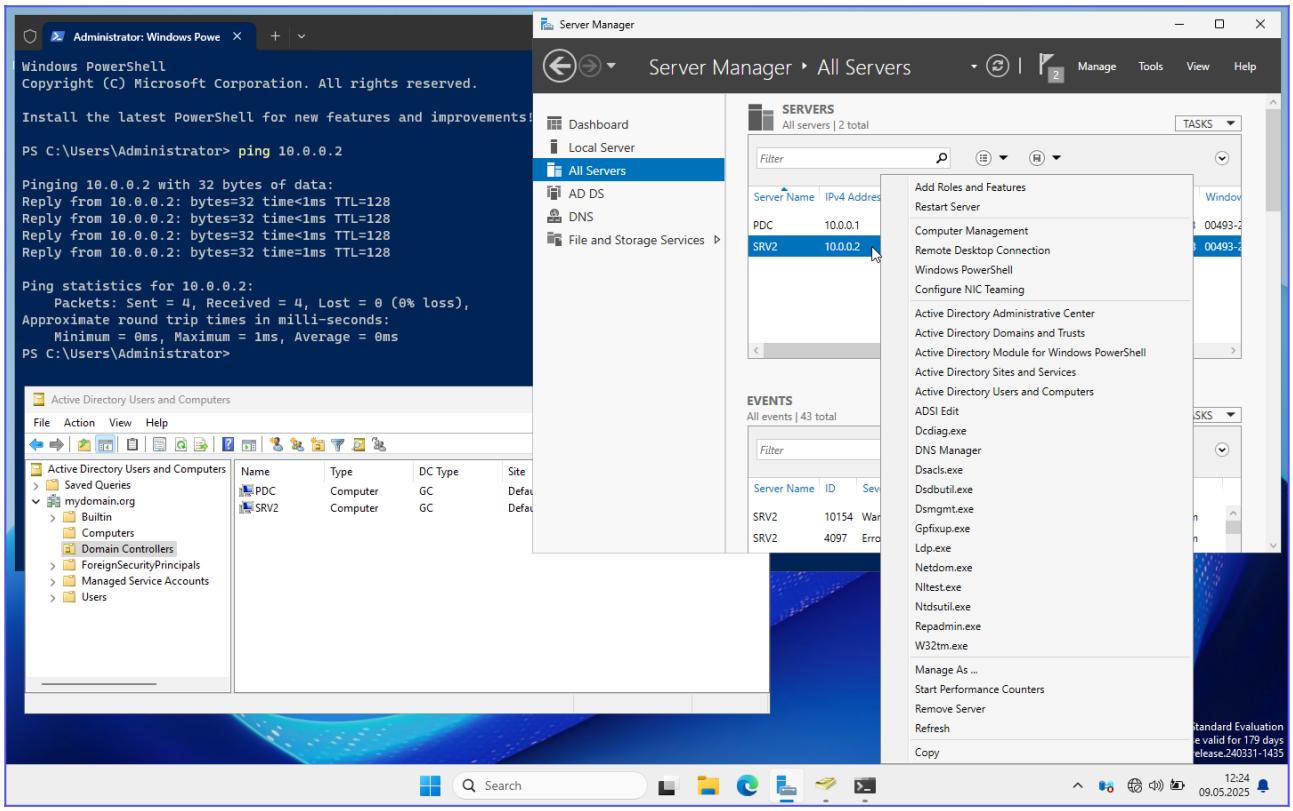


Рис. 2.5. Результат створення на сервері *SRV2* контролеру домену *mydomain.org*

При роботі із командним рядком MS Windows Server Core виникають ситуації, коли потрібно швидко перезавантажити або завершити роботу сервера. Це виконується, наприклад, командами: `shutdown /r` (швидке

перезавантаження), `shutdown /r /t 0` (швидке перезавантаження без очікування), `shutdown /p` (завершення роботи).

Після перезавантаження, етап *Applying computer settings* може зайняти певний час.

Завдання

1. Використовуючи теоретично-практичну частину роботи, виконати встановлення MS Windows Server 2025 без графічної оболонки, налаштувати його та встановити AD DS з DNS, створити на базі нього резервний контролер домену *mydomain.org*.

2. Використовуючи ISO-образ з MS Windows 10, встановити пробну версію на віртуальну машину (Language: *English*, Time and currency format: *Ukrainian (Ukraine)*, Keyboard or input method: *Ukrainian*). Дати ім'я комп'ютеру: *Win10*, IP-адресу: 10.0.0.3 та включити її в домен *mydomain.org*. Ім'я ISO-файлу офіційного пробного образу (пробна ліцензія на 90 діб, рис. 2.6), що доступна в хмарі курсу:

`19045.2006.220908-0225.22h2_release_svc_refresh_CLIENTENTERPRISEEVAL_OEMRET_x64FRE_en-us.iso`

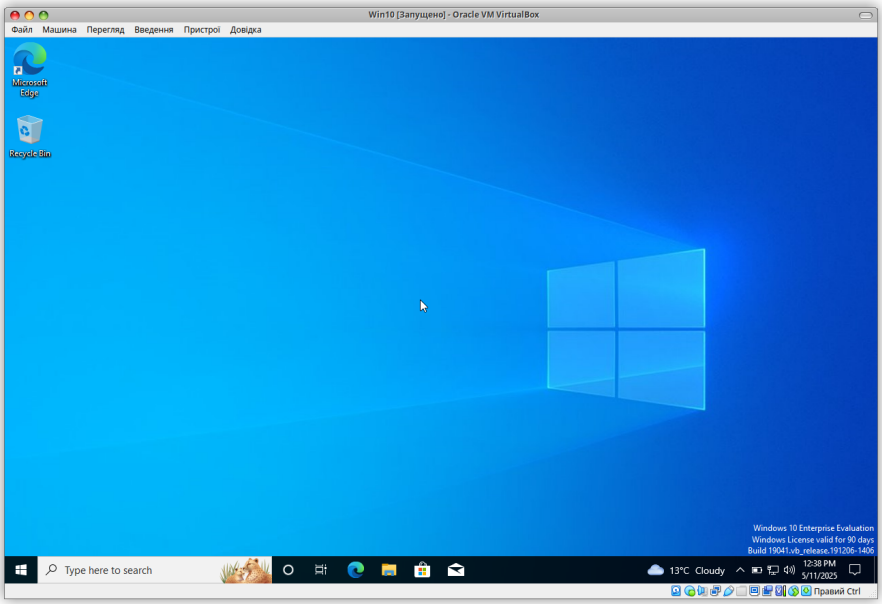


Рис. 2.6. Головний екран офіційної пробної версії Windows 10 після встановлення

Відобразити у звіті основні кроки налаштування ОС. Продемонструвати викладачу результати налаштування. Правила оформлення звіту подані у додатку А.

При захисті роботи володіти знаннями для відповіді на питання викладача за матеріалами лекцій та теоретично-практичної частини роботи.

Робота №3.
Розгортання та налаштування шлюзового хосту та мережевого екрану

Мета роботи: встановити на віртуальну машину дистрибутив IPFire. Налаштувати підтримку мережевого екрану між внутрішньою віртуальною мережею та Internet.

Теоретично-практична частина

Встановлення проводиться з ISO-файлу образа диску з IPFire із хмари курсу. Ім’я файлу:

```
ipfire-2.29-core194-x86_64.iso
```

Останні роки дистрибутив IPFire є досить популярним серверним рішенням на базі ядра Linux, що включає різноманітні серверні служби (наприклад: DNS, DHCP, Proxy Server та ін.). Головне призначення цього дистрибутиву – виконання маршрутизації та створення мережевих екранів.

При встановленні в Oracle VirtualBox вказати тип ОС: Linux, версія: Other Linux (64-bit), об’єм пам’яті: 512 Мб, кількість ядер CPU: 1, розмір дискового простору: 8 Гб, увімкнути опцію процесора PAE/NX, віртуальний оптичний пристрій створити на інтерфейсі SATA. Увімкнути опцію використання кешу контролером введення/виведення хосту. Під’єднати перший мережевий адаптер до внутрішньої мережі (**intnet**), а другий – до проміжного адаптеру, який пов’язаний з реальним мережевим адаптером, що має фізичне з’єднання з мережею Internet.

При налаштуванні мережі у VirtualBox, в якості типу першого мережевого адаптеру оберіть Intel PRO/1000 MT Desktop (82540EM), а в якості другого: PCnet-FAST III (Am79C973). Це дасть змогу в подальшому розрізнити мережеві інтерфейси при їх налаштуваннях для роботи мережевого екрану.

В якості мови для встановлення IPFire залишити *English*. В якості файлової системи, обрати *ext4*. Після основного етапу встановлення, виконати перезавантаження, обрати розкладку клавіатури *us*. В якості Time zone, обрати *Europe/Kyiv*. Назва гостьового хосту – ***ipfire***. Назва локального домену – *mydomain.org*. Паролі для користувачів *root* та *admin* повинні бути складні. Наприклад: `#123&456ms`.

На етапі конфігурування мережі, оберіть пункт меню *Drivers and card assignment* при поточній конфігурації для мережевого екрану GREEN+RED.

Для GREEN-інтерфейсу оберіть мережевий адаптер 82540EM, а для RED-інтерфейсу: 79C97x.

Таким чином, GREEN-інтерфейс буде прив'язаний до внутрішньої мережі, що створена у VirtualBox – **intnet**, а RED-інтерфейс буде зв'язаний із мережею Internet.

Оберіть пункт меню *Address settings* при поточній конфігурації для мережевого екрану GREEN+RED.

Задайте такі налаштування IPv4 для GREEN-інтерфейсу:

IP address: 10.0.0.254

Network mask: 255.255.255.0

Для RED-інтерфейсу оберіть режим *DHCP* (якщо зовнішня адреса не пов'язана із пристроєм, на якому працює DHCP-сервер, то потрібно буде обрати інші власні налаштування).

Після мережевих налаштувань виконують налаштування вбудованого серверу *DHCP*. На цьому етапі його можна не вмикати, завершити налаштування та перезавантажити IPFire-хост.

Завантажте MS Windows Server з GUI та в налаштуваннях мережевого адаптеру вкажіть IP-адресу шлюзової машини: 10.0.0.254 (рис. 3.1). Після цього дочекайтеся встановлення Internet-з'єднання та перевірте зв'язок з певним Internet-вузлом, увівши його IP-адресу або символьне ім'я.

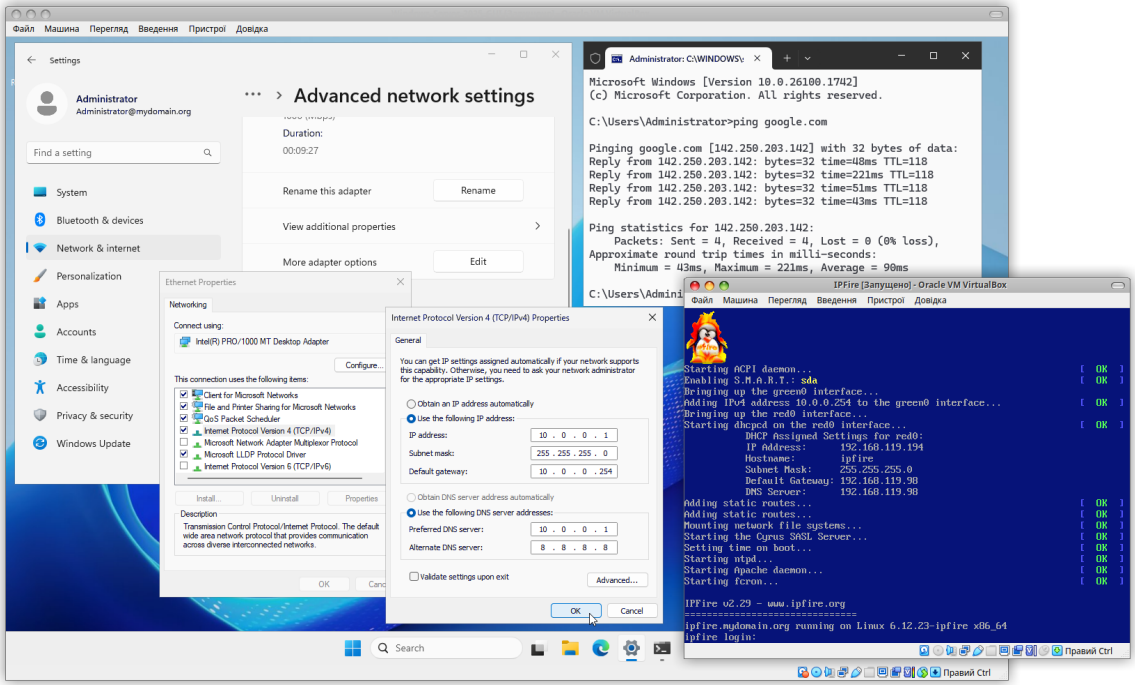


Рис. 3.1. Встановлення IP-адреси шлюзової машини та перевірка Internet-з'єднання

Примітка: в командному рядку Windows PowerShell для швидкого виведення мережевих налаштувань використовуйте команду `ipconfig`, а для швидкого призначення шлюзу наступного набору команд у режимі адміністратора (перша команда покаже ім'я мережевого інтерфейсу для виконання наступної команди; символ ‘`’ дозволяє формувати довгі рядки з перенесенням на новий рядок):

```
netsh interface show intefrace

netsh interface ipv4 set address name="Ethernet" `
static 10.0.0.1 255.255.255.0 10.0.0.254

netsh interface ipv4 show address
```

Для подальшого зручного конфігурування IPFire в MS Windows відкрийте Internet-браузер та введіть такий URL: https://10.0.0.254:444/. Адміністративний вхід у Web-консоль IPFire здійснюється від користувача *admin* з визначеним раніше паролем (рис. 3.2).

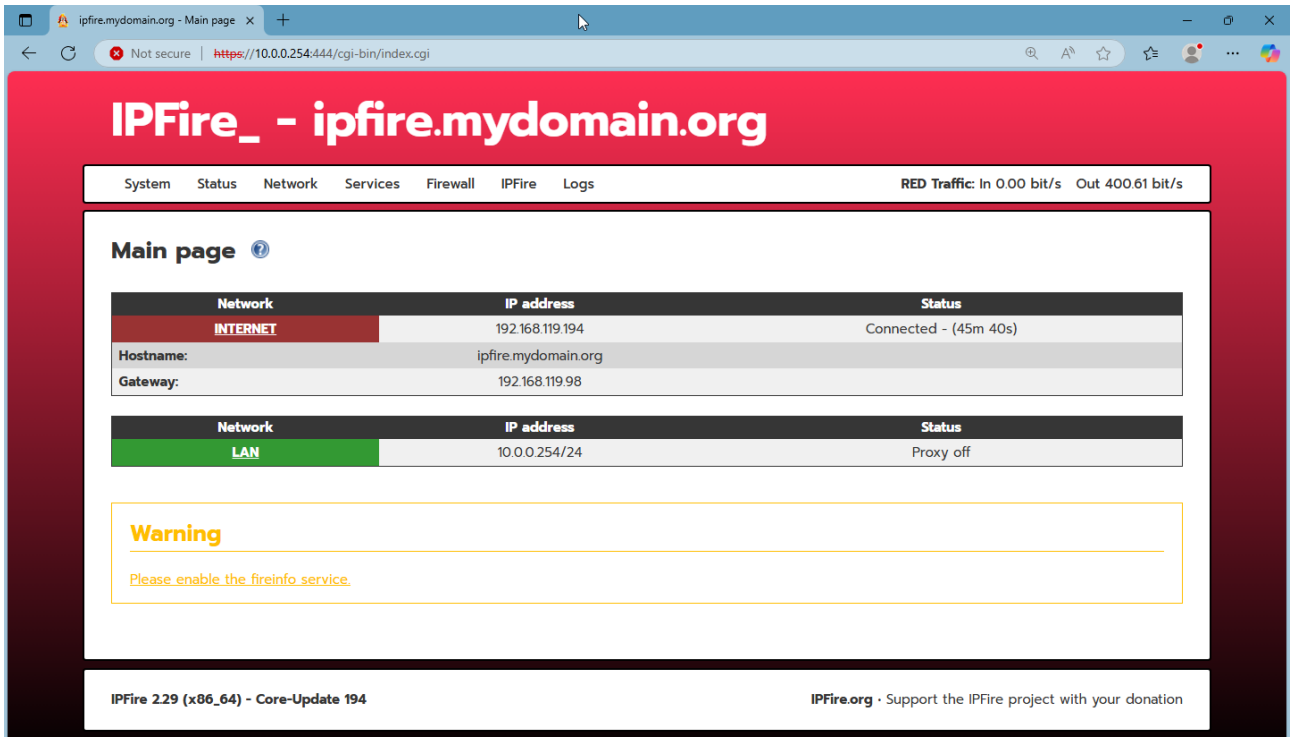


Рис. 3.2. Web-консоль управління IPFire

Налаштування мережевого екрану містяться у меню *Firewall*. Важливою частиною є логування. Управління цим процесом йде на різних рівнях. Наприклад, можна увімкнути логування певних відхилень пакетів через опції пункту меню *Firewall \ Firewall Options* – група опцій *Firewall logging*.

Важливим є пункт меню *Firewall \ Firewall Rules*. На цій сторінці можна задавати різноманітні правила керування мережевим екраном. Наприклад, нехай потрібно повністю заблокувати процедуру перевірки доступності зовнішніх хостів через протокол ICMP (приклад – утиліта ping). Для цього достатньо створити нове правило, де в частині *Protocol* обрати протокол *ICMP*, а в частині типу протоколу – *echo-request*. Далі обрати опцію *DROP* та в додаткових правилах вказати, наприклад, позицію правила, активувати роль та увімкнути логування. Після цього додати нове правило натиснувши на кнопку *Add*.

За замовченням включено правило блокування всіх outgoing-з'єднань по 25-му порту протокола TCP. Цей порт використовується протоколом *SMTP* (Simple Mail Transfer Protocol) для передавання електронної пошти між поштовими серверами Internet.

Серед правил роботи мережевого екрану є також режим NAT (Network Address Translation), який дозволяє змінювати IP-адресу в заголовках пакетів при проходженні через маршрутизатор IPFire та підвищувати таким чином захищеність внутрішньої мережі.

Завдання

1. Здійснити встановлення дистрибутиву IPFire в оточені Oracle VirtualBox з двома мережевими адаптерами (один для GREEN-, інший для RED-інтерфейсу).

2. Встановити IP-адресу шлюзу в налаштуваннях мережевих адаптерів хостів *PDC*, *SRV2*, *Win10*.

3. Увімкнути NAT в IPFire.

Описати у звіті основні кроки налаштування IPFire. Продемонструвати викладачу результати налаштувань. Правила оформлення звіту подані у додатку А.

При захисті роботи володіти знаннями для відповіді на питання викладача за матеріалами лекцій та теоретично-практичної частини роботи.

Робота №4.
Встановлення та налаштування Ubuntu Server

Мета роботи: встановити на віртуальну машину Ubuntu Server. Розгорнути підтримку декількох користувачів через SSH-сеанс.

Теоретично-практична частина

Встановлення проводиться з ISO-файлу образа диску з Ubuntu Server 24.04.2 LTS із хмари курсу:

```
ubuntu-24.04.2-live-server-amd64.iso
```

Встановлення в Oracle VirtualBox робити у режимі *Skip Unattended Installation*. Задати назву віртуальної машини як *Ubuntu_Server_24_04*.

При встановлені Ubuntu Server на віртуальну машину вказати два ядра процесору, увімкнути опцію процесора PAE/NX, 15 Гб розмір диску, 2048 Мб оперативної пам'яті (або більше за бажанням). Віртуальний оптичний пристрій створити на інтерфейсі SATA. Увімкнути опцію використання кешу контролером введення/виведення хосту. Під'єднати мережевий адаптер до *NAT* у VirtualBox.

На етапі встановлення оберіть в якості мови *English* з такою ж розкладкою за замовченням. Не обирайте встановлення оновлень та відмовтеся від підтримки LVM group при розмітці диску.

В якості імені користувача оберіть *stud*, в якості імені серверу вкажіть ***ubuntusrv***. Як варіант складного комплексного паролю для *root* та *stud* можна вказати, наприклад, пароль: `#123&456ms`.

При встановлені обрати опцію *Install OpenSSH Server* (встановлення серверу OpenSSH) без імпорту ключів із відомих сховищ.

Featured server snaps не встановлювати.

Всі інші опції при встановлені залишати за замовченням.

Після завершення процедури встановлення, під час перезавантаження, натиснути на клавішу *Enter* для вилучення CD-диску з віртуального пристрою читання.

Після перезавантаження, дочекайтеся завершення виведення на консоль різноманітної службової інформації, натисніть *Enter* та закрийте вікно віртуальної машини, при цьому оберіть опцію *Надіслати сигнал завершення* (*Send the shutdown signal*) у діалоговому вікні Oracle VirtualBox.

В налаштуваннях віртуальної машини з Ubuntu Server вилучить CD-диск з віртуального оптичного носія, закрийте вікно налаштувань та повторно запустіть віртуальну машину з Ubuntu Server.

Після виведення рядку повідомлення *ubuntusrv login*, введіть ім'я користувача *stud* та його пароль (пароль при введені не повинен відображатися).

Якщо процедура встановлення успішно завершена та зроблений вірний вхід в систему, то на екрані буде зображення, яке подібне тому, що представлено на рис. 4.1.

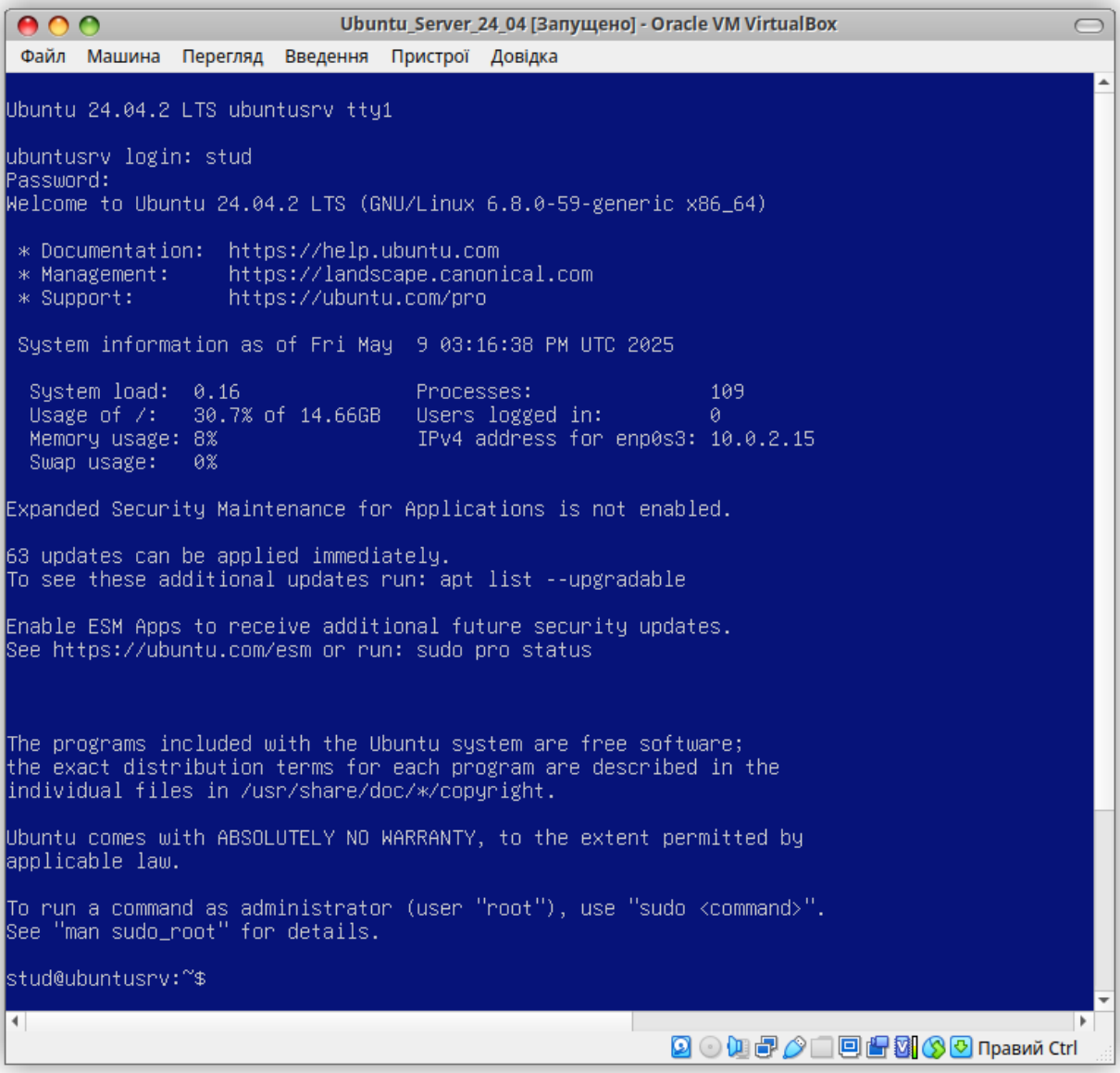


Рис. 4.1. Приклад зображення екрану після першого входу в оточення Ubuntu Server (кольорова палітра змінена, IPv4-адреса може бути іншою)

Для продовження виконання роботи запустіть віртуальний хост IPFire, що був налаштований в роботі № 3.

Для управління мережевими налаштуваннями в Ubuntu Server, починаючи з версії Ubuntu 17.10, мовою Python створений спеціальний інструмент *netplan*. З версії Ubuntu 18.04 *netplan* є засобом за замовченням для мережевого конфігурування. Для виведення стану налаштувань мережевих інтерфейсів скористуйтеся командою:

```
sudo netplan status
```

За замовченням мережеві налаштування *netplan* зберігаються в каталозі */etc/netplan* у файлах YAML-формату. Так, в каталозі розміщений тільки файл *50-cloud-init.yaml*. Для швидкого виведення інформації в YAML-форматі використовують команду:

```
sudo netplan get
```

Виконайте наступні команди для зміни налаштування мережевого адаптеру (передбачається, що наявний мережевий інтерфейс має назву *enp0s3*):

```
sudo netplan set ethernets.enp0s3.dhcp=false
sudo netplan set ethernets.enp0s3.addresses=[10.0.0.4/24]
sudo netplan set ethernets.enp0s3.routes='[{"to":"deafult", "via": "10.0.0.254"}]'
sudo netplan set ethernets.enp0s3.nameservers='{"addresses":[10.0.0.1, 8.8.8.8]}'
sudo netplan apply
sudo netplan status
sudo shutdown -h now
```

Примітка: для висвітлення всіх активних мережевих інтерфейсів використовуйте команду:

```
ip -c link
```

Після вимикання віртуальної машини вкажіть в налаштуваннях мережевого адаптеру під’єднання до внутрішньої мережі (ім’я: **intnet**) та закрийте вікно налаштувань віртуальної машини.

Виконайте повторний запуск та виведіть стан з’єднання командою *netplan*. Результат показаний на рис. 4.2.

Таким чином, Ubuntu Server введено в створену раніше локальну мережу, та дозволено під’єднуватися до мережі Internet через мережевий екран – шлюзову машину на IPFire.

За допомогою команди *adduser* можна створити нового користувача та відповідний домашній каталог. Наприклад:

```
sudo adduser user126
```

На відміну від файлу *useradd*, файл *adduser* є скриптом, що написаний мовою Perl. Головна його мета – спростити та зробити зручним створення нового користувача з консолі.

При виконанні команди, можна залишити всі поля на запит за замовченням, а при запиті паролю вказати, наприклад, *stud*.

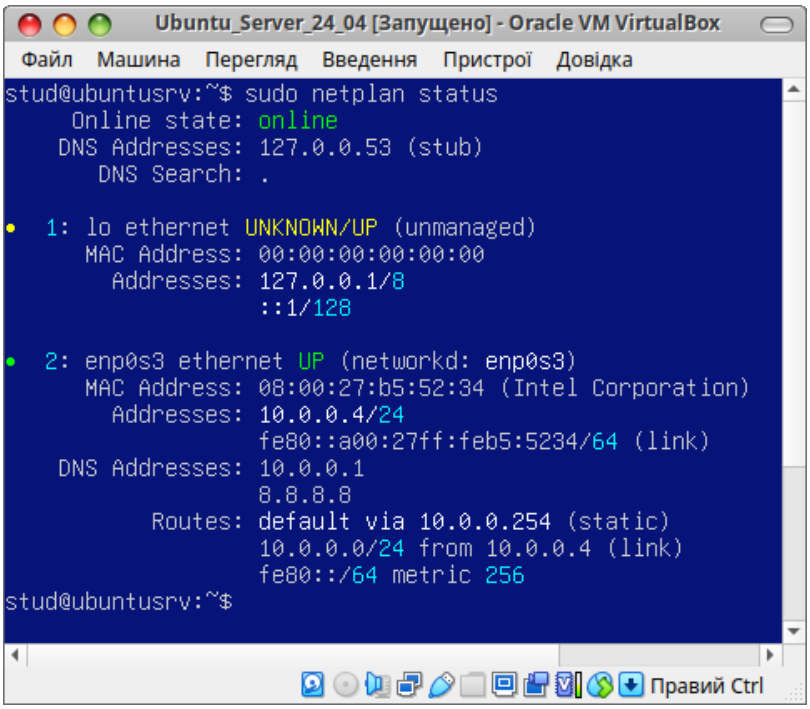


Рис. 4.2. Результат перевірки мережевих налаштувань після змін (кольорова палітра змінена)

Після створення користувача, перевірте атрибути каталогів в */home* та надайте їм більш суворі права. Наприклад:

```
sudo chmod g-rx,o-rx /home/stud /home/user126
```

або

```
sudo chmod 700 /home/stud /home/user126
```

Базова робота з OpenSSH

Оскільки був встановлений OpenSSH сервер, то за замовченням він буде стартувати при запуску системи. Для перевірки підключення по SSH-протоколу у вікні терміналу консолі (наприклад, в MS Windows Server Core) виконайте команду:

```
ssh user126@10.0.0.4
```

IP-адреса, що наведена в прикладі, повинна відповідати IP-адресі мережевого інтерфейсу встановленого Ubuntu Server.

Слід зауважити, що команда *ssh* присутня майже на всіх GNU/Linux-сумісних системах, а також в ОС Microsoft за замовченням починаючи з версій Windows Server 2019 та Windows 10 1809. Якщо команда *ssh* відсутня з якихось причин, то потрібно додатково встановити або пакунок *openssh-client* (або *openssh*, або *ssh*), або під платформу MS Windows ранніх версій одну з програм, наприклад: PuTTY, MTPuTTY, MobaXterm або подібну, або використати оточення MSYS2.

Після виконання цієї команди, якщо вхід за SSH-сеансом відбувається вперше, необхідно зберегти ключ доступу до вказаного серверу. Далі ввести пароль користувача у відповідь на запит. Для завершення SSH-сеансу в командному рядку вводять команду *exit*.

Подивитися список TCP-портів, що використовуються на сервері в поточний час, можна командою: `ss -atn`. Можна побачити, що в переліку буде прослуховування 22-го порту TCP для обслуговування протоколу *SSH*.

Дуже часто для приховування відкритого SSH-порту використовують його зміну для певного протоколу (наприклад, для *SSH*). Для цього виконайте команду:

```
sudo nano /etc/ssh/sshd_config
```

Далі можна після коментованого рядку із вказівкою номеру порту, вказати потрібний порт. Наприклад, змінюємо стандартний номер порту на, наприклад, порт 8230:

```
#Port 22
Port 8230
```

Збережіть зміни в файлі (Ctrl+O та Enter) та вийдіть з редактору (Ctrl+X). Далі можна просто перезапустити сервер (`sudo reboot`) або окремо робити додаткові команди для перезапуску служби *ssh* на новому порту. Після цього потрібна перевірка командою `ss -atn`.

Якщо все зроблене вірно, то порт 22 буде змінено на 8230.

Тепер команда *ssh* буде мати такий вигляд:

```
ssh -p 8230 user126@10.0.0.4
```

Робота з мережевим екраном

За замовченням Ubuntu Server використовує в якості мережевого екрану програмне забезпечення *ufw*. Перевірка активності мережевого екрану здійснюється командою:

```
sudo ufw status
```

Для його увімкнення використовують команду:

```
sudo ufw enable
```

Для вимкнення:

```
sudo ufw disable
```

Для висвітлення більш детального стану використовують команду:

```
sudo ufw status verbose
```

Якщо виконати останню, то бачимо, що за замовченням *ufw* буде повністю блокувати доступ до серверу із зовні. Наприклад, хочемо створити правило, за яким мережевий екран дозволить підключатися із всіх хостів внутрішньої мережі. Це виконується командою:

```
sudo ufw allow from 10.0.0.0/24
```

Після виведення статусу мережевого екрану бачимо, що з'явилося нове правило на дозвіл щодо доступу.

Часто різні програми створюють для *ufw* вже готові профілі, в яких зазначені порти для опрацювання *ufw*. Список таких профілів можна побачити командою:

```
sudo ufw app list
```

У нашому випадку буде профіль OpenSSH. Інформацію по ньому можна подивитися командою:

```
sudo ufw app info OpenSSH
```

Таким чином бачимо, що в профілі вказаний порт 22 протоколу TCP. Опис параметрів профілю зберігається в каталозі */etc/ufw/applications.d*. Для профілю OpenSSH – це файл *openssh-server*.

Видалимо правило доступу із всієї мережі, внесемо новий номер порту (змінюємо 22 на 8230 у файлі *openssh-server*), оновлюємо профіль OpenSSH та вводимо правило за цим профілем:

```
sudo ufw delete allow from 10.0.0.0/24
sudo nano /etc/ufw/applications.d/openssh-server
sudo ufw app update OpenSSH
sudo ufw allow OpenSSH
sudo ufw status verbose
```

Додаємо правило блокування відправлення через порт 25 TCP (як і раніше в IPFire):

```
sudo ufw deny out 25
```

Також часто для підвищення безпеки серверу блокують вхідні *echo-request*-запити протоколу ICMP. Це можна зробити через редагування файлу налаштувань передвизначених правил *ufw – before.rules*:

```
sudo nano /etc/ufw/before.rules
знаходимо рядок:
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT
змінюємо ACCEPT на DROP та зберігаємо зміни
перезавантажуємо мережевий екран:
sudo ufw reload
```

Слід зауважити, що правила, які описані у файлах *before.rules* та *before6.rules* завжди виконуються до правил, які встановлені з командного рядку *ufw*. Синтаксис цих правил відповідає синтаксису створення правил для іншого мережевого екрану – відомої утиліти *iptables*.

Налаштування Samba

Розгорнемо на сервері підтримку *Samba* та надамо користувачам доступ до певного загального каталогу.

Для виконання цього потрібне підключення до мережі Internet. Нехай з'єднання буде відбуватися через шлюзовий вузол *ipfire* (10.0.0.254).

Samba – це open source ПЗ, яке надає можливості обміну файлами та друку для клієнтів SMB/CIFS як з GNU/Linux-сумісних систем, так із ОС MS Windows.

Для встановлення Samba-серверу та клієнту вводять команди:

```
sudo apt update
sudo apt -y install samba smbclient
sudo ufw app info Samba
```

Як бачимо, Samba буде використовувати 137 та 138 порти UDP та 139 та 445 порти TCP для організації роботи за протоколом SMB/CIFS.

Порти 137 та 138 UDP використовуються протоколом NetBIOS (Network Basic Input/Output System). Зокрема, порт 137 UDP зазвичай використовується для служби імен NetBIOS (NetBIOS Name Service), яка відповідає за перетворення імен NetBIOS на IP-адреси, а порт 138 UDP – для служби

дейтаграм NetBIOS (NetBIOS Datagram Service), яка забезпечує передачу невеликих пакетів даних між пристроями в мережі.

Порти 139 та 445 TCP використовуються для мережевих служб. Порт 139 використовується для NetBIOS сеансів. Порт 445 призначений для протоколу SMB (Server Message Block), який використовується для спільного доступу до файлів, принтерів та інших ресурсів між комп'ютерами мережі.

Створимо окремі каталоги, які будуть виступати мережевим ресурсом для певного користувача:

```
sudo mkdir /home/share
sudo chown -R user126:user126 /home/share
sudo chomod -R 700 /home/share
```

Виконаємо редагування основного файлу конфігурації *Samba*-серверу – */etc/samba/smb.conf*, попередньо зробивши копію старої версії налаштувань:

```
sudo cp /etc/samba/smb.conf{,.backup}
sudo tee -a /etc/samba/smb.conf > /dev/null << EOF
[share]
path = /home/share
browseable = yes
read only = no
guest ok = no
create mask = 0644
directory mask = 0755
EOF
testparm
```

Команда `testparm` перевіряє коректність синтаксису та параметрів у файлі *smb.conf*.

Опис полів *smb.conf* та правила його оформлення описані в документації проєкту *Samba* та доступні, наприклад, за посиланням:

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

Так в представленій секції `share` описані параметри доступу до загального ресурсу, який розміщений в оточені локальної файлової системи сервера за шляхом */home/share*. Прапорець `browseable` визначає, чи відображається цей спільний ресурс у списку доступних спільних ресурсів у мережевому поданні та у списку перегляду. Він має значення *yes* за замовченням та наведений явно для підтвердження цього стану явно.

Прапорець `read only` контролює, чи дозволено в зазначеному ресурсу створювати чи модифікувати файли чи каталоги. Тобто значення *no* каже про те, що є дозвіл змін зовні для цього ресурсу.

Прапорець `guest ok` контролює, чи буде потрібне відкриття ресурсу без вказівки імені та пароля користувача, чи ні. Значення *no* вкаже *Samba*, що при зверненні до вказаного ресурсу потрібен запит на введення імені та пароля користувача.

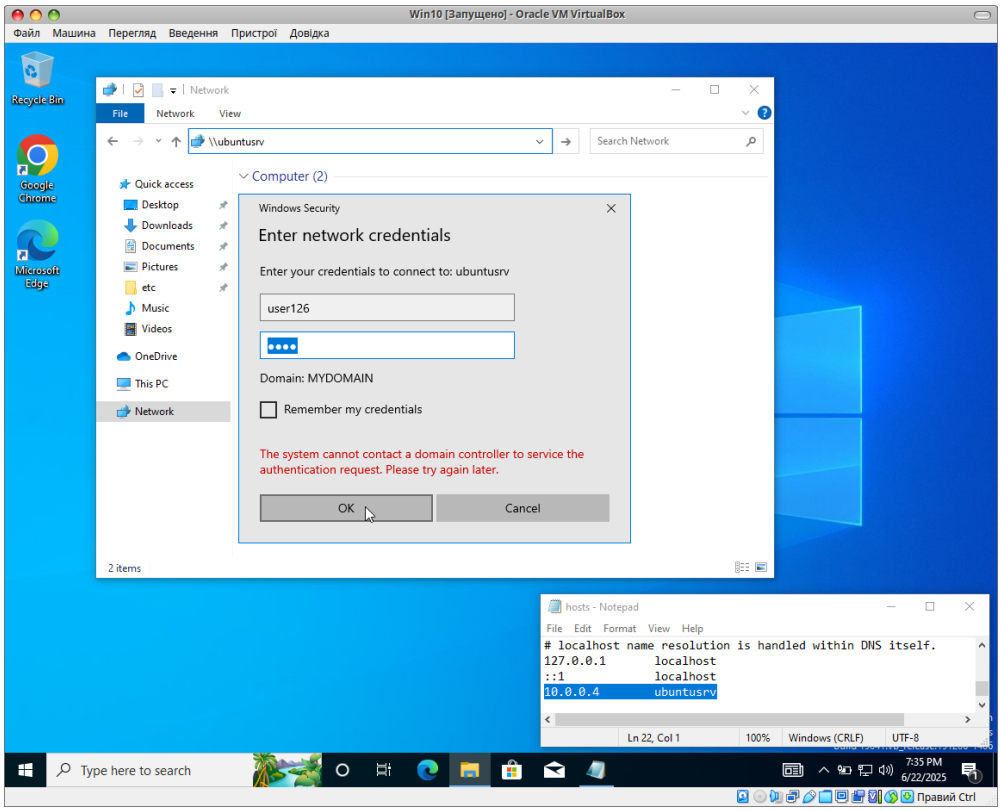


Рис. 4.3. Вікно введення імені користувача та паролю для доступу в мережеву теку *share*, яка фізично розміщена у файловій системі Ubuntu Server

Параметр `create mask` задає побітову маску для режимів створення Unix-файлу. Будь-який біт, не встановлений тут, буде видалено з режимів, встановлених для файлу під час його створення. Параметр не впливає на маску для каталогів.

Дефолтні права безпеки для файлу: 0644 (rw-r--r--).

Параметр `directory mask` задає побітову маску для режимів створення Unix-каталогу. Будь-який біт, не встановлений тут, буде видалено з режимів, встановлених для файлу під час його створення.

Дефолтні права безпеки для каталогу: 0755 (rwxr-xr-x).

Після цього потрібно включити користувача *user126* в базу даних SMB та назначити йому пароль (наприклад, *stud*) і перезапустити демони *smbd* та *nmbd*. Також, якщо увімкнений мережевий екран *ufw*, то потрібно надати дозвіл на використання певних портів за профілем *Samba*:

```
sudo smbpasswd -a user126
sudo systemctl restart smbd nmbd
sudo ufw allow Samba
```

За замовченням *Samba*-сервер працює в режимі *Standalone Server* – автономний файловий сервер. Після цього в мережі буде доступний загальний каталог, доступ в який буде обмежений користувачем *user126* (рис. 4.3). Слід зауважити, що для уникнення певних проблем з'єднання із *Samba*-сервером зі сторони клієнту MS Windows (наприклад, в MS Windows 10), потрібно зробити під адміністратором відповідність IP-адресу та символьного імені або у файлі hosts, що розміщений за шляхом: *C:\Windows\System32\drivers\etc\hosts* (рис. 4.3), або робити додаткові налаштування DNS домену.

Завдання

Виконати встановлення та налаштування Ubuntu Server, описані в теоретично-практичній частині роботи.

Додати в систему користувачів *user1* та *user2*.

Об'єднати користувачів *user1, user2* та *user126* в нову групу *students*.

Організувати доступ для користувачів з групи *students* в каталог */home/share*.

Виконати налаштування таким чином, щоб користувач *user1* мав персональний мережевий доступ до свого домашнього каталогу.

В якості додаткового довідникового матеріалу використовувати посилання:

https://ubuntu.com/server/docs/security-users
https://ubuntu.com/server/docs/samba-file-server

Відобразити у звіті основні налаштування серверу. Продемонструвати викладачу результати налаштування та відповісти на питання стосовно виконаного завдання.

У звіт до роботи включити команди налаштування серверу та *Samba*, вміст файлу конфігурування *Samba*.

Правила оформлення звіту подані у додатку А.

Робота №5.
Адміністрування користувачів, груп, файлів та каталогів в Ubuntu Server

Мета роботи: опанувати основні команди та технології адміністрування користувачів, груп, файлів та каталогів на прикладі операційного середовища Ubuntu Server.

Теоретично-практична частина

Адміністрування користувачів та груп користувачів

Інформація про користувачів та псевдокористувачів зберігається у файлі */etc/passwd*. Його перегляд можливий будь якими командами, які дозволяють робити перегляд звичайних форматованих ASCII-файлів. Наприклад:

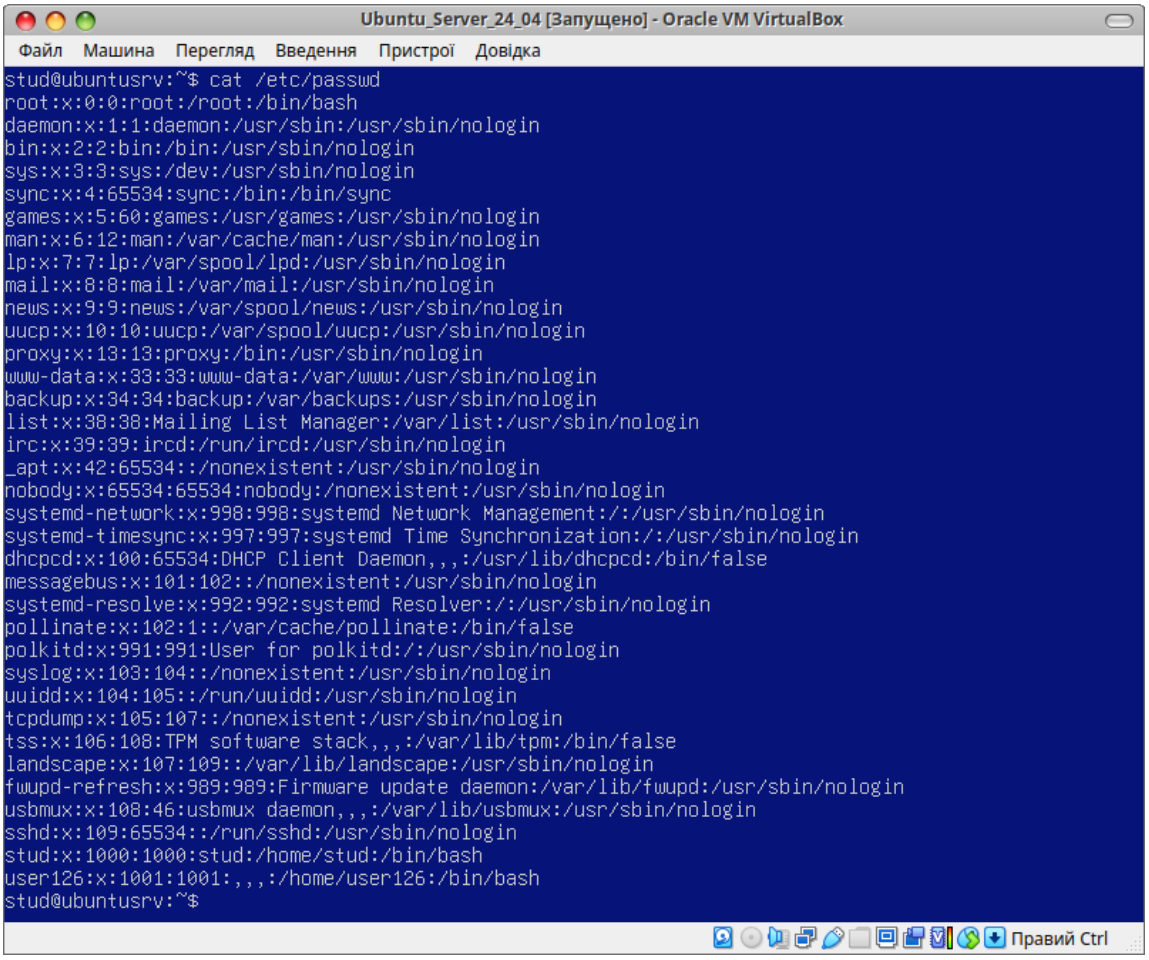


Рис. 5.1. Приклад вмісту файлу */etc/passwd*

Процес створення користувача коротко розглядався в роботі №4 – для створення нового користувача в GNU/Linux-сумісних ОС використовуються команди *adduser* або, наприклад, *useradd*. Після створення користувача, у файлі */etc/passwd* буде автоматично доданий відповідний рядок, що пов'язаний з ним. Головними складовими рядка є (рис. 5.1): ім'я користувача (перше поле), його UID (третє поле), GID (четверте поле), домашній каталог (передостаннє поле) та консольний командний процесор (консольна оболонка – останнє поле).

Команда *adduser* з вказівкою імені нового користувача, створює за замовченням домашній каталог користувача в */home*. В новому домашньому каталозі будуть розміщені ресурси, які сформовані як шаблон з каталогу */etc/skel* (за замовченням в переважній більшості GNU/Linux-сумісних ОС).

Команда *adduser* представлена в каталозі */usr/sbin* як perl-скрипт та використовує для виконання спеціальні налаштування з файлу */etc/adduser.conf*. Так, наприклад, через конфігураційну опцію SKEL можна вказати інший каталог-шаблон для нових користувачів.

Створення нової групи користувачів може бути виконано командою *addgroup*, яка також використовує конфігураційний файл */etc/adduser.conf*. У файлі можна знайти конфігураційну опцію DIR_MODE, яка містить права за замовченням на домашній каталог несистемних користувачів, що створюються. За замовченням в Ubuntu Server це значення дорівнює 0750 (drwxr-x---).

При використанні утиліти *useradd* для створення нового користувача, будуть задіяні конфігураційні опції з файлів */etc/login.defs* та */etc/default/useradd*.

Зверніть увагу, що при використанні *adduser*, командним процесором за замовченням для звичайного користувача буде призначений */bin/bash* (конфігураційна опція DSHELL у файлі */etc/adduser.conf*). А при використанні команди *useradd* – буде призначений командний процесор */bin/sh* (змінна SHELL у файлі */etc/default/useradd*). Також зверніть увагу, що при використанні *useradd* завжди можна призначити певні особливості профайлу користувача через окремі опції команди (наприклад, такі опції, як: -m, -d, -G, -k, -p, -s та ін.).

Примітка: в Unix-подібній серверній ОС FreeBSD новий користувач створюється через POSIX shell-скрипт *adduser*. При відсутності файлу */etc/adduser.conf*, його можна створити викликавши *adduser* з опцією -C. За замовченням *skel*-каталог у FreeBSD – це каталог */usr/share/skel*. В якості командного процесору для звичайного користувача за замовченням у FreeBSD йде командний процесор */bin/sh*. За замовченням права на домашній каталог користувача у FreeBSD дорівнюють 0755 (drwxr-xr-x). У FreeBSD існує також команда *pw* із параметром *useradd* для створення нового користувача. Через опцію -M можна задавати окремо інші права на домашній каталог.

Розглянемо детальніше подання прав на файли та каталоги в Unix-подібних ОС. В таких системах робота з файлами та каталогами передбачає встановлення прав доступу для трьох категорій користувачів:

– власника (user, u);

– групи (group, g), в яку може входити власник, а також інші користувачі;

– інших користувачів (other, o).

При встановленні прав для цих трьох груп використовують або символьні позначення (u, g, o, a – all, всі), або цифри у вісімковій системі числення. При цьому використовується наступна таблиця:

Таблиця 5.1

Варіанти запису прав користувачів в Unix-подібних ОС

У двійковій системі	*У вісімковій системі*	*В символьному поданні*	*Права на файл*	*Права на каталог*
000	0	---	відсутнє	відсутнє
001	1	--x	виконання	читання файлів та їх властивостей
010	2	-w-	запис	відсутнє
011	3	-wx	запис та виконання	все, окрім читання списку файлів
100	4	r--	читання	читання імен файлів
101	5	r-x	читання та виконання	доступ на читання
110	6	rw-	читання та запис	читання імен файлів
111	7	rwx	всі права	всі права

Частина прав має сенс тільки в поєднані з іншими. Наприклад, для каталогів використовують тільки значення 0, 5 та 7 – відповідно: відмова всіх прав, читання та виконання, повний доступ.

Окремо можна зазначити, що є можливість дати запуск на виконання файлу від імені власника (SUID) або групи (SGID), встановивши спеціальний S-біт (sticky bit). Значення для SUID та SGID відповідно 4000 та 2000. Для каталогів можна також призначати S-біт, а також спеціальний t-біт (restricted deletion flag). t-біт має значення 1000. Коли t-біт для каталогу не встановлений, файл в даному каталозі може видалити (перейменувати) будь-який користувач, який має доступ на запис до даного каталогу. Встановлюючи t-біт на каталог, змінюють це правило таким чином, що видалити (перейменувати) файл може тільки власник цього файлу.

Важливе зауваження: якщо для каталогу задано право на запис (w), то файл всередині цього каталогу можна буде видалити, навіть якщо право на запис для нього не встановлено!

Популярні значення прав на доступ представлені в таблиці 5.2.

Таблиця 5.2

Популярні значення прав доступу в Unix-подібних ОС

Значення у вісімковій системі числення	*Символьне подання*	*Опис*
0400	-r--------	Власник має право читання; ніхто інший не має права виконувати ніякі дії
0440	-r--r-----	Тільки власник та група мають право читання
0444	-r--r--r--	Усі користувачі мають права читання
0555	-r-xr-xr-x	Усі користувачі мають право читання та виконання
0644	-rw-r--r--	Усі користувачі мають право читання; власник може редагувати
0660	-rw-rw----	Власник і група можуть читати та редагувати, решта не мають права виконувати ніякі дії
0664	-rw-rw-r--	Усі користувачі мають право читання; власник і група можуть редагувати
0666	-rw-rw-rw-	Усі користувачі можуть читати та редагувати
0700	-rwx------	Власник може читати, записувати та запускати на виконання; ніхто інший не має права виконувати ніякі дії
0744	-rwxr--r--	Кожен користувач може читати, власник має право редагувати та запускати на виконання
0755	-rwxr-xr-x	Кожен користувач має право читати і запускати на виконання; власник може редагувати
0777	-rwxrwxrwx	Кожен користувач може читати, редагувати та запускати на виконання
1555	-r-xr-xr-t	Кожен користувач має право читати і запускати на виконання (відкривати каталог); видалити каталог може тільки його власник
2555	-r-xr-Sr-x	Кожен користувач має право читати та запускати на виконання з правами групи користувача файлу
4555	-r-Sr-xr-x	Кожен користувач має право читати та запускати на виконання з правами власника файлу

Для зміни прав доступу використовують команду *chmod*.

Таким чином, в GNU/Linux-сумісних ОС у файлі /*etc/adduser.conf* можна привласнити нове значення DIR_MODE=0700 і таким чином виконувати створення каталогу для нового користувача з більш жорсткими правилами доступу для всіх інших користувачів.

Слід також зауважити, що окрім зазначених вище значень прав для створення нових файлів та каталогів, встановлюються права з врахуванням спеціальної маски користувача режиму створення файлів – *umask*. Так, якщо за замовченням значення маски дорівнює 022 (0022), то за правилами,

встановленими стандартом POSIX для створення нового каталогу будуть встановлені права 0755, а для створюваного файлу – права 0644, оскільки за замовчанням для каталогу та файлу йдуть відповідно значення 0777 та 0666.

Маскування значень за замовченням відбуваються за наступною схемою.

1. Інвертуються всі біти заданої маски. Наприклад, для маски 022 (0022) це буде значення 7755:

```
 0022:  000 000 010 010
~0022:  111 111 101 101    <- 7755
```

2. Виконується побітова операція ТА (&) й на виході отримуємо кінцевий результат. Наприклад, при інвертованому значені маски 7755 та значенню прав для каталогу за замовченням 0777, будемо мати результат 0755:

```
 0777:  000 111 111 111
 7755:  111 111 101 101
0777 & 7755:  000 111 101 101   <- 0755
```

За замовченням значення *umask* задано у файлі */etc/login.defs* і може бути змінено в сеансі користувача командою *umask* (наприклад, через файл *${HOME}/.profile*). Тобто, якщо користувач хоче, щоб за замовченням при створенні каталогу або файлу до нього був доступ тільки у власника, то він повинен розкоментувати та задати у файлі *${HOME}/.profile* значення: `umask 0077`.

```
 0077:  000 000 111 111
~0077:  111 111 000 000    <- 7700
```

Отримаємо для каталогів:

```
 0777:  000 111 111 111
 7700:  111 111 000 000
0777  & 7700:  000 111 000 000   <- 0700
```

Отримаємо для файлів:

```
 0666:  000 110 110 110
 7700:  111 111 000 000
0666 & 7700:  000 110 000 000   <- 0600
```

При виконанні команди створення нового користувача *adduser*, вона запитує за замовченням додаткові відомості. Цей процес контролюється через опцію `--gecos`. Якщо вказати пустий рядок за цією опцією, або за замовченням повне ім’я користувача, то команда не буде видавати запити на введення цієї

додаткової інформації. Наприклад (в процесі створення буде наданий запит на введення пароля користувача):

```
sudo adduser --gecos "" user7
sudo adduser --gecos "New User Full Name" user9
```

Для отримання більш повної інформації по команді *adduser*, дивитися довідку:

```
man adduser
adduser --help
```

Ще однією командою створення користувача є команда *useradd* (*/usr/sbin/useradd*), яка, на відміну від perl-скрипту *adduser*, є двійковим файлом, що виконується (згадувалася вище). Для створення домашнього каталогу нового користувача потрібно вказувати додаткову опцію -m, а для вказівки командного процесору – опцію -s. Наприклад:

```
sudo useradd -m -s /bin/bash user8
```

Слід зазначити, що така команда створює нового користувача з заблокованим паролем, оскільки він не заданий.

Пароль користувача може бути заданий окремою командою *passwd*, яка має вигляд:

```
sudo passwd ім'я_користувача
```

Якщо користувач сам змінює свій пароль, то для цього просто потрібно ввести команду *passwd*.

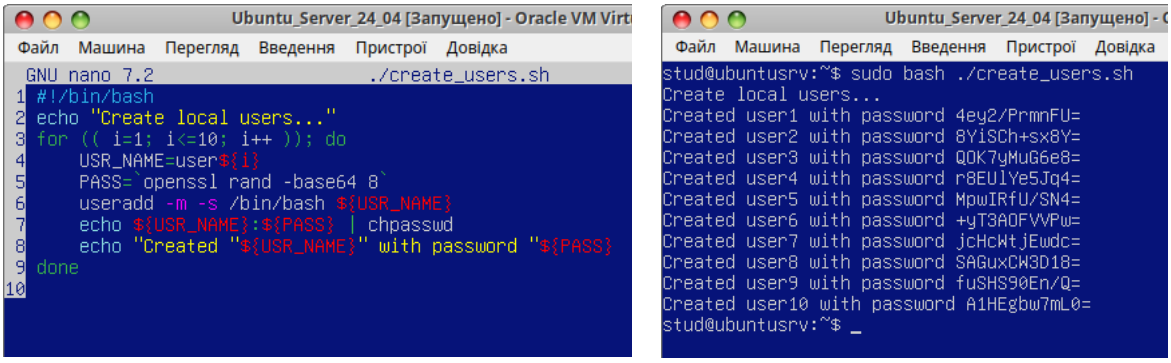
Якщо пароль користувача створюється через скрипт (наприклад, при створені великої кількості користувачів у системі) в Ubuntu Server, то можна використовувати наступний рядок із додатковою командою *chpasswd* (в цьому прикладі користувачу *user10* буде заданий пароль `#123&456ms`):

```
echo "user10:#123&456ms" | sudo chpasswd
```

Для генерування випадкового пароля для користувача можна використовувати можливості програми *openssl*. Приклад команди генерування випадкового паролю:

```
openssl rand -base64 8
```

Приклад командного скрипту створення 10 локальних користувачів із випадково згенерованими паролями, представлений рис. 5.2.



а) б)

Рис. 5.2. Командний скрипт створення 10 локальних користувачів в Ubuntu Server (а) та результат його виконання (б)

Перелік груп та їх склад міститься у файлі */etc/group*.

Створення нової локальної групи користувачів здійснюється командами *addgroup* (в Ubuntu Server це символічне посилання на perl-скрипт *adduser*) та *groupadd* (бінарний файл). Приклад створення нової групи:

```
sudo groupadd localusers
```

За замовченням група, що створюється, має значення GID наступне вільне з певного діапазону, який контролюється значеннями GID_MIN та GID_MAX. Їх значення задані у файлі */etc/login.defs*. Але можна вказати ідентифікатор групи й примусово. Наприклад:

```
sudo groupadd -g 1010 localusers2
```

Якщо група із вказаним ідентифікатором вже існує, то створення групи виконано не буде. Значення GID_MIN та GID_MAX можна швидко побачити, виконавши команду:

```
cat /etc/login.defs | grep GID
```

За замовченням ці значення находяться у діапазоні 1000 – 60000. Як правило значення ідентифікаторів для користувачів починаються в GNU/Linux-сумісних системах із значення 1000.

Щоб швидко отримати відомості про локального користувача, можна скористатися командою `id`.

За допомогою команди `groups` з іменем користувача, можна отримати тільки повний список груп, до яких входить вказаний користувач.

Команда `who -a` надасть повні відомості про те, хто з користувачів на даний момент працює із системою (хто здійснив логін).

Команда `users` надасть просто список користувачів, які здійснили логін та працюють на даний час із системою (включаючи SSH-сеанси).

Можна поєднувати декілька команд для отримання відразу повних відомостей про користувачів, які здійснили логін та працюють на даний час із системою:

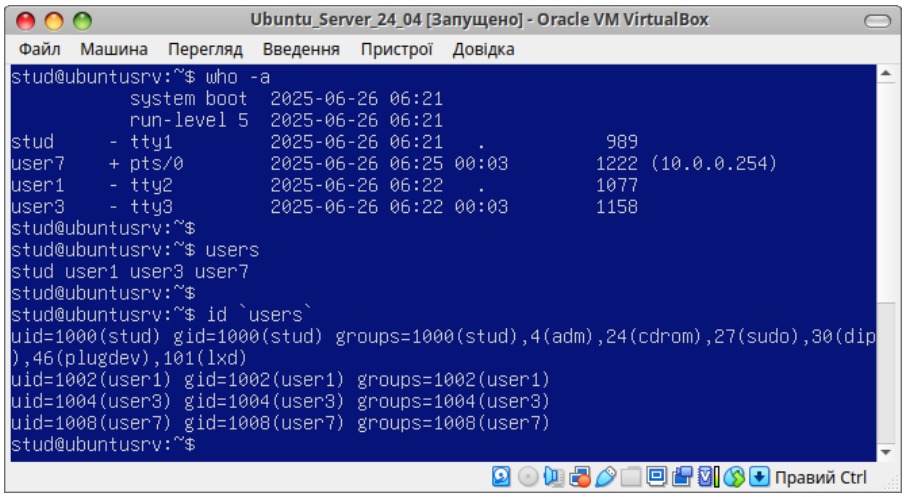


Рис. 5.3. Отримання інформації про користувачів,
які в поточний момент часу працюють із сервером

З рис. 5.3 бачимо, що із системою працюють чотири користувачі: *stud*, *user1*, *user3* та *user7*. Причому здійснили логін локально користувачі: *stud*, *user1* та *user3*. Користувач *user7* здійснив віддалений вхід в систему з хосту із IP-адресою 10.0.0.254. Наступна команда покаже інформацію за яким портом та протоколом встановлено з'єднання із цим хостом:

```
ss -an | grep 10.0.0.254
```

Для зміни певних параметрів користувача використовують команду *usermod* з різноманітними опціями.

Наприклад, в системі був створений користувач *user2* та призначений для роботи командний процесор */bin/bash*. Потрібно змінити його оболонку на */bin/sh*, зробити у файловій системі каталог */home/local_share*, через який локальні користувачі з групи *localusers* будуть обмінюватися файлами. В групу *localusers* повинні входити користувачі *stud* та *user2*. Для цих змін виконуємо такі команди:

```
sudo usermod -s /bin/sh user2
sudo usermod -aG localusers stud
sudo usermod -aG localusers user2
sudo mkdir /home/local_share
sudo chown -R root:localusers /home/local_share
sudo chmod -R 1770 /home/local_share
```

Опція -a в команді *usermod* дозволяє додавати до списку існуючих груп користувача нову групу або групи. Якщо це декілька груп, то їх потрібно перелічувати в рядку через кому без пробілів. Додавання користувача до певної групи також можна здійснювати командою *gpasswd* з опцією -a.

Для вилучення користувача з групи використовують команду *gpasswd* з опцією -d. Наприклад, видалити з групи *localusers* користувача *user2*:

```
sudo gpasswd -d user2 localusers
```

Додаткове ПЗ для моніторингу та адміністрування

Для додаткового адміністрування серверу може бути встановлене певне ПЗ, яке полегшує процес моніторингу та адміністрування. Дуже корисними для адміністраторів в Ubuntu Server є такі спеціалізовані програмні пакунки:

– Cockpit;
– shellinabox;
– консольні утиліти: chkservice, cpu-x, hwinfo, lshw, curl, htop;
та інші.

Для встановлення Cockpit та інших утиліт використовують команди:

```
sudo apt update

sudo apt -y install \
cockpit cockpit-pcp shellinabox \
chkservice cpu-x hwinfo lshw curl htop aptitude

sudo ufw allow 9090/tcp
sudo ufw allow 4200/tcp
```

На рис. 5.4 – 5.9 показані приклади вікон системи моніторингу та керування Cockpit. За замовчанням Cockpit прослуховує TCP-порт 9090. Оскільки вхід під користувачем *root* блокований, то треба здійснювати вхід від користувача, який входить, наприклад, в *sudo*-групу користувачів.

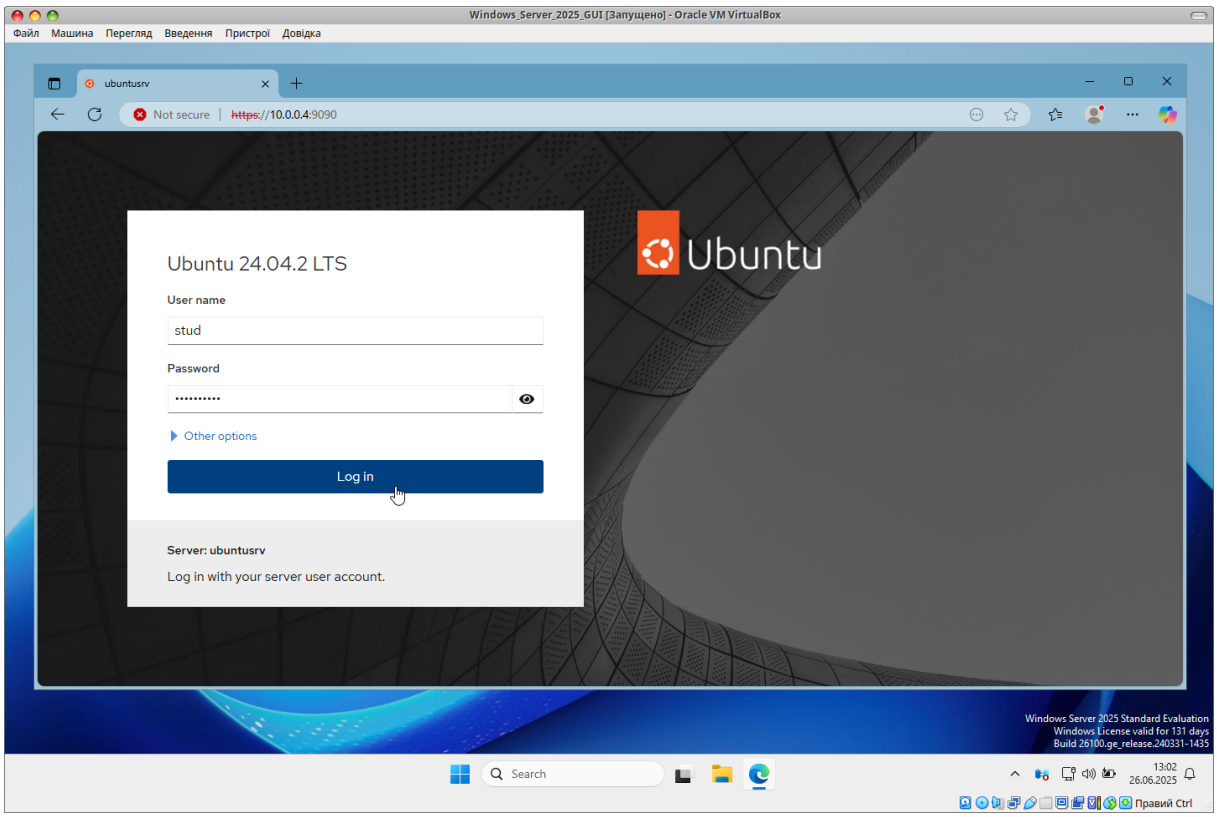


Рис. 5.4. Web-консоль Cockpit. Інтерфейс сторінки входу

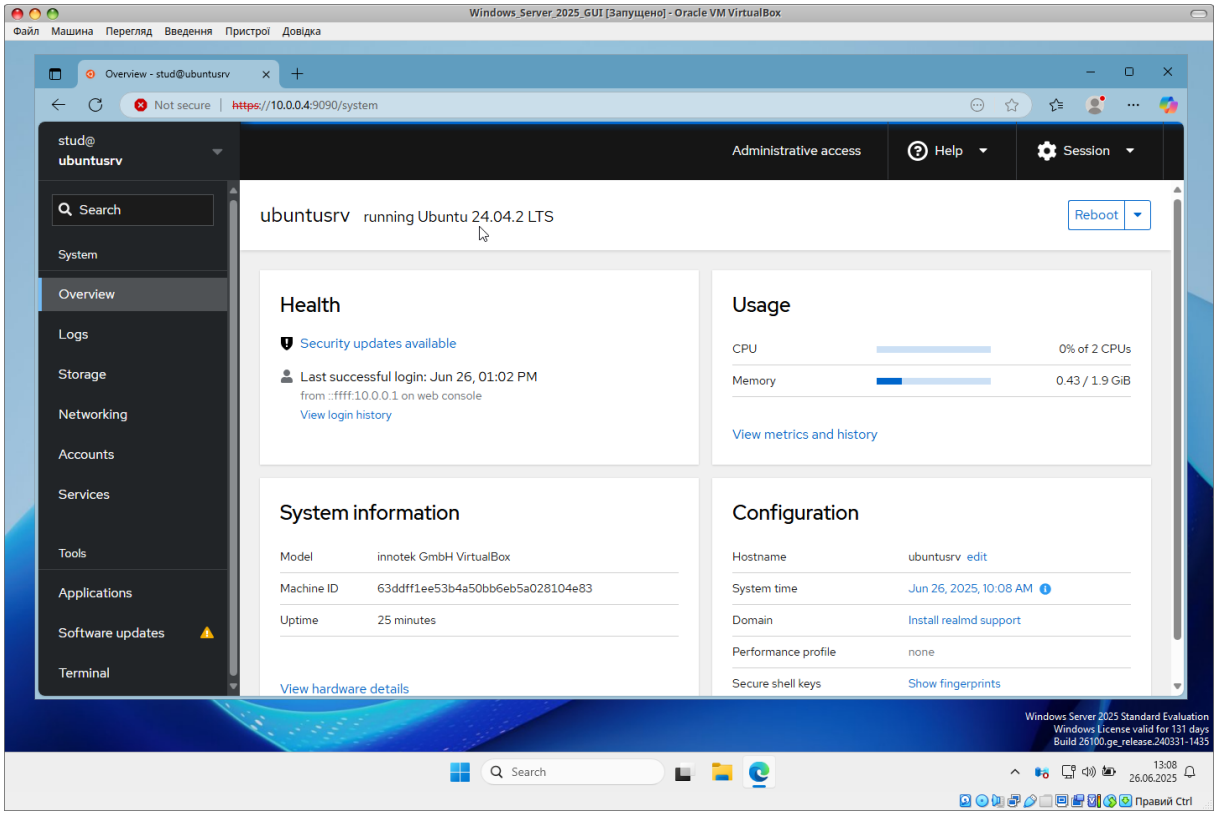


Рис. 5.5. Web-консоль Cockpit. Початкова сторінка з адміністративним доступом

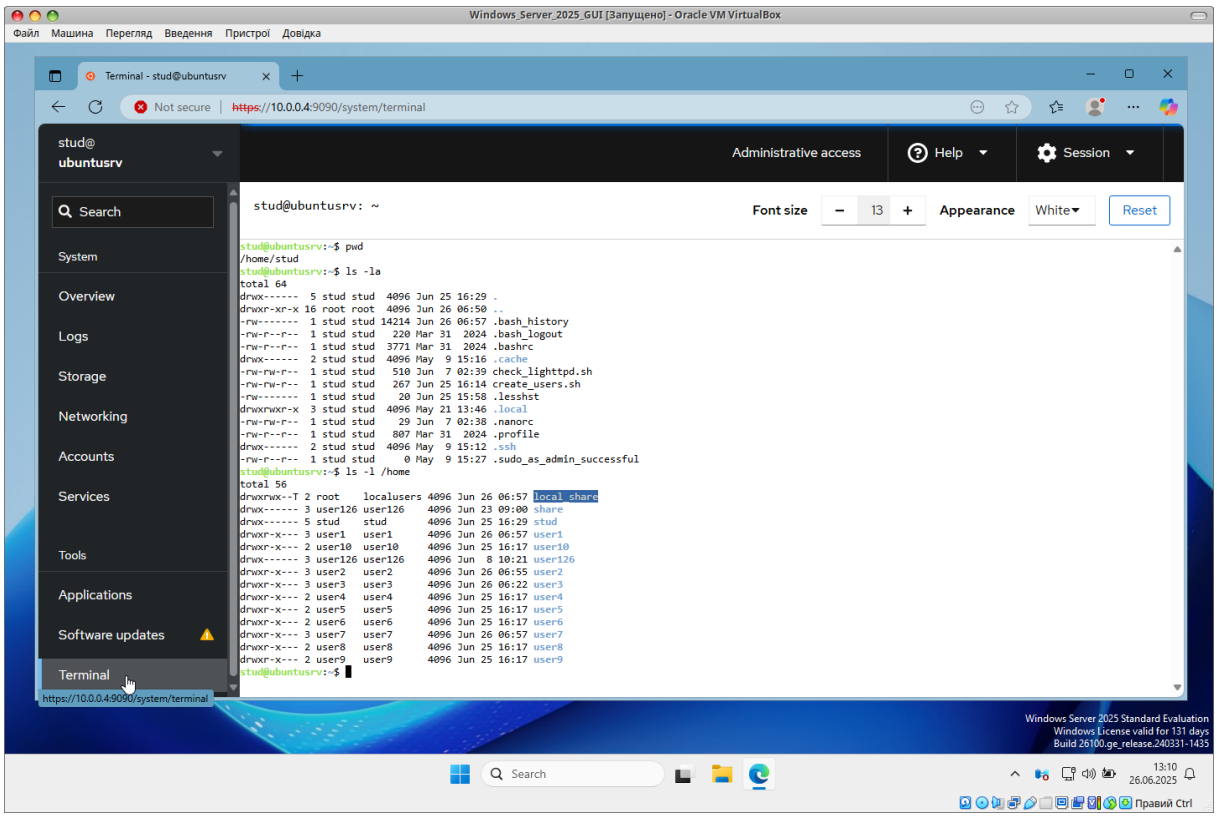


Рис. 5.6. Web-консоль Cockpit. Вікно терміналу консолі для віддаленого доступу

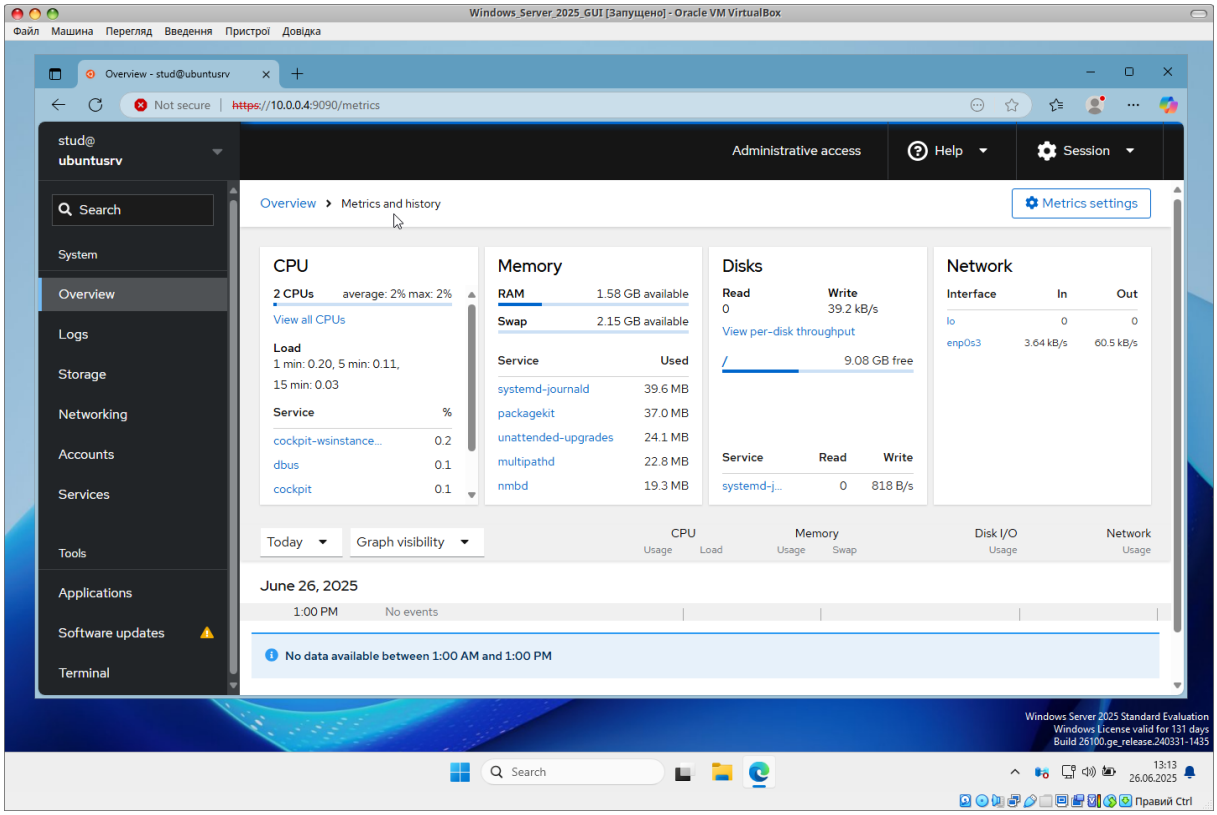


Рис. 5.7. Web-консоль Cockpit. Моніторинг ресурсів системи

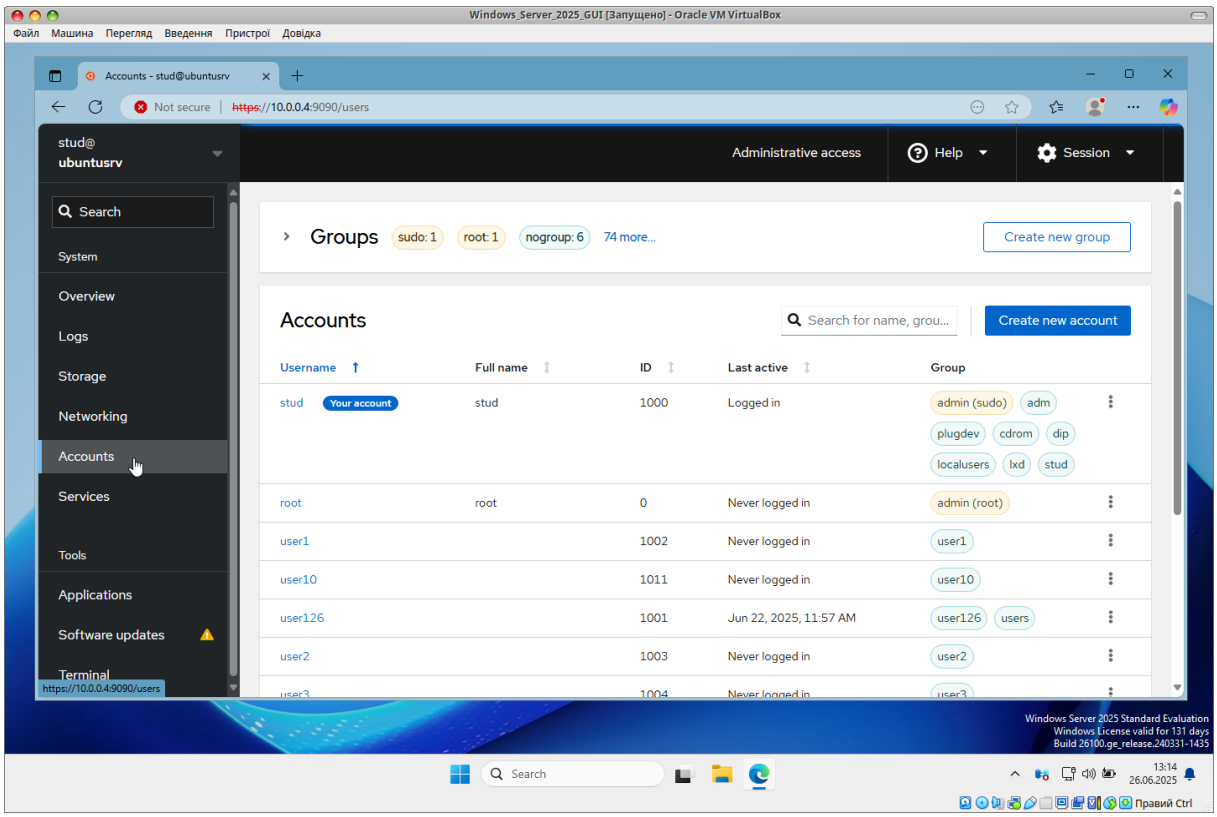


Рис. 5.8. Web-консоль Cockpit. Доступ до акаунтів користувачів із сервера

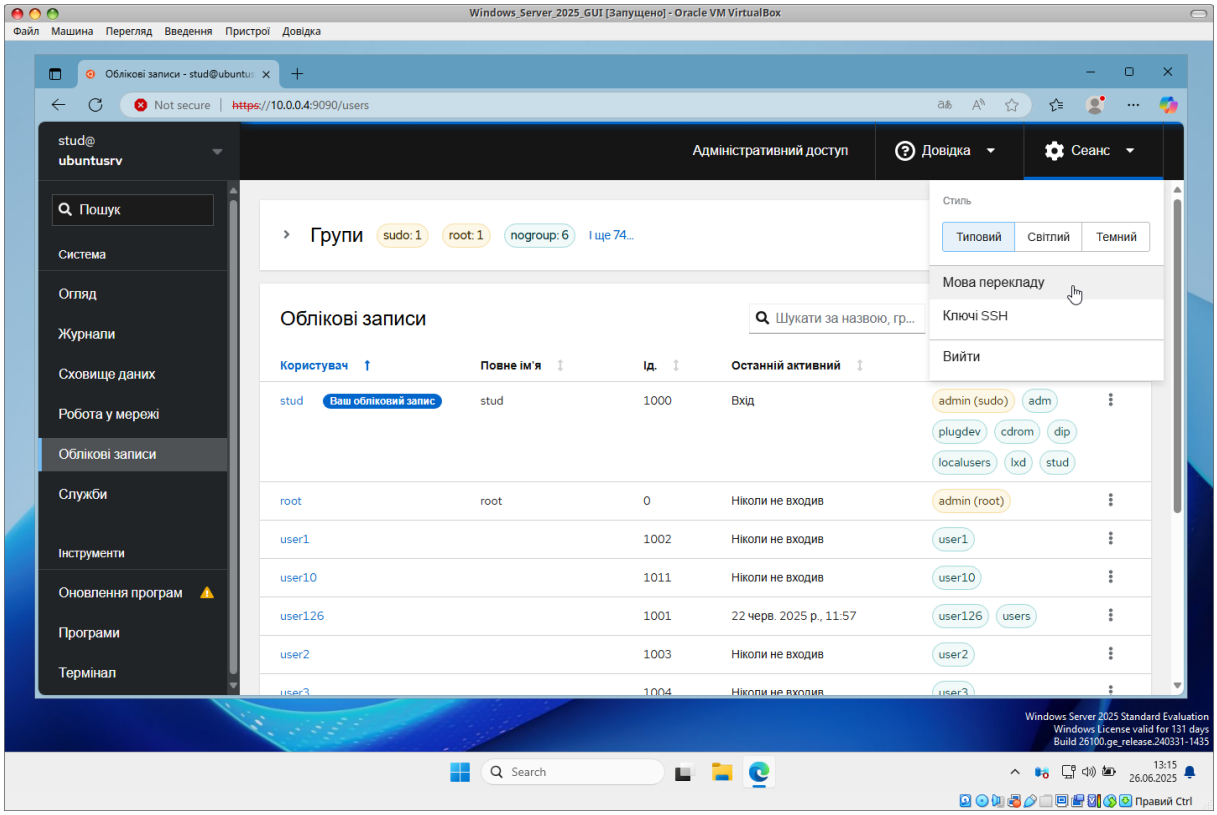


Рис. 5.9. Web-консоль Cockpit. Керування темою та мовою інтерфейсу

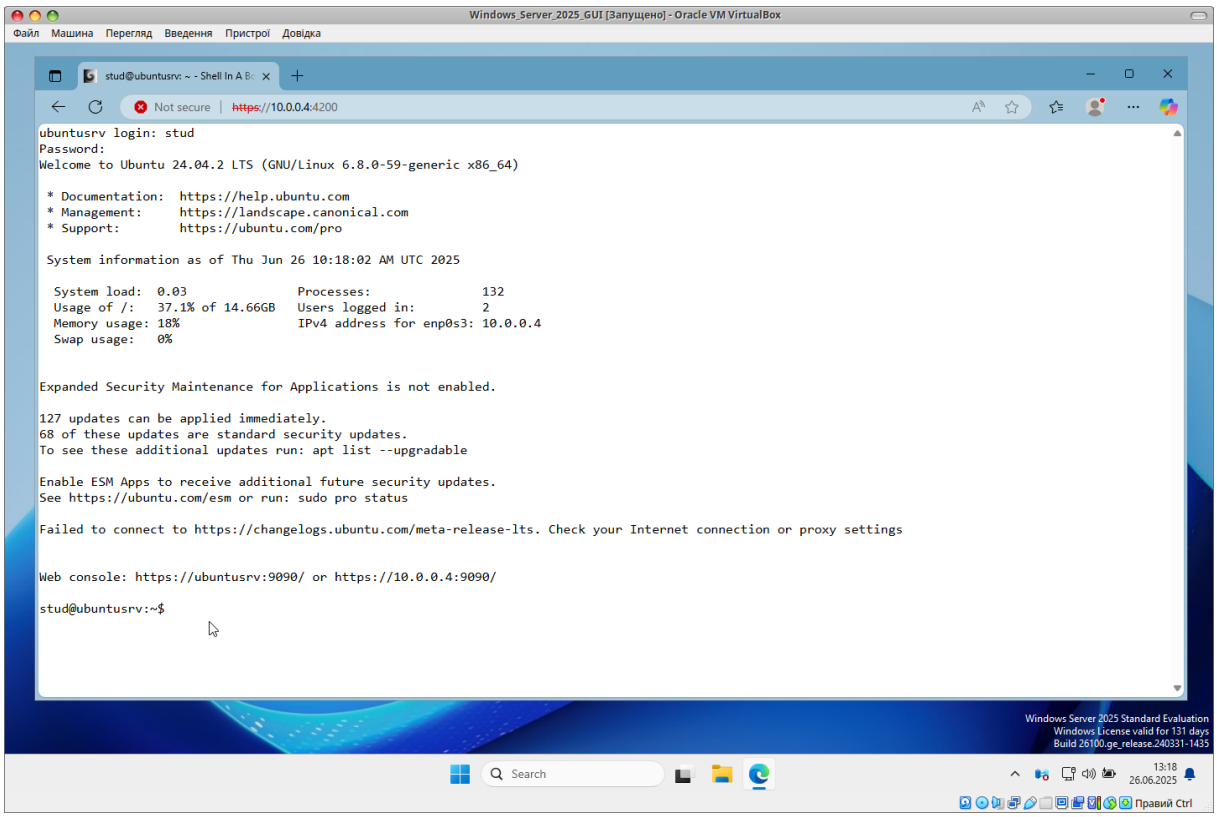


Рис. 5.10. Віддалений сеанс роботи через Web-браузер та пакунок *shellinabox*

Далі для отримання адміністративного доступу в Cockpit треба скористатися відповідною кнопкою інтерфейсу та ввести пароль користувача *root*.

Мова інтерфейсу вікон Cockpit обирається через певне меню налаштування сеансу (рис. 5.9) – в переліку мов є українська.

Для розширення можливостей моніторингу та керування ресурсами серверу у Cockpit є різноманітні плагіни.

Спеціалізований пакунок *shellinabox* (Shell In A Box) є Web-емулятором терміналу, створеним на AJAX із запуском власного Web-серверу. За замовченням *shellinabox* прослуховує TCP-порт 4200. Всі з'єднання шифруються.

В каталог */var/lib/shellinabox* за замовченням встановлюється власно підписаний SSL-сертифікат. Є можливість використання свого сертифікату.

Керування сервісами Cockpit та shellinabox відбувається за допомогою команди *systemctl*. Наприклад:

```
systemctl status cockpit
systemctl status cockpit.socket
sudo systemctl stop cockpit.service cockpit.socket
systemctl status shellinabox
sudo systemctl stop shellinabox
```

Пакунки *chkservice*, *cpu-x*, *htop*, *aptitude* побудовані із залученням бібліотеки *ncurses*, яка дозволяє будувати програми з TUI (Text User Interface).

Програма *chkservice* дозволяє переглядати список запущених сервісів в системі ініціалізації systemd та керувати ними (вихід з програми – швидка клавіша q – quit).

Програма *cpu-x* виводить інформацію про апаратуру (вихід з програми – швидка клавіша q – quit).

Детальніше інформацію про апаратуру виводять консольні команди (без TUI): *hwinfo*, *hwinfo --short*, *lshw* (інформацію можна перенаправляти за потреби, наприклад, у файли).

Програма *htop* виконує моніторинг процесів в системі в реальному часі (вихід з програми – швидка клавіша F10 або q – quit).

Програма *aptitude* є TUI-версією для менеджера пакунків *APT* (вихід з програми – швидка клавіша q – quit).

Програма *curl* дозволяє завантажувати файли з мережі, виконувати HTTP/HTTPS-запити різними методами до Web-серверів, часто використовується для роботи з API Internet-вузлів.

В Ubuntu Server адміністратори також часто використовують додаткові утилітарні консольні програми та їх поєднання, наприклад: *ip, ss, ufw, ethtool, netplan, iftop, bmon, tcpdump, nmap, traceroute, wget, lscpu, lspci, lsblk, cfdisk, mount/umount, df, free, du, less, tee, find, grep, sed, awk, top, ps, pgrep, kill, pkill, journalctl* та інші. Також дуже розповсюдженою практикою є написання *bash*- та *python*-скриптів для автоматизації певних задач.

Завдання

1. Розробити *bash*-скрипт, який автоматизує створення п’яти локальних користувачів *user21 – user25* за допомогою команди *adduser* та п’яти користувачів *user26 – user30* за допомогою *useradd*. При створенні отримувати випадкові паролі не менш ніж з 8 символів, які додавати до форматованого файлу */root/users_passwords.txt* із правом 0600. Файл повинен бути форматованим у дві колонки із символом-роздільником ‘**:**’. В якості командної оболонки для нових користувачів задати */bin/bash*. При створенні користувачів в скрипту встановлювати права на домашні каталоги – 0700.

2. Додати нові групи користувачів *department1* та *department2*, до яких включити відповідно користувачів *user21 – user25* та *user26 – user30*.

3. Створити загальний каталог */home/department1*, до якого надати доступ користувачам *user21 – user25*. Всі ці п’ять користувачів повинні мати повні права на створення та редагування файлів та каталогів один одного. Всі інші користувачі системи не повинні мати доступу до цього каталогу.

4. Створити загальний каталог */home/department2*, до якого надати доступ користувачам *user26 – user30*. Всі ці п’ять користувачів повинні мати повні права на створення та редагування файлів та каталогів один одного. Всі інші користувачі системи не повинні мати доступу до цього каталогу.

5. Створити командний *bash*-скрипт для автоматизованого видалення користувачів *user21 – user30* з їх домашніми каталогами, видаленням груп *department1* та *department2*, каталогів */home/department1* та */home/department2*, видалення файлу */root/users_passwords.txt*.

6. Перевірити роботу створених скриптів.

7. Доналаштувати сервер пакетами програм Cockpit та shellinabox. Продемонструвати роботу з ними.

8. Продемонструвати створення нового акаунту користувача через Web-консоль Cockpit. Створення виконувати через Web-браузер із оточення встановленого раніше MS Windows Server з GUI.

Відобразити у звіті основні елементи налаштування Ubuntu Server та вміст створених *bash*-скриптів. Правила оформлення звіту подані в додатку А.

Продемонструвати викладачу результати налаштувань та тестування пунктів завдання.

При захисті роботи володіти знаннями для відповіді на питання викладача за матеріалами лекцій та теоретично-практичної частини роботи.

Робота №6.
Встановлення та налаштування Web-серверу Apache2

Мета роботи: розгорнути в оточенні Ubuntu Server Web-сервер Apache2 та виконати його основні конфігурування.

Теоретично-практична частина

Конфігурування Apache2 для роботи за протоколом HTTP

Web-сервер Apache2 можна встановлювати як окремо, так і у складі, наприклад, пакетів LAMP (абревіатура від назв множини ПЗ: **L**inux, **A**pache Web-сервер, **M**ySQL, **P**HP/**P**ython/**P**erl), WAMP (**W**indows, **A**pache Web-сервер, **M**ySQL, **P**HP/**P**ython/**P**erl), XAMPP (крос-платформний, **A**pache Web-сервер, **M**ySQL, **P**HP, **P**erl). Ці пакети ПЗ дозволяють розгортати Web-сервер із підтримкою баз даних та певними інтерпретаторами для обробки Web-запитів й створення динамічного Web-контенту.

За замовченням в репозиторій Ubuntu Server версії, наприклад, 24.04.2, включений Apache2 Web-сервер версії 2.4.58.

Встановлення Web-серверу Apache2 проводять командами:

```
sudo apt update
sudo apt -y install apache2
sudo ufw allow 'Apache Full'
```

Після встановлення Apache2 буде доступним. На стороні MS Windows Server з GUI відкрийте Web-браузер та перевірте доступність Web-серверу Apache2 (рис. 6.1).

Керування службою Apache2 відбувається за допомогою команд *systemctl*:

```
systemctl status apache2
sudo systemctl stop apache2
sudo systemctl start apache2
sudo systemctl restart apache2
```

Перегляд журналу Web-серверу Apache2 відбувається за допомогою, наприклад, команди *less*:

```
less /var/log/apache2/error.log
less /var/log/apache2/access.log
```

Або, наприклад, перегляд останніх 10 рядків з журналу доступу:

```
tail -n 10 /var/log/apache2/access.log
```

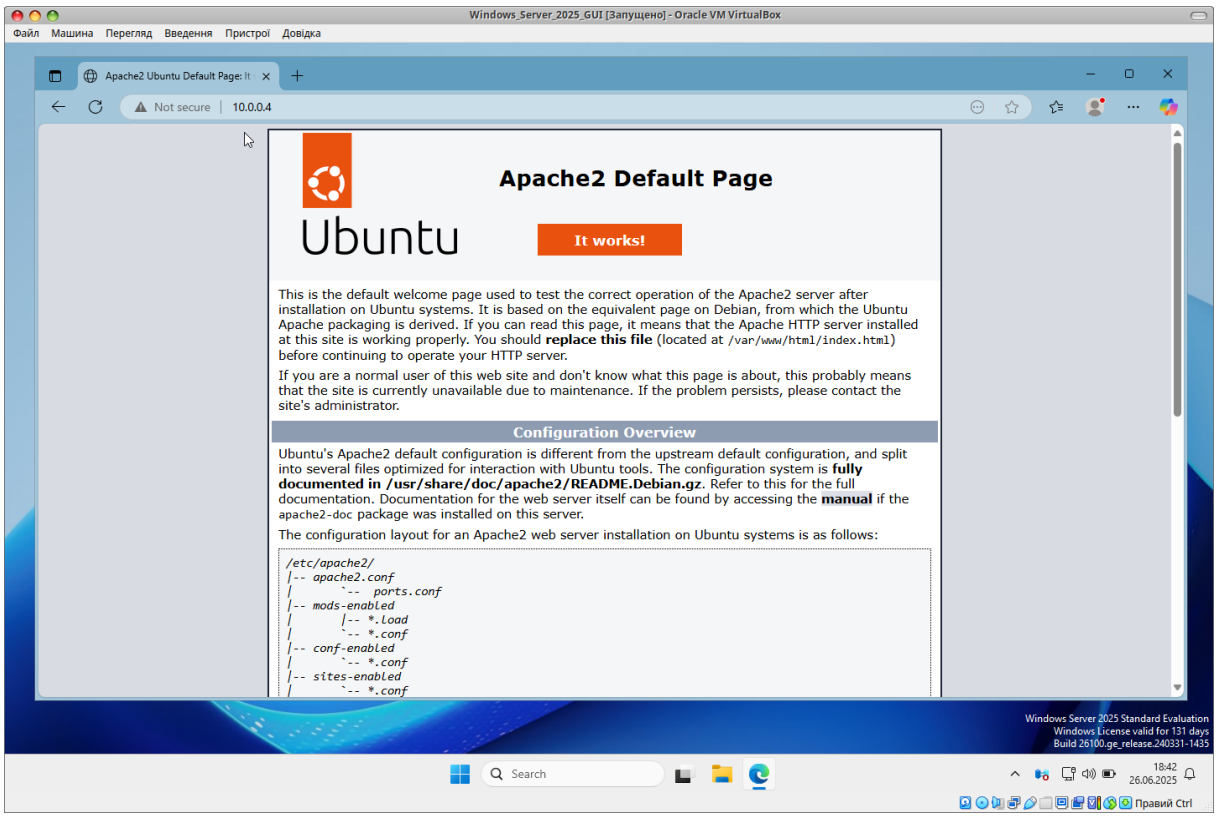


Рис. 6.1. Звернення до Web-сервера Apache2, який розгорнутий в оточені Ubuntu Server

Основні налаштування Web-серверу Apache2 знаходяться в підкаталозі */etc/apache2*. Один з основних файлів – це файл */etc/apache2/apache2.conf*.

Файли налаштування модулів Apache2 розміщені у підкаталогах */etc/apache2/mods-available* та */etc/apache2/mods-enabled*. Зверніть увагу, що файли в каталозі *mods-enabled* – це символьні посилання на відповідні модулі з каталогу *mods-available*.

Налаштування віртуальних хостів Web-серверу відбуваються через файли, які розташовані в каталогах */etc/apache2/sites-available* та */etc/apache2/sites-enabled*. Причому файли в каталозі *sites-enabled* – це символьні посилання на відповідні конфігураційні файли з каталогу *sites-available*.

За замовченням налаштований один віртуальний хост через файл /etc/*apache2/sites-available/000-default.conf*. Якщо переглянути цей файл, то стає зрозуміло, що на хосту буде прослуховуватися 80 порт TCP для роботи Web-серверу по протоколу HTTP, а домашній каталог для розміщення ресурсів сайту (*DocumentRoot*) – це каталог */var/www/html*.

Зробіть копію файлу *000-default.conf* під новим іменем *mysite.conf* та внесіть в нього зміни, що показані на рис. 6.2.

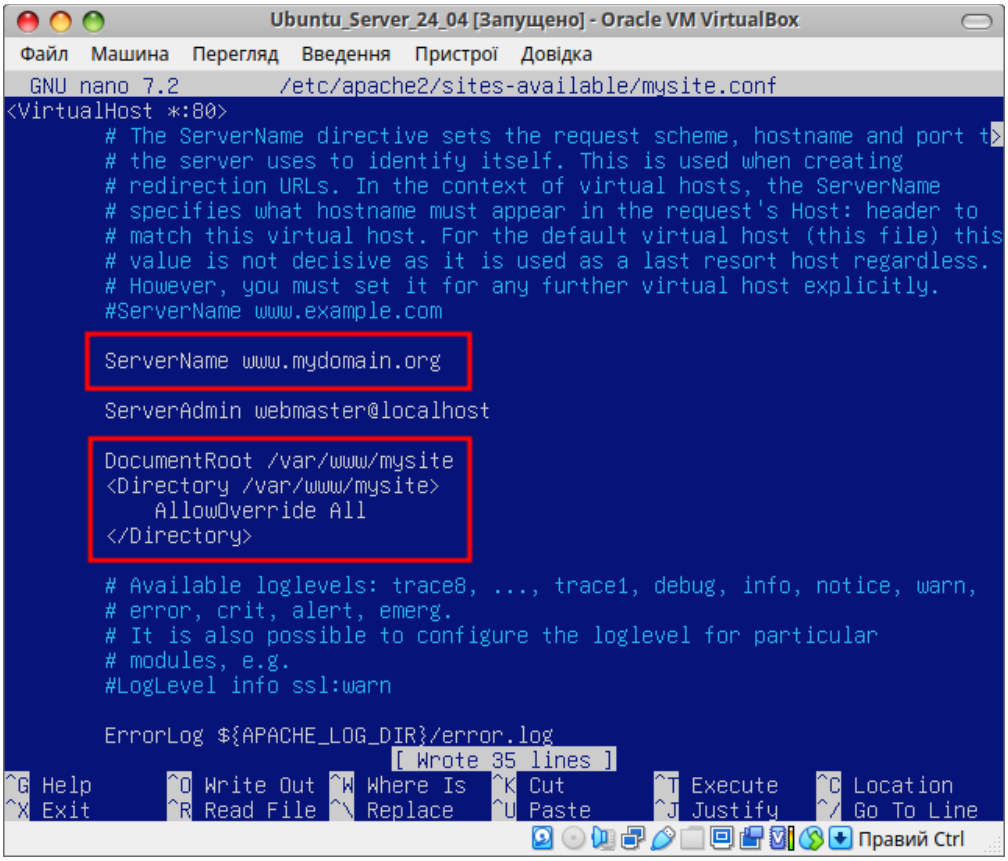


Рис. 6.2. Змінений вміст файлу */etc/apache2/sites-available/mysite.conf*

Після створення файлу конфігурації нового віртуального хосту, виконайте наступні команди для перевірки конфігурації та створення фізичного оточення у межах файлової системи сервера для розміщення складових нового сайту:

```
sudo apachectl configtest

sudo mkdir /var/www/mysite
sudo tee /var/www/mysite/index.html > /dev/null << EOF
<!DOCTYPE html>
<html lang="en">
<head>
    <title>My Site</title>
</head>
<body>
    <h1>Hello!</h1>
</body>
</html>
EOF
sudo a2ensite mysite
sudo systemctl reload apache2
```

Команда *a2ensite* робить сайт чи віртуальний хост активним та доступним. У підкаталозі */etc/apache2/sites-enabled* з'явиться символьне посилання на створену конфігурацію віртуального хосту (сайту). Інша команда *a2dissite* – відключає вказаний сайт чи віртуальний хост.

Внесіть A-записи DNS для хостів *ubuntusrv* та *www* через устаткування DNS в MS Windows Server з GUI та протестуйте завантаження тестової сторінки у Web-браузері за URL: http://www.mydomain.org/ (рис. 6.3).

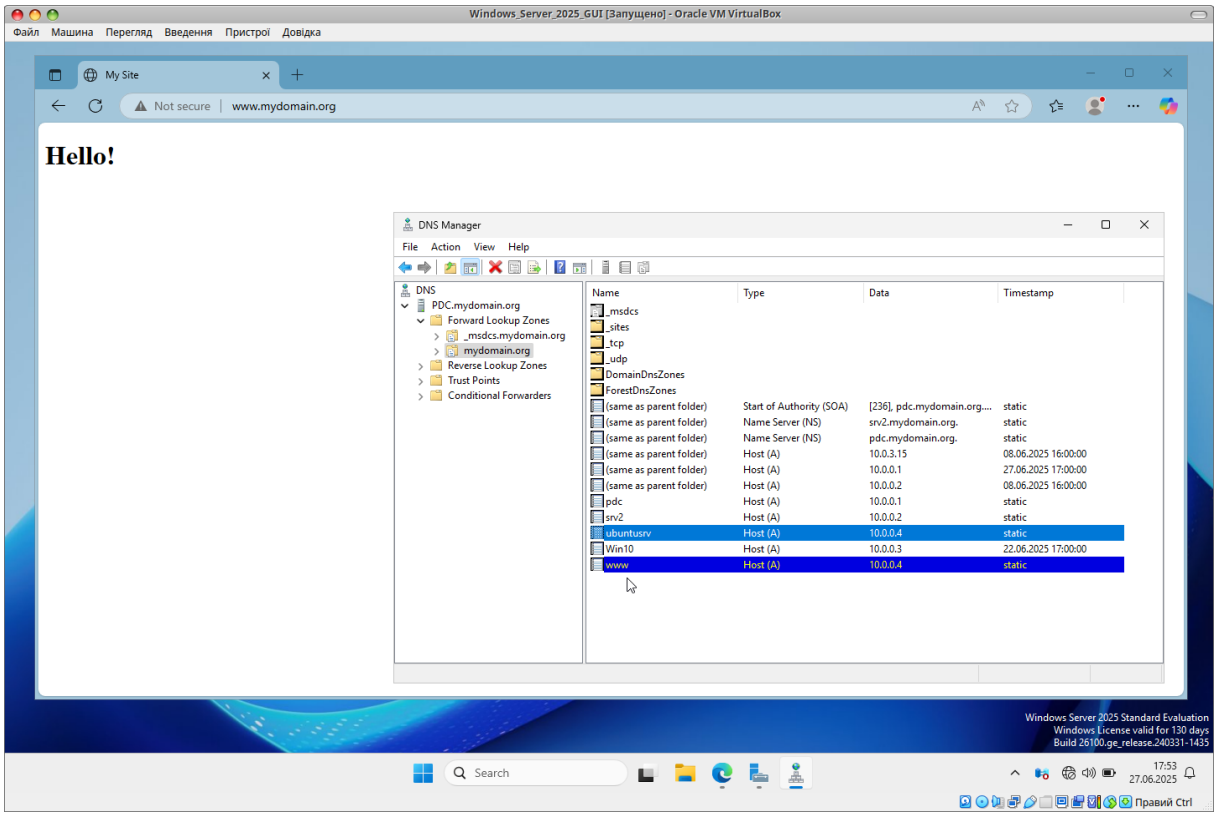


Рис. 6.3. Результат завантаження сторінки віртуального хосту *www.mydomain.org* та налаштування у зоні прямого перегляду DNS двох A-записів: *ubuntusrv* та *www*

Підключення підтримки CGI (Common Gateway Interface)

Дуже часто є необхідність використання у складі Web-серверу інтерфейсу CGI. CGI є стандартним інтерфейсом, що використовується для зв'язку Web-сервера із зовнішніми програмами (скриптами). CGI-скрипти пишуть різними мовами програмування. Найчастіше використовують, наприклад, мови: PHP, Python, Perl, C/C++ та мову командного процесора Bash.

Для використання модуля підтримки CGI у складі Apache2, виконайте команди:

```
sudo a2enmod cgi
sudo systemctl restart apache2
```

Конфігурація CGI зберігається у файлі */etc/apache2/conf-available/serve-cgi-bin.conf*. Зверніть увагу, що за замовченням каталог для CGI-скриптів в Ubuntu Server – це каталог */usr/lib/cgi-bin*. Дуже рекомендується враховувати це, оскільки розміщувати CGI-скрипти в кореневому каталозі віртуального хосту в цілях безпеки не рекомендується!

Для створення CGI-скрипту мовою Python, виконайте наступні команди:

```
sudo tee /usr/lib/cgi-bin/hello > /dev/null << EOF
#!/usr/bin/env python3

print("Content-Type: text/html")
print()
print("<html><body>")
print("<h1>HELLO, CGI!</h1>")
print("</body></html>")
EOF
sudo chmod +x /usr/lib/cgi-bin/hello
```

Зверніть увагу, що для формування вірного CGI-скрипту потрібно додати порожній виклик функції `print()` для формування ще одного символу переведення курсору на новий рядок. Роботу CGI-скрипту можна подивитися, увівши у Web-браузері URL: http://www.mydomain.org/cgi-bin/hello.

Примітка: в Ubuntu Server версії 24.04.2 використовується Python версії 3.12.3. Більш детальніше про роботу із CGI мовою Python можна подивитися за посиланням: https://docs.python.org/3.12/library/cgi.html. Слід зауважити, що модуль *cgi.py* із складу стандартної бібліотеки мови Python, був помічений розробниками Python як застарілий у версії 3.11 та видалений зі складу стандартної бібліотеки з версії 3.13. Як зазначено в документації, модуль *cgitb* не використовується жодним з основних Web-фреймворків мовою Python (Django, Pyramid, Plone, Flask, CherryPy та Bottle). В якості альтернативи для версій 3.13 та вище можна використовувати форк: https://github.com/jackrosenthal/legacy-cgi, або скористатися більш новітніми технологіями.

Для використання CGI виключно для певного віртуального хосту, потрібні окремі доналаштування конфігураційного файлу цього хосту. Більш детальніше це описано на сторінці документації:

https://httpd.apache.org/docs/2.4/mod/mod_cgi.html

Конфігурування Apache2 для роботи за протоколом HTTPS

Розглянутий вище приклад розгортання Web-серверу, що працює за протоколом HTTP, як сучасне рішення, не є вдалим. Це простий приклад, але в сучасному світі використовують для більшості сайтів протокол HTTPS, який підтримує шифрування з'єднань.

Перед активуванням режиму доступу за протоколом HTTPS, потрібно виконати певні команди, для генерування/отримання сертифікату безпеки та ключа. Сертифікат серверу є публічним, а ключ – приватним.

Сертифікати, які підписані певними організаціями та видані компаніям для їх сайтів на певний період, є свідоцтвом того, що сайт, до якого звертається клієнт, є саме тим сайтом, а не підробкою. Такі сертифікати платні. Але є можливість використовувати власноруч підписані сертифікати.

Перед початком створення сертифікату потрібно перевірити налаштування часу в Ubuntu Server. Наприклад, можна скористатися командами:

```
sudo dpkg-reconfigure tzdata
обрати time zone: Europe / Kyiv
скоригувати за необхідністю час:
sudo date -s 13:07
перевірити поточні налаштування:
timedatectl
```

Для створення ключа та власноруч підписаного сертифікату виконують, наприклад, команди:

```
sudo -s
cd /root
openssl req -x509 -newkey rsa:4096 \
-keyout server.key -out server.crt -sha256 -days 30 -nodes
```

Врахуйте необхідну інформацію при відповідях на питання останньої команди:

– PEM pass phrase, наприклад: *mydomain* (не буде відображатися при введені);

– Country Name: UA;

– State or Province Name: Dnipro;

– Locality Name: Dnipro;

– Organization Name: My organization;

– Organizational Unit Name: IT;

– Common Name: *www.mydomain.org*;

– Email Address: для прикладу можна залишити порожнім, натиснувши клавішу Enter.

Термін дії такого сертифікату заданий у відповідній опції та складає у прикладі 30 днів.

Далі в *root*-оточені виконують команди по підготовці використання створених файлів в системі:

```
cp server.crt /etc/ssl/certs/
cp server.key /etc/ssl/private/
```

Для роботи Apache2 через HTTPS залучають модуль *ssl* та активізують віртуальний хост з конфігурацією, яка налаштована на прослуховування 443-го порту TCP (або створюють власний віртуальний хост за зразком):

```
sudo a2enmod ssl
sudo a2ensite default-ssl
```

Наступним кроком є редагування файлу конфігурації віртуального хосту (рис. 6.4) – потрібно внести відомості про використання згенерованого сертифікату та приватного ключа.

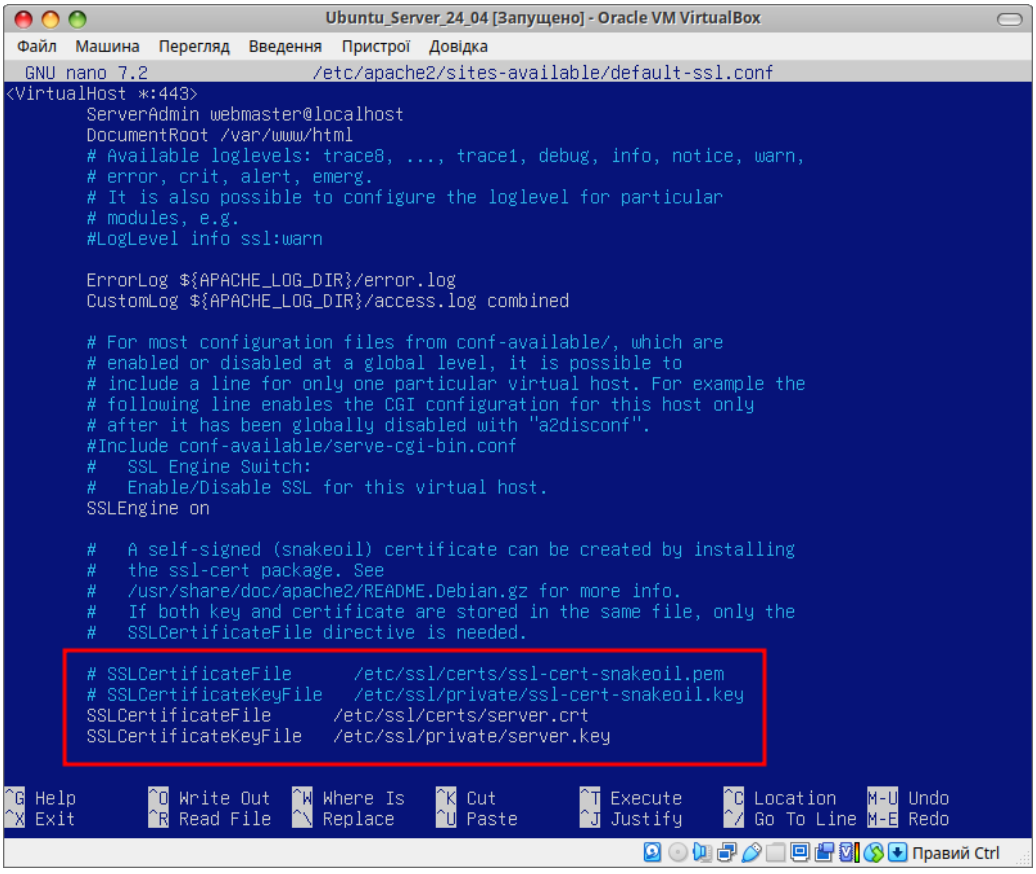


Рис. 6.4. Приклад внесення змін у конфігураційний файл віртуального хосту, що буде працювати за протоколом HTTPS

Після цього роблять перезавантаження сервісу (`sudo systemctl restart apache2`) та тестують роботу по протоколу HTTPS через Web-браузер. Зверніть увагу, що при роботі із сайтом у Web-браузері потрібно погодитися на з'єднання при власно підписаному сертифікаті. Як правило в подальшому, для уникнення подібного повідомлення, потрібно експортувати сертифікат із серверу та імпортувати його до переліку сертифікатів до яких є довіра.

Завдання

Налаштувати Apache2 у складі Ubuntu Server. Розгорнути два віртуальні хости *www.mydomain.org* та *console.mydomain.org* із доступом по протоколу HTTPS. Для хосту *www.mydomain.org* організувати CGI, в якому буде функціонувати CGI-скрипт *systeminfo*. Скрипт повинен формувати html-сторінку з основною інформацією про сервер. За основу можна взяти, наприклад, наступний програмний код мовою Python з використанням викликів команд GNU/Linux-сумісних ОС:

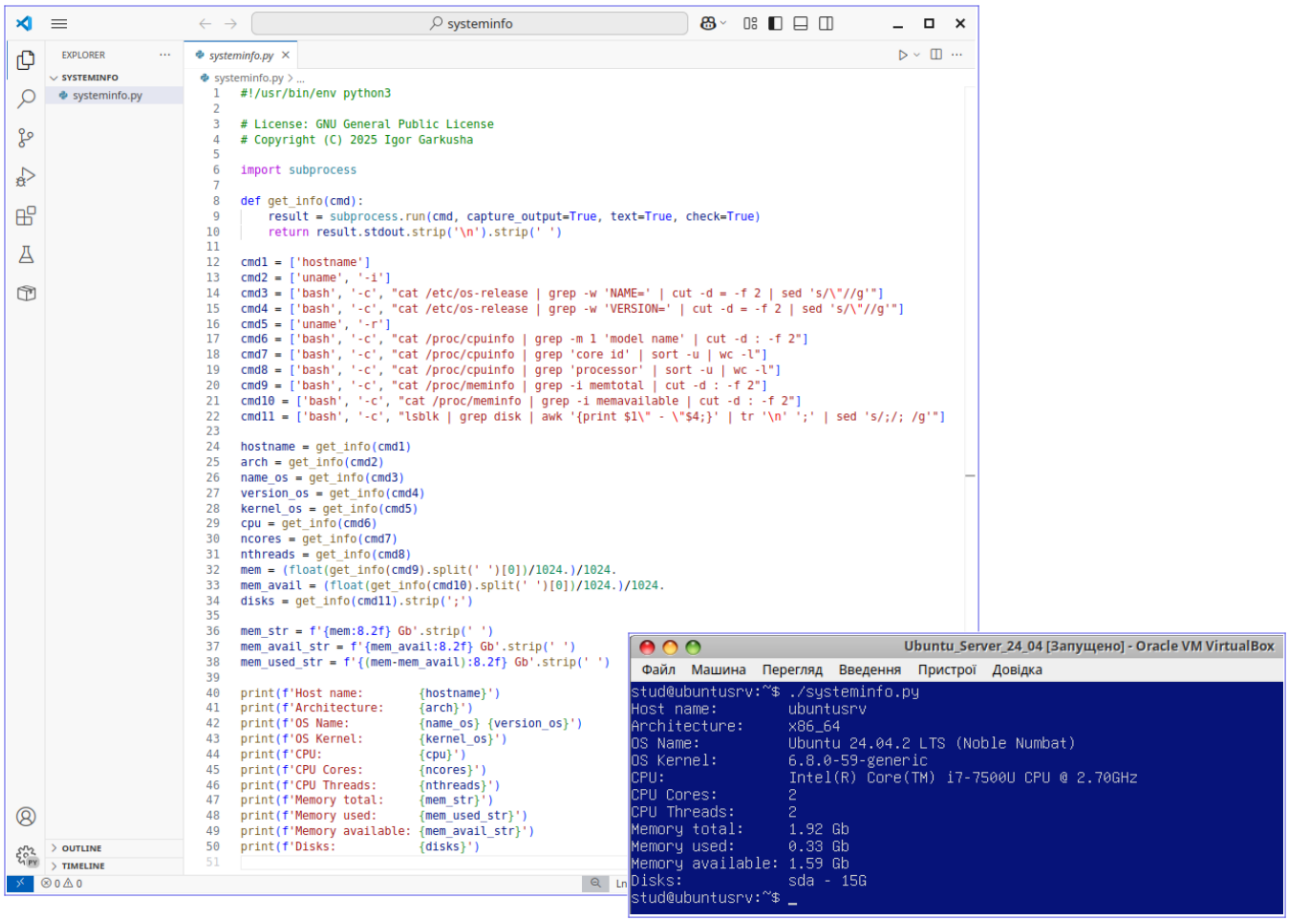


Рис. 6.5. Приклад скрипту мовою Python для виведення в термінал консолі основної інформації про апаратні та програмні особливості системи з результатом виконання в Ubuntu Server

При зверненні до віртуального хосту *console.mydomain.org* повинно відбуватися перенаправлення на адресу з портом для роботи через пакет *shellinabox*, що був розглянутий в попередній роботі. Для виконання цієї частини завдання, скористатися можливістю перенаправлення, яка вказується у конфігураційному файлі віртуального хосту (дивитися у документації Apache2: https://httpd.apache.org/docs/2.4/mod/mod_alias.html#redirect).

Відобразити у звіті конфігураційні файли налаштування віртуальних хостів, програмний код створеного CGI-скрипту з коментарями та результати його роботи. Правила оформлення звіту подані у додатку А.

Продемонструвати викладачу результати налаштування та відповісти на питання стосовно виконаного завдання.

Критерії оцінювання виконання робіт

Виконання завдань, які описані в практичних частинах робіт, та захист результатів, що подані здобувачем у звітах, є обов'язковим.

В залежності від складності практичної частини роботи, на виконання завдань відводиться певна кількість годин, обсягом, що представлений в робочій програмі дисципліни.

Після виконання практичної частини роботи, здобувач складає звіт, в якому повинен описати хід виконання завдання та надати висновки щодо отриманих результатів роботи. Вимоги по оформленню звітності подані у додатку А.

Захист звіту з виконаної роботи проводиться під час проведення заняття у встановлений розкладом основний час або у додатковий час, який погоджений із викладачем.

Узагальнені критерії оцінки виконаної роботи наведені у таблиці:

Критерії оцінювання виконання та захисту роботи здобувачем	*Рейтингова оцінка*	*Інституційна оцінка*
Результати виконання роботи вірні згідно вимог, описаних в завданні та наданих викладачем в ході лекційних занять. Звіт оформлений згідно вимог, описаних в додатку А. На всі поставлені питання викладача при захисті роботи надані вірні відповіді. Робота захищена.	90 – 100	відмінно
Результати виконання роботи вірні згідно вимог, описаних в завданні та наданих викладачем в ході лекційних занять. Звіт оформлений згідно вимог, описаних в додатку А. На 80% поставлених питань викладача при захисті роботи були надані вірні відповіді. Робота захищена.	80 – 89	добре
Результати виконання роботи вірні згідно вимог, описаних в завданні та наданих викладачем в ході лекційних занять. Звіт оформлений згідно вимог, описаних в додатку А. На 70% поставлених питань викладача при захисті роботи були надані вірні відповіді. Робота захищена.	74 – 79	
Результати виконання роботи містять помилки. Є відхилення від поставлених вимог оформлення звітності. Під час захисту здобувач надав 50% вірних відповідей на поставлені питання викладача. Робота захищена.	60 – 73	задовільно
Результати виконання роботи невірні або звіт відсутній, або здобувач не може під час захисту результатів роботи відповісти на питання викладача. Робота не була захищена.	0 – 59	незадовільно

Перелік рекомендованих джерел

1. Bekim Dauti, Dr. Erdal Ozkaya. Windows Server 2025 Administration Fundamentals: A beginner's guide to managing and administering Windows Server environments, 4th Edition. – Packt Publishing, 2025. – 630 p. ISBN-10: 1836205015, ISBN-13: 978-1836205012.

2. Thomas Lee. Windows Server 2019 Automation with PowerShell Cookbook: Powerful ways to automate and manage Windows administrative tasks, 3rd Edition. – Packt Publishing, 2019. – 542 p. ISBN-10: 1789808537, ISBN-13: 978-1789808537.

3. Richard Petersen. Ubuntu 24.04 LTS Server: Administration and Reference. – Surfing Turtle Press, 2025. – 720 p. ISBN-10: 1949857549, ISBN-13: 978-1949857542.

4. Richard Blum, Christine Bresnahan. Linux Command Line and Shell Scripting Bible, 4th Edition. – Wiley, 2021. – 832 p. ISBN-10: 1119700914, ISBN-13: 978-1119700913.

5. Al Sweigart. Automate the Boring Stuff with Python, 3rd Edition. – No Starch Press, 2025. – 672 p. ISBN-10: 1718503407, ISBN-13: 978-1718503403.

6. Ganesh Sanjiv Naik. Mastering Python Scripting for System Administrators: Write scripts and automate them for real-world administration tasks using Python. – Packt Publishing, 2019. – 318 p. ISBN-10: 178913322X, ISBN-13: 978-1789133226.

7. Mastering Apache Web Server: A Comprehensive Guide / CloudMatrix s.r.o. – Independently published, 2024. – 340 p. ISBN-13: 979-8340786579.

Додаток А.
Вимоги до оформлення звітності

Звіт оформлюється на листах формату А4 та включає титульний аркуш (зразок оформлення представлений на рис. А.1) та опис роботи за представленим нижче зразком.

У разі захисту звіту з виконання роботи при аудиторній формі навчання, звіт друкується та надається викладачу на розгляд.

Для захисту виконаної роботи у дистанційній (online) формі навчання, звіт подається до захисту в електронному форматі PDF (Portable Document Format) та надсилається викладачеві через засоби online-спілкування для розгляду.

Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Факультет інформаційних технологій
Кафедра інформаційних технологій та комп'ютерної інженерії

Звіт
з роботи № __
дисципліни АОСМ

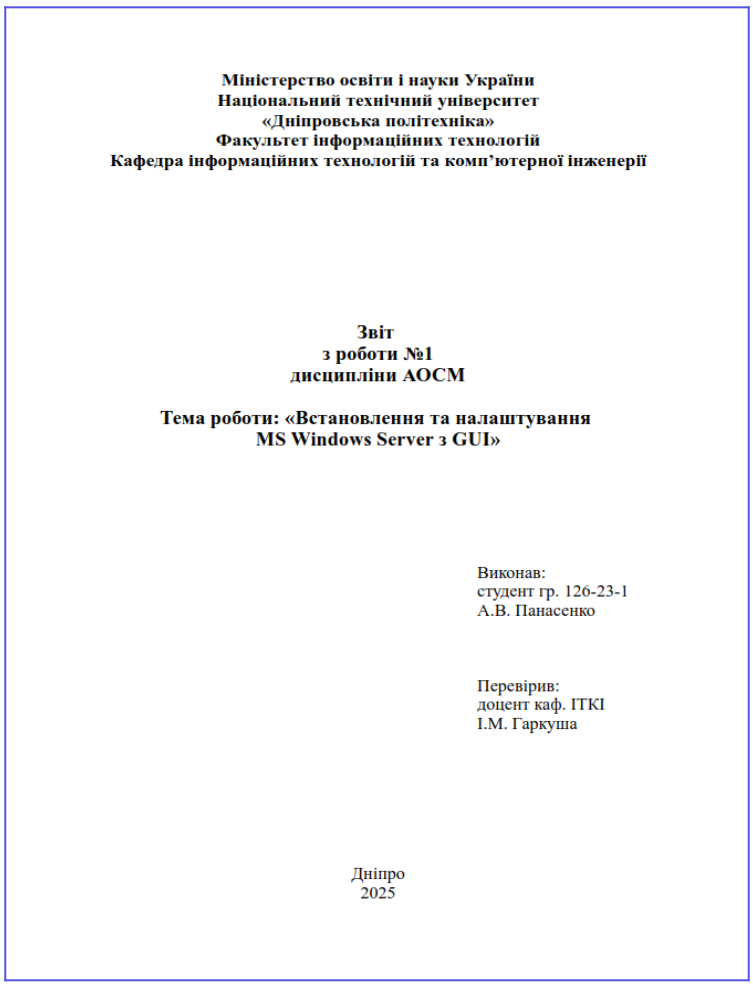
Тема роботи: « _____ »

Виконав:
студент гр. *шифр групи*
Ініціали та прізвище студента

Перевірив:
посада каф. ІТКІ
Ініціали та прізвище викладача

Дніпро
Поточний рік складання звіту

Рис. А.1. Форма титульного аркуша звіту



Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Факультет інформаційних технологій
Кафедра інформаційних технологій та комп'ютерної інженерії

Звіт
з роботи №1
дисципліни АОСМ

Тема роботи: «Встановлення та налаштування
MS Windows Server з GUI»

Виконав:
студент гр. 126-23-1
А.В. Панасенко

Перевірив:
доцент каф. ІТКІ
І.М. Гаркуша

Дніпро
2025

Рис. А.2. Приклад оформленого титульного аркуша звіту

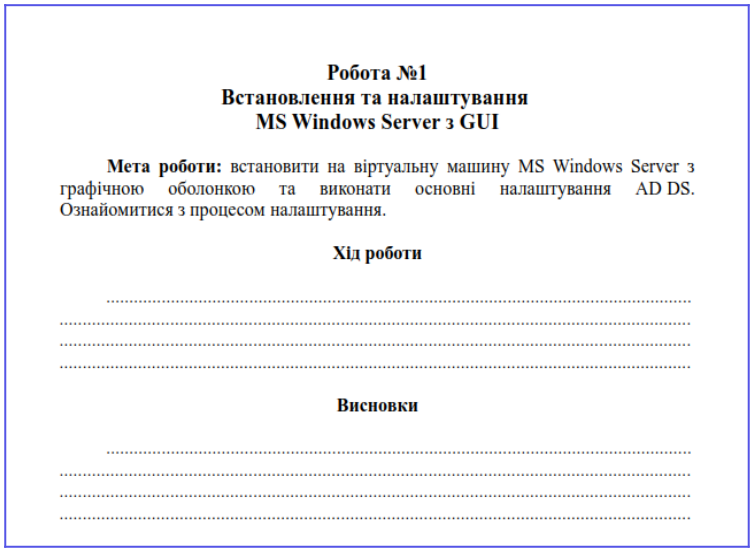
Опис виконаної роботи в звіті розпочинається з наступного аркуша. В горі сторінки, по центру, вказується номер роботи та її тема. Після цього вказується мета роботи. Через рядок по центру сторінки йдуть слова *Хід роботи* і далі через рядок розпочинається основний текст опису виконаної роботи.

Після завершення опису роботи, через рядок, йде частина, яка присвячена висновкам по проведеній роботі. Вона починається зі слова *Висновки*, розміщеного по центру листа та через рядок починається текст з висновками по роботі.

Приклад загального вмісту опису роботи представлений на рис. А.3.

Написання основного тексту ходу роботи та висновків йде **від третьої особи**!!! Тобто, є невірним використання у звіті висловів, на кшталт: “В ході роботи я встановив Ubuntu Server”. Замість такого вислову вірно буде написати: “В ході роботи в оточенні Oracle VirtualBox створена віртуальна машина та встановлено Ubuntu Server”. Або замість вислову, на кшталт: “Під час виконання роботи ми опанували налаштування серверу

домену MS Windows”, вірно буде написати: “Під час виконання роботи опановано налаштування серверу домену MS Windows”.



Робота №1
Встановлення та налаштування
MS Windows Server з GUI

Мета роботи: встановити на віртуальну машину MS Windows Server з графічною оболонкою та виконати основні налаштування AD DS. Ознайомитися з процесом налаштування.

Хід роботи

.....
.....
.....
.....

Висновки

.....
.....
.....
.....

Рис. А.3. Приклад загального подання опису роботи

Текст звіту оформляється шрифтом Times New Roman з розміром 14, міжрядковий інтервал 1 – 1,5. Абзацний відступ – 5 символів.

Шрифтом з розміром 10 оформлюють тексти скриптів. При цьому бажано використовувати один з наступних моноширинних шрифтів: Source Code Pro, Monospace, Consolas, DejaVu Sans Mono, Courier New, Monospaced, Menlo, SF Mono або подібні.

Вирівнювання тексту опису в звіті – по ширині сторінки.

Вирівнювання тексту скрипту в звіті – ліворуч.

Вирівнювання рисунків та підписів до них – по центру сторінки.

Вирівнювання таблиць (якщо такі будуть) – по центру сторінки.

Якщо текст коду скрипту не є великим за обсягом, то його можна подати у вигляді знімку з екрану, причому фон повинен бути не чорного кольору, а текст коду скрипту повинен добре виділятися. Приклади таких знімків з екрану представлені на рис. 5.2, 6.2 та 6.5. Рисунок розміщують по центру сторінки звіту та нижче за ним по центру дають підпис для нього. Наприклад: “Рисунок 1 – Текст коду скрипту для створення користувачів”.

Якщо в тексті звіту наводиться рисунок, то на нього обов’язково повинно бути посилання з тексту опису ходу роботи та пояснення певних особливостей, що є на рисунку.

При складанні тексту висновків, потрібно вказати на результати щодо досягнення поставленої мети роботи. Вказати особливості виконання роботи та складнощі. При цьому доречно залучати вислови на кшталт: “В роботі розглянуті...”, “...виконані...”, “Отриманий результат дозволив...”, “Використання умов дозволило...” та ін.

Навчальне видання

Гаркуша Ігор Миколайович

АДМІНІСТРУВАННЯ ОПЕРАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Методичні рекомендації до виконання лабораторних робіт
для здобувачів ступеня бакалавра освітньо-професійної програми
«Інформаційні системи та технології»
спеціальності 126 Інформаційні системи та технології

Видано в авторській редакції.

Електронний ресурс.
Підписано до видання 03.08.2025. Авт. арк. 4,4.

Національний технічний університет «Дніпровська політехніка».
49005, м. Дніпро, просп. Дмитра Яворницького, 19.