Лабораторна робота №3

Встановлення служби каталогів Active Directory у Windows Server 2022

Мета: навчитися налаштовувати контролер домену Active Directory на базі Windows Server 2022.

Інструменти: гіпервізор VirtualBox, (за потреби) мережний емулятор GNS3, модель комп'ютерної мережі, що будується у відповідності до варіанту завдання.

Теоретичні відомості

Опишемо основні кроки, потрібні для розгортання контролера домену Active Directory на основі Windows Server 2022.

Створюємо схему адресації, яка відповідає схемі (рис. 3.1) та таблиці 3.2.

Для прикладу використаємо схему адресації для мережі 192.168.40.240/28, яка подана у таблиці 3.1.

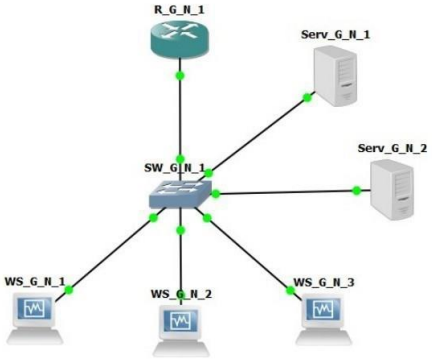


Рис. 3.1. Топологія мережі

Таблиця 3.1

Параметри адресації мережі

Мережа / Пристрій	Інтерфейс / Мережний адаптер / Шлюз	IP-адреса	Маска	Префікс
Мережа A	-	192.168.40.240	255.255.255.240	/28
Маршрутизатор R_22_40_1 або резерв NAT Network VirtualBox	Eth1/0	192.168.40.241	255.255.255.240	/28
Комутатор SW_22_40_1 або резерв NAT Network VirtualBox	Інтерфейс Vlan 1	192.168.40.242	255.255.255.240	/28
Сервер Serv_22_40_1	Мережний адаптер	192.168.40.243	255.255.255.240	/28
	Шлюз за замовчуванням	192.168.40.241	-	-
Сервер Serv_22_40_2	Мережний адаптер	192.168.40.244	255.255.255.240	/28
	Шлюз за замовчуванням	192.168.40.241	-	-
Робочі станції WS_22_40_1 - WS_22_40_3	Мережний адаптер	DHCP	255.255.255.240	/28
	Шлюз за замовчуванням	192.168.40.241	-	-

Створюємо в Oracle VirtualBox дві віртуальні машини Windows Server 2022, як у лабораторній роботі №1. Імена віртуальних машин та серверів (під серверами маються на увазі імена віртуальних хостів) – відповідно до топології мережі (рис. 2.1. Serv_G_N_1 та Serv_G_N_2). Рекомендовано використати, створені у лабораторних роботах №1 та 2 віртуальні машини Windows Server 2022 у якості серверів Serv_G_N_1 та Serv_G_N_2.

Зверніть увагу: Serv_G_N_2 створено шляхом клонування Serv_G_N_1. У такому випадку MAC-адреси мережевих адаптерів можуть бути однаковими, що викликає мережеві конфлікти. Перед запуском необхідно перевірити та змінити MAC-адресу Serv_G_N_2 на унікальну.

Важливо. Імена серверів та робочих станцій у домені мають відповідати умовам завдання.

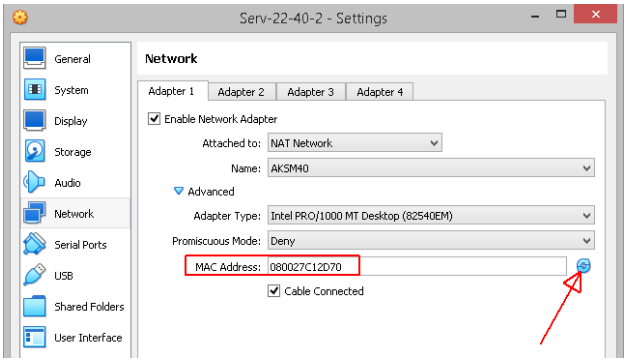


Рис. 3.2. Генерація MAC-адреси в мережевому інтерфейсі. Виконується на вимкненій ВМ

Налаштовуємо ір-адреси та підключення серверів відповідно до створеної схеми адресації та реалізації роботи. Дозволяємо на обох серверах вхідний icmp v4 трафік. Для цього обираємо ***[Local Server][Windows Defender Firewall]-[Advanced Settings]-[Inbound Rules]-[File and Printer Sharing (Echo Request ICMP v4 In)]*** (рис. 3.3).

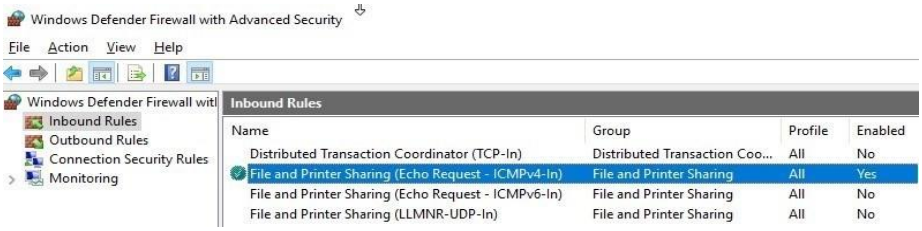


Рис. 3.3. Налаштування правила для вхідного трафіку за ICMP-v4

Якщо ви будуєте модель мережі лише у VirtualBox,* без використання GNS,** то в Oracle VirtualBox налаштовуємо параметри підключення до мережі для обох серверів як NAT Network, Internal Network або Host-Only adapter (рис. 3.3). Використання NAT Network найбільш універсальний метод. ***Якщо ви будуєте модель мережі у GNS та VirtualBox, то для серверів можна лишити віртуальний адаптер за замовчуванням – маршрутизація налаштовується на GNS3.

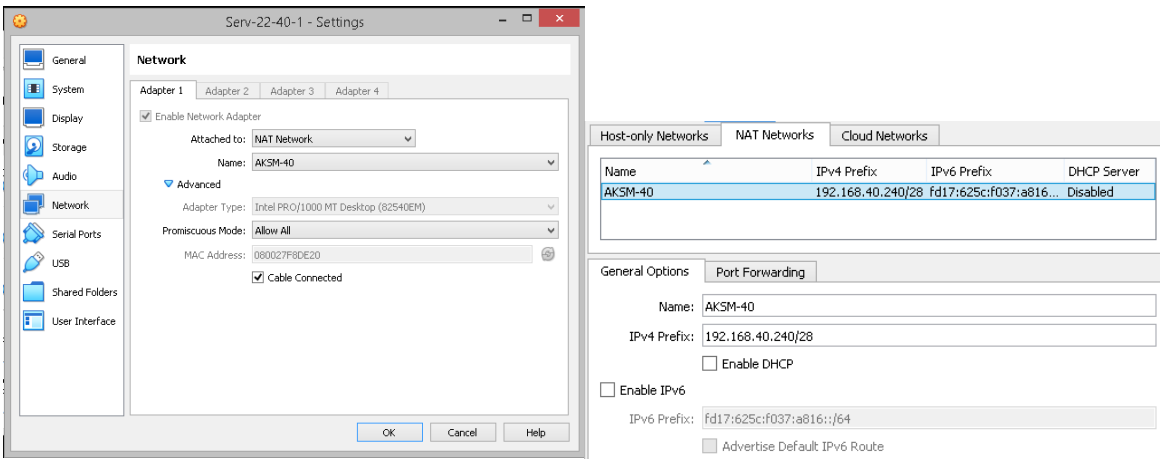


Рис. 3.4. Налаштування віртуального адаптера VirtualBox та мережі NAT Network (для моделі мережі, побудованої у VirtualBox без використання GNS)

Налаштування мережевих параметрів перед встановленням контролерів домену

Перед запуском майстра встановлення служби Active Directory Domain Services (AD DS) необхідно виконати попереднє налаштування мережевих параметрів серверів. Правильна конфігурація мережі є важливою умовою коректної роботи служби DNS, яка використовується Active Directory для автоматичної реєстрації службових записів та забезпечення взаємодії між контролерами домену.

У процесі встановлення контролера домену система автоматично створює та реєструє у DNS низку службових записів (SRV-записів), які використовуються клієнтами та іншими контролерами домену для пошуку необхідних служб каталогу. Тому до запуску майстра встановлення необхідно переконатися, що адреси DNS-серверів налаштовані коректно.

У даній лабораторній роботі використовується віртуальна мережа NAT Network VirtualBox з адресним простором 192.168.40.240/27. Шлюз (Gateway) цієї мережі має адресу 192.168.40.241

У межах лабораторного стенду використовуються два сервери, які будуть виконувати роль контролерів домену:

Serv-22-40-1 DC1 192.168.40.243
Serv-22-40-2 DC2 192.168.40.244

Перед встановленням ролі контролера домену на кожному сервері необхідно задати такі параметри DNS:

Для сервера Serv-22-40-1 (DC1)
Preferred DNS server: 127.0.0.1
Alternate DNS server: 192.168.40.244
Для сервера Serv-22-40-2 (DC2)
Preferred DNS server: 192.168.40.243

У даній конфігурації як основний DNS-сервер використовується локальний сервер (127.0.0.1), що дозволяє контролеру домену використовувати власну службу DNS. Як альтернативний DNS-сервер вказується адреса другого контролера домену, що забезпечує відмовостійкість та можливість взаємної реплікації DNS-даних між серверами.

Власна служба DNS встановлюється та налаштовується під час виконання майстра встановлення контролера домену (Active Directory Domain Services Configuration Wizard). У процесі інсталяції майстер автоматично створює DNS-зону домену та реєструє необхідні службові записи (SRV-записи), які використовуються для пошуку контролерів домену та інших служб Active Directory у мережі.

Після завершення конфігурації мережевих параметрів рекомендується перевірити правильність введених значень IP-адреси, маски підмережі, шлюзу та DNS-серверів. Некоректні мережеві налаштування можуть призвести до помилок під час встановлення служби Active Directory або до некоректної реєстрації DNS-записів.

На рисунку нижче наведено приклад типових налаштувань мережевих адаптерів серверів.

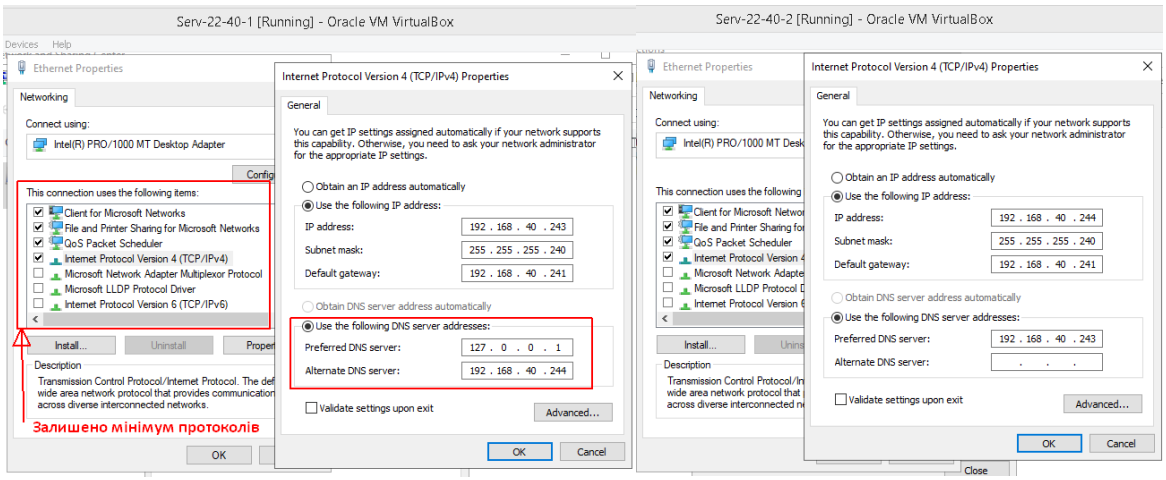


Рис. 3.5. Зразок мережевих налаштувань серверів для NAT Network 192.168.40.240/28. Для мінімізації трафіку залишено мінімум протоколів.

Перевіряємо можливість інформаційного обміну між серверами (ping, rpcping, tracert)

Встановлення ролі Active Directory Domain Services та створення контролера домену

Додаємо ролі AD DS та DC через меню ***[Dashboard][Add roles and features]*** Ім'я домену верхнього рівня - **surname.net**, де **surname** - ваше прізвище транслітом. Основні кроки налаштування цих ролей показано на рис. 3.6-3.14.

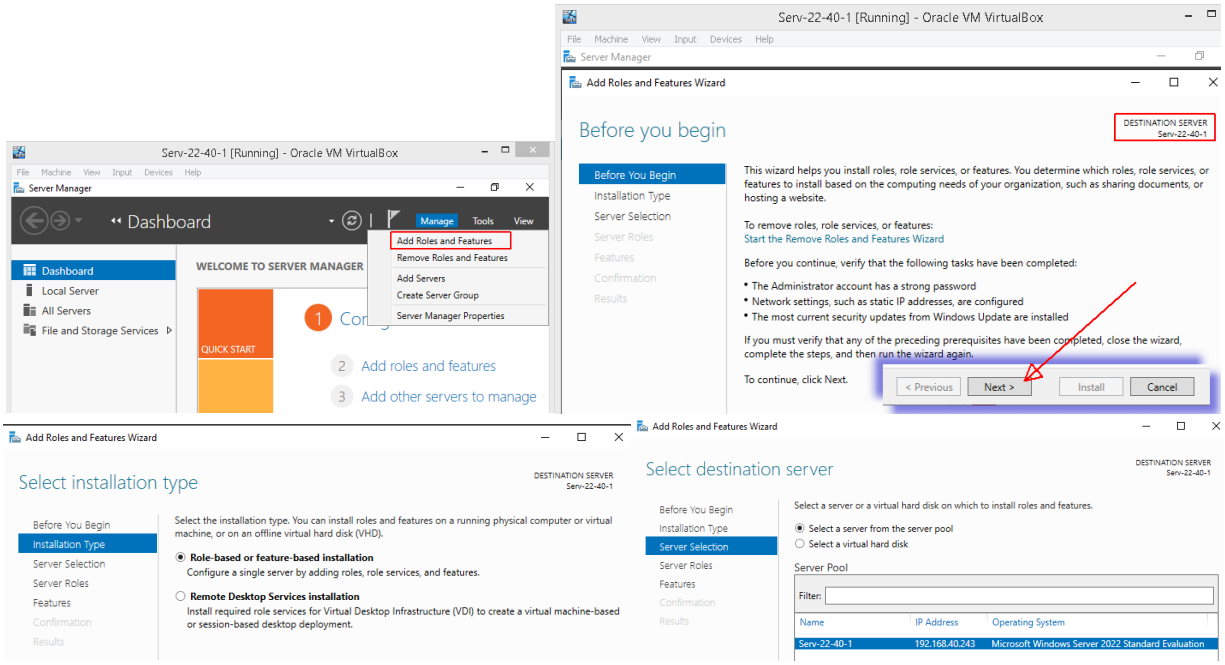


Рис. 3.6

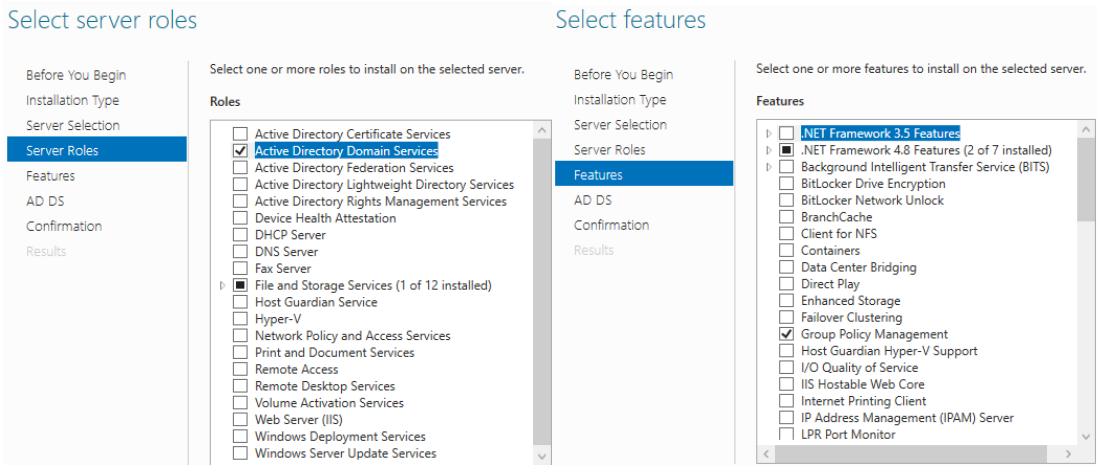


Рис. 3.7

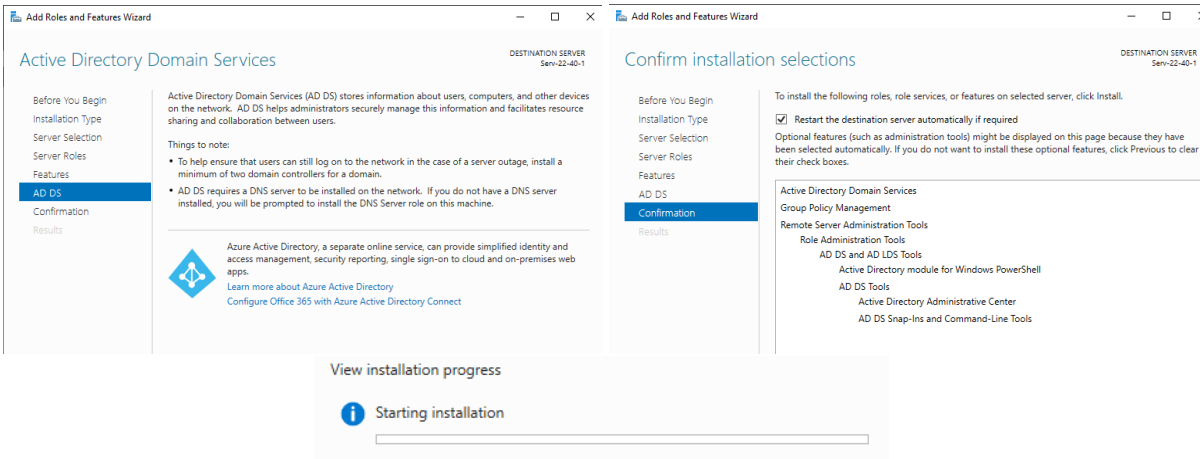


Рис. 3.8

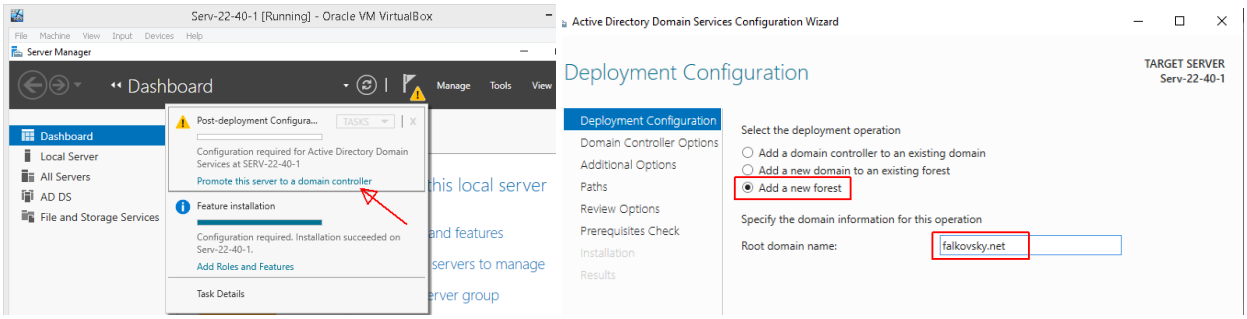


Рис. 3.9

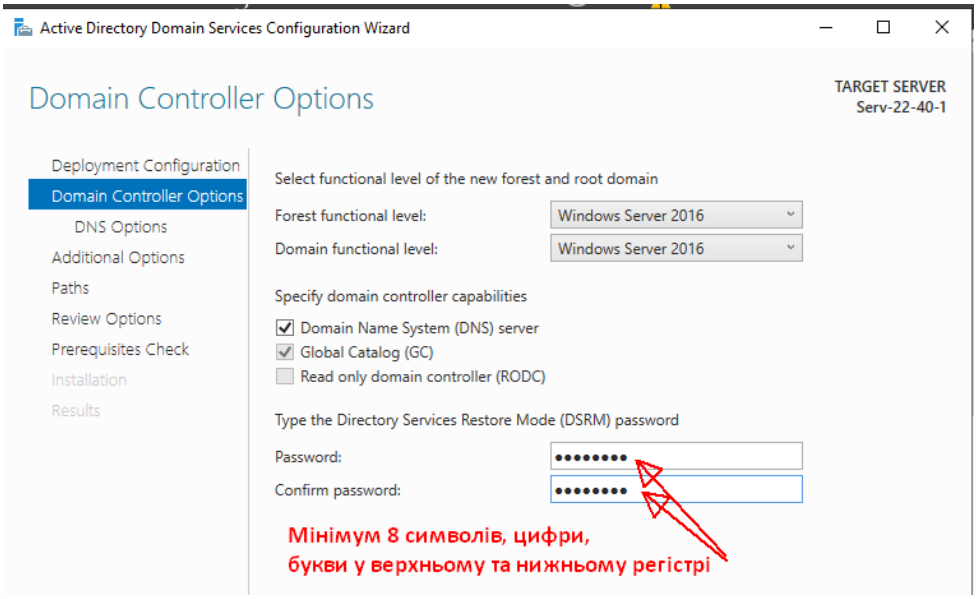


Рис. 3.10

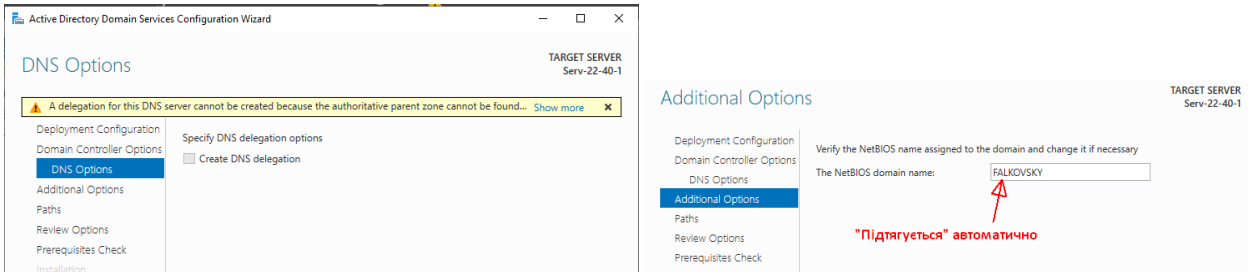


Рис. 3.11

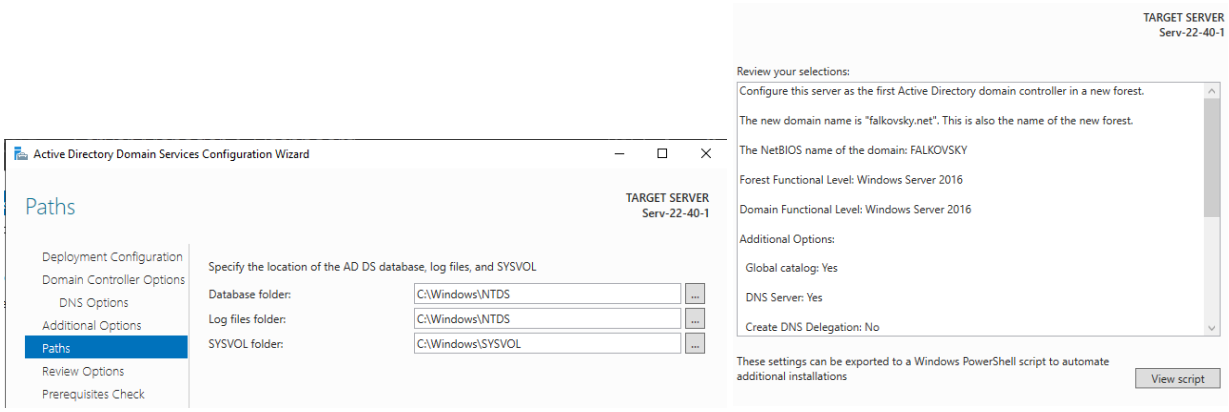


Рис. 3.12

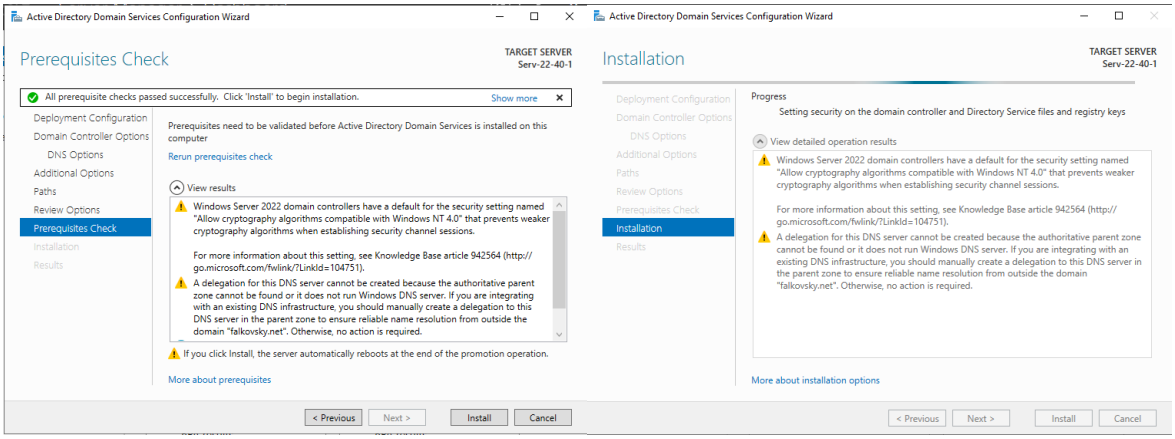


Рис. 3.13

Завершуємо сеанс локального адміністратора на проінстальованому контролері домену та входимо під адміністратором домену. Перевіряємо зв'язок та дієздатність DC-серверу на обох серверах командою

nslookup surname.net

Додаємо у домен **Serv_G_N_2** та надаємо йому роль додаткового DC. Щоб зробити другий сервер додатковим контролером домену, на ньому також потрібно встановити роль Active Directory Domain Services, але на етапі вибору конфігурації розгортання (Deployment Configuration) замість *Add to a new forest* (рис.3.9) обрати *Add a domain controller to an existing domain.* У якості облікових даних адміністратора домену ***surname.net*** при включенні серверу чи робочої станції до домену ***surname.net*** можливе використання двох типів рядків:

surname.net\Administrator або ***Administrator@surname.net***

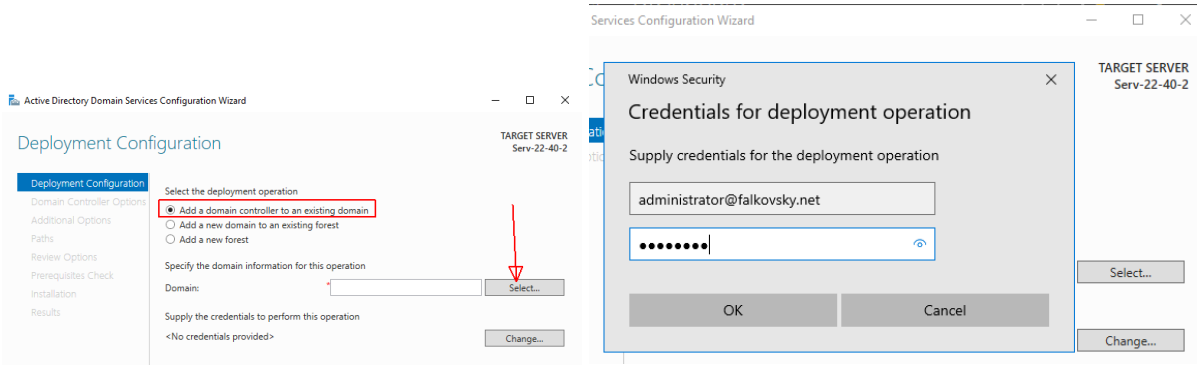


Рис. 3.14

Вказівки

- Імена комп'ютерів на першому і другому сервері мають відрізнятися та відповідати іменам у таблиці адресації, що ви створюєте у відповідності до завдання. (у домені імена комп'ютерів не можуть повторюватися!)
- MAC-адреси віртуальних машин з серверами мають відрізнятися.
- На другому сервері у налаштуваннях IPv4 змінюємо адресу DNS сервера на адресу вашого першого сервера (DC-servers).

Створюємо ВМ **WS_G_N_1** відповідно до завдання. ОС ВМ – Windows 10 (за потреби можна використати одну з попередніх настільних версій Windows).

Включаємо **WS_G_N_1** до домену *surname.net*. Створюємо на першому контролері домену тестову групу користувачів **GR_G_N**, а в ній - нового користувача. Перевіряємо, чи вдається ввійти у систему робочої станції під новоствореним обліковим записом.

Завдання до лабораторної роботи

1. У середовищі програмного емулятора створіть проект комп'ютерної мережі (рис. 3.1).

2. Розробіть схему адресації пристроїв мережі. Для цього скористайтеся даними табл. 3.2. Під час розрахунку враховуйте, що для схеми використовується мережа /28 задана у таблиці 3.2.

Таблиця 3.2

Параметри для розрахунку у завданні №3.2

№ варіанта(N)	IP-адреса мережі	№ варіанта(N)	IP-адреса мережі	№ варіанта (N)	IP-адреса мережі
1	192.168.N.32/28	13	192.168.N.32/28	25	192.168.N.32/28
2	192.168.N.48 /28	14	192.168.N.48 /28	26	192.168.N.48 /28
3	192.168.N.64/28	15	192.168.N.64/28	27	192.168.N.64/28
4	192.168.N.80/28	16	192.168.N.80/28	28	192.168.N.80/28
5	192.168.N.96/28	17	192.168.N.96/28	29	192.168.N.96/28
6	192.168.N.112/28	18	192.168.N.112/28	30	192.168.N.112/28
7	192.168.N.128/28	19	192.168.N.128/28	31	192.168.N.128/28
8	192.168.N.144/28	20	192.168.N.144/28	32	192.168.N.144/28
9	192.168.N.160/28	21	192.168.N.160/28	33	192.168.N.160/28
10	192.168.N.176/28	22	192.168.N.176/28	34	192.168.N.176/28
11	192.168.N.192/28	23	192.168.N.192/28	35	192.168.N.192/28
12	192.168.N.208/28	24	192.168.N.208/28	36	192.168.N.208/28

3. Перевірте можливість інформаційного обміну між хостами мережі. У разі виявлення проблем зв'язку знайдіть та усуньте їх причини.

4. На сервері Serv_G_N_1 проведіть встановлення Active Directory, а сервер Serv_G_N_2 додайте у домен та надайте йому роль додаткового контролеру домену. Ім'я домену верхнього рівня - *surname*.net, де *surname* - ваше прізвище.

Примітка. На сервері Serv_G_N_2 також потрібно встановити роль *Active Directory Domain Services*, але на етапі вибору конфігурації розгортання (Deployment Configuration) замість *Add to a new forest* вибрати *Add a domain controller to an existing domain*.

5. Додайте у домен робочі станції. У разі браку ресурсів рекомендовано під'єднати меншу кількість робочих станцій, ніж у розробленій вами схемі адресації. Однієї робочої станції буде достатньо.

6. На сервері Serv_G_N_1 в Active Directory створіть тестову групу користувачів GR_G_N. В цій групі створіть нового користувача та, використовуючи цей обліковий запис, здійсніть вхід у систему з робочої станції.

Звіт має містити:

- схему адресації мережі;
- скриншоти та короткий опис основних кроків створення структури домену та перевірки можливості входу з-під одного з новостворених облікових записів.

Корисні посилання

Посібник з Active Directory для початківців
https://corewin.ua/blog/active-directory-delegation-tutorial-for-beginners/

Setting up Active Directory in VirtualBox
https://medium.com/@mando_elnino/setting-up-active-directory-in-virtualbox-part-1-windows-server-2019-d9ea8c70d3c
https://medium.com/@mando_elnino/setting-up-active-directory-in-virtualbox-part-2-windows-virtual-machine-9faf590f51b1

How To Enable Ping In Windows Server 2022 Firewall
https://www.rootusers.com/how-to-enable-ping-in-windows-server-2022-firewall/