Лабораторна робота №4

# Налаштування служби DNS у домені Active Directory

**Мета:** навчитися виконувати базове адміністрування служби DNS у домені Active Directory: налаштовувати DNS-сервери контролерів домену, забезпечувати їх взаємну відмовостійкість, а також конфігурувати механізм переспрямування (DNS Forwarding) для обробки запитів до зовнішніх доменів.

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

## Теоретичні відомості

У попередній лабораторній роботі було виконано розгортання доменної інфраструктури Active Directory на базі операційної системи Windows Server 2022. У процесі роботи створено домен surname.net та налаштовано два контролери домену, які забезпечують зберігання та реплікацію даних служби каталогів. Разом із встановленням контролерів домену було автоматично розгорнуто службу DNS, яка використовується Active Directory для зберігання службових записів та забезпечення пошуку мережевих ресурсів у межах домену.

Налаштована у попередній роботі DNS-інфраструктура забезпечує коректну обробку запитів до доменних імен внутрішнього домену. Водночас вона не виконує резолюцію імен публічних доменів мережі Інтернет, оскільки механізм переспрямування DNS-запитів (DNS Forwarding) ще не був налаштований.

Крім того, під час розгортання доменної інфраструктури налаштування DNS на другому контролері домену було виконано лише частково. Така конфігурація використовувалася для забезпечення коректного встановлення ролі контролера домену, проте для повноцінної та відмовостійкої роботи DNS-служби необхідно виконати остаточне налаштування параметрів DNS-серверів на обох контролерах домену.

У даній лабораторній роботі буде виконано завершальне налаштування служби DNS у домені Active Directory, а також реалізовано механізм переспрямування DNS-запитів до зовнішніх DNS-серверів для забезпечення резолюції публічних доменних імен.

Виконаємо «симетричне» налаштування DNS-адрес для серверу Serv-22-40-2 (DC2):

*Preferred DNS server: 127.0.0.1*

*Alternate DNS server: 192.168.40.243*

Нагадаю що налаштування DNS-адрес для серверу Serv-22-40-1 (DC1)

*Preferred DNS server: 127.0.0.1*

*Alternate DNS server: 192.168.40.244*

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 роботи служби імен та можливість взаємної реплікації DNS-даних між серверами.

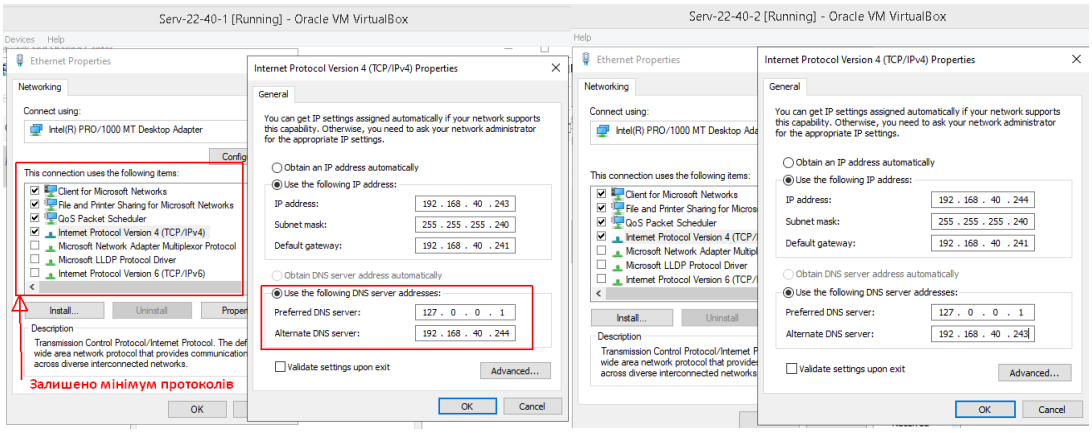



*Рис. 4.1. Зразок мережевих налаштувань серверів для NAT Network 192.168.40.240/28.*

**Налаштування переспрямування DNS-запитів (DNS Forwarding) у домені Active Directory**

Виконано налаштування внутрішніх DNS-серверів контролерів домену, що забезпечує коректну роботу Active Directory у межах локальної мережі. Ці DNS-сервери обробляють запити до доменних імен внутрішнього домену, створюючи та реплікуючи необхідні записи для контролерів домену та інших служб AD.

Водночас, у такій конфігурації DNS-сервери не здатні безпосередньо обробляти запити до публічних доменів Інтернету. Для забезпечення резолюції зовнішніх імен у Windows Server використовується механізм DNS Forwarding (переспрямування DNS-запитів).

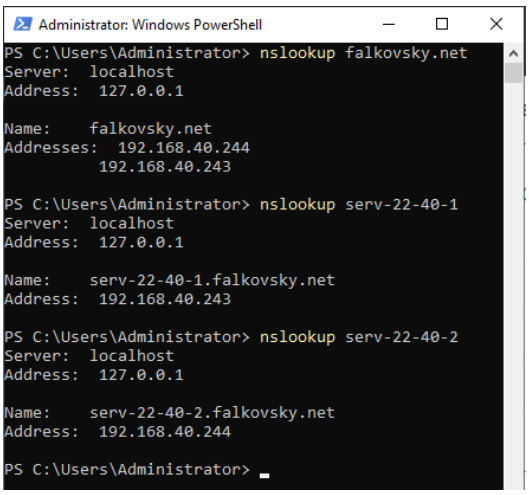



*Рис. 4.2.*

DNS Forwarder — це спеціальна конфігурація DNS-сервера, яка дозволяє переспрямовувати запити, які сервер не може розв'язати самостійно, на інші зовнішні DNS-сервери (наприклад, DNS провайдера або публічні DNS-сервери). У середовищі Active Directory Forwarder використовується для того, щоб внутрішні DNS-сервери могли обробляти запити до доменів Інтернету, не перешкоджаючи при цьому роботі внутрішніх зон домену.

Налаштування DNS Forwarder є важливим кроком для забезпечення повноцінної роботи мережі, адже дозволяє внутрішнім клієнтам і серверам домену коректно резолювати як внутрішні, так і зовнішні імена.

Відкриваємо на Serv-G-N-1 (DC1) системне меню Server Manager – Tools – DNS. У вікні DNS Manager знаходимо сервер Serv-G-N-1 у списку ліворуч. Клікаємо правою кнопкою на ім'я сервера Properties та переходимо на вкладку Forwarders (Переспрямування).

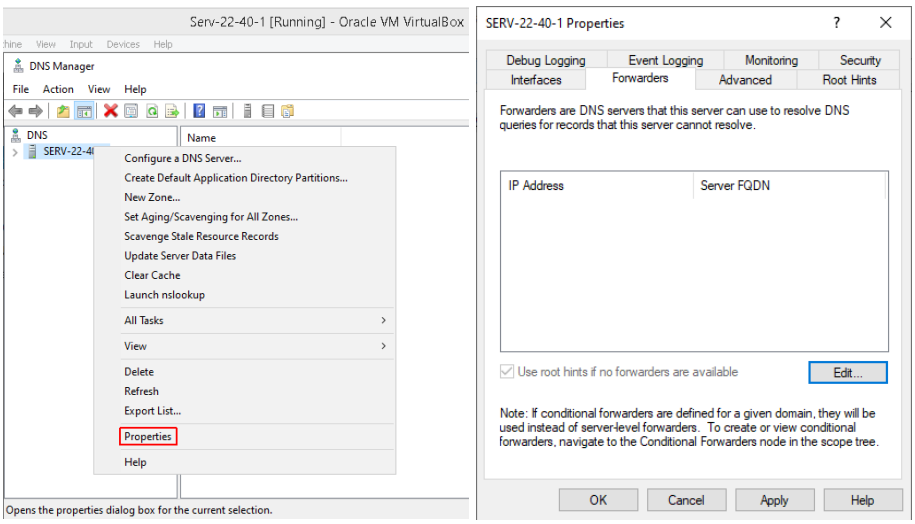



*Рис. 4.3. Server Manager – Tools – DNS – Serv-G-N-1 – Properties – Forwarders.*

Додаємо зовнішній DNS Forwarder – натискаємо кнопку Edit та вводимо IP-адресу зовнішнього DNS-сервера з наступного переліку:

| Провайдер | Основний ДНС | Резервний ДНС | Коментар |
|---|---|---|---|
| Ukrtelecom | 195.70.39.20 | 195.70.39.40 | |
| Kyivstar | 77.88.8.8 | 77.88.8.1 | |
| Volia | 95.108.200.200 | 95.108.200.201 | |
| Cloudflare | 1.1.1.1 | 1.0.0.1 | |

Натискаємо OK, щоб додати Forwarder та переконуємось, що у списку з'явився сервер.

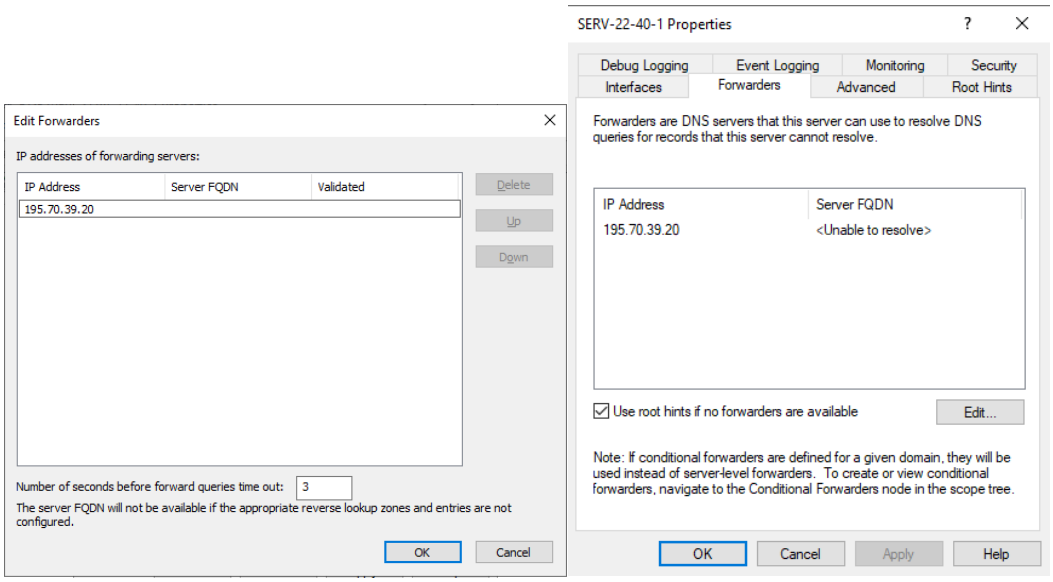



*Рис. 4.4. Додавання у якості Forwarders Ukrtelecom DNS на Server-22-40-1.*

Перевіряємо, що доданий Forwarder активний та не містить попереджень або повідомлень про помилки. Після цього виконуємо аналогічне налаштування на другому контролері домену.

Правильність виконаних налаштувань перевіряється за допомогою утиліти nslookup. У результаті DNS-сервер повинен успішно обробляти запити як до публічних доменів мережі Інтернет, так і до внутрішнього домену surname.net.

У лабораторному середовищі замість використання класичного механізму DNS Forwarding інколи застосовується альтернативний підхід, за якого у налаштуваннях DNS-серверів або мережевих адаптерів вказується адреса шлюзу NAT Network як транслятора DNS-запитів.

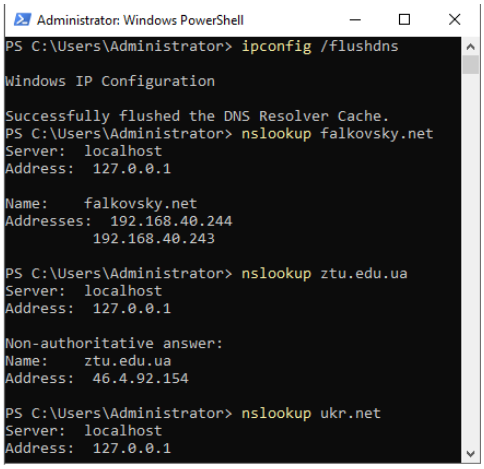



*Рис. 4.5. Очистка кешу ДНС та nslookup*

У такому випадку DNS-запити, які не можуть бути оброблені локальним DNS-сервером домену, передаються на мережевий шлюз. Шлюз, у свою чергу, виконує функцію DNS-проксі та переспрямовує ці запити до зовнішніх DNS-серверів мережі Інтернет. Такий механізм часто використовується у віртуалізованих середовищах (наприклад, VirtualBox або VMware), де NAT-шлюз забезпечує доступ віртуальних машин до зовнішньої мережі.

Проте слід враховувати, що подібна конфігурація не є повноцінною заміною механізму DNS Forwarder, який реалізований безпосередньо у службі DNS Windows Server. Крім того, можливість використання шлюзу як транслятора DNS-запитів залежить від політики мережі та налаштувань інтернет-провайдера. У деяких випадках провайдер може обмежувати або фільтрувати DNS-запити, що надсилаються на сторонні сервери, дозволяючи використання лише власних DNS-серверів.

З цієї причини у виробничих мережах рекомендується застосовувати стандартний механізм DNS Forwarding, що забезпечує більш передбачувану та стабільну роботу служби DNS.

**Завдання до лабораторної роботи**

1. Виконайте остаточне налаштування параметрів DNS на контролерах домену та забезпечте їх симетричну конфігурацію для підвищення відмовостійкості служби DNS.
2. Налаштуйте механізм DNS Forwarding на DNS-серверах домену для забезпечення обробки запитів до зовнішніх доменів мережі Інтернет.
3. Перевірте коректність роботи DNS-служби за допомогою утиліти nslookup, виконавши запити до внутрішнього домену та до кількох публічних доменів.
4. Проаналізуйте результати виконаних налаштувань та переконатися у коректній роботі DNS-інфраструктури домену.
5. Доповніть звіт скріншотами виконання команд:
   nslookup surname.net, nslookup serv-G-N-1, nslookup serv-G-N-1, nslookup ztu.edu.ua

**Звіт має містити:**
- скриншоти та короткий опис основних кроків виконання завдань.

**Корисні посилання**

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

Windows Server. DNS Forwarding
https://learn.microsoft.com/en-us/windows-server/networking/dns/forwarding

How To Properly Setup DNS Forwarders On Windows Server
https://serverfault.com/questions/583247/how-to-properly-setup-dns-forwarders-on-windows-server

Thoughts on DNS forwarders. Needed or not?
https://www.reddit.com/r/sysadmin/comments/1ay3079/thoughts_on_dns_forwarders_needed_or_not/