Лабораторна робота №7

Налаштування DNS-сервера на основному контролері домену Active Directory

Мета: навчитися інтерпретувати та змінювати основні налаштування DNSсервера на основному контролері домену в Active Directory (на прикладі Windows Server 2022).

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №3-6.

Теоретичні відомості та завдання до лабораторної роботи

DNS: основні поняття

DNS (*Domain Name System*, доменна система імен) - це ієрархічна децентралізована система імен для комп'ютерів, служб та інших мережних ресурсів.

На DNS-сервері зберігається перелік записів, які ставлять у відповідність доменним іменам конкретні IP-адреси. Використовуються записи різних типів (зокрема A, AAA, CNAME, MX, NS, PTR, SOA, SRV тощо). Деякі з цих типів буде розглянуто далі у цій роботі.

Зона DNS - частина простору імен, для якого DNS-сервер може виконувати операції з перетворення імен (*name resolution*).

Важливо. Зона не є тотожною домену. У межах одного домену зон DNS може бути декілька. Але якщо домен невеликий, то він може мати й одну зону.

Розрізняють зону прямого перегляду і зону зворотного перегляду.

Зона прямого перегляду (*forward lookup zone*) використовується для перетворення доменного імені в IP-адресу (є доменне ім'я - за ним треба одержати IP-адресу). Це пряме перетворення імені.

Зона зворотного перегляду (*reverse lookup zone*) використовується для перетворення IP-адреси у доменне ім'я (є IP-адреса - за нею треба одержати доменне ім'я). Це зворотне перетворення імені.

Сервер імен (*name server*, *NS*) - сервер, на якому зберігаються DNSзаписи. Серверів імен може бути декілька.

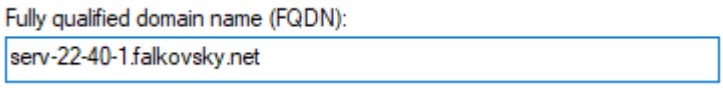
У налаштуваннях Active Directory абревіатурою NS позначаються *авторитетні сервери імен*.

Авторитетний сервер імен (*authorative name server*) - сервер імен, записи якого вважаються найбільш достовірними у домені на противагу записам інших серверів імена, котрі можуть бути кешованою версією записів авторитетного сервера. Тільки такі сервери можуть повертати авторизовані відповіді.

Абсолютні доменні імена записуються у форматі FQDN.

FQDN (*Fully Qualified Domain Name*) - повне доменне ім'я, яке визначає точне розташування ресурсу в ієрархічній структурі DNS.

Наприклад:



Деякі типи DNS-записів

Запис A (*A host address*) ставить у відповідність текстовому імені ресурсу IP-адресу цього ресурсу за протоколом IPv4.

Запис AAAA (*AAAA host address*) ставить у відповідність текстовому імені ресурсу IP-адресу цього ресурсу за протоколом IPv6.

Запис CNAME є псевдонімом, що перескеровує з одного імені (псевдоніму) на інше.

Прикладом використання запису *CNAME* є присвоєння псевдоніму спільному мережному ресурсу (наприклад, вебсерверу, файловому серверу тощо), який би дозволив звертатися до цього ресурсу за коротшим і зручнішим ім’ям, ніж його доменне ім’я.

Запис NS (*Name Server*) містить ім'я авторитетного сервера імен (таких записів може бути декілька - для кожного авторитетного сервера окремий).

Запис SOA (*Start of Authority*) містить адміністративну інформацію про дану зону.

До такої адміністративної інформації, зокрема, належать наступні відомості:

первинний сервер (*primary server*, головний авторитетний сервер, на якому може відбуватися зміна DNS-записів, після чого решта серверів імен також оновлюють свої записи відповідним чином);

інтервал оновлення (*refresh interval*, часовий проміжок, через який вторинні сервери імен повинні надіслати первинному серверу імен запит на виявлення можливих змін у зоні DNS);

інтервал повторення (*retry interval*, часовий проміжок, через який вторинні сервери імена мають повторити запит на виявлення можливих змін у зоні DNS, якщо первинний сервер не відповідає; цей інтервал має бути меншим за інтервал оновлення);

дійсний до (*expires after*, часовий проміжок, через який вторинні сервери повинні припинити відповідати на запити, пов'язані з даною зоною DNS, якщо первинний сервер не відповідає; цей інтервал має бути більшим за суму інтервалу оновлення та інтервалу повторення).

Запис PTR (скорочення від *pointer* - вказівник) автоматично створюється в зоні зворотного перегляду для кожного запису A чи AAAA із зони прямого перегляду.

Встановлення ролі DNS-сервера в Active Directory

Часто роль DNS-сервера в Active Directory вже встановлено. Якщо ж її потрібно встановити, виконайте наступну послідовність кроків.

1. У вікні *Server Manager* на панелі Dashboard виберіть опцію *2 Add roles and features*. (рис. 7.1).

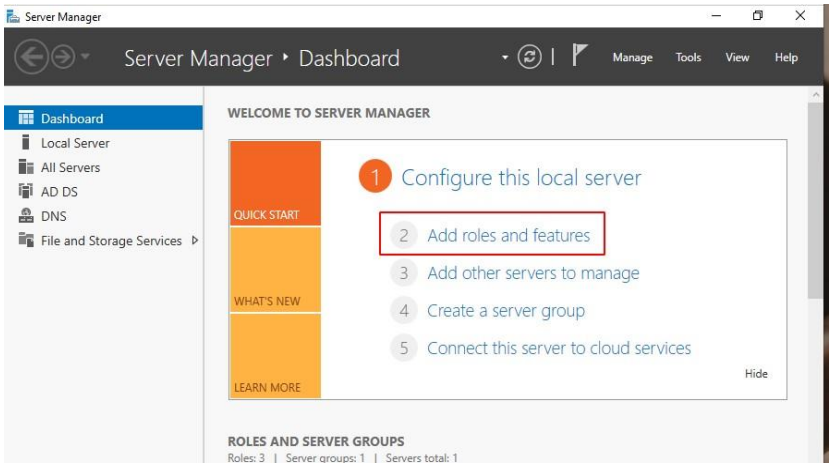


Рис. 7.1

2. Оберіть опцію *Role-based or feature-based installation* (рис. 7.2).

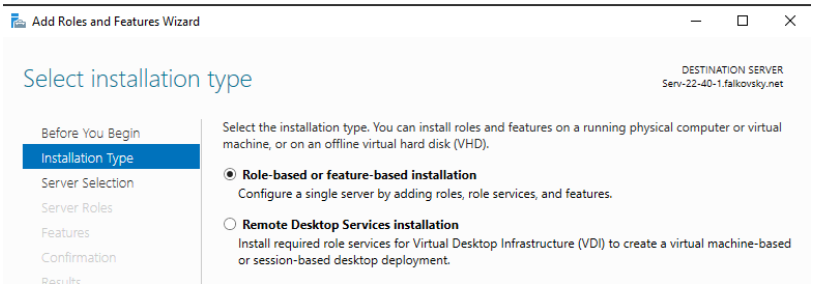


Рис. 7.2

3. Вкажіть сервер домену, на якому необхідно встановити роль DNSсервера. На рис. 7.3 це основний контролер домену.

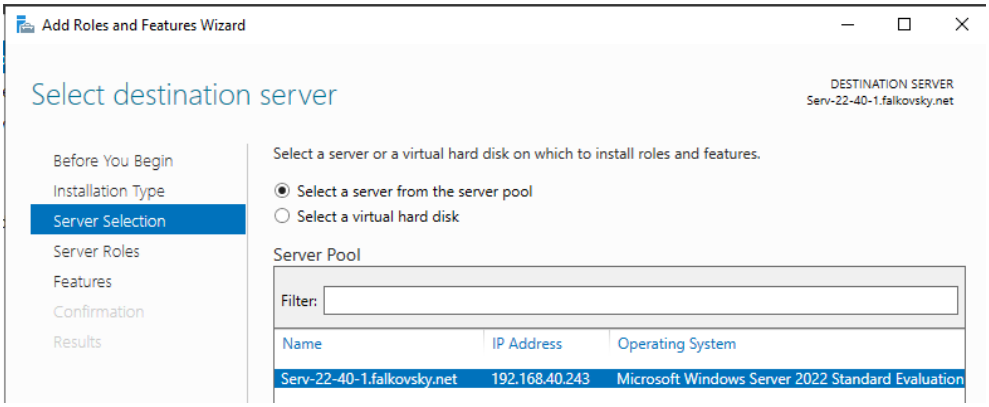


Рис. 7.3

4. Оберіть роль, яку необхідно довстановити - у даному випадку це роль *DNS Server*. Якщо роль вже встановлено, опцію буде обраною і неактивною, як на рис. 7.4. В іншому разі встановіть прапорець навпроти опції.



Рис. 7.4

5. Якщо роль DNS Server встановлена, але відповідні меню на сервері відсутні, виконайте у PowerShell з правами адміністратора домену команду

Install-WindowsFeature -Name RSAT-DNS-Server

```
PS C:\Users\Administrator> Get-WindowsFeature -Name DNS

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] DNS Server                                          DNS                            Installed


PS C:\Users\Administrator>
PS C:\Users\Administrator> Install-WindowsFeature -Name RSAT-DNS-Server

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {DNS Server Tools}
```

Рис. 7.5

<u>Завдання №7.1</u>. Довстановлення ролі DNS-сервера (за потреби)

1. Запустіть основний контролер вашого домену і перевірте, чи встановлено на ньому роль DNS-сервера. Якщо ні - встановіть.

<u>Звіт має містити</u> скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

<u>Оснащення *DNS Manager*</u>

Основний функціонал, пов'язаний з налаштуваннями DNS-сервера у Windows Server, міститься в оснащенні *DNS Manager* (меню *Tools* -> *DNS*, рис. 7.5).

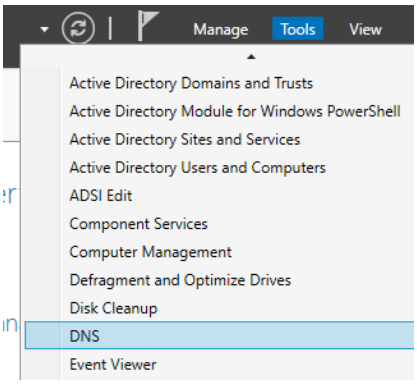


Рис. 7.6

Вікно оснащення *DNS Manager* має вигляд, подібний до зображеного на рис. 7.7.

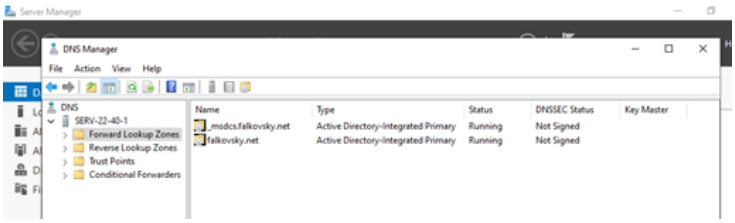


Рис. 7.7

Завдання №7.2. Дослідження наявних налаштувань DNS-сервера

1. Запустіть оснащення *DNS Manager*.
2. Дослідіть наявні налаштування DNS у вашому домені. Перегляньте основні записи в домені (для перегляду подробиць двічі клацніть по відповідному запису). Дайте відповіді на наступні запитання (можуть бути наявні не всі типи записів):

- Чи створено в домені зону прямого перегляду? зону зворотного перегляду?
- Чи є у домені записи типу A? Які повні доменні імена та IP-адреси вказані у цих записах.
- Чи є у домені записи типу AAAA? Які повні доменні імена та IP-адреси вказані у цих записах.
- Чи є у домені записи типу NS? Які доменні імена та IP-адреси відповідають серверам із цих записів?
- Чи є у домені записи типу SOA? Який із серверів домену є первинним? Які значення задано для інтервалів оновлення, повторення та поля *дійсний до*?
- Чи є у домені записи типу PTR? Яким записам типу A (AAAA) вони відповідають?

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Створення DNS-запису для маршрутизатора

Зазвичай DNS-запис для маршрутизатора початково відсутній і за замовчуванням не створюється. Створення такого запису для порту маршрутизатора, що виконує роль шлюзу за замовчуванням, допоможе на практиці побачити, як створюється новий DNS-запис.

1) З'ясуйте адресу порту маршрутизатора, що виконує роль шлюзу за замовчуванням у вашій мережі. У прикладі це буде адреса 192.168.40.241 за протоколом IPv4 (рис. 7.8). Тобто створювати будемо DNS-запис типу A.

```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.40.243
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 192.168.40.241
PS C:\Users\Administrator>
```

Рис. 7.8

2) Зараз шлюз за замовчуванням може пінгуватися безпосередньо за IPадресою (все одно не пінгуватиметься, якщо ви використовуєте внутрішню мережу VirtualBox). Але пінгування за ім'ям *router* буде завершуватися помилкою, так і не розпочавшись. Наприклад, так:

```
PS C:\Users\Administrator> ping router
Ping request could not find host router. Please check the name and try again.
```

3) Додамо DNS-запис для порту маршрутизатора, що є шлюзом за замовчуванням для даної мережі. У контекстному меню домену виберіть пункт *New Host (A or AAAA)...* (рис. 7.9).

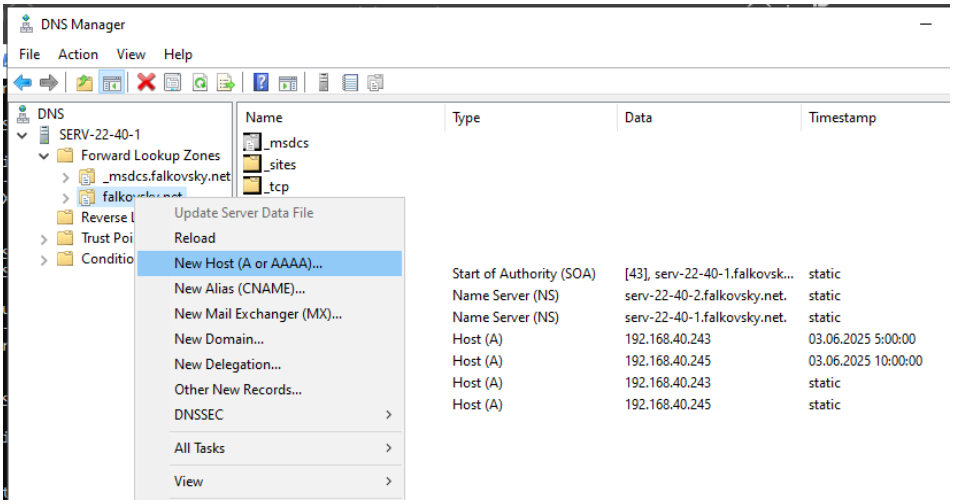


Рис. 7.9

4) У вікні *New Host* (рис. 7.10) вкажіть відносне доменне ім’я для маршрутизатора, зазначте IP-адресу шлюзу за замовчуванням та натисніть *Add Host*.

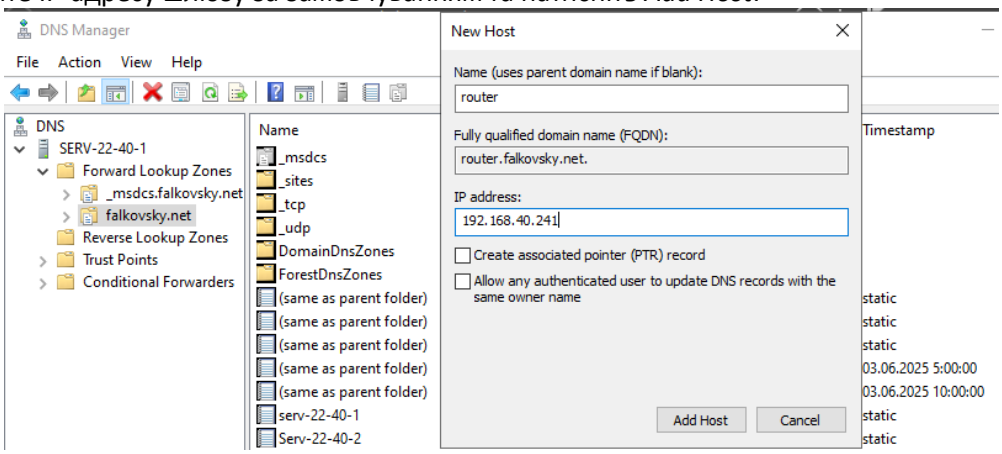


Рис. 7.10

5) Відповідний DNS-запис з’явиться у переліку DNS-записів домену.
6) Здійсніть повторне пінгування шлюзу за замовчуванням через доменне ім’я:

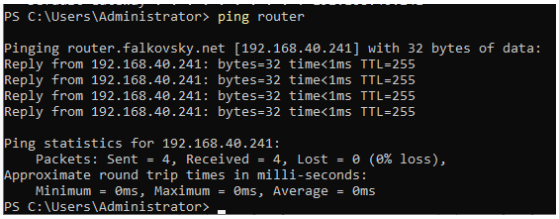


Рис. 7.11

Пінг по імені router працює, оскільки в DNS-сервері був створений A-запис (типу Host), який зв'язує ім'я router з IP-адресою 192.168.40.241.

Коли комп’ютер виконує команду ping router, він спочатку надсилає DNS-запит для визначення IP-адреси, що відповідає імені router.

DNS-сервер відповідає згідно з наявним A-записом, вказуючи на IP-адресу 192.168.40.241. Після цього вже здійснюється ICMP (ping) запит до цієї IP-адреси.

- Ім’я router → DNS-запит → DNS-сервер повертає 192.168.40.241 (завдяки A-запису).

- Потім: ping 192.168.40.241 → якщо IP активний і не блокує ICMP — отримуємо відповідь.

Без запису в DNS або відсутності альтернативних джерел (файл hosts, NetBIOS) ім'я router не могло б бути резольвованим, і пінг завершився б помилкою "Ping request could not find host".

<u>Завдання №7.3</u>. Створення DNS-запису для маршрутизатора

1) Перевірте, чи успішним є пінгування з контролера домену маршрутизатора за доменним ім'ям *router*.

2) Створіть у вашому DNS-запис для порту маршрутизатора, що відповідає шлюзу за замовчування у вашій моделі мережі.

3) Повторіть п. 3 і переконайтеся, що перетворення доменного імені *router* у відповідну IP-адресу було коректним.

<u>Звіт має містити</u> скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

<u>Створення зони зворотного перегляду</u>

Наявність зони зворотного перегляду може знадобитися для коректної роботи окремих служб. Розглянемо приклад створення зони зворотного перегляду у домені *holovnia.net*.

1) У вікні оснащення *DNS Manager* виберіть *Action* → *New Zone* (рис. 7.12).
2) Запуститься майстер створення нової зони (рис. 7.13).

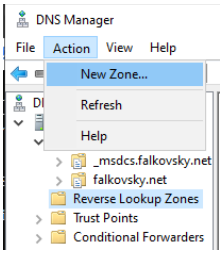


Рис. 7.12



Рис. 7.13

3) Оберіть первинну зону (*primary zone*), щоб майбутню зону зворотного перегляду було створено на поточному сервері (рис. 7.14).

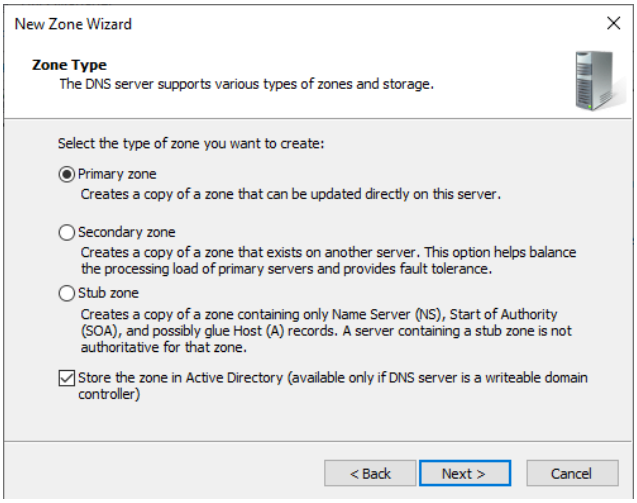


Рис. 7.14

4) Оберіть зону реплікації для створюваної зони DNS - у даному випадку це опція *To all*

DNS domain controllers in this domain..., тобто буде відбуватися реплікація даних з цієї зони DNS на всіх DNS-серверах, організованих на контролерах домену (рис. 7.15). У створюваній нами моделі мережі таких контролерів і, відповідно, DNS-серверів буде два.

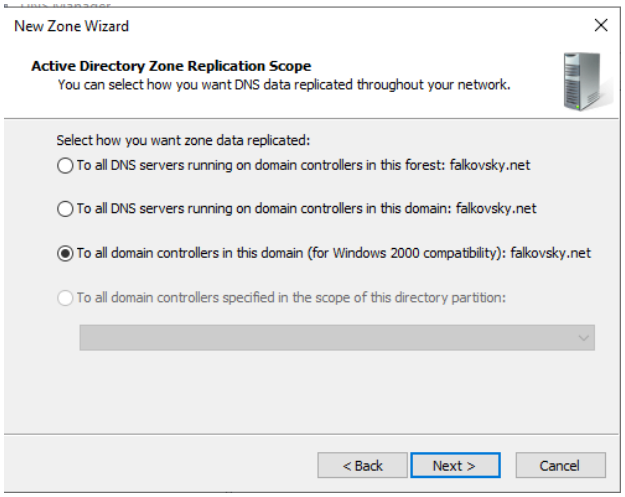


Рис. 7.15

5) Вкажіть, яка версія протоколу IP буде використовуватися у створюваній зоні зворотного перегляду. У даній мережі застосовується протокол IPv4 (рис. 7.16).

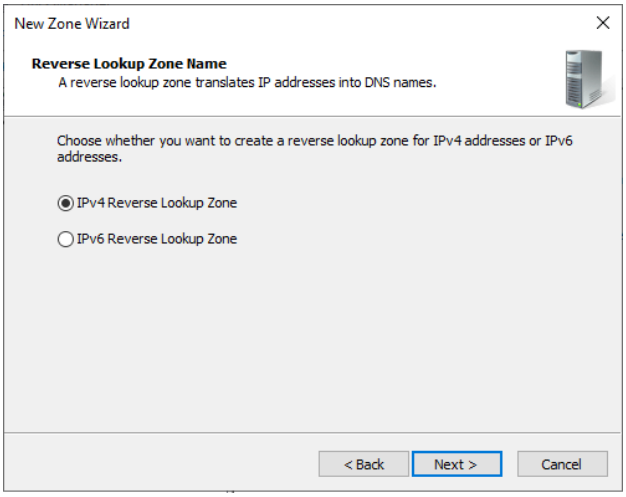


Рис. 7.16

6) Дайте ім'я створюваній зоні зворотного перегляду. Це можна зробити, вказавши адресу мережі або безпосередньо задавши ім'я зони зворотного перегляду. На рис. 7.17 введено адресу мережі. Тоді ім'я зони зворотного перегляду згенерується автоматично і буде таким, як прописано в неактивному полі в нижній частині вікна (рис. 7.17): 40.168..in-addr.arpa.

Зверніть увагу, як утворюється ім'я зони зворотного перегляду. Октети адреси мережі пишуться у зворотній послідовності, а далі записується *in-addr.arpa*.

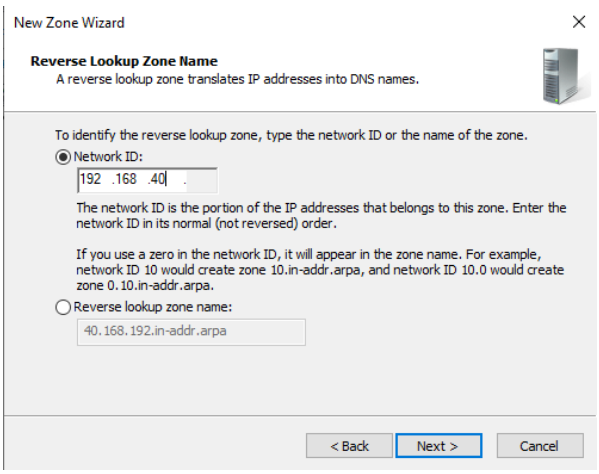


Рис. 7.17

7) Налаштуйте динамічне оновлення створюваної зони DNS. Оберіть *Allow only secure dynamic updates*, щоб здійснювалися лише безпечні динамічні оновлення (рис. 7.18). Тоді такі оновлення будуть відбуватися лише з довірених джерел (рекомендоване налаштування).

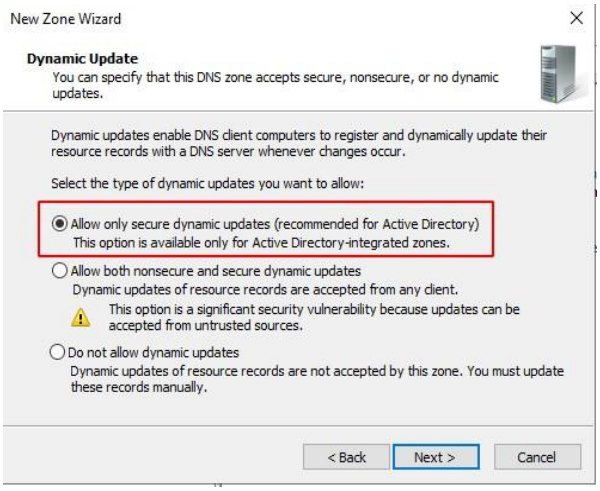


Рис. 7.18

8) Створення зони зворотного перегляду завершене (рис. 7.19).

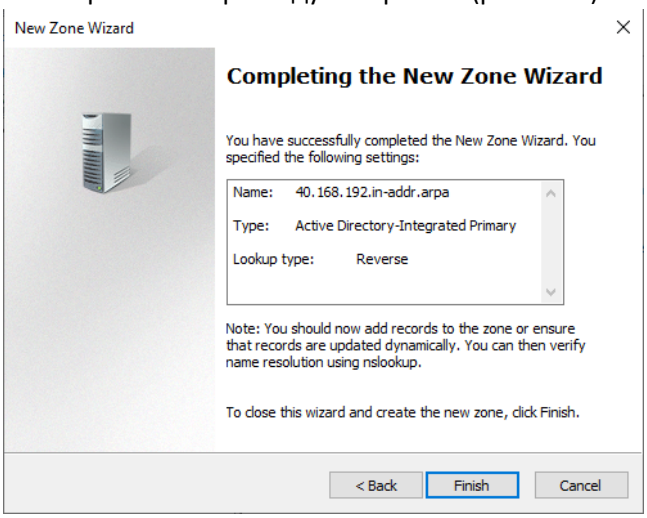


Рис. 7.19

9) Ініціюємо реєстрацію DNS-записів основних ресурсів. У нашому випадку це стосується реєстрації DNS-серверів у зоні зворотного перегляду. Для цього на контролері домену введемо команду ipconfig /registerdns. У разі успішного виконання одержимо вивід, подібний до зображеного на рис. 7.20.

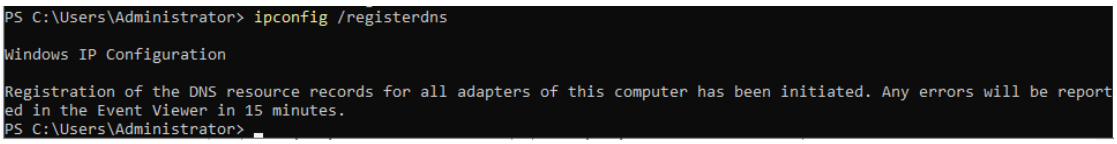


Рис. 7.20

10) Перевіримо ефективність виконаних налаштувань. Для цього ввійдемо в систему на одній з робочих станцій домену і введемо команду nslookup, у ролі аргументу вказавши IP-адресу контролера домену, на якому налаштовували DNS-сервер.

Якщо налаштування успішні, то результат роботи команди nslookup буде подібний на той, що зображений на рис. 7.21.

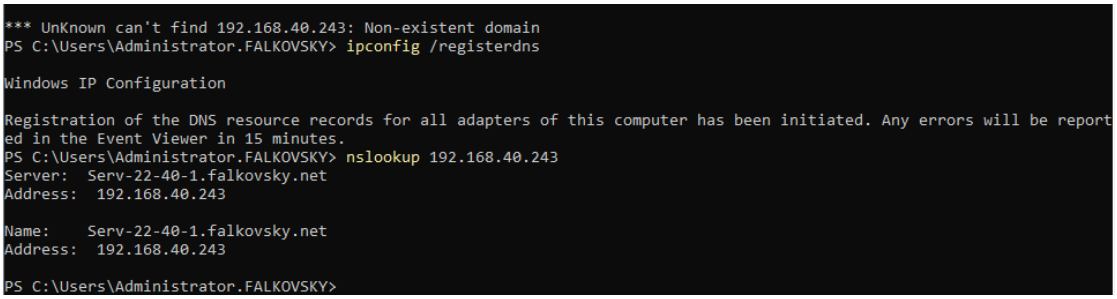


Рис. 7.21

Перші два рядки показують ім’я сервера, з якого одержано дані, а останні два рядки - відомості про ресурс, який міститься за заданою адресою. На рис. 7.21 DNS-сервер надав відомості сам про себе.

Завдання №7.4. Створення зони зворотного перегляду

1. За допомогою оснащення *DNS Manager* переконайтеся, що зону зворотного перегляду ще не створено.

2. Створіть зону зворотного перегляду на DNS-сервері, що працює на основному контролері домену. Поки що не виконуйте команду ipconfig /registerdns.

3. За допомогою оснащення *DNS Manager* перегляньте новостворену зону зворотного перегляду. Чи відображаються у ній DNS-записи для серверів?

4. З командного рядка запустіть реєстрацію DNS-записів основних ресурсів. Чи відображаються DNS-записи для серверів у зоні зворотного перегляду тепер?

5. За допомогою команди nslookup перевірте, що зона зворотного перегляду налаштована успішно.

Звіт має містити скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 7.1-7.4.

Рекомендовані джерела

1. M. Henderson, J. Krause. Windows Server 2019 Cookbook Second Edition (Second Edition). Packt Publishing, 2020 (p. 82).
2. Gilbert Held. Windows Networking Tools: The Complete Guide to Management, Troubleshooting, and Security. CRC Press, 2013 (команда *nslookup*).