Лекція 4

DNS в Active Directory

План

1. DNS: основні поняття
2. Основні типи DNS записів в Active Directory

1. 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, AAAA, CNAME, MX, NS, PTR, SOA, SRV тощо).

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.

1. DNS: основні поняття

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 DNS-записи. Серверів імен може бути декілька.

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

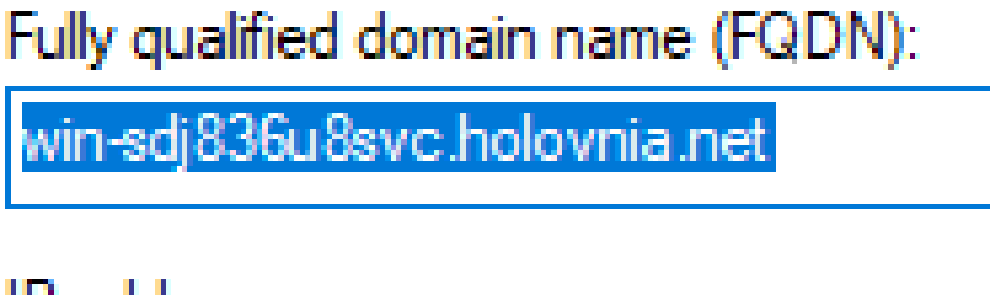
Авторитетний сервер імен (*authorative name server*) - сервер імен, записи якого вважаються найбільш достовірними у домені на противагу записам інших серверів імена, котрі можуть бути кешованою версією записів авторитетного сервера. Тільки такі сервери можуть повертати авторизовані відповіді.

1. DNS: основні поняття

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:



2. Основні типи DNS-записів в Active Directory

Розглянемо основні типи DNS-записів, які використовуються в Active Directory.

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

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

2. Основні типи DNS-записів в Active Directory

До адміністративної інформації в SOA, 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).